Bounds of Falcon's Fast Fourier Sampler with Fixed-Point Arithmetic (Draft v0.1)

Vincent Hwang
Boston, USA
vincentvbh7@gmail.com

November 15, 2026

Abstract

Falcon was selected by NIST for standardization as FN-DSA in the forthcoming FIPS 206, and its signature generation is driven by the fast Fourier sampler, defined over the complex numbers. This report bounds the Rényi divergence between the sampler in real arithmetic and its fixed-point implementation, on the tail-cut event, where every sample stays within a fixed number of standard deviations of its center. For a reference bit security $\lambda = 128$ at $n = 512$ and $\lambda = 256$ at $n = 1024$ over 2^{64} signatures, the bound keeps 126.28 and 248.78 bits at the plain center, and 126.70 and 253.53 bits at the fractional center, for every key the key generation accepts. The floating-point signer's analysis is left open: it stopped at a numerical contradiction while closing its hypotheses.

We propose four changes to the fixed-point implementation. (i) The one-dimensional sampler SamplerZ rejects a candidate at a saturated shift instead of saturating the shift. (ii) The key generation runs three new checks on the tree: it bounds the largest relative deviation of a leaf standard deviation, the multiplicative perturbation of the tree map, and the largest remainder on the tail-cut event. The first two changes carry the proof: dropping (i) costs the saturated leaves' term, and dropping (ii) leaves no security level at any number of signatures for our proof. (iii) The root node is computed with the NTRU identity, and (iv) an inversion followed by a multiplication becomes a division; these two simplify the proofs.

The bits rest on machine-checked proofs and on three code-alignment hypotheses. The sampler's kernels and its recursion are proved in CryptoLine on the aarch64 objects of the C code, compiled at `-O3` and traced under QEMU's Cortex-A72, and composed in Lean. The analysis is carried in Lean where its model reaches, every proof line it does not reach recorded as such, and the Lean theorems take the summability of their series as a hypothesis. The bound samples nothing.

This report was written with agents under the human author's detailed guidance, a blend of formal verification of machine code, the Rényi divergence argument of lattice sampling, and the engineering of an agent harness; the tree map's perturbation is a multiplicative one, in the sense of relative perturbation theory. The compiled objects have known timing side channels: in the key generation's arithmetic the compiler turned constant-time C into key-dependent branches in the Cortex-A72 build, so that arithmetic is verified on the object compiled for the Apple M1, which selects, and a branchless assembly reference is future work with the agents.

Keywords: Falcon, fast Fourier sampling, Rényi divergence, formal verification, lattice-based signatures, AI agents

Contents

1 Introduction **4**
1.1 The theorems 5

2 Provenance, gates and machine-checked proofs **10**
2.1 How a claim is backed . . . 10
2.2 Machine-checked proofs . . . 12
2.3 The agents' doctrine . . . 13

3 Definitions and notation **14**
3.1 The numbers and the arithmetic . . . 14
3.2 The fast Fourier sampler and the tree of a key . . . 17
3.3 The objects of the main theorem . . . 31

4 The roadmap of the proof **33**
4.1 The end result and its terms . . . 34
4.2 The divergence at one leaf . . . 35
4.3 Composition and probability preservation . . . 37
4.4 The fringe extension . . . 38
4.5 The Falcon-type signer . . . 39

5 Instantiations **49**
5.1 The bit security over Q_s signatures . . . 49
5.2 The checked key . . . 52
5.3 The bounds on ffSampling$^{\mathcal{F}}$ . . . 55
5.4 The changes . . . 59
5.5 The losses . . . 62
5.6 Comparison with the fixed-point analysis . . . 64

A Definitions and notation **68**
A.1 The primitives . . . 69
A.2 The realization . . . 70
A.3 Relations on approximation . . . 73
A.4 The fast Fourier sampler . . . 74
A.5 The objects of the main theorem . . . 84
A.6 The tree . . . 87
A.7 The Rényi divergence argument . . . 89
A.8 The facts the proofs use . . . 92

B The relative form of a modulus bound, the complex operations, the split butterfly's even half, and the tail of a sum of offsets **97**
B.1 The relative form of a deviation bound . . . 98
B.2 The complex operations . . . 99
B.3 The split butterfly . . . 103
B.4 The tail of a sum of discrete Gaussian offsets . . . 104

C The arithmetic and harmonic means **107**
C.1 Compositions of the arithmetic and harmonic means . . . 108

D Proofs of the tree **111**
D.1 The child's diagonals as means . . . 112
D.2 The Gram form . . . 115
D.3 Exact structure of the diagonals . . . 120

E Proofs of the Rényi divergence argument **130**
E.1 The divergence at one leaf . . . 130
E.2 The normalizer ratio to second order . . . 132
E.3 Composition along the samples . . . 150
E.4 Probability preservation . . . 155
E.5 The base sampler's divergence at a leaf . . . 162

F Proofs of the theorem **163**

G Proofs of Section 4.5 **185**
G.1 The relative form and the rounding factors . . . 186
G.2 The tree map and the output measures . . . 190
G.3 Elementary bounds under a realization . . . 200
G.4 The computed diagonals . . . 223
G.5 The centers . . . 260
G.6 The base sampler under $\mathcal{F}$ . . . 291
G.7 The terms of $\ln R$ . . . 316
G.8 The tail of the leaf sum . . . 347

H Proofs of Section 5 **354**
H.1 The bit security over Q_s signatures . . . 354
H.2 The induced form, the computed FFT entry, the checked key's bounds and the acceptance word . . . 360

I The fixed-point signer **410**
I.1 The realization . . . 413
I.2 The checked key . . . 453
I.3 The tree at $u = 0$ . . . 453
I.4 The base sampler's perturbation budget in $\mathcal{F}_{\mathrm{fx}}$ . . . 552
I.5 The terms of $\ln R$ . . . 556
I.6 $\mathrm{ffSampling}^{\mathcal{F}}(B, s, t)$ . . . 606
I.7 $\mathrm{ffSampling}^{\mathcal{F}}(B, s, t_{\mathrm{frac}})$ . . . 621
I.8 The tail checks' hypothesis . . . 641
I.9 The result . . . 643

J The floating-point signer: `c-fn-dsa` **649**
J.1 The realization . . . 652
J.2 The key . . . 690
J.3 The tree and the centers at $\zeta = 0$ . . . 696
J.4 The base sampler's perturbation budget . . . 704
J.5 The loss . . . 723
J.6 The gates, the machine-checked proofs and the imported facts . . . 747

K The relative-error lemma **749**

L Indexes: the Lean theorems, the routines and the definitions **755**

M The gates, the machine-checked proofs and the imported facts **786**
M.1 The gates . . . 786
M.2 The machine-checked proofs . . . 788
M.3 Provenance of every imported fact . . . 790
M.4 Conditions . . . 790
M.5 What is not gated . . . 791

M.6 The dependency graphs 791

1 Introduction

Falcon [FHK+20] is a lattice-based post-quantum digital signature. NIST selected it for standardization in 2022, at the end of the third round of its post-quantum process, with three other schemes [AAC+22]; two of them, ML-KEM and ML-DSA, became FIPS 203 and 204 on August 13, 2024 [NIS24b, NIS24a], and Falcon is to become FN-DSA in the forthcoming FIPS 206 [NIS26]. On September 28, 2026, NIST presented on its forum a new plan for FN-DSA, which specifies fixed-point arithmetic in both key generation and signing, and asked the community for feedback on it, in light of the fixed-point implementation published at CRYPTO [BFLP26] and Pornin's implementation [Por26] [NIS26]. In the signature generation, Falcon samples a signature with the fast Fourier sampler over the complex numbers [DP16], converting the high-dimensional sampling into several one-dimensional samplings. The security proof relies on the idealized sampler over the complex numbers, while the program approximates each complex number with finite computer arithmetic; we want to settle how many bits of security the approximation costs.

The arithmetic. On modern computers, complex arithmetic is implemented with computer arithmetic defined over finite storage. Typical approaches include floating-point arithmetic such as IEEE binary64, and fixed-point arithmetic. In the literature, there are various instruments, claims and conditional statements on the bit security losses between the formulation over the complex numbers and the ones implemented by computer programs. The Rényi divergence argument bounds the precision loss of the Klein sampler through relative error bounds [Pre17]; [FGdG+26] carry the analysis of the idealized Klein sampler over to the fast Fourier sampler; the isochronous sampler implemented in Falcon comes with its own security and timing analysis of the one-dimensional sampler [HPRR20]; the fixed-point implementation samples at the fractional center and carries an absolute-error version of the Rényi argument in place of the relative one of the binary64 analyses, under several assumptions [BFLP26].

This report. This report bounds the Rényi divergence between the idealized fast Fourier sampler and its fixed-point implementation, for every key the key generation accepts, and turns the bound into bits of security over 2^{64} signatures. The bound rests on machine-checked proofs of the arithmetic's kernels and of their composition, and on three hypotheses of code alignment; the author is on the way to closing the assurance at the machine-code level. We make four changes to the fixed-point implementation: the rejection at the one-dimensional sampler, the three key checks, the root node computed with the NTRU identity, and a division in place of an inversion followed by a multiplication. The first two carry the proof; the last two simplify it.

The rejection at the one-dimensional sampler. The reference accepts a candidate whose exponent si reaches 64 with the shift saturated at 63, so its acceptance probability is 2^{si-63} times the ideal one, a factor that grows with the exponent (Definition J.55, $\bar{U}$). The fixed-point signer rejects such a candidate (Definition I.20, item 1). Every fringe set is then empty (Lemma G.80) and the fringe leaves' term of the bit security vanishes (Theorem 5.11, item 4).

Key check 1: the leaf standard deviations. The key generation bounds the largest relative deviation $\bar{\delta}_K$ of a leaf standard deviation (Definition 4.12, item 1) by the threshold D_n. This check fixes the input $\bar{\delta}$ (Definition A.27) of Theorem 1.1 (Theorem 5.12, item 1), where BFLP26, Thm. 1 assumes it.

Key check 2: the leaf centers. The key generation bounds the largest remainder $\bar{B}_K$ of the leaf sum on the tail-cut event (Definition 4.12, item 3) by the threshold B_n. This check bounds the

roundings' part of the leaf centers' shift (Lemma 4.14), and η is subtracted from the bit security for the event outside the bound (Theorem 5.12, items 2 and 3).

Key check 3: the tree map's perturbation. Let $\mathcal{L}$ be the tree map and $\widetilde{\mathcal{L}}$ the computed one. $K := \widetilde{\mathcal{L}}^{-1}\mathcal{L} - I_N$ is the multiplicative perturbation of the tree map (Definition 4.12; [EI93]). The key generation bounds the weighted square sum μ_{key} of K (Definition 4.12, item 2) by the threshold M_n. This check bounds the leaf centers' shift (Lemma 4.14), where BFLP26, Thm. 1 assumes it.

1.1 The theorems

The main result. Three theorems, in layers. Theorem 1.1, the core: in a realization $\mathcal{F}$ of $\mathbb{R}$ with a relative and an absolute perturbation, ffSampling$^{\mathcal{F}}$ is, on a sub-event S' of its tail-cut event S, within Rényi divergence $R\,(1 - P(S'^c))^{-\alpha/(\alpha-1)}$ of ffSampling$^{\mathbb{R}}$, with $\ln R$ four explicit terms. A sharper bound comes with a more involved statement and proof: Theorem F.4 (Appendix F) takes the suprema of Definition A.30 where Theorem 1.1 takes explicit bounds. Theorem 1.2, the wrapper: a divergence bound on the sampler keeps $\lambda_{\mathcal{F}}$ of λ bits over Q_s signatures against the adversary's event (Definition 5.1). Theorem 1.3: the fixed-point signer of Appendix I keeps $\lambda_{\mathcal{F}}$ bits of λ at both centers.

The symbols of Theorem 1.1. Table 1 lists every symbol of the theorem's statement with its definition and its source, so the theorem reads without Section 3.

Symbol	Definition	Where
n; N	The degree, $n \in \{512, 1024\}$; $2n$, the number of integer samples	Definition A.25
$\mathcal{F}$; $\mathbb{R}$	A realization, the arithmetic with the perturbations (u, ζ); real arithmetic	Definition A.4
$\mathrm{ffSampling}^{\mathcal{F}}$; $\mathrm{ffSampling}^{\mathbb{R}}$	The signer's sampler in $\mathcal{F}$; in real arithmetic	Definition A.25
P; Q	The output probability measure of $\mathrm{ffSampling}^{\mathcal{F}}$ on $\mathbb{Z}^N$; that of $\mathrm{ffSampling}^{\mathbb{R}}$	Definition A.25
$z_{<i}$	$(z_1, \ldots, z_{i-1})$, the samples before leaf i	Definition A.25
$\widetilde{\sigma}_i$, $\widetilde{t}_i$; σ_i, t_i	Leaf i's computed standard deviation and center; the ideal ones, functions of $z_{<i}$	Definition A.25
α; $R_\alpha(\mu \,\|\, \nu)$	The Rényi order, $\alpha > 1$; the Rényi divergence of order α	Definition A.3
$\rho_{s,c}$; $D_{\mathbb{Z},s,c}$	$z \mapsto e^{-(z-c)^2/(2s^2)}$; the discrete Gaussian on $\mathbb{Z}$, $\rho_{s,c}/\rho_{s,c}(\mathbb{Z})$	Definition A.2
α_L; τ	$2\alpha - 1$, the order of the one-leaf comparison; the tail-cut radius, $\tau > 1$	Section 3.3
S; S'; S'^c; $S_{<i}$	$\{z \in \mathbb{Z}^N : \forall i \ \lvert z_i - \widetilde{t}_i \rvert \le \tau\widetilde{\sigma}_i\}$, the tail-cut event; a sub-event of S; $\mathbb{Z}^N \setminus S'$; the prefix sets of S	Definition A.26
C_i	The fringe sets, empty here	Definition A.26
$P_{S'}$; $Q_{S'}$	P conditioned on S'; Q conditioned on S'	Theorem 1.1
δ_i; $\bar{\delta}$	$\widetilde{\sigma}_i/\sigma_i - 1$, the relative perturbation of the standard deviation; the bound of the relative perturbation over S'	Definition A.27
Δ_i; $\bar{W}_{S'}$	$\widetilde{t}_i - t_i$, the shift of the center; $\sup_{z \in S'} \sum_{i \le N} \Delta_i^2/\sigma_i^2$, the weighted square sum of the shifts over S'	Definition A.27
$\mathcal{Z}_i$; $\widetilde{B}_i$; $\widetilde{D}_i$	$\{z_i \in \mathbb{Z} : \lvert z_i - \widetilde{t}_i \rvert \le \tau\widetilde{\sigma}_i\}$, the leaf set; the base sampler's measure in $\mathcal{F}$ at $(\widetilde{\sigma}_i, \widetilde{t}_i)$; the discrete Gaussian $D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$	Definition A.28
$\bar{\rho}_B$	$\max_{i \le N} \sup_{z_{<i} \in S_{<i}} R_{2\alpha}^{\mathcal{Z}_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)$, the moment of the base sampler	Definition A.28
$\Phi_{\alpha_L,i}$; $\bar{\phi}$	The normalizer ratio at leaf i; the bound of its logarithm over S'	Definition A.29
$\bar{x}$; r	$(1+\bar{\delta})^2 - 1$; the remainder of the standard deviations' term, of third order in $\bar{x}$	Theorem 1.1
$\bar{\theta}_{\alpha_L}(\bar{\delta})$	$1/(\alpha_L - (\alpha_L - 1)(1+\bar{\delta})^2)$, the factor on the shift, 1 at $\bar{\delta} = 0$ and infinite at the pole	Theorem 1.1
R	The divergence factor; $\ln R$ is the moment's, the normalizers', the standard deviations' and the shift's term	Theorem 1.1

Table 1: Symbols of Theorem 1.1.

Theorem 1.1 (The divergence bound with four explicit terms [to table] [to proof])**.** *The signer in $\mathcal{F}$ stays within the factor R of the signer over $\mathbb{R}$ on a sub-event of the tail-cut event, $\ln R$ the sum of four explicit terms. Let:*

- *S, the tail-cut event (Definition A.26);*
- *$C_i := \emptyset$ for $i \le N$, the fringe sets (Definition A.26);*
- *$S_{<i}$, its prefix sets (Definition A.26);*
- *$S' \subseteq S$, a sub-event (Definition A.26);*
- *S'^c, its complement (Definition A.26);*
- *$\bar{\delta}$, the bound of the relative perturbation over S' (Definition A.27);*
- *$\bar{W}_{S'}$, the weighted square sum of the shifts over S' (Definition A.27);*
- *$\bar{\rho}_B$, the moment of the base sampler (Definition A.28);*
- *$\bar{\phi}$, the bound of the normalizer ratio's logarithm over S' (Definition A.29).*

Define:

- *$P_{S'}(A) := P(A \cap S')/P(S')$ for $A \subseteq \mathbb{Z}^N$;*
- *$Q_{S'}(A) := Q(A \cap S')/Q(S')$;*
- *$\bar{x} := 2\bar{\delta} + \bar{\delta}^2$;*

- $r := \left(((\alpha_L-1)\bar{x})^3/(1-(\alpha_L-1)\bar{x}) + (\alpha_L-1)\bar{x}^3/(1-\bar{x})\right)/6$;
- $\bar{\theta}_{\alpha_L}(\bar{\delta}) := 1/(1-(\alpha_L-1)\bar{x})$;
- $R := \exp\left(\frac{N}{\alpha-1}\left(\frac{\alpha_L}{2}\ln\bar{\rho}_B + \frac{\bar{\phi}}{2}\right) + N\alpha_L\bar{\delta}^2(1+\bar{\delta}/2)^2 + \frac{N}{2(\alpha-1)}\,r + \frac{\alpha_L}{2}\,\bar{\theta}_{\alpha_L}(\bar{\delta})\bar{W}_{S'}\right)$.

Assume:

(A1) $(1+\bar{\delta})^2 < \alpha_L/(\alpha_L-1)$;

(A2) $\bar{x} < 1$;

(A3) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i > 0$;

(A4) $\bar{\rho}_B > 0$;

(A5) $P(S') > 0$;

(A6) $Q(S') > 0$.

Then

$$R_\alpha(P_{S'} \,\|\, Q_{S'}) \le R\,(1-P(S'^c))^{-\alpha/(\alpha-1)}.$$

Theorem 1.2 (Bit security over Q_s signatures [to table] [to proof])**.** *Over Q_s independent signatures, the Rényi divergences on the fringe classes S'_k of a sub-event S' of the tail-cut event, to the power $\alpha-1$, and the masses of its fringe leaves bound the computed signer's probability of the adversary's event by $2^{-\lambda_{\mathcal{F}}}$. Let:*

- *$\lambda \in \mathbb{R}$, the ideal signer's bit security (Definition 5.1);*
- *$Q_s \in \mathbb{Z}_{>0}$, the number of signatures (Definition 5.1);*
- *$A \ge 0$;*
- *$M_C \in \mathbb{Z}_{\ge 0}$;*
- *$R > 0$;*
- *S'_k, the fringe classes of S' (Definition A.26);*
- *κ_C and $\bar{p}_C$, the fringe quantities (Definition A.28);*
- *$\lambda_{\mathcal{F}}$, the bit security of the signer against A_{adv} (Definition 5.3) at (λ, Q_s, A, M_C);*

Define:

- *$R_\alpha^{S'_k}(P \,\|\, Q)$, that of Definition A.28 at $\mathcal{Y} := S'_k$;*
- *$P^{\otimes Q_s}$, the probability measure of Q_s independent signatures on $(\mathbb{Z}^N)^{Q_s}$ (Fact A.45, item 1).*

Let:

- *$A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s}$, an adversary's event (Definition 5.1) at (λ, Q_s).*

Assume:

(A1) $\ln R \le A$;

(A2) $\forall k \le N :\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k}\,\kappa_C^k\,R^{\alpha-1}$;

(A3) $\forall I \subseteq \{1,\dots,N\} :\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$.

Then

$$P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}.$$

Theorem 1.3 (Under **Hypotheses I.21, I.22 and I.91**, the fixed-point signer's bit security at both centers [to table] [to proof])**.** *The items bound the fixed-point signer's bit security from below at both centers and at every number of signatures of the sweep: the bound, its least value over the sweep, and the probability that the tail bound fails. **Under Hypotheses I.21, I.22 and I.91**, define:*

- *q, the modulus of Definition A.13.*

Let:

- *$c \in \{t, t_{\mathrm{frac}}\}$ be a center (Definition A.25);*
- *(f, g, F, G) be a checked key of degree n (Definition 5.5) passing the tail checks at c (Definition 5.6);*
- *$\mathsf{h}(\mathsf{m}) \in \{0,\dots,q-1\}^n$ be a hashed message (Definition A.25);*
- *$Q_s \in \{2^{32}, 2^{36}, \dots, 2^{64}\}$, the number of signatures (Definition 5.1).*

Define:

- *$\lambda := 128$ at $n = 512$ and $\lambda := 256$ at $n = 1024$ (Definition I.62).*

Let:

- *P and Q, the output measures of* ffSampling$^{\mathcal{F}}$ *and* ffSampling$^{\mathbb{R}}$ *(Definition A.25 at the key,* $\mathsf{h}(\mathsf{m})$ *and c);*
- *S_τ, the tail-cut event (Definition A.26) at the rate τ of Corollary I.80 at $c = t$ and of Corollary I.89 at $c = t_{\mathrm{frac}}$, at the key,* $\mathsf{h}(\mathsf{m})$ *and Q_s;*
- *E, the sub-event of Corollary I.80 at $c = t$ and of Corollary I.89 at $c = t_{\mathrm{frac}}$, at the key,* $\mathsf{h}(\mathsf{m})$ *and Q_s;*
- *$\lambda_{\mathcal{F}}$, the bit security (Definition 5.3), that of Corollary I.80 at $c = t$ and that of Corollary I.89 at $c = t_{\mathrm{frac}}$, at (n, λ, Q_s).*

Define:

- *$P^{\otimes Q_s}$ and $Q^{\otimes Q_s}$, the probability measures of Q_s independent outputs $(z^{(1)}, \ldots, z^{(Q_s)})$ of P and of Q on $(\mathbb{Z}^N)^{Q_s}$ (Fact A.45, item 1).*

Then

1. *At $c = t$ or $c = t_{\mathrm{frac}}$:* $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$;

	$c = t$	$c = t_{\mathrm{frac}}$
$n = 512$	2. $\lambda_{\mathcal{F}} \ge 126.28$	3. $\lambda_{\mathcal{F}} \ge 126.70$
$n = 1024$	4. $\lambda_{\mathcal{F}} \ge 248.78$	5. $\lambda_{\mathcal{F}} \ge 253.53$

6. *At $c = t$ or $c = t_{\mathrm{frac}}$:* $Q_s P(S_\tau \cap E^c) \le 2^{-\lambda}$.

Other results.

- We replace the relative-error lemma of [Pre17] by a second-moment method (Section 4.2; the comparison at the report's inputs is Appendix K).
- We extend the CryptoLine tool for the machine-checked proofs: the kernels' proofs compose along the recursion and the composed objects are proved as the code calls them (Section 2.2, Appendix M.2).

One gap inside the proof assistant. The Lean theorems take the summability of every infinite series they handle as a hypothesis. Mathlib defines the sum of a non-summable series as 0, so a bound on such a series without the hypothesis would be false in Lean; the report reads a series of nonnegative terms in $[0, \infty]$. The hypothesis holds for the fixed-point signer by an argument on the page: the program's output has finite support (Lemma I.49, Theorem I.54), so every series the proofs sum over it is a finite sum. The record of the Lean binders lists each hypothesis (Section 2). We expect to close this gap once the code-alignment hypotheses, **Hypotheses I.21, I.22 and I.91**, are closed: the sampler's measure then becomes a Lean object with its finite support, and the hypothesis is discharged.

The use of AI. This report was written with an AI coding agent, Anthropic's Claude, in the Claude Code CLI. The agent drafted the statements and the proofs on the author's plans, wrote the Lean carriers, the CryptoLine models and the checkers of Section 2, and ran the gates. The author set the questions, the structure and every decision, and reviewed the results. A statement is carried by Lean, by a CryptoLine proof or by a gate that reruns, or it is a hypothesis named as such, and the records of Section 2 list what each check covers. The human author takes the full responsibility of the statements of this report.

The cost of this project. The author has worked on this project since July 2026. The first table lists the usage of its Claude Code sessions by model, in millions of tokens, and the usage's price in dollars at the API's list prices. The second table lists the same dollars by month and by part of the project.

Model	Replies	Input	Cache write	Cache read	Output	$
Claude Fable 5	5,985	0.1	34.1	2,367.1	8.0	3,439
Claude Fable 5.1	18,780	0.6	138.9	8,991.5	31.8	6,444
Claude Fable 5.2	3,067	0.0	14.1	1,506.3	3.9	684
Claude Opus 4.8	821	0.0	4.6	236.5	1.1	188
Claude Opus 5	9,671	0.0	75.3	4,812.9	12.4	3,229
Claude Opus 5.5	63,404	0.1	426.6	25,539.9	44.9	8,349
Claude Sonnet 5	6,028	0.0	54.9	2,725.6	6.9	752
Claude Sonnet 5.5	2,073	0.0	14.5	399.8	0.7	84
Total						23,169

	$			
Month	Proofs (this report)	CryptoLine extension	Harness	Total
July 2026	–	2,226	–	2,226
August 2026	–	1,511	–	1,511
September 2026	8,297	17	–	8,314
October 2026	7,550	27	160	7,738
November 1–15, 2026	2,949	355	76	3,381
Total	18,796	4,136	237	23,169

The status of this report. This report is a draft. It is long and involved because its goal, from the beginning, is a machine-checked proof from the machine code up to the mathematical security statement as a single whole. The author will split it into several shorter papers before submitting them for peer review, and will release the artifact, with the tools a reader needs to replay it, once the split is settled. The final shape of the artifact is not yet settled and is subject to restructuring. The author has not thoroughly reviewed the related work on the mathematical instruments, and parts of the statements may already exist in the literature. The author plans to extend the citations and the literature review once time permits.

Structure of this report. Section 2 defines how a claim is backed; Section 3 the objects; Section 4 describes the roadmap of the proof; Section 5 states the fixed-point signer's bit security. Appendix I proves the bound on the fixed-point signer's bit security; Appendix M lists the gates, the machine-checked proofs and the imported facts; Appendix M.6 describes the dependency graphs. Table 2 lists how the three theorems above are verified.

Statement	**Lean**	**CryptoLine**	**Gate**	**Hypotheses**	**Source**
Thm. 1.1	✓				
Thm. 1.2	✓				
Thm. 1.3	✓		✓	**I.21**, **I.22**, **I.91**	

Table 2: Section 1: how each theorem is verified.

Why this structure. Agents walk through long derivations without tiring, and the report lets them: every proof is a derivation block, one relation per line, each line with its justification. A proof of a statement has at least two kinds of consumers in science: the research that takes the end result, and the research that takes the intermediate steps, modularizes them and broadens their applications. This report aims to serve both. The end results the agents proved are Theorems 1.1 to 1.3, stated in Section 1 in a short form, their objects imported by name and definition number. The intermediate steps and the core anchors the statements rest on are the body: the roadmap of Section 4, one statement per phase of the proof; the definitions and the imported facts of Appendix A that every chain starts from; the proof appendices with every line; and the dependency graphs and indexes that say which statement each line reaches and which theorem checks it.

2 Provenance, gates and machine-checked proofs

Structure. This section defines how a claim of the report is backed. Section 2.1 describes the reference tree, the gates and the status tables; Section 2.2 the machine-checked proofs; Section 2.3 the agents' doctrine. Appendix M lists the gates, the machine-checked proofs and the imported facts.

2.1 How a claim is backed

Every claim in this report is attributed to a node of a tree rooted at ground truth. A tag names the node. Figure 1 describes the tree.

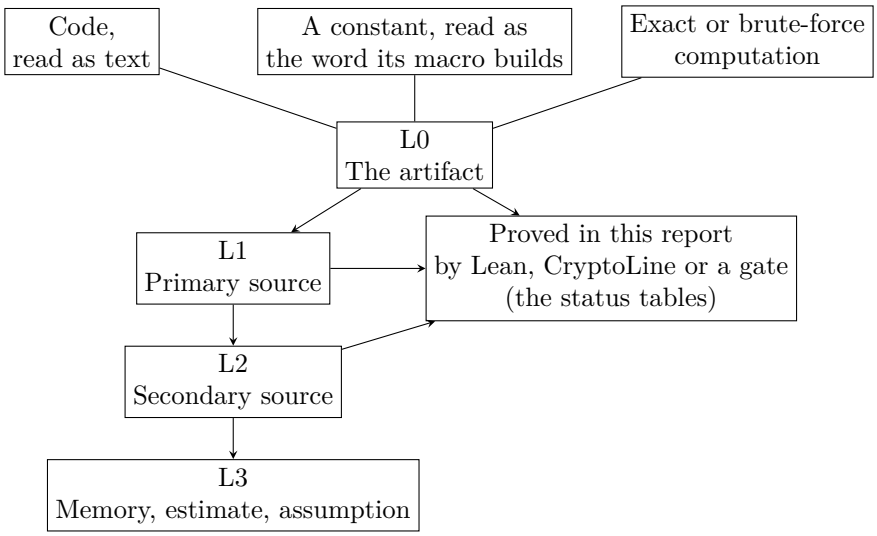


Figure 1: The reference tree.

L0 The artifact itself: its code, read as text; a constant, read as the word its macro builds; a computation in exact rational arithmetic or by brute force. The tag names a file and a line, **[L0: *file*:*line*]**.

L1 A primary source read this session, cited by item. The tag names the item, **[L1: *source, item*]**.

L2 A secondary source: a classical lemma quoted without re-derivation, or a paper read for one fact. The tag names the item, **[L2: *source, item*]**.

L3 Memory, an estimate, or an assumption.

proved A statement proved in this report from tagged ones, carried by Lean, by a CryptoLine proof or by a gate as its status table says (Section 2.2); a proof step without a tag is proved in this report.

Numbers are never retyped. Numbers are never retyped: every table and every number in the text is written by `paper/gen_tables.py`, which runs the checkers and parses their output, except for the number of signatures 2^{64} and the reference bit security.

What a gate verifies. A gate is a checker under `verify/`. A gate verifies exactly the elements it lists, at the instances it runs, and nothing else: its verdict *pass* means that no instance violated the bound. A gate never proves a lemma; the proof does. A gate tagged sampled runs on random or measured instances, a sweep of parameter values, seeds or a key sample, not on the whole

domain, so it settles those instances and nothing beyond them: a sampled gate is an item of a named hypothesis, and a statement that rests on it names the hypothesis at its head. A sampled measurement no statement rests on is an item of a Statistics statement instead. In the text a sampled gate is tagged **[hypothesis, sampled gate: ...]** beside the hypothesis's item, or **[statistics, sampled gate: ...]** beside the Statistics item. In a proof, a line's justification that cites a hypothesis is set in bold, so the assumptions a proof rests on are found without reading it. A gate without the mark is exhaustive over its finite domain or a computation of the quantity it reports.

A statement cites a gate only where it depends on it. A statement cites a gate only where its proof or its measured row depends on it: a stored constant, a measured quantity, a computed bit security, an exhaustive scan. A complete derivation cites none, and a check of Appendix M.1 that runs on such a derivation's constants stands beside the proof as a test, not as part of it.

The status tables. Every section opens with the table of how its statements are verified; Table 3 lists its columns.

Column	Meaning	Mark
Lean	A theorem proves the statement or some of its items	✓
CryptoLine	A machine-checked proof about a compiled object proves it, Section 2.2	✓
Gate	An exact gate, an exhaustive checker, runs it on the code	✓
Hypotheses	The hypotheses the statement names; on a hypothesis's row, its kind	Their numbers, bold
Source	Where an imported fact comes from, at L1 or L2	The citation
Eyes	A lemma, proposition, corollary or theorem with none of these	✓

Table 3: The columns of the status tables.

The three kinds of hypothesis. A hypothesis is of one of three kinds, Table 4, and its first words name its kind.

Kind	What it takes	Mark
Mathematical	A hypothesis on a quantity of the model, nothing in it measured	**[L3: mathematical]**
Sampled	A value or a distribution read from a sample; each sampled gate that measures it is an item of the hypothesis	**[L3: sampled]**
Code alignment	That the code computes the algorithms	**[L3: code alignment]**

Table 4: The kinds of hypothesis.

What a status table claims. A definition defines and a hypothesis is assumed, so neither is verified, and no table claims it: a table's caption names the definitions, facts and hypotheses its section holds and says of the lemmas, propositions, corollaries and theorems alone that they are verified. On a definition's or a hypothesis's row the marks still carry information, and this is what they say: the Lean column, that the kernel carries the object or the assumption, the type or the predicate the theorems quantify over; the gate column, that a checker measures what the definition records or what the hypothesis's discharge rests on; the hypotheses column, the hypotheses the definition's head names.

The links of a statement. Each statement links to its place, and the tag **[to table]** in its title links back to its table. A statement whose proof is in a proof appendix carries the tag **[to proof]**

in its title, linked to its restatement there by number and title, and the restatement carries the tag **[to statement]**, linked back to the statement.

The statements no tool checks. A lemma, proposition, corollary or theorem that neither a Lean theorem nor a gate checks carries the tag **[eyes only]** in its title and a mark in the eyes column of its status table. The statements that carry it are the floating-point signer's three loss propositions, whose measured rows a report prints and no gate compares (Table 37), and Lemma I.73, which summarizes the leaf sum's inputs of the fixed-point signer from the chain's bounds on the page (Table 25); the three corollaries stating other works' statements in our symbols (Table 52) are carried by Lean. [gate: `paper/check_lean.py`] pairs the tag with the tables' data after every build, so that it neither outlives a check nor precedes one.

2.2 Machine-checked proofs

A machine-checked proof is a CryptoLine theorem about a compiled object, proved by `cv` for every input of the domain. Figure 2 describes its chain from the object to the statement. In the text such a proof is tagged **[CryptoLine: ...]**, a path under `real_approx/`.

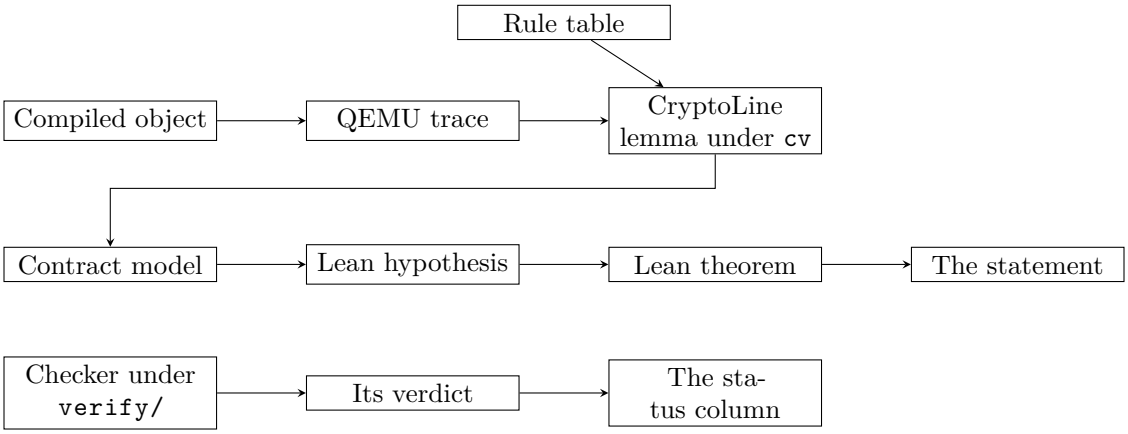


Figure 2: The chain of a machine-checked proof and the path of a gate.

The controls of a proof. Each proof has controls, and each control must fail:

- A vacuity control, a false postcondition on the range part or on the algebraic part of the claim: on the range part the SMT solver's rejection means that an input satisfies the proof's assumptions; on the algebraic part the rejection shows that the algebraic assumptions do not derive $1 \equiv 0 \pmod 2$;
- At least one rejection: the claim misread (truncation for rounding, the sign dropped, a tie rounded the other way, a carry lost), or the precondition relaxed to admit the first value outside the domain ($Y = 0$ for `fxp_div`, $e = 0$ or $e = 64$, $X - Y$ the first value outside its interval).

The trusted base of a proof. A proof trusts:

- The rule table of its instruction set, whose primitives are pinned against the target by probes;
- The tracer and QEMU;
- That every input sends the object through the trace's instructions and memory addresses;
- The base sampler's footprint, the registers it restores and the memory cells it writes;
- The definition each claim states, which its generator transcribes from the C code by hand;
- The binding of a contract's memory cells at a call site, by the order of first access;
- The harnesses' stand-ins for the C library's `memcpy` and `memmove`;
- `cv`, its verdict cache included.

The summability hypotheses of the Lean theorems. A Lean theorem that handles an infinite series takes the series' summability as a hypothesis, the gap Section 1 states: Mathlib defines the sum of a non-summable series as 0, where the report reads a series of nonnegative terms in $[0, \infty]$. Where the series is the mass of a probability measure, the hypothesis follows from the statement's objects; where it is a Rényi divergence of Definition A.3 to the power $\alpha - 1$, or its restriction to an event, it is open, and it holds for the fixed-point signer by an argument on the page, its output having finite support (Lemma I.49, Theorem I.54). The record of the Lean binders, `paper/lean_binders.json`, classes every hypothesis of every carrier against the statement it carries and lists each summability hypothesis of this kind as open; [gate: `paper/check_binders.py`] keeps the record at the current carriers and statements.

2.3 The agents' doctrine

The doctrine. The agents work under a doctrine, a body of standing rules loaded at every turn and kept outside the report. Its philosophy is that an agent's fluency is not evidence: whatever the agent asserts, it must first attribute to a node of the reference tree, and it reports at the level it reached, never higher. A number is read from its source in the session and never remembered; a conflict between two sources descends to their common ancestor and is never settled by counting them; a result accepted by a tool is not a result verified; a claim the author dictates stays marked as dictated until a proof or a gate settles it. The rules are prescriptive and layered by authority: the boundaries, the actions never taken whatever the goal, which only the author adds or lifts; the principles, the engineering invariants; the workflows, the procedures with their approval gates; the conventions; the reference data with its provenance; and a casebook of symptoms. A lesson learned on one incident is recorded as a conclusion freed of the incident's names, so that the next task meets the rule and not the story; a word is the field's established term, never one coined for the occasion; and the doctrine quotes no one, it states what was decided and when.

The fallback. We do not claim that agents do not err. The doctrine assumes that they do, and sets a default for the moment something goes wrong, so that an error is caught where it costs least and is never settled by the agent's own judgment. When rules conflict, a fixed order of authority decides: a live instruction of the author for the one case, then the boundaries, then the rules of the repository, then the principles, the workflows and the conventions, then the reference data, and last the casebook, a prior to check first and never a conclusion. When the evidence runs out, the agent falls back rather than forward: a claim it cannot attribute is reported as open, with its position in the tree, never as settled; a conflict between a new instruction and a standing rule stops the work before the next edit and is put to the author; working alone, the agent documents the conflict, takes the choice it can undo and leaves the decision open. A gate that fails stops the build, and nothing past it is reported; a build that passes settles what its gates list and nothing more. A rule's known fragility is kept beside it as a reminder that enforces nothing, so the rule itself stays whole.

Why the gates. Agents are capable of many things: they draft statements and proofs, write Lean and CryptoLine, build checkers and run them. The author found that what keeps them on track is not more guidance but gates against catastrophic errors: a retyped number, a recollection reported as a measurement, a proof line whose citation does not state what it is cited for, a record edited by hand. Each gate checks one such error mechanically, on the bytes of the sources; the build of the report runs every gate, so a report that builds is one in which no gate found its error. An agent's reading never passes a gate. The gates are the doctrine's rule on claims made mechanical where it can be. The work crosses fields, the verification of machine code, the Rényi divergence argument of lattice sampling and the engineering of agents, and a statement that moves between their surfaces, the C code, its CryptoLine model, the Lean theorem, the derivation on the page and the notes, is where an error slips in unseen, since no one surface's reader checks the

others. The agent harness exists for that transfer: it records each one as an edge from a claim to the artifact, the execution or the claim it rests on, with the level of the edge and whether bytes settled it or a reader asserted it, so the chain from an artifact to a claim is replayed, never recalled.

3 Definitions and notation

Shaded lines and tildes. In an algorithm, a shaded line computes over $\mathbb{R}$, in ffSampling$^{\mathbb{R}}$. A line with a tilde computes in $\mathcal{F}$, in ffSampling$^{\mathcal{F}}$. An unshaded line without a tilde is shared by ffSampling$^{\mathcal{F}}$ and ffSampling$^{\mathbb{R}}$, or states a bound. The L0 tags on a line name the code that performs it.

The meaning of a standing symbol. A standing symbol is a symbol named once and assumed from then on, so that a statement carries no superfluous notation.

Deliberate terms and conventions. Vectors are rows and a matrix acts on the right of a vector, the convention of FHK+20, Section 3.3; an identity that a source states for columns is stated here transposed (Fact A.16). We call the arithmetic over $\mathbb{R}$ real arithmetic. An operation of $\mathcal{F}$ is exact when its rounding returns the real result, as $\mathrm{fl}(-x) = -x$ (Fact A.6). A star marks a bound computed from the key checks' thresholds; T^* and z^* are two other fixed objects. $N := 2n$ is the sample count, so the integer ranges are written $\mathbb{Z}_{>0}$ and $\mathbb{Z}_{\geq 0}$. "Level" names a level of the tree, of the FFT or of the recursion; the quantity in bits is the bit security (Definition 5.3). We name the sets C_i of Definition A.26 fringe sets, since the other words collide: "saturated" names the shift, the word, the exponent and the acceptance, "tail" names S^c, and "edge" names a link of a tree and a link from a claim to what it rests on.

Structure. This section defines the objects of the report. Section 3.1 describes the rings, the Gaussians, the Rényi divergence, the realization $\mathcal{F}$, the two relations and the code's complex operations. Section 3.2 describes the fast Fourier sampler. Section 3.3 describes the objects of Theorem 1.1.

3.1 The numbers and the arithmetic

Standing symbols. The standing symbols of this section are:

- $\mathcal{F}$, the realization, fl, the rounding of one operation in $\mathcal{F}$, and (u, ζ), the relative and the absolute bound of $\mathcal{F}$ (Definition A.4);
- $\mathcal{F}_{\mathrm{fx}}$, the fixed-point signer's realization (Definition I.1);
- $\widetilde{x}$, the value the code computes for x, and $\widetilde{c} \in \mathcal{F}$, the stored value of a constant c (Definition A.4);
- a_{fx64}, the fixed-point representation of a of precision 64, and W_a, the word that stores a (Definition A.5);
- $C_{\mathcal{F}}$, the complex layer of $\mathcal{F}$, and $\oplus$, $\ominus$, $\otimes$, the code's complex operations on it (Definition A.8);
- $\mathcal{I}(\mathcal{I}_0, \mathcal{I}_1)$ and $\mathcal{N}_{||}(u, \zeta)$, the relation on approximation and the relation on the bound of the difference (Definitions A.10 and A.11).

The integers, the ring and its FFT form (Definition A.1). The set of **positive integers** is $\mathbb{Z}_{>0} := \{ k \in \mathbb{Z} : k > 0 \}$. The set of **nonnegative integers** is $\mathbb{Z}_{\geq 0} := \{ k \in \mathbb{Z} : k \geq 0 \}$. For m a power of two, let $\mathcal{R}_m := \mathbb{R}[x]/(x^m + 1)$ be the **ring of real polynomials** modulo $x^m + 1$. Let $f = \sum_{i<m} f_{[i]} x^i \in \mathcal{R}_m$ be a polynomial. The i-th **coefficient** of f is $f_{[i]}$. The **coefficient norm** of f is $\|f\| := \left(\sum_{i<m} f_{[i]}^2\right)^{1/2}$. Let $\psi := e^{i\pi/m}$ be the primitive $2m$-th root of unity over $\mathbb{C}$. For $k = 0, \ldots, m/2 - 1$, define $\psi_k := \psi^{2k+1}$. The **FFT form** of f is $(f(\psi_k))_{k<m/2}$.

Gaussians and the Rényi divergence (Definitions A.2 and A.3). Let $k \geq 1$ be an integer. Let $s > 0$ be a real, and $c \in \mathbb{R}^k$ a point. The **Euclidean norm** of $x \in \mathbb{R}^k$ is $\|x\| := \left(\sum_{j \leq k} x_j^2\right)^{1/2}$. The **Gaussian function** with center c and standard deviation s at the point $x \in \mathbb{R}^k$ is $\rho_{s,c}(x) := \exp(-\|x-c\|^2/(2s^2))$. We denote $\rho_s := \rho_{s,0}$. Let $A \subseteq \mathbb{R}^k$ be a countable set. Define $\rho_{s,c}(A) := \sum_{x \in A} \rho_{s,c}(x) \in [0, \infty]$. Assume $0 < \rho_{s,c}(A) < \infty$. The **discrete Gaussian** over A at the point $x \in A$ is $D_{A,s,c}(x) := \rho_{s,c}(x)/\rho_{s,c}(A)$. Let X be a countable set. Let μ and ν be probability measures on X, and $\alpha > 1$ a real. The **support** of μ is $\mathrm{Supp}(\mu) := \{x \in X : \mu(x) > 0\}$. Assume $\mathrm{Supp}(\mu) \subseteq \mathrm{Supp}(\nu)$. The **Rényi divergence** of order α between μ and ν is defined as $R_\alpha(\mu \,\|\, \nu) := \left(\sum_{x \in \mathrm{Supp}(\mu)} \mu(x)^\alpha \, \nu(x)^{1-\alpha}\right)^{1/(\alpha-1)}$. Let $f \colon X \to \mathbb{R}$ be a function with $\sum_{x \in X} \mu(x)|f(x)| < \infty$. The **expectation** of f under μ is $\mathbb{E}_\mu[f] := \sum_{x \in X} \mu(x) f(x)$. We denote $\mathbb{E}_{x \leftarrow \mu}[f(x)] := \mathbb{E}_\mu[f]$. Let $E \subseteq X$ be an event with $\mu(E) > 0$. The **conditioning** of μ on E at $A \subseteq X$ is $\mu(A \,|\, E) := \mu(A \cap E)/\mu(E)$. The expectation of f conditioned on E is defined as $\mathbb{E}_\mu[f \,|\, E] := \sum_{x \in X} \mu(\{x\} \,|\, E) f(x)$. A prefix of a sequence in the place of E names the event of the sequences that start with it.

The rounding model and its bounds (Definition A.4). Let $\mathcal{F} \subset \mathbb{R}$ be a set with $\forall \circ \in \{+, -, \times, /\}$ $\forall x, y \in \mathcal{F}$: $\mathrm{fl}(x \circ y) \in \mathcal{F}$ and $\mathrm{fl}(\sqrt{x}) \in \mathcal{F}$. Let $u \geq 0$ be a **relative bound**, and $\zeta \geq 0$ an **absolute bound**. The model is the standard model of rounding error analysis with an absolute term, which [Hig02, (2.8)] adds for underflow. We believe the model had been proposed in the literature, not necessarily for covering the underflow, due to its simplicity, but the author has not found a source. The **stored value** of a constant $c \in \mathbb{R}$ of the code is $\widetilde{c} \in \mathcal{F}$. $\mathbb{R}$ itself is a realization, with fl the identity function over $\mathbb{R}$ and $(u, \zeta) = (0, 0)$: real arithmetic. The **complex numbers** are $\mathbb{C} := \mathbb{R}[x]/(x^2 + 1)$.

- In `fxp/`, $\mathrm{fl}(x) \in 2^{-64}\mathbb{Z}$ with $|\mathrm{fl}(x) - x| \leq 2^{-65}$, a tie away from 0.
- In `fxp/`, `fxp_inv`(x) = `fxp_div`$(1, x)$.
- $\forall \circ \in \{+, -, \times, /\}$ $\forall x, y \in \mathcal{F}$ $\exists\, u_\circ, \zeta_\circ \in \mathbb{R}$, $|u_\circ| \leq u$, $|\zeta_\circ| \leq \zeta$: $\mathrm{fl}(x \circ y) = (x \circ y)(1 + u_\circ) + \zeta_\circ$.
- $\forall x \in \mathcal{F}$ $\exists\, u_\circ, \zeta_\circ \in \mathbb{R}$, $|u_\circ| \leq u$, $|\zeta_\circ| \leq \zeta$: $\mathrm{fl}(\sqrt{x}) = \sqrt{x}(1 + u_\circ) + \zeta_\circ$.
- The preconditions the shared algorithms take on $\mathcal{F}$, stated bare: $\forall x \in \mathcal{F}$ $\exists\, \zeta_\circ \in \mathbb{R}$, $|\zeta_\circ| \leq \zeta/2$: $\mathrm{fl}(x/2) = x/2 + \zeta_\circ$; $\forall \circ \in \{+, -\}$ $\forall x, y \in \mathcal{F}$ $\exists\, u_\circ, \zeta_\circ \in \mathbb{R}$, $|u_\circ| \leq u$, $|\zeta_\circ| \leq \zeta$: $\mathrm{fl}(\mathrm{fl}(x \circ y)/2) = ((x \circ y)(1 + u_\circ) + \zeta_\circ)/2$; $\mathrm{fl}(i) = i$ for $i \in \mathbb{Z}$, $|i| < 2^{53}$; $\mathrm{fl}(-x) = -x$ and $\mathrm{fl}(\mathrm{conj}\, x) = \mathrm{conj}\, x$ for $x \in \mathcal{F}$.
- At f fractional bits, the fixed-point signer has $(u, \zeta) = (0, 2^{-f})$, by Definition I.1, and meets the preconditions, by Fact A.7, items 1, 2, 3, 4 and 5.

The fixed-point words (Definition A.5). Let $a \in 2^{-64}\mathbb{Z}$ be a number, and $W \in \{0, \ldots, 2^{128} - 1\}$ a word.

- The **fixed-point representation** of a of precision 64 is $a_{\mathrm{fx64}} := 2^{64} a \in \mathbb{Z}$.
- The **word** the fixed-point signer stores for a number a a line of it computes is $W_a \in \{0, \ldots, 2^{128} - 1\}$. The signer stores W_a in two 64-bit limbs.
- The **limbs** of W are $(W_0, W_1) \in \{0, \ldots, 2^{64} - 1\}^2$ with $W = W_0 + 2^{64} W_1$.
- W **stores** a when $W = a_{\mathrm{fx64}} \bmod 2^{128}$ and $|a_{\mathrm{fx64}}| < 2^{127}$.

The shifts and the values of an integer on w bits. Let $v \in \mathbb{Z}$, $e \in \mathbb{Z}_{\geq 0}$ and $w \in \mathbb{Z}_{>0}$ be integers.

- The **left shift** of v by e is $v \ll e := 2^e v$.
- The **right shift** of $v \geq 0$ by e is $v \gg e := \lfloor v/2^e \rfloor$.
- The **arithmetic right shift** of the two's-complement word v by e is $v \gg_{\mathrm{a}} e := \lfloor v/2^e \rfloor$.
- The **unsigned value** of v on w bits is $\mathrm{u}_w(v) := v \bmod 2^w$.
- The **signed value** of v on w bits is $\mathrm{s}_w(v) \in [-2^{w-1}, 2^{w-1})$ with $\mathrm{s}_w(v) \equiv v \pmod{2^w}$.
- The **lowest bit** of v is $v \,\&\, 1 := v \bmod 2$.

The exact operations (Fact A.6). In the fixed-point signer, let $x, y \in \mathcal{F}$ be values, and $i \in \mathbb{Z}$ an integer. Let $\operatorname{trunc} x := \operatorname{sgn}(x)\lfloor |x| \rfloor$ be the **truncation** of x, and $\operatorname{rint} x$ the integer nearest to x, a tie to even.

- $\operatorname{fl}(-x) = -x$ and $\operatorname{fl}(\operatorname{conj} x) = \operatorname{conj} x$.
- Halving costs one rounding at 2^{-65}.
- For $1 \le e \le 63$, $\operatorname{fl}(2^e x) = 2^e x$.
- For $|i| < 2^{63}$, $\operatorname{fl}(i) = i$.
- $\lfloor x \rfloor, \operatorname{trunc} x, \operatorname{rint} x \in \mathbb{Z}$, exact.
- $\operatorname{fl}(x + 0) = x$ and $\operatorname{fl}(x \times 1) = x$.
- $\operatorname{fl}(x \circ y) = \operatorname{fl}(y \circ x)$ for $\circ \in \{+, \times\}$.
- $\operatorname{fl}(x - y) = x - y$.
- $\forall a, b \in \mathbb{R},\ a \le b :\ \operatorname{fl}(a) \le \operatorname{fl}(b)$, and $\operatorname{fl}(x) = x$.

The complex layer (Definition A.8). The **complex layer** of $\mathcal{F}$ is $C_{\mathcal{F}} := \mathcal{F}[x]/(x^2 + 1) = \{a_r + ia_i : a_r, a_i \in \mathcal{F}\}$. Let $a = a_r + ia_i \in C_{\mathcal{F}}$ and $b = b_r + ib_i \in C_{\mathcal{F}}$ be values. Let $c \in \mathcal{F}$ be a real, and $f \in \mathcal{R}_n$ a polynomial.

- The FFT form of f in the code is $(\operatorname{Re} f(\psi_k))_{k<n/2} \,\|\, (\operatorname{Im} f(\psi_k))_{k<n/2}$.
- Define $a \oplus b := \operatorname{fl}(a_r + b_r) + i\ \operatorname{fl}(a_i + b_i)$.
- $a \ominus b := a \oplus (-b)$.
- Define $a \otimes b := \operatorname{fl}(\operatorname{fl}(a_r b_r) - \operatorname{fl}(a_i b_i)) + i\ \operatorname{fl}(\operatorname{fl}(a_r b_i) + \operatorname{fl}(a_i b_r))$.
- Define $c \otimes a := \operatorname{fl}(ca_r) + i\ \operatorname{fl}(ca_i)$.
- $a \otimes c := c \otimes a$.
- The **adjoint** of a is $\operatorname{conj} a := a_r - ia_i$.
- $\widetilde{\operatorname{conj}}\, a = \operatorname{conj} a$.
- In `fxp/`, $a \oplus b = a + b$ and $a \ominus b = a - b$.
- A quantity without a tilde is defined by exact operations from its inputs.

Intervals and the two relations (Definitions A.9, A.10 and A.11). Let $\mathcal{A}$ be an algebraic structure with a norm $||$, and $x \in \operatorname{Img}(||)$ a value of the norm. The **ball** of radius x in $\mathcal{A}$ is $x^{\pm} := \{a \in \mathcal{A} : |a| \le x\}$. On $\mathbb{R}$, $x^{\pm} = [-x, x]$. An expression carrying signs $\pm$, each chosen independently, stands for the interval of $\mathcal{A}$ between the least and the largest of the values it takes: for $a, b, c \ge 0$, $a \pm b \pm c$ is $[a - b - c, a + b + c]$.

- Let $\mathcal{I}_0, \mathcal{I}_1 \subset \mathcal{A}$ be intervals. The **relation on approximation** is defined as the binary relation $\mathcal{I}(\mathcal{I}_0, \mathcal{I}_1)$: $\mathcal{A}^2 \to \{0, 1\}$ with $\forall a, b \in \mathcal{A} :\ a\ \mathcal{I}(\mathcal{I}_0, \mathcal{I}_1)\ b \iff \exists u_\circ, \zeta_\circ \in \mathcal{A}, u_\circ \in \mathcal{I}_0, \zeta_\circ \in \mathcal{I}_1 :\ a = b(1 + u_\circ) + \zeta_\circ$.
- Let $u, \zeta \in \operatorname{Img}(||)$ be a relative and an absolute bound. The **relation on the bound of the difference** is defined as the binary relation $\mathcal{N}_{||}(u, \zeta) : \mathcal{A}^2 \to \{0, 1\}$ with $\forall a, b \in \mathcal{A} :$ $a\ \mathcal{N}_{||}(u, \zeta)\ b \iff |a - b| \le u|b| + \zeta$.
- When the context is clear, we omit the norm operator $||$.

Algorithm 1 $\oplus$, $\ominus$, $\otimes$, the code's complex operations of Definition A.8 [L0: `sign_inner.h:327`] [L0: `fxp/sign_fxp.h:436-447`]

Input: $a = a_r + ia_i$, $b = b_r + ib_i \in C_{\mathcal{F}}$
Output (code): $a \oplus b$, $a \ominus b$, $a \otimes b \in C_{\mathcal{F}}$
Output (idealized): $a + b$, $a - b$, $ab \in \mathbb{C}$

1: $a \oplus b \leftarrow \operatorname{fl}(a_r + b_r) + i\ \operatorname{fl}(a_i + b_i)$
2: $a \ominus b \leftarrow a \oplus (-b)$ ▷ $-b = -b_r - ib_i$, exact (Definition A.4, item 6)
3: $a \otimes b \leftarrow \operatorname{fl}(\operatorname{fl}(a_r b_r) - \operatorname{fl}(a_i b_i)) + i\ \operatorname{fl}(\operatorname{fl}(a_r b_i) + \operatorname{fl}(a_i b_r))$

The bounds of the complex operations (Lemma B.2). Define $k_B := \sqrt{2}(3 + 2u)$. Let $|a|$ be the complex modulus of $a \in \mathbb{C}$, and $\|\cdot\|$ the Euclidean norm of a tuple. In the relations of

Definitions A.10 and A.11:

- $\forall a, b \in C_{\mathcal{F}} : (a \oplus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\zeta^{\pm}\right)\ (a+b)$.
- $\forall a, b \in C_{\mathcal{F}} : (a \ominus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\zeta^{\pm}\right)\ (a-b)$.
- $\forall a, b \in C_{\mathcal{F}} : (a \otimes b)\ \mathcal{I}\left(\left(\sqrt{2}u(2+u)\right)^{\pm}, k_B\zeta^{\pm}\right)\ ab$.
- $\forall a \in \mathbb{C}, |a| = 1\ \forall \tilde{a} \in C_{\mathcal{F}}, \tilde{a}_r\ \mathcal{I}\left(u^{\pm}, \zeta^{\pm}\right)\ a_r, \tilde{a}_i\ \mathcal{I}\left(u^{\pm}, \zeta^{\pm}\right)\ a_i : \tilde{a}\ \mathcal{I}\left(u^{\pm} + \sqrt{2}\zeta^{\pm}, 0\right)\ a$.
- $\forall m \geq 1\ \forall (a_k), (b_k) \in C_{\mathcal{F}}^m : (a_k \otimes b_k)_k\ \mathcal{N}\left(\sqrt{2}u(2+u), \sqrt{m}k_B\zeta\right)\ (a_k b_k)_k$.

3.2 The fast Fourier sampler and the tree of a key

Figure 3 draws the call graph of the algorithms.

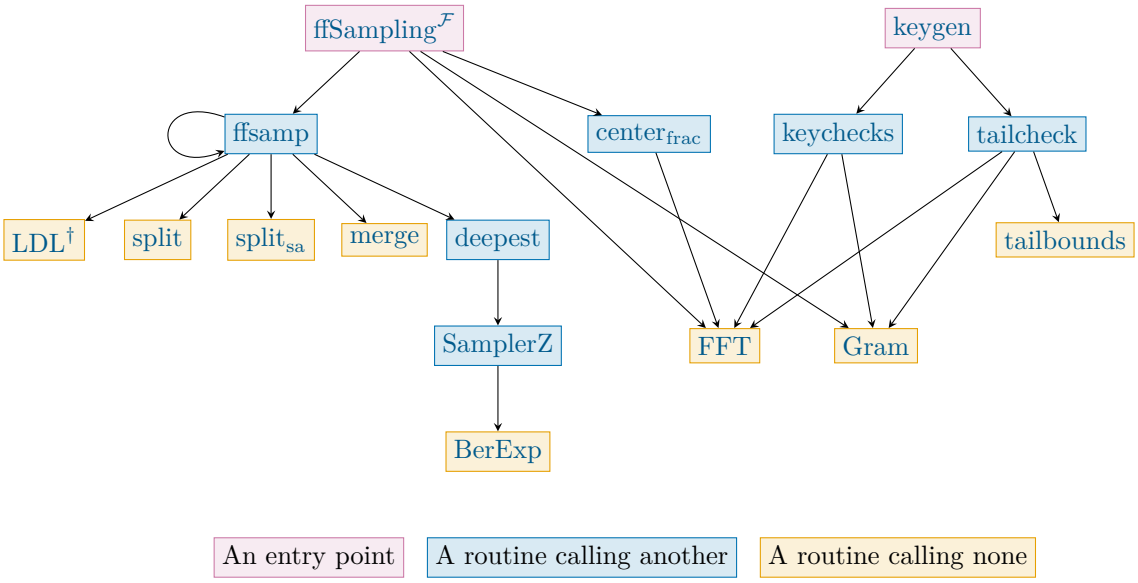


Figure 3: The call graph of the algorithms.

Standing symbols. Let $n \in \{512, 1024\}$ be the degree, and (f, g, F, G) a key of degree n of keygen (Algorithm 11, line 3). The ring is $\mathcal{R}_n$, and $\psi \in \mathbb{C}$ a root of $x^n + 1$ (Definition A.1). Define $q := 12289$, the **modulus**. Define $N := 2n$, the number of integer samples. The other standing symbols are:

- B, the basis of (f, g, F, G), and $\mathcal{G}$, its Gram matrix (Definition A.12);
- $\mathsf{h}(\mathsf{m})$, the hashed message, t, its center, $(t_0, t_1) := t$, and t_{int} and t_{frac}, the integer and the fractional part of t (Definition A.13);
- $i \leq N$, a sample position (Definition A.19);
- $T := \text{ffLDL}^{\dagger}(\mathcal{G})$, the tree (Definition A.20);
- $z = (z_i)_{i \leq N} \in \mathbb{Z}^N$, the samples of one signature (Definition A.21);
- (σ_i, t_i), the leaf parameters at the position i, $\sigma_{\min}$, the signer's standard deviation parameter, and $s := 1.17\sqrt{q}\,\sigma_{\min}$ (Definition A.25);
- ν, a node of the tree T (Definition A.18), and $\mathcal{G}_\nu$, its Gram matrix (Definition A.32);
- g_{00}, g_{01}, g_{11}, the entries of $\mathcal{G}_\nu$, and l_{10}, d_{00}, d_{11}, the factor and the diagonals of its $LDL^{\dagger}$ step (Definition A.17).

The generic definitions read at the standing symbols. A definition below stated for a generic degree m, a tree, a center or a real s is read at the standing symbols: $m := n$, the tree T, the center t and the parameter s.

The basis and its lattice (Definition A.12). The **basis** of (f, g, F, G) is $B := \begin{pmatrix} g & -f \\ G & -F \end{pmatrix} \in \mathcal{R}_n^{2\times 2}$. The **lattice** of B is $\Lambda(B) := \{(z_0, z_1)B : z_0, z_1 \in \mathbb{Z}[x]/(x^n+1)\} \subset \mathcal{R}_n^2$. Let $s > 0$ be a real, and $c \in \mathcal{R}_n^2$ a point. Define $D_{\Lambda(B),s,c} := D_{A,s,c}$ at $k := 2n$ and $A := \Lambda(B)$, $D_{A,s,c}$ that of Definition A.2, each pair of $\mathcal{R}_n^2$ read as its $2n$ coefficients in $\mathbb{R}^{2n}$. The **Gram matrix** of B is $\mathcal{G} \in \mathcal{R}_n^{2\times 2}$ with $\forall \psi \in \mathbb{C},\ \psi^n = -1 :\ \mathcal{G}(\psi) := B(\psi)B(\psi)^\dagger$, $B(\psi)^\dagger$ the conjugate transpose.

The center of a hashed message (Definition A.13). The **hashed message** $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$ is read as the polynomial $\sum_{i<n} \mathsf{h}(\mathsf{m})_{[i]} x^i \in \mathbb{Z}[x]/(x^n+1)$. The **center** of $\mathsf{h}(\mathsf{m})$ is $t := (\mathsf{h}(\mathsf{m}), 0)\, B^{-1} \in \mathcal{R}_n^2$. Define $(t_0, t_1) := t$, with $\forall \psi \in \mathbb{C},\ \psi^n = -1 :\ t_0(\psi) = \mathsf{h}(\mathsf{m})(\psi)\,(-F(\psi))\,(1/q)$, $t_1(\psi) = (-f(\psi))\,\mathsf{h}(\mathsf{m})(\psi)\,(-1/q)$. Define $qt := (-\mathsf{h}(\mathsf{m})\, F,\ \mathsf{h}(\mathsf{m})\, f) \in (\mathbb{Z}[x]/(x^n+1))^2$. Define $qt_{\text{frac}} = (qt_{\text{frac},0}, qt_{\text{frac},1}) \in (\mathbb{Z}[x]/(x^n+1))^2$ by $\forall j \in \{0,1\}\ \forall i < n :\ (qt_{\text{frac},j})_{[i]} \in [-q/2, q/2)$ and $(qt_{\text{frac},j})_{[i]} \equiv (qt_j)_{[i]} \pmod q$. The **integer part** of t is $t_{\text{int}} := (qt - qt_{\text{frac}})/q \in (\mathbb{Z}[x]/(x^n+1))^2$. The **fractional part** of t is $t_{\text{frac}} := qt_{\text{frac}}/q \in \mathcal{R}_n^2$.

The Gram matrix (Definition A.14). Let m be a power of two, and $\psi \in \mathbb{C}$ a root with $\psi^m = -1$. Let $g_{00}, g_{11} \in \mathcal{R}_m$ be polynomials with $g_{00} = \operatorname{conj} g_{00}$ and $g_{11} = \operatorname{conj} g_{11}$, and $g_{01} \in \mathcal{R}_m$ a polynomial. Define $\mathcal{G} := \begin{pmatrix} g_{00} & g_{01} \\ \operatorname{conj} g_{01} & g_{11} \end{pmatrix}$. The set of Gram matrices of degree m is $\text{Gram}_m := \{\mathcal{G} : \forall \psi :\ g_{00}(\psi) > 0,\ g_{00}(\psi)g_{11}(\psi) > |g_{01}(\psi)|^2\}$.

Split and merge (Definition A.15, Fact A.16). Let $m \geq 4$ be a power of two, and $a, b \in \mathcal{R}_m$ polynomials. The **even part** of a is $a_0 := \sum_{i<m/2} a_{[2i]} x^i \in \mathcal{R}_{m/2}$. The **odd part** of a is $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i \in \mathcal{R}_{m/2}$. Define $V_m \colon \mathcal{R}_m \to \mathcal{R}_{m/2}^2$ as $V_m(a) := (a_0, a_1)$. Define $M_m \colon \mathcal{R}_m \to \mathcal{R}_{m/2}^{2\times 2}$ as $M_m(a) := \begin{pmatrix} a_0 & a_1 \\ xa_1 & a_0 \end{pmatrix}$. The **split** is $\text{split} \colon \mathcal{R}_m \to \mathcal{R}_{m/2}^2$, $\text{split}(a) := V_m(a)$. Let $(f_0, f_1), (g_0, g_1) \in \mathcal{R}_{m/2}^2$ be pairs. The **merge** is $\text{merge} \colon \mathcal{R}_{m/2}^2 \to \mathcal{R}_m$, $\text{merge}(f_0, f_1) := f_0(x^2) + x f_1(x^2)$. The **coefficient inner product** is $\langle a, b \rangle := \sum_{i<m} a_{[i]} b_{[i]}$. Define $\langle (f_0, f_1), (g_0, g_1) \rangle := \langle f_0, g_0 \rangle + \langle f_1, g_1 \rangle$.

- $\langle V_m(a), V_m(b) \rangle = \langle a, b \rangle$.
- $V_m(ab) = V_m(b)\, M_m(a)$.

Algorithm 2 split(f), the split butterflies of one level [L0: `sign_fpoly.c:2258-2272`] [L0: `fxp/sign_fxpoly.c:168-193`]

Input: $f \in \mathcal{R}_m$; $\psi_k \in \mathbb{C}$, $\widetilde{\psi}_k \in C_{\mathcal{F}}$ (Definition A.8, item 1)
Precondition: $m \geq 4$. $|\psi| = 1$ and $\psi^m = -1$. $|\widetilde{\psi} - \psi| \leq u + \sqrt{2}\,\zeta$ (Definition A.8, item 1).
Output (code): $\forall \psi:\ \widetilde{f}_0(\psi^2), \widetilde{f}_1(\psi^2) \in C_{\mathcal{F}}$
Output (idealized): $\forall \psi:\ f_0(\psi^2) = (f(\psi) + f(-\psi))/2$, $f_1(\psi^2) = (f(\psi) - f(-\psi))/(2\psi)$
Postcondition: $f = f_0(x^2) + x f_1(x^2)$
In the proofs: $f(\psi)$, $f(-\psi)$

1: **for all** $\{\psi, -\psi\}$, $\psi^m = -1$ **do**
2: $\quad \widetilde{s} \leftarrow \widetilde{\psi}_{i+m/2}$ ▷ GM$[i + m/2]$ (Definition A.8, item 1)
3: $\quad s \leftarrow \psi$
4: $\quad \widetilde{f}_0(\psi^2) \leftarrow \mathrm{fl}((f(\psi) \oplus f(-\psi))/2)$ ▷ [L0: `sign_fpoly.c:2263-2266`] [L0: `fxp/sign_fxpoly.c:183-186`]
5: $\quad f_0(\psi^2) \leftarrow (f(\psi) + f(-\psi))/2$
6: $\quad \widetilde{f}_1(\psi^2) \leftarrow \mathrm{fl}(((f(\psi) \ominus f(-\psi)) \otimes \mathrm{conj}\,\widetilde{s})/2)$ ▷ [L0: `sign_fpoly.c:2267-2271`] [L0: `fxp/sign_fxpoly.c:187-191`]
7: $\quad f_1(\psi^2) \leftarrow ((f(\psi) - f(-\psi))/2)\ \mathrm{conj}\, s$
8: **end for**
9: **return** $(\widetilde{f}_0, \widetilde{f}_1)$
10: **return** (f_0, f_1)

Algorithm 3 $\mathrm{split}_{\mathrm{sa}}(f)$, the split butterflies of one level for a self-adjoint f [L0: `sign_fpoly.c:2351-2362`] [L0: `fxp/sign_fxpoly.c:195-215`]

Input: $f \in \mathcal{R}_m$ self-adjoint; $\psi_k \in \mathbb{C}$, $\widetilde{\psi}_k \in C_{\mathcal{F}}$ (Definition A.8, item 1)
Precondition: $m \geq 4$. $|\psi| = 1$ and $\psi^m = -1$. $|\widetilde{\psi} - \psi| \leq u + \sqrt{2}\,\zeta$ (Definition A.8, item 1).
Output (code): $\forall \psi:\ \widetilde{f}_0(\psi^2) \in \mathcal{F}$, $\widetilde{f}_1(\psi^2) \in C_{\mathcal{F}}$
Output (idealized): $\forall \psi:\ f_0(\psi^2) = (f(\psi) + f(-\psi))/2$, $f_1(\psi^2) = (f(\psi) - f(-\psi))/(2\psi)$
Postcondition: $f = f_0(x^2) + x f_1(x^2)$, f_0 self-adjoint
In the proofs: $f(\psi)$, $f(-\psi)$

1: **for all** $\{\psi, -\psi\}$, $\psi^m = -1$ **do**
2: $\quad \widetilde{s} \leftarrow \widetilde{\psi}_{i+m/2}$ ▷ GM$[i + m/2]$ (Definition A.8, item 1)
3: $\quad s \leftarrow \psi$
4: $\quad \widetilde{f}_0(\psi^2) \leftarrow \mathrm{fl}((f(\psi) \oplus f(-\psi))/2)$ ▷ [L0: `sign_fpoly.c:2356-2358`] [L0: `fxp/sign_fxpoly.c:208-210`]
5: $\quad f_0(\psi^2) \leftarrow (f(\psi) + f(-\psi))/2$
6: $\quad \widetilde{f}_1(\psi^2) \leftarrow \mathrm{fl}((f(\psi) \ominus f(-\psi))/2) \otimes \mathrm{conj}\,\widetilde{s}$ ▷ [L0: `sign_fpoly.c:2359-2361`] [L0: `fxp/sign_fxpoly.c:211-213`]
7: $\quad f_1(\psi^2) \leftarrow ((f(\psi) - f(-\psi))/2)\ \mathrm{conj}\, s$
8: **end for**
9: **return** $(\widetilde{f}_0, \widetilde{f}_1)$
10: **return** (f_0, f_1)

Algorithm 4 merge(f_0, f_1), the merge butterflies of one level [LO: `sign_fpoly.c:2452-2463`] [LO: `fxp/sign_fxpoly.c:217-241`]

Input: $(f_0, f_1) \in \mathcal{R}_{m/2} \times \mathcal{R}_{m/2}$; $\psi_k \in \mathbb{C}$, $\widetilde{\psi_k} \in C_{\mathcal{F}}$ (Definition A.8, item 1)
Precondition: $m \geq 4$. $|\widetilde{\psi} - \psi| \leq u + \sqrt{2}\,\zeta$ (Definition A.8, item 1).
Output (code): $\forall \psi :\ \widetilde{a}, \widetilde{b} \in C_{\mathcal{F}}$
Output (idealized): $\forall \psi :\ f(\pm\psi) = f_0(\psi^2) \pm \psi f_1(\psi^2)$
Postcondition: $f = f_0(x^2) + x f_1(x^2)$ (Lemma G.18)
In the proofs: $\widetilde{z}$, z

1: **for all** $\{\psi, -\psi\}$, $\psi^m = -1$ **do**
2: $\quad \widetilde{s} \leftarrow \widetilde{\psi}_{i+m/2}$ ▷ GM$[i + m/2]$ (Definition A.8, item 1)
3: $\quad s \leftarrow \psi$
4: $\quad \widetilde{z} \leftarrow f_1(\psi^2) \otimes \widetilde{s}$
5: $\quad z \leftarrow f_1(\psi^2)\, s$
6: $\quad \widetilde{a} \leftarrow f_0(\psi^2) \oplus \widetilde{z}$
7: $\quad f(\psi) \leftarrow f_0(\psi^2) + z$
8: $\quad \widetilde{b} \leftarrow f_0(\psi^2) \ominus \widetilde{z}$
9: $\quad f(-\psi) \leftarrow f_0(\psi^2) - z$
10: **end for**
11: **return** $(\widetilde{a}, \widetilde{b})$
12: **return** f

The $LDL^\dagger$ step (Definition A.17). Let $m \geq 2$ be a power of two. Let $g_{00} \in \mathcal{R}_m$ be a polynomial with $g_{00} = \operatorname{conj} g_{00}$ and $\forall \psi \in \mathbb{C},\ \psi^m = -1 :\ g_{00}(\psi) > 0$. Let $g_{11} \in \mathcal{R}_m$ be a polynomial with $g_{11} = \operatorname{conj} g_{11}$, and $g_{01} \in \mathcal{R}_m$ a polynomial. Define $\mathcal{G} := \begin{pmatrix} g_{00} & g_{01} \\ \operatorname{conj} g_{01} & g_{11} \end{pmatrix}$. The **off-diagonal factor** of $\mathcal{G}$ is $l_{10} \in \mathcal{R}_m$ with $\forall \psi \in \mathbb{C},\ \psi^m = -1 :\ l_{10}(\psi) := \operatorname{conj} g_{01}(\psi)/g_{00}(\psi)$. The **diagonals** of $\mathcal{G}$ are $d_{00} := g_{00}$ and $d_{11} \in \mathcal{R}_m$ with $\forall \psi \in \mathbb{C},\ \psi^m = -1 :\ d_{11}(\psi) := g_{11}(\psi) - |g_{01}(\psi)|^2/g_{00}(\psi)$. The $LDL^\dagger$ **step** of $\mathcal{G}$ is $\mathrm{LDL}^\dagger(\mathcal{G}) := (l_{10}, d_{00}, d_{11})$.

Algorithm 5 $\mathrm{LDL}^\dagger(\mathcal{G})$, the $LDL^\dagger$ step of one node [L0: `sign_fpoly.c:2136-2149`] [L0: `fxp/sign_fxpoly.c:131-148`]

Input: $\mathcal{G} = \begin{pmatrix} g_{00} & g_{01} \\ \operatorname{conj} g_{01} & g_{11} \end{pmatrix}$ over $\mathcal{R}_m$, g_{00}, g_{11} self-adjoint; $\forall \psi:\ g_{00}, g_{11} \in \mathcal{F}$, $g_{01} = g_{01,r} + i g_{01,i} \in C_\mathcal{F}$

Precondition: $\forall \psi:\ g_{00} > 0$. $\forall \psi:\ g_{00} g_{11} > |g_{01}|^2$.

Output (code): $\forall \psi:\ \widetilde{l}_{10} \in C_\mathcal{F}$, $\widetilde{d}_{00}, \widetilde{d}_{11} \in \mathcal{F}$

Output (idealized): $\forall \psi:\ (l_{10}, d_{00}, d_{11}) = (\operatorname{conj} g_{01}/g_{00},\ g_{00},\ g_{11} - |g_{01}|^2/g_{00})$; $l_{10} \in \mathcal{R}_m$, d_{00}, d_{11} self-adjoint

Postcondition: $\mathcal{G} = \begin{pmatrix} 1 & 0 \\ l_{10} & 1 \end{pmatrix} \begin{pmatrix} d_{00} & 0 \\ 0 & d_{11} \end{pmatrix} \begin{pmatrix} 1 & \operatorname{conj} l_{10} \\ 0 & 1 \end{pmatrix}$ (Lemma D.4)

In the proofs: $\widetilde{\iota}$, ι, $\widetilde{\mu}$, μ, $\widetilde{zo}$, zo

if $\mathcal{F} \neq \mathcal{F}_{\mathrm{fx}}$ **then**
  $\widetilde{\iota} \leftarrow \mathrm{fl}(1/g_{00})$
  $\iota \leftarrow 1/g_{00}$
  $\widetilde{\mu}_r \leftarrow \mathrm{fl}(g_{01,r}\,\widetilde{\iota})$
  $\widetilde{\mu}_i \leftarrow \mathrm{fl}(g_{01,i}\,\widetilde{\iota})$
else
  $\widetilde{\mu}_r \leftarrow \mathrm{fl}(g_{01,r}/g_{00})$ ▷ $\mathcal{F}_{\mathrm{fx}}$, Lemma G.24 [L0: `fxp/sign_fxpoly.c:140`]
  $\widetilde{\mu}_i \leftarrow \mathrm{fl}(g_{01,i}/g_{00})$ ▷ $\mathcal{F}_{\mathrm{fx}}$, Lemma G.24 [L0: `fxp/sign_fxpoly.c:141`]
end if
$\widetilde{\mu} \leftarrow \widetilde{\mu}_r + i\,\widetilde{\mu}_i$
$\mu \leftarrow g_{01}/g_{00}$
$\widetilde{l}_{10} \leftarrow \operatorname{conj} \widetilde{\mu}$
$l_{10} \leftarrow \operatorname{conj} \mu$
$\widetilde{zo} \leftarrow \mathrm{fl}(\mathrm{fl}(\widetilde{\mu}_r\, g_{01,r}) + \mathrm{fl}(\widetilde{\mu}_i\, g_{01,i}))$
$zo \leftarrow \mu_r\, g_{01,r} + \mu_i\, g_{01,i}$ ▷ $= |g_{01}|^2/g_{00}$
$\widetilde{d}_{00} \leftarrow g_{00}$
$d_{00} \leftarrow g_{00}$
$\widetilde{d}_{11} \leftarrow \mathrm{fl}(g_{11} - \widetilde{zo})$
$d_{11} \leftarrow g_{11} - zo$
return $(\widetilde{l}_{10}, \widetilde{d}_{00}, \widetilde{d}_{11})$
return (l_{10}, d_{00}, d_{11})

The tree (Definition A.18). Let $m = 2^k$ be a degree, $k \geq 1$, and $l_{10} \in \mathcal{R}_m$ a polynomial. Let A and B be two **leaf diagonals** in $(0, \infty)$ if $m = 2$, and two nodes of degree $m/2$ if $m \geq 4$. The **node** of degree m is $\mathrm{node}(l_{10};\ A, B)$, the triple of l_{10} and its two **children** A and B. The **leaf node** is $\mathrm{node}(l_{10};\ d_{00}, d_{11})$ at $m = 2$, with the leaf diagonals d_{00} and d_{11} as children. The **non-leaf node** is $\mathrm{node}(l_{10};\ A, B)$ at $m \geq 4$. The set of nodes of degree m is $\mathcal{T}_m$. Let $T \in \mathcal{T}_m$ be a **tree**, and $\nu = \mathrm{node}(l_{10};\ A, B) \in \mathcal{T}_{m'}$ a node, $m' \leq m$. Define $h := \log_2 m$. The children, the **subtrees** and the **depths** are defined as

$$
\begin{aligned}
&L(\nu) = A, \qquad R(\nu) = B, \\
&\forall d \in \mathbb{R}:\ \mathrm{Sub}(d) = \{d\}, \qquad \mathrm{Sub}(\nu) = \{\nu\} \cup \mathrm{Sub}(L(\nu)) \cup \mathrm{Sub}(R(\nu)), \\
&\forall d \in \mathrm{Sub}(T) \cap \mathbb{R}:\ \mathrm{depth}(d) = h, \\
&\forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}:\ \mathrm{depth}(T') = \log_2(m/m').
\end{aligned}
$$

The sample positions and the ffLDL† tree (Definitions A.19 and A.20). Define $N := 2m$, the standing N at $m := n$. The **sample positions** of T are $I(T) := \{1, \ldots, N\}$, ordered by $<$, the **sampling order**. Let $\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}$ be a subtree with $I(\nu) = \{a, \ldots, a + 2m' - 1\}$.

Define $I(R(\nu)) := \{a, \dots, a+m'-1\}$ and $I(L(\nu)) := \{a+m', \dots, a+2m'-1\}$. Let $d \in \mathrm{Sub}(T) \cap \mathbb{R}$ be a leaf diagonal of T. The leaf diagonal at the position $i \in I(d)$ is $d_i := d$. For $v \le m$, define $d_v := d_{2v-1}$, equal to d_{2v}. Let $\mathcal{G} \in \mathrm{Gram}_m$ be a Gram matrix (Definition A.14). Define $(l_{10}, d_{00}, d_{11}) := \mathrm{LDL}^\dagger(\mathcal{G})$ (Definition A.17). At $m \ge 4$, define $(d_0, d_1) := \mathrm{split}(d_{00})$ and $(d'_0, d'_1) := \mathrm{split}(d_{11})$ (Definition A.15), $\mathcal{G}_{d_{00}} := \begin{pmatrix} d_0 & d_1 \\ \mathrm{conj}\, d_1 & d_0 \end{pmatrix}$ and $\mathcal{G}_{d_{11}} := \begin{pmatrix} d'_0 & d'_1 \\ \mathrm{conj}\, d'_1 & d'_0 \end{pmatrix}$, then $T_{00} := \mathrm{ffLDL}^\dagger(\mathcal{G}_{d_{00}})$ and $T_{11} := \mathrm{ffLDL}^\dagger(\mathcal{G}_{d_{11}})$. The ffLDL† **tree** of $\mathcal{G}$ is defined as $\mathrm{ffLDL}^\dagger(\mathcal{G}) \in \mathcal{T}_m$, by recursion on m:

$$\mathrm{ffLDL}^\dagger(\mathcal{G}) := \mathrm{node}(l_{10};\ d_{00}, d_{11}) \quad (m = 2),$$
$$\mathrm{ffLDL}^\dagger(\mathcal{G}) := \mathrm{node}(l_{10};\ T_{00}, T_{11}) \quad (m \ge 4).$$

The sampler on a tree (Definition A.21). Let $T \in \mathcal{T}_m$ be a tree, and $t \in \mathcal{R}_m^2$ a center. Let $s > 0$ be a real. Let N and d_i be those of Definition A.19. Let $d \in \mathrm{Sub}(T) \cap \mathbb{R}$ be a leaf diagonal with $I(d) = \{j, j+1\}$, and $t_d \in \mathbb{C}$ a center. Define $(\sigma_j, \sigma_{j+1}) := (s/\sqrt{d_j},\ s/\sqrt{d_{j+1}})$ and $(c_j, c_{j+1}) := (\mathrm{Re}\, t_d,\ \mathrm{Im}\, t_d)$. Define the samples $z_j \leftarrow D_{\mathbb{Z}, \sigma_j, c_j}$ and $z_{j+1} \leftarrow D_{\mathbb{Z}, \sigma_{j+1}, c_{j+1}}$, $\hat{z}_d := z_j + i z_{j+1}$ and $\mathrm{leaf}(d, t_d) := \hat{z}_d \in \mathbb{Z} + i\mathbb{Z}$. Define $t_T := t$. For $\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}$ and $t_\nu \in \mathcal{R}_{m'}^2$, define the **sampler on a tree** ν as $\mathrm{ffSampling}(t_\nu, \nu) := \hat{z}_\nu \in (\mathbb{Z}[x]/(x^{m'}+1))^2$, by recursion on m':

$(t_0, t_1) := t_\nu;$
$m' = 2:$
$\quad t_{T_{11}} := t_1, \quad \hat{z}_{T_{11}} := \mathrm{leaf}(T_{11}, t_{T_{11}}),$
$\quad tb_0 := t_0 + (t_1 - \hat{z}_{T_{11}})\, l_{10},$
$\quad t_{T_{00}} := tb_0, \quad \hat{z}_{T_{00}} := \mathrm{leaf}(T_{00}, t_{T_{00}}),$
$\quad \hat{z}_\nu := (\hat{z}_{T_{00}}, \hat{z}_{T_{11}});$
$m' \ge 4:$
$\quad t_{T_{11}} := \mathrm{split}(t_1), \quad \hat{z}_{T_{11}} := \mathrm{ffSampling}(t_{T_{11}}, T_{11}), \quad z_1 := \mathrm{merge}(\hat{z}_{T_{11}}),$
$\quad tb_0 := t_0 + (t_1 - z_1)\, l_{10},$
$\quad t_{T_{00}} := \mathrm{split}(tb_0), \quad \hat{z}_{T_{00}} := \mathrm{ffSampling}(t_{T_{00}}, T_{00}), \quad z_0 := \mathrm{merge}(\hat{z}_{T_{00}}),$
$\quad \hat{z}_\nu := (z_0, z_1).$

The output measure of the sampler on a tree (Definition A.21, Fact A.22). The samples of $\mathrm{ffSampling}(t, T)$ are $z := (z_i)_{i \le N} \in \mathbb{Z}^N$. For $A \subseteq \mathbb{Z}^N$, the **output measure** of $\mathrm{ffSampling}(t, T)$ is $Q_{T,t}(A) := \Pr[z \in A]$. Let (f, g, F, G) satisfy $\forall \psi \in \mathbb{C},\ \psi^n = -1 :\ (fG - gF)(\psi) \ne 0$, and $\epsilon \in (0, 1)$ be a real. The **smoothing parameter** of $\mathbb{Z}^n$ is $\eta_\epsilon(\mathbb{Z}^n) := \inf\{s' > 0 : \rho_{1/s'}(\mathbb{Z}^n \setminus \{0\}) \le \epsilon\}$. The **Gram–Schmidt norm** of B is defined as $\|B\|_{\mathrm{GS}}$, the largest norm of the Gram–Schmidt vectors of the $2n$ rows $x^j(g, -f)$, $j < n$, then $x^j(G, -F)$, $j < n$, each read as its $2n$ coefficients. Let $s \ge \eta_\epsilon(\mathbb{Z}^n)\, \|B\|_{\mathrm{GS}}$ be a real. Let $\mathrm{ffSampling}(t, T)$ and σ_i, $i \le N$, be those of Definition A.21 at (T, t, s). The value of $\mathrm{ffSampling}(t, T)$ at the samples $z := z^* \in \mathbb{Z}^N$ is $\hat{z}(z^*) \in (\mathbb{Z}[x]/(x^n+1))^2$. For $i \le N$, the center c_i at the samples $z_{<i} := z^*_{<i}$ is $c_i(z^*_{<i})$.

$$\forall z^* \in \mathbb{Z}^N :\quad \Pr[\mathrm{ffSampling}(t, T) = \hat{z}(z^*)] = \rho_s((t - \hat{z}(z^*))B) \prod_{i \le N} \rho_{\sigma_i, c_i(z^*_{<i})}(\mathbb{Z})^{-1}.$$

The sampler on a Gram matrix (Definition A.23). Let $m = 2^k$ be a degree, $k \ge 1$, and $\mathcal{G} \in \mathrm{Gram}_m$ a Gram matrix (Definition A.14). Let $t \in \mathcal{R}_m^2$ be a center, and $s > 0$ a real. For $m' \ge 4$ a power of two and $d \in \mathcal{R}_{m'}$, define $(d_0, d_1) := \mathrm{split}(d)$ (Definition A.15) and $\mathcal{G}_d := \begin{pmatrix} d_0 & d_1 \\ \mathrm{conj}\, d_1 & d_0 \end{pmatrix}$. For $d > 0$ and $c \in \mathbb{C}$, define the samples $y' \leftarrow D_{\mathbb{Z}, s/\sqrt{d}, \mathrm{Re}\, c}$ and

$y'' \leftarrow D_{\mathbb{Z},s/\sqrt{d},\mathrm{Im}\,c}$, and $\mathrm{leaf}_s(d,c) := y' + iy'' \in \mathbb{Z} + i\mathbb{Z}$. For $m' = 2^{k'}$ with $1 \le k' \le k$, $\mathcal{G}' \in \mathrm{Gram}_{m'}$ and $t' = (t'_0, t'_1) \in \mathcal{R}^2_{m'}$, define $(l_{10}, d_{00}, d_{11}) := \mathrm{LDL}^\dagger(\mathcal{G}')$ (Definition A.17) and the **sampler on a Gram matrix** $\mathcal{G}'$ as $\mathrm{ffsamp}(t', \mathcal{G}') \in (\mathbb{Z}[x]/(x^{m'}+1))^2$, by recursion on m':

$$
\begin{aligned}
&m' = 2 : \\
&\quad y_1 := \mathrm{leaf}_s(d_{11}, t'_1), \\
&\quad y_0 := \mathrm{leaf}_s(d_{00},\ t'_0 + (t'_1 - y_1)\, l_{10}), \\
&\quad \mathrm{ffsamp}(t', \mathcal{G}') := (y_0, y_1); \\
&m' \ge 4 : \\
&\quad y_1 := \mathrm{merge}(\mathrm{ffsamp}(\mathrm{split}(t'_1), \mathcal{G}_{d_{11}})), \\
&\quad y_0 := \mathrm{merge}(\mathrm{ffsamp}(\mathrm{split}(t'_0 + (t'_1 - y_1)\, l_{10}), \mathcal{G}_{d_{00}})), \\
&\quad \mathrm{ffsamp}(t', \mathcal{G}') := (y_0, y_1).
\end{aligned}
$$

The output measure of the sampler on a Gram matrix. ffsamp is ffsamp (Algorithm 6) at `root` $= 0$ with deepest (Algorithm 7) over $\mathbb{R}$, at `INV_SIGMA` $:= 1/s$. The samples of $\mathrm{ffsamp}(t, \mathcal{G})$, in the order they are taken, are $z := (z_i)_{i \le N} \in \mathbb{Z}^N$, at $N := 2m$. For $A \subseteq \mathbb{Z}^N$, the output measure of $\mathrm{ffsamp}(t, \mathcal{G})$ is $Q'_{\mathcal{G},t}(A) := \Pr[z \in A]$. The equality of $Q'_{\mathcal{G},t}$ and the output measure $Q_{T,t}$ at $T := \mathrm{ffLDL}^\dagger(\mathcal{G})$ is Fact G.12.

Algorithm 6 ffsamp$(t, \mathcal{G}, \texttt{root})$ [L0: `sign_sampler.c:1245-1350`] [L0: `fxp/sign_fxsampler.c:287-329`]

Input: $t \in \mathcal{R}_m^2$; $\mathcal{G}$ (LDL† (Algorithm 5)) at $\nu \in T$ (Definition A.18); s; $\texttt{root} \in \{0,1\}$; $\widetilde{t}_\nu \in (C_{\mathcal{F}}^{m/2})^2$; $\widetilde{\mathcal{G}}$
Precondition: $m \geq 2$ and $s > 0$. $\forall \nu \in T\ \forall \psi:\ g_{00} > 0,\ d_{11} > 0$.
Output (code): $(\widetilde{z}_0, \widetilde{z}_1)$
Output (idealized): $(z_0, z_1) = \text{ffSampling}(t, \text{ffLDL}^\dagger(\mathcal{G}))$ (Fact G.12)
Postcondition: $z_0, z_1 \in \mathbb{Z}[x]/(x^m + 1)$
In the proofs: $\widetilde{t}_j$, l_{10}, d_{jj}, $\mathcal{G}_{d_{jj}}$, $t_{1,j}$, $z_{j,k}$, f_ν^R, $f_\nu^{\mathcal{L}}$, $\widetilde{z}_1$, X, X_0, tb_0, $\widetilde{tb}_0$

$(\widetilde{t}_0, \widetilde{t}_1) \leftarrow \widetilde{t}_\nu$
$(t_0, t_1) \leftarrow t$
$(\widetilde{l}_{10}, \widetilde{d}_{00}, \widetilde{d}_{11}) \leftarrow \text{LDL}^\dagger(\widetilde{\mathcal{G}})$ ▷ in $\mathcal{F}$
$(l_{10}, d_{00}, d_{11}) \leftarrow \text{LDL}^\dagger(\mathcal{G})$
if $\texttt{root} = 1$ **then** ▷ the root only: recursive calls pass 0
  $\widetilde{d}_{11} \leftarrow \text{fl}(q^2/\widetilde{g}_{00})$ ▷ [L0: `fxp/sign_fxpoly.c:162`]
  $d_{11} \leftarrow q^2/g_{00}$
end if
if $m = 2$ **then** ▷ the recursion's end
  return deepest$(\widetilde{t}_\nu, \widetilde{l}_{10}, \widetilde{d}_{00}, \widetilde{d}_{11})$ ▷ in $\mathcal{F}$
  return deepest$(t, l_{10}, d_{00}, d_{11})$ ▷ Algorithm 7
end if
$(\widetilde{d}'_0, \widetilde{d}'_1) \leftarrow \widetilde{\text{split}}_{\text{sa}}(\widetilde{d}_{11})$
$(d'_0, d'_1) \leftarrow \text{split}_{\text{sa}}(d_{11})$
$\widetilde{\mathcal{G}}_{d_{11}} \leftarrow \begin{pmatrix} \widetilde{d}'_0 & \widetilde{d}'_1 \\ \text{conj}\, \widetilde{d}'_1 & \widetilde{d}'_0 \end{pmatrix}$
$\mathcal{G}_{d_{11}} \leftarrow \begin{pmatrix} d'_0 & d'_1 \\ \text{conj}\, d'_1 & d'_0 \end{pmatrix}$
$(t_{1,0}, t_{1,1}) \leftarrow \text{split}(t_1)$
$f_\nu^R \leftarrow \widetilde{\text{split}}(\widetilde{t}_1) - \text{split}(\widetilde{t}_1)$ ▷ in $\mathcal{F}$; the entry shift at T_{11}
$(\widetilde{z}_{1,0}, \widetilde{z}_{1,1}) \leftarrow \text{ffsamp}(\widetilde{\text{split}}(\widetilde{t}_1), \widetilde{\mathcal{G}}_{d_{11}}, 0)$
$(z_{1,0}, z_{1,1}) \leftarrow \text{ffsamp}((t_{1,0}, t_{1,1}), \mathcal{G}_{d_{11}}, 0)$
$\widetilde{z}_1 \leftarrow \widetilde{\text{merge}}(\widetilde{z}_{1,0}, \widetilde{z}_{1,1})$ ▷ Lemma G.18
$z_1 \leftarrow \text{merge}(z_{1,0}, z_{1,1})$
$X \leftarrow \widetilde{t}_0 + (\widetilde{t}_1 - \widetilde{z}_1)\, \widetilde{l}_{10}$ ▷ line 26 on the computed values
$X_0 \leftarrow \widetilde{t}_0 + (\widetilde{t}_1 - z_1)\, l_{10}$ ▷ on the exact z_1, l_{10}
$\widetilde{tb}_0 \leftarrow \widetilde{t}_0 \oplus ((\widetilde{t}_1 \ominus \widetilde{z}_1) \otimes \widetilde{l}_{10})$ ▷ line 26 in $\mathcal{F}$ (Definition A.8)
$tb_0 \leftarrow t_0 + (t_1 - z_1)\, l_{10}$
$(\widetilde{d}_0, \widetilde{d}_1) \leftarrow \widetilde{\text{split}}_{\text{sa}}(\widetilde{d}_{00})$
$(d_0, d_1) \leftarrow \text{split}_{\text{sa}}(d_{00})$
$\widetilde{\mathcal{G}}_{d_{00}} \leftarrow \begin{pmatrix} \widetilde{d}_0 & \widetilde{d}_1 \\ \text{conj}\, \widetilde{d}_1 & \widetilde{d}_0 \end{pmatrix}$
$\mathcal{G}_{d_{00}} \leftarrow \begin{pmatrix} d_0 & d_1 \\ \text{conj}\, d_1 & d_0 \end{pmatrix}$
$(tb_{0,0}, tb_{0,1}) \leftarrow \text{split}(tb_0)$
$f_\nu^{\mathcal{L}} \leftarrow \widetilde{\text{split}}(\widetilde{tb}_0) - \text{split}(X_0)$ ▷ in $\mathcal{F}$; the entry shift at T_{00}
$(\widetilde{z}_{0,0}, \widetilde{z}_{0,1}) \leftarrow \text{ffsamp}(\widetilde{\text{split}}(\widetilde{tb}_0), \widetilde{\mathcal{G}}_{d_{00}}, 0)$
$(z_{0,0}, z_{0,1}) \leftarrow \text{ffsamp}((tb_{0,0}, tb_{0,1}), \mathcal{G}_{d_{00}}, 0)$
$\widetilde{z}_0 \leftarrow \widetilde{\text{merge}}(\widetilde{z}_{0,0}, \widetilde{z}_{0,1})$
$z_0 \leftarrow \text{merge}(z_{0,0}, z_{0,1})$
return $(\widetilde{z}_0, \widetilde{z}_1)$
return (z_0, z_1)

Algorithm 7 deepest$(t, l_{10}, d_{00}, d_{11})$, the recursion's deepest level [L0: `sign_sampler.c:1185-1234`] [L0: `fxp/sign_fxsampler.c:228-269`]

Input: $t = (t_0, t_1) \in \mathbb{C} \times \mathbb{C}$; (l_{10}, d_{00}, d_{11}) (LDL† (Algorithm 5)) at $m = 2$; $\widetilde{t} = (\widetilde{t_0}, \widetilde{t_1}) \in C_{\mathcal{F}} \times C_{\mathcal{F}}$; $(\widetilde{l_{10}}, \widetilde{d_{00}}, \widetilde{d_{11}})$

Precondition: $d_{00}, d_{11} > 0$. $\widetilde{d_{00}}, \widetilde{d_{11}} \geq 0$.

Output (code): $(\widetilde{z_0}, \widetilde{z_1}) \in (\mathbb{Z} + i\mathbb{Z})^2$

Output (idealized): $(z_0, z_1) \in (\mathbb{Z} + i\mathbb{Z})^2$; $\mathrm{Re}\, z_j$, $\mathrm{Im}\, z_j \sim D_{\mathbb{Z},\sigma_j,c}$ at the σ_j and the center c of their lines (Definition A.2)

In the proofs: $\widetilde{r_1}$, r_1, $1/\widetilde{\sigma_1}$, $1/\sigma_1$, $\widetilde{r_0}$, r_0, $1/\widetilde{\sigma_0}$, $1/\sigma_0$, $\widetilde{tb_0}$, tb_0

1: $\widetilde{r_1} \leftarrow \mathrm{fl}(\sqrt{\widetilde{d_{11}}})$
2: $r_1 \leftarrow \sqrt{d_{11}}$
3: $1/\widetilde{\sigma_1} \leftarrow \mathrm{fl}(\widetilde{r_1} \cdot \texttt{INV_SIGMA})$
4: $1/\sigma_1 \leftarrow r_1 \cdot \texttt{INV_SIGMA}$
5: $\mathrm{Re}\, \widetilde{z_1} \leftarrow \mathrm{SamplerZ}(\mathrm{Re}\, \widetilde{t_1}, 1/\widetilde{\sigma_1})$
6: $\mathrm{Re}\, z_1 \leftarrow D_{\mathbb{Z},\sigma_1,\mathrm{Re}\, t_1}$
7: $\mathrm{Im}\, \widetilde{z_1} \leftarrow \mathrm{SamplerZ}(\mathrm{Im}\, \widetilde{t_1}, 1/\widetilde{\sigma_1})$
8: $\mathrm{Im}\, z_1 \leftarrow D_{\mathbb{Z},\sigma_1,\mathrm{Im}\, t_1}$
9: $\widetilde{tb_0} \leftarrow \widetilde{t_0} \oplus ((\widetilde{t_1} \ominus \widetilde{z_1}) \otimes \widetilde{l_{10}})$
10: $tb_0 \leftarrow t_0 + (t_1 - z_1)\, l_{10}$
11: $\widetilde{r_0} \leftarrow \mathrm{fl}(\sqrt{\widetilde{d_{00}}})$
12: $r_0 \leftarrow \sqrt{d_{00}}$
13: $1/\widetilde{\sigma_0} \leftarrow \mathrm{fl}(\widetilde{r_0} \cdot \texttt{INV_SIGMA})$
14: $1/\sigma_0 \leftarrow r_0 \cdot \texttt{INV_SIGMA}$
15: $\mathrm{Re}\, \widetilde{z_0} \leftarrow \mathrm{SamplerZ}(\mathrm{Re}\, \widetilde{tb_0}, 1/\widetilde{\sigma_0})$
16: $\mathrm{Re}\, z_0 \leftarrow D_{\mathbb{Z},\sigma_0,\mathrm{Re}\, tb_0}$
17: $\mathrm{Im}\, \widetilde{z_0} \leftarrow \mathrm{SamplerZ}(\mathrm{Im}\, \widetilde{tb_0}, 1/\widetilde{\sigma_0})$
18: $\mathrm{Im}\, z_0 \leftarrow D_{\mathbb{Z},\sigma_0,\mathrm{Im}\, tb_0}$
19: **return** $(\widetilde{z_0}, \widetilde{z_1})$
20: **return** (z_0, z_1)

The base sampler (Definition A.24). The **base sampler** is SamplerZ (Algorithm 8). Let $\mathcal{F}$ be a realization (Definition A.4). Let `isigma` $\in \mathcal{F}$ with `isigma` > 0, and $c \in \mathcal{F}$ a center. Define $\sigma := 1/\texttt{isigma}$. For $A \subseteq \mathbb{Z}$, the probability measure of the base sampler in $\mathcal{F}$ is defined as $B^{\mathcal{F}}_{\sigma,c}(A) := \Pr[\mathrm{SamplerZ}(c, \texttt{isigma}) \in A]$, over the samples of SamplerZ and BerExp (Algorithm 9), SamplerZ executed in $\mathcal{F}$ at $\mu := c$.

Algorithm 8 SamplerZ(μ, isigma), the base sampler `sampler_next` [L0: `sign_sampler.c:916-968`] [L0: `fxp/sign_fxsampler.c:183-216`] [L1: FHK+20, Alg. 15, their SamplerZ(μ, σ') at $\sigma' := 1/\texttt{isigma}$; their BaseSampler's 72-bit table FHK+20, Alg. 12 replaced by the code's table `GAUSS0` [L0: `sign_sampler.c:89-108`]]

Input: $\mu \in \mathcal{F}$; $\texttt{isigma} \in \mathcal{F}$; $\sigma_{\min}$ (Definition A.25); $C_0 = \widetilde{(1/(2\sigma_0^2))}$, $\sigma_0 = 1.8205$ [L0: `sign_sampler.c:18-30`] [L0: `fxp/fxp_consts.h:2073-2089`]
Precondition: $\texttt{isigma} > 0$.
Output (code): $s + z \in \mathbb{Z}$
Output (idealized): $s + z \sim P_0$ (Lemma G.64) at $(1/\texttt{isigma}, \mu)$
In the proofs: s, $\widetilde{r}$, r, $\widetilde{dss}$, dss, $\widetilde{ccs}$, ccs, (z_0, b), z, $\widetilde{a}_x$, a_x, $\widetilde{b}_x$, b_x, $\widetilde{x}$, x

1: $s \leftarrow \lfloor \mu \rceil$
2: $\widetilde{r} \leftarrow \mathrm{fl}(\mu - s)$
3: $r \leftarrow \mu - s$
4: $\widetilde{dss} \leftarrow \mathrm{fl}(\mathrm{fl}(\texttt{isigma}^2)/2)$
5: $dss \leftarrow \texttt{isigma}^2/2$
6: $\widetilde{ccs} \leftarrow \mathrm{fl}(\texttt{isigma} \cdot \sigma_{\min})$
7: $ccs \leftarrow \texttt{isigma} \cdot \sigma_{\min}$
8: **loop**
9: $\quad (z_0, b) \leftarrow (\texttt{GAUSS0}, \{0, 1\})$
10: $\quad z \leftarrow b + (2b - 1)z_0$
11: $\quad \widetilde{a}_x \leftarrow \mathrm{fl}(\mathrm{fl}((z - \widetilde{r})^2)\, \widetilde{dss})$
12: $\quad a_x \leftarrow (z - r)^2 dss$
13: $\quad \widetilde{b}_x \leftarrow \mathrm{fl}(z_0^2 C_0)$
14: $\quad b_x \leftarrow z_0^2 C_0$
15: $\quad \widetilde{x} \leftarrow \mathrm{fl}(\widetilde{a}_x - \widetilde{b}_x)$
16: $\quad x \leftarrow (z - r)^2 dss - z_0^2 C_0$ $\quad \triangleright = a_x - b_x$
17: $\quad$ **if** BerExp$(\widetilde{x}, \widetilde{ccs}) = 1$ **then**
18: $\quad\quad$ **return** $s + z$
19: $\quad$ **end if**
20: $\quad$ **if** BerExp$(x, ccs) = 1$ **then**
21: $\quad\quad$ **return** $s + z$
22: $\quad$ **end if**
23: **end loop**

Algorithm 9 BerExp(x, ccs), the acceptance `ber_exp` with `expm_p63` [L0: `sign_sampler.c:780-912`] [L0: `fxp/sign_fxsampler.c:88-181`] [L1: FHK+20, Alg. 14, their BerExp(x, ccs) at the same (x, ccs)]

Input: $x \in \mathcal{F}$; $ccs \in \mathcal{F}$; `LOG2` $= \widetilde{\ln 2}$, `INV_LOG2` $= \widetilde{(1/\ln 2)}$; $(C_i)_{i \le 12}$ the FACCT coefficients [L0: `sign_sampler.c:787-801`]
Precondition: $x \ge 0$. $0 < ccs \le 1$.
Output (code): $\beta = [w < z_{\text{acc}}] \in \{0, 1\}$
Output (idealized): $\beta \in \{0, 1\}$, $\Pr[\beta = 1] = ccs\, e^{-x}$
Postcondition: $\Pr[\beta = 1] = z_{\text{acc}}/2^{64}$ (Fact G.66)
In the proofs: ϵ_L, si, $\widetilde{r}'$, r', s, y, z_{acc}

1: $\epsilon_L \leftarrow$ `INV_LOG2` $\cdot$ `LOG2` $- 1$
2: $si \leftarrow \text{trunc}(\text{fl}(\widetilde{x} \cdot$ `INV_LOG2`$))$
3: $\widetilde{r}' \leftarrow \text{fl}(\widetilde{x} - \text{fl}(si \cdot$ `LOG2`$))$
4: $r' \leftarrow \max(\widetilde{r}', 0)$ ▷ `fxp/` only
5: $s \leftarrow \min(si, 63)$
6: $Z \leftarrow \lfloor r' 2^{63} \rfloor \ll 1$ ▷ to line 12: their ApproxExp(r', ccs) FHK+20, Alg. 13
7: $y \leftarrow C_0$
8: **for** $i = 1, \ldots, 12$ **do**
9: $\quad y \leftarrow C_i - \lfloor Zy/2^{64} \rfloor$
10: **end for**
11: $W \leftarrow \lfloor ccs\, 2^{63} \rfloor \ll 1$
12: $y \leftarrow \lfloor Wy/2^{64} \rfloor$
13: $z_{\text{acc}} \leftarrow ((y \ll 1) - 1) \gg s$
14: **if** $si \ge 64$ **then**
15: $\quad z_{\text{acc}} \leftarrow 0$ ▷ `fxp/` only (Lemma G.80) [L0: `fxp/sign_fxsampler.c:169`]
16: **end if**
17: $w \leftarrow \{0, \ldots, 2^{64} - 1\}$
18: **return** $[w < z_{\text{acc}}]$

The signer and its two probability measures (Definition A.25). The hashed message $\mathsf{h}(\mathsf{m})$ is the input of ffSampling$^{\mathcal{F}}$ (Algorithm 10). Let $\sigma_{\min}$ be the number of the signer's stored word at $\log_2 n$: in the fixed-point signer, `FXP_SIGMA_MIN` of `fxp/` in the realization of Definition A.4, item 8. The **standard deviation parameter** of the signer is $s := 1.17\sqrt{q}\,\sigma_{\min}$. Define $\Lambda := \Lambda(B)$. The lattice Gaussian at the center is $D_{\Lambda,s,tB} := D_{\Lambda(B),s,tB}$ (Definition A.12). Let $c \in \{t, t_{\text{frac}}\}$ be the center the signer takes. The center c of a statement names the rule by which the signer forms it from $\mathsf{h}(\mathsf{m})$: t at line 17 or t_{frac} at line 7 of ffSampling$^{\mathcal{F}}$. The **signer** in a realization $\mathcal{F}$ is ffSampling$^{\mathcal{F}}(B, s, c)$, ffSampling$^{\mathcal{F}}$ (Algorithm 10) executed in $\mathcal{F}$ at (B, s, c). Define ffSampling$^{\mathcal{F}}$:= ffSampling$^{\mathcal{F}}(B, s, c)$, $\mathcal{F}$ a realization of Definition A.4. Define ffSampling$^{\mathbb{R}}$:= ffSampling$^{\mathbb{R}}(B, s, c)$, $\mathbb{R}$ the realization of Definition A.4. At the i-th leaf sample, line 24 of ffSampling$^{\mathcal{F}}$, define $z_{<i} := (z_1, \ldots, z_{i-1})$. For $A \subseteq \mathbb{Z}^N$ and z the output of ffSampling$^{\mathcal{F}}$, define $P(A) := \Pr[z \in A]$. For $A \subseteq \mathbb{Z}^N$ and z the output of ffSampling$^{\mathbb{R}}$, define $Q(A) := \Pr[z \in A]$. Let $(\mu,$ `isigma`$)$ be the arguments of the i-th call SamplerZ$(\mu,$ `isigma`$)$ of ffSampling$^{\mathcal{F}}$. The **leaf parameters**, functions of $z_{<i}$, are:

- $\widetilde{t}_i := \mu$ at that call of ffSampling$^{\mathcal{F}}$, lines 1 to 18 of deepest (Algorithm 7) in $\mathcal{F}$;
- $\widetilde{\sigma}_i :=$ 1/`isigma` at that call of ffSampling$^{\mathcal{F}}$;
- t_i, the center of the i-th leaf sample of ffSampling$^{\mathbb{R}}$, the shaded lines 1 to 18 of deepest over $\mathbb{R}$;
- σ_i, the standard deviation of that sample.

The conditional measures of a leaf sample.

- $\forall x \in \mathbb{Z}: \; P(z_i = x \,|\, z_{<i}) = B^{\mathcal{F}}_{\widetilde{\sigma}_i, \widetilde{t}_i}(\{x\})$.

- $\forall x \in \mathbb{Z}:\ Q(z_i = x \mid z_{<i}) = D_{\mathbb{Z},\sigma_i,t_i}(x)$.
- In ffSampling$^{\mathbb{R}}$, the leaf samples are taken from $D_{\mathbb{Z},\sigma_i,t_i}$, not from the base sampler executed in real arithmetic, whose output measure is P_0 of Lemma G.64.

Algorithm 10 ffSampling$^{\mathcal{F}}(B, s, t)$, the signer's sampler [L0: `sign_core.c:130-204`] [L0: `fxp/sign_fxcore.c:158-216`] [L0: `sign_fpoly.c:2663-2712`] [L0: `fxp/sign_fxcore.c:198`]

Input: (f, g, F, G) (keygen (Algorithm 11)); $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$; s; $\mathcal{F}$ (Definition A.4); `fractional_mode` $\in \{0, 1\}$, the code's `target_mode` [L0: `fxp/sign_fxcore.c:110`]
Precondition: $s > 0$. Fact A.34 at (f, g, F, G).
Output (code): $(\widetilde{z}_i)_{i \le N} = \text{ffSampling}^{\mathcal{F}}(B, s, t) \in \mathbb{Z}^N$, $N = 2n$
Output (idealized): $(z_i)_{i \le N} = \text{ffSampling}^{\mathbb{R}}(B, s, t) \in \mathbb{Z}^N$
Postcondition: $z = (z_i)_{i \le N}$, z_i the i-th output of SamplerZ at line 24
In the proofs: $\widetilde{B}$, B, $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$, (g_{00}, g_{01}, g_{11}), $\widetilde{\hat{h}}$, $\hat{h}$, H, $\widetilde{t}$, t, e_{root}, $\widetilde{z}'$, z'

1: $\widetilde{B} \leftarrow \widetilde{\text{FFT}} \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}$
2: $B \leftarrow \text{FFT} \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}$
3: $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11}) \leftarrow \text{Gram}(\widetilde{B})$ ▷ in $\mathcal{F}$
4: $(g_{00}, g_{01}, g_{11}) \leftarrow \text{Gram}(B)$
5: **if** `fractional_mode` $= 1$ **then**
6: $\quad(\widetilde{t}, t_{\text{int}}) \leftarrow \text{center}_{\text{frac}}(\mathsf{h}(\mathsf{m}), f, F)$ ▷ in $\mathcal{F}_{\text{fx}}$
7: $\quad(t, t_{\text{int}}) \leftarrow \text{center}_{\text{frac}}(\mathsf{h}(\mathsf{m}), f, F)$
8: **else**
9: $\quad\widetilde{\hat{h}} \leftarrow \widetilde{\text{FFT}}(\mathsf{h}(\mathsf{m}))$ ▷ $\|\mathsf{h}(\mathsf{m})\| < \sqrt{n}\,q$, $\|\mathsf{h}(\mathsf{m})\|_1 < nq$
10: $\quad\hat{h} \leftarrow \text{FFT}(\mathsf{h}(\mathsf{m}))$
11: $\quad H \leftarrow nq$ ▷ $\ge \max_\psi |\hat{h}(\psi)|$
12: $\quad(\widetilde{b}_{01}, \widetilde{b}_{11}) \leftarrow (\widetilde{\text{FFT}}(-f), \widetilde{\text{FFT}}(-F))$
13: $\quad(\hat{f}, \hat{F}) \leftarrow (\text{FFT}(f), \text{FFT}(F))$
14: $\quad(b_{01}, b_{11}) \leftarrow (-\hat{f}, -\hat{F})$ ▷ Fact A.33, item 2
15: $\quad\widetilde{(1/q)} \leftarrow \text{fl}(1/q)$ ▷ Definition A.4
16: $\quad\widetilde{t}_0 \leftarrow (\widetilde{\hat{h}} \otimes \widetilde{b}_{11}) \otimes \widetilde{(1/q)}$
17: $\quad t_0 \leftarrow \text{FFT}(\mathsf{h}(\mathsf{m}))\,(-F)\,(1/q)$
18: $\quad\widetilde{t}_1 \leftarrow (\widetilde{\hat{h}} \otimes \widetilde{b}_{01}) \otimes \widetilde{(-1/q)}$
19: $\quad t_1 \leftarrow (-f)\,\text{FFT}(\mathsf{h}(\mathsf{m}))\,(-1/q)$
20: $\quad e_{\text{root}} \leftarrow \widetilde{t} - t$ ▷ Lemma G.54
21: **end if**
22: `root` $\leftarrow [\mathcal{F} = \mathcal{F}_{\text{fx}}]$ ▷ 1 in $\mathcal{F}_{\text{fx}}$ at both centers: the root's d_{11} by the NTRU identity [L0: `fxp/sign_fxsampler.c:338`]
23: $(\widetilde{z}_0, \widetilde{z}_1) \leftarrow \text{ffsamp}(\widetilde{t}, (\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11}), \texttt{root})$ ▷ in $\mathcal{F}$
24: $(z_0, z_1) \leftarrow \text{ffsamp}(t, (g_{00}, g_{01}, g_{11}), \texttt{root})$
25: **if** `fractional_mode` $= 1$ **then**
26: $\quad\widetilde{z}' \leftarrow (\widetilde{z}_0, \widetilde{z}_1)$
27: $\quad z' \leftarrow (z_0, z_1)$
28: $\quad(\widetilde{z}_0, \widetilde{z}_1) \leftarrow (t_{\text{int}} + \widetilde{z}') \bmod q$ ▷ [L0: `fxp/sign_fxcore.c:94-105`]
29: $\quad(z_0, z_1) \leftarrow (t_{\text{int}} + z') \bmod q$
30: **end if**
31: **return** $(\widetilde{z}_i)_{i \le N}$
32: **return** $(z_i)_{i \le N}$

Counts of a tree (Fact A.31). Let m be a degree and $T \in \mathcal{T}_m$ a tree. Define $h := \log_2 m$.

- $\forall k < h : |\{T' \in \mathrm{Sub}(T) : \mathrm{depth}(T') = k\}| = 2^k$ and $|\mathrm{Sub}(T) \cap \mathbb{R}| = m$.
- $\forall \nu \in \mathrm{Sub}(T) \setminus \mathbb{R} : I(\nu) = I(R(\nu)) \sqcup I(L(\nu))$ and $\max I(R(\nu)) < \min I(L(\nu))$.

The Gram form of $\mathcal{G}$ and the Gram matrix of a node ν (Definition A.32). Let m be a power of two, $\mathcal{G} \in \mathrm{Gram}_m$ a Gram matrix (Definition A.14), and $x = (x_0, x_1) \in \mathcal{R}_m^2$ a pair. The **half roots** are $\psi_k := e^{i\pi(2k+1)/m}$, $k < m/2$, the roots of $x^m + 1$ with positive imaginary part. The **Gram form** of $\mathcal{G}$ is $Q_{\mathcal{G}}(x) := \frac{2}{m} \sum_{k<m/2} x(\psi_k)\mathcal{G}(\psi_k)x(\psi_k)^\dagger$. Define $T := \mathrm{ffLDL}^\dagger(\mathcal{G})$ at $m = n$. The Gram matrix of the root is $\mathcal{G}_T := \mathcal{G}$. Let $\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T)$ be a node with $\nu = \mathrm{ffLDL}^\dagger(\mathcal{G}_\nu)$. The Gram matrices of its children are $\mathcal{G}_{T_{00}} := \mathcal{G}_{d_{00}}$ and $\mathcal{G}_{T_{11}} := \mathcal{G}_{d_{11}}$, those of Definition A.20 at $\mathcal{G}_\nu$.

The Gram form of a basis is the squared norm. By Proposition G.15, $Q_{BB^\dagger}(x) = \|xB\|^2$ for a basis B over $\mathcal{R}_n$.

The key's Gram determinant (Fact A.33). Let $\psi \in \mathbb{C}$ with $\psi^n = -1$ be a root of $x^n + 1$. Define $g_{00} := |f(\psi)|^2 + |g(\psi)|^2$, $g_{11} := |F(\psi)|^2 + |G(\psi)|^2$ and $g_{01} := g(\psi)\,\mathrm{conj}\,G(\psi) + f(\psi)\,\mathrm{conj}\,F(\psi)$, the entries of $\mathcal{G}(\psi)$. Define $d_{11} := g_{11} - |g_{01}|^2/g_{00}$, that of Definition A.17. At the root node, $\kappa := |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$, and $\kappa_{\mathrm{root}} := \max_\psi \kappa$.

- $fG - gF = q$ in $\mathcal{R}_n$.
- $g_{00}g_{11} - |g_{01}|^2 = q^2$.
- $g_{00} > 0$.
- $d_{11} = q^2/g_{00}$.
- $\kappa = |g_{01}|^2/q^2$.
- $\kappa_{\mathrm{root}} = \max_\psi |g_{01}|^2/q^2$.

Algorithm 11 keygeneration(seed, c), the reference's key generation under the four checks of [L2: BFLP26, Alg. 2] and the three tail checks at the center c, over $\mathbb{R}$ and in $\mathcal{F}_{\mathrm{fx}}$ [L0: `fxp/kgen_fx.c:113-212`]

Input: seed; $c \in \{t, t_{\mathrm{frac}}\}$ (Definition A.25), by default `FXP_TARGET_MODE` [L0: `fxp/sign_fxp.h:704-706`]; $(\gamma_{fg}, \gamma_{\mathrm{hyb}}, \gamma_{FG}, \gamma_{\mathrm{root}}) = (275, 4.75, 4500, 27)$ at $n = 512$, $(280, 5.75, 6800, 34)$ at $n = 1024$ [L0: `fxp/kgen_fx.c:97-111`]

Output (code): (f, g, F, G) or $\perp$

Postcondition: the condition of line 10 (Proposition 5.8; Definition 5.5)

1: attempt $\leftarrow 0$ ▷ a failed check regenerates the pair [L0: `fxp/kgen_fx.c:160-212`]
2: **repeat** ▷ at most `max_attempts` times [L0: `fxp/kgen_fx.c:160`]
3: $(f, g, F, G) \leftarrow$ `fndsa_keygen_seeded`$(\mathrm{seed} \,\|\, (\mathrm{attempt} \bmod 2^8))$ ▷ [L0: `kgen.c:41-53`]
4: **if** $f \bmod q \notin ((\mathbb{Z}/q\mathbb{Z})[x]/(x^n + 1))^\times \vee \exists i < n :\ (gF/f \bmod q)_{[i]} \in [128, q - 128]$ **then**
5: **return** $\perp$ ▷ an abort [L0: `fxp/kgen_fx.c:170-184`]
6: **end if**
7: attempt $\leftarrow$ attempt $+ 1$
8: $(\widetilde{sq}_{fg}, \widetilde{sq}_{\mathrm{hyb}}, \widetilde{sq}_{FG}, \widetilde{sq}_{\mathrm{root}}) \leftarrow$ keychecks(f, g, F, G) ▷ [L0: `fxp/kgen_fx.c:186`]
9: $(ok_\mu, ok_\delta, ok_B) \leftarrow$ tailcheck(f, g, F, G, c) ▷ [L0: `fxp/kgen_fx.c:205-209`]
10: **until** $\widetilde{sq}_{fg} \le \mathrm{fl}(\gamma_{fg}^2) \wedge \widetilde{sq}_{\mathrm{hyb}} \le \mathrm{fl}(\gamma_{\mathrm{hyb}}^2) \wedge \widetilde{sq}_{FG} \le \mathrm{fl}(\gamma_{FG}^2) \wedge \widetilde{sq}_{\mathrm{root}} \le \mathrm{fl}(\gamma_{\mathrm{root}}^2) \wedge ok_\mu \wedge ok_\delta \wedge ok_B$ ▷ Definition I.19, items 3, 4, 5 [L0: `fxp/kgen_fx.c:188-208`]
11: **return** (f, g, F, G)

The rounded thresholds of the key checks (Definition A.35). Let $(\gamma_{fg}, \gamma_{\mathrm{hyb}}, \gamma_{FG}, \gamma_{\mathrm{root}})$ be the degree's thresholds of keygen (Algorithm 11). The **rounded thresholds** raise the four thresholds by the roundings of the checks' comparisons:

- $\check{\gamma}_{fg} := (\gamma_{fg}^2 + 2^{-64})^{1/2}$;

- $\check{\gamma}_{FG} := (\gamma_{FG}^2 + 2^{-64})^{1/2}$;
- $\check{\gamma}_{\text{hyb}} := (\gamma_{\text{hyb}}^2 + 2^{-65})^{1/2}$;
- $\check{\gamma}_{\text{root}} := ((\gamma_{\text{root}}^2 + 2^{-65})(1 + 2^{-65}\check{\gamma}_{\text{hyb}}^4/q^2) + 2^{-64}\check{\gamma}_{\text{hyb}}^4/q^2)^{1/2}$.

The Gram deltas of a checked key (Definition A.36). Let $h := \log_2 n$, and ζ the absolute bound of $\mathcal{F}$. Define $R_{h-1} := (1+\sqrt{2}\,\zeta)^{h-1} - 1$, $A_0 := 0$ and, for $j < h-1$, $A_{j+1} := \sqrt{2}(1+\sqrt{2}\,\zeta)A_j + 4\sqrt{2}\,\zeta\sqrt{n}$, the bounds of Lemma H.11 at $(0,\zeta)$, and $k_H := 7$ and $k'_H := 7\sqrt{2}$, the constants of Lemmas G.22 and G.23 at $u = 0$. The **Gram deltas** bound the perturbations of a checked key's computed FFT images and computed Gram matrix entries:

- $\delta_{fg} := R_{h-1}(\check{\gamma}_{fg}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$;
- $\delta_{FG} := R_{h-1}(\check{\gamma}_{FG}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$;
- $\gamma'_{fg} := \check{\gamma}_{fg} + \delta_{fg}$;
- $\gamma'_{FG} := \check{\gamma}_{FG} + \delta_{FG}$;
- $E_{00} := k_H\zeta + 4\gamma'_{fg}\delta_{fg} + 2\delta_{fg}^2$;
- $E_{11} := k_H\zeta + 4\gamma'_{FG}\delta_{FG} + 2\delta_{FG}^2$;
- $E_{01} := k'_H\zeta + 2(\gamma'_{fg}\delta_{FG} + \gamma'_{FG}\delta_{fg} + \delta_{fg}\delta_{FG})$.

The perturbation bounds of a checked key (Definition A.37). The **perturbation bounds** are the floor, the ceiling and the spread of the diagonals a checked key's Gram deltas admit:

- $m_0 := q/\check{\gamma}_{\text{hyb}}^2 - E_{00}$;
- $M_0 := q\check{\gamma}_{\text{hyb}}^2 + E_{00}$;
- $d_{\text{lo}} := \min(m_0, q^2/M_0)$;
- $d_{\text{hi}} := \max(M_0, q^2/m_0)$;
- $\bar{\varsigma} := d_{\text{hi}}/d_{\text{lo}}$;
- $\bar{g}_{11} := 2\gamma'^2_{FG}$.

Algorithm 12 keychecks(f,g,F,G), the four coefficient checks of [L2: BFLP26, Alg. 2] on a key, over $\mathbb{R}$ and in $\mathcal{F}_{\text{fx}}$ [L0: `fxp/kgen_fx.c:60-94`] [L0: `fxp/kgen_fx.c:186-202`]

Input: (f,g,F,G) (keygen (Algorithm 11), line 3); $(\gamma_{fg}, \gamma_{\text{hyb}}, \gamma_{FG}, \gamma_{\text{root}})$ (keygen) [L0: `fxp/kgen_fx.c:97-111`]

Output (code): $\widetilde{sq}_{fg}, \widetilde{sq}_{\text{hyb}}, \widetilde{sq}_{FG}, \widetilde{sq}_{\text{root}} \in \mathcal{F}_{\text{fx}}$

In the proofs: $\widetilde{\hat{p}}$, $\hat{p}$, $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$, (g_{00}, g_{01}, g_{11}), lo, hi, num_ψ

1: $\forall p \in \{f,g,F,G\}:\ \widetilde{\hat{p}} \leftarrow \widetilde{\text{FFT}}(p)$ ▷ [L0: `fxp/kgen_fx.c:71-78`]

2: $\forall p \in \{f,g,F,G\}:\ \hat{p} \leftarrow \text{FFT}(p)$

3: $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11}) \leftarrow \text{Gram}\begin{pmatrix} \widetilde{\hat{g}} & \widetilde{\hat{f}} \\ \widetilde{\hat{G}} & \widetilde{\hat{F}} \end{pmatrix}$ ▷ [L0: `fxp/kgen_fx.c:81`]

4: $(g_{00}, g_{01}, g_{11}) \leftarrow \text{Gram}\begin{pmatrix} \hat{g} & -\hat{f} \\ \hat{G} & -\hat{F} \end{pmatrix}$ ▷ Lemma G.22

5: $\widetilde{sq}_{fg} \leftarrow \max_\psi \max(\text{fl}(\widetilde{\hat{f}}_r^2) + \text{fl}(\widetilde{\hat{f}}_i^2), \text{fl}(\widetilde{\hat{g}}_r^2) + \text{fl}(\widetilde{\hat{g}}_i^2))$ ▷ [L0: `fxp/kgen_fx.c:37`] [L0: `fxp/kgen_fx.c:79`]

6: $lo \leftarrow \min_\psi \widetilde{g}_{00}$ ▷ [L0: `fxp/kgen_fx.c:88`]

7: $hi \leftarrow \max_\psi \widetilde{g}_{00}$ ▷ [L0: `fxp/kgen_fx.c:89`]

8: $\widetilde{sq}_{\text{hyb}} \leftarrow \max(\text{fl}(hi/q), \text{fl}(q/lo))$ ▷ [L0: `fxp/kgen_fx.c:93`]

9: $\widetilde{sq}_{FG} \leftarrow \max_\psi \max(\text{fl}(\widetilde{\hat{F}}_r^2) + \text{fl}(\widetilde{\hat{F}}_i^2), \text{fl}(\widetilde{\hat{G}}_r^2) + \text{fl}(\widetilde{\hat{G}}_i^2))$ ▷ [L0: `fxp/kgen_fx.c:80`]

10: $\forall \psi:\ num_\psi \leftarrow \text{fl}(\widetilde{g}_{01,r}(\psi)^2) + \text{fl}(\widetilde{g}_{01,i}(\psi)^2)$ ▷ [L0: `fxp/kgen_fx.c:90`]

11: $\widetilde{sq}_{\text{root}} \leftarrow \max_\psi \text{fl}(num_\psi / \text{fl}(\widetilde{g}_{00}^2))$ ▷ [L0: `fxp/kgen_fx.c:91`]

12: **return** $(\widetilde{sq}_{fg}, \widetilde{sq}_{\text{hyb}}, \widetilde{sq}_{FG}, \widetilde{sq}_{\text{root}})$

Key generation checks (Fact A.34). Let $\psi \in \{\psi_k : k < n/2\}$ be a half root (Definition A.32 at $m := n$). Define $f_{[i]}$ and $g_{[i]}$ as the coefficients of $f = \sum_{i<n} f_{[i]} x^i$ and $g = \sum_{i<n} g_{[i]} x^i$. Define $\mathrm{AM}_\psi(x) := \mathrm{AM}_{\mathrm{all}}((x(\psi))_\psi) = (2/n)\sum_\psi x(\psi)$ (Definition A.46), the **mean over the half roots**.

- $\sum_{i<n} f_{[i]}^2 + g_{[i]}^2 < 16823$ and $\mathrm{AM}_\psi(g_{00}) = \sum_{i<n} f_{[i]}^2 + g_{[i]}^2 \le 16822 < 1.17^2 q$.
- $\mathrm{AM}_\psi(q^2/g_{00}) < (0.999 \cdot 1.17)^2 q = 16788.7841$.

From the coefficient norms to the means over the half roots. The two identities are Proposition G.15; `check_ortho_norm` bounds the coefficient norm of the pair $x \in \mathcal{R}_n^2$ with $\forall \psi \in \mathbb{C},\ \psi^n = -1 :\ x(\psi) = q\,(\mathrm{conj}\, g(\psi), -\mathrm{conj}\, f(\psi))/g_{00}(\psi)$ and $|x(\psi)|^2 = q^2/g_{00}(\psi)$.

3.3 The objects of the main theorem

Structure. Theorem 1.1 names five objects: the event on which it holds, the perturbations the arithmetic leaves at a leaf, the base sampler's two measures at a leaf, the ratio of the three normalizers at a leaf, and the factor R its bound carries; the last paragraph's divergence factor is that of its sharper form, Theorem F.4. Sections 4.3 and 4.5 use the first two at their own Rényi orders.

Standing symbols. The standing symbols of Section 3.2 stand here. The other standing symbols are:

- $\alpha > 1$, the Rényi order, and $\tau > 1$, the tail-cut radius;
- $(\widetilde{\sigma}_i, \widetilde{t}_i)$, the computed leaf parameters, (σ_i, t_i), the ideal ones, and P and Q, the output measures of ffSampling$^{\mathcal{F}}$ and ffSampling$^{\mathbb{R}}$ (Definition A.25);
- S, the tail-cut event, $S' \subseteq S$, a sub-event, $S'_{<i}$, the prefix sets of S', and C_i, the fringe sets (Definition A.26);
- δ_i and Δ_i, the leaf perturbations, $\bar{\delta}$, the bound of δ_i, and $\bar{W}_{S'}$, the supremum of the sum of the squared shifts over the squared standard deviations (Definition A.27);
- $\mathcal{Z}_i$, the leaf sets, $\widetilde{B}_i$ and $\widetilde{D}_i$, the computed and the ideal measure at a leaf, $\bar{\rho}_B$, the base sampler's moment, and $\bar{U}$, $\bar{p}_C$, κ_C, the fringe quantities (Definition A.28);
- $\Phi_{\alpha_L, i}$, the normalizer ratio at a leaf, and $\bar{\phi}$, its bound (Definition A.29);
- $\alpha_L := 2\alpha - 1$, and R, the factor of the bound (Definition A.30).

The tail-cut event, a sub-event and the conditional probability measures (Definition A.26). The **tail-cut event** is defined as $S := \{\, z \in \mathbb{Z}^N : \forall i \le N\ |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$, and the **tail** is $S^c := \mathbb{Z}^N \setminus S$. A **sub-event** is an event $S' \subseteq S$, taken as S where a statement names no other. Define $S'^c := \mathbb{Z}^N \setminus S'$. For $i \le N$, the **prefix sets** of S' are $S'_{<i} := \{\, z_{<i} : z \in S' \,\}$, and $S_{<i}$ is $S'_{<i}$ at $S' := S$. For $i \le N$, let $C_i(z_{<i}) \subseteq \{\, z_i \in \mathbb{Z} : |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$ be the **fringe sets**, empty unless the signer's base sampler names them. The **fringe leaves** of $z \in \mathbb{Z}^N$ are $\mathcal{K}(z) := \{\, i \le N : z_i \in C_i(z_{<i}) \,\}$. The **fringe class** of S with $k \le N$ fringe leaves is $S_k := \{\, z \in S : |\mathcal{K}(z)| = k \,\}$, and that of S' is $S'_k := \{\, z \in S' : |\mathcal{K}(z)| = k \,\}$. For $A \subseteq \mathbb{Z}^N$, the **conditional probability measures** on S are $P_S(A) := P(A \cap S)/P(S)$ and $Q_S(A) := Q(A \cap S)/Q(S)$, and those on the core class of S' are $P_{S'_0}(A) := P(A \cap S'_0)/P(S'_0)$ and $Q_{S'_0}(A) := Q(A \cap S'_0)/Q(S'_0)$.

The leaf perturbations of one signature (Definition A.27). Let $i \le N$ and $z_{<i}$ be a prefix. The **relative perturbation** $\delta_i(z_{<i})$ is defined by $\widetilde{\sigma}_i(z_{<i}) =: \sigma_i(z_{<i})\,(1 + \delta_i(z_{<i}))$, and the **shift** is $\Delta_i(z_{<i}) := \widetilde{t}_i(z_{<i}) - t_i(z_{<i})$. The **weighted square sum** of the shifts over S' is $\bar{W}_{S'} := \sup_{z \in S'} \sum_{i \le N} \Delta_i(z_{<i})^2/\sigma_i(z_{<i})^2$, and $\bar{W}_S$ is $\bar{W}_{S'}$ at $S' := S$. Let $\bar{\delta} \ge \max_{i \le N} \sup_{z_{<i} \in S'_{<i}} |\delta_i(z_{<i})|$ be the **bound** of the relative perturbation.

A leaf's computed and ideal probability measures on $\mathcal{Z}_i$ (Definition A.28). Let $i \le N$ and $z_{<i}$ be a prefix. The **computed measure** at the leaf is $\widetilde{B}_i := B^{\mathcal{F}}_{\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}$, the conditional measure $A \mapsto P(z_i \in A \mid z_{<i})$ on $A \subseteq \mathbb{Z}$ (Definition A.25, item 1), and the **ideal measure** is $\widetilde{D}_i := D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$. For $z \in \mathbb{Z}^N$, define $P_D(z) := \prod_{i\le N} D_{\mathbb{Z},\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}(z_i)$. The **leaf set** is $\mathcal{Z}_i := \left(|\cdot - \widetilde{t}_i|/\widetilde{\sigma}_i\right)^{-1}([0,\tau]) \subseteq \mathbb{Z}$. Let μ, ν be probability measures on $\mathbb{Z}$, $\mathcal{Y} \subseteq \mathbb{Z}$ a set and $a > 1$ an order. The **Rényi divergence on** $\mathcal{Y}$ is $R^{\mathcal{Y}}_a(\mu \,\|\, \nu) := \left(\sum_{z\in\mathcal{Y}} \mu(z)^a\, \nu(z)^{1-a}\right)^{1/(a-1)}$. With $\sup\emptyset := 0$, the **moment** of the base sampler is $\bar{\rho}_B := \max_{i\le N} \sup_{z_{<i}\in S_{<i}} R^{\mathcal{Z}_i\setminus C_i}_{2\alpha}(\widetilde{B}_i \,\|\, \widetilde{D}_i)$. The **fringe quantities** are $\bar{U} := \max_{i\le N} \sup_{z_{<i}\in S_{<i}} \sup_{z_i\in C_i} \widetilde{B}_i(z_i)/\widetilde{D}_i(z_i)$, the largest ratio on a fringe set, $\bar{p}_C := \max_{i\le N} \sup_{z_{<i}\in S_{<i}} \widetilde{B}_i(C_i)$, the largest mass of a fringe set, and $\kappa_C := \bar{U}^{\alpha}\, \bar{\rho}_B^{-\alpha_L/2}$. Let $\epsilon_{\text{hi}} \ge 0$ be a real with $\forall i \le N\ \forall z_{<i}\ \forall z_i \notin C_i:\ \widetilde{B}_i(z_i) \le (1+\epsilon_{\text{hi}})\, \widetilde{D}_i(z_i)$.

The normalizer ratio at a leaf (Definition A.29). Let $\bar{\delta}$ satisfy $(1+\bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$. The **normalizer deviation** of a standard deviation $s > 0$ and a center $c \in \mathbb{R}$ is $d(s,c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\, s) - 1$. For $|\delta| \le \bar{\delta}$, define $\theta_{\alpha_L}(\delta) := 1/(\alpha_L + (1-\alpha_L)(1+\delta)^2)$. For $i \le N$ and every $z_{<i} \in S'_{<i}$, the **mixed standard deviation** is $s''_i := \sigma_i(1+\delta_i)\,\theta_{\alpha_L}(\delta_i)^{1/2}$ and the **mixed center** is $m_i := t_i + \alpha_L \theta_{\alpha_L}(\delta_i)\,\Delta_i$. The **normalizer ratio** at the leaf is $\Phi_{\alpha_L,i} := (1 + d(s''_i, m_i))\left(1 + d(\widetilde{\sigma}_i, \widetilde{t}_i)\right)^{-\alpha_L} (1 + d(\sigma_i, t_i))^{\alpha_L - 1}$. Let $\bar{\phi} \ge \max_{i\le N} \sup_{z_{<i}\in S'_{<i}} |\ln \Phi_{\alpha_L,i}(z_{<i})|$ be the **bound** of its logarithm.

The divergence factor R (Definition A.30). Let $\bar{\theta}_{\alpha_L} \ge 0$ be a real with $\forall \delta > -1,\ |\delta| \le \bar{\delta}:\ \theta_{\alpha_L}(\delta) \le \bar{\theta}_{\alpha_L}$, and $\bar{W}_{\alpha_L} > 0$ a real with $\forall \delta > -1,\ |\delta| \le \bar{\delta}:\ \theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \le \bar{W}_{\alpha_L}$. The **factor of the base sampler** is $R_B := \bar{\rho}_B^{\alpha_L N/(2(\alpha-1))}$, the **factor of the standard deviations** is $R_\sigma := (e^{\bar{\phi}}\, \bar{W}_{\alpha_L})^{N/(2(\alpha-1))}$, and the **factor of the centers** is $R_t := \exp\left(\alpha_L\, \bar{\theta}_{\alpha_L}\, \bar{W}_{S'}/2\right)$. The **divergence factor** is $R := R_B R_\sigma R_t$.

Symbol	Definition	Where
$\mathcal{R}_m$; $\|f\|$	$\mathbb{R}[x]/(x^m+1)$; the coefficient norm	Definition A.1
$\rho_{s,c}$; $D_{A,s,c}$	The Gaussian function; the discrete Gaussian over A	Definition A.2
R_α; $\mathbb{E}_\mu$	The Rényi divergence; the expectation	Definition A.3
$\mathrm{Supp}(\mu)$	The support of μ	Definition A.3
B; $\Lambda(B)$; $\mathcal{G}$	The basis; its lattice; its Gram matrix	Definition A.12
Gram_m	The Gram matrices of degree m	Definition A.14
V_m; M_m	The two split operators	Definition A.15
split; merge	The split; the merge	Definition A.15
$\langle a, b\rangle$	The coefficient inner product	Definition A.15
$\mathrm{LDL}^\dagger$	The $LDL^\dagger$ step	Definition A.17
l_{10}; d_{00}, d_{11}	Its factor; its two diagonals	Definition A.17
$\mathcal{T}_m$; Sub	The trees of degree m; the subtrees	Definition A.18
I; d_i	The sample positions; the leaf diagonals	Definition A.19
$\mathrm{ffLDL}^\dagger$	The $\mathrm{ffLDL}^\dagger$ tree of a Gram matrix	Definition A.20
ffSampling	The sampler on a tree	Definition A.21
$Q_{T,t}$	Its output measure	Definition A.21
$\eta_\epsilon(\mathbb{Z}^n)$	The smoothing parameter of $\mathbb{Z}^n$	Fact A.22
$\|B\|_{\mathrm{GS}}$	The Gram–Schmidt norm of B	Fact A.22
P, Q	$\mathrm{ffSampling}^{\mathcal{F}}$; $\mathrm{ffSampling}^{\mathbb{R}}$	Definition A.25
α	Rényi order, $\alpha > 1$	Definition A.3
σ_i, t_i; $\widetilde{\sigma}_i, \widetilde{t}_i$	Leaf i over $\mathbb{R}$; computed	Definition A.25
$\widetilde{B}_i$, $\widetilde{D}_i$	SamplerZ at $(\widetilde{\sigma}_i, \widetilde{t}_i)$; $D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$	Theorem F.4
S; P_S, Q_S	$\{z : \forall i\ \|z_i - \widetilde{t}_i\| \le \tau\widetilde{\sigma}_i\}$; $P(\cdot \mid S)$, $Q(\cdot \mid S)$	Definition A.26
S'; $S'_{<i}$	A sub-event of S, S unless named; $\{z_{<i} : z \in S'\}$	Definition A.26
S^c; S'^c	$\mathbb{Z}^N \setminus S$, the tail; $\mathbb{Z}^N \setminus S'$	Definition A.26
$\mathbb{Z}_{>0}$; $\mathbb{Z}_{\ge 0}$	The positive integers; the nonnegative integers	Definition A.1
R	The divergence factor	Theorem F.4
A_{adv}	The adversary's event, $Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda}$	Definition 5.1
Δ_i	$\widetilde{t}_i - t_i$	Definition A.27
q, $\sigma_{\min}$, σ_0	12289; [L0: `sign_sampler.c:21-56`]; 1.8205	Appendix G.6
u, ζ	$(0, 2^{-64})$ for `fxp/`	Definitions A.4, I.1
h, n, N	$\log_2 n$; degree; $2n$	Section 3.2
ϵ	Normalizer deviation	Corollary E.21; Definition I.62
$\Phi_{\alpha_L,i}$, $\bar{\phi}$	$(1 + d(s_i'', m_i))(1 + d(\widetilde{\sigma}_i, \widetilde{t}_i))^{-\alpha_L}(1 + d(\sigma_i, t_i))^{\alpha_L - 1}$, $d(s,c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}s) - 1$; $\bar{\phi} \ge \sup\lvert\ln \Phi_{\alpha_L,i}\rvert$	Definition A.29
$\bar{\phi}_{\mathrm{u}}$	The uniform bound, one admissible $\bar{\phi}$	Definition A.40
$\bar{\delta}$	$\max_i\lvert\widetilde{\sigma}_i/\sigma_i - 1\rvert$	Definition A.27
$\bar{W}_{\alpha_L}, \bar{\theta}_{\alpha_L}$	Upper bounds over $\delta > -1$, $\lvert\delta\rvert \le \bar{\delta}$ of $s''/(s_1^{\alpha_L} s_2^{1-\alpha_L})$, of $\theta_{\alpha_L}(\delta)$	Definition A.30
$\bar{W}_{S'}$; $\bar{W}_S$	$\sup_{S'} \sum_i \Delta_i^2/\sigma_i^2$; $\bar{W}_{S'}$ at $S' = S$	Definition A.27
$\|\Delta\|$	$\|(\Delta_i)_i\|$ on S	Theorem G.59
$\mathcal{Z}_i$; $\bar{\rho}_B$	$\{z_i : \lvert z_i - \widetilde{t}_i\rvert \le \tau\widetilde{\sigma}_i\}$; $\sup R_{2\alpha}^{\mathcal{Z}_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)$	Definition A.28
ϵ_{hi}	$\epsilon_{\mathrm{hi}} \ge \sup_{z_i \notin C_i}(\widetilde{B}_i/\widetilde{D}_i - 1)$	Definition A.28
τ	Tail-cut rate of S	Lemma E.18
κ	$\lvert g_{01}\rvert^2/(g_{00}g_{11} - \lvert g_{01}\rvert^2)$	Lemma G.25
Ξ', Ξ	$\max_\nu\|\mathcal{L}_\nu\|$, $\max_\nu\|\mathcal{L}_\nu^{-1}\|$	Definition 4.6

Table 5: Symbols of the definitions and of Theorem 1.1.

4 The roadmap of the proof

This section describes the statements that set the four terms of $\ln R$ in Theorem 1.1. Section 4.1 describes the four terms of $\ln R$; Section 4.2 states the product bound on a leaf's Rényi divergence; Section 4.3 states probability preservation; Section 4.4 states the divergence bound with fringe

sets; Section 4.5 states the divergence of a Falcon-type signer.

How each statement is verified. Table 6 lists the definitions of this section, Table 7 how each lemma, proposition and theorem is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Def. 4.5					
Def. 4.6	✓				
Def. 4.12					L2: EI93, Section 1 at $B := \widetilde{\mathcal{L}}$, $\delta B := \mathcal{L} - \widetilde{\mathcal{L}}$, $D_L := I_N$ and $D_R := I_N + K$

Table 6: Section 4: its definitions.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma 4.1	✓				
Prop. 4.2	✓				
Thm. 4.3	✓				
Thm. 4.4	✓				
Lemma 4.7	✓				
Lemma 4.8	✓				
Lemma 4.9	✓				
Cor. 4.10	✓				
Thm. 4.11	✓				
Lemma 4.13	✓				
Lemma 4.14	✓				

Table 7: Section 4: how each lemma, proposition, corollary and theorem is verified.

4.1 The end result and its terms

Figure 4 describes the theorem's four terms on the tree.

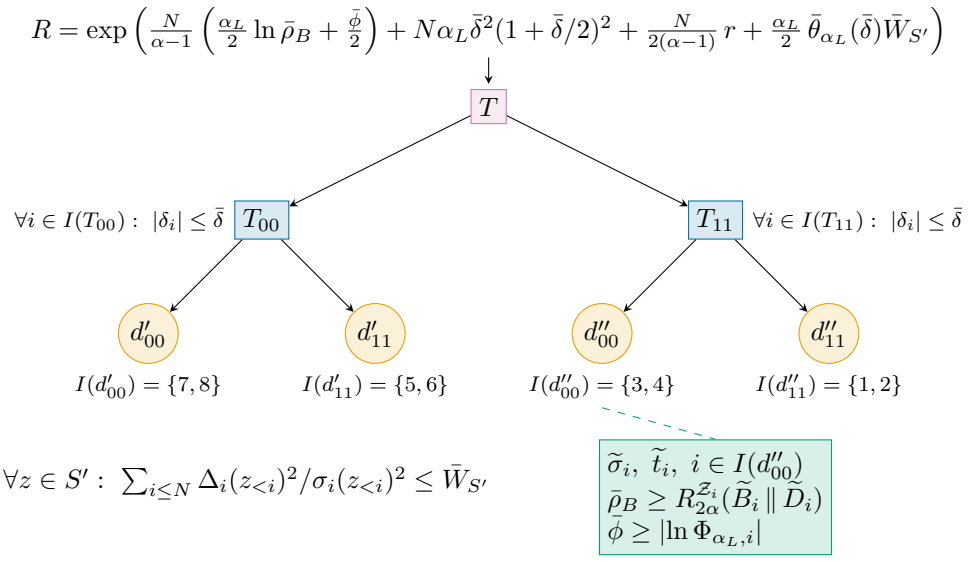


Figure 4: The terms of $\ln R$ on the tree of Figure 22 (Theorem 1.1; Definitions A.27, A.28 and A.29).

Theorem 1.1 (restated). The signer in $\mathcal{F}$ stays within the factor R of the signer over $\mathbb{R}$ on a sub-event of the tail-cut event, $\ln R$ the sum of four explicit terms. Define:

- $S := \{\, z \in \mathbb{Z}^N : \forall i \le N \ |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$, the tail-cut event.

Let:

- $S' \subseteq S$, an event.

Define:

- The sub-event
  - $S'^c := \mathbb{Z}^N \setminus S'$;
- The prefix sets
  - $S_{<i} := \{\, z_{<i} : z \in S \,\}$ for $i \le N$;
- The conditional probability measures
  - $P_{S'}(A) := P(A \cap S')/P(S')$ for $A \subseteq \mathbb{Z}^N$;
  - $Q_{S'}(A) := Q(A \cap S')/Q(S')$;
- The leaf measures
  - $\widetilde{B}_i(A) := P(z_i \in A \mid z_{<i})$ for $i \le N$, $z_{<i} \in S_{<i}$ and $A \subseteq \mathbb{Z}$, the base sampler's conditional probability measure at leaf i;
  - $\widetilde{D}_i := D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$, the discrete Gaussian at the computed parameters;
- The tail cut
  - $\mathcal{Z}_i := \{\, z_i \in \mathbb{Z} : |z_i - \widetilde{t}_i| \le \tau\, \widetilde{\sigma}_i \,\}$;
- The moments
  - $\bar{\rho}_B := \max_{i \le N} \ \sup_{z_{<i} \in S_{<i}} \Big(\sum_{z_i \in \mathcal{Z}_i} \widetilde{B}_i(z_i)^{2\alpha}\, \widetilde{D}_i(z_i)^{1-2\alpha} \Big)^{1/(2\alpha-1)}$;
- The terms
  - $\bar{x} := 2\bar{\delta} + \bar{\delta}^2$;
  - $r := \big(((\alpha_L - 1)\bar{x})^3/(1 - (\alpha_L - 1)\bar{x}) + (\alpha_L - 1)\bar{x}^3/(1 - \bar{x})\big)/6$;
  - $\bar{\theta}_{\alpha_L}(\bar{\delta}) := 1/(1 - (\alpha_L - 1)\bar{x})$;
  - $R := \exp\Big(\frac{N}{\alpha - 1} \Big(\frac{\alpha_L}{2} \ln \bar{\rho}_B + \frac{\bar{\phi}}{2} \Big) + N\alpha_L \bar{\delta}^2 (1 + \bar{\delta}/2)^2 + \frac{N}{2(\alpha-1)}\, r + \frac{\alpha_L}{2}\, \bar{\theta}_{\alpha_L}(\bar{\delta}) \bar{W}_{S'} \Big)$.

Assume:

(A1) $(1 + \bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$;
(A2) $\bar{x} < 1$;
(A3) $\forall i \le N \ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i > 0$;
(A4) $\bar{\rho}_B > 0$;
(A5) $P(S') > 0$;
(A6) $Q(S') > 0$.

Then

$$R_\alpha(P_{S'} \,\|\, Q_{S'}) \le R\,(1 - P(S'^c))^{-\alpha/(\alpha-1)}.$$

4.2 The divergence at one leaf

Figure 5 describes the measures at one leaf.

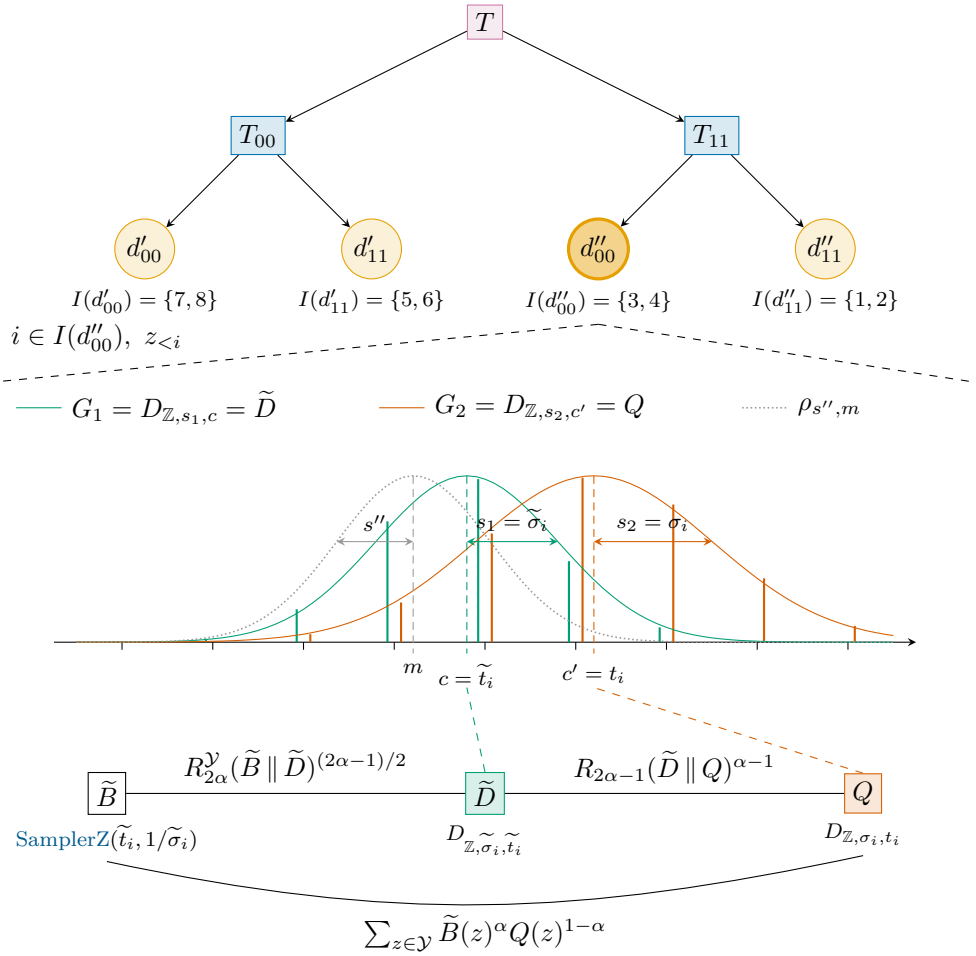


Figure 5: One leaf of the tree of Figure 22, with the two Gaussians of Lemma 4.1 and the three measures of Proposition 4.2: $\widetilde{B}$, the base sampler's measure in $\mathcal{F}$ at the computed leaf parameters; $\widetilde{D}$, the discrete Gaussian at those parameters; Q, the discrete Gaussian at the leaf parameters of ffSampling$^{\mathbb{R}}$.

Standing symbols. The standing symbols of Section 3.2 stand here. The other standing symbols are:

- $\alpha > 1$, the Rényi order;
- $s_1, s_2 > 0$, the standard deviations of a leaf, and $c, c' \in \mathbb{R}$, its centers (Lemma 4.1);
- $\delta > -1$, a relative perturbation, $\Delta \in \mathbb{R}$, a shift, and $\theta_\alpha(\delta) := 1/(\alpha + (1-\alpha)(1+\delta)^2)$ (Definition A.39);
- ε_j, the series of the normalizer deviation (Definition A.38).

Lemma 4.1 (The Rényi divergence of two leaf Gaussians in closed form [to table] [to proof])**.** *The Rényi divergence of two leaf Gaussians at the order α is a closed form in a merged standard deviation s'' and a merged center m. Define:*

- *$G_1 = D_{\mathbb{Z},s_1,c}$ and $G_2 = D_{\mathbb{Z},s_2,c'}$, the $D_{\mathbb{Z},s,c}$ of Definition A.2 at $s := s_1$ and at $(s, c) := (s_2, c')$;*
- *$A = \alpha/s_1^2$;*
- *$B = (1-\alpha)/s_2^2$;*
- *$m = (Ac + Bc')/(A + B)$ (Lemma E.1);*
- *$s'' = (A + B)^{-1/2}$.*

Assume:

(A1) $s_1^2 < s_2^2\,\alpha/(\alpha - 1)$.

Then

$$R_\alpha(G_1 \| G_2)^{\alpha-1} = \frac{\rho_{s'',m}(\mathbb{Z})\ \exp\left(\alpha(\alpha-1)(c-c')^2 s''^2/(2s_1^2 s_2^2)\right)}{\rho_{s_1,c}(\mathbb{Z})^\alpha\ \rho_{s_2,c'}(\mathbb{Z})^{1-\alpha}}.$$

Proposition 4.2 (The product bound on a leaf's Rényi divergence [to table] [to proof])**.** *The leaf's Rényi divergence on a set from the ideal measure, to the power $\alpha-1$, is at most a product of two leaf divergences. Let:*

- $\mathcal{Y} \subseteq \mathbb{Z}$;
- $i \le N$;
- $z_{<i} \in \mathbb{Z}^{i-1}$.

Define:

- $\widetilde{B} := B^{\mathcal{F}}_{\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}$ *and* $\widetilde{D} := D_{\mathbb{Z},\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}$ *at* $z_{<i}$ *(Definition A.28);*
- $R^{\mathcal{Y}}_a(\widetilde{B}\,\|\,\widetilde{D}) := \left(\sum_{x\in\mathcal{Y}} \widetilde{B}(x)^a\,\widetilde{D}(x)^{1-a}\right)^{1/(a-1)}$ *for* $a>1$ *(Definition A.28);*
- $Q = D_{\mathbb{Z},\sigma_i,t_i}$ *at* $z_{<i}$*, the ideal measure at the parameters over* $\mathbb{R}$ *(Definition A.25, item 2).*

Assume:

(A1) $\sum_{z\in\mathcal{Y}} \widetilde{B}^{2\alpha}\widetilde{D}^{1-2\alpha} < \infty$;

(A2) $\sum_{z\in\mathbb{Z}} \widetilde{D}^{2\alpha-1}Q^{2-2\alpha} < \infty$.

Then

$$\sum_{z\in\mathcal{Y}} \widetilde{B}(z)^\alpha Q(z)^{1-\alpha} \le R^{\mathcal{Y}}_{2\alpha}(\widetilde{B}\,\|\,\widetilde{D})^{(2\alpha-1)/2}\, R_{2\alpha-1}(\widetilde{D}\,\|\,Q)^{\alpha-1}.$$

4.3 Composition and probability preservation

Figure 6 describes the composition along the samples.

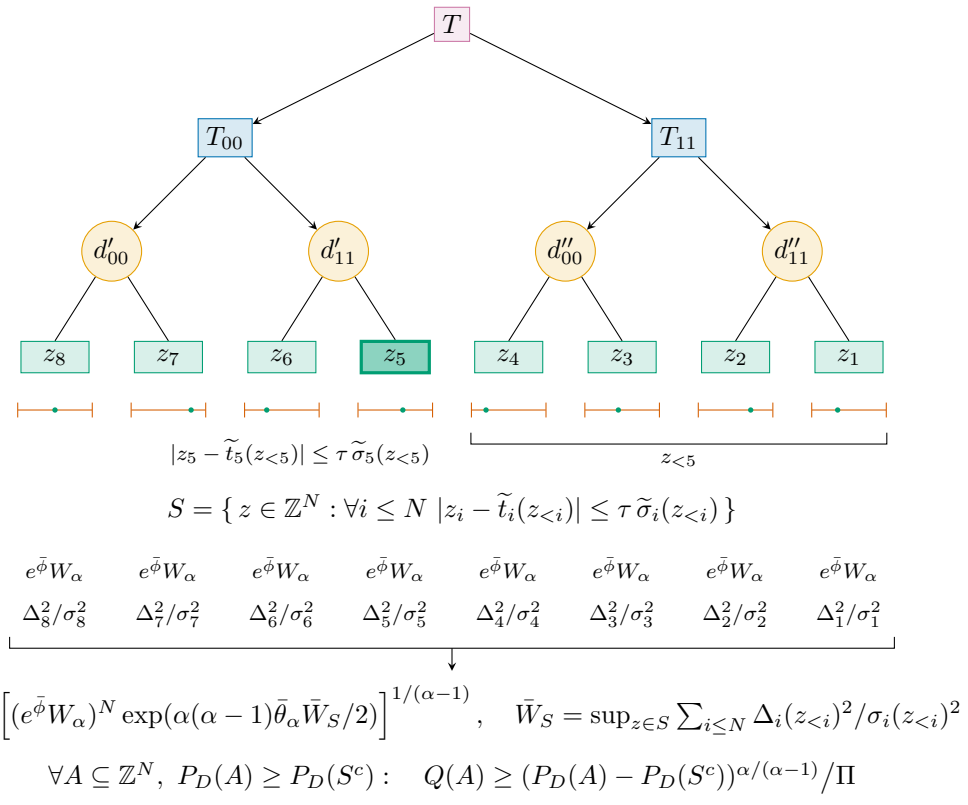


Figure 6: The composition along the samples on the tree of Figure 22 (Theorem 4.3; Definition A.26).

Theorem 4.3 (Probability preservation [to table] [to proof])**.** *On the tail-cut event, the divergence of the computed from the ideal measure is at most* Π *up to the event's masses, and every event keeps a mass under the ideal measure. Let:*

- $\bar{\delta}$, $\bar{\theta}_\alpha$, W_α, $\bar{\phi} \in \mathbb{R}$.

Define:

- *The probability measures*
  - Q, *the measure of* ffSampling$^{\mathbb{R}}$ *(Definition A.25);*
  - $P_D(z) := \prod_{i \le N} D_{\mathbb{Z},\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}(z_i)$ *for* $z \in \mathbb{Z}^N$ *(Definition A.28);*
- *The tail-cut event*
  - $S := \{\, z \in \mathbb{Z}^N : \forall i \le N \;\; |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$, *the tail-cut event (Definition A.26);*
  - $S_{<i} := \{\, z_{<i} : z \in S \,\}$ *and* $Q_S(A) := Q(A \cap S)/Q(S)$ *(Definition A.26);*
- *The conditional probability measures*
  - $(P_D)_S(A) := P_D(A \cap S)/P_D(S)$ *for* $A \subseteq \mathbb{Z}^N$;
- *The normalizer ratio*
  - Φ, *the normalizer ratio of Definition A.39;*
  - $\Phi_{\alpha,i} := \Phi(\sigma_i, \delta_i, t_i, \Delta_i)$;
- *The terms*
  - $\bar{W}_S := \sup_{z \in S} \sum_{i \le N} \Delta_i(z_{<i})^2/\sigma_i(z_{<i})^2$ *(Lemma E.17);*
  - $\Pi := \left[(e^{\bar{\phi}} W_\alpha)^N \exp(\alpha(\alpha-1)\bar{\theta}_\alpha \bar{W}_S/2)\right]^{1/(\alpha-1)}$.

Assume:

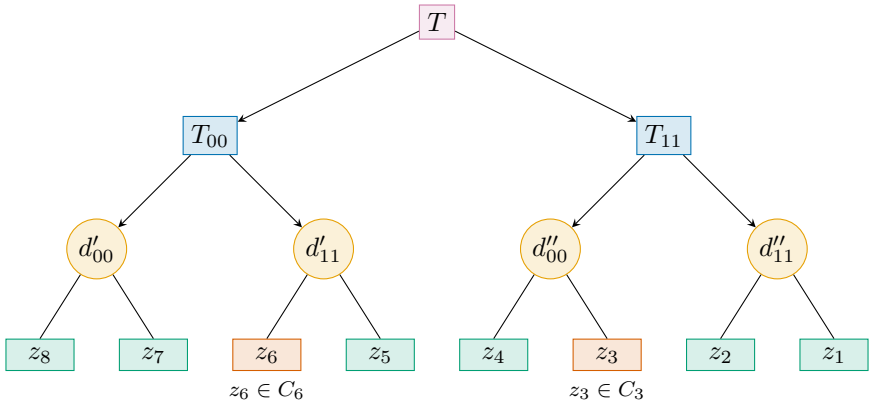
(A1) $P_D(S) > 0$;
(A2) $Q(S) > 0$;
(A3) $\bar{\delta} \ge \max_{i \le N} \sup_{z_{<i} \in S_{<i}} |\delta_i(z_{<i})|$;
(A4) $\bar{\delta} < (\alpha/(\alpha-1))^{1/2} - 1$;
(A5) $\bar{\theta}_\alpha \ge 0$;
(A6) $\forall \delta > -1,\; |\delta| \le \bar{\delta} :\; \theta_\alpha(\delta) \le \bar{\theta}_\alpha$;
(A7) $W_\alpha > 0$;
(A8) $\forall \delta > -1,\; |\delta| \le \bar{\delta} :\; \theta_\alpha(\delta)^{1/2}(1+\delta)^{1-\alpha} \le W_\alpha$;
(A9) $\bar{\phi} \ge \max_{i \le N} \sup_{z_{<i} \in S_{<i}} |\ln \Phi_{\alpha,i}(z_{<i})|$.

Then the conditioned measures' divergence and every event's ideal mass are bounded:

1. $R_\alpha((P_D)_S \,\|\, Q_S) \le Q(S)\, P_D(S)^{-\alpha/(\alpha-1)}\, \Pi$;
2. $\forall A \subseteq \mathbb{Z}^N,\; P_D(A) \ge P_D(S^c) :\quad Q(A) \ge (P_D(A) - P_D(S^c))^{\alpha/(\alpha-1)}/\Pi$.

4.4 The fringe extension

Figure 7 describes the fringe extension.



$$\mathcal{K}(z) = \{3, 6\}, \quad z \in S'_2, \quad S'_k = \{\, z \in S' : |\mathcal{K}(z)| = k \,\}$$

$$\forall i \in \mathcal{K}(z) : \ \widetilde{B}_i(C_i) \le \bar{p}_C, \quad \sup_{z_i \in C_i} \widetilde{B}_i(z_i)/\widetilde{D}_i(z_i) \le \bar{U}, \quad \kappa_C = \bar{U}^{\alpha}\, \bar{\rho}_B^{-\alpha_L/2}$$

$$R_\alpha(P_{S'_0} \,\|\, Q_{S'_0}) \le R\,(1 - P((S'_0)^c))^{-\alpha/(\alpha-1)}, \quad \forall k \le N : \ \textstyle\sum_{z \in S'_k} P(z)^{\alpha} Q(z)^{1-\alpha} \le \binom{N}{k} \kappa_C^k\, R^{\alpha-1}$$

Figure 7: The fringe sets on the tree of Figure 22 (Theorem 4.4; Definitions A.26 and A.28).

Theorem 4.4 (The divergence bound with fringe sets [to table] [to proof])**.** *Where the fringe sets are not empty, the signer in $\mathcal{F}$ stays within the factor R of the signer over $\mathbb{R}$ on the core class of a sub-event of the tail-cut event, and a fringe leaf costs κ_C in a class's Rényi divergence to the power $\alpha - 1$ and $\bar{p}_C$ in mass. Define:*

- $\mathcal{K}(z) := \{\, i \le N : z_i \in C_i(z_{<i}) \,\}$ *(Definition A.26);*
- $S'_k := \{\, z \in S' : |\mathcal{K}(z)| = k \,\}$ *for $k \le N$ (Definition A.26);*
- $R_\alpha^{S'_k}(P \,\|\, Q)$*, that of Definition A.28 at $\mathcal{Y} := S'_k$;*
- $P_{S'_0}(A) := P(A \cap S'_0)/P(S'_0)$ *(Definition A.26);*
- $Q_{S'_0}(A) := Q(A \cap S'_0)/Q(S'_0)$ *(Definition A.26);*
- $\bar{W}_{\alpha_L} > 0$ *with* $\forall \delta > -1,\ |\delta| \le \bar{\delta} :\ \theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \le \bar{W}_{\alpha_L}$ *(Definition A.30);*
- $\bar{\theta}_{\alpha_L} \ge 0$ *with* $\forall \delta > -1,\ |\delta| \le \bar{\delta} :\ \theta_{\alpha_L}(\delta) \le \bar{\theta}_{\alpha_L}$ *(Definition A.30).*

Assume:

(A1) $(1+\bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$*;*

(A2) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i > 0$*;*

(A3) $\bar{\rho}_B > 0$*.*

Then the core class keeps the factor R, and the classes and the fringe leaves' masses are bounded:

1. *Assume:*

   (A4) $P(S'_0) > 0$*;*

   (A5) $Q(S'_0) > 0$*.*

   Then $R_\alpha(P_{S'_0} \,\|\, Q_{S'_0}) \le R\,(1 - P((S'_0)^c))^{-\alpha/(\alpha-1)}$*;*

2. $\forall k \le N :\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k\, R^{\alpha-1}$*;*

3. $\forall I \subseteq \{1, \ldots, N\} :\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$*.*

4.5 The Falcon-type signer

Figure 8 describes a Falcon-type signer's deviations down the tree; Section 4.5.1 states the family; Section 4.5.2 the key constants; Section 4.5.3 the tree; Section 4.5.4 the centers; Section 4.5.5 the base sampler; Section 4.5.6 the terms of $\ln R$; Section 4.5.7 the tail of the leaf sum.

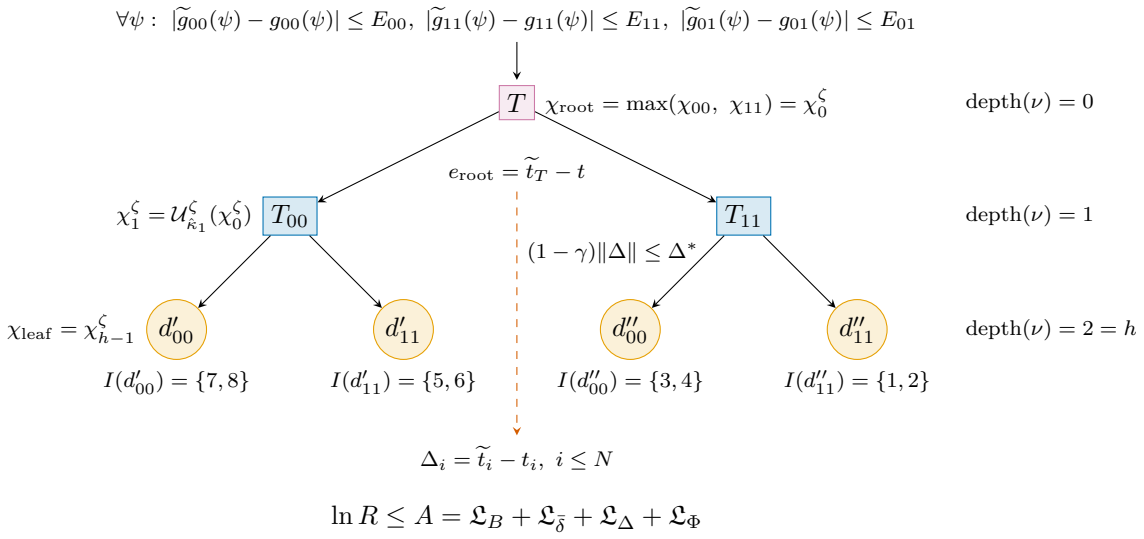


Figure 8: The deviations down the tree of Figure 23 (Theorem 4.11; Corollary G.36; Theorem G.59).

4.5.1 The family

Definition 4.5 (A Falcon-type signer [to table])**.** A Falcon-type signer is ffSampling$^{\mathcal{F}}$ executed in a realization, with a key generation's four checks and a base sampler. Let:

- $\mathcal{F}\subset\mathcal{A}$, a realization with its error bounds (u,ζ), $u\in[0,1)$, and rounding $\text{fl}\colon\mathcal{A}\to\mathcal{F}$ (Definition A.4);
- A key generation with the four checks of keychecks (Algorithm 12) at thresholds $(\gamma_{fg},\gamma_{\text{hyb}},\gamma_{FG},\gamma_{\text{root}})$ (keygen (Algorithm 11));
- A base sampler SamplerZ (Algorithm 8) with the acceptance BerExp (Algorithm 9).

Define:

- $n=2^h$, $\sigma_{\min}$ and σ_0, those of Table 5;
- The Falcon-type signer at (u,ζ), ffSampling$^{\mathcal{F}}$ (Algorithm 10) executed in $\mathcal{F}$;
- t, the center at line 17 of ffSampling$^{\mathcal{F}}$ (Algorithm 10);
- t_{frac}, the center at line 7 of ffSampling$^{\mathcal{F}}$.

The Falcon-type signer computes the Gram matrix $\mathcal{G}(\psi)$ of the key's basis (Gram (Algorithm 13)), the $LDL^\dagger$ tree computed when the recursion reaches a node (ffsamp (Algorithm 6)), the center t or t_{frac}, and the N integer samples of the base sampler at the leaves. Its instantiation is the fixed-point signer at $(0,2^{-64})$ (Appendix I).

4.5.2 The key constants

Definition 4.6 (The key constants [to table])**.** A key's constants are eight maxima over its tree, with four bounds on its diagonals; a signer's are their maxima over a sample of keys. Let:

- (f,g,F,G), a key of a Falcon-type signer;
- $m_0>0$, a floor of the root node's diagonal g_{00};
- $M_0\ge m_0$, a ceiling of the root node's diagonal g_{00};
- $d_{\text{lo}}>0$, a floor of the diagonals below the root node;
- $d_{\text{hi}}\ge d_{\text{lo}}$, a ceiling of the diagonals below the root node.

Define:

1. $\mathcal{G}$, the key's Gram matrix (Gram (Algorithm 13));
2. $T:=\text{ffLDL}^\dagger(\mathcal{G})$ (Definition A.20);
3. $\kappa_{\text{root}}:=\max_\psi|g_{01}|^2/q^2$ (Fact A.33, item 6);

4. $(g^{\nu}_{00}, g^{\nu}_{01}, g^{\nu}_{11})$, the entries of $\mathcal{G}_\nu(\psi)$, $\nu \in \mathrm{Sub}(T)$, ψ a root of ν's ring (Definition A.32);
5. $\kappa_k := \max_{\nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu)=k}\ \max_\psi |g^{\nu}_{01}|^2/(g^{\nu}_{00} g^{\nu}_{11} - |g^{\nu}_{01}|^2)$;
6. $\|x\|$, the coefficient norm;
7. $\|A\| := \max_{x \neq 0} \|xA\|/\|x\|$ for $A \in \{\mathcal{L}_{T'}, \mathcal{L}^{-1}_{T'}\}$, $T' \in \mathrm{Sub}(T)$, with $\mathcal{L}^{-1}_{T'}$ the inverse of $\mathcal{L}_{T'}$ (Lemma G.11 at $T := T'$; Fact A.44, item 5);
8. $\Xi'_k := \max_{\mathrm{depth}(\nu)=k} \|\mathcal{L}_\nu\|$;
9. $\Xi_k := \max_{\mathrm{depth}(\nu)=k} \|\mathcal{L}^{-1}_\nu\|$;
10. $\Xi'_{\mathrm{root}} := \|\mathcal{L}_T\|$;
11. $h := \log_2 n$;
12. $\Xi' := \max(\{1\} \cup \{\Xi'_k : 1 \le k \le h-1\})$, a maximum below the root;
13. $\Xi := \max(\{1\} \cup \{\Xi_k : 1 \le k \le h-1\})$, a maximum below the root;
14. $\ell := \max_\psi |l_{10}|$ over the nodes;
15. $\bar{g}_2 := \max_\psi |g_{01}|^2 g_{00}$;
16. $\bar{g}_0 := \max_\psi g_{00}$;
17. $\hat{K} := (\kappa_{\mathrm{root}},\ \kappa_k,\ \Xi',\ \Xi'_{\mathrm{root}},\ \Xi,\ \ell,\ \bar{g}_2,\ \bar{g}_0)$, the key constants, each a maximum over the key.

$\bar{g}_2$ and $\bar{g}_0$ are inputs of Z_E of Lemma G.40, item 2, a multiple of ζ, so a signer at $\zeta = 0$, or one whose root takes its second diagonal by the NTRU identity, reads the first six entries of $\hat{K}$.

```
def FTree.opBoundC {k : Nat} (T : FTree k) (Xi : Real) : Prop := forall x, T.coordNorm x <= Xi
    ^ 2 * pairSqC x

def FTree.invBoundC {k : Nat} (T : FTree k) (Xi : Real) : Prop := forall x, pairSqC x <= Xi ^ 2
    * T.coordNorm x

noncomputable def coordNorm {k : Nat} (T : FTree k) (x : SlotVec k x SlotVec k) : Real :=
  ((T.coords x).map (fun c => ||c|| ^ 2)).sum

noncomputable def pairSqC {k : Nat} (x : SlotVec k x SlotVec k) : Real := (2:Real)^-1 ^ k *
    pairSq x
```

Figure 9: The Lean declarations carrying Definition 4.6: `FTree.opBoundC`, `FTree.invBoundC`, `FTree.coordNorm`, `pairSqC` (`Centers.lean`, `Shift.lean`); with `FTree` of Figure 21; Lean's symbols in ASCII.

4.5.3 The tree

Lemma 4.7 states the leaf standard deviations; Lemma 4.8 the node factors.

Lemma 4.7 (Leaf standard deviations of a Falcon-type signer [to table] [to proof])**.** *At every leaf the computed standard deviation is within $\bar{\delta}$ of the one over $\mathbb{R}$. Let:*

- *The signer be a Falcon-type signer at (u, ζ) (Definition 4.5);*
- *$E_{00}, E_{11}, E_{01} \ge 0$;*
- *$\chi_{00}, \chi_{11} \ge 0$.*

Define:

- $\hat{K}$, *the signer's key constants, and* m_0, M_0, d_{lo} *and* d_{hi}, *the key's diagonal floors and ceilings (Definition 4.6);*
- $T := \mathrm{ffLDL}^{\dagger}(\mathcal{G})$ *and* $\mathcal{G}$, *those of Definition 4.6;*
- $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\} :\ d_j^{\nu}$, *that of Corollary G.36 at* $\mathcal{G}$*;*
- $e_{00} := E_{00}/m_0$*;*
- $\texttt{INV_SIGMA}[\log_2 n]$, *the stored inverse standard deviation of* ffsamp *(Algorithm 6) at the signer's degree* n.

Define:

Precondition 1. $\chi_{\mathrm{root}} := \max(\chi_{00},\ \chi_{11})$*:* χ_{00} *the bound* e_{00} *of Lemma G.40, item 1, or the signer's own bound;* χ_{11} *the bound of Lemma G.40, item 2 at* (u, ζ), E_{00}, E_{11}, E_{01} *when* $\widetilde{d}_{11}$ *is the LDL*† *step's, or the signer's own bound, from the NTRU identity (Fact A.33, item 2) or from its own corollary;*

Precondition 2. $\chi_{\mathrm{leaf}} := \chi_{h-1}^{\zeta}$, *the iterate* $\chi_k^{\zeta} = \mathcal{U}_{\hat{\kappa}_k}^{\zeta}(\chi_{k-1}^{\zeta})$ *from* $\chi_0^{\zeta} = \chi_{\mathrm{root}}$ *of Corollary G.36 at* (u, ζ), d_{lo}, d_{hi} *and* κ_k *of* $\hat{K}$, *every iterate in its admissible set* $\mathcal{A}$*;*

Precondition 3. $k_J := (|c_n| + \sqrt{d_{\mathrm{hi}}(1 + \chi_{\mathrm{leaf}})})(1 + u)^2 + (1 + u)\zeta + 1$ *and* $\chi_{\sigma}^{\zeta} := \chi_{\sigma} + k_J\zeta/s_{\min}$, *with* χ_{σ} *of Corollary G.41 at* χ_{leaf}, $s_{\min} := \sqrt{d_{\mathrm{lo}}}\, c_n$, $c_n := 1/s$ *with* s *of Definition A.25;*

Precondition 4. $\bar{\delta} := \chi_{\sigma}^{\zeta}/(1 - \chi_{\sigma}^{\zeta})$ *(Definition A.27);*

Assume:

(A1) $\forall \psi :\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi_{00}^{\pm}, 0\right) d_{00}(\psi)$ *at the root node;*

(A2) $\forall \psi :\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi_{11}^{\pm}, 0\right) d_{11}(\psi)$ *at the root node;*

(A3) $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi :\ d_j^{\nu}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$ *(Proposition D.9);*

(A4) $\forall k \in \{0, \ldots, h-1\} :\ \chi_k^{\zeta} \in \mathcal{A}$, *the admissible set of Corollary G.36;*

(A5) $\chi_{\sigma}^{\zeta} < 1$*;*

(A6) $\texttt{INV_SIGMA}[\log_2 n]\ \mathcal{I}\,(u^{\pm}, \zeta^{\pm})\ c_n$.

Then the leaf standard deviations are within $\bar{\delta}$ *at every prefix and on the tail-cut event:*

1. $\forall i \le N\ \forall z_{<i} :\ |\delta_i| \le \bar{\delta}$*;*
2. $\forall z \in S\ \forall i \le N :\ |\delta_i| \le \bar{\delta}$.

Lemma 4.8 (Node factors of a Falcon-type signer [to table] [to proof])**.** *At every node the computed factor* l_{10} *is within* E_l *of the one over* $\mathbb{R}$. *Let:*

- *The signer be a Falcon-type signer at* (u, ζ) *(Definition 4.5);*
- $E_{00}, E_{11}, E_{01} \ge 0$*;*
- $\chi_{00}, \chi_{11} \ge 0$.

Define:

- *The signer's words and parameters*
  - $n := 2^h$, *the signer's degree (Definition 4.5);*
  - $\Psi_n := \{\psi_k : k < n/2\}$, *that of Fact A.43 at* $m := n$*;*
- *The key constants*
  - $\hat{K}$, *the signer's key constants, and* m_0, M_0, d_{lo} *and* d_{hi}, *the key's diagonal floors and ceilings (Definition 4.6);*
  - ℓ *and* κ_{root}, *those of* $\hat{K}$ *(Definition 4.6);*
- *The tree*
  - $T := \mathrm{ffLDL}^{\dagger}(\mathcal{G})$ *and* $\mathcal{G}$, *those of Definition 4.6;*
  - $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\} :\ d_j^{\nu}$, *that of Corollary G.36 at* $\mathcal{G}$*;*
- *The error chain*
  - $e_{00} := E_{00}/m_0$*;*
  - $\chi_{\mathrm{root}} := \max(\chi_{00},\ \chi_{11})$*;*

  - $\forall k \in \{1,\dots,h-1\}:\ \vartheta_{k-1} := (1+\chi^{\zeta}_{k-1})/(1-\chi^{\zeta}_{k-1})$ *(Corollary G.36);*
  - $\forall k \in \{1,\dots,h-1\}:\ \hat{\kappa}_k := \vartheta_{k-1}\kappa_k + (\vartheta_{k-1}-1)/2$ *(Corollary G.36);*
  - $\chi^{\zeta}_k := \mathcal{U}^{\zeta}_{\hat{\kappa}_k}(\chi^{\zeta}_{k-1})$ *from* $\chi^{\zeta}_0 := \chi_{\mathrm{root}}$, $\mathcal{U}^{\zeta}_{\kappa}$ *that of Corollary G.36 at* (u,ζ), d_{lo}, d_{hi} *and* κ_k *of* $\hat{K}$*;*
  - $\chi_{\mathrm{leaf}} := \chi^{\zeta}_{h-1}$*;*
- *The node bounds*
  - $u_0 := (1+u)(1+\zeta/(2d_{\mathrm{lo}}(1-\chi_{\mathrm{leaf}})(1-u))) - 1$ *and* $\bar{\delta}_\mu := (1+u)^2 - 1$ *(Corollary G.43 at* $\chi := \chi_{\mathrm{leaf}}$*);*
  - $c_{\mathrm{sa}} := (1+u)^2(1+u+\sqrt{2}\,\zeta)-1$ *and* $k_{\mathrm{sa}} := (1+u)(1+u+\sqrt{2}\,\zeta)/2+\sqrt{2}$ *(Corollary G.43);*
  - $M_2 := d_{\mathrm{hi}}(1+\chi_{\mathrm{leaf}})(1+c_{\mathrm{sa}})/2 + k_{\mathrm{sa}}\zeta$ *and* $\bar{e}_0 := (1+\chi_{\mathrm{leaf}})(1+u_0)-1$ *(Corollary G.43 at* $\chi := \chi_{\mathrm{leaf}}$*);*
  - $\bar{a}_1 := c_{\mathrm{sa}} + \chi_{\mathrm{leaf}}(1+c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta/d_{\mathrm{lo}}$ *(Corollary G.43);*
  - $E_l^{\mathrm{child}} := \dfrac{\bar{\delta}_\mu + \bar{e}_0}{1-\bar{e}_0} + \bar{a}_1\,\dfrac{1+\bar{\delta}_\mu}{1-\bar{e}_0} + \sqrt{2}\,(M_2(1+u)+1)\,\zeta$ *(Corollary G.43);*
  - $E_l^{\mathrm{root}} := \ell\,\dfrac{\bar{\delta}_\mu + e_{00}}{1-e_{00}} + \dfrac{E_{01}}{m_0}\,\dfrac{1+\bar{\delta}_\mu}{1-e_{00}} + \sqrt{2}\,((\sqrt{\kappa_{\mathrm{root}}}\,q + E_{01})(1+u)+1)\,\zeta$ *(Corollary G.43).*

Define:

Precondition 1. $E_l := \max(E_l^{\mathrm{child}}, E_l^{\mathrm{root}})$ *of Corollary G.43 at* (u,ζ), $\chi := \chi_{\mathrm{leaf}}$, d_{lo}, d_{hi}, ℓ, m_0, e_{00}, E_{01} *and* κ_{root} *of* $\hat{K}$*, and* $\widetilde{\ell} := \ell + E_l$*;*

Assume:

(A1) $\forall \psi:\ |\widetilde{g}_{00}(\psi) - g_{00}(\psi)| \le E_{00}$*, for the computed Gram matrix entries against the Gram matrix over* $\mathbb{R}$ *of the images;*

(A2) $\forall \psi:\ |\widetilde{g}_{11}(\psi) - g_{11}(\psi)| \le E_{11}$*;*

(A3) $\forall \psi:\ |\widetilde{g}_{01}(\psi) - g_{01}(\psi)| \le E_{01}$*;*

(A4) $e_{00} < 1$*;*

(A5) $\forall \psi \in \Psi_n:\ g_{00}(\psi) \ge m_0$*;*

(A6) $\forall \psi \in \Psi_n:\ g_{00}(\psi) \le M_0$*;*

(A7) $\forall \psi:\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{00}, 0\right) d_{00}(\psi)$ *at the root node;*

(A8) $\forall \psi:\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{11}, 0\right) d_{11}(\psi)$ *at the root node;*

(A9) $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi:\ d^{\nu}_j(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$ *(Proposition D.9);*

(A10) $\forall k \in \{0,\dots,h-1\}:\ \chi^{\zeta}_k \in \mathcal{A}$*, the admissible set of Corollary G.36;*

(A11) $\bar{e}_0 < 1$*, with* $\bar{e}_0$ *that of Corollary G.43 at* (u,ζ), $\chi := \chi_{\mathrm{leaf}}$ *and* d_{lo}*.*

Then the computed factors satisfy:

1. $\max_\psi |\widetilde{l}_{10} - l_{10}| \le E_l$*;*
2. $\max_\psi |\widetilde{l}_{10}| \le \widetilde{\ell}$*.*

4.5.4 The centers

Lemma 4.9 (Center shift of a Falcon-type signer [to table] [to proof])**.** *The shift of the leaf centers is at most* D_S*, so the sum of the squared relative shifts is at most* W° *on the tail-cut event. Let:*

- *The signer be a Falcon-type signer at* (u,ζ) *(Definition 4.5);*
- $t \in \mathcal{R}_n \times \mathcal{R}_n$*, a center;*
- $\widetilde{t}_T$*, the value the signer computes for* t *in* $\mathcal{F}$*;*
- $e_{\mathrm{root}} \in \mathcal{R}_n \times \mathcal{R}_n$*;*
- $\bar{T} \ge 0$*;*
- $\bar{Z} \ge 0$*;*
- $\bar{\delta} \in [0,1)$ *with* $\forall z \in S\ \forall i \le N:\ |\delta_i| \le \bar{\delta}$*,* δ_i *of Definition A.27;*
- $E_l \in \mathbb{R}$ *with* $\max_\psi |\widetilde{l}_{10} - l_{10}| \le E_l$ *at every node of the key's tree;*
- $\widetilde{\ell} \in \mathbb{R}$ *with* $\max_\psi |\widetilde{l}_{10}| \le \widetilde{\ell}$ *at every node of the key's tree.*

Define:

- *The key constants*
  - $\hat{K}$, *the signer's key constants (Definition 4.6);*
  - ℓ, *that of* $\hat{K}$ *(Definition 4.6);*
- *The samples*
  - $z' := (z_0, z_1)$, *the sample* ffsamp *(Algorithm 6) returns at* t (ffSampling$^{\mathcal{F}}$ *(Algorithm 10), line 24);*
- *The leaf perturbations*
  - $\forall i \le N\ \forall z_{<i} :\ \Delta_i(z_{<i}) := \widetilde{t}_i(z_{<i}) - t_i(z_{<i})$ *(Definition A.27);*
  - $\Delta := (\Delta_i)_{i \le N}$;
  - $W(z) := \sum_{i \le N} \Delta_i(z_{<i})^2 / \sigma_i(z_{<i})^2$.

Define:

Precondition 1. $D_S := D^\circ/(1 - \gamma - \gamma_S)$ *with* D°, γ, γ_S *of Corollary G.62 at* (u, ζ) *and the key's own constants: at* $T := \text{ffLDL}^\dagger(\mathcal{G})$ *(Definition 4.6), the key's tree, its* Ξ'_{root}, Ξ'_k *and* Ξ *(Definition 4.6), its* ℓ *of* $\hat{K}$*, and the maxima* $\max_{\nu,\psi} |\widetilde{l}_{10}|$ *and* $\max_{\nu,\psi} |\widetilde{l}_{10} - l_{10}|$ *over* T*'s nodes (Theorem G.59); at* $\|e_{\text{root}}\|$, $\bar{T}$, $Z := \bar{Z}$, τ *and* $\sigma_{\max} := 1.17^2 \sigma_{\min}$;

Precondition 2. $W^\circ := D_S^2 / \sigma_{\min}^2$;

Assume:
(A1) $\|\widetilde{t}_T - t\| \le \|e_{\text{root}}\|$, *in the coefficient norm (Appendix G.5);*
(A2) $\|t\| \le \bar{T}$;
(A3) $\forall z \in S :\ \|z'\| \le \bar{Z}$;
(A4) $\gamma + \gamma_S < 1$;
(A5) $\sigma_{\min} > 0$;
(A6) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \sigma_i \ge \sigma_{\min}$.
Then the center shift and its relative square satisfy:

1. $\|\Delta\| \le D_S$;
2. $\forall z \in S :\ W(z) \le W^\circ$;
3. $\bar{W}_S \le W^\circ$ *(Definition A.27).*

4.5.5 The base sampler

Corollary 4.10 (Base sampler of a Falcon-type signer [to table] [to proof])**.** *At leaf standard deviations within* $\bar{\delta}$*, the base sampler's row bounds bound its divergence, its factor* κ_C*, the tail of the tail-cut event and the masses of the fringe leaves. Let:*

- $\mathcal{F} \subset \mathcal{A}$ *be the realization of a Falcon-type signer at* (u, ζ)*, the signer (Definition 4.5);*
- $e_{+,k} \ge 0$, $k \le 18$, *and* $e_{\text{ccs}} \in [0, 1)$*, the row bounds of the signer's base sampler;*
- $\epsilon \in [0, 1)$;
- $\bar{\delta} \ge 0$ *with* $\forall z \in S\ \forall i \le N :\ |\delta_i| \le \bar{\delta}$, δ_i *of Definition A.27.*

Define:

- *The signer's parameters*
  - $\sigma_0 := 1.8205$ *(Lemma G.64);*
  - $\sigma_{\max} := 1.17^2 \sigma_{\min}$;
- *The prefix sets*
  - $\forall i \le N :\ S_{<i} := \{\, z_{<i} : z \in S \,\}$ *(Definition A.26);*
- *The leaf measures*
  - $\widetilde{B}_i$, $\widetilde{D}_i$ *and* $\bar{\rho}_B$*, those of Definition A.28 at the signer's base sampler;*
  - $\epsilon_{\text{hi}} \ge 0$ *with* $\forall i \le N\ \forall z_{<i}\ \forall z_i \notin C_i :\ \widetilde{B}_i(z_i) \le (1 + \epsilon_{\text{hi}})\, \widetilde{D}_i(z_i)$ *(Definition A.28).*

Define:

Precondition 1. $M_{2\alpha} := (\sqrt{\bar{M}_{\mathrm{tab}}} + \sqrt{\bar{M}_{\mathrm{ar}}})^2$, *with* $\bar{M}_{\mathrm{tab}}$ *and* $\bar{M}_{\mathrm{ar}}$ *of Lemma G.73 at order* 2α, $\sigma_{\min}$, $\sigma_{\max}(1+\bar{\delta})$, τ, *the row bounds* $e_{+,k}$ *and* e_{ccs}, *and* ϖ, $\bar{e}_{\mathrm{norm}}$ *that lemma's at these;*

Precondition 2. $p_\tau := \frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}\,\epsilon_{\mathcal{Z}} + p_C^D$, *with* $\epsilon_{\mathcal{Z}} \in [0,1]$ *bounding* $\epsilon_{\mathcal{Z}_i \setminus C_i}$ *at every* $i \le N$ *and* $z_{<i} \in S_{<i}$ *(Corollary G.75),* $\widetilde{D}_i(\mathcal{Z}_i^c)$ *bounded by Lemma E.18, item 2, at* $(\widetilde{\sigma}_i, \widetilde{t}_i)$ *under assumptions A2, A4 and A7, and* $p_C^D \ge 0$ *bounding* $\widetilde{D}_i(C_i)$ *at every* $i \le N$ *and* $z_{<i} \in S_{<i}$, $p_C^D = 0$ *when every* C_i *is empty;*

Precondition 3. $p'_\tau := (1+\epsilon_{\mathrm{hi}})\,\frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$ *(Corollary E.21), at which* κ_C *is read (Corollary G.75, item 3:* $\kappa_C \le \bar{U}^\alpha (1 - p'_\tau - \bar{p}_C)^{-\alpha}$*).*

Assume:

(A1) $e_{+,k}$ *and* e_{ccs} *bound the base sampler's relative perturbation of the acceptance on the row* k *at every leaf, and the relative rounding of its computed* $\widetilde{ccs}$*, as Lemma G.73 assumes, on* $\mathcal{Y} := \mathcal{Z}_i \setminus C_i$ *(Definitions A.26, A.28);*

(A2) $\sigma_{\min} > 0$*;*

(A3) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \sigma_i \in [\sigma_{\min}, \sigma_{\max}]$*, with* σ_i *that of Definition A.25;*

(A4) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i \ge \sigma_{\min}$*;*

(A5) $\sigma_{\max}(1+\bar{\delta}) \le \sigma_0$*;*

(A6) $\bar{\delta} < 1$*;*

(A7) $\forall i \le N\ \forall z_{<i}\ \forall c \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$*;*

(A8) $\varpi < 1$*, with* ϖ *that of precondition 1;*

(A9) $\bar{e}_{\mathrm{norm}} < 1$*, with* $\bar{e}_{\mathrm{norm}}$ *that of precondition 1;*

(A10) $p'_\tau + \bar{p}_C < 1$.

Then the leaves' divergence and the factor κ_C *are bounded, the computed leaves' mass off* $\mathcal{Z}_i$ *is at most* p'_τ*, the tail and the fringe masses are bounded, each leaf's divergence on* $\mathcal{Z}_i \setminus C_i$ *is bounded, and* p_τ *is nonnegative:*

1. $\ln \bar{\rho}_B \le \alpha\, M_{2\alpha} + 2\, p_\tau$*;*
2. $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$*;*
3. $\kappa_C \le \bar{U}^\alpha\, (1 - p'_\tau - \bar{p}_C)^{-\alpha}$*;*
4. $\forall i \le N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$*;*
5. $P(S^c) \le N\, p'_\tau$*;*
6. $\forall S' \subseteq S\ \forall I \subseteq \{1, \ldots, N\} :\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$*;*
7. $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}$*;*
8. $p_\tau \ge 0$.

4.5.6 The terms of $\ln R$

Theorem 4.11 (Divergence of a Falcon-type signer [to table] [to proof])**.** *A Falcon-type signer's* $\ln R$ *is at most the sum* A *of its terms, and at* $S' = S$ *its divergence conditioned on the core class* S_0 *is at most* R *times the conditioning factor. Let:*

- *The signer be a Falcon-type signer at* (u, ζ) *(Definition 4.5);*
- $\bar{\delta}_{S'} \in [0, 1)$*;*
- $W^\circ_{S'} \ge 0$.

Define:

- *The signer's parameters*
  - $\sigma_{\max} := 1.17^2 \sigma_{\min}$ *(Lemma 4.9, precondition 1);*

- *The prefix sets*
  - $\forall i \le N:\ S_{<i} := \{\, z_{<i} : z \in S \,\}$ *and* $\forall i \le N:\ S'_{<i} := \{\, z_{<i} : z \in S' \,\}$ *(Definition A.26);*
- *The leaf measures*
  - $\widetilde{B}_i$, $\widetilde{D}_i$ *and* $\bar{\rho}_B$, *those of Definition A.28 at the signer's base sampler;*
- *The fringe classes*
  - $\mathcal{K}(z) := \{\, i \le N : z_i \in C_i(z_{<i}) \,\}$ *(Definition A.26);*
  - $\forall k \le N:\ S'_k := \{\, z \in S' : |\mathcal{K}(z)| = k \,\}$ *(Definition A.26);*
  - $R_\alpha^{S'_k}(P \,\|\, Q)$, *that of Definition A.28 at* $\mathcal{Y} := S'_k$;
  - $S_0 := \{\, z \in S : |\mathcal{K}(z)| = 0 \,\}$ *(Definition A.26);*
- *The conditional probability measures*
  - $P_{S_0}(A) := P(A \cap S_0)/P(S_0)$ *and* $Q_{S_0}(A) := Q(A \cap S_0)/Q(S_0)$ *(Definition A.26 at* $S := S_0$*).*

Let:

- $M_{2\alpha}, p_\tau \in \mathbb{R}$ *with* $p_\tau \ge 0$ *and* $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}$;
- $p'_\tau \in \mathbb{R}$ *with* $\forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$ *and* $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$.

Define:

Precondition 1. $\mathfrak{L}_B$, $\mathfrak{L}_{\bar{\delta}}$, $\mathfrak{L}_\Delta$, $\mathfrak{L}_\Phi$ *and* $A := \mathfrak{L}_B + \mathfrak{L}_{\bar{\delta}} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$, *the four terms of* $\ln R$ *and their sum, written under "where" below at* $\bar{\delta}_{S'}$, $W^\circ_{S'}$ *and* $\bar{\phi} := \bar{\phi}_{\mathrm{u}}$: *the terms those of Definition A.30 and Corollary G.75,* $\bar{\phi}_{\mathrm{u}}$ *that of Definition A.40.*

Assume:

(A1) $\sigma_{\min} > 0$;
(A2) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ \sigma_i \in [\sigma_{\min}, \sigma_{\max}]$, *with* σ_i *and* $\widetilde{\sigma}_i$ *those of Definition A.25,* $S_{<i}$ *that of Definition A.26 and* $\sigma_{\max}$ *that of Lemma 4.9, precondition 1;*
(A3) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ \widetilde{\sigma}_i \ge \sigma_{\min}$;
(A4) $(1 + \bar{\delta}_{S'})^2 < \alpha_L/(\alpha_L - 1)$;
(A5) $p'_\tau + \bar{p}_C < 1$;
(A6) $\varepsilon_0^\circ < 1$, *with* ε_0° *that of Definition A.40 at* $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \bar{\delta}_{S'}, \bar{\Delta})$;
(A7) $\forall z \in S'\ \forall i \le N:\ |\delta_i(z_{<i})| \le \bar{\delta}_{S'}$;
(A8) $\forall z \in S':\ \sum_{i \le N} \Delta_i(z_{<i})^2/\sigma_i^2 \le W^\circ_{S'}$.

Then the divergence is at most its terms, the fringe classes are bounded, and at $S' = S$ *the conditional divergence on* S_0 *is at most* R *times the conditioning factor:*

1. $\ln R \le A$ *(*R *of Definition A.30 at* S'*);*
2. $\forall k \le N:\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k\, R^{\alpha-1}$;
3. *Let* $S' := S$. *Then* $R_\alpha(P_{S_0} \,\|\, Q_{S_0}) \le R\,(1 - P(S_0^c))^{-\alpha/(\alpha-1)}$, *with* R *of Definition A.30 at* S.

where

$$\mathfrak{L}_B = N \frac{\alpha_L\,(\alpha\, M_{2\alpha} + 2\, p_\tau)}{2(\alpha - 1)}, \qquad \mathfrak{L}_{\bar{\delta}} = \frac{N \ln \bar{W}_{\alpha_L}}{2(\alpha - 1)},$$

$$\mathfrak{L}_\Delta = \frac{\alpha_L\, \bar{\theta}_{\alpha_L}\, W^\circ_{S'}}{2}, \qquad \mathfrak{L}_\Phi = \frac{N \bar{\phi}}{2(\alpha - 1)}, \qquad \bar{\Delta} = \sigma_{\max}(W^\circ_{S'})^{1/2},$$

with $\bar{W}_{\alpha_L}$, $\bar{\theta}_{\alpha_L}$ *of Definition A.30 at* $\bar{\delta}_{S'}$ *and* $\bar{\phi}$ *of Definition A.40 at* $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \bar{\delta}_{S'}, \bar{\Delta})$.

The fixed-point signer has no fringe terms. The fixed-point signer's rejection at the saturated exponent removes the fringe terms of the theorem (Lemma G.80).

4.5.7 The tail of the leaf sum

Structure. Definition 4.12 states the three quantities of a key at a center; Lemma 4.13 the linear form of the leaf center shift; Lemma 4.14 the leaf sum's tail.

The shift's structure. K is the multiplicative perturbation of the tree map, $\mathcal{L} = \widetilde{\mathcal{L}}(I_N + K)$: the class $B + \delta B = D_L B D_R$ of [EI93, Section 1] at $D_L = I_N$ and $D_R = I_N + K$. The exact tree's leaf centers are $\widetilde{c} - (z - \widetilde{c})K$, so the shift from them to the code's centers $\widetilde{c} + r$ is $\Delta = r + (z - \widetilde{c})K$: the rounding remainder r plus the offsets from the computed tree's centers pushed through the tree's mismatch K. The offsets split as $z - \widetilde{c} = e + r$, the random offsets e and the rounding remainder r, and the shift becomes $eK + r(I_N + K)$.

The three quantities. $\bar{\delta}_K$ is the largest relative deviation of a computed leaf standard deviation from the exact one. It sets the factor $(1 + D)^2$ of W^{tail}. μ_{key} is the relative perturbation of the tree map over every direction as the sampler weighs them: $\mu_{\text{key}} = \|\widetilde{\Sigma} K \widetilde{\Sigma}^{-1}\|_{\text{F}}^2$ at $\widetilde{\Sigma} := \text{diag}(\widetilde{\sigma}_i)_{i \le N}$, the expected normalized squared shift of the centers by offsets of variances $\widetilde{\sigma}_j^2$. The relative perturbation bounds of a matrix's eigenvalues take the worst direction instead. μ_{key} sets the term $2M \ln(1/\eta')$. $\bar{B}_K$ is the largest leaf sum of the remainder's image $r(I_N + K)$ on the tail-cut event. It sets the term $B^{1/2}$.

Definition 4.12 (The three quantities of a key at a center [to table])**.** The three quantities are read on the exact tree and the computed tree of one key at one center. Define:

- $q := 12289$ (Definition A.13).

Let:

- $\mathcal{F} \subset \mathcal{A}$ be the realization of a Falcon-type signer at (u, ζ) (Definition 4.5);
- (f, g, F, G) be a key of degree n of the signer (Definition 4.6);
- $\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ be a hashed message (Definition A.25);
- $t_{\text{c}} \in \{t, t_{\text{frac}}\}$ be a center, t and t_{frac} those of Definition 4.5 at the key and $\mathsf{h}(\mathsf{m})$;
- $\tau_K > 1$;
- $z \in \mathbb{Z}^{2n}$.

Define:

- The parameters
  - $N := 2n$ (Definition A.25);
- The tree
  - T, that of Definition 4.6 at the key;
  - $\widetilde{T} \in \mathcal{T}_n$, the tree with the leaf diagonals of T whose node at each call of ffsamp (Algorithm 6) in $\mathcal{F}$ at the key and t_{c} holds the $\widetilde{l}_{10}$ of LDL† (Algorithm 5), line 12, at that call;
- The matrices
  - $\mathcal{L} := \mathcal{L}_T$, the matrix of the tree map (Definition G.6 at $T' := T$);
  - $\widetilde{\mathcal{L}} := \mathcal{L}_{\widetilde{T}}$, the matrix of the tree map (Definition G.6);
  - $\widetilde{\mathcal{L}}^{-1}$, the inverse of $\widetilde{\mathcal{L}}$ (Lemma G.11 at $\widetilde{T}$; Fact A.44, item 5);
  - I_N, the identity matrix of size N;
  - $K := \widetilde{\mathcal{L}}^{-1}\mathcal{L} - I_N$, the multiplicative perturbation of the tree map [L2: EI93, Section 1 at $B := \widetilde{\mathcal{L}}$, $\delta B := \mathcal{L} - \widetilde{\mathcal{L}}$, $D_L := I_N$ and $D_R := I_N + K$];
- The centers and the samples
  - $(\sigma_i, t_i)(z_{<i})$ and $(\widetilde{\sigma}_i, \widetilde{t}_i)(z_{<i})$, $i \le N$, those of Definition A.25 at the key, $\mathsf{h}(\mathsf{m})$ and the center t_{c};
  - $t_{\text{leaf}} := (t_i(z_{<i}))_{i \le N}$;
  - $\widetilde{t}_{\text{leaf}} := (\widetilde{t}_i(z_{<i}))_{i \le N}$;
  - $\widetilde{c} := (\widetilde{c}_i)_{i \le N}$, the leaf centers of ffSampling$(t_{\text{c}}, \widetilde{T})$ with the sample z, the c_i of Definition G.9 at $(t, T) := (t_{\text{c}}, \widetilde{T})$;
- The leaf perturbations
  - $\Delta := \widetilde{t}_{\text{leaf}} - t_{\text{leaf}}$;
  - $e := z - \widetilde{t}_{\text{leaf}}$;
  - $r := \widetilde{t}_{\text{leaf}} - \widetilde{c}$;

  - $\delta_i(z_{<i})$, $i \le N$, by $\widetilde{\sigma}_i =: \sigma_i(1+\delta_i)$ at every $z_{<i}$ (Definition A.27 at the key, $\mathsf{h}(\mathsf{m})$ and t_c);
- The tail-cut event
  - $S_{\tau_K} := \{\, z \in \mathbb{Z}^N : \forall i \le N \ |z_i - \widetilde{t}_i(z_{<i})| \le \tau_K\, \widetilde{\sigma}_i(z_{<i}) \,\}$ (Definition A.26 at $\tau := \tau_K$).

We define:

1. $\bar{\delta}_K := \max_{i\le N} \sup_{z_{<i}} |\delta_i(z_{<i})|$;
2. $\mu_{\text{key}} := \sum_{i\le N} \sum_{j<i} K_{ji}^2 \widetilde{\sigma}_j^2 / \widetilde{\sigma}_i^2$;
3. $\bar{B}_K := \sup_{z\in S_{\tau_K}} \sum_{i\le N} (r(I_N+K))_i^2 / \widetilde{\sigma}_i^2$.

Lemma 4.13 (Linear form of the leaf center shift [to table] [to proof])**.** *The leaf center shift at either center is the leaf offsets times a matrix the key and the center fix, plus the remainder times $I_N + K$. Let:*

- *$\mathcal{F} \subset \mathcal{A}$ be the realization of a Falcon-type signer at (u, ζ) (Definition 4.5);*
- *(f, g, F, G) be a key of degree n of the signer (Definition 4.6);*
- *$t_c \in \{t, t_{\text{frac}}\}$ be a center, t and t_{frac} those of Definition 4.5 at the key and $\mathsf{h}(\mathsf{m})$;*
- *$z \in \mathbb{Z}^{2n}$.*

Define:

- *$\mathcal{G}$ and T, those of Definition 4.6 at the key;*
- *$\widetilde{T}$, $\mathcal{L}$, $\widetilde{\mathcal{L}}$, $\widetilde{\mathcal{L}}^{-1}$, I_N, K, σ_i, $\widetilde{\sigma}_i$, t_{leaf}, $\widetilde{t}_{\text{leaf}}$, $\widetilde{c}$, Δ, e and r, those of Definition 4.12 at $\mathcal{F}$, the key, $\mathsf{h}(\mathsf{m})$, t_c and z.*

Assume:

(A1) $\sigma_{\min} > 0$.

Then the shift is e times K plus the remainder times $I_N + K$, K is strictly lower triangular in the sampling order, and the leaf standard deviations do not depend on the sample:

1. $\Delta = eK + r(I_N + K)$;
2. $\forall i, j \le N,\ j \ge i :\ K_{ji} = 0$;
3. $\forall i \le N\ \forall z' \in \mathbb{Z}^N :\ (\sigma_i, \widetilde{\sigma}_i)(z'_{<i}) = (\sigma_i, \widetilde{\sigma}_i)(z_{<i})$.

Lemma 4.14 (The leaf sum's tail [to table] [to proof])**.** *At a key whose three quantities lie within D, M and B, the leaf sum of one signature at either center exceeds W^{tail} on the tail-cut event with probability at most η_1. Let:*

- *$\mathcal{F} \subset \mathcal{A}$ be the realization of a Falcon-type signer at (u, ζ) (Definition 4.5);*
- *(f, g, F, G) be a key of degree n of the signer (Definition 4.6);*
- *$t_c \in \{t, t_{\text{frac}}\}$ be a center, t and t_{frac} those of Definition 4.5 at the key and $\mathsf{h}(\mathsf{m})$;*
- *$D \in [0, 1)$;*
- *$M \ge 0$;*
- *$B \ge 0$;*
- *$\eta_1 \in (0, 1)$;*
- *$\epsilon \in [0, 1)$.*

Define:

- *The leaf perturbations*
  - *N, σ_i, $\widetilde{\sigma}_i$, $\widetilde{t}_i$, I_N, K, Δ, e, r, δ_i, $\bar{\delta}_K$, μ_{key} and $\bar{B}_K$, those of Definition 4.12 at $\mathcal{F}$, the key, $\mathsf{h}(\mathsf{m})$, t_c and $\tau_K := \tau$;*
  - *$W(z) := \sum_{i\le N} \Delta_i^2 / \sigma_i^2$ for $z \in \mathbb{Z}^N$;*
- *The probability measures*
  - *$P(A) := \Pr[z \in A]$, z the output of $\text{ffSampling}^{\mathcal{F}}$ (Definition A.25 at the key, $\mathsf{h}(\mathsf{m})$ and t_c);*
  - *$\epsilon_{\text{hi}} \ge 0$ with $\forall i \le N\ \forall z_{<i}\ \forall z_i \notin C_i :\ \widetilde{B}_i(z_i) \le (1+\epsilon_{\text{hi}})\, \widetilde{D}_i(z_i)$ (Definition A.28);*
- *The tail-cut event*

  - $S := \{\, z \in \mathbb{Z}^N : \forall i \le N \ |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$ *(Definition A.26);*
- *The terms*
  - $\kappa := (1+\epsilon)/(1-\epsilon)$;
  - $\eta' := \eta_1/(2N(1+\epsilon_{\mathrm{hi}})^N \kappa^N)$;
  - $W^{\mathrm{tail}} := (1+D)^2 \left((2M\ln(1/\eta'))^{1/2} + B^{1/2}\right)^2$.

Assume:
(A1) $\bar{\delta}_K \le D$;
(A2) $\mu_{\mathrm{key}} \le M$;
(A3) $\bar{B}_K \le B$;
(A4) $\forall i \le N\ \forall z_{<i}\ \forall c \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$;
(A5) $\forall i \le N\ \forall z_{<i} :\ C_i(z_{<i}) = \emptyset$;
(A6) $\sigma_{\min} > 0$;
(A7) $\forall i \le N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$.
Then

$$P(S \cap \{z \in \mathbb{Z}^N : W(z) > W^{\mathrm{tail}}\}) \le \eta_1.$$

5 Instantiations

Structure. This section states the fixed-point signer's bit security. Section 5.1 states the bit security over Q_s signatures; Section 5.2 the checked key; Section 5.3 the bounds on ffSampling$^{\mathcal{F}}$; Section 5.4 the changes; Section 5.5 the losses; Section 5.6 describes the comparison with the fixed-point analysis of [BFLP26].

How each statement is verified. Table 8 lists this section's definitions, and Table 9 how each lemma and proposition is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Def. 5.1					L1: FGdG$^+$26, Thm. 1
Def. 5.2	✓				
Def. 5.3	✓				
Def. 5.5					
Def. 5.6					

Table 8: Section 5: its definitions.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma 5.4	✓				
Lemma 5.7	✓			**I.91**	
Prop. 5.8	✓				
Prop. 5.9	✓			**I.21**, **I.22**	
Cor. 5.10	✓			**I.21**, **I.22**	
Thm. 5.11	✓				
Thm. 5.12	✓			**I.21**, **I.22**, **I.91**	

Table 9: Section 5: how each lemma, proposition, corollary and theorem is verified.

5.1 The bit security over Q_s signatures

Structure. Definition 5.1 states the adversary's event; Definition 5.2 the fringe leaves' term; Definition 5.3 the loss; Theorem 1.2 the bit security over Q_s signatures.

Definition 5.1 (The adversary's event A_{adv} [to table])**.** Let Q_s be the **number of signatures** and λ the ideal signer's bit security. An **adversary's event** is an event of the Q_s signatures whose

probability under the ideal signer is at most $2^{-\lambda}$. The ideal signer's security at λ bits against an attack that reads the signatures says that the attack's success is such an event [L1: FGdG+26, Thm. 1]; Theorem 1.2 bounds the event's probability under the signer in $\mathcal{F}$ and uses nothing else about the attack. Let:

- $\lambda \in \mathbb{R}$;
- $Q_s \in \mathbb{Z}_{>0}$.

Define:

- $Q^{\otimes Q_s}$, the probability measure of Q_s independent signatures on $(\mathbb{Z}^N)^{Q_s}$ (Fact A.45, item 1).

Let:

- $A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s}$, an event with $Q^{\otimes Q_s}(A_{\text{adv}}) \leq 2^{-\lambda}$.

Definition 5.2 (The fringe leaves' term Π_C [to table])**.** Over Q_s signatures there are $Q_s N$ leaves, and m counts those whose sample is saturated. $\Pi_C(y)$ bounds the probability of the adversary's event on the Q_s-tuples with at least one fringe leaf: one term per $m \leq M_C$ for the tuples with exactly m, the last term for the tuples with more than M_C. Let:

- $Q_s \in \mathbb{Z}_{>0}$;
- $M_C \in \mathbb{Z}_{\geq 0}$;
- $y \geq 0$.

Define:

- $\Pi_C(y) := \sum_{m=1}^{M_C} \min\left(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha}\, y,\ \binom{Q_s N}{m} \bar{p}_C^{\,m} \right) + \binom{Q_s N}{M_C+1} \bar{p}_C^{\,M_C+1}$.

```
noncomputable def satTerm (K MC : Nat) (alpha kappa p y : Real) : Real :=
  (Sum i in Finset.range MC,
      min (((K.choose (i + 1) : Nat) : Real) ^ (1 / alpha) * kappa ^ (((i + 1 : Nat) : Real) /
          alpha) * y)
        (((K.choose (i + 1) : Nat) : Real) * p ^ (i + 1)))
    + ((K.choose (MC + 1) : Nat) : Real) * p ^ (MC + 1)
```

Figure 10: The Lean declarations carrying Definition 5.2: `satTerm` (`Cap.lean`); Lean's symbols in ASCII.

Definition 5.3 (The loss [to table])**.** Over Q_s signatures the signer keeps a **bit security** $\lambda_{\mathcal{F}}$ where the ideal keeps λ. The loss is not a constant. It carries a term λ/α, where α is the Rényi order. The tail and the fringe leaves' masses put a ceiling on $\lambda_{\mathcal{F}}$ that no λ raises. Let:

- $\lambda \in \mathbb{R}$;
- $Q_s \in \mathbb{Z}_{>0}$;
- $A \in \mathbb{R}$;
- $M_C \in \mathbb{Z}_{\geq 0}$;
- $S' \subseteq S$ be an event (Definition A.26);
- $A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s}$ be an event with $Q^{\otimes Q_s}(A_{\text{adv}}) \leq 2^{-\lambda}$ (Definition 5.1).

Define:

- The tail-cut event
  - $S := \{\, z \in \mathbb{Z}^N : \forall i \leq N\ |z_i - \widetilde{t}_i(z_{<i})| \leq \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$ (Definition A.26);
- The fringe classes
  - $\mathcal{K}(z) := \{\, i \leq N : z_i \in C_i(z_{<i}) \,\}$ (Definition A.26);
  - $S'_k := \{\, z \in S' : |\mathcal{K}(z)| = k \,\}$ for $k \leq N$ (Definition A.26);
- The terms
  - $\beta := (Q_s / \ln 2)\, A$;
  - $y := (2^{-\lambda} e^{Q_s A})^{(\alpha-1)/\alpha}$;
  - $\Pi_C(y)$, that of Definition 5.2 at (Q_s, M_C);
- The bit security

  - $\lambda_{\mathcal{F}}$, the bit security of the signer against A_{adv}, by

$$2^{-\lambda_{\mathcal{F}}} = Q_s\, P(S'^c) + y + \Pi_C(y);$$

- The loss
  - $\lambda - \lambda_{\mathcal{F}}$, the loss at Q_s signatures.

The bit security is the bound of Theorem 1.2 over Q_s signatures. The **probability-preservation bound** y bounds the probability of the adversary's event on the Q_s-tuples of signatures with no fringe leaf. $\Pi_C(y)$ bounds it on the tuples with at least one.

```
noncomputable def levelMass (Qs N MC : Nat) (alpha kappa p y c : Real) : Real :=
  c + y + satTerm (Qs * N) MC alpha kappa p y

theorem loss_log2 {alpha lam lamF beta x c Qs A : Real} (halpha : 1 < alpha) (hc : 0 <= c)
    (hbeta : beta = Qs / Real.log 2 * A)
    (hx : x = lam * (1 - 1 / alpha) - (alpha - 1) / alpha * beta)
    (hlev : (2:Real) ^ (-lamF) = c + ((2:Real) ^ (-lam) * Real.exp (Qs * A)) ^ ((alpha - 1) /
        alpha)) :
    lam - lamF = lam / alpha + (alpha - 1) / alpha * beta + Real.logb 2 (1 + c * 2 ^ x) := by
```

Figure 11: The Lean declarations carrying Definition 5.3: `levelMass`, `loss_log2` (`Cap.lean`, `Main.lean`); with `satTerm` of Figure 10; Lean's symbols in ASCII.

Lemma 5.4 (Fringe bounds over Q_s signatures [to table] [to proof])**.** *The bounds of one signature on its fringe classes and on its fringe leaves' masses hold, compounded, on the tuples of Q_s independent signatures. Let:*

- $Q_s \in \mathbb{Z}_{>0}$;
- $R > 0$;
- $S' \subseteq S$ *be a sub-event (Definition A.26);*
- κ_C *and* $\bar{p}_C$ *be the fringe quantities (Definition A.28).*

Define:

- $\mathcal{K}(z)$ *and* S'_k*, those of Definition A.26;*
- $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$*, the probability measures of Q_s independent signatures on $(\mathbb{Z}^N)^{Q_s}$ (Fact A.45, item 1);*
- $\mathcal{E} := \{\, w \in (\mathbb{Z}^N)^{Q_s} : \forall j \le Q_s\ w_j \in S' \,\}$;
- $\forall m \le Q_s N:\ E_m := \{\, w \in \mathcal{E} : \sum_{j \le Q_s} |\mathcal{K}(w_j)| = m \,\}$;
- $R_\alpha^{S'_k}(P \,\|\, Q)$ *and* $R_\alpha^{E_m}(P^{\otimes Q_s} \,\|\, Q^{\otimes Q_s})$*, those of Definition A.28 at $\mathcal{Y} := S'_k$ and at $\mathcal{Y} := E_m$.*

Assume:

(A1) $\forall k \le N:\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k\, R^{\alpha-1}$;

(A2) $\forall I \subseteq \{1, \ldots, N\}:\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$.

Then

1. $\forall m \le Q_s N:\ R_\alpha^{E_m}(P^{\otimes Q_s} \,\|\, Q^{\otimes Q_s})^{\alpha-1} \le \binom{Q_s N}{m} \kappa_C^m R^{(\alpha-1)Q_s}$;
2. $\forall I \subseteq \{1, \ldots, Q_s\} \times \{1, \ldots, N\}:\ P^{\otimes Q_s}(\{w \in \mathcal{E} : \forall (j,i) \in I\ (w_j)_i \in C_i\}) \le \bar{p}_C^{|I|}$;
3. $\forall m \le Q_s N:\ P^{\otimes Q_s}(E_m) \le \binom{Q_s N}{m} \bar{p}_C^m$.

Theorem 1.2 (restated). Over Q_s independent signatures, the Rényi divergences on the fringe classes S'_k of a sub-event S' of the tail-cut event, to the power $\alpha - 1$, and the masses of its fringe leaves bound the computed signer's probability of the adversary's event by $2^{-\lambda_{\mathcal{F}}}$. Let:

- $\lambda \in \mathbb{R}$;
- $Q_s \in \mathbb{Z}_{>0}$;
- $A \ge 0$;

- $M_C \in \mathbb{Z}_{\geq 0}$;
- $R > 0$.

Define:

- $y := (2^{-\lambda} e^{Q_s A})^{(\alpha-1)/\alpha}$ (Definition 5.3);
- S'_k, that of Definition A.26;
- $R_\alpha^{S'_k}(P \,\|\, Q)$, that of Definition A.28 at $\mathcal{Y} := S'_k$;
- $\lambda_{\mathcal{F}}$, that of Definition 5.3 at (λ, Q_s, A, M_C);
- $P^{\otimes Q_s}$ and $Q^{\otimes Q_s}$, the probability measures of Q_s independent signatures on $(\mathbb{Z}^N)^{Q_s}$ (Fact A.45, item 1).

Let:

- $A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s}$, an adversary's event (Definition 5.1) at (λ, Q_s).

Assume:

(A1) $\ln R \leq A$;

(A2) $\forall k \leq N : \; R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \leq \binom{N}{k} \kappa_C^k \, R^{\alpha-1}$;

(A3) $\forall I \subseteq \{1, \ldots, N\} : \; P(\{z \in S' : \forall i \in I \; z_i \in C_i(z_{<i})\}) \leq \bar{p}_C^{|I|}$.

Then

$$P^{\otimes Q_s}(A_{\text{adv}}) \leq 2^{-\lambda_{\mathcal{F}}}.$$

5.2 The checked key

Definition 5.5 states the checked key; Definition 5.6 a key passing the tail checks at a center; Lemma 5.7 the three quantities' bounds; Proposition 5.8 the tree's bounds at a checked key. The tail checks are this work's addition to the four checks of [L2: BFLP26, Alg. 2], a key-dependent computation of the key generation on every key.

Definition 5.5 (A checked key [to table])**.** A checked key is a key of degree 512 or 1024 within the key generation's coefficient bounds that passes the four checks of keychecks (Algorithm 12), as keygen calls it, line 8 [L0: `fxp/kgen_fx.c:60-94`]. Define:

- The stored words
  - $(\gamma_{fg}, \gamma_{\text{hyb}}, \gamma_{FG}, \gamma_{\text{root}}) := \begin{cases} (275, 4.75, 4500, 27) & n = 512 \\ (280, 5.75, 6800, 34) & n = 1024 \end{cases}$ (keygen (Algorithm 11), Require) [L0: `fxp/kgen_fx.c:97-111`];
  - $B_{fg} := \begin{cases} 31 & n = 512 \\ 15 & n = 1024 \end{cases}$ [L0: `kgen_gauss.c:14-16`];
- The parameters
  - $q := 12289$ (Definition A.13);
  - $\Psi_n := \{\psi_k : k < n/2\}$ (Fact A.43 at $m := n$);
- The components
  - $\forall z \in \mathbb{C} : \; z_r := \operatorname{Re} z, \; z_i := \operatorname{Im} z$;
- The images
  - $\forall p \in \{f, g, F, G\} : \; \hat{p} := \text{FFT}(p)$ (keychecks (Algorithm 12), line 2);
  - $\forall p \in \{f, g, F, G\} : \; \widetilde{\hat{p}} := \widetilde{\text{FFT}}(p)$ (keychecks, line 1) [L0: `fxp/kgen_fx.c:71-78`];
- The Gram matrix entries
  - $(g_{00}, g_{01}, g_{11}) := \text{Gram}\begin{pmatrix} \hat{g} & -\hat{f} \\ \hat{G} & -\hat{F} \end{pmatrix}$ (keychecks, line 4);
  - $(\tilde{g}_{00}, \tilde{g}_{01}, \tilde{g}_{11}) := \text{Gram}\begin{pmatrix} \widetilde{\hat{g}} & \widetilde{\hat{f}} \\ \widetilde{\hat{G}} & \widetilde{\hat{F}} \end{pmatrix}$ (keychecks, line 3) [L0: `fxp/kgen_fx.c:81`];
- The key's quantities
  - $sq_{fg} := \max_{\psi \in \Psi_n} \max(|\hat{f}(\psi)|^2, |\hat{g}(\psi)|^2)$;
  - $sq_{\text{hyb}} := \max_{\psi \in \Psi_n} \max(g_{00}(\psi)/q, q/g_{00}(\psi))$;
  - $sq_{FG} := \max_{\psi \in \Psi_n} \max(|\hat{F}(\psi)|^2, |\hat{G}(\psi)|^2)$;

  - $sq_{\text{root}} := \max_{\psi\in\Psi_n} |g_{01}(\psi)|^2/g_{00}(\psi)^2$;
- The computed values
  - $\widetilde{sq}_{fg} := \max_{\psi\in\Psi_n} \max(\text{fl}(\widetilde{f}_r(\psi)^2)+\text{fl}(\widetilde{f}_i(\psi)^2), \text{fl}(\widetilde{g}_r(\psi)^2)+\text{fl}(\widetilde{g}_i(\psi)^2))$ (keychecks, line 5) [L0: `fxp/kgen_fx.c:37`] [L0: `fxp/kgen_fx.c:79`];
  - $\widetilde{sq}_{\text{hyb}} := \max(\text{fl}(\max_{\psi\in\Psi_n} \widetilde{g}_{00}(\psi)/q), \text{fl}(q/\min_{\psi\in\Psi_n} \widetilde{g}_{00}(\psi)))$ (keychecks, lines 6 to 8) [L0: `fxp/kgen_fx.c:88`] [L0: `fxp/kgen_fx.c:89`] [L0: `fxp/kgen_fx.c:93`];
  - $\widetilde{sq}_{FG} := \max_{\psi\in\Psi_n} \max(\text{fl}(\widetilde{F}_r(\psi)^2) + \text{fl}(\widetilde{F}_i(\psi)^2), \text{fl}(\widetilde{G}_r(\psi)^2) + \text{fl}(\widetilde{G}_i(\psi)^2))$ (keychecks, line 9) [L0: `fxp/kgen_fx.c:80`];
  - $\widetilde{sq}_{\text{root}} := \max_{\psi\in\Psi_n} \text{fl}((\text{fl}(\widetilde{g}_{01,r}(\psi)^2) + \text{fl}(\widetilde{g}_{01,i}(\psi)^2))/\text{fl}(\widetilde{g}_{00}(\psi)^2))$ (keychecks, lines 10 and 11) [L0: `fxp/kgen_fx.c:90`] [L0: `fxp/kgen_fx.c:91`].

The key is a checked key when:

1. $n \in \{512, 1024\}$;
2. $\forall a < n:\ f_{[a]}, g_{[a]} \in [-B_{fg}, B_{fg}]$ [L0: `fxp/sign_fxcore.c:128-141`];
3. $\forall a < n:\ F_{[a]}, G_{[a]} \in [-127, 127]$ [L0: `kgen_ntru.c:1887-1895`];
4. $\widetilde{sq}_{fg} \le \text{fl}(\gamma_{fg}^2)$;
5. $\widetilde{sq}_{\text{hyb}} \le \text{fl}(\gamma_{\text{hyb}}^2)$;
6. $\widetilde{sq}_{FG} \le \text{fl}(\gamma_{FG}^2)$;
7. $\widetilde{sq}_{\text{root}} \le \text{fl}(\gamma_{\text{root}}^2)$.

Definition 5.6 (A key passing the tail checks at c [to table])**.** keygen calls tailcheck (Algorithm 15) at c, line 9 [L0: `fxp/kgen_fx.c:205`]. The three upper bounds $\delta^{\uparrow}$, $\mu^{\uparrow}$ and $B^{\uparrow}$ are the code's upper bounds of $\bar{\delta}_K$, μ_{key} and $\bar{B}_K$ (Definition 4.12), every rounding upward. **Hypothesis I.91** assumes each lies at or above its quantity, and Lemma 5.7 then puts the three quantities within the thresholds. The rule of Appendix I.2 sets the thresholds. Define:

- $q := 12289$ (Definition A.13).

Let:

- (f, g, F, G) be a checked key (Definition 5.5) of degree n;
- $c \in \{t, t_{\text{frac}}\}$ be a center (Definition A.25);
- $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$ be a hashed message (Definition A.25).

Define:

- The arithmetic
  - $\upsilon := 2^{-160}$, $\forall x \in \mathbb{R}:\ \lceil x \rceil_\upsilon := \upsilon\lceil x/\upsilon \rceil$ (Definition I.13);
  - `fxi_sub`, `fxi_mag`, `fxc_mag`, those of Definition I.13;
- The parameters
  - $N := 2n$ (Definition A.25);
- The stored words
  - $M_n := \begin{cases} \lceil 2^{-112.85} \rceil_\upsilon & (n,c) = (512, t) \\ \lceil 2^{-110.64} \rceil_\upsilon & (n,c) = (1024, t) \\ \lceil 2^{-112.85} \rceil_\upsilon & (n,c) = (512, t_{\text{frac}}) \\ \lceil 2^{-110.64} \rceil_\upsilon & (n,c) = (1024, t_{\text{frac}}) \end{cases}$ (Definition I.14) [L0: `fxp/fxp_consts.h:2102`] [L0: `fxp/fxp_consts.h:2106`] [L0: `fxp/fxp_consts.h:2110`] [L0: `fxp/fxp_consts.h:2114`];
  - $D_n := \begin{cases} \lceil 2^{-57.95} \rceil_\upsilon & (n,c) = (512, t) \\ \lceil 2^{-57.38} \rceil_\upsilon & (n,c) = (1024, t) \\ \lceil 2^{-57.95} \rceil_\upsilon & (n,c) = (512, t_{\text{frac}}) \\ \lceil 2^{-57.38} \rceil_\upsilon & (n,c) = (1024, t_{\text{frac}}) \end{cases}$ (Definition I.14) [L0: `fxp/fxp_consts.h:2103`] [L0: `fxp/fxp_consts.h:2107`] [L0: `fxp/fxp_consts.h:2111`] [L0: `fxp/fxp_consts.h:2115`];

  - $B_n := \begin{cases} \lceil 2^{-73.16} \rceil_v & (n,c) = (512,t) \\ \lceil 2^{-71.19} \rceil_v & (n,c) = (1024,t) \\ \lceil 2^{-82.22} \rceil_v & (n,c) = (512,t_{\text{frac}}) \\ \lceil 2^{-79.17} \rceil_v & (n,c) = (1024,t_{\text{frac}}) \end{cases}$ (Definition I.14) [L0: `fxp/fxp_consts.h:2104`] [L0: `fxp/fxp_consts.h:2108`] [L0: `fxp/fxp_consts.h:2112`] [L0: `fxp/fxp_consts.h:2116`];
  - τ_K, that of Definition I.14 at the key and c;
- The leaf perturbations
  - I_N, $\widetilde{\sigma}_i$, $\widetilde{t}_i$, K, r and δ_i, those of Definition 4.12 at $\mathcal{F}_{\text{fx}}$, the key, $\mathsf{h}(\mathsf{m})$ and $t_{\text{c}} := c$;
- The tail-cut event
  - $S_{\tau_K} := \{\, z \in \mathbb{Z}^N : \forall i \le N \ |z_i - \widetilde{t}_i(z_{<i})| \le \tau_K \, \widetilde{\sigma}_i(z_{<i}) \,\}$ (Definition A.26 at $\tau := \tau_K$);
- The key's quantities
  - $\bar{\delta}_K := \max_{i \le N} \sup_{z_{<i}} |\delta_i(z_{<i})|$ (Definition 4.12, item 1);
  - $\mu_{\text{key}} := \sum_{i \le N} \sum_{j<i} K_{ji}^2 \widetilde{\sigma}_j^2 / \widetilde{\sigma}_i^2$ (Definition 4.12, item 2);
  - $\bar{B}_K := \sup_{z \in S_{\tau_K}} \sum_{i \le N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2$ (Definition 4.12, item 3);
- The leaf words
  - $\mathtt{isigma}_i$, Σ_i, $i \le N$, those of Definition I.17 at the key and c;
- The matrices
  - $K^{\mathcal{J}}$, that of Definition I.18 at the key and c;
- The bounds
  - x_i, $\mathtt{b_rem}_i$, $i \le N$, those of Definition I.19 at the key and c;
  - $\delta^{\uparrow} := \max_{i \le N} \mathtt{fxi_mag}(\mathtt{fxi_sub}(x_i, [1,1]))$ (Definition I.19, item 1; tailcheck (Algorithm 15), line 15) [L0: `fxp/kgen_fx.c:1735-1739`];
  - $\mu^{\uparrow} := \sum_{i \le N} \left\lceil \lceil \mathtt{isigma}_i^2 \rceil_v \sum_{j \le N} \lceil \lceil \mathtt{fxc_mag}(K_{ij}^{\mathcal{J}})^2 \rceil_v \lceil (\max \Sigma_j)^2 \rceil_v \rceil_v \right\rceil_v$ (Definition I.19, item 2; tailbounds (Algorithm 16), line 29) [L0: `fxp/kgen_fx.c:1773`];
  - $B^{\uparrow} := \sum_{i \le N} \lceil \lceil \mathtt{isigma}_i^2 \rceil_v \lceil \mathtt{b_rem}_i^2 \rceil_v \rceil_v$ (Definition I.19, item 2; tailbounds (Algorithm 16), line 31) [L0: `fxp/kgen_fx.c:1776-1777`].

The key passes the tail checks at c when:

1. $\delta^{\uparrow} \le D_n$;
2. $\mu^{\uparrow} \le M_n$;
3. $B^{\uparrow} \le B_n$.

Lemma 5.7 (Under **Hypothesis I.91**, the three quantities' bounds [to table] [to proof])**.** *The items bound the three quantities of a key passing the tail checks at a center by the center's thresholds.* ***Under Hypothesis I.91****, let:*

- $c \in \{t, t_{\text{frac}}\}$ *be a center (Definition A.25);*
- (f, g, F, G) *be a checked key of degree* n *(Definition 5.5) passing the tail checks at* c *(Definition 5.6);*
- $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$ *be a hashed message (Definition A.25).*

Define:

- M_n, D_n, B_n *and* τ_K, *those of Definition I.14 at* n *and* c;
- N, S_{τ_K}, I_N, $\widetilde{\sigma}_i$, K, r, δ_i *and* μ_{key}, *those of Definition 4.12 at* $\mathcal{F}_{\text{fx}}$, *the key,* $\mathsf{h}(\mathsf{m})$, $t_{\text{c}} := c$ *and* τ_K.

Then

1. $\mu_{\text{key}} \le M_n$;
2. $\forall i \le N \ \forall z_{<i} : \ |\delta_i(z_{<i})| \le D_n$;
3. $\forall z \in S_{\tau_K} : \ \sum_{i \le N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2 \le B_n$.

Proposition 5.8 (The tree's bounds at a checked key [to table] [to proof])**.** *A key that passes the four rounded checks has every diagonal of its tree, κ_k and κ_{root} of the LDL subtractions $d_{11} = g_{11} - |g_{01}|^2/g_{00}$ at its nodes, the off-diagonal factors and the norms of the tree maps below the root within bounds computed from the thresholds and the FFT's bound. Let:*

- *(f, g, F, G) be a checked key (Definition 5.5) of degree n;*
- *h with $n = 2^h$, as FFT (Algorithm 14) takes them (Precondition).*

Define:

- *The Gram deltas*
  - *$c_{\mathrm{merge}} := \sqrt{2} \cdot 2^{-64}$ (Lemma G.18 at $(u, \zeta) = (0, 2^{-64})$);*
  - *$R_{h-1} := (1 + c_{\mathrm{merge}})^{h-1} - 1$;*
  - *E_{00} and E_{01}, those of Definition A.36, items 5 and 7;*
  - *γ'_{FG}, that of Definition A.37;*
- *The key bounds*
  - *γ_{hyb}, that of Definition A.35;*
  - *$\check{\gamma}_{\mathrm{hyb}} := (\gamma_{\mathrm{hyb}}^2 + 2^{-65})^{1/2}$ and $\check{\gamma}_{\mathrm{root}}$, its root threshold (Definition A.35);*
  - *$m_0 := q/\check{\gamma}_{\mathrm{hyb}}^2 - E_{00}$, $M_0 := q\check{\gamma}_{\mathrm{hyb}}^2 + E_{00}$ and $\bar{g}_{11} := 2\gamma'^2_{FG}$ (Definition A.37);*
  - *$d_{\mathrm{lo}} := \min(m_0, q^2/M_0)$, $d_{\mathrm{hi}} := \max(M_0, q^2/m_0)$ and $\bar{\varsigma} := d_{\mathrm{hi}}/d_{\mathrm{lo}}$ (Definition A.37);*
- *The Gram matrix entries*
  - *g_{00}, g_{01}, g_{11}, the exact Gram matrix entries, keychecks (Algorithm 12), line 4;*
  - *$\mathcal{G} := \begin{pmatrix} g_{00} & g_{01} \\ \mathrm{conj}\, g_{01} & g_{11} \end{pmatrix}$;*
  - *$\widetilde{g}_{00}$ and $\widetilde{g}_{01}$, the values keychecks computes in $\mathcal{F}_{\mathrm{fx}}$, lines 1 to 11 [LO: fxp/kgen_fx.c:81];*
- *The tree*
  - *$T :=$ ffLDL$^\dagger(\mathcal{G})$ (Definition A.20);*
  - *d_{00}^{ν} and d_{11}^{ν}, those of Proposition G.38 at $\mathcal{G}$ and at $\nu \in \mathrm{Sub}(T)$;*
  - *l_{10}, that of LDL† (Algorithm 5), line 13, at the root node of T;*
- *The key constants*
  - *κ_k, that of Definition 4.6 at the key;*
  - *$\kappa_{\mathrm{root}} := \max_\psi |g_{01}|^2/q^2$ (Definition 4.6);*
  - *Ξ', Ξ and ℓ, those of Definition 4.6 at the key.*

Measured `verify/reports/fx/terms.py`:

- *$R_{h-1} < 1$ at both degrees;*
- *$E_{00} < q/\check{\gamma}_{\mathrm{hyb}}^2$ at both degrees.*

Then the diagonals, κ_k and κ_{root}, the factors and the tree maps' norms satisfy:

1. *$\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi :\ d_j^{\nu}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$;*
2. *$\forall k \in \{1, \ldots, h-1\} :\ \kappa_k \le (\bar{\varsigma} - 1)^2/(4\bar{\varsigma})$;*
3. *$\kappa_{\mathrm{root}} \le (\check{\gamma}_{\mathrm{root}}\, q\check{\gamma}_{\mathrm{hyb}}^2 + E_{01})^2/q^2$;*
4. *$\max_\psi |l_{10}| \le \check{\gamma}_{\mathrm{root}}/(1 - E_{00}\check{\gamma}_{\mathrm{hyb}}^2/q) + E_{01}/m_0$;*
5. *$\Xi' \le \bar{\varsigma}^{1/2}$;*
6. *$\Xi \le \bar{\varsigma}^{1/2}$;*
7. *$\ell \le \max(1,\ \check{\gamma}_{\mathrm{root}}/(1 - E_{00}\check{\gamma}_{\mathrm{hyb}}^2/q) + E_{01}/m_0)$;*
8. *$m_0 > 0$.*

5.3 The bounds on ffSampling$^{\mathcal{F}}$

Figure 12 describes the objects of the bounds; Proposition 5.9 states the inputs the fixed-point signer meets; Corollary 5.10 its bit security.

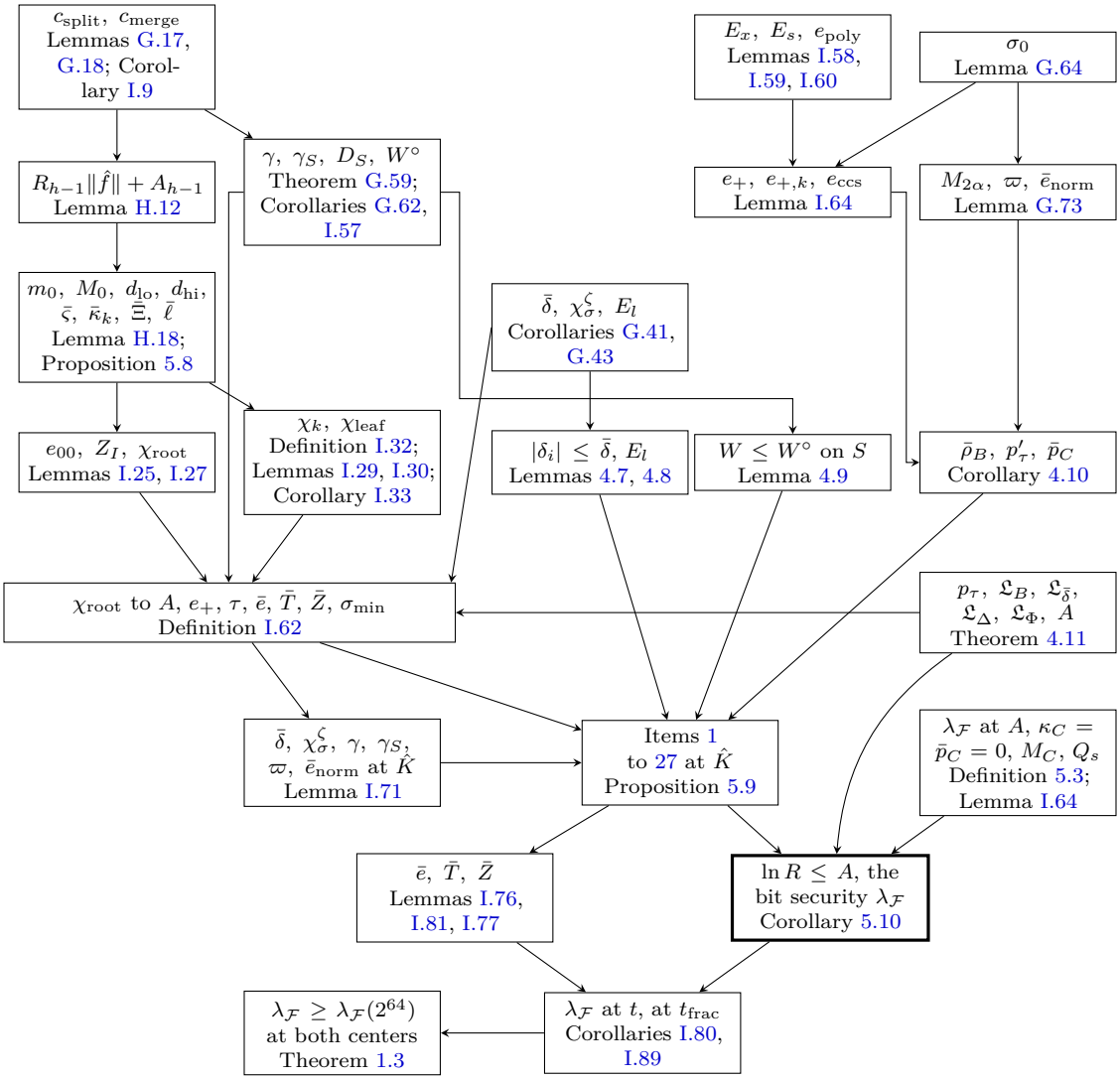


Figure 12: The objects of Proposition 5.9 and Corollary 5.10, each with the statement that bounds it, and the way to Theorem 1.3; an arrow runs from a statement to the statement whose proof cites it.

Proposition 5.9 (Inputs of the phase statements at the fixed-point signer [to table] [to proof])**.** *At a computed center within the bounds below, the fixed-point signer meets the inputs of Lemmas 4.7, 4.8 and 4.9, Corollary 4.10 and Theorem 4.11 at its key's constants, with the terms of Definition I.62, and those statements' bounds hold there.* ***Under Hypotheses I.21 and I.22****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $c \in \{t, t_{\text{frac}}\}$ *be a center,* t *and* t_{frac} *those of Definition 4.5 at the key and* $\mathsf{h}(\mathsf{m})$*;*
- $\bar{e}, \bar{T}, \bar{Z} \in [0, \infty)$.

Define:

- *The signer's words and parameters*
  - $\sigma_{\min}$*, that of Definition I.62;*
  - σ_0*, that of Lemma G.64;*
- *The coefficient norm*
  - $\|\cdot\|$*, the coefficient norm (Appendix G.5);*
- *The center and the samples*
  - $\widetilde{t}_T$*, the computed value of* c *in* $\mathcal{F}_{\text{fx}}$ *(*ffSampling$^{\mathcal{F}}$ *(Algorithm 10) at* $\mathsf{h}(\mathsf{m})$*, lines 9 to 20 at* $c = t$*,* center$_{\text{frac}}$ *(Algorithm 17) at* $c = t_{\text{frac}}$*);*
  - $z' := (z_0, z_1)$*, the sample* ffsamp *(Algorithm 6) returns at* c *(*ffSampling$^{\mathcal{F}}$*, line 24);*

- *The terms*
  - α, $e_{+,k}$ *and* e_{ccs}, *those of Definition I.62;*
  - c_n, $\sigma_{\max}$, $\bar{\delta}$, ϵ *and* ε_0°, *those of Definition I.62;*
  - R°, W°, p_τ *and* $\mathfrak{L}_B$, *those of Definition I.62;*
  - p'_τ, *that of Corollary 4.10, precondition 3;*
- *The key constants*
  - $\hat{K}$, *the key's constants (Definition 4.6);*
  - $\bar{\delta}(\hat{K})$, $\chi^\zeta_\sigma(\hat{K})$, $\gamma(\hat{K})$, $\gamma_S(\hat{K})$, $\varpi(\hat{K})$, $\bar{e}_{\mathrm{norm}}(\hat{K})$, $M_{2\alpha}(\hat{K})$ *and* $\mathfrak{L}_B(\hat{K})$, *those of Lemma I.71 at* τ, $\bar{e}$, $\bar{T}$ *and* $\bar{Z}$;
- *The leaves*
  - $\forall z \in \mathbb{Z}^N :\ W(z) := \sum_{i \le N} \Delta_i(z_{<i})^2 / \sigma_i(z_{<i})^2$;
  - $\widetilde{B}_i$, $\bar{\rho}_B$ *and* $\bar{p}_C$, *those of Definition A.28 at the signer's base sampler;*
  - C_i, *the fringe sets of Definition A.26 at the signer's base sampler;*
  - $\forall s > 0\ \forall c, x \in \mathbb{R} :\ \rho_{s,c}(x) := e^{-(x-c)^2/(2s^2)}$ *(Definition A.2 at* $k := 1$*);*
  - $\forall s > 0\ \forall c \in \mathbb{R} :\ \rho_{s,c}(\mathbb{Z}) := \sum_{x \in \mathbb{Z}} \rho_{s,c}(x)$ *(Definition A.2 at* $k := 1$ *and* $A := \mathbb{Z}$*).*

Assume:

(A1) $\|\widetilde{t}_T - c\| \le \bar{e}$;

(A2) $\|c\| \le \bar{T}$;

(A3) $\forall z \in S :\ \|z'\| \le \bar{Z}$;

(A4) $p'_\tau < 1$.

Then the signer meets the inputs of the tree, the centers, the base sampler and the summary at its key's constants, and their bounds hold there:

1. *The signer is a Falcon-type signer at* $(0, \zeta)$;
2. $\forall k \le 18 :\ e_{+,k} \ge 0$;
3. $e_{\mathrm{ccs}} \in [0, 1)$;
4. $\chi^\zeta_\sigma(\hat{K}) < 1$;
5. $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$;
6. $\forall z \in S\ \forall i \le N :\ |\delta_i| \le \bar{\delta}(\hat{K})$;
7. $\gamma(\hat{K}) + \gamma_S(\hat{K}) < 1$;
8. $\forall z \in S :\ W(z) \le W^\circ$;
9. $\bar{\delta}(\hat{K}) < 1$;
10. $\sigma_{\max}(1 + \bar{\delta}(\hat{K})) \le \sigma_0$;
11. $\varpi(\hat{K}) < 1$;
12. $\bar{e}_{\mathrm{norm}}(\hat{K}) < 1$;
13. $\forall i \le N\ \forall z_{<i}\ \forall c \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$;
14. $\mathfrak{L}_B(\hat{K}) \le \mathfrak{L}_B$;
15. $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}(\hat{K})$;
16. $p_\tau \ge 0$;
17. $\forall i \le N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$;
18. $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$;

19. $\forall S' \subseteq S\ \forall I \subseteq \{1,\dots,N\}:\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$;

20. $\sigma_{\min} > 0$;

21. $\forall i \le N:\ \sigma_i \in (\sigma_{\min}, \sigma_{\max})$;

22. $\forall i \le N\ \forall z_{<i}:\ \widetilde{\sigma}_i > \sigma_{\min}$;

23. $(1+\bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$;

24. $\varepsilon_0^\circ < 1$;

25. $p'_\tau + \bar{p}_C < 1$;

26. $\bar{\delta} \in [0, 1)$;

27. $W^\circ \ge 0$.

Corollary 5.10 (The fixed-point signer's divergence and bit security [to table] [to proof])**.** *At a computed center within the bounds below, the fixed-point signer's* $\ln R$ *is at most* A*, its fringe classes and its divergence conditioned on* S_0 *are bounded, and its signatures keep the bit security* $\lambda_{\mathcal{F}}$*.* ***Under Hypotheses I.21 and I.22****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $c \in \{t, t_{\text{frac}}\}$ *be a center,* t *and* t_{frac} *those of Definition 4.5 at the key and* $\mathsf{h}(\mathsf{m})$*;*
- $\bar{e}, \bar{T}, \bar{Z} \in [0, \infty)$*;*
- $Q_s \in \mathbb{Z}_{>0}$*;*
- $M_C \in \mathbb{Z}_{\ge 0}$.

Define:

- *The coefficient norm*
  - $\|\cdot\|$*, the coefficient norm (Appendix G.5);*
- *The center and the samples*
  - $\widetilde{t}_T$*, the computed value of* c *in* $\mathcal{F}_{\text{fx}}$ *(*ffSampling$^{\mathcal{F}}$ *(Algorithm 10) at* $\mathsf{h}(\mathsf{m})$*, lines 9 to 20 at* $c = t$*,* center$_{\text{frac}}$ *(Algorithm 17) at* $c = t_{\text{frac}}$*);*
  - $z' := (z_0, z_1)$*, the sample* ffsamp *(Algorithm 6) returns at* c *(*ffSampling$^{\mathcal{F}}$*, line 24);*
- *The terms*
  - λ *and* α*, those of Definition I.62;*
  - $\sigma_{\max}$*,* $\bar{\delta}$ *and* ε_0°*, those of Definition I.62;*
  - W°*,* p_τ*,* $\mathfrak{L}_B$*,* $\mathfrak{L}_{\bar{\delta}}$*,* $\mathfrak{L}_\Delta$*,* $\mathfrak{L}_\Phi$ *and* A*, those of Definition I.62;*
  - p'_τ*, that of Corollary 4.10, precondition 3;*
- *The classes and the measures*
  - S_k*,* S_0*,* P_{S_0} *and* Q_{S_0}*, those of Theorem 4.11 at* $S' := S$*;*
  - $R_\alpha^{S_k}(P \,\|\, Q)$*, that of Definition A.28 at* $\mathcal{Y} := S_k$*;*
  - κ_C *and* $\bar{p}_C$*, those of Definition A.28 at the signer's base sampler;*
  - R*, that of Definition A.30 at* S*,* $\bar{\delta}$ *and the signer's* $\bar{\rho}_B$*;*
  - $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$*, the probability measures of* Q_s *independent signatures on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1);*
- *The bit security*
  - $\lambda_{\mathcal{F}}$*, that of Definition 5.3 at* A*,* κ_C*,* $\bar{p}_C$ *and* M_C.

Assume:

(A1) $\|\widetilde{t}_T - c\| \le \bar{e}$*;*

(A2) $\|c\| \le \bar{T}$*;*

(A3) $\forall z \in S:\ \|z'\| \le \bar{Z}$*;*

(A4) $p'_\tau < 1$.

Then $\ln R$ *is at most* A*, the fringe classes and the conditional divergence are bounded, and the bit security holds:*

1. $\ln R \le A$;

2. $\forall k \le N:\ R_\alpha^{S_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k R^{\alpha-1}$;

3. $R_\alpha(P_{S_0} \,\|\, Q_{S_0}) \le R\,(1 - P(S_0^c))^{-\alpha/(\alpha-1)}$;

4. $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda}:\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$.

5.4 The changes

This subsection describes the four changes to the fixed-point implementation.

The rejection at the saturated exponent. BerExp in $\mathcal{F}_{\text{fx}}$ rejects the candidates at which the reference's shift saturates (Definition I.20, item 1), so every fringe set is empty (Figure 13). Theorem 5.11 is the fringe leaves' cost in bits, none at empty fringe sets.

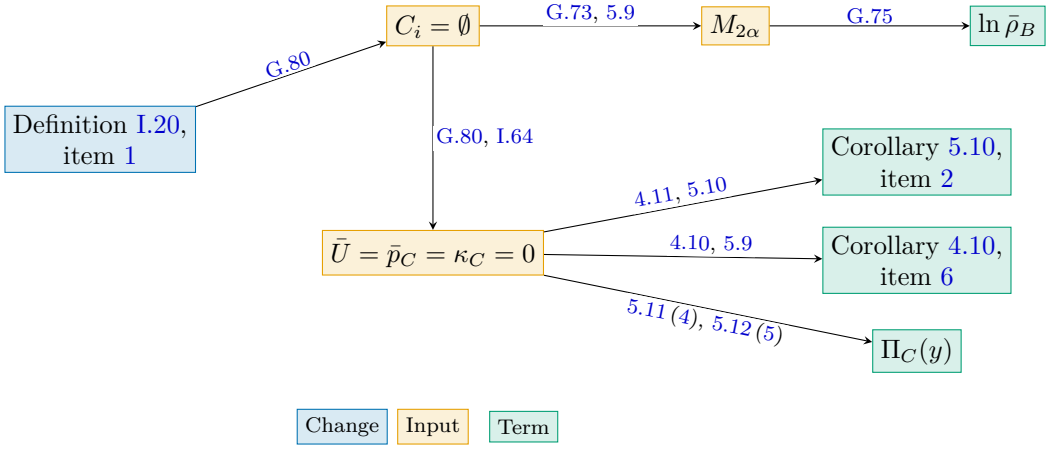


Figure 13: The inputs the rejection at the saturated exponent sets and the terms it moves, each arrow labeled by its statements.

Theorem 5.11 (Bit cost of the fringe leaves [to table] [to proof]). *The level $\lambda_{\mathcal{F}}$ with fringe leaves is the level $\lambda_{\mathcal{F}}^{\emptyset}$ at empty fringe sets less $\log_2(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}}\Pi_C(y))$ bits. Each fringe leaf multiplies the probability-preservation bound y in $\Pi_C(y)$ by at most g_C. The union bound of m fringe leaves is at most $\mu_C^m/m!$. Let:*

- $\lambda \in \mathbb{R}$;
- $Q_s \in \mathbb{Z}_{>0}$;
- $A \in \mathbb{R}$;
- $M_C \in \mathbb{Z}_{\ge 0}$.

Define:

- *y and $\lambda_{\mathcal{F}}$, those of Definition 5.3 at (λ, Q_s, A, M_C);*
- *$\Pi_C(y)$, that of Definition 5.2 at (Q_s, M_C);*
- *$\lambda_{\mathcal{F}}^{\emptyset}$ by $2^{-\lambda_{\mathcal{F}}^{\emptyset}} := Q_s\,P(S'^c) + y$;*
- *$g_C := (Q_s N)^{1/\alpha}\,\bar{U}\,\bar{\rho}_B^{-\alpha_L/(2\alpha)}$;*
- *$\mu_C := Q_s N\,\bar{p}_C$.*

Assume:

(A1) $\bar{\rho}_B > 0$;

(A2) $\bar{U} < \infty$.

Then the fringe leaves' cost in bits is exact, bounded in g_C and μ_C, and zero at empty fringe sets:

1. $\lambda_{\mathcal{F}}^{\emptyset} - \lambda_{\mathcal{F}} = \log_2(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}}\,\Pi_C(y))$;

2. $\Pi_C(y) \le \sum_{m=1}^{M_C} \min(g_C^m\, y,\ \mu_C^m/m!) + \mu_C^{M_C+1}/(M_C+1)!$;

3. $\lambda_{\mathcal{F}}^{\emptyset} - \lambda_{\mathcal{F}} \le \log_2\Big(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}}\Big(\sum_{m=1}^{M_C} \min(g_C^m\, y,\ \mu_C^m/m!) + \mu_C^{M_C+1}/(M_C+1)!\Big)\Big)$;

4. *Assume:*

   (A3) $\bar{p}_C = 0$.

   Then $\lambda_{\mathcal{F}} = \lambda_{\mathcal{F}}^{\emptyset}$.

The three thresholds. The tail checks add the thresholds M_n, D_n and B_n to the four coefficient checks (Definition 5.6), a heavier computation than the four (Statistics I.23, item 4). Theorem 5.12 singles out what the tail checks change in the bit security of Theorem 1.3; Figures 14 and 15 lay out the changes, the inputs they set and the terms the inputs set.

Theorem 5.12 (Under **Hypotheses I.21, I.22 and I.91**, the checks' impact [to table] [to proof])**.** *The items single out what the tail checks of Definition 5.6 change in the fixed-point signer's bit security: the bit security our proof keeps without them is that of Corollaries I.79, item 1, and I.88, item 1, the bit security with them that of Theorem 1.3. The bit security of item 4 consists of these terms: $Q_s P(S_\tau^c)$, η, y and $\Pi_C(y)$. **Under Hypotheses I.21, I.22 and I.91**, define:*

- $q := 12289$ *(Definition A.13).*

Let:

- $c \in \{t, t_{\mathrm{frac}}\}$ *be a center (Definition A.25);*
- (f, g, F, G) *be a checked key of degree n (Definition 5.5) passing the tail checks at c (Definition 5.6);*
- $\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ *be a hashed message (Definition A.25);*
- $Q_s \in \{2^{32}, 2^{36}, \dots, 2^{64}\}$;
- $M_C \in \mathbb{Z}_{\ge 0}$.

Define:

- *The signer's words and parameters*
  - $(\lambda, \alpha) := \begin{cases} (128, 257) & n = 512 \\ (256, 513) & n = 1024 \end{cases}$ *(Definition I.62);*
  - $N := 2n$ *(Definition A.25);*
  - $\eta := 2^{-\lambda}$;
- *The stored words*
  - M_n, D_n *and* B_n, *those of Definition I.14 at n and c;*
- *The probability measures*
  - P, *the output measure of* $\mathrm{ffSampling}^{\mathcal{F}}$ *(Definition A.25 at the key,* $\mathsf{h}(\mathsf{m})$ *and c);*
- *The tail-cut event*
  - τ, S_τ *and* E, *those of Corollary I.80 at $c = t$ and those of Corollary I.89 at $c = t_{\mathrm{frac}}$, at the key,* $\mathsf{h}(\mathsf{m})$ *and* Q_s;
- *The leaf perturbations*
  - δ_i, W *and* W^{tail}, *those of Lemma 4.14 at* $\mathcal{F}_{\mathrm{fx}}$, *the key,* $\mathsf{h}(\mathsf{m})$, $t_{\mathrm{c}} := c$, τ, $M := M_n$, $D := D_n$, $B := B_n$, $\eta_1 := \eta/Q_s$ *and the inputs of Lemma I.73;*
- *The terms*
  - $\mathfrak{L}_B$, *that of Definition I.62 at c and τ, and at the $\bar{e}$, $\bar{T}$ and $\bar{Z}$ of Lemma I.77 at $c = t$ and of Lemma I.81 at $c = t_{\mathrm{frac}}$, at τ;*
  - $\mathfrak{L}_{\bar{\delta}}$, $\mathfrak{L}_\Delta$ *and* $\mathfrak{L}_\Phi$, *those of Proposition I.72 at c, Q_s, τ, $W^\circ := W^{\mathrm{tail}}$, $\bar{\delta} := D_n$, E and $\eta_E := \eta$, and at the $\bar{e}$, $\bar{T}$ and $\bar{Z}$ of Lemma I.77 at $c = t$ and of Lemma I.81 at $c = t_{\mathrm{frac}}$, at τ;*
  - $A := \mathfrak{L}_B + \mathfrak{L}_{\bar{\delta}} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$ *(Proposition I.72);*
  - $y := (2^{-\lambda} e^{Q_s A})^{(\alpha-1)/\alpha}$ *(Definition 5.3);*
  - $\Pi_C(y)$, *that of Definition 5.2 at* (Q_s, M_C);

– $\lambda_{\mathcal{F}}$, *that of Corollary I.80 at* $c = t$ *and that of Corollary I.89 at* $c = t_{\mathrm{frac}}$, *at the key,* $\mathsf{h}(\mathsf{m})$ *and* Q_s.

Then the thresholds bound $|\delta_i|$ *and the leaf sum, the event* E *costs* η, *and* $2^{-\lambda_{\mathcal{F}}}$ *is the sum of four terms, the last zero:*

1. $\forall i \le N\ \forall z_{<i}:\ |\delta_i(z_{<i})| \le D_n$;
2. $\forall z \in S_\tau \cap E:\ W(z) \le W^{\mathrm{tail}}$;
3. $Q_s P(S_\tau \cap E^c) \le \eta$;
4. $2^{-\lambda_{\mathcal{F}}} = Q_s\, P(S_\tau^c) + \eta + y + \Pi_C(y)$;
5. $\Pi_C(y) = 0$.

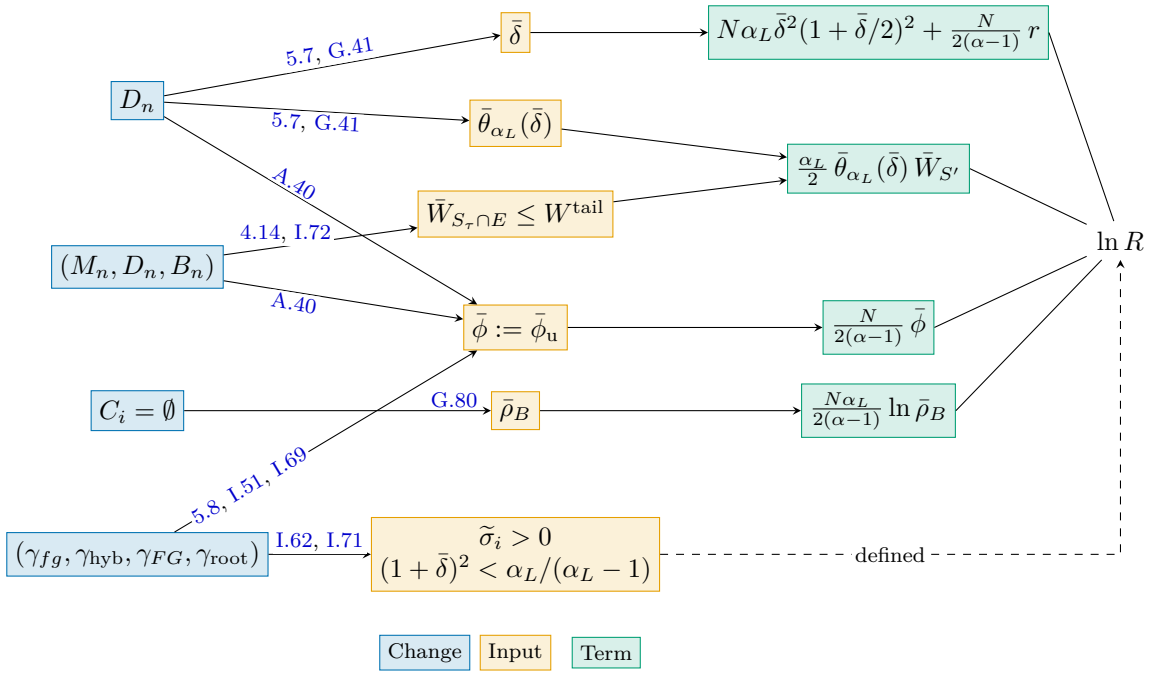


Figure 14: The terms of $\ln R$ of Theorem 1.1, the inputs that set them and the changes that set the inputs, each arrow labeled by its statements, $S' := S_\tau \cap E$ (Theorem 5.12).

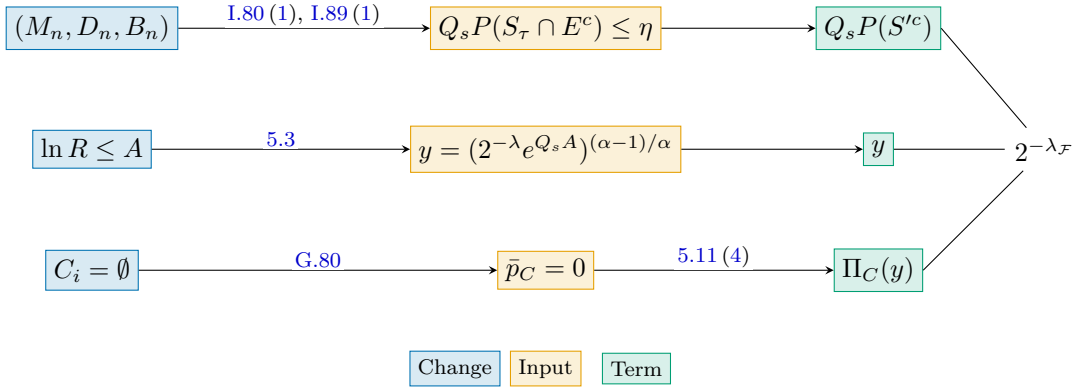


Figure 15: The terms of the bit security $2^{-\lambda_{\mathcal{F}}} = Q_s\, P(S'^c) + y + \Pi_C(y)$ of Theorem 1.2, the inputs that set them and the changes that set the inputs, each arrow labeled by its statements, $S' := S_\tau \cap E$ (Theorem 5.12).

The root's identity. The root node's second diagonal is computed through the NTRU identity (Lemma I.27), which sets the head of the chain from the root's diagonals to $\bar{\delta}$ and E_l (Figure 16). The chain meets assumptions of the tree, the centers, the base sampler and the summary; the terms of $\ln R$ themselves are read at the thresholds.

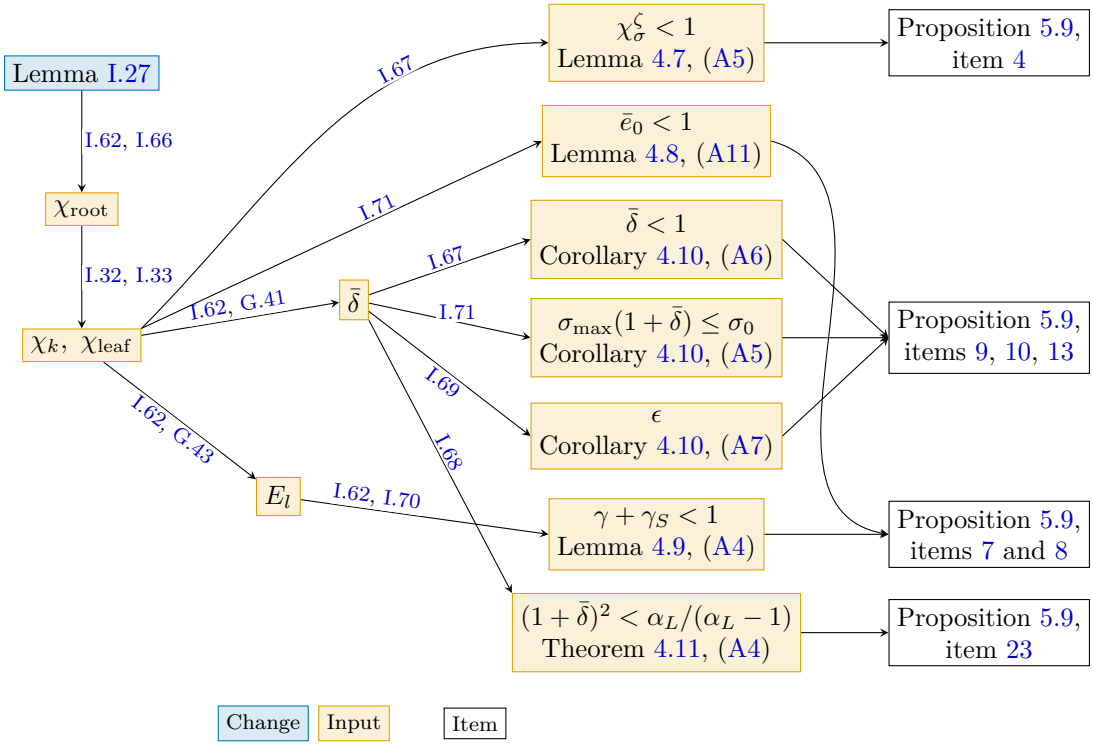


Figure 16: The inputs the root's identity sets, the assumptions of the tree, the centers, the base sampler and the summary they meet, and the items of Proposition 5.9 that state them, each arrow labeled by its statements.

The one division. Each $LDL^\dagger$ step takes one division where the reference inverts and then multiplies (Lemma I.10, items 5 and 6), and the no-overflow lemmas of those steps read it (Figure 17).

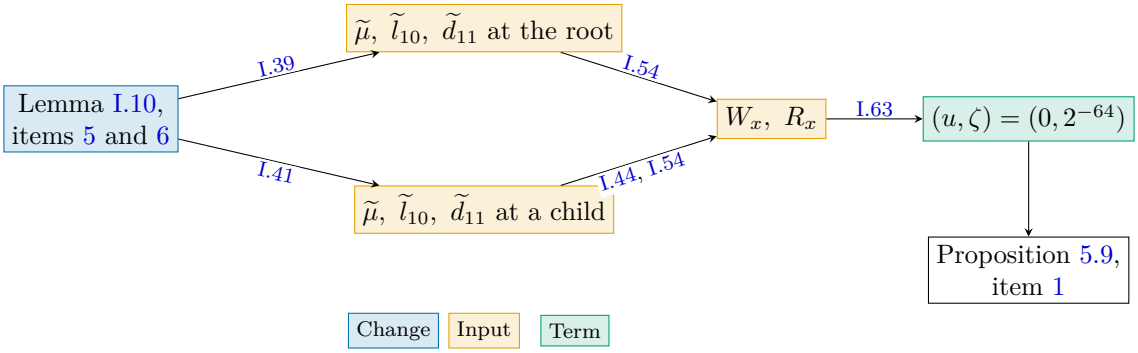


Figure 17: The inputs the one division sets and the realization it defines for the signer, the first item of Proposition 5.9, each arrow labeled by its statements.

5.5 The losses

Theorem 1.3 bounds the fixed-point signer's bit security from below; Tables 10 and 11 list the bounds at $n = 512$ and at $n = 1024$.

Theorem 1.3 (restated). The items bound the fixed-point signer's bit security from below at both centers and at every number of signatures of the sweep: the bound, its least value over the sweep, and the probability that the tail bound fails. **Under Hypotheses I.21, I.22 and I.91,** define:

- q, the modulus of Definition A.13.

Let:

- $c \in \{t, t_{\text{frac}}\}$ be a center (Definition A.25);
- (f, g, F, G) be a checked key of degree n (Definition 5.5) passing the tail checks at c (Definition 5.6);
- $\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ be a hashed message (Definition A.25);
- $Q_s \in \{2^{32}, 2^{36}, \dots, 2^{64}\}$.

Define:

- The signer's words and parameters
  - $\lambda := 128$ at $n = 512$ and $\lambda := 256$ at $n = 1024$ (Definition I.62);
  - $N := 2n$ (Definition A.25);
  - $\eta := 2^{-\lambda}$;
- The stored words
  - M_n, D_n and B_n, those of Corollary I.80 at $c = t$ and those of Corollary I.89 at $c = t_{\text{frac}}$, at the key, $\mathsf{h}(\mathsf{m})$ and Q_s;
- The tail-cut events
  - S_τ and S_{τ_K}, those of Corollary I.80 at $c = t$ and those of Corollary I.89 at $c = t_{\text{frac}}$, at the key, $\mathsf{h}(\mathsf{m})$ and Q_s;
- The three quantities
  - μ_{key}, that of Corollary I.80 at $c = t$ and that of Corollary I.89 at $c = t_{\text{frac}}$, at the key, $\mathsf{h}(\mathsf{m})$ and Q_s;
- The sub-event
  - E, that of Corollary I.80 at $c = t$ and that of Corollary I.89 at $c = t_{\text{frac}}$, at the key, $\mathsf{h}(\mathsf{m})$ and Q_s;
- The probability measures
  - P and Q, the output measures of $\text{ffSampling}^{\mathcal{F}}$ and $\text{ffSampling}^{\mathbb{R}}$ (Definition A.25 at the key, $\mathsf{h}(\mathsf{m})$ and c);
  - $P^{\otimes Q_s}$ and $Q^{\otimes Q_s}$, the probability measures of Q_s independent outputs $(z^{(1)}, \dots, z^{(Q_s)})$ of P and of Q on $(\mathbb{Z}^N)^{Q_s}$ (Fact A.45, item 1);
- The leaf perturbations
  - I_N, $\widetilde{\sigma}_i$, K, r and δ_i, those of Definition 4.12 at $\mathcal{F}_{\text{fx}}$, the key, $\mathsf{h}(\mathsf{m})$ and $t_{\text{c}} := c$;
- The terms
  - $\lambda_{\mathcal{F}}$, that of Corollary I.80 at $c = t$ and that of Corollary I.89 at $c = t_{\text{frac}}$, at (n, λ, Q_s).

Then

1. At $c = t$ or $c = t_{\text{frac}}$: $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$;

	$c = t$	$c = t_{\text{frac}}$
$n = 512$	2. $\lambda_{\mathcal{F}} \ge 126.28$	3. $\lambda_{\mathcal{F}} \ge 126.70$
$n = 1024$	4. $\lambda_{\mathcal{F}} \ge 248.78$	5. $\lambda_{\mathcal{F}} \ge 253.53$

6. At $c = t$ or $c = t_{\text{frac}}$: $Q_s P(S_\tau \cap E^c) \le 2^{-\lambda}$.

Signer	Center	R of	2^{48}	2^{52}	2^{56}	2^{60}	2^{64}
fixed-point	t	Theorems 1.1 and F.4	126.7290	126.7289	126.7274	126.7037	126.2885
fixed-point	t_{frac}	Theorems 1.1 and F.4	126.7290	126.7289	126.7289	126.7274	126.7031

Table 10: The fixed-point signer at $(n, \lambda) = (512, 128)$: a lower bound of the bit security $\lambda_{\mathcal{F}}$ in bits at the tail of Lemma 4.14 at both centers (Theorem 1.3; Corollaries I.80 and I.89) by Q_s; $\ln R$ at the pair $(\bar{W}_{\alpha_L}(\bar{\delta}), \bar{\theta}_{\alpha_L}(\bar{\delta}))$ of Theorem 1.1 and at the suprema of Theorem F.4 (Definition A.30) yield the same cell. Gate: `verify/gates/fx/tail_level_cells.py`.

Signer	Center	R of	2^{48}	2^{52}	2^{56}	2^{60}	2^{64}
fixed-point	t	Theorems 1.1 and F.4	254.7284	254.7275	254.7131	254.4684	248.7806
fixed-point	t_{frac}	Theorems 1.1 and F.4	254.7284	254.7282	254.7246	254.6661	253.5356

Table 11: The fixed-point signer at $(n, \lambda) = (1024, 256)$: a lower bound of the bit security $\lambda_{\mathcal{F}}$ in bits at the tail of Lemma 4.14 at both centers (Theorem 1.3; Corollaries I.80 and I.89) by Q_s; $\ln R$ at the pair $(\bar{W}_{\alpha_L}(\bar{\delta}), \bar{\theta}_{\alpha_L}(\bar{\delta}))$ of Theorem 1.1 and at the suprema of Theorem F.4 (Definition A.30) yield the same cell. Gate: `verify/gates/fx/tail_level_cells.py`.

5.6 Comparison with the fixed-point analysis

[L2: BFLP26, Thm. 1] bounds the loss of an idealized fixed-point Falcon from constants it assumes; Theorem 1.3 bounds the loss of the fixed-point signer from quantities it bounds under three code-alignment hypotheses. The two share the leading term of the leaf bound; they differ in how the leaf bounds combine into the signature's bound, and in where the leaf deviations come from.

The base sampler. BFLP26, Thm. 1 takes the base sampler as a perfect discrete Gaussian and points at HPRR20, Thm. 7 for the real one, which rests on a pointwise relative bound on the exponential's approximation and on the table's divergence at order $2\lambda + 1$ against the half Gaussian at $\sigma_{\max}$. Theorem 1.3 takes the sampler's moment $\bar{\rho}_B$ (Corollary 4.10), bounded from the rounding of BerExp (Corollary G.75). The base sampler's term of the loss is the weighted second moment of the sampler's relative deviation (Lemma G.65); its ϵ_{hi} also bounds the tail's mass (Corollary E.21). The truncation of the sampler's support, where no pointwise bound applies, is one term of that moment (Appendix K).

The leaf standard deviations. BFLP26, Thm. 1 assumes one relative bound over every leaf and every random tape. Here the bound $\bar{\delta}$ holds over the sub-event S' and is derived from the key down the tree (Lemma 4.7). Under **Hypothesis I.91**, the key generation's check 1 bounds the largest leaf deviation $\bar{\delta}_K$ by the threshold D_n (Definition 5.6, Theorem 5.12).

The leaf centers. BFLP26, Thm. 1 assumes one absolute bound per leaf. Here the centers' shift is the weighted square sum $\bar{W}_{S'}$ (Definition A.27), bounded on the event E by the tail of the leaf sum (Lemma 4.14) from the two quantities checks 2 and 3 bound under **Hypothesis I.91**, the remainder $\bar{B}_K$ and the weighted square sum μ_{key} of K (Definition 4.12). The event outside E costs η, subtracted from the bit security.

The leaf bounds. BFLP26, Lem. 4 and 5 bound one leaf at order α with a remainder written $O(\cdot)$, the smoothing parameter at every leaf and a tail probability fixed at 2^{-80}. Here Lemma 4.1 is the exact identity for a shifted center and a scaled standard deviation at once, read at order $\alpha_L = 2\alpha - 1$ (Proposition 4.2). The remainder r is explicit, the normalizer ratio is bounded explicitly (Corollary E.14, Definition A.40), and the pole $(1 + \bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$ is an assumption of Theorem 1.1.

The numbers. BFLP26, Sec. 5.5 measures the leaf deviations of a 64-bit fixed-point Falcon-512 against an arbitrary-precision one and replaces the two bounds by root mean square errors. Here the numbers are read from the thresholds M_n, D_n and B_n the key generation checks, and hold, under the three code-alignment hypotheses, for every key it accepts, at both degrees and both centers (Tables 10 and 11).

The code. The arithmetic's kernels are machine-checked (Lemma I.10, Section 2.2), and the rest of the C code rests on **Hypotheses I.21, I.22 and I.91**, all three of code alignment.

The loss. BFLP26, Thm. 1 loses 2 bits over the signatures under its two inequalities. Under its three code-alignment hypotheses, Theorem 1.3 bounds the bits from below at both centers for every key its key generation accepts.

References

[AAC+22] Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone. NISTIR 8413-upd1: Status report on the third round of the NIST post-quantum cryptography standardization process. NIST Interagency Report, 2022. doi:10.6028/NIST.IR.8413-upd1. 4

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296:625–635, 1993. doi:10.1007/BF01445125. 157, 790

[BFLP26] Daniel De Almeida Braga, Pierre-Alain Fouque, Bachir Lachguel, and Thomas Prest. Toward a secure fixed-point implementation of the Falcon signature scheme. In *CRYPTO 2026*, LNCS 16802, pages 166–197. Springer, 2026. doi:10.1007/978-3-032-35377-1_6. 4, 5, 29, 30, 49, 52, 64, 65, 410, 411, 412, 451, 452, 453, 455, 622, 641, 649, 728, 782, 795

[DP16] Léo Ducas and Thomas Prest. Fast Fourier orthogonalization. In *ISSAC 2016*, pages 191–198. ACM, 2016. doi:10.1145/2930889.2930923. 4

[DRS14] Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. On the closest vector problem with a distance guarantee. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 98–109. IEEE, 2014. The version read is arXiv:1409.8063v2, 26 December 2014. doi:10.1109/CCC.2014.18. 130, 155

[EI93] Stanley C. Eisenstat and Ilse C. F. Ipsen. Relative perturbation techniques for singular value problems. Technical Report YALEU/DCS/RR-942, Yale University, Department of Computer Science, July 1993. 22 July 1993. Published as SIAM Journal on Numerical Analysis 32(6):1972–1988, December 1995, https://www.jstor.org/stable/2158536; the report is the version read and the one the statement numbers cite. 5, 34, 47

[FGdG+26] Pierre-Alain Fouque, Phillip Gajland, Hubert de Groote, Jonas Janneck, and Eike Kiltz. A closer look at Falcon. In Joan Daemen and Emmanuel Thomé, editors, *Advances in Cryptology – EUROCRYPT 2026*, volume 16544 of *Lecture Notes in Computer Science*, pages 3–31, Cham, 2026. Springer. The full version, 2nd March 2026; a preliminary version in the proceedings of EUROCRYPT 2026. doi:10.1007/978-3-032-25327-9_1. 4, 49, 50, 68, 69, 70, 74, 75, 78, 79, 80, 81, 724, 750, 791

[FHK+20] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Specification v1.2, the round-3 submission to the NIST Post-Quantum Cryptography Standardization Project, 2020. 1 October 2020. URL: https://falcon-sign.info/. 4, 14, 26, 27, 68, 77, 83, 796

[Hig02] Nicholas J. Higham. *Accuracy and Stability of Numerical Algorithms*. Society for Industrial and Applied Mathematics, Philadelphia, second edition, 2002. doi:10.1137/1.9780898718027. 15, 68, 70

[HPRR20] James Howe, Thomas Prest, Thomas Ricosset, and Mélissa Rossi. Isochronous Gaussian sampling: From inception to implementation. In *PQCrypto 2020*, pages 53–71. Springer, 2020. doi:10.1007/978-3-030-44223-1_4. 4, 64, 67, 724

[LSS14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld. GGHLite: More efficient multilinear maps from ideal lattices. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 239–256, Berlin, Heidelberg, 2014. Springer. The full version of a paper presented at the EUROCRYPT 2014 conference. doi:10.1007/978-3-642-55220-5_14. 162

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718, Berlin, Heidelberg, 2012. Springer. The full version, September 14, 2011. doi:10.1007/978-3-642-29011-4_41. 133, 790

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007. The authors' copy, December 27, 2005; a preliminary version in the Proceedings of the 45th Annual Symposium on Foundations of Computer Science, FOCS 2004, DOI 10.1109/FOCS.2004.72. doi:10.1137/S0097539705447360. 68, 97

[NIS24a] Module-lattice-based digital signature standard. Federal Information Processing Standards Publication 204, 2024. Published August 13, 2024. doi:10.6028/NIST.FIPS.204. 4

[NIS24b] Module-lattice-based key-encapsulation mechanism standard. Federal Information Processing Standards Publication 203, 2024. Published August 13, 2024. doi:10.6028/NIST.FIPS.203. 4

[NIS26] New plan for FN-DSA. Message to the pqc-forum, the NIST post-quantum cryptography forum, posted by Ray A. Perlner on behalf of NIST, 2026. September 28, 2026. URL: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/7z-y5qp-W2Y. 4

[Por26] Thomas Pornin. A RAM-efficient implementation of Falcon. Cryptology ePrint Archive, Paper 2026/1915, 2026. 9 September 2026; the code at https://github.com/pornin/c-fn-dsa-alt. URL: https://eprint.iacr.org/2026/1915. 4

[Pre17] Thomas Prest. Sharper bounds in lattice-based cryptography using the Rényi divergence. In *ASIACRYPT 2017*, LNCS 10624, pages 347–374. Springer, 2017. doi:10.1007/978-3-319-70694-8_13. 4, 8, 724, 750, 752, 754, 790

[PRR19] Thomas Prest, Thomas Ricosset, and Mélissa Rossi. Simple, fast and constant-time Gaussian sampling over the integers for Falcon, 2019. The version read, 17 pages, names no venue; its published form is [HPRR20]. 724

[ZSS19] Raymond K. Zhao, Ron Steinfeld, and Amin Sakzad. FACCT: Fast, compact, and constant-time discrete Gaussian sampler over integers. *IEEE Transactions on Computers*, 69(1):126–137, 2019. The version read is the authors' version, whose first line names the version of record at the DOI. doi:10.1109/TC.2019.2940949. 724

A Definitions and notation

Structure. This appendix states formally the definitions and facts of Section 3. Appendix A.1 states the primitives, Appendix A.2 the realization, Appendix A.3 the relations, Appendix A.4 the fast Fourier sampler, Appendix A.5 the objects of the main theorem, Appendix A.6 the tree of a key, Appendix A.7 the normalizer ratio and Appendix A.8 the facts the proofs use. Table 12 lists this appendix's definitions and facts.

Table 12: Appendix A: its definitions and facts.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Def. A.1					
Def. A.2					L1: FGdG+26, Def. 6
Def. A.3					L1: FGdG+26, Def. 8
Def. A.4	✓				L1: Hig02, (2.8)
Def. A.5					
Fact A.6					
Fact A.7					
Def. A.8	✓				
Def. A.9					
Def. A.10	✓				
Def. A.11					
Def. A.12					L1: FGdG+26, Def. 4; L1: FGdG+26, Def. 6
Def. A.13					
Def. A.14					
Def. A.15					L1: FGdG+26, App. F.3
Fact A.16	✓				L1: FGdG+26, App. F.3
Def. A.17					
Def. A.18	✓				
Def. A.19	✓				
Def. A.20					L1: FGdG+26, Alg. 2
Def. A.21	✓				L1: FGdG+26, Alg. 3
Fact A.22					L1: FGdG+26, Section 2.3; L1: FGdG+26, Def. 7; L1: FGdG+26, Lem. 22
Def. A.23	✓				
Def. A.24					L1: FHK+20, Alg. 15 at $\sigma' := \sigma$, $\mu := c$
Def. A.25	✓				
Def. A.26					
Def. A.27					
Def. A.28	✓				
Def. A.29	✓				
Def. A.30	✓				
Fact A.31	✓				
Def. A.32	✓				
Fact A.33	✓				
Fact A.34					
Def. A.35					
Def. A.36					
Def. A.37					
Def. A.38	✓				
Def. A.39	✓				
Def. A.40	✓				
Fact A.41	✓				
Fact A.42	✓				
Fact A.43	✓				
Fact A.44	✓				
Fact A.45	✓				L1: MR07, Lem. 2.8
Def. A.46	✓				

A.1 The primitives

Definition A.1 (The integers' ranges, the ring of real polynomials and its FFT form [to table])**.** The positive and the nonnegative integers are two ranges of the integers; the ring of real polynomials modulo $x^m + 1$ carries the coefficient norm, and the FFT form of a polynomial f is $(f(\psi_k))_{k<m/2}$, ψ_k the odd powers of a primitive $2m$-th root of unity. Define:

- $\mathbb{Z}_{>0} := \{\, k \in \mathbb{Z} : k > 0 \,\}$ and $\mathbb{Z}_{\geq 0} := \{\, k \in \mathbb{Z} : k \geq 0 \,\}$, the positive and the nonnegative integers.

Let:

- $m \in \mathbb{Z}_{>0}$, a power of two.

Define:

- $\mathcal{R}_m := \mathbb{R}[x]/(x^m + 1)$, the ring of real polynomials modulo $x^m + 1$.

Let:

- $f \in \mathcal{R}_m$.

Define:

- $f_{[i]} \in \mathbb{R}$ for $i < m$, the i-th coefficient of f: $f = \sum_{i<m} f_{[i]} x^i$;
- $\|f\| := \left(\sum_{i<m} f_{[i]}^2\right)^{1/2}$, the coefficient norm;
- $\psi := e^{i\pi/m}$, the primitive $2m$-th root of unity over $\mathbb{C}$;
- $\psi_k := \psi^{2k+1}$ for $k = 0, \ldots, m/2 - 1$;
- $(f(\psi_k))_{k<m/2}$, the FFT form of f.

Definition A.2 (The Gaussian function and the discrete Gaussian [to table])**.** The Gaussian function weighs a point by its distance to a center, and the discrete Gaussian over a countable set is the Gaussian function normalized on that set. Let:

- $k \geq 1$, an integer;
- $s > 0$;
- $c \in \mathbb{R}^k$;
- $A \subseteq \mathbb{R}^k$, a countable set.

Define:

- $\|x\| := \left(\sum_{j \leq k} x_j^2\right)^{1/2}$ for $x \in \mathbb{R}^k$, the Euclidean norm;
- $\rho_{s,c}(x) := \exp(-\|x - c\|^2/(2s^2))$ for $x \in \mathbb{R}^k$, the Gaussian function with standard deviation s and center c [L1: FGdG+26, Def. 6];
- $\rho_s := \rho_{s,0}$;
- $\rho_{s,c}(A) := \sum_{x \in A} \rho_{s,c}(x) \in [0, \infty]$;
- $D_{A,s,c}(x) := \rho_{s,c}(x)/\rho_{s,c}(A) \in (0, 1]$ for $x \in A$, where $0 < \rho_{s,c}(A) < \infty$, the discrete Gaussian over A [L1: FGdG+26, Def. 6];
- $D_{\mathbb{Z},s,c} := D_{A,s,c}$ at $k := 1$ and $A := \mathbb{Z}$, the discrete Gaussian over $\mathbb{Z}$.

The items write out the Gaussian function and the discrete Gaussian at $k := 1$ and $A := \mathbb{Z}$.

1. $\forall x \in \mathbb{R} :\ \rho_{s,c}(x) = e^{-(x-c)^2/(2s^2)}$;
2. $\forall z \in \mathbb{Z} :\ D_{\mathbb{Z},s,c}(z) = \rho_{s,c}(z)/\rho_{s,c}(\mathbb{Z})$, where $\rho_{s,c}(\mathbb{Z}) \in (0, \infty)$.

Definition A.3 (The Rényi divergence and the expectations [to table])**.** The Rényi divergence compares two probability measures on a countable set, and the expectation and the conditioning are taken under one of them. Let:

- X, a countable set;
- μ, a probability measure on X;
- ν, a probability measure on X;
- $\alpha > 1$;
- $f \colon X \to \mathbb{R}$ with $\sum_{x \in X} \mu(x)|f(x)| < \infty$;
- $E \subseteq X$ with $\mu(E) > 0$.

Define:

- $\mathrm{Supp}(\mu) := \{x \in X : \mu(x) > 0\}$, the support of μ;
- $R_\alpha(\mu \,\|\, \nu) := \left(\sum_{x \in \mathrm{Supp}(\mu)} \mu(x)^\alpha \, \nu(x)^{1-\alpha}\right)^{1/(\alpha-1)} \in (0, \infty]$, where $\mathrm{Supp}(\mu) \subseteq \mathrm{Supp}(\nu)$, the Rényi divergence of order α [L1: FGdG+26, Def. 8];
- $\mathbb{E}_\mu[f] := \sum_{x \in X} \mu(x) f(x)$, the expectation, also written $\mathbb{E}_{x \leftarrow \mu}[f(x)]$;
- $\mu(A \,|\, E) := \mu(A \cap E)/\mu(E)$ for $A \subseteq X$, the probability measure μ conditioned on E;
- $\mathbb{E}_\mu[f \,|\, E] := \sum_{x \in X} \mu(\{x\} \,|\, E) f(x)$, the expectation conditioned on E.

A prefix of a sequence in the place of E names the event of the sequences that start with it.

The proofs frequently use the following identities, the $(\alpha-1)$-th power of the Rényi divergence as a sum over $\mathrm{Supp}(\mu)$ and as a sum over X.

1. $R_\alpha(\mu \,\|\, \nu)^{\alpha-1} = \sum_{x \in \mathrm{Supp}(\mu)} \mu(x)^\alpha \, \nu(x)^{1-\alpha}$, where $\mathrm{Supp}(\mu) \subseteq \mathrm{Supp}(\nu)$;
2. $R_\alpha(\mu \,\|\, \nu)^{\alpha-1} = \sum_{x \in X} \mu(x)^\alpha \, \nu(x)^{1-\alpha}$, where $\forall x \in X : \ \nu(x) > 0$.

A.2 The realization

Definition A.4 (The model [to table])**.** A realization is a set of reals closed under the code's rounded operations, each within a relative bound u and an absolute bound ζ, in which the shared algorithms' preconditions on the halving, the small integers, the negation and the conjugate hold; $\mathbb{R}$ itself is one, with the identity as fl and $(0, 0)$ as (u, ζ). Let:

- $\mathcal{F} \subset \mathbb{R}$, with $\mathrm{fl}(x \circ y) \in \mathcal{F}$ for $\circ \in \{+, -, \times, /\}$ and $\mathrm{fl}(\sqrt{x}) \in \mathcal{F}$ for $x, y \in \mathcal{F}$;
- $u \geq 0$;
- $\zeta \geq 0$.

Define:

- $\widetilde{c} \in \mathcal{F}$, the stored value of each constant $c \in \mathbb{R}$ of the code;
- $\mathbb{C} := \mathbb{R}[x]/(x^2 + 1)$.

The code computes:

- In `fxp/`, $\mathrm{fl}(x) \in 2^{-64}\mathbb{Z}$ with $|\mathrm{fl}(x) - x| \leq 2^{-65}$, a tie away from 0 [L0: `fxp/sign_fxp.c:101`];
- In `fxp/`, `fxp_inv`$(x) =$ `fxp_div`$(1, x)$ [L0: `fxp/sign_fxp.h:412`].

We have

1. $\forall \circ \in \{+, -, \times, /\}\ \forall x, y \in \mathcal{F}\ \exists u_\circ, \zeta_\circ \in \mathbb{R},\ |u_\circ| \leq u,\ |\zeta_\circ| \leq \zeta :\ \mathrm{fl}(x \circ y) = (x \circ y)(1 + u_\circ) + \zeta_\circ$ [L1: Hig02, (2.8)], their model with underflow at $(\delta, \eta) := (u_\circ, \zeta_\circ)$ and $\lambda u := \zeta$, without their restriction that one of δ, η is zero; their (2.4), the standard model, at $\zeta := 0$;
2. $\forall x \in \mathcal{F}\ \exists u_\circ, \zeta_\circ \in \mathbb{R},\ |u_\circ| \leq u,\ |\zeta_\circ| \leq \zeta :\ \mathrm{fl}(\sqrt{x}) = \sqrt{x}(1 + u_\circ) + \zeta_\circ$;
3. $\forall x \in \mathcal{F}\ \exists \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \leq \zeta/2 :\ \mathrm{fl}(x/2) = x/2 + \zeta_\circ$;
4. $\forall \circ \in \{+, -\}\ \forall x, y \in \mathcal{F}\ \exists u_\circ, \zeta_\circ \in \mathbb{R},\ |u_\circ| \leq u,\ |\zeta_\circ| \leq \zeta :\ \mathrm{fl}(\mathrm{fl}(x \circ y)/2) = ((x \circ y)(1 + u_\circ) + \zeta_\circ)/2$;
5. $\forall i \in \mathbb{Z},\ |i| < 2^{53} :\ \mathrm{fl}(i) = i$;
6. $\forall x \in \mathcal{F} :\ \mathrm{fl}(-x) = -x$;
7. $\forall x \in \mathcal{F} :\ \mathrm{fl}(\mathrm{conj}\, x) = \mathrm{conj}\, x$;
8. $(u, \zeta) = (0, 2^{-f})$ at f fractional bits: the fixed-point signer (Definition I.1).

Items 3 to 7 are the preconditions the shared algorithms take on $\mathcal{F}$, stated bare; each signer discharges them, and $\mathbb{R}$ meets them with $u_\circ = \zeta_\circ = 0$.

```
def Rounds (u zeta x fl : Real) : Prop :=
  exists theta eta : Real, |theta| <= u /\ |eta| <= zeta /\ fl = x * (1 + theta) + eta
```

Figure 18: The Lean declarations carrying Definition A.4: `Rounds` (`Model.lean`); Lean's symbols in ASCII.

Definition A.5 (The fixed-point representation [to table])**.** A number of $2^{-64}\mathbb{Z}$ is the integer 2^{64} times it, and the signer stores that integer in a word. Let:

- $a \in 2^{-64}\mathbb{Z}$;
- $W \in \{0, \dots, 2^{128} - 1\}$.

Define:

- The arithmetic
  - $v \ll e := 2^e v$ for $v \in \mathbb{Z}$ and $e \in \mathbb{Z}_{\geq 0}$, the left shift;
  - $v \gg e := \lfloor v/2^e \rfloor$ for $v \in \mathbb{Z}_{\geq 0}$ and $e \in \mathbb{Z}_{\geq 0}$, the right shift;
  - $v \gg_{\mathrm{a}} e := \lfloor v/2^e \rfloor$ for $v \in \mathbb{Z}$ and $e \in \mathbb{Z}_{\geq 0}$, the arithmetic right shift of a two's-complement word;
  - $\mathrm{u}_w(v) := v \bmod 2^w$ for $v \in \mathbb{Z}$ and $w \in \mathbb{Z}_{>0}$, the value of v on w bits, unsigned;
  - $\mathrm{s}_w(v)$, for $v \in \mathbb{Z}$ and $w \in \mathbb{Z}_{>0}$, the element of $[-2^{w-1}, 2^{w-1})$ congruent to v modulo 2^w, the value of v on w bits, signed;
  - $v \,\&\, 1 := v \bmod 2$ for $v \in \mathbb{Z}$, the lowest bit;
- The words
  - $a_{\mathrm{fx64}} := 2^{64} a \in \mathbb{Z}$, the fixed-point representation of a of precision 64;
  - $\mathcal{V}_{\mathrm{fx}} := \{x \in 2^{-64}\mathbb{Z} :$ a line of keygen or ffSampling$^{\mathcal{F}}$ executed in $2^{-64}\mathbb{Z}$ computes $x\}$, the lines of the algorithms they call included (Algorithms 11 and 10);
  - $\forall x \in \mathcal{V}_{\mathrm{fx}} : \ W_x \in \{0, \dots, 2^{128} - 1\}$, the word the signer stores for x, in two 64-bit limbs [L0: `fxp/sign_fxp.h:28-30`];
  - $(W_0, W_1) \in \{0, \dots, 2^{64} - 1\}^2$, the limbs of W: $W = W_0 + 2^{64} W_1$.

The word W stores a when $W = a_{\mathrm{fx64}} \bmod 2^{128}$ and $|a_{\mathrm{fx64}}| < 2^{127}$.

Fact A.6 (Exact operations [to table])**.** The sign, the conjugate, the doublings $2^e x$, the small integers and the roundings to integers are exact, and the halving rounds once. Let:

- $x \in \mathcal{F}$;
- $y \in \mathcal{F}$;
- $e \in \mathbb{Z}$;
- $i \in \mathbb{Z}$.

In the fixed-point signer, we have

1. $\mathrm{fl}(-x) = -x$, $\mathrm{fl}(\mathrm{conj}\, x) = \mathrm{conj}\, x$ [L0: `fxp/sign_fxp.h:225-227`] (Lemma I.2, item 3)
2. $\mathrm{fl}(x/2)$ one rounding at 2^{-65} [L0: `fxp/sign_fxp.h:316-318`] (Definition I.1, item 2) (Lemma I.6, item 1)
3. $\mathrm{fl}(2^e x) = 2^e x$ for $1 \leq e \leq 63$ [L0: `fxp/sign_fxp.h:329-334`] (Lemma I.6, item 3)
4. $\mathrm{fl}(i) = i$ for $|i| < 2^{63}$ [L0: `fxp/sign_fxp.h:179-184`] (Lemma I.7, item 1)
5. $\lfloor x \rfloor$, $\mathrm{trunc}\, x$, $\mathrm{rint}\, x \in \mathbb{Z}$, exact, where $\mathrm{trunc}\, x = \mathrm{sgn}(x)\lfloor |x| \rfloor$ and $\mathrm{rint}\, x$ is the integer nearest to x, a tie to even [L0: `fxp/sign_fxp.h:345-378`] (Lemma I.7, items 2 to 4)
6. $\mathrm{fl}(x + 0) = x$, $\mathrm{fl}(x \times 1) = x$ [derived]
7. $\mathrm{fl}(x \circ y) = \mathrm{fl}(y \circ x)$, $\circ \in \{+, \times\}$ [derived]
8. $\mathrm{fl}(x - y) = x - y$ [L0: `fxp/sign_fxp.h:210-216`] (Lemma I.2, item 2)
9. $\forall a, b \in \mathbb{R},\ a \leq b$: $\mathrm{fl}(a) \leq \mathrm{fl}(b)$, and $\mathrm{fl}(x) = x$: the rounding to nearest is nondecreasing and fixes $\mathcal{F}$ [derived]

Fact A.7 (Halvings and exact operations of the fixed-point signer [to table])**.** In the fixed-point signer, the halving rounds by at most $\zeta/2$, the halved sum or difference of two values is one rounding of the model followed by the halving, and an integer of modulus below 2^{53}, a negation and a conjugate are exact: the signer meets Definition A.4, items 3 to 7. Let:

- $\mathcal{F}$ be the realization of the fixed-point signer, $\mathcal{F}_{\text{fx}}$ of Definition I.1, at $(u, \zeta) = (0, 2^{-64})$;
- $x, y \in \mathcal{F}$;
- $i \in \mathbb{Z}$.

We have

1. $\exists\, \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \le \zeta/2 :\ \text{fl}(x/2) = x/2 + \zeta_\circ$ [L0: `fxp/sign_fxp.h:316-318`] (Fact A.6, item 2);
2. $\forall \circ \in \{+, -\}\ \exists\, u_\circ, \zeta_\circ \in \mathbb{R},\ |u_\circ| \le u,\ |\zeta_\circ| \le \zeta :\ \text{fl}(\text{fl}(x \circ y)/2) = ((x \circ y)(1 + u_\circ) + \zeta_\circ)/2$ [L0: `fxp/sign_fxp.h:316-318`] (Definition I.1, items 1 and 2);
3. $|i| < 2^{53} \Rightarrow\ \text{fl}(i) = i$ [L0: `fxp/sign_fxp.h:179-184`] (Fact A.6, item 4);
4. $\text{fl}(-x) = -x$ [L0: `fxp/sign_fxp.h:225-227`] (Fact A.6, item 1);
5. $\text{fl}(\text{conj}\, x) = \text{conj}\, x$ [L0: `fxp/sign_fxp.h:225-227`] (Fact A.6, item 1).

Definition A.8 (The complex layer [to table])**.** The code's complex operations round each real operation of the complex one. Define:

- $C_{\mathcal{F}} := \mathcal{F}[x]/(x^2 + 1) = \{a_r + i a_i : a_r, a_i \in \mathcal{F}\}$.

Let:

- $a = a_r + i a_i \in C_{\mathcal{F}}$;
- $b = b_r + i b_i \in C_{\mathcal{F}}$;
- $c \in \mathcal{F}$;
- $f \in \mathcal{R}_n$.

Define:

- $(\text{Re}\, f(\psi_k))_{k<n/2} \,\|\, (\text{Im}\, f(\psi_k))_{k<n/2}$, the FFT form of f [L0: `fxp/sign_fxpoly.c:168-193`];
- $a \oplus b := \text{fl}(a_r + b_r) + i\ \text{fl}(a_i + b_i)$ [L0: `fxp/sign_fxp.h:194-200`];
- $a \ominus b := a \oplus (-b)$;
- $a \otimes b := \text{fl}(\text{fl}(a_r b_r) - \text{fl}(a_i b_i)) + i\ \text{fl}(\text{fl}(a_r b_i) + \text{fl}(a_i b_r))$ [L0: `fxp/sign_fxp.h:436-447`];
- $c \otimes a := \text{fl}(c a_r) + i\ \text{fl}(c a_i)$;
- $a \otimes c := c \otimes a$, the order in which the algorithms write it;
- $\text{conj}\, a := a_r - i a_i$, the adjoint;
- $\widetilde{\psi} \in C_{\mathcal{F}}$, the stored value of each root of unity $\psi \in \mathbb{C}$ of the code.

We have

1. $\forall \psi \in \mathbb{C},\ \psi^{2^{11}} = 1,\ \text{Im}\, \psi > 0\ \exists\, u_\circ \in \mathbb{C},\ |u_\circ| \le u + \sqrt{2}\,\zeta :\ \widetilde{\psi} = \psi(1 + u_\circ)$.

Item 1 is a precondition the shared algorithms take on $\mathcal{F}$, stated bare; each signer discharges it. A quantifier $\forall \psi$ on a computed value that names no range ranges over the roots ψ_k, $k < n/2$, at which the FFT form stores the values. The adjoint is exact, $\widetilde{\text{conj}\, a} = \text{conj}\, a$. In `fxp/`, $a \oplus b = a + b$ and $a \ominus b = a - b$ (Definition I.1, item 1).

```
def CAdd (u zeta : Real) (a b s : Complex) : Prop :=
  CRound u zeta (a + b) s

def CMul (u zeta : Real) (a b p : Complex) : Prop :=
  exists prr pii pri pir : Real,
    Rounds u zeta (a.re * b.re) prr /\ Rounds u zeta (a.im * b.im) pii /\
    Rounds u zeta (a.re * b.im) pri /\ Rounds u zeta (a.im * b.re) pir /\
    Rounds u zeta (prr - pii) p.re /\ Rounds u zeta (pri + pir) p.im

def CSub (u zeta : Real) (a b d : Complex) : Prop :=
  CAdd u zeta a (-b) d

noncomputable def CConj (a : Complex) : Complex := starRingEnd Complex a

def CRound (u zeta : Real) (z w : Complex) : Prop :=
  Rounds u zeta z.re w.re /\ Rounds u zeta z.im w.im
```

Figure 19: The Lean declarations carrying Definition A.8: `CAdd`, `CMul`, `CSub`, `CConj`, `CRound` (`Model.lean`); with `Rounds` of Figure 18; Lean's symbols in ASCII.

Throughout, a quantity without a tilde is defined by exact operations from its inputs, the mathematical definition, and a tilde marks the value the code computes for it, defined where it is used by the operations the code performs: fl is one rounding, $\oplus$, $\ominus$, $\otimes$ one complex operation each, and $\widetilde{x}$ a computed value.

A.3 Relations on approximation

Definition A.9 (Sign convention [to table])**.** An expression with signs $\pm$ stands for an interval. Let:

- $\mathcal{A}$, an algebraic structure with a norm $||$;
- $x \in \mathrm{Img}\,(||)$.

Define:

- $x^{\pm} := \{a \in \mathcal{A} : |a| \leq x\}$, the ball, on $\mathbb{R}$ the interval $[-x, x]$.

An expression carrying signs $\pm$, each chosen independently, stands for the interval of $\mathcal{A}$ between the least and the largest of the values it takes: for $a, b, c \geq 0$, $a \pm b \pm c$ is $[a - b - c, a + b + c]$.

Definition A.10 (Relation on approximation [to table])**.** A value approximates another when it is the other times a factor in one interval plus a term in a second. Let:

- $\mathcal{A}$, an algebraic structure;
- $\mathcal{I}_0 \subset \mathcal{A}$, an interval (Definition A.9);
- $\mathcal{I}_1 \subset \mathcal{A}$, an interval.

Define:

- $\mathcal{I}\,(\mathcal{I}_0, \mathcal{I}_1)$: $\mathcal{A}^2 \to \{0, 1\}$,

$$\forall a, b \in \mathcal{A}, a\ \mathcal{I}\,(\mathcal{I}_0, \mathcal{I}_1)\ b \iff \exists u_\circ, \zeta_\circ \in \mathcal{A}, u_\circ \in \mathcal{I}_0, \zeta_\circ \in \mathcal{I}_1 : a = b(1 + u_\circ) + \zeta_\circ.$$

```
def RelI {A : Type*} [Ring A] (I0 I1 : Set A) (a b : A) : Prop :=
  exists u in I0, exists zeta in I1, a = b * (1 + u) + zeta
```

Figure 20: The Lean declarations carrying Definition A.10: `RelI` (`Depth.lean`); Lean's symbols in ASCII.

Definition A.11 (Relation on the bound of the difference [to table])**.** A value is within a relative and an absolute bound of another when their difference is. Let:

- $\mathcal{A}$, an algebraic structure with its norm operator $||$;

- $u \in \mathrm{Img}\,(||)$;
- $\zeta \in \mathrm{Img}\,(||)$.

Define:

- $\mathcal{N}_{||}\,(u,\zeta) \;: \mathcal{A}^2 \to \{0,1\}$,

$$\forall a, b \in \mathcal{A}, a\ \mathcal{N}_{||}\,(u,\zeta)\ \ b \iff |a-b| \leq u|b| + \zeta.$$

When the context is clear, we omit the norm operator $||$.

A.4 The fast Fourier sampler

This subsection states formally the objects of Section 3.2, after [L1: FGdG+26, App. F.3], with vectors as rows.

Definition A.12 (The basis of a key, its lattice and its Gram matrix [to table])**.** A key's four polynomials are the rows of a basis, which generates a lattice and has a Gram matrix. Let:

- $n \geq 2$, a power of two;
- (f, g, F, G), four polynomials of $\mathbb{Z}[x]/(x^n+1)$;
- $s > 0$;
- $c \in \mathcal{R}_n^2$.

Define:

- $\mathcal{R}_n := \mathbb{R}[x]/(x^n+1)$ (Definition A.1);
- $B := \begin{pmatrix} g & -f \\ G & -F \end{pmatrix} \in \mathcal{R}_n^{2\times 2}$, the basis;
- $\Lambda(B) := \{(z_0, z_1)B : z_0, z_1 \in \mathbb{Z}[x]/(x^n+1)\} \subset \mathcal{R}_n^2$, the lattice of B [L1: FGdG+26, Def. 4];
- $D_{\Lambda(B),s,c} := D_{A,s,c}$ at $k := 2n$ and $A := \Lambda(B)$, $D_{A,s,c}$ that of Definition A.2, each pair of $\mathcal{R}_n^2$ read as its $2n$ coefficients in $\mathbb{R}^{2n}$, the discrete Gaussian over $\Lambda(B)$ [L1: FGdG+26, Def. 6];
- $\mathcal{G} \in \mathcal{R}_n^{2\times 2}$, the Gram matrix of B, with $\forall \psi \in \mathbb{C},\ \psi^n = -1 :\ \mathcal{G}(\psi) := B(\psi)B(\psi)^\dagger$, $B(\psi)^\dagger$ the conjugate transpose.

Definition A.13 (The center of a hashed message and its parts [to table])**.** The center is the hashed message in the coordinates of the basis, and the coefficients of its multiple by the modulus, divided by the modulus with remainder, define its integer part and its fractional part. Define:

- $q := 12289$, the modulus.

Let:

- $n \in \{512, 1024\}$;
- (f, g, F, G), a key of keygen (Algorithm 11), line 3;
- $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$, read as the polynomial $\sum_{i<n} \mathsf{h}(\mathsf{m})_{[i]} x^i \in \mathbb{Z}[x]/(x^n+1)$.

Define:

- $\mathcal{R}_n := \mathbb{R}[x]/(x^n+1)$ (Definition A.1);
- $B := \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}$ (Definition A.12);
- $t := (\mathsf{h}(\mathsf{m}), 0)\, B^{-1} \in \mathcal{R}_n^2$, the center;
- $(t_0, t_1) := t$, with $\forall \psi \in \mathbb{C},\ \psi^n = -1 :\ t_0(\psi) = \mathsf{h}(\mathsf{m})(\psi)\,(-F(\psi))\,(1/q)$, $t_1(\psi) = (-f(\psi))\,\mathsf{h}(\mathsf{m})(\psi)\,(-1/q)$ (Fact A.33, item 1; ffSampling$^{\mathcal{F}}$ (Algorithm 10), lines 17 and 19);
- $qt := (-\mathsf{h}(\mathsf{m})\,F,\ \mathsf{h}(\mathsf{m})\,f) \in (\mathbb{Z}[x]/(x^n+1))^2$ (center$_{\mathrm{frac}}$ (Algorithm 17), line 1);
- $qt_{\mathrm{frac}} = (qt_{\mathrm{frac},0}, qt_{\mathrm{frac},1}) \in (\mathbb{Z}[x]/(x^n+1))^2$, by $(qt_{\mathrm{frac},j})_{[i]} \in [-q/2, q/2)$ and $(qt_{\mathrm{frac},j})_{[i]} \equiv (qt_j)_{[i]} \pmod q$ for $j \in \{0,1\}$ and $i < n$ (line 4);
- $t_{\mathrm{int}} := (qt - qt_{\mathrm{frac}})/q \in (\mathbb{Z}[x]/(x^n+1))^2$, the integer part (line 5);
- $t_{\mathrm{frac}} := qt_{\mathrm{frac}}/q \in \mathcal{R}_n^2$, the fractional part (center$_{\mathrm{frac}}$ (Algorithm 17), the output over $\mathbb{R}$).

Definition A.14 (The Gram matrices Gram$_m$ [to table])**.** A Gram matrix of degree m is a self-adjoint 2×2 matrix $\mathcal{G}$ over $\mathcal{R}_m$ with $\forall \psi :\ \mathcal{G}(\psi)$ positive definite. Let:

- m, a power of two;

- $\psi \in \mathbb{C}$ with $\psi^m = -1$;
- $g_{00} \in \mathcal{R}_m$ with $g_{00} = \operatorname{conj} g_{00}$, $\mathcal{R}_m$ that of Definition A.1;
- $g_{11} \in \mathcal{R}_m$ with $g_{11} = \operatorname{conj} g_{11}$;
- $g_{01} \in \mathcal{R}_m$.

Define:

- $\mathcal{G} := \begin{pmatrix} g_{00} & g_{01} \\ \operatorname{conj} g_{01} & g_{11} \end{pmatrix}$;
- $\operatorname{Gram}_m := \{\mathcal{G} : \forall \psi :\ g_{00}(\psi) > 0,\ g_{00}(\psi) g_{11}(\psi) > |g_{01}(\psi)|^2\}$.

Definition A.15 (The split and the merge [to table])**.** The split takes a polynomial to its even and its odd part, and the merge takes the two parts back. Let:

- $m \geq 4$, a power of two;
- $a \in \mathcal{R}_m$;
- $b \in \mathcal{R}_m$;
- $(f_0, f_1) \in \mathcal{R}_{m/2}^2$;
- $(g_0, g_1) \in \mathcal{R}_{m/2}^2$.

Define:

- $a_0 := \sum_{i<m/2} a_{[2i]} x^i \in \mathcal{R}_{m/2}$, the even part of a;
- $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i \in \mathcal{R}_{m/2}$, the odd part of a;
- $V_m \colon \mathcal{R}_m \to \mathcal{R}_{m/2}^2$, $V_m(a) := (a_0, a_1)$ [L1: FGdG+26, App. F.3];
- $M_m \colon \mathcal{R}_m \to \mathcal{R}_{m/2}^{2\times 2}$, $M_m(a) := \begin{pmatrix} a_0 & a_1 \\ x a_1 & a_0 \end{pmatrix}$ [L1: FGdG+26, App. F.3];
- $\operatorname{split} \colon \mathcal{R}_m \to \mathcal{R}_{m/2}^2$, $\operatorname{split}(a) := V_m(a)$;
- $\operatorname{merge} \colon \mathcal{R}_{m/2}^2 \to \mathcal{R}_m$, $\operatorname{merge}(f_0, f_1) := f_0(x^2) + x f_1(x^2)$;
- $\langle a, b \rangle := \sum_{i<m} a_{[i]} b_{[i]}$, the coefficient inner product;
- $\langle (f_0, f_1), (g_0, g_1) \rangle := \langle f_0, g_0 \rangle + \langle f_1, g_1 \rangle$, its form on pairs.

Fact A.16 (Split and products [to table])**.** The split is an isometry of the coefficient inner product, and it takes the product by a to the matrix $M_m(a)$. Let:

- $m \geq 4$, a power of two;
- $a \in \mathcal{R}_m$;
- $b \in \mathcal{R}_m$.

Define:

- $V_m(a) := (a_0, a_1)$ for $a \in \mathcal{R}_m$, $m \geq 4$ (Definition A.15);
- $a_0 := \sum_{i<m/2} a_{[2i]} x^i$ and $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i$ (Definition A.15);
- $M_m(a) := \begin{pmatrix} a_0 & a_1 \\ x a_1 & a_0 \end{pmatrix}$ for $a \in \mathcal{R}_m$, $m \geq 4$ (Definition A.15);
- $\langle a, b \rangle := \sum_{i<m} a_{[i]} b_{[i]}$, the coefficient inner product (Definition A.15);
- $\langle (f_0, f_1), (g_0, g_1) \rangle := \langle f_0, g_0 \rangle + \langle f_1, g_1 \rangle$ (Definition A.15).

We have

1. $\langle V_m(a), V_m(b) \rangle = \langle a, b \rangle$ [L1: FGdG+26, App. F.3];
2. $V_m(ab) = V_m(b)\, M_m(a)$ [L1: FGdG+26, App. F.3].

The butterflies of one level. split (Algorithm 2), split_{sa} (Algorithm 3) and merge (Algorithm 4) are the butterflies of one level, called by ffsamp (Algorithm 6) and by the FFT; split_{sa} splits the diagonals, split the centers; Lemma G.17 bounds the computed split in the pair norm and Lemma G.18 the computed merge.

Definition A.17 (The $LDL^\dagger$ step [to table])**.** The $LDL^\dagger$ step of a self-adjoint 2×2 matrix computes its off-diagonal factor and its two diagonals. Let:

- $m \geq 2$, a power of two;
- $g_{00} \in \mathcal{R}_m$ with $g_{00} = \operatorname{conj} g_{00}$ and $\forall \psi \in \mathbb{C},\ \psi^m = -1 :\ g_{00}(\psi) > 0$;
- $g_{11} \in \mathcal{R}_m$ with $g_{11} = \operatorname{conj} g_{11}$;
- $g_{01} \in \mathcal{R}_m$.

Define:

- $\mathcal{G} := \begin{pmatrix} g_{00} & g_{01} \\ \operatorname{conj} g_{01} & g_{11} \end{pmatrix}$;
- $l_{10} \in \mathcal{R}_m$ with $\forall \psi \in \mathbb{C},\ \psi^m = -1 :\ l_{10}(\psi) := \operatorname{conj} g_{01}(\psi)/g_{00}(\psi)$;
- $d_{00} := g_{00}$;
- $d_{11} \in \mathcal{R}_m$ with $\forall \psi \in \mathbb{C},\ \psi^m = -1 :\ d_{11}(\psi) := g_{11}(\psi) - |g_{01}(\psi)|^2/g_{00}(\psi)$;
- $\mathrm{LDL}^\dagger(\mathcal{G}) := (l_{10}, d_{00}, d_{11})$.

The $LDL^\dagger$ step reproduces the Gram matrix. By Lemma D.4, $\forall \psi \in \mathbb{C},\ \psi^m = -1$: the values $l_{10}(\psi)$, $d_{00}(\psi)$ and $d_{11}(\psi)$ reproduce $\mathcal{G}(\psi)$.

Definition A.18 (Tree, subtrees and depth [to table])**.** A node of degree m holds a factor and two children, leaf diagonals at $m = 2$ and nodes of degree $m/2$ above. Let:

- $m = 2^k$, $k \geq 1$;
- $l_{10} \in \mathcal{R}_m$;
- A, a leaf diagonal in $(0, \infty)$ if $m = 2$, a node of degree $m/2$ if $m \geq 4$;
- B, a leaf diagonal in $(0, \infty)$ if $m = 2$, a node of degree $m/2$ if $m \geq 4$.

Define:

- $\mathrm{node}(l_{10};\ A, B)$, the node of degree m: the triple of l_{10} and its two children A, B, a leaf node at $m = 2$ with the leaf diagonals d_{00}, d_{11} as children and a non-leaf node at $m \geq 4$ (Figure 22);
- $\mathcal{T}_m$, the set of nodes of degree m.

Let:

- $T \in \mathcal{T}_m$;
- $\nu = \mathrm{node}(l_{10};\ A, B) \in \mathcal{T}_{m'}$, $m' \leq m$.

Define:

- $h := \log_2 m$;
- $L(\nu) := A$;
- $R(\nu) := B$;
- $\forall d \in \mathbb{R} :\ \mathrm{Sub}(d) := \{d\}$ and $\mathrm{Sub}(\nu) := \{\nu\} \cup \mathrm{Sub}(L(\nu)) \cup \mathrm{Sub}(R(\nu))$ (Figure 23);
- $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R} :\ \mathrm{depth}(d) := h$ and $\forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'} :\ \mathrm{depth}(T') := \log_2(m/m')$.

```
inductive FTree : Nat -> Type
  | base (d0 d1 : Real) (l10 : Complex) : FTree 0
  | node {k : Nat} (psi : Fin (2 ^ k) -> Complex) (l10 : SlotVec (k + 1)) (T0 T1 : FTree k) :
      FTree (k + 1)

abbrev SlotVec (k : Nat) := Fin (2 ^ k) -> Complex
```

Figure 21: The Lean declarations carrying Definition A.18: `FTree`, `SlotVec` (`TreeRec.lean`); Lean's symbols in ASCII.

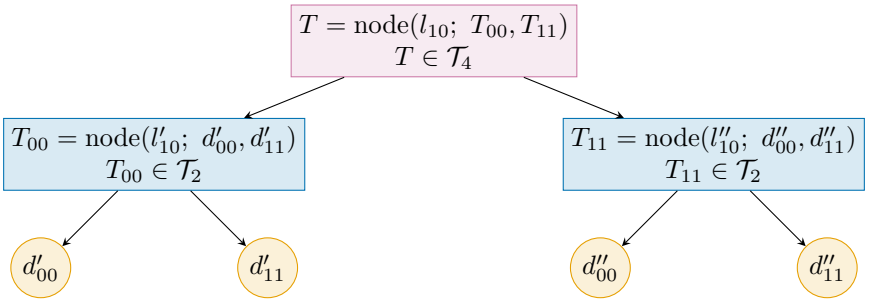


Figure 22: A tree $T \in \mathcal{T}_4$ (Definition A.18): a node as a rectangle with its constructor, a leaf diagonal as a circle, the left subtree on the left as in FHK+20, Figure 3.1; the sample positions (Definition A.19) read from right to left.

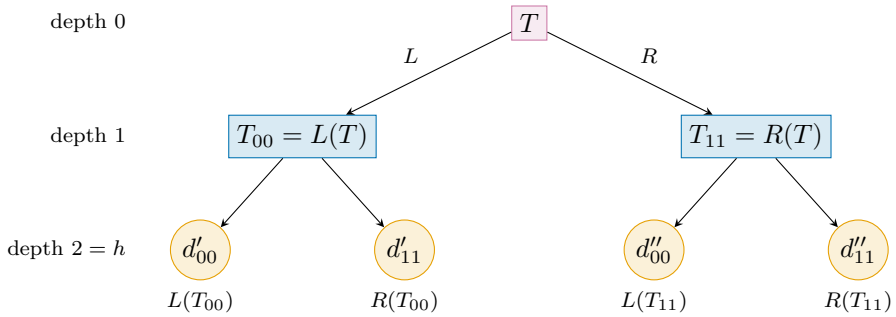


Figure 23: The subtrees of the tree of Figure 22: $\mathrm{Sub}(T) = \{T, T_{00}, T_{11}, d'_{00}, d'_{11}, d''_{00}, d''_{11}\}$ (Definition A.18, the subtrees); an edge is L or R, a row is a depth.

Definition A.19 (Sample positions and leaf diagonals [to table])**.** Each subtree of a tree holds an interval of sample positions, the right subtree's before the left's. Let:

- $T \in \mathcal{T}_m$;
- $\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}$, with $I(\nu) = \{a, \dots, a + 2m' - 1\}$;
- $d \in \mathrm{Sub}(T) \cap \mathbb{R}$.

Define:

- $N := 2m$;
- $I(T) := \{1, \dots, N\}$, ordered by $<$, the sampling order;
- $I(R(\nu)) := \{a, \dots, a + m' - 1\}$;
- $I(L(\nu)) := \{a + m', \dots, a + 2m' - 1\}$;
- $d_i := d$ for $i \in I(d)$, the leaf diagonal at the position i;
- $d_v := d_{2v-1}$ for $v \le m$, equal to d_{2v} (Figure 25).

```
def posNode (a m : Nat) : Finset Nat := Finset.Ico a (a + 2 * m)

def posR (a m : Nat) : Finset Nat := Finset.Ico a (a + m)

def posL (a m : Nat) : Finset Nat := Finset.Ico (a + m) (a + 2 * m)

theorem pos_split (a m : Nat) :
    posNode a m = posR a m cup posL a m /\ Disjoint (posR a m) (posL a m)
      /\ forall i in posR a m, forall j in posL a m, i < j := by

theorem pos_min (a : Nat) {m : Nat} (hm : 0 < m) :
    (posNode a m).min' (posNode_nonempty a hm) = a /\ (posR a m).min' (posR_nonempty a hm) = a
      /\ (posL a m).min' (posL_nonempty a hm) = a + m := by

noncomputable def rd {k : Nat} (T : FTree k) (i : Nat) : Real := T.weights.getD (i / 2) 0
```

Figure 24: The Lean declarations carrying Definition A.19: `posNode`, `posR`, `posL`, `pos_split`, `pos_min`, `FTree.rd` (`DefsFacts.lean`, `Ldl.lean`); with `FTree` of Figure 21; Lean's symbols in ASCII.

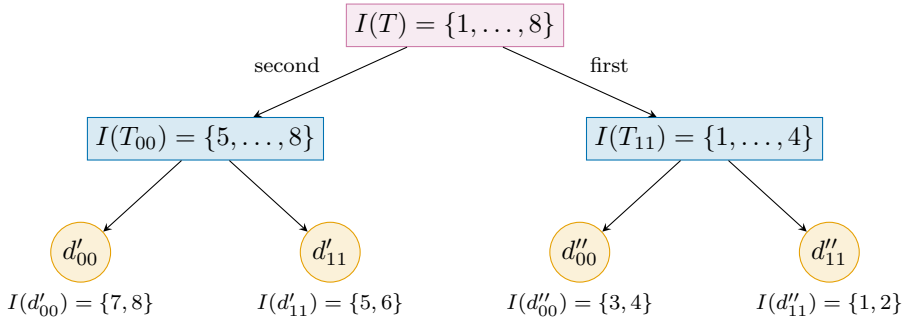


Figure 25: The sample positions on the tree of Figure 22, $N = 8$ (Definition A.19): at every node the right subtree's positions precede the left's; the leaf diagonals at the positions are $d_1 = d_2 = d''_{11}$, $d_3 = d_4 = d''_{00}$, $d_5 = d_6 = d'_{11}$, $d_7 = d_8 = d'_{00}$ (Definition A.19, the leaf diagonal).

Definition A.20 (The ffLDL† tree of a Gram matrix [to table])**.** The tree holds the factor of the $LDL^\dagger$ step at its root and, below it, the trees of the Gram matrices of the two diagonals' splits. Let:

- $m = 2^k$, $k \geq 1$;
- $\mathcal{G} \in \mathrm{Gram}_m$ (Definition A.14).

Define:

- $\mathcal{T}_m$, the set of nodes of degree m (Definition A.18);
- node, that of Definition A.18;
- $\mathrm{split}(a) := (a_0, a_1)$ for $a \in \mathcal{R}_m$, $m \geq 4$ (Definition A.15);
- $a_0 := \sum_{i<m/2} a_{[2i]} x^i$ and $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i$ (Definition A.15);
- $\mathrm{ffLDL}^\dagger(\mathcal{G}) \in \mathcal{T}_m$, by recursion on m through items 1 to 7 [L1: FGdG+26, Alg. 2].

Define, at $\mathcal{G}$ and m:

1. $(l_{10}, d_{00}, d_{11}) := \mathrm{LDL}^\dagger(\mathcal{G})$ (Definition A.17);
2. $\mathrm{ffLDL}^\dagger(\mathcal{G}) := \mathrm{node}(l_{10};\ d_{00}, d_{11})$ at $m = 2$;
3. $\mathcal{G}_{d_{00}} := \begin{pmatrix} d_0 & d_1 \\ \mathrm{conj}\, d_1 & d_0 \end{pmatrix}$ at $(d_0, d_1) := \mathrm{split}(d_{00})$ and $m \geq 4$;

4. $\mathcal{G}_{d_{11}} := \begin{pmatrix} d'_0 & d'_1 \\ \operatorname{conj} d'_1 & d'_0 \end{pmatrix}$ at $(d'_0, d'_1) := \operatorname{split}(d_{11})$ and $m \geq 4$;

5. $T_{00} := \mathrm{ffLDL}^\dagger(\mathcal{G}_{d_{00}})$ at $m \geq 4$;

6. $T_{11} := \mathrm{ffLDL}^\dagger(\mathcal{G}_{d_{11}})$ at $m \geq 4$;

7. $\mathrm{ffLDL}^\dagger(\mathcal{G}) := \operatorname{node}(l_{10};\ T_{00}, T_{11})$ at $m \geq 4$.

The recursion stays in the Gram matrices. Lemma D.6 shows that both diagonals at every node take positive values, so each $\mathcal{G}_{d_{00}}$ and $\mathcal{G}_{d_{11}}$ the recursion reaches is in $\mathrm{Gram}_{m/2}$.

Definition A.21 (The sampler ffSampling on a tree and its output measure [to table])**.** The sampler takes two integer samples at each leaf diagonal, the right subtree's before the left's, and shifts each center by the samples before it. Let:

- $m = 2^k$, $k \geq 1$;
- $T \in \mathcal{T}_m$ (Definition A.18);
- $t \in \mathcal{R}_m^2$;
- $s > 0$.

Define:

- The coordinates
  - $N := 2m$;
  - I and d_i, $i \leq N$, those of Definition A.19;
- The split
  - $\operatorname{split}(a) := (a_0, a_1)$ for $a \in \mathcal{R}_m$, $m \geq 4$ (Definition A.15);
  - $a_0 := \sum_{i<m/2} a_{[2i]} x^i$ and $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i$ (Definition A.15);
  - $\operatorname{merge}(f_0, f_1) := f_0(x^2) + x f_1(x^2)$ (Definition A.15);
- The discrete Gaussian
  - $D_{\mathbb{Z},\sigma,c}(z) := \rho_{\sigma,c}(z)/\rho_{\sigma,c}(\mathbb{Z})$ for $z \in \mathbb{Z}$ (Definition A.2);
- The samplers
  - $\operatorname{leaf}(d, t_d) := \hat{z}_d \in \mathbb{Z} + i\mathbb{Z}$ for $d \in \mathrm{Sub}(T) \cap \mathbb{R}$ with $I(d) = \{j, j+1\}$ and $t_d \in \mathbb{C}$, through items 1 to 4;
  - $\mathrm{ffSampling}(t_\nu, \nu) := \hat{z}_\nu \in (\mathbb{Z}[x]/(x^{m'}+1))^2$ for $\nu = \operatorname{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}$ and $t_\nu \in \mathcal{R}_{m'}^2$, by recursion on m' through items 6 to 20, each sample taken at the parameters the samples before it fix [L1: FGdG+26, Alg. 3];
- The centers and the samples
  - $z := (z_i)_{i \leq N} \in \mathbb{Z}^N$, the samples of $\mathrm{ffSampling}(t, T)$;
- The probability measures
  - $Q_{T,t}(A) := \Pr[z \in A]$ for $A \subseteq \mathbb{Z}^N$, the output measure of $\mathrm{ffSampling}(t, T)$.

Define, at d, j and t_d of leaf, and at ν, m' and t_ν of ffSampling:

1. $(\sigma_j, \sigma_{j+1}) := (s/\sqrt{d_j},\ s/\sqrt{d_{j+1}})$;

2. $(c_j, c_{j+1}) := (\operatorname{Re} t_d,\ \operatorname{Im} t_d)$;

3. $z_j \leftarrow D_{\mathbb{Z},\sigma_j,c_j}$, then $z_{j+1} \leftarrow D_{\mathbb{Z},\sigma_{j+1},c_{j+1}}$;

4. $\hat{z}_d := z_j + i z_{j+1}$;

5. $t_T := t$;

6. $(t_0, t_1) := t_\nu$;

7. $t_{T_{11}} := t_1$ at $m' = 2$;

8. $\hat{z}_{T_{11}} := \operatorname{leaf}(T_{11}, t_{T_{11}})$ at $m' = 2$;

9. $tb_0 := t_0 + (t_1 - \hat{z}_{T_{11}})\, l_{10}$ at $m' = 2$;
10. $t_{T_{00}} := tb_0$ at $m' = 2$;
11. $\hat{z}_{T_{00}} := \mathrm{leaf}(T_{00}, t_{T_{00}})$ at $m' = 2$;
12. $\hat{z}_\nu := (\hat{z}_{T_{00}}, \hat{z}_{T_{11}})$ at $m' = 2$;
13. $t_{T_{11}} := \mathrm{split}(t_1)$ at $m' \geq 4$;
14. $\hat{z}_{T_{11}} := \mathrm{ffSampling}(t_{T_{11}}, T_{11})$ at $m' \geq 4$;
15. $z_1 := \mathrm{merge}(\hat{z}_{T_{11}})$ at $m' \geq 4$;
16. $tb_0 := t_0 + (t_1 - z_1)\, l_{10}$ at $m' \geq 4$;
17. $t_{T_{00}} := \mathrm{split}(tb_0)$ at $m' \geq 4$;
18. $\hat{z}_{T_{00}} := \mathrm{ffSampling}(t_{T_{00}}, T_{00})$ at $m' \geq 4$;
19. $z_0 := \mathrm{merge}(\hat{z}_{T_{00}})$ at $m' \geq 4$;
20. $\hat{z}_\nu := (z_0, z_1)$ at $m' \geq 4$.

```
noncomputable def centers : {k : Nat} -> FTree k -> SlotVec k x SlotVec k -> SlotVec k x
    SlotVec k
    -> List Complex
  | _, base _ _ l10, t, z => [t.2 0, t.1 0 + (t.2 0 - z.2 0) * l10]
  | _, node psi l10 T0 T1, t, z =>
      T1.centers (splitV psi t.2) (splitV psi z.2)
        ++ T0.centers (splitV psi (t.1 + (t.2 - z.2) * l10)) (splitV psi z.1)

noncomputable def splitV {k : Nat} (psi : Fin (2 ^ k) -> Complex) (x : SlotVec (k + 1)) :
    SlotVec k x SlotVec k :=
  (fun j => (x (pr k (j, 0)) + x (pr k (j, 1))) / 2,
   fun j => (x (pr k (j, 0)) - x (pr k (j, 1))) / 2 * conj (psi j))
```

Figure 26: The Lean declarations carrying Definition A.21: `FTree.centers`, `splitV` (`TreeRec.lean`); with `SlotVec`, `FTree` of Figure 21; Lean's symbols in ASCII.

The output measure is a lattice Gaussian. On the tree of a basis's Gram matrix the output measure is a lattice Gaussian over the leaves' normalizers. Its proof in [L1: FGdG+26, App. F.3] uses the two identities of Fact A.16, items 1 and 2.

Fact A.22 (Output probability of the sampler on a tree [to table])**.** On the ffLDL† tree of a basis's Gram matrix, the sampler outputs each pair with the Gaussian weight of its lattice point, divided by the normalizers of its samples. Let:

- $n \geq 2$, a power of two;
- (f, g, F, G), four polynomials of $\mathbb{Z}[x]/(x^n + 1)$ with $\forall \psi \in \mathbb{C},\ \psi^n = -1 :\ (fG - gF)(\psi) \neq 0$;
- $t \in \mathcal{R}_n^2$;
- $\epsilon \in (0, 1)$.

Define:

- $B := \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}$ (Definition A.12);
- $\mathcal{G}$, the Gram matrix of B, with $\forall \psi \in \mathbb{C},\ \psi^n = -1 :\ \mathcal{G}(\psi) := B(\psi)B(\psi)^\dagger$ (Definition A.12);
- $\rho_s := \rho_{s,0}$ (Definition A.2);

- $\eta_\epsilon(\mathbb{Z}^n) := \inf\{s' > 0 : \rho_{1/s'}(\mathbb{Z}^n \setminus \{0\}) \le \epsilon\}$, the smoothing parameter of $\mathbb{Z}^n$ [L1: FGdG+26, Section 2.3];
- $\|B\|_{\mathrm{GS}}$, the largest norm of the Gram–Schmidt vectors of the $2n$ rows $x^j(g, -f)$, $j < n$, then $x^j(G, -F)$, $j < n$, each read as its $2n$ coefficients [L1: FGdG+26, Def. 7].

Let:

- $s \ge \eta_\epsilon(\mathbb{Z}^n)\, \|B\|_{\mathrm{GS}}$.

Define:

- $N := 2n$;
- $T := \mathrm{ffLDL}^\dagger(\mathcal{G})$ (Definition A.20);
- $\mathrm{ffSampling}(t, T)$ and σ_i, $i \le N$, those of Definition A.21 at (T, t, s);
- $\forall z^* \in \mathbb{Z}^N :\ \hat{z}(z^*) := \mathrm{ffSampling}(t, T) \in (\mathbb{Z}[x]/(x^n + 1))^2$ (Definition A.21 at $z := z^*$);
- $\forall i \le N\ \forall z^* \in \mathbb{Z}^N :\ c_i(z^*_{<i})$, that of Definition A.21 at $z_{<i} := z^*_{<i}$.

Then [L1: FGdG+26, Lem. 22]

$$\forall z^* \in \mathbb{Z}^N :\quad \Pr[\mathrm{ffSampling}(t, T) = \hat{z}(z^*)] = \rho_s((t - \hat{z}(z^*))B) \prod_{i \le N} \rho_{\sigma_i, c_i(z^*_{<i})}(\mathbb{Z})^{-1}.$$

One item per step of the imported algorithm. Each item of Definitions A.20 and A.21 is one step of the algorithm the definition imports, over $\mathbb{R}$ and at the values $f(\psi)$, with the symbols the statements use.

Definition A.23 (The sampler ffsamp on a Gram matrix and its output measure [to table])**.** The sampler on a Gram matrix takes the $LDL^\dagger$ step at each node it reaches, samples the second diagonal's Gram matrix before the first's, and takes two integer samples at each leaf diagonal. Let:

- $m = 2^k$, $k \ge 1$;
- $\mathcal{G} \in \mathrm{Gram}_m$ (Definition A.14);
- $t \in \mathcal{R}_m^2$;
- $s > 0$.

Define:

- The coordinates
  - $N := 2m$;
- The Gram matrix entries
  - g_{00}, g_{01} and g_{11}, the entries of $\mathcal{G}$ (Definition A.17);
- The decomposition
  - $\mathrm{LDL}^\dagger(\mathcal{G}) := (l_{10}, d_{00}, d_{11})$ and $d_{00} := g_{00}$ (Definition A.17);
  - $l_{10}(\psi) := \mathrm{conj}\, g_{01}(\psi)/g_{00}(\psi)$ for $\psi^m = -1$ (Definition A.17);
  - $d_{11}(\psi) := g_{11}(\psi) - |g_{01}(\psi)|^2/g_{00}(\psi)$ for $\psi^m = -1$ (Definition A.17);
- The split
  - $\mathrm{split}(a) := (a_0, a_1)$ for $a \in \mathcal{R}_m$, $m \ge 4$ (Definition A.15);
  - $a_0 := \sum_{i < m/2} a_{[2i]} x^i$ and $a_1 := \sum_{i < m/2} a_{[2i+1]} x^i$ (Definition A.15);
  - $\mathrm{merge}(f_0, f_1) := f_0(x^2) + x f_1(x^2)$ (Definition A.15);
  - $\mathcal{G}_d := \begin{pmatrix} d_0 & d_1 \\ \mathrm{conj}\, d_1 & d_0 \end{pmatrix}$ at $(d_0, d_1) := \mathrm{split}(d)$, for $d \in \mathcal{R}_{m'}$ and $m' \ge 4$ a power of two;
- The discrete Gaussian
  - $D_{\mathbb{Z},\sigma,c}(z) := \rho_{\sigma,c}(z)/\rho_{\sigma,c}(\mathbb{Z})$ for $z \in \mathbb{Z}$ (Definition A.2);
- The samplers
  - $\mathrm{leaf}_s(d, c) := y' + iy'' \in \mathbb{Z} + i\mathbb{Z}$ for $d > 0$ and $c \in \mathbb{C}$, with the sample $y' \leftarrow D_{\mathbb{Z}, s/\sqrt{d}, \mathrm{Re}\, c}$ taken before the sample $y'' \leftarrow D_{\mathbb{Z}, s/\sqrt{d}, \mathrm{Im}\, c}$;
  - $\mathrm{ffsamp}(t', \mathcal{G}') \in (\mathbb{Z}[x]/(x^{m'} + 1))^2$ for $m' = 2^{k'}$ with $1 \le k' \le k$, $\mathcal{G}' \in \mathrm{Gram}_{m'}$ and $t' = (t'_0, t'_1) \in \mathcal{R}_{m'}^2$, by recursion on m' at $(l_{10}, d_{00}, d_{11}) := \mathrm{LDL}^\dagger(\mathcal{G}')$, each sample taken at the parameters the samples before it fix (ffsamp (Algorithm 6) at `root` $= 0$ and

deepest (Algorithm 7) over $\mathbb{R}$, at `INV_SIGMA` $:= 1/s$):

$$
\begin{aligned}
m' = 2 :&\\
&y_1 := \mathrm{leaf}_s(d_{11}, t'_1),\\
&y_0 := \mathrm{leaf}_s(d_{00},\ t'_0 + (t'_1 - y_1)\, l_{10}),\\
&\mathrm{ffsamp}(t', \mathcal{G}') := (y_0, y_1);\\
m' \geq 4 :&\\
&y_1 := \mathrm{merge}(\mathrm{ffsamp}(\mathrm{split}(t'_1), \mathcal{G}_{d_{11}})),\\
&y_0 := \mathrm{merge}(\mathrm{ffsamp}(\mathrm{split}(t'_0 + (t'_1 - y_1)\, l_{10}), \mathcal{G}_{d_{00}})),\\
&\mathrm{ffsamp}(t', \mathcal{G}') := (y_0, y_1);
\end{aligned}
$$

- The centers and the samples
  - $z := (z_i)_{i \leq N} \in \mathbb{Z}^N$, the samples of $\mathrm{ffsamp}(t, \mathcal{G})$ in the order they are taken;
- The probability measures
  - $Q'_{\mathcal{G},t}(A) := \Pr[z \in A]$ for $A \subseteq \mathbb{Z}^N$, the output measure of $\mathrm{ffsamp}(t, \mathcal{G})$.

```
noncomputable def fusedProb (s : Real) (psis : (k : Nat) -> Fin (2 ^ k) -> Complex) :
    {k : Nat} -> RSlot (k + 1) -> SlotVec k x SlotVec k -> SlotVec k x SlotVec k -> Real
  | 0, d, t, z =>
      rho (s / Real.sqrt (hmPairs d 0)) ((t.2 0).re - (z.2 0).re)
          / rhoZ (s / Real.sqrt (hmPairs d 0)) (t.2 0).re
        * (rho (s / Real.sqrt (hmPairs d 0)) ((t.2 0).im - (z.2 0).im)
          / rhoZ (s / Real.sqrt (hmPairs d 0)) (t.2 0).im)
        * (rho (s / Real.sqrt (amPairs d 0))
              ((t.1 0 + (t.2 0 - z.2 0) * ldlFactor (psis 0) d 0).re - (z.1 0).re)
              / rhoZ (s / Real.sqrt (amPairs d 0))
                (t.1 0 + (t.2 0 - z.2 0) * ldlFactor (psis 0) d 0).re
            * (rho (s / Real.sqrt (amPairs d 0))
              ((t.1 0 + (t.2 0 - z.2 0) * ldlFactor (psis 0) d 0).im - (z.1 0).im)
              / rhoZ (s / Real.sqrt (amPairs d 0))
                (t.1 0 + (t.2 0 - z.2 0) * ldlFactor (psis 0) d 0).im))
  | k + 1, d, t, z =>
      fusedProb s psis (hmPairs d) (splitV (psis k) t.2) (splitV (psis k) z.2)
        * fusedProb s psis (amPairs d)
            (splitV (psis k) (t.1 + (t.2 - z.2) * ldlFactor (psis (k + 1)) d)) (splitV (psis k)
               z.1)

noncomputable def rhoZ (s c : Real) : Real := Sum' z : Int, rho s (z - c)

abbrev RSlot (k : Nat) := Fin (2 ^ k) -> Real

noncomputable def amPairs {k : Nat} (d : RSlot (k + 1)) : RSlot k :=
  fun j => (d (pr k (j, 0)) + d (pr k (j, 1))) / 2

noncomputable def hmPairs {k : Nat} (d : RSlot (k + 1)) : RSlot k :=
  fun j => 2 * d (pr k (j, 0)) * d (pr k (j, 1)) / (d (pr k (j, 0)) + d (pr k (j, 1)))

noncomputable def ldlFactor {k : Nat} (psi : Fin (2 ^ k) -> Complex) (d : RSlot (k + 1)) :
    SlotVec k :=
  fun j => conj (((d (pr k (j, 0)) - d (pr k (j, 1)) : Real) : Complex) / 2 * conj (psi j))
    / ((amPairs d j : Real) : Complex)

noncomputable def rho (sigma y : Real) : Real := Real.exp (-(y ^ 2) / (2 * sigma ^ 2))
```

Figure 27: The Lean declarations carrying Definition A.23: `fusedProb`, `rhoZ`, `RSlot`, `amPairs`, `hmPairs`, `ldlFactor`, `rho` (`Bridge.lean`, `Fused.lean`, `Leafrange.lean`, `Sampler.lean`); with `SlotVec` of Figure 21; with `splitV` of Figure 26; Lean's symbols in ASCII.

The sampler on a Gram matrix stays in the Gram matrices. Lemma D.6 shows that each $\mathcal{G}_d$ the recursion reaches is in $\mathrm{Gram}_{m'/2}$, as for the ffLDL† tree.

Definition A.24 (The base sampler's probability measure on $\mathbb{Z}$ in a realization [to table])**.** Executed in a realization, the base sampler defines a probability measure on the integers at each center and each standard deviation. Let:

- $\mathcal{F}$, a realization (Definition A.4);
- $\texttt{isigma} \in \mathcal{F}$ with $\texttt{isigma} > 0$;
- $c \in \mathcal{F}$.

Define:

- $\sigma := 1/\texttt{isigma}$;
- $B^{\mathcal{F}}_{\sigma,c}(A) := \Pr[\mathrm{SamplerZ}(c, \texttt{isigma}) \in A]$ for $A \subseteq \mathbb{Z}$, over the samples of SamplerZ (Algorithm 8) and BerExp (Algorithm 9), SamplerZ executed in $\mathcal{F}$ at $\mu := c$ [L1: FHK+20, Alg. 15 at $\sigma' := \sigma$, $\mu := c$].

The base sampler, the last routine of the sampler. The last routine of the sampler is the base sampler: ffsamp (Algorithm 6) calls deepest (Algorithm 7), which calls SamplerZ (Algorithm 8) at each of the N sample positions (lines 1 to 18), and SamplerZ calls BerExp (Algorithm 9) at each trial. The code's $dss = 1/(2\sigma^2)$ [L0: `sign_sampler.c:923`] [L0: `fxp/sign_fxsampler.c:191`] is the convention of the Gaussian function of Definition A.2.

The base sampler in the code's names. SamplerZ (Algorithm 8) is `sampler_next` [L0: `sign_sampler.c:916-968`] [L0: `fxp/sign_fxsampler.c:183-216`], with inputs the center μ and the inverse standard deviation $\texttt{isigma} = 1/\sigma$, both values of $\mathcal{F}$, and with $\sigma_0 = 1.8205$ the proposal's standard deviation [L0: `sign_sampler.c:18-19`] [L0: `fxp/fxp_consts.h:2089`] and $\sigma_{\min}$ the code's table value [L0: `sign_sampler.c:21-30`] [L0: `fxp/fxp_consts.h:2073`], in the code's names, the same procedure in both signers: Algorithms 8 and 9. Both name every value the statements bound, over $\mathbb{R}$ and in $\mathcal{F}$: the exponent's argument at lines 1 to 15 of SamplerZ (Algorithm 8), its split at lines 1 to 12 of BerExp (Algorithm 9).

What the fixed-point base sampler changes. The table, the bit, the candidate and the acceptance's integer code are the reference's, verbatim, in `fxp/`, the rejection at $si \geq 64$ apart (Definition I.20, item 1); the arithmetic of r, dss, ccs and x is the signer's: Lemma I.58 for `fxp/` (Appendix I).

Definition A.25 (The two probability measures [to table])**.** The signer in the realization and in real arithmetic defines two probability measures on the samples. Let:

- $n \in \{512, 1024\}$;
- (f, g, F, G), a key of keygen (Algorithm 11), line 3;
- $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$, a hashed message, the input of ffSampling$^{\mathcal{F}}$ (Algorithm 10);
- $t \in \mathcal{R}_n \times \mathcal{R}_n$, a center;
- $i \in \{1, \ldots, 2n\}$, a sample position in the sampling order (Definition A.19), the i-th leaf sample of line 24 of ffSampling$^{\mathcal{F}}$ (Algorithm 10).

Define:

- The signer's words and parameters
  - $N := 2n$;
  - $\sigma_{\min}$, the number of the signer's stored word at $\log_2 n$: in the fixed-point signer, `FXP_SIGMA_MIN` of `fxp/` [L0: `fxp/fxp_consts.h:2073-2084`] in the realization of Definition A.4, item 8;
  - $s := 1.17\sqrt{q}\,\sigma_{\min}$, the standard deviation parameter of the signer;
- The lattice
  - $B := \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}$ (Definition A.12);

  - $\Lambda := \Lambda(B)$ (Definition A.12);
  - $D_{\Lambda,s,tB} := D_{\Lambda(B),s,c}$ (Definition A.12 at $c := tB$);
- The centers
  - $(\mathsf{h}(\mathsf{m}), 0)B^{-1}$, that of Definition A.13 at (f, g, F, G) and $\mathsf{h}(\mathsf{m})$;
  - $t_{\text{frac}} := qt_{\text{frac}}/q$, with qt_{frac} that of Definition A.13 at (f, g, F, G) and $\mathsf{h}(\mathsf{m})$;
- The samplers
  - $\text{ffSampling}^{\mathcal{F}}(B, s, t)$, $\text{ffSampling}^{\mathcal{F}}$ (Algorithm 10) (Section 3.2) in the arithmetic $\mathcal{F}$ of Definition A.4, at (B, s, t);
  - $\text{ffSampling}^{\mathcal{F}} := \text{ffSampling}^{\mathcal{F}}(B, s, t)$ (Definition A.4; line 17 of $\text{ffSampling}^{\mathcal{F}}$ (Algorithm 10) at $t := (\mathsf{h}(\mathsf{m}), 0)B^{-1}$, or line 7 at $t := t_{\text{frac}}$);
  - $\text{ffSampling}^{\mathbb{R}} := \text{ffSampling}^{\mathbb{R}}(B, s, t)$ (Definition A.4);
- The probability measures
  - $P(A) := \Pr[z \in A]$ for every $A \subseteq \mathbb{Z}^N$, z the output of $\text{ffSampling}^{\mathcal{F}}$;
  - $Q(A) := \Pr[z \in A]$ for every $A \subseteq \mathbb{Z}^N$, z the output of $\text{ffSampling}^{\mathbb{R}}$;
- The leaf parameters
  - $z_{<i} := (z_1, \ldots, z_{i-1})$;
  - $(\mu, \texttt{isigma})$, the arguments of the i-th call $\text{SamplerZ}(\mu, \texttt{isigma})$ of $\text{ffSampling}^{\mathcal{F}}$;
  - $\widetilde{t}_i := \mu$ at that call of $\text{ffSampling}^{\mathcal{F}}$ (lines 1 to 18 of deepest (Algorithm 7) in $\mathcal{F}$);
  - $\widetilde{\sigma}_i := 1/\texttt{isigma}$ at that call of $\text{ffSampling}^{\mathcal{F}}$;
  - t_i, the center of the i-th leaf sample of $\text{ffSampling}^{\mathbb{R}}$ (the shaded lines 1 to 18 of deepest (Algorithm 7) over $\mathbb{R}$);
  - σ_i, the standard deviation of that sample.

A center $c \in \{t, t_{\text{frac}}\}$ of the statements below names the rule by which the signer forms its center from $\mathsf{h}(\mathsf{m})$: t at line 17 or t_{frac} at line 7 of $\text{ffSampling}^{\mathcal{F}}$ (Algorithm 10). The leaf parameters $\widetilde{t}_i$, $\widetilde{\sigma}_i$, t_i and σ_i are functions of $z_{<i}$. We have

1. $\forall z_{<i}\ \forall x \in \mathbb{Z}:\ P(z_i = x \mid z_{<i}) = \Pr[\text{SamplerZ}(\widetilde{t}_i, 1/\widetilde{\sigma}_i) = x]$ in $\mathcal{F}$;
2. $\forall z_{<i}\ \forall x \in \mathbb{Z}:\ Q(z_i = x \mid z_{<i}) = D_{\mathbb{Z},\sigma_i,t_i}(x)$ (Definition A.2).

$\text{ffSampling}^{\mathbb{R}}$ is $\text{ffSampling}^{\mathcal{F}}$ over $\mathbb{R}$ with the leaf samples taken from $D_{\mathbb{Z},\sigma_i,t_i}$ (deepest (Algorithm 7), the shaded lines 1 to 18), not the base sampler executed in exact arithmetic, whose output measure is P_0 of Lemma G.64.

```
noncomputable def chainMeasure {N : Nat} (B : Fin N -> (Fin N -> Int) -> Int -> Real) :
    (Fin N -> Int) -> Real :=
  fun z => Prod i, B i z (z i)
```

Figure 28: The Lean declarations carrying Definition A.25: `chainMeasure` (`LeafTail.lean`); Lean's symbols in ASCII.

The measure Q and the sampler on a tree. Fact G.12 relates Q to the output measure of the sampler on the $\text{ffLDL}^{\dagger}$ tree of the key's Gram matrix (Definitions A.20 and A.21). Fact A.22 states that measure as a lattice Gaussian over the leaves' normalizers.

A.5 The objects of the main theorem

Structure. This subsection states formally the objects of Section 3.3.

Definition A.26 (The tail-cut event and its sub-events [to table])**.** The tail-cut event S holds the samples within τ standard deviations of their centers at every leaf; a sub-event $S' \subseteq S$ has its own prefix sets and classes. Let:

- $C_i(z_{<i}) \subseteq \{\, z_i \in \mathbb{Z} : |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$, $i \le N$, the fringe sets, empty unless the signer's base sampler names them.

Define:

- $S := \{\, z \in \mathbb{Z}^N : \forall i \le N\ |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$;
- $S^c := \mathbb{Z}^N \setminus S$, the tail;
- $\mathcal{K}(z) := \{\, i \le N : z_i \in C_i(z_{<i}) \,\}$;
- $\forall k \le N :\ S_k := \{\, z \in S : |\mathcal{K}(z)| = k \,\}$;
- $\forall A \subseteq \mathbb{Z}^N :\ P_S(A) := P(A \cap S)/P(S)$;
- $Q_S(A) := Q(A \cap S)/Q(S)$.

Let:

- $S' \subseteq S$, $S' := S$ where a statement names no other.

Define:

- $S'^c := \mathbb{Z}^N \setminus S'$;
- $\forall i \le N :\ S'_{<i} := \{\, z_{<i} : z \in S' \,\}$, the prefix sets of S';
- $S_{<i} := S'_{<i}$ at $S' := S$;
- $\forall k \le N :\ S'_k := \{\, z \in S' : |\mathcal{K}(z)| = k \,\}$;
- $P_{S'_0}(A) := P(A \cap S'_0)/P(S'_0)$;
- $Q_{S'_0}(A) := Q(A \cap S'_0)/Q(S'_0)$. [derived]

Definition A.27 (The leaf perturbations of one signature [to table])**.** At each leaf the arithmetic perturbs the standard deviation by a factor and the center by a shift. Define:

- $\delta_i(z_{<i})$ for $i \le N$ and every $z_{<i}$, by $\widetilde{\sigma}_i(z_{<i}) =: \sigma_i(z_{<i})\,(1 + \delta_i(z_{<i}))$;
- $\Delta_i(z_{<i}) := \widetilde{t}_i(z_{<i}) - t_i(z_{<i})$ for $i \le N$ and every $z_{<i}$;
- $\bar{W}_{S'} := \sup_{z \in S'} \sum_{i \le N} \Delta_i(z_{<i})^2/\sigma_i(z_{<i})^2$;
- $\bar{W}_S := \bar{W}_{S'}$ at $S' := S$.

Let:

- $\bar{\delta} \ge \max_{i \le N} \sup_{z_{<i} \in S'_{<i}} |\delta_i(z_{<i})|$. [derived]

Definition A.28 (A leaf's computed and ideal probability measures on $\mathcal{Z}_i$ [to table])**.** At a leaf the base sampler in $\mathcal{F}$ defines a computed probability measure, compared with the discrete Gaussian at the computed parameters on the set $\mathcal{Z}_i$. Define:

- The leaf measures
  - $D_{\mathbb{Z},\sigma,c}(z) := \rho_{\sigma,c}(z)/\rho_{\sigma,c}(\mathbb{Z})$ for $z \in \mathbb{Z}$ (Definition A.2);
  - $B^{\mathcal{F}}_{\sigma,c}(A) := \Pr[\mathrm{SamplerZ}(c, 1/\sigma) \in A]$ for $A \subseteq \mathbb{Z}$, $\mathcal{F}$ that of $\mathrm{ffSampling}^{\mathcal{F}}$ (Definition A.24);
  - $\widetilde{B}_i := B^{\mathcal{F}}_{\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}$ for $i \le N$ and every $z_{<i}$, the conditional measure $A \mapsto P(z_i \in A \mid z_{<i})$ on $A \subseteq \mathbb{Z}$ (Definition A.25, item 1);
  - $\widetilde{D}_i := D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$;
  - $P_D(z) := \prod_{i \le N} D_{\mathbb{Z},\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}(z_i)$ for $z \in \mathbb{Z}^N$;
- The tail cut
  - $\mathcal{Z}_i := \left(|\cdot - \widetilde{t}_i|/\widetilde{\sigma}_i\right)^{-1}([0,\tau]) \subseteq \mathbb{Z}$ for $i \le N$ and every $z_{<i}$;
- The Rényi divergence
  - $R^{\mathcal{Y}}_a(\mu \,\|\, \nu) := \left(\sum_{z \in \mathcal{Y}} \mu(z)^a\, \nu(z)^{1-a}\right)^{1/(a-1)}$ for probability measures μ, ν on a countable set X, $a > 1$ and $\mathcal{Y} \subseteq X$, the Rényi divergence on $\mathcal{Y}$;
- The moments
  - $\bar{\rho}_B := \max_{i \le N}\ \sup_{z_{<i} \in S_{<i}} R^{\mathcal{Z}_i \setminus C_i}_{2\alpha}(\widetilde{B}_i \,\|\, \widetilde{D}_i)$;
- The fringe sets
  - $\sup \emptyset := 0$;
  - $\bar{U} := \max_{i \le N}\ \sup_{z_{<i} \in S_{<i}}\ \sup_{z_i \in C_i} \widetilde{B}_i(z_i)/\widetilde{D}_i(z_i)$;
  - $\bar{p}_C := \max_{i \le N}\ \sup_{z_{<i} \in S_{<i}} \widetilde{B}_i(C_i)$;
  - $\kappa_C := \bar{U}^{\alpha}\, \bar{\rho}_B^{-\alpha_L/2}$.

Let:

- $\epsilon_{\mathrm{hi}} \geq 0$ with $\forall i \leq N\ \forall z_{<i}\ \forall z_i \notin C_i :\ \widetilde{B}_i(z_i) \leq (1+\epsilon_{\mathrm{hi}})\,\widetilde{D}_i(z_i)$. [derived]

```
noncomputable def renyiPowZ_set (alpha : Real) (F : Set Int) (B D : Int -> Real) : Real :=
  Sum' z, F.indicator (fun z => B z ^ alpha * D z ^ (1 - alpha)) z

noncomputable def renyiDivZ_set (alpha : Real) (F : Set Int) (B D : Int -> Real) : Real :=
  renyiPowZ_set alpha F B D ^ (1 / (alpha - 1))
```

Figure 29: The Lean declarations carrying Definition A.28: `renyiPowZ_set`, `renyiDivZ_set` (`Renyi.lean`); Lean's symbols in ASCII.

Definition A.29 (The normalizer ratio at a leaf [to table])**.** At a leaf the three normalizers, of the computed, the ideal and the mixed Gaussian, form a ratio $\Phi_{\alpha_L,i}$. Define:

- $\bar{\delta} \geq \max_{i\leq N} \sup_{z_{<i}\in S'_{<i}} |\delta_i(z_{<i})|$ (Definition A.27), with $(1+\bar{\delta})^2 < \alpha_L/(\alpha_L-1)$;
- $\rho_{s,c}(\mathbb{Z}) := \sum_{x\in\mathbb{Z}} \rho_{s,c}(x)$ (Definition A.2);
- $d(s,c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\,s) - 1$ for $s>0$ and $c\in\mathbb{R}$;
- $\theta_{\alpha_L}(\delta) := 1/(\alpha_L + (1-\alpha_L)(1+\delta)^2)$ for $|\delta| \leq \bar{\delta}$;
- $s''_i := \sigma_i(1+\delta_i)\,\theta_{\alpha_L}(\delta_i)^{1/2}$ for $i\leq N$ and every $z_{<i}\in S'_{<i}$;
- $m_i := t_i + \alpha_L\theta_{\alpha_L}(\delta_i)\,\Delta_i$;
- $\Phi_{\alpha_L,i} := (1+d(s''_i,m_i))\left(1+d(\widetilde{\sigma}_i,\widetilde{t}_i)\right)^{-\alpha_L}(1+d(\sigma_i,t_i))^{\alpha_L-1}$.

Let:

- $\bar{\phi} \geq \max_{i\leq N}\ \sup_{z_{<i}\in S'_{<i}} |\ln \Phi_{\alpha_L,i}(z_{<i})|$. [derived]

```
noncomputable def dev (s c : Real) : Real := rhoZ s c / (Real.sqrt (2 * Real.pi) * s) - 1
```

Figure 30: The Lean declarations carrying Definition A.29: `dev` (`Bridge.lean`); with `rhoZ` of Figure 27; Lean's symbols in ASCII.

Definition A.30 (The divergence factor R [to table])**.** The bound of the main theorem carries the factor R, built from the leaf perturbations, the base sampler's moment and the normalizer ratio. Define:

- $\theta_{\alpha_L}(\delta) := 1/(\alpha_L + (1-\alpha_L)(1+\delta)^2)$.

Let:

- $N \in \mathbb{Z}_{>0}$;
- $\bar{\theta}_{\alpha_L} \geq 0$ with $\forall \delta > -1,\ |\delta|\leq\bar{\delta} :\ \theta_{\alpha_L}(\delta) \leq \bar{\theta}_{\alpha_L}$;
- $\bar{W}_{\alpha_L} > 0$ with $\forall \delta > -1,\ |\delta|\leq\bar{\delta} :\ \theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \leq \bar{W}_{\alpha_L}$.

Define:

- $R_B := \bar{\rho}_B^{\,\alpha_L N/(2(\alpha-1))}$;
- $R_\sigma := (e^{\bar{\phi}}\,\bar{W}_{\alpha_L})^{N/(2(\alpha-1))}$;
- $R_t := \exp\left(\alpha_L\,\bar{\theta}_{\alpha_L}\,\bar{W}_{S'}/2\right)$;
- $R := R_B R_\sigma R_t$. [derived]

```
noncomputable def factorR (N : Nat) (alpha rhoB phi Walpha theta WS : Real) : Real :=
  rhoB ^ ((2 * alpha - 1) * N / (2 * (alpha - 1))) * (Real.exp phi * Walpha) ^ ((N : Real) / (2
      * (alpha - 1)))
    * Real.exp ((2 * alpha - 1) * theta * WS / 2)
```

Figure 31: The Lean declarations carrying Definition A.30: `factorR` (`LeadingOrder.lean`); Lean's symbols in ASCII.

A.6 The tree

Structure. This subsection states formally the tree of a key of Section 3.2.

Fact A.31 (Counts of a tree [to table])**.** A tree of degree m has 2^k subtrees at depth k, and each node's positions split between its children. Let:

- $T \in \mathcal{T}_m$.

Define:

- $h := \log_2 m$;
- I, that of Definition A.19;
- L and R, with $L(\text{node}(l_{10};\ A, B)) = A$ and $R(\text{node}(l_{10};\ A, B)) = B$ (Definition A.18).

We have

1. $\forall k < h : |\{T' \in \text{Sub}(T) : \text{depth}(T') = k\}| = 2^k$ and $|\text{Sub}(T) \cap \mathbb{R}| = m$;
2. $\forall \nu \in \text{Sub}(T) \setminus \mathbb{R} : I(\nu) = I(R(\nu)) \sqcup I(L(\nu))$ and $\max I(R(\nu)) < \min I(L(\nu))$.

Definition A.32 (Gram form and the nodes' Gram matrices [to table])**.** A Gram matrix has a quadratic form, and its tree's nodes carry Gram matrices. Let:

- $\mathcal{G} \in \text{Gram}_m$ (Definition A.14);
- $x = (x_0, x_1) \in \mathcal{R}_m^2$.

Define:

- $\psi_k := e^{i\pi(2k+1)/m}$, $k < m/2$, the roots of $x^m + 1$ with positive imaginary part;
- $Q_{\mathcal{G}}(x) := \frac{2}{m} \sum_{k<m/2} x(\psi_k)\mathcal{G}(\psi_k)x(\psi_k)^\dagger$, the Gram form;
- $T := \text{ffLDL}^\dagger(\mathcal{G})$ at $m = n$;
- $\mathcal{G}_T := \mathcal{G}$;
- $\mathcal{G}_{T_{00}} := \mathcal{G}_{d_{00}}$ for $\nu = \text{node}(l_{10};\ T_{00}, T_{11}) \in \text{Sub}(T)$ with $\nu = \text{ffLDL}^\dagger(\mathcal{G}_\nu)$, Definition A.20, items 1 to 7;
- $\mathcal{G}_{T_{11}} := \mathcal{G}_{d_{11}}$ for the same ν.

```
noncomputable def gramRoot (m k : Nat) : Complex :=
  Complex.exp (((Real.pi * (2 * k + 1) / m : Real) : Complex) * Complex.I)

noncomputable def gramQuadAt {m : Nat} (g00 g01 g11 x0 x1 : Fin m -> Real) (psi : Complex) :
    Complex :=
  (evalAt x0 psi * evalAt g00 psi + evalAt x1 psi * conj (evalAt g01 psi)) * conj (evalAt x0
      psi)
    + (evalAt x0 psi * evalAt g01 psi + evalAt x1 psi * evalAt g11 psi) * conj (evalAt x1 psi)

noncomputable def evalAt {n : Nat} (f : Fin n -> Real) (x : Complex) : Complex :=
  Sum a, (f a : Complex) * x ^ (a : Nat)
```

Figure 32: The Lean declarations carrying Definition A.32: `gramRoot`, `gramQuadAt`, `evalAt` (`GramPairing.lean`, `Parseval.lean`); Lean's symbols in ASCII.

Fact A.33 (The key's Gram determinant [to table] [to proof])**.** The NTRU equation makes the root's Gram determinant q^2, which fixes the second diagonal $d_{11} = g_{11} - |g_{01}|^2/g_{00}$ and $\kappa = |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$. Let:

- $\psi \in \mathbb{C}$ with $\psi^n = -1$, a root of $x^n + 1$.

Define:

- $g_{00} = |f(\psi)|^2 + |g(\psi)|^2$;
- $g_{11} = |F(\psi)|^2 + |G(\psi)|^2$;
- $g_{01} = g(\psi)\,\text{conj}\,G(\psi) + f(\psi)\,\text{conj}\,F(\psi)$ [L0: `sign_core.c:112-120`] [L0: `fxp/sign_fxcore.c:177-193`] (ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 4);
- $d_{11} = g_{11} - |g_{01}|^2/g_{00}$ at the root node (LDL† (Algorithm 5), line 19);

- $\kappa = |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$ at the root node (LDL† (Algorithm 5), line 15);
- $\kappa_{\text{root}} = \max_\psi \kappa$.

Then the NTRU equation, the determinant, the first diagonal's sign, the second diagonal, κ and κ_{root} are:

1. $fG - gF = q$ in $\mathcal{R}_n$ [L0: `kgen.c:57-59`];
2. $g_{00}g_{11} - |g_{01}|^2 = q^2$;
3. $g_{00} > 0$;
4. $d_{11} = q^2/g_{00}$;
5. $\kappa = |g_{01}|^2/q^2$;
6. $\kappa_{\text{root}} = \max_\psi |g_{01}|^2/q^2$.

Fact A.34 (Key generation checks [to table])**.** The key generation of `c-fn-dsa` bounds the mean of g_{00} and of q^2/g_{00} over the roots. Let:

- $\psi \in \{\psi_k : k < n/2\}$ (Definition A.32 at $m := n$).

Define:

- $f_{[i]}$, the coefficients of $f = \sum_{i<n} f_{[i]}x^i$;
- $g_{[i]}$, the coefficients of $g = \sum_{i<n} g_{[i]}x^i$;
- $\text{AM}_\psi(x) := \text{AM}_{\text{all}}((x(\psi))_\psi) = (2/n)\sum_\psi x(\psi)$ (Definition A.46).

We have

1. $\sum_{i<n} f_{[i]}^2 + g_{[i]}^2 < 16823$ and $\text{AM}_\psi(g_{00}) = \sum_{i<n} f_{[i]}^2 + g_{[i]}^2 \le 16822 < 1.17^2 q$ [L0: `kgen.c:41-49`];
2. $\text{AM}_\psi(q^2/g_{00}) < (0.999 \cdot 1.17)^2 q = 16788.7841$ [L0: `kgen.c:53`] [L0: `kgen_ntru.c:1904-1934`].

Definition A.35 (The rounded thresholds of the key checks [to table])**.** The rounded thresholds raise the four thresholds of the key checks by the roundings of the checks' comparisons. Let:

- $n \in \{512, 1024\}$ be a degree.

Define:

- $(\gamma_{fg}, \gamma_{\text{hyb}}, \gamma_{FG}, \gamma_{\text{root}}) := \begin{cases} (275, 4.75, 4500, 27) & n = 512 \\ (280, 5.75, 6800, 34) & n = 1024 \end{cases}$ (keygen (Algorithm 11), Require) [L0: `fxp/kgen_fx.c:97-111`];
- $q := 12289$ (Definition A.13).

We define:

1. $\check{\gamma}_{fg} := (\gamma_{fg}^2 + 2^{-64})^{1/2}$;
2. $\check{\gamma}_{FG} := (\gamma_{FG}^2 + 2^{-64})^{1/2}$;
3. $\check{\gamma}_{\text{hyb}} := (\gamma_{\text{hyb}}^2 + 2^{-65})^{1/2}$;
4. $\check{\gamma}_{\text{root}} := \left((\gamma_{\text{root}}^2 + 2^{-65})(1 + 2^{-65}\check{\gamma}_{\text{hyb}}^4/q^2) + 2^{-64}\check{\gamma}_{\text{hyb}}^4/q^2\right)^{1/2}$.

Definition A.36 (The Gram deltas of a checked key [to table])**.** The Gram deltas bound the perturbations of a checked key's computed FFT images and computed Gram matrix entries. Let:

- $h \ge 1$;
- $n = 2^h$;
- $\zeta \ge 0$.

Define:

- $\check{\gamma}_{fg} := (\gamma_{fg}^2 + 2^{-64})^{1/2}$ and $\check{\gamma}_{FG} := (\gamma_{FG}^2 + 2^{-64})^{1/2}$ (Definition A.35);
- $R_{h-1} := (1 + \sqrt{2}\,\zeta)^{h-1} - 1$ (Lemma H.11 at $(0, \zeta)$);
- $A_0 := 0$ and $A_{j+1} := \sqrt{2}(1 + \sqrt{2}\,\zeta)A_j + 4\sqrt{2}\,\zeta\sqrt{n}$ for $j < h - 1$ (Lemma H.11 at $(0, \zeta)$);

- $k_H := 7$ and $k'_H := 7\sqrt{2}$ (Lemmas G.22 and G.23 at $u = 0$).

The Gram deltas are:

1. $\delta_{fg} := R_{h-1}(\check{\gamma}_{fg}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$;
2. $\delta_{FG} := R_{h-1}(\check{\gamma}_{FG}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$;
3. $\gamma'_{fg} := \check{\gamma}_{fg} + \delta_{fg}$;
4. $\gamma'_{FG} := \check{\gamma}_{FG} + \delta_{FG}$;
5. $E_{00} := k_H\zeta + 4\gamma'_{fg}\delta_{fg} + 2\delta^2_{fg}$;
6. $E_{11} := k_H\zeta + 4\gamma'_{FG}\delta_{FG} + 2\delta^2_{FG}$;
7. $E_{01} := k'_H\zeta + 2(\gamma'_{fg}\delta_{FG} + \gamma'_{FG}\delta_{fg} + \delta_{fg}\delta_{FG})$.

Definition A.37 (The perturbation bounds of a checked key [to table])**.** The perturbation bounds are the floor, the ceiling and the spread of the diagonals a checked key's Gram deltas admit. Let:

- $q = 12289$;
- $\zeta \geq 0$.

Define:

- $\check{\gamma}_{\mathrm{hyb}} := (\gamma^2_{\mathrm{hyb}} + 2^{-65})^{1/2}$ (Definition A.35);
- $\gamma'_{FG} := \check{\gamma}_{FG} + \delta_{FG}$ and $E_{00} := k_H\zeta + 4\gamma'_{fg}\delta_{fg} + 2\delta^2_{fg}$ (Definition A.36);
- δ_{fg}, δ_{FG}, γ'_{fg} and k_H, those of Definition A.36.

The perturbation bounds are:

1. $m_0 := q/\check{\gamma}^2_{\mathrm{hyb}} - E_{00}$;
2. $M_0 := q\check{\gamma}^2_{\mathrm{hyb}} + E_{00}$;
3. $d_{\mathrm{lo}} := \min(m_0, q^2/M_0)$;
4. $d_{\mathrm{hi}} := \max(M_0, q^2/m_0)$;
5. $\bar{\varsigma} := d_{\mathrm{hi}}/d_{\mathrm{lo}}$;
6. $\bar{g}_{11} := 2\gamma'^2_{FG}$.

A.7 The Rényi divergence argument

Structure. This subsection states formally the normalizer ratio of Appendix E.2.

Definition A.38 (The series of the normalizer deviation [to table])**.** The normalizer deviation $d(s, c)$ (Definition A.29) and its derivatives are bounded by series in s. Let:

- $s > 0$;
- $j \in \{0, 1, 2, 3, 4\}$.

Define:

- $\varepsilon_j(s) := 2\sum_{k\geq 1}(2\pi k)^j e^{-2\pi^2 s^2 k^2}$. [derived]

```
noncomputable def epsJ (s : Real) (j : Nat) : Real :=
  2 * Sum' k : Nat, (2 * Real.pi * ((k : Real) + 1)) ^ j
    * Real.exp (-(2 * Real.pi ^ 2 * s ^ 2) * ((k : Real) + 1) ^ 2)
```

Figure 33: The Lean declarations carrying Definition A.38: `epsJ` (`Normratio.lean`); Lean's symbols in ASCII.

Definition A.39 (The normalizer ratio, its differences and the remainder form [to table])**.** At one leaf the three normalizers form the ratio Φ; two differences and a remainder form bound its logarithm. Let:

- $\alpha > 1$, an order;
- $s > 0$;
- $\delta > -1$ with $\alpha + (1-\alpha)(1+\delta)^2 > 0$;
- $c' \in \mathbb{R}$;
- $\Delta \in \mathbb{R}$;
- $v = (v_s, v_c) \in \mathbb{R}^2$.

Define:

- The leaf parameters
  - $s_1 := s(1+\delta)$;
  - $s_2 := s$;
  - $c := c' + \Delta$;
  - $\theta_\alpha(\delta) := 1/(\alpha + (1-\alpha)(1+\delta)^2)$;
  - $s'' := s(1+\delta)\theta_\alpha(\delta)^{1/2}$, the s'' of Lemma 4.1 at (s_1, s_2, c, c');
  - $m := c' + \alpha\theta_\alpha(\delta)\Delta$, the m of Lemma 4.1 at (s_1, s_2, c, c');
- The normalizer
  - $d(s,c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\, s) - 1$ for $s > 0$ and $c \in \mathbb{R}$ (Definition A.29);
  - $\varepsilon_j(s) := 2\sum_{k\geq 1}(2\pi k)^j e^{-2\pi^2 s^2 k^2}$ (Definition A.38);
- The normalizer ratio
  - $\Phi(s, \delta, c', \Delta) := (1 + d(s'', m))\,(1 + d(s_1, c))^{-\alpha}\,(1 + d(s_2, c'))^{\alpha-1}$, the normalizer ratio;
- The differences
  - $v_1 := (s_1, c) - (s_2, c')$, the first difference;
  - $v'' := (s'', m) - (s_2, c')$, the second difference;
- The remainder form
  - $s_- := \min(s, s_1, s'')$;
  - $s_+ := \max(s, s_1, s'')$;
  - $Q(v) := (s_+^2\varepsilon_4(s_-) + \varepsilon_2(s_-))\, v_s^2 + 2s_+\varepsilon_3(s_-)|v_s||v_c| + \varepsilon_2(s_-)v_c^2$, the remainder form. [derived]

```
noncomputable def normPhi (alpha s delta c' Delta : Real) : Real :=
  (1 + dev (sPP alpha s delta) (mCenter alpha delta c' Delta)) * (1 + dev (s * (1 + delta)) (c'
      + Delta)) ^ (-alpha)
    * (1 + dev s c') ^ (alpha - 1)

noncomputable def sMinN (alpha s delta : Real) : Real := min s (min (s * (1 + delta)) (sPP
    alpha s delta))

noncomputable def Qform (sp e2 e3 e4 vs vc : Real) : Real :=
  (sp ^ 2 * e4 + e2) * vs ^ 2 + 2 * sp * e3 * |vs| * |vc| + e2 * vc ^ 2

noncomputable def sPP (alpha s delta : Real) : Real := s * (1 + delta) * Real.sqrt (thetaN
    alpha delta)

noncomputable def mCenter (alpha delta c' Delta : Real) : Real := c' + alpha * thetaN alpha
    delta * Delta
```

Figure 34: The Lean declarations carrying Definition A.39: `normPhi`, `sMinN`, `Qform`, `sPP`, `mCenter` (`Normratio.lean`); with `dev` of Figure 30; Lean's symbols in ASCII.

Definition A.40 (The uniform bound $\bar{\phi}_{\mathrm{u}}$ [to table])**.** Over the four ranges of the standard deviation, the ratio, the center and the center shift, the constants below build one bound $\bar{\phi}_{\mathrm{u}}$. Let:

- $\alpha > 1$, an order;

- $s_{\mathrm{lo}} > 0$;
- $s_{\mathrm{hi}} \geq s_{\mathrm{lo}}$;
- $\bar{\delta} \in [0, 1)$ with $(1+\bar{\delta})^2 < \alpha/(\alpha-1)$;
- $\bar{\Delta} \geq 0$.

Define:

- The leaf parameters
  - $\theta_\alpha(\delta) := 1/(\alpha + (1-\alpha)(1+\delta)^2)$ (Definition A.39);
- The ranges
  - $r_- := (1-\bar{\delta})\,\theta_\alpha(-\bar{\delta})^{1/2}$;
  - $r_+ := (1+\bar{\delta})\,\theta_\alpha(\bar{\delta})^{1/2}$;
  - $\underline{s} := s_{\mathrm{lo}} r_-$;
  - $\overline{s} := s_{\mathrm{hi}} r_+$;
- The normalizer
  - $\varepsilon_j(s) := 2\sum_{k\geq 1} (2\pi k)^j e^{-2\pi^2 s^2 k^2}$ (Definition A.38);
  - $\varepsilon_j^\circ := \varepsilon_j(\underline{s})$;
- The difference bounds
  - $g(\delta) := (1+\delta)(2+\delta)\,\theta_\alpha(\delta)/(\theta_\alpha(\delta)^{1/2}+1) - 1$;
  - $a_s := (\alpha-1)\,\bar{\delta}\,\max\Big(|g(-\bar{\delta})|, |g(\bar{\delta})|\Big)$;
  - $a_c := \alpha(\alpha-1)(2\bar{\delta}+\bar{\delta}^2)\,\theta_\alpha(\bar{\delta})\,\bar{\Delta}$;
  - $b_s := \max(1-r_-,\ r_+ - 1)$;
  - $b_c := \alpha\,\theta_\alpha(\bar{\delta})\,\bar{\Delta}$;
- The remainder form
  - $\bar{Q}(x,y) := (\overline{s}^2\varepsilon_4^\circ + \varepsilon_2^\circ)\,x^2 + 2\overline{s}\,\varepsilon_3^\circ\,xy + \varepsilon_2^\circ y^2$ for $x, y \geq 0$;
- The uniform bound
  - $\bar{\phi}_{\mathrm{u}} := \alpha(\varepsilon_0^\circ)^2/(1-\varepsilon_0^\circ) + \overline{s}\,\varepsilon_2^\circ\,s_{\mathrm{hi}} a_s + \varepsilon_1^\circ a_c + \Big(\bar{Q}(s_{\mathrm{hi}} b_s, b_c) + \alpha\bar{Q}(s_{\mathrm{hi}}\bar{\delta}, \bar{\Delta})\Big)/2.$ [derived]

```
noncomputable def phiBox (alpha slo shi deltab Deltab : Real) : Real :=
  alpha * epsJ (sUnder alpha slo deltab) 0 ^ 2 / (1 - epsJ (sUnder alpha slo deltab) 0)
    + sOver alpha shi deltab * epsJ (sUnder alpha slo deltab) 2 * (shi * aSbox alpha deltab)
    + epsJ (sUnder alpha slo deltab) 1 * aCbox alpha deltab Deltab
    + (Qform (sOver alpha shi deltab) (epsJ (sUnder alpha slo deltab) 2) (epsJ (sUnder alpha
        slo deltab) 3)
          (epsJ (sUnder alpha slo deltab) 4) (shi * bSbox alpha deltab) (bCbox alpha deltab
              Deltab)
        + alpha * Qform (sOver alpha shi deltab) (epsJ (sUnder alpha slo deltab) 2) (epsJ
            (sUnder alpha slo deltab) 3)
          (epsJ (sUnder alpha slo deltab) 4) (shi * deltab) Deltab) / 2

noncomputable def sUnder (alpha slo deltab : Real) : Real := slo * rMinus alpha deltab

noncomputable def sOver (alpha shi deltab : Real) : Real := shi * rPlus alpha deltab

noncomputable def aSbox (alpha deltab : Real) : Real := (alpha - 1) * deltab * max |gBox alpha
    (-deltab)| |gBox alpha deltab|

noncomputable def aCbox (alpha deltab Deltab : Real) : Real :=
  alpha * (alpha - 1) * (2 * deltab + deltab ^ 2) * thetaN alpha deltab * Deltab

noncomputable def bSbox (alpha deltab : Real) : Real := max (1 - rMinus alpha deltab) (rPlus
    alpha deltab - 1)

noncomputable def bCbox (alpha deltab Deltab : Real) : Real := alpha * thetaN alpha deltab *
    Deltab
```

Figure 35: The Lean declarations carrying Definition A.40: `phiBox`, `sUnder`, `sOver`, `aSbox`, `aCbox`, `bSbox`, `bCbox` (`Normratio.lean`); with `epsJ` of Figure 33; with `Qform` of Figure 34; Lean's symbols in ASCII.

A.8 The facts the proofs use

Structure. Appendix A.8.1 states the elementary facts; Appendix A.8.2 the arithmetic and harmonic means.

A.8.1 Elementary facts used in the proofs

This subsection states the standard facts the derivation lines cite by item.

Fact A.41 (Real and complex numbers [to table])**.** The derivation lines cite these facts of real and complex numbers. Let:

- $x \in \mathbb{C}$;
- $y \in \mathbb{C}$;
- $k \in \mathbb{Z}_{\geq 0}$;
- $X \in \mathbb{C}^k$;
- $Y \in \mathbb{C}^k$;
- $w \in [0,\infty)^k$.

Define:

- $\|X\|^2 := \sum_i |X_i|^2$;
- $\|X\|_w^2 := \sum_i w_i |X_i|^2$;
- $\|(X,Y)\|^2 := \|X\|^2 + \|Y\|^2$.

We have

1. $|x| \geq 0$; $|x+y| \leq |x|+|y|$; $||x|-|y|| \leq |x-y|$; $|xy| = |x||y|$; $|\operatorname{conj} x| = |x|$; $|\operatorname{Re} x|, |\operatorname{Im} x| \leq |x|$; $\forall a, b \in \mathbb{R}:\ |a+ib|^2 = a^2+b^2$; $x + \operatorname{conj} x = 2 \operatorname{Re} x$; $x \operatorname{conj} x = |x|^2$;
2. $|x+y|^2 + |x-y|^2 = 2(|x|^2 + |y|^2)$;

3. $\|X\|_w \geq 0$; $\|X+Y\|_w \leq \|X\|_w + \|Y\|_w$ ($w = (1,\ldots,1)$ for $\|\cdot\|$); $|X_i| \leq \|X\|$; $\|(x,y)\| \leq |x|+|y|$; $\|(x,y)\| \leq \sqrt{2}\max(|x|,|y|)$; $\|(X,Y)\| \leq \sqrt{2}\max(\|X\|,\|Y\|)$;

4. $\sum_i |X_i||Y_i| \leq \|X\|\|Y\|$ and $|\sum_i X_i \operatorname{conj} Y_i| \leq \|X\|\|Y\|$; $\left(\sum_i w_i a_i b_i\right)^2 \leq \sum_i w_i a_i^2 \sum_i w_i b_i^2$ for real a_i, b_i;

5. $\forall p \geq 0$: $t \mapsto t^p$ is nondecreasing on $[0,\infty)$; $t \mapsto \sqrt{t}$ is nondecreasing on $[0,\infty)$; $t \mapsto 1/t$ is nonincreasing on $(0,\infty)$; $t \mapsto t + 1/t$ is nondecreasing on $[1,\infty)$; exp is increasing on $\mathbb{R}$; $\forall t > -1$: $\ln(1+t) \leq t$; $\forall t$: $|e^t - 1| \leq e^{|t|} - 1$; a function continuous on an interval with a nonnegative derivative inside it is nondecreasing there;

6. $\forall \alpha \geq 2\ \forall \epsilon \geq -1$: $(1+\epsilon)^\alpha \leq 1 + \alpha\epsilon + \frac{\alpha(\alpha-1)}{2}(1+\max(\epsilon,0))^{\alpha-2}\epsilon^2$;

7. $\forall \omega \in \mathbb{C} \setminus \{1\}\ \forall N$: $\sum_{j<N} \omega^j = (\omega^N - 1)/(\omega - 1)$;

8. $\forall a, a', b, b' \in \mathbb{R},\ 0 \leq a \leq a',\ 0 \leq b \leq b' :\ ab \leq a'b'$; $\forall m \geq 0\ \forall s,t \geq m :\ m(s+t)/2 \leq m\max(s,t) \leq st$;

9. $\forall a, b > 0$: $\min(a,b) \leq 2ab/(a+b) \leq (a+b)/2 \leq \max(a,b)$;

10. $\forall x, y, A, b \in \mathbb{R},\ |x-1| \leq A,\ |y-1| \leq b < 1$: $|x/y - 1| \leq (1+A)/(1-b) - 1$;

11. $\forall g, g', g'' : [0,1] \to \mathbb{R}\ \forall M \geq 0$, g' the derivative of g and g'' that of g' on $[0,1]$, $|g''| \leq M$ on $[0,1]$: $|g(1) - g(0) - g'(0)| \leq M/2$;

12. $e^x e^y = e^{x+y}$; $\forall t \in \mathbb{R}$: $e^t > 0$; $\forall \theta \in \mathbb{R}$: $e^{i\theta} = \cos\theta + i\sin\theta$, $\operatorname{conj} e^{i\theta} = e^{-i\theta}$, $\cos^2\theta + \sin^2\theta = 1$, $|\cos\theta| \leq 1$, $|\sin\theta| \leq 1$; $e^{i\pi} = -1$; $\forall t \in \mathbb{R}$: $2^t = e^{t\ln 2}$; $\forall y > 0\ \forall a \in \mathbb{R}$: $\ln(y^a) = a\ln y$;

13. $\operatorname{conj} x + y = \operatorname{conj} x + \operatorname{conj} y$; $\operatorname{conj} xy = \operatorname{conj} x \operatorname{conj} y$; $\forall a, b \geq 0$: $\sqrt{ab} = \sqrt{a}\sqrt{b}$; $\forall t \in \mathbb{R}\ \forall j \in \mathbb{Z}_{\geq 0}$: $t^{2j} \geq 0$;

14. $\forall \alpha \geq 1\ \forall a, b, t \in \mathbb{R},\ 0 \leq a < b,\ a \leq t \leq b$: $t^\alpha \leq a^\alpha + (t-a)(b^\alpha - a^\alpha)/(b-a)$;

15. $\forall \epsilon \in [0,1)\ \forall x \in \mathbb{R},\ |x| \leq \epsilon$: $|\ln(1+x) - x| \leq x^2/(2(1-\epsilon))$;

16. $\forall a, b, c, d, s \in \mathbb{R},\ a \leq s \leq b$: $cs + d \leq \max(ca + d,\ cb + d)$;

17. $\forall A, B$ subsets of one set: $(A \setminus B)^c = A^c \cup B$; $A \cap B \subseteq A$, $A \cap B \subseteq B$; $A \subseteq (A \cap B) \cup B^c$; $\forall N \in \mathbb{Z}_{>0}$: $\mathbb{Z}^N$ is countable;

18. $\forall k \in \mathbb{Z}_{\geq 0}\ \forall A, c, x \in \mathbb{R}$, $x \leq Ac'^k$ at every $c' > c$: $x \leq Ac^k$;

19. $\forall d : \mathbb{R}^2 \to \mathbb{R}$ differentiable at $y \in \mathbb{R}^2\ \forall v \in \mathbb{R}^2$: $r \mapsto d(y + rv)$ has the derivative $\nabla d(y) \cdot v$ at $r = 0$;

20. $\forall a, b \in \mathbb{R}$: $\min(a,b) \leq a$, $\min(a,b) \leq b$, $a \leq \max(a,b)$, $b \leq \max(a,b)$; $\forall A \subseteq \mathbb{R}$ finite and nonempty $\forall a \in A$: $a \leq \max A$; $\forall A \subseteq \mathbb{R}\ \forall a \in A$: $a \leq \sup A \in (-\infty, \infty]$; $\forall A \subseteq \mathbb{R}\ \forall b \in \mathbb{R}$, $(\forall a \in A :\ a \leq b)$: $\sup A \leq b$;

21. $\forall E \geq 0$: $e^E + e^{-E} \geq 2$; $\forall E, p \geq 0$: $1 - e^{-E}(1-p) \leq e^E(1+p) - 1$;

22. $\forall y \in \mathbb{R}$: $\lfloor y \rfloor \in (y-1, y]$, $\lceil y \rceil = -\lfloor -y \rfloor$; $\forall a, d \in \mathbb{Z},\ d \geq 1$: $\lceil a/d \rceil = \lfloor (a+d-1)/d \rfloor$;

23. $\forall p \in (1,2)\ \forall \epsilon > -1$: $(1+\epsilon)^p \leq 1 + p\epsilon + \frac{p(p-1)}{2}(1+\min(\epsilon,0))^{p-2}\epsilon^2$; $\forall b \geq 1\ \forall p \leq q$: $b^p \leq b^q$;

24. $\forall a, a', b, b' \in \mathbb{R},\ a \leq a',\ b \leq b'$: $\max(a,b) \leq \max(a',b')$;

25. $\forall a, a', b, b' \in \mathbb{R},\ a \leq a',\ b \leq b'$: $\min(a,b) \leq \min(a',b')$;

26. $\forall a, b, c \in \mathbb{R},\ a \leq b,\ c \geq 0$: $ca \leq cb$; $\forall a, b, c \in \mathbb{R},\ a < b,\ c > 0$: $ca < cb$;

27. $\forall x \geq 0$: $e^x \geq 1$;
28. $\forall y > 0$: $e^{\ln y} = y$ and $e^{-\ln y} = 1/y$; $\forall y \geq 1$: $\ln y \geq 0$; $\forall t \geq 0$: $(\sqrt{t})^2 = t$;
29. $\forall s, t > 0$: $\ln(st) = \ln s + \ln t$;
30. $\forall t \in \mathbb{R}$: $\ln e^t = t$;
31. $\forall y \in (-1, 1)$: $\ln(1 + y) = \sum_{k \geq 1} (-1)^{k+1} y^k / k$;
32. $\forall p \in [0, 1)$: $\sum_{k \geq 3} p^k = p^3/(1 - p)$;
33. $|x + y|^2 = |x|^2 + |y|^2 + 2 \operatorname{Re}(x \operatorname{conj} y)$;
34. $|x - y|^2 = |x|^2 + |y|^2 - 2 \operatorname{Re}(x \operatorname{conj} y)$;
35. $\operatorname{conj} \operatorname{conj} x = x$;
36. $\operatorname{Re} \operatorname{conj} x = \operatorname{Re} x$;
37. $\forall K, m \in \mathbb{Z}_{\geq 0}$: $\binom{K}{m} \in [0, K^m/m!]$;
38. $\forall K, m \in \mathbb{Z}_{\geq 0}$: $K^m/m! \leq K^m$;
39. $\forall K \in \mathbb{Z}_{\geq 0}$: $\binom{K}{0} = 1$;
40. $\forall t \geq 0\ \forall a \in \mathbb{R}$: $t^a \geq 0$;
41. $\forall t \in \mathbb{R}$: $t^0 = 1$;
42. $\forall t \geq 0$: $t^1 = t$;
43. $\forall a \in \mathbb{R}$: $1^a = 1$;
44. $\forall a > 0$: $0^a = 0$;
45. $\forall s, t \geq 0\ \forall a \in \mathbb{R}$: $(st)^a = s^a t^a$;
46. $\forall t \geq 0\ \forall a, b \in \mathbb{R}$: $(t^a)^b = t^{ab}$;
47. $\forall a, b, c \in \mathbb{R},\ c \leq a,\ c \leq b$: $c \leq \min(a, b)$.

Fact A.42 (Polynomial values and the split [to table])**.** The derivation lines cite these facts of polynomials f and their values $f(\psi)$, $\psi^m = -1$. Let:

- $m \geq 2$, a power of two;
- $f \in \mathcal{R}_m$;
- $g \in \mathcal{R}_m$;
- $c \in \mathbb{R}$;
- $\psi \in \mathbb{C}$ with $\psi^m = -1$.

Define:

- $\operatorname{split}(a) := (a_0, a_1)$ for $a \in \mathcal{R}_m$, $m \geq 4$ (Definition A.15);
- $a_0 := \sum_{i < m/2} a_{[2i]} x^i$ and $a_1 := \sum_{i < m/2} a_{[2i+1]} x^i$ (Definition A.15);
- $\operatorname{merge}(f_0, f_1) := f_0(x^2) + x f_1(x^2)$ (Definition A.15).

We have

1. $|\psi| = 1$ and $\psi \operatorname{conj} \psi = 1$;
2. $\operatorname{conj} \psi^m = -1$ and $f(\operatorname{conj} \psi) = \operatorname{conj} f(\psi)$;
3. $|f(\psi)| \leq \sum_{a < m} |f_{[a]}|$;

4. At $m \geq 4$: $\operatorname{split}(f + cg) = \operatorname{split}(f) + c \operatorname{split}(g)$ and $\operatorname{merge}(\operatorname{split}(f)) = f$;
5. At $m \geq 4$: $\forall (f_0, f_1) \in \mathcal{R}_{m/2}^2 :\ \operatorname{split}(\operatorname{merge}(f_0, f_1)) = (f_0, f_1)$;
6. $(f + g)(\psi) = f(\psi) + g(\psi)$;
7. $(fg)(\psi) = f(\psi)g(\psi)$;
8. $c(\psi) = c$, c read as a constant of $\mathcal{R}_m$;
9. $\forall \xi_0, \dots, \xi_{m-1} \in \mathbb{C}$ pairwise distinct with $\forall j < m :\ \xi_j^m = -1$: $x^m + 1 = \prod_{j<m}(x - \xi_j)$.

Fact A.43 (The roots with positive imaginary part [to table])**.** The derivation lines cite these facts of the roots of $x^m + 1$ and their half with positive imaginary part. Let:

- $m \geq 2$, a power of two.

Define:

- $\xi_j = e^{i\pi(2j+1)/m}$, $j < m$;
- $\psi_k = e^{i\pi(2k+1)/m}$, $k < m/2$;
- $Z_m = \{\psi \in \mathbb{C} : \psi^m = -1\}$;
- $\Psi_m = \{\psi_k : k < m/2\}$.

We have

1. $\forall j < m :\ \xi_j^m = -1$; the ξ_j are pairwise distinct; $x^m + 1 = \prod_{j<m}(x - \xi_j)$ (Fact A.42, item 9, at the ξ_j); $Z_m = \{\xi_j : j < m\}$;
2. $\forall k < m/2 :\ \operatorname{conj} \psi_k = \xi_{m-1-k}$; $\Psi_m = \{\psi \in Z_m : \operatorname{Im} \psi > 0\}$; $Z_m = \Psi_m \sqcup \operatorname{conj} \Psi_m$;
3. $-\Psi_m = \operatorname{conj} \Psi_m$;
4. $\forall \omega, \psi' \in \mathbb{C},\ \psi' \neq 0,\ \psi'^2 = \omega :\ \{z \in \mathbb{C} : z^2 = \omega\} = \{\psi', -\psi'\}$ and $\psi' \neq -\psi'$;
5. At $m \geq 4$: $\psi \mapsto \psi^2$ is a bijection $\Psi_m \to Z_{m/2}$;
6. $\forall g : Z_m \to \mathbb{C},\ \forall \psi \in Z_m :\ g(\operatorname{conj} \psi) = g(\psi)$ implies $\sum_{\psi \in Z_m} g(\psi) = 2 \sum_{k<m/2} g(\psi_k)$;
7. For g as in item 6: $\sum_{\psi^{m/2}=i} g(\psi) = \sum_{k<m/2} g(\psi_k)$, and $|\{\psi \in \mathbb{C} : \psi^{m/2} = i\}| = m/2$.

Fact A.44 (Hermitian 2×2 matrices [to table])**.** The derivation lines cite these facts of Hermitian 2×2 matrices. Let:

- $g_{00} \in \mathbb{R}$;
- $g_{11} \in \mathbb{R}$;
- $g_{01} \in \mathbb{C}$;
- $l \in \mathbb{C}$;
- $x = (x_0, x_1) \in \mathbb{C}^2$.

Define:

- $\mathcal{G} := \begin{pmatrix} g_{00} & g_{01} \\ \operatorname{conj} g_{01} & g_{11} \end{pmatrix}$;
- $L := \begin{pmatrix} 1 & 0 \\ l & 1 \end{pmatrix}$;
- $m := (g_{00} + g_{11})/2$;
- $r := \sqrt{((g_{00} - g_{11})/2)^2 + |g_{01}|^2}$;
- $\lambda_\pm := m \pm r$.

We have

1. $x\mathcal{G}x^\dagger = g_{00}|x_0|^2 + 2 \operatorname{Re}(x_0 g_{01} \operatorname{conj} x_1) + g_{11}|x_1|^2 \in \mathbb{R}$;
2. $\lambda_\pm$ are the two eigenvalues of $\mathcal{G}$: $(\lambda_\pm - g_{00})(\lambda_\pm - g_{11}) = |g_{01}|^2$; for $g_{00} = g_{11} = d_0$, $\lambda_\pm = d_0 \pm |g_{01}|$;

3. $\lambda_-(|x_0|^2 + |x_1|^2) \le x\mathcal{G}x^\dagger \le \lambda_+(|x_0|^2 + |x_1|^2)$;

4. $g_{00}, g_{11} \ge 0$ and $g_{00}g_{11} \ge |g_{01}|^2$ imply $\lambda_- \ge 0$ and $\lambda_+ \le g_{00} + g_{11} = \operatorname{trace}\mathcal{G}$;

5. $L^{-1} = \begin{pmatrix} 1 & 0 \\ -l & 1 \end{pmatrix}$; $\det L = 1$; a product of unit lower triangular matrices is unit lower triangular and invertible.

Fact A.45 (Probability and Gaussian sums on $\mathbb{Z}$ [to table])**.** The derivation lines cite these facts of probability measures, rejection sampling, Gaussian sums on $\mathbb{Z}$ and Rényi divergences.

1. Let $N \ge 1$ and $z = (z_1, \dots, z_N)$ a random sequence with the conditional probabilities $P_i(z_i \mid z_{<i})$. Then $P(z) = \prod_i P_i(z_i \mid z_{<i})$; the same for densities.

2. Let $N \ge 1$, μ a probability measure on $\mathbb{Z}^N$ with the conditional probabilities $\mu_i(x \mid q)$ of item 1, and $\forall i \le N\ \forall q \in \mathbb{Z}^{i-1}\ \forall x \in \mathbb{Z} :\ \mu_i(x \mid q) > 0$. Then $\forall i \le N+1\ \forall p \in \mathbb{Z}^{i-1} :\ \mu(p) > 0$, $\mu(p)$ the mass of the event the prefix p names (Definition A.3).

3. Let $N \ge 1$, μ a probability measure on $\mathbb{Z}^N$, $i \le N$, $p \in \mathbb{Z}^{i-1}$ with $\mu(p) > 0$, $\mu_i(x \mid p) := \mu(\{z \in \mathbb{Z}^N : z_i = x\} \,|\, p)$ for $x \in \mathbb{Z}$, ν a probability measure on $\mathbb{Z}$, $Y \subseteq \mathbb{Z}$ with $\forall x \in Y :\ \mu_i(x \mid p) > 0$, $\alpha > 1$, and the function $\mathbf{1}_Y(\nu/\mu_i(\cdot \mid p))^\alpha$ on $\mathbb{Z}$ read at the i-th coordinate of $\mathbb{Z}^N$. Then $\mathbb{E}_\mu[\mathbf{1}_Y(\nu/\mu_i(\cdot \mid p))^\alpha \,|\, p] = \sum_{x\in Y} \nu(x)^\alpha\, \mu_i(x \mid p)^{1-\alpha}$, both sides in $[0, \infty]$ (Definition A.3).

4. Let q be a probability measure on a finite set and acc with values in $[0, 1]$ and $\sum_z q(z)acc(z) > 0$. Then rejection sampling from q with the acceptance acc outputs z with probability

$$\frac{q(z)\, acc(z)}{\sum_{z'} q(z')\, acc(z')}.$$

5. Let P be a probability measure and $A, A_1, \dots, A_N$ events. Then $P(\bigcup_i A_i) \le \sum_i P(A_i)$ and $P(A) = 1 - P(A^c) \le 1$.

6. Let $s > 0$ and $c \in \mathbb{R}$. Then $\rho_{s,c}(\mathbb{Z}) = \sum_{z\in\mathbb{Z}} e^{-(z-c)^2/(2s^2)}$ converges, and $\rho_{s,c}(\mathbb{Z}) = \sqrt{2\pi}\, s \sum_{k\in\mathbb{Z}} e^{-2\pi^2 s^2 k^2} \cos(2\pi k c)$.

7. Let μ, ν be probability measures on a countable set X with $\operatorname{Supp}(\mu) \subseteq \operatorname{Supp}(\nu)$, $B \subseteq X$ and $\alpha > 1$. Then $\mu(B) \le \left(\sum_{x\in B} \mu(x)^\alpha\, \nu(x)^{1-\alpha}\right)^{1/\alpha} \nu(B)^{(\alpha-1)/\alpha}$.

8. Let μ, ν be probability measures on $\mathbb{Z}$ with $\forall z \in \mathbb{Z} :\ \nu(z) > 0$, and $a > 1$. Then $R_a(\mu \,\|\, \nu) \le R_{2a-1}(\mu \,\|\, \nu)$ (Definition A.3).

9. Let Y be a countable set, $a, b \in \mathbb{R}$ and $f, g : Y \to \mathbb{R}$. If $\forall y \in Y :\ 0 \le f(y) \le g(y)$ and $\sum_{y\in Y} g(y)$ converges, then $\sum_{y\in Y} f(y)$ converges and $\sum_{y\in Y} f(y) \le \sum_{y\in Y} g(y)$. If $\sum_{y\in Y} f(y)$ and $\sum_{y\in Y} g(y)$ converge, then $\sum_{y\in Y}(af(y) + bg(y)) = a\sum_{y\in Y} f(y) + b\sum_{y\in Y} g(y)$.

10. Let μ, ν be probability measures on a countable set X, $B \subseteq X$ with $\mu(B) > 0$ and $\nu(B) > 0$, $\mu_B(A) := \mu(A \cap B)/\mu(B)$ and $\nu_B(A) := \nu(A \cap B)/\nu(B)$ for $A \subseteq X$, and $\alpha > 1$. Then $R_\alpha(\mu_B \,\|\, \nu_B)^{\alpha-1} = \nu(B)^{\alpha-1}\mu(B)^{-\alpha} \sum_{x\in B} \mu(x)^\alpha\, \nu(x)^{1-\alpha}$.

11. Let Y, Y' be countable sets and $f : Y \times Y' \to [0, \infty)$. Then $\sum_{(y,y')\in Y\times Y'} f(y, y') = \sum_{y\in Y} \sum_{y'\in Y'} f(y, y')$, both sides in $[0, \infty]$.

12. Let P be a probability measure and $A \subseteq B$ events. Then $P(\emptyset) = 0$ and $P(A) \le P(B)$.

13. Let P be a probability measure, $m \in \mathbb{R}$, $s \geq 0$, X a real random variable Gaussian under P of mean m and standard deviation s, and $\xi \geq 0$. Then $P(X > m + \xi s) \leq e^{-\xi^2/2}$ and $P(|X - m| > \xi s) \leq 2e^{-\xi^2/2}$.

14. Let $m \geq 1$, $\Lambda \subset \mathbb{R}^m$ a lattice, and $f : \mathbb{R}^m \to \mathbb{C}$ with the niceness assumptions of [MR07, footnote 10]. Define $\hat{f}(w) := \int_{\mathbb{R}^m} f(x) e^{-2\pi i \langle x, w \rangle}\, dx$ for $w \in \mathbb{R}^m$, the dual lattice $\Lambda^\dagger$ by $\forall x \in \mathbb{R}^m : \ x \in \Lambda^\dagger \iff (\forall y \in \Lambda : \ \langle x, y \rangle \in \mathbb{Z})$, $\det \Lambda^\dagger$ the volume of a fundamental parallelepiped of $\Lambda^\dagger$, and $f(A) := \sum_{x \in A} f(x)$ for a countable $A \subset \mathbb{R}^m$. Then [L1: MR07, Lem. 2.8]

$$f(\Lambda) = \det(\Lambda^\dagger)\, \hat{f}(\Lambda^\dagger).$$

Item 6 is its instance at $m = 1$, $\Lambda := \mathbb{Z}$, $\Lambda^\dagger = \mathbb{Z}$, $\det \Lambda^\dagger = 1$ and $f := \rho_{s,c}$, where $\hat{f}(k) = \sqrt{2\pi}\, s\, e^{-2\pi^2 s^2 k^2} e^{-2\pi i k c}$ by their (2) at $v := -c$, and by $\hat{\rho}_s = s^n \rho_{1/s}$, theirs, at $s := \sqrt{2\pi}\, s$ of theirs, for $\rho(x) = e^{-\pi x^2}$, theirs; the terms k and $-k$ paired.

A.8.2 The arithmetic and harmonic means

Definition A.46 (The arithmetic and harmonic means, their compositions [to table])**.** The two-argument means compose along a binary tree into means of 2^k values. Let:

- $a > 0$;
- $b > 0$;
- $m \geq 1$;
- $a_1, \ldots, a_m > 0$;
- $k \geq 0$.

Define:

- $\mathrm{AM}(a, b) := (a + b)/2$;
- $\mathrm{HM}(a, b) := 2ab/(a + b)$;
- $\mathrm{AM}_{\mathrm{all}} := (1/m) \sum_i a_i$, the arithmetic mean over all values;
- $\mathrm{HM}_{\mathrm{all}} := m / \sum_i a_i^{-1}$, the harmonic mean over all values;
- $$\begin{aligned} \mathcal{C}_0 &:= \{a_1 \mapsto a_1\}, \\ \forall k \geq 1 : \ \mathcal{C}_k &:= \{(a_1, \ldots, a_{2^k}) \mapsto M(C_L(a_1, \ldots, a_{2^{k-1}}),\ C_R(a_{2^{k-1}+1}, \ldots, a_{2^k})) : \\ &\qquad M \in \{\mathrm{AM}, \mathrm{HM}\},\ C_L, C_R \in \mathcal{C}_{k-1}\}, \end{aligned}$$
- $C_{\mathrm{AM}} \in \mathcal{C}_k$, the composition with $M = \mathrm{AM}$ and $C_L = C_R = C_{\mathrm{AM}} \in \mathcal{C}_{k-1}$ at every depth;
- $C_{\mathrm{HM}} \in \mathcal{C}_k$, the composition with $M = \mathrm{HM}$ and $C_L = C_R = C_{\mathrm{HM}} \in \mathcal{C}_{k-1}$ at every depth.

```
inductive Cascade : Nat -> Type
  | leaf (x : Real) : Cascade 0
  | am {k : Nat} (l r : Cascade k) : Cascade (k + 1)
  | hm {k : Nat} (l r : Cascade k) : Cascade (k + 1)
```

Figure 36: The Lean declarations carrying Definition A.46: `Cascade` (`Tree.lean`); Lean's symbols in ASCII.

B The relative form of a modulus bound, the complex operations, the split butterfly's even half, and the tail of a sum of offsets

Structure. This appendix proves the steps the other proofs take. Section B.1 states the relative form of a modulus bound over $\mathbb{C}$; Section B.2 the bounds of the complex operations; Section B.3 the even half of the split butterfly; Section B.4 the tail of a sum of discrete Gaussian offsets. The first three hold for the pair (u, ζ) of any realization.

How each statement is verified. Table 13 lists how each lemma of this appendix is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma B.1	✓				
Lemma B.2	✓				
Lemma B.3	✓				
Lemma B.4	✓				
Lemma B.5	✓				

Table 13: Appendix B: how each lemma is verified.

How a proof line is cited. A line of a proof is cited from anywhere in the report as "(Lk)" of the statement it proves.

B.1 The relative form of a deviation bound

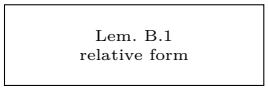


Figure 37: Dependencies, Section B.1.

Lemma B.1 (The relative form of a modulus bound over $\mathbb{C}$ [to table])**.** *A value within c times the modulus of its reference is the reference times a factor within c of 1. Let:*

- $c \geq 0$;
- $x \in \mathbb{C}$;
- $p \in \mathbb{C}$ *with* $|p - x| \leq c|x|$.

Define:

- $\delta(p, x) := (p - x)/x$ *for* $x \neq 0$;
- $\delta(p, 0) := 0$.

We have

$$|\delta(p, x)| \leq c, \qquad p = x(1 + \delta(p, x)).$$

Proof. (L1) $x = 0 \Rightarrow\ |p| \leq 0 \Rightarrow\ p = 0$

[the constraint at $x = 0$]

(L2) $x = 0 \Rightarrow\ x(1 + \delta(p, 0)) = 0$

[expand]

(L3) $x = 0 \Rightarrow\ p = x(1 + \delta(p, 0))$

[(L1), (L2)]

(L4) $x \neq 0 \Rightarrow\ |\delta(p, x)| = |p - x|/|x|$

[$\delta(p, x) = (p - x)/x$ (the statement); $|y/x| = |y|/|x|$ (Fact A.41, item 1)]

(L5) $x \neq 0 \Rightarrow\ |\delta(p, x)| \leq c$

[(L4); $|p - x| \leq c|x|$ (the statement), divided by $|x| > 0$]

(L6) $x \neq 0 \Rightarrow\ x(1 + \delta(p, x)) = x + (p - x)$

[$\delta(p, x) = (p - x)/x$ (the statement)]

(L7) $x + (p - x) = p$

[expand]

(L8) $x \neq 0 \Rightarrow\ x(1 + \delta(p, x)) = p$

[(L6), (L7)]

(L9) $\Rightarrow$ the statement

[(L3) at $x = 0$ with $\delta(p, 0) = 0$ and $c \geq 0$ (the statement); (L5), (L8) at $x \neq 0$]

□

B.2 The complex operations

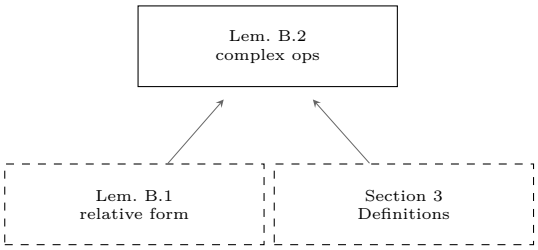


Figure 38: Dependencies, Section B.2.

Lemma B.2 (Complex operations [to table])**.** *Each complex operation of the code is within a relative and an absolute bound of the exact one. Define:*

- $a \oplus b := \mathrm{fl}(a_r + b_r) + i\ \mathrm{fl}(a_i + b_i)$ *(Definition A.8 at (u, ζ));*
- $a \ominus b := a \oplus (-b)$ *(Definition A.8 at (u, ζ));*
- $a \otimes b := \mathrm{fl}(\mathrm{fl}(a_r b_r) - \mathrm{fl}(a_i b_i)) + i\ \mathrm{fl}(\mathrm{fl}(a_r b_i) + \mathrm{fl}(a_i b_r))$ *(Definition A.8 at (u, ζ));*
- $k_B := \sqrt{2}(3 + 2u)$.

We have, in the relation $\mathcal{I}(\cdot, \cdot)$ (Definition A.10):

1. $\forall a, b \in C_{\mathcal{F}} : (a \oplus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\zeta^{\pm}\right)\ (a + b)$.
2. $\forall a, b \in C_{\mathcal{F}} : (a \ominus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\zeta^{\pm}\right)\ (a - b)$.
3. $\forall a, b \in C_{\mathcal{F}} : (a \otimes b)\ \mathcal{I}\left(\left(\sqrt{2}u(2 + u)\right)^{\pm}, k_B\zeta^{\pm}\right)\ ab$.
4. $\forall a \in \mathbb{C}, |a| = 1\ \forall \tilde{a} \in C_{\mathcal{F}}, \tilde{a}_r\ \mathcal{I}(u^{\pm}, \zeta^{\pm})\ a_r, \tilde{a}_i\ \mathcal{I}(u^{\pm}, \zeta^{\pm})\ a_i : \tilde{a}\ \mathcal{I}\left(u^{\pm} + \sqrt{2}\zeta^{\pm}, 0\right)\ a$.
5. $\forall m \geq 1\ \forall (a_k), (b_k) \in C_{\mathcal{F}}^m : (a_k \otimes b_k)_k\ \mathcal{N}\left(\sqrt{2}u(2 + u), \sqrt{m}k_B\zeta\right)\ (a_k b_k)_k$ *[L0: sign_fpoly.c: 1750] [L0: fxp/sign_fxpoly.c: 115].*

Proof.

DEFINES item 1: $\mathrm{Re} := a_r + b_r$, $\mathrm{Im} := a_i + b_i$; $a \oplus b = \mathrm{fl}(\mathrm{Re}) + i\ \mathrm{fl}(\mathrm{Im})$ ($\oplus \ominus \otimes$ (Algorithm 1), line 1); $e := \zeta_r + i\zeta_i$, ζ_r, ζ_i those of (L1), (L2)
item 3: $\mathrm{Re} := a_r b_r - a_i b_i$, $\mathrm{Im} := a_r b_i + a_i b_r$; $\widetilde{\mathrm{Re}} := \mathrm{fl}(\mathrm{fl}(a_r b_r) - \mathrm{fl}(a_i b_i))$, $\widetilde{\mathrm{Im}} := \mathrm{fl}(\mathrm{fl}(a_r b_i) + \mathrm{fl}(a_i b_r))$, $a \otimes b = \widetilde{\mathrm{Re}} + i\,\widetilde{\mathrm{Im}}$ ($\oplus \ominus \otimes$ (Algorithm 1), line 3);
$E_r := (\zeta_{rr} - \zeta_{ii})(1 + u_{\mathrm{Re}}) + \zeta_{\mathrm{Re}}$, $E_i := (\zeta_{ri} + \zeta_{ir})(1 + u_{\mathrm{Im}}) + \zeta_{\mathrm{Im}}$, $e := E_r + iE_i$, $u.$, $\zeta.$ those of (L21), (L28)
item 4: $e := \zeta_r + i\zeta_i$, ζ_r, ζ_i those of (L41), (L42)
item 5: $m \geq 1$ and $(a_k)_k, (b_k)_k \in C_{\mathcal{F}}^m$, those of the item; $f := (a_k)_k$, $g := (b_k)_k$, $(fg)_k := a_k b_k$, $\widetilde{p}_k := a_k \otimes b_k$, $\|x\|^2 := \sum_{k<m} |x_k|^2$

Proof of item 1.

(L1) $\exists\, u_r, \zeta_r \in \mathbb{R},\ |u_r| \leq u,\ |\zeta_r| \leq \zeta :\ \mathrm{fl}(\mathrm{Re}) = \mathrm{Re}\,(1 + u_r) + \zeta_r$
[Def. A.4 for $+$; Def. A.8: $a \oplus b = \mathrm{fl}(\mathrm{Re}) + i\ \mathrm{fl}(\mathrm{Im})$]

(L2) $\exists\, u_i, \zeta_i \in \mathbb{R},\ |u_i| \leq u,\ |\zeta_i| \leq \zeta :\ \mathrm{fl}(\mathrm{Im}) = \mathrm{Im}\,(1 + u_i) + \zeta_i$
[Def. A.4 for $+$; Def. A.8]

(L3) $\Rightarrow\ |e|^2 = \zeta_r^2 + \zeta_i^2$
[e (the proof's block); $|x + iy|^2 = x^2 + y^2$ (Fact A.41, item 1)]

(L4) $\zeta_r^2 + \zeta_i^2 \leq 2\zeta^2$
[$|\zeta_r|, |\zeta_i| \leq \zeta$ ((L1), (L2))]

(L5) $\Rightarrow\ |e|^2 \leq 2\zeta^2$
[(L3), (L4)]

(L6) $\Rightarrow$ $|a \oplus b - e - (a+b)|^2 = (\operatorname{Re} u_r)^2 + (\operatorname{Im} u_i)^2$

[(L1), (L2); $|x+iy|^2 = x^2+y^2$ (Fact A.41, item 1)]

(L7) $(\operatorname{Re} u_r)^2 + (\operatorname{Im} u_i)^2 \le u^2|a+b|^2$

[$|u_r|, |u_i| \le u$ ((L1), (L2)); $\mathrm{Re}^2 + \mathrm{Im}^2 = |a+b|^2$ (Fact A.41, item 1)]

(L8) $\Rightarrow$ $|a \oplus b - e - (a+b)|^2 \le u^2|a+b|^2$

[(L6), (L7)]

(L9) $\Rightarrow$ $|a \oplus b - e - (a+b)| \le u|a+b|$

[square root of (L8)]

(L10) $\Rightarrow$ $|e| \le \sqrt{2}\,\zeta$

[square root of (L5)]

(I1)

Lemma B.1	This proof
p	$a \oplus b - e$ (the proof's block)
x	$a+b$
c	u
$c \ge 0$	$u \ge 0$ (Definition A.4)
$x, p \in \mathbb{C}$	$a, b \in C_{\mathcal{F}}$ (the statement); Definition A.8
$\lvert p - x\rvert \le c\lvert x\rvert$	(L9)
Its conclusion: $\lvert\delta(p,x)\rvert \le c,\ p = x(1+\delta(p,x))$	

(L11) $\Rightarrow$ $\exists\,\delta \in \mathbb{C},\ |\delta| \le u :\ a \oplus b = (a+b)(1+\delta) + e$

[(I1)]

(L12) $\Rightarrow$ $(a \oplus b)\ \mathcal{I}\left(u^{\pm}, (\sqrt{2}\,\zeta)^{\pm}\right)\ (a+b)$

[Definition A.10 at $u_\circ := \delta$, $\zeta_\circ := e$, the discs of Definition A.9; (L10), (L11)]

(L13) $\Rightarrow$ item 1

[(L12)]

□ (item 1)

Proof of item 2.

(L14) $-b \in C_{\mathcal{F}}$

[Definition A.4, item 6: $\mathrm{fl}(-x) = -x$, at $-b = -b_r - ib_i$]

(L15) $a \ominus b = a \oplus (-b)$

[Definition A.8]

(I2)

Lemma B.2, item 1	This proof
Shared: a	
b	$-b$
$a, b \in C_{\mathcal{F}}$	$a \in C_{\mathcal{F}}$ (item 2); (L14)
Its item 1: $\forall a, b \in C_{\mathcal{F}} : (a \oplus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\zeta^{\pm}\right)\ (a+b)$	

(L16) $\Rightarrow$ $\exists\,\delta', e' \in \mathbb{C},\ |\delta'| \le u,\ |e'| \le \sqrt{2}\,\zeta :\ a \ominus b = (a + (-b))(1+\delta') + e'$

[(I2); (L14), (L15); Definition A.10]

(L17) $a + (-b) = a - b$

[expand]

(L18) $\Rightarrow$ $\exists\,\delta', e' \in \mathbb{C},\ |\delta'| \le u,\ |e'| \le \sqrt{2}\,\zeta :\ a \ominus b = (a-b)(1+\delta') + e'$

[(L16), (L17)]

(L19) $\Rightarrow$ $(a \ominus b)\ \mathcal{I}\left(u^{\pm}, (\sqrt{2}\,\zeta)^{\pm}\right)\ (a-b)$

[Definition A.10 at $u_\circ := \delta'$, $\zeta_\circ := e'$, the discs of Definition A.9; (L18)]

(L20) $\Rightarrow$ item 2

[(L19)]

□ (item 2)

Proof of item 3.

(L21) $\exists\, u_{rr}, u_{ii}, u_{\mathrm{Re}}, \zeta_{rr}, \zeta_{ii}, \zeta_{\mathrm{Re}} \in \mathbb{R},\ |u_\cdot| \le u,\ |\zeta_\cdot| \le \zeta :\ \widetilde{\mathrm{Re}} = (a_r b_r(1+u_{rr}) + \zeta_{rr} - a_i b_i(1+$

$u_{ii}) - \zeta_{ii})(1 + u_{\mathrm{Re}}) + \zeta_{\mathrm{Re}}$

[Def. A.4: $\mathrm{fl}(x \circ y) = (x \circ y)(1 + u_\circ) + \zeta_\circ$, $|u_\circ| \le u$, $|\zeta_\circ| \le \zeta$, for $\times$, $\times$, $-$]

(L22) $\Rightarrow$ $|E_r| \le (3 + 2u)\,\zeta$

[E_r (the proof's block); $|\zeta_\cdot| \le \zeta$ ((L21)); $|1 + u_{\mathrm{Re}}| \le 1 + u$ ((L21); Fact A.41, item 1); $|x + y| \le |x| + |y|$ (Fact A.41, item 1)]

(L23) $\Rightarrow$ $\widetilde{\mathrm{Re}} - E_r - \mathrm{Re} = \mathrm{Re}\, u_{\mathrm{Re}} + (a_r b_r u_{rr} - a_i b_i u_{ii})(1 + u_{\mathrm{Re}})$

[(L21), (L22); $\mathrm{Re} = a_r b_r - a_i b_i$; $x(1 + t) = x + xt$]

(L24) $\Rightarrow$ $|\widetilde{\mathrm{Re}} - E_r - \mathrm{Re}| \le |\mathrm{Re}||u_{\mathrm{Re}}| + (|a_r||b_r||u_{rr}| + |a_i||b_i||u_{ii}|)(1 + |u_{\mathrm{Re}}|)$

[$|x + y| \le |x| + |y|$ (Fact A.41, item 1); $|xy| = |x||y|$ (Fact A.41, item 1)]

(L25) $\Rightarrow$ $|\widetilde{\mathrm{Re}} - E_r - \mathrm{Re}| \le u|\mathrm{Re}| + u(1 + u)(|a_r||b_r| + |a_i||b_i|)$

[$|u_\cdot| \le u$ ((L21))]

(L26) $\Rightarrow$ $|\widetilde{\mathrm{Re}} - E_r - \mathrm{Re}| \le u|a||b| + u(1 + u)|a||b|$

[$|\mathrm{Re}\, z| \le |z|$, $|ab| = |a||b|$ (Fact A.41, item 1); $|a_r||b_r| + |a_i||b_i| \le |a||b|$ (Fact A.41, item 4)]

(L27) $\Rightarrow$ $|\widetilde{\mathrm{Re}} - E_r - \mathrm{Re}| \le u(2 + u)|a||b|$

[$u + u(1 + u) = u(2 + u)$]

(L28) $\exists\, u_{ri}, u_{ir}, u_{\mathrm{Im}}, \zeta_{ri}, \zeta_{ir}, \zeta_{\mathrm{Im}} \in \mathbb{R},\ |u_\cdot| \le u,\ |\zeta_\cdot| \le \zeta :\ \widetilde{\mathrm{Im}} = (a_r b_i(1 + u_{ri}) + \zeta_{ri} + a_i b_r(1 + u_{ir}) + \zeta_{ir})(1 + u_{\mathrm{Im}}) + \zeta_{\mathrm{Im}}$

[Def. A.4: $\mathrm{fl}(x \circ y) = (x \circ y)(1 + u_\circ) + \zeta_\circ$, $|u_\circ| \le u$, $|\zeta_\circ| \le \zeta$, for $\times$, $\times$, $+$]

(L29) $\Rightarrow$ $|E_i| \le (3 + 2u)\,\zeta$

[E_i (the proof's block); $|\zeta_\cdot| \le \zeta$ ((L28)); $|1 + u_{\mathrm{Im}}| \le 1 + u$ ((L28); Fact A.41, item 1); $|x + y| \le |x| + |y|$ (Fact A.41, item 1)]

(L30) $\Rightarrow$ $|\widetilde{\mathrm{Im}} - E_i - \mathrm{Im}| \le u(2 + u)|a||b|$

[(L23) to (L27) at $\mathrm{Im} = a_r b_i + a_i b_r$, with $(u_{ri}, u_{ir}, u_{\mathrm{Im}}, \zeta_{ri}, \zeta_{ir}, \zeta_{\mathrm{Im}})$ in place of $(u_{rr}, u_{ii}, u_{\mathrm{Re}}, \zeta_{rr}, \zeta_{ii}, \zeta_{\mathrm{Re}})$]

(L31) $|e|^2 \le 2(3 + 2u)^2\zeta^2$

[(L22), (L29); e (the proof's block); $|x + iy|^2 = x^2 + y^2$ (Fact A.41, item 1)]

(L32) $|a \otimes b - e - ab|^2 = (\widetilde{\mathrm{Re}} - E_r - \mathrm{Re})^2 + (\widetilde{\mathrm{Im}} - E_i - \mathrm{Im})^2$

[Def. A.8: $a \otimes b = \widetilde{\mathrm{Re}} + i\,\widetilde{\mathrm{Im}}$; $|x + iy|^2 = x^2 + y^2$ (Fact A.41, item 1)]

(L33) $(\widetilde{\mathrm{Re}} - E_r - \mathrm{Re})^2 + (\widetilde{\mathrm{Im}} - E_i - \mathrm{Im})^2 \le 2\,(u(2 + u)|a||b|)^2$

[(L27), (L30)]

(L34) $\Rightarrow$ $|a \otimes b - e - ab|^2 \le 2\,(u(2 + u)|a||b|)^2$

[(L32), (L33)]

(L35) $\Rightarrow$ $|e| \le \sqrt{2}(3 + 2u)\,\zeta$

[square root of (L31)]

(L36) $\Rightarrow$ $|e| \le k_B\,\zeta$

[(L35); k_B (the statement)]

(L37) $\Rightarrow$ $|a \otimes b - e - ab| \le \sqrt{2}\,u(2 + u)|a||b|$

[square root of (L34)]

(I3)

Lemma B.1	This proof
p	$a \otimes b - e$ (the proof's block)
x	ab
c	$\sqrt{2}\,u(2 + u)$
$c \ge 0$	$u \ge 0$ (Definition A.4)
$x, p \in \mathbb{C}$	$a, b \in C_{\mathcal{F}}$ (the statement); Definition A.8
$\lvert p - x\rvert \le c\lvert x\rvert$	(L37); $\lvert ab\rvert = \lvert a\rvert\lvert b\rvert$ (Fact A.41, item 1)
Its conclusion: $\lvert\delta(p, x)\rvert \le c,\ p = x(1 + \delta(p, x))$	

(L38) $\Rightarrow$ $\exists\, \delta \in \mathbb{C},\ |\delta| \le \sqrt{2}\,u(2 + u) :\ a \otimes b = ab(1 + \delta) + e$

[(I3)]

(L39) $\Rightarrow$ $(a \otimes b)\ \mathcal{I}\left((\sqrt{2}\,u(2 + u))^{\pm}, (k_B\,\zeta)^{\pm}\right) ab$

[Definition A.10 at $u_\circ := \delta$, $\zeta_\circ := e$, the discs of Definition A.9; (L36), (L38)]

(L40) $\Rightarrow$ item 3

[(L39)]

□ (item 3)

Proof of item 4.

(L41) $\exists\, u_r, \zeta_r \in \mathbb{R},\ |u_r| \le u,\ |\zeta_r| \le \zeta :\ \widetilde{a}_r = a_r(1+u_r) + \zeta_r$
[the hypotheses of item 4: Definition A.10 on $\mathbb{R}$, Definition A.9]

(L42) $\exists\, u_i, \zeta_i \in \mathbb{R},\ |u_i| \le u,\ |\zeta_i| \le \zeta :\ \widetilde{a}_i = a_i(1+u_i) + \zeta_i$
[the hypotheses of item 4: Definition A.10 on $\mathbb{R}$, Definition A.9]

(L43) $\Rightarrow\ |e| \le \sqrt{2}\,\zeta$
[e (the proof's block); $|x+iy|^2 = x^2+y^2$ (Fact A.41, item 1); $|\zeta_r|, |\zeta_i| \le \zeta$ ((L41), (L42))]

(L44) $|\widetilde{a} - e - a|^2 = (a_r u_r)^2 + (a_i u_i)^2$
[(L41), (L42); $|x+iy|^2 = x^2+y^2$ (Fact A.41, item 1)]

(L45) $(a_r u_r)^2 + (a_i u_i)^2 \le u^2(a_r^2 + a_i^2)$
[$|u_r|, |u_i| \le u$ ((L41), (L42))]

(L46) $u^2(a_r^2 + a_i^2) = u^2$
[$|a| = 1$ (the statement)]

(L47) $\Rightarrow\ |\widetilde{a} - e - a|^2 \le u^2$
[(L44), (L45), (L46)]

(L48) $\Rightarrow\ |\widetilde{a} - e - a| \le u$
[square root]

	Lemma B.1	This proof
	p	$\widetilde{a} - e$ (the proof's block)
	x	a
	c	u
(I4)	$\delta(p, x)$	δ'
	$c \ge 0$	$u \ge 0$ (Definition A.4)
	$x, p \in \mathbb{C}$	$a \in \mathbb{C}$, $\widetilde{a} \in C_{\mathcal{F}}$ (the statement); Definition A.8
	$\lvert p - x\rvert \le c\lvert x\rvert$	(L48); $\lvert a\rvert = 1$ (the statement)
	Its conclusion: $\lvert\delta(p,x)\rvert \le c,\ p = x(1+\delta(p,x))$	

(L49) $\Rightarrow\ \exists\, \delta \in \mathbb{C},\ |\delta| \le u + \sqrt{2}\,\zeta :\ \widetilde{a} = a(1+\delta)$
[(I4); (L43); $\delta := \delta' + e/a$; $|a| = 1$ (the statement); $|x+y| \le |x| + |y|$ (Fact A.41, item 1)]

(L50) $\Rightarrow\ \widetilde{a}\ \mathcal{I}\left(u^{\pm} + \sqrt{2}\,\zeta^{\pm}, 0\right) a$
[Definition A.10 at $u_\circ := \delta$, $\zeta_\circ := 0$, the ball of Definition A.9; (L49)]

(L51) $\Rightarrow$ item 4
[(L50)]

□ (item 4)

Proof of item 5.

(L52) $\forall k < m\ \exists\, \delta_k, e_k \in \mathbb{C},\ |\delta_k| \le \sqrt{2}u(2+u),\ |e_k| \le k_B\,\zeta :\ \widetilde{p}_k = (fg)_k(1+\delta_k) + e_k$
[item 3, $\forall k < m$]

(L53) $\Rightarrow\ \forall k < m :\ |\widetilde{p}_k - (fg)_k| \le \sqrt{2}u(2+u)|(fg)_k| + k_B\,\zeta$
[(L52); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$]

(L54) $\Rightarrow\ \|\widetilde{p} - fg\| \le \|(\sqrt{2}u(2+u)|(fg)_k|)_k\| + \|(k_B\,\zeta)_k\|$
[(L53); $\|x\|^2 = \sum_k |x_k|^2$ (Fact A.41, its lead) nondecreasing in each $|x_k|$ (Fact A.41, item 5); $\|x+y\| \le \|x\| + \|y\|$ over k (Fact A.41, item 3)]

(L55) $\|(\sqrt{2}u(2+u)|(fg)_k|)_k\| + \|(k_B\,\zeta)_k\| = \sqrt{2}u(2+u)\|fg\| + k_B\,\zeta\sqrt{m}$
[$\sum_k (k_B\,\zeta)^2 = m(k_B\,\zeta)^2$; square root]

(L56) $\Rightarrow\ \|\widetilde{p} - fg\| \le \sqrt{2}u(2+u)\|fg\| + k_B\,\zeta\sqrt{m}$
[(L54), (L55)]

(L57) $\Rightarrow\ \widetilde{p}\ \mathcal{N}\left(\sqrt{2}\,u(2+u), k_B\,\zeta\sqrt{m}\right) fg$
[Definition A.11 with the norm of the statement; (L56)]

(L58) $\Rightarrow$ item 5

[(L57)]

□ (item 5)

B.3 The split butterfly

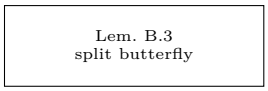


Figure 39: Dependencies, Section B.3.

Lemma B.3 (The split butterfly, the even half [to table])**.** *The even half of a split butterfly is its exact value within u relatively and $(\sqrt{2}/2)\,\zeta$ absolutely. Let:*

- $a \in C_{\mathcal{F}}$*;*
- $b \in C_{\mathcal{F}}$*.*

Define:

- $f_0 := (a+b)/2$ *(split (Algorithm 2), line 5);*
- $\widetilde{f_0} := \mathrm{fl}(\mathrm{fl}(a_r + b_r)/2) + i\ \mathrm{fl}(\mathrm{fl}(a_i + b_i)/2)$*, the value* split *(Algorithm 2) computes at line 4.*

We have

$$\forall a, b \in C_{\mathcal{F}}\ \exists\, \delta_0, e_0 \in \mathbb{C},\ |\delta_0| \le u,\ |e_0| \le (\sqrt{2}/2)\,\zeta : \quad \widetilde{f_0} = f_0(1+\delta_0) + e_0.$$

Proof.

DEFINES $s_r := a_r + b_r$, $s_i := a_i + b_i$

DEFINES $e_0 := (\zeta_r + i\zeta_i)/2$, ζ_r, ζ_i those of (L1), (L2)

(L1) $\exists\, u_r, \zeta_r \in \mathbb{R},\ |u_r| \le u,\ |\zeta_r| \le \zeta :\ \mathrm{fl}(\mathrm{fl}(a_r + b_r)/2) = (s_r(1+u_r) + \zeta_r)/2$

[Definition A.4, item 4, at $(x, y) := (a_r, b_r)$; s_r (the proof's block)]

(L2) $\exists\, u_i, \zeta_i \in \mathbb{R},\ |u_i| \le u,\ |\zeta_i| \le \zeta :\ \mathrm{fl}(\mathrm{fl}(a_i + b_i)/2) = (s_i(1+u_i) + \zeta_i)/2$

[Definition A.4, item 4, at $(x, y) := (a_i, b_i)$; s_i (the proof's block)]

(L3) $\Rightarrow\ \widetilde{f_0} - e_0 - f_0 = (s_r u_r + i s_i u_i)/2$

[(L1), (L2); $\widetilde{f_0}$, f_0 (the statement); e_0, s_r, s_i (the proof's block)]

(L4) $|s_r u_r + i s_i u_i|^2 = (s_r u_r)^2 + (s_i u_i)^2$

[$|x+iy|^2 = x^2 + y^2$ (Fact A.41, item 1)]

(L5) $(s_r u_r)^2 + (s_i u_i)^2 \le u^2 |a+b|^2$

[$|u_r|, |u_i| \le u$ ((L1), (L2)); $s_r^2 + s_i^2 = |a+b|^2$ (Fact A.41, item 1)]

(L6) $\Rightarrow\ |\widetilde{f_0} - e_0 - f_0| \le u|f_0|$

[square root of (L4), (L5), halved; (L3); $f_0 = (a+b)/2$ (the statement)]

(L7) $|e_0|^2 = (\zeta_r^2 + \zeta_i^2)/4$

[e_0 (the proof's block); $|x+iy|^2 = x^2 + y^2$ (Fact A.41, item 1)]

(L8) $(\zeta_r^2 + \zeta_i^2)/4 \le \zeta^2/2$

[$|\zeta_r|, |\zeta_i| \le \zeta$ ((L1), (L2))]

(L9) $\Rightarrow\ |e_0| \le (\sqrt{2}/2)\,\zeta$

[square root of (L7), (L8)]

	Lemma B.1	This proof
	p	$\widetilde{f}_0 - e_0$ (the proof's block)
	x	f_0
(I1)	c	u
	$c \geq 0$	$u \geq 0$ (Definition A.4)
	$x, p \in \mathbb{C}$	$a, b \in C_{\mathcal{F}}$ (the statement); Definition A.8
	$\lvert p - x\rvert \leq c\lvert x\rvert$	(L6)
	Its conclusion: $\lvert\delta(p,x)\rvert \leq c,\ p = x(1+\delta(p,x))$	

(L10) $\Rightarrow\ \exists\, \delta_0 \in \mathbb{C},\ |\delta_0| \leq u :\ \widetilde{f}_0 = f_0(1+\delta_0) + e_0$

[(I1)]

(L11) $\Rightarrow$ the statement

[(L9), (L10)]

□

B.4 The tail of a sum of discrete Gaussian offsets



Figure 40: Dependencies, Section B.4.

Structure. Lemma B.4 states the moment-generating function of a discrete Gaussian's offset; Lemma B.5 the tail of a weighted sum of offsets.

Lemma B.4 (Moment-generating function of a discrete Gaussian's offset [to table])**.** *Summed against a discrete Gaussian, the exponential of the offset is the continuous Gaussian's moment-generating function times a ratio of two normalizers. Let:*

- $s > 0$;
- $c \in \mathbb{R}$;
- $\ell \in \mathbb{R}$.

Define:

- $\rho_{s,c}(x) := e^{-(x-c)^2/(2s^2)}$ *and* $\rho_{s,c}(\mathbb{Z}) := \sum_{x\in\mathbb{Z}} \rho_{s,c}(x)$ *(Definition A.2);*
- $D_{\mathbb{Z},s,c}(z) := \rho_{s,c}(z)/\rho_{s,c}(\mathbb{Z})$ *(Definition A.2);*
- $M_{s,c}(\ell) := \sum_{z\in\mathbb{Z}} e^{\ell(z-c)} D_{\mathbb{Z},s,c}(z)$.

Then the sum moves the Gaussian's center by ℓs^2, and the normalizer bounds bound it:

1. $\sum_{z\in\mathbb{Z}} e^{\ell(z-c)}\rho_{s,c}(z) = e^{\ell^2 s^2/2}\rho_{s,\,c+\ell s^2}(\mathbb{Z})$;
2. *Let $\epsilon \in [0,1)$. Assume:*

   (A1) $\forall c' \in \mathbb{R} :\ \rho_{s,c'}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\, s, (1+\epsilon)\sqrt{2\pi}\, s]$.

   Then $M_{s,c}(\ell) \leq \frac{1+\epsilon}{1-\epsilon} e^{\ell^2 s^2/2}$.

Proof.

DEFINES $m := c + \ell s^2$

Proof of item 1.

(L1) $\forall z \in \mathbb{Z} :\ \ell(z-c) - (z-c)^2/(2s^2) = \ell^2 s^2/2 - (z-m)^2/(2s^2)$

[expand at $m = c + \ell s^2$ (the proof's block)]

(L2) $\Rightarrow\ \forall z \in \mathbb{Z} :\ e^{\ell(z-c)}\rho_{s,c}(z) = e^{\ell^2 s^2/2}\rho_{s,m}(z)$

[(L1); Definition A.2, item 1, at (s,c) and at (s,m); $e^x e^y = e^{x+y}$ (Fact A.41, item 12)]

(L3) $\sum_{z\in\mathbb{Z}} \rho_{s,m}(z) = \rho_{s,m}(\mathbb{Z})$
[Fact A.45, item 6, at (s, m)]

(L4) $\Rightarrow$ $\sum_{z\in\mathbb{Z}} e^{\ell(z-c)}\rho_{s,c}(z) = e^{\ell^2 s^2/2}\rho_{s,m}(\mathbb{Z})$
[(L2), (L3); Fact A.45, item 9, at $a := e^{\ell^2 s^2/2}$, $b := 0$ and $f = g := \rho_{s,m}$ on $\mathbb{Z}$]

(L5) $\Rightarrow$ item 1
[(L4)]

□ (item 1)

Proof of item 2.

(L6) $\rho_{s,c}(\mathbb{Z}) \geq (1-\epsilon)\sqrt{2\pi}\, s$
[assumption A1 at $c' := c$]

(L7) $(1-\epsilon)\sqrt{2\pi}\, s > 0$
[$\epsilon < 1$ and $s > 0$ (the statement)]

(L8) $\rho_{s,m}(\mathbb{Z}) \leq (1+\epsilon)\sqrt{2\pi}\, s$
[assumption A1 at $c' := m$]

(L9) $M_{s,c}(\ell) = \sum_{z\in\mathbb{Z}} e^{\ell(z-c)}\rho_{s,c}(z)/\rho_{s,c}(\mathbb{Z})$
[$M_{s,c}$ (the statement); $D_{\mathbb{Z},s,c}(z) = \rho_{s,c}(z)/\rho_{s,c}(\mathbb{Z})$ (Definition A.2, item 2)]

(L10) $\Rightarrow$ $M_{s,c}(\ell) = e^{\ell^2 s^2/2}\rho_{s,m}(\mathbb{Z})/\rho_{s,c}(\mathbb{Z})$
[(L9), (L4); Fact A.45, item 9, at $a := 1/\rho_{s,c}(\mathbb{Z})$, $b := 0$, its denominator positive by (L6), (L7)]

(L11) $\Rightarrow$ $M_{s,c}(\ell) \leq e^{\ell^2 s^2/2}(1+\epsilon)\sqrt{2\pi}\, s/\rho_{s,c}(\mathbb{Z})$
[(L10), (L8); $e^{\ell^2 s^2/2} > 0$ (Fact A.41, item 12); Fact A.41, item 26]

(L12) $1/\rho_{s,c}(\mathbb{Z}) \leq 1/((1-\epsilon)\sqrt{2\pi}\, s)$
[(L6), (L7); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L13) $\Rightarrow$ $M_{s,c}(\ell) \leq \frac{1+\epsilon}{1-\epsilon}\, e^{\ell^2 s^2/2}$
[(L11), (L12); Fact A.41, item 26]

(L14) $\Rightarrow$ item 2
[(L13)]

□ (item 2)

Lemma B.5 (Tail bound on a weighted sum of offsets [to table])**.** *A weighted sum of terms sampled in sequence, each with a Gaussian moment-generating function up to the factor κ given the samples before it, has a Gaussian tail of variance V up to the factor $2\kappa^N$. Let:*

- $N \in \mathbb{Z}_{>0}$ *(Definition A.1);*
- $P_j(\cdot \mid y_{<j})$, $j \leq N$, *a probability measure on $\mathbb{Z}$ for every $y_{<j} \in \mathbb{Z}^{j-1}$;*
- $g_j : \mathbb{Z}^j \to \mathbb{R}$, $j \leq N$;
- $a = (a_j)_{j\leq N} \in \mathbb{R}^N$;
- $s = (s_j)_{j\leq N} \in (0,\infty)^N$;
- $\kappa \geq 1$;
- $t \geq 0$.

Define:

- $P(y) := \prod_{j\leq N} P_j(y_j \mid y_{<j})$ *for $y \in \mathbb{Z}^N$ (Fact A.45, item 1);*
- $P(A) := \sum_{y\in A} P(y)$ *for $A \subseteq \mathbb{Z}^N$;*
- $X(y) := \sum_{j\leq N} a_j g_j(y_{\leq j})$ *for $y \in \mathbb{Z}^N$;*
- $V := \sum_{j\leq N} a_j^2 s_j^2$.

Assume:

(A1) $\forall j \leq N\ \forall y_{<j} \in \mathbb{Z}^{j-1}\ \forall \ell \in \mathbb{R}:\ \sum_{y_j\in\mathbb{Z}} P_j(y_j \mid y_{<j})\, e^{\ell g_j(y_{\leq j})} \leq \kappa\, e^{\ell^2 s_j^2/2}$;

(A2) $V > 0$.

Then the moment-generating function and the tail of X are bounded:

1. $\forall \ell \in \mathbb{R}:\ \sum_{y\in\mathbb{Z}^N} P(y)\, e^{\ell X(y)} \leq \kappa^N e^{\ell^2 V/2}$;

2. $P(\{y \in \mathbb{Z}^N : |X(y)| > t\}) \le 2\kappa^N e^{-t^2/(2V)}$.

Proof.

DEFINES $X_k(y_{\le k}) := \sum_{j\le k} a_j g_j(y_{\le j})$ for $k \le N$ and $y_{\le k} \in \mathbb{Z}^k$, $\mathbb{Z}^0 := \{()\}$; $X_0(()) = 0$, the empty sum

$V_k := \sum_{j\le k} a_j^2 s_j^2$ for $k \le N$; $V_0 = 0$, the empty sum

$E_k(\ell) := \sum_{y_{\le k}\in\mathbb{Z}^k} \prod_{j\le k} P_j(y_j \mid y_{<j})\, e^{\ell X_k(y_{\le k})}$ for $k \le N$ and $\ell \in \mathbb{R}$

$\ell_t := t/V$

Proof of item 1.

(L1) $\forall \ell \in \mathbb{R}:\ E_0(\ell) = e^{\ell X_0(())}$

[E_0, $\mathbb{Z}^0 = \{()\}$ (the proof's block); expand]

(L2) $\forall \ell \in \mathbb{R}:\ e^{\ell X_0(())} = 1$

[$X_0(()) = 0$ (the proof's block); expand]

(L3) $\forall \ell \in \mathbb{R}:\ \kappa^0 e^{\ell^2 V_0/2} = 1$

[$V_0 = 0$ (the proof's block); expand]

(L4) $\Rightarrow\ \forall \ell \in \mathbb{R}:\ E_0(\ell) = \kappa^0 e^{\ell^2 V_0/2}$

[(L1), (L2), (L3)]

(L5) $\forall k < N\ \forall \ell \in \mathbb{R}:\ E_{k+1}(\ell) = \sum_{y_{\le k}\in\mathbb{Z}^k} \sum_{y_{k+1}\in\mathbb{Z}} \prod_{j\le k+1} P_j(y_j \mid y_{<j})\, e^{\ell X_{k+1}(y_{\le k+1})}$

[E_{k+1} (the proof's block); Fact A.45, item 11, at $Y := \mathbb{Z}^k$ and $Y' := \mathbb{Z}$]

(L6) $\forall k < N\ \forall y_{\le k+1} \in \mathbb{Z}^{k+1}:\ \prod_{j\le k+1} P_j(y_j \mid y_{<j}) = \prod_{j\le k} P_j(y_j \mid y_{<j})\, P_{k+1}(y_{k+1} \mid y_{\le k})$

[expand]

(L7) $\forall k < N\ \forall y_{\le k+1} \in \mathbb{Z}^{k+1}\ \forall \ell \in \mathbb{R}:\ e^{\ell X_{k+1}(y_{\le k+1})} = e^{\ell X_k(y_{\le k})}\, e^{\ell a_{k+1} g_{k+1}(y_{\le k+1})}$

[$X_{k+1}(y_{\le k+1}) = X_k(y_{\le k}) + a_{k+1} g_{k+1}(y_{\le k+1})$ (the proof's block); $e^x e^y = e^{x+y}$ (Fact A.41, item 12)]

(L8) $\Rightarrow\ \forall k < N\ \forall \ell \in \mathbb{R}:\ E_{k+1}(\ell) = \sum_{y_{\le k}\in\mathbb{Z}^k} \prod_{j\le k} P_j(y_j \mid y_{<j})\, e^{\ell X_k(y_{\le k})} \sum_{y_{k+1}\in\mathbb{Z}} P_{k+1}(y_{k+1} \mid y_{\le k})\, e^{\ell a_{k+1} g_{k+1}(y_{\le k+1})}$

[(L5), (L6), (L7); the factors without y_{k+1} out of the inner sum (Fact A.45, item 9, linearity)]

(L9) $\forall k < N\ \forall y_{\le k} \in \mathbb{Z}^k\ \forall \ell \in \mathbb{R}:\ \sum_{y_{k+1}\in\mathbb{Z}} P_{k+1}(y_{k+1} \mid y_{\le k})\, e^{\ell a_{k+1} g_{k+1}(y_{\le k+1})} \le \kappa\, e^{\ell^2 a_{k+1}^2 s_{k+1}^2/2}$

[assumption A1 at $j := k+1$ and $\ell := \ell a_{k+1}$]

(L10) $\Rightarrow\ \forall k < N\ \forall \ell \in \mathbb{R}:\ E_{k+1}(\ell) \le \kappa\, e^{\ell^2 a_{k+1}^2 s_{k+1}^2/2} E_k(\ell)$

[(L8), (L9); Fact A.45, item 9; E_k (the proof's block)]

(L11) $\forall k < N\ \forall \ell \in \mathbb{R}:\ E_k(\ell) \le \kappa^k e^{\ell^2 V_k/2} \Rightarrow\ E_{k+1}(\ell) \le \kappa\, e^{\ell^2 a_{k+1}^2 s_{k+1}^2/2} \kappa^k e^{\ell^2 V_k/2}$

[(L10); $\kappa\, e^{\ell^2 a_{k+1}^2 s_{k+1}^2/2} \ge 0$ (Fact A.41, item 12); Fact A.41, item 26]

(L12) $\forall k < N\ \forall \ell \in \mathbb{R}:\ \kappa\, e^{\ell^2 a_{k+1}^2 s_{k+1}^2/2} \kappa^k e^{\ell^2 V_k/2} = \kappa^{k+1} e^{\ell^2 V_{k+1}/2}$

[$V_{k+1} = V_k + a_{k+1}^2 s_{k+1}^2$ (the proof's block); $e^x e^y = e^{x+y}$ (Fact A.41, item 12)]

(L13) $\Rightarrow\ \forall k < N\ \forall \ell \in \mathbb{R}:\ E_k(\ell) \le \kappa^k e^{\ell^2 V_k/2} \Rightarrow\ E_{k+1}(\ell) \le \kappa^{k+1} e^{\ell^2 V_{k+1}/2}$

[(L11), (L12)]

(L14) $\Rightarrow\ \forall k \le N\ \forall \ell \in \mathbb{R}:\ E_k(\ell) \le \kappa^k e^{\ell^2 V_k/2}$

[induction on k: (L4) the base; (L13) the step]

(L15) $\forall \ell \in \mathbb{R}:\ E_N(\ell) = \sum_{y\in\mathbb{Z}^N} P(y)\, e^{\ell X(y)}$

[E_N and $X_N = X$ (the proof's block); P (the statement)]

(L16) $\Rightarrow\ \forall \ell \in \mathbb{R}:\ \sum_{y\in\mathbb{Z}^N} P(y)\, e^{\ell X(y)} \le \kappa^N e^{\ell^2 V/2}$

[(L14) at $k := N$, (L15); $V_N = V$ (the proof's block)]

(L17) $\Rightarrow$ item 1

[(L16)]

□ (item 1)

Proof of item 2.

(L18) $\ell_t \ge 0$

[$t \ge 0$ (the statement); assumption A2; ℓ_t (the proof's block)]

(L19) $\forall y \in \mathbb{Z}^N,\ X(y) > t:\ e^{\ell_t(X(y)-t)} \geq 1$

[(L18); Fact A.41, item 27, at $x := \ell_t(X(y) - t)$]

(L20) $\Rightarrow\ P(\{y : X(y) > t\}) \leq e^{-\ell_t t} \sum_{y\in\mathbb{Z}^N} P(y)\, e^{\ell_t X(y)}$

[(L19); $P(y)\, e^{\ell_t(X(y)-t)} \geq 0$ (Fact A.41, item 12); Fact A.45, item 9, comparison and linearity; Fact A.41, item 12]

(L21) $\Rightarrow\ P(\{y : X(y) > t\}) \leq \kappa^N e^{-\ell_t t+\ell_t^2 V/2}$

[(L20), item 1 at $\ell := \ell_t$; $e^x e^y = e^{x+y}$ (Fact A.41, item 12)]

(L22) $-\ell_t t + \ell_t^2 V/2 = -t^2/(2V)$

[$\ell_t = t/V$ (the proof's block); expand]

(L23) $\Rightarrow\ P(\{y : X(y) > t\}) \leq \kappa^N e^{-t^2/(2V)}$

[(L21), (L22)]

(L24) $\forall y \in \mathbb{Z}^N,\ X(y) < -t:\ e^{-\ell_t(X(y)+t)} \geq 1$

[(L18); Fact A.41, item 27, at $x := -\ell_t(X(y) + t)$]

(L25) $\Rightarrow\ P(\{y : X(y) < -t\}) \leq e^{-\ell_t t} \sum_{y\in\mathbb{Z}^N} P(y)\, e^{-\ell_t X(y)}$

[(L24); as at (L20)]

(L26) $\Rightarrow\ P(\{y : X(y) < -t\}) \leq \kappa^N e^{-t^2/(2V)}$

[(L25), item 1 at $\ell := -\ell_t$; (L22) at $\ell_t^2 := (-\ell_t)^2$]

(L27) $\{y : |X(y)| > t\} = \{y : X(y) > t\} \cup \{y : X(y) < -t\}$

[expand]

(L28) $\Rightarrow\ P(\{y : |X(y)| > t\}) \leq 2\kappa^N e^{-t^2/(2V)}$

[(L23), (L26), (L27); Fact A.45, item 5]

(L29) $\Rightarrow$ item 2

[(L28)]

□ (item 2)

C The arithmetic and harmonic means

This appendix proves the bounds on compositions of the arithmetic and harmonic means. Lemma C.1 states the pure compositions; Lemma C.2 the mixed ones.

Both lemmas need balanced compositions. Both lemmas rest on the compositions being balanced: every argument of a $C \in \mathcal{C}_k$ reaches the composition's root through exactly k two-argument means, so the arguments are 2^k and each carries the same weight. An unbalanced composition weights its arguments unequally, and both lemmas fail for it: $\mathrm{AM}(\mathrm{AM}(1,1),4) = 2.5$ where $\mathrm{AM}_{\mathrm{all}}(1,1,4) = 2$, and $\mathrm{HM}(1,\mathrm{HM}(100,\ldots,100)) = \mathrm{HM}(1,100) = 200/101$ where $\mathrm{HM}_{\mathrm{all}}$ of one 1 and ninety-nine 100s is $100/1.99$.

How each statement is verified. Table 14 lists how each lemma of this appendix is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma C.1	✓				
Lemma C.2	✓				

Table 14: Appendix C: how each lemma is verified.

C.1 Compositions of the arithmetic and harmonic means

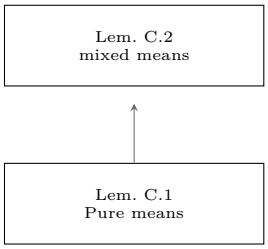


Figure 41: Dependencies, Section C.1.

Lemma C.1 (Pure compositions of the means [to table])**.** *The arithmetic composition is the arithmetic mean over all values, and the harmonic one the harmonic mean. Let:*

- $k \geq 0$;
- $a_1, \ldots, a_{2^k} > 0$.

Define:

- $m := 2^k$;
- $\mathrm{AM}_{\mathrm{all}} := (1/m) \sum_i a_i$, *the arithmetic mean over all values (Definition A.46);*
- $\mathrm{HM}_{\mathrm{all}} := m / \sum_i a_i^{-1}$, *the harmonic mean over all values (Definition A.46);*
- $C_{\mathrm{AM}} \in \mathcal{C}_k$, *with* $M = \mathrm{AM}$ *and* $C_L = C_R = C_{\mathrm{AM}}$ *at every level (Definition A.46);*
- $C_{\mathrm{HM}} \in \mathcal{C}_k$, *with* $M = \mathrm{HM}$ *and* $C_L = C_R = C_{\mathrm{HM}}$ *at every level (Definition A.46).*

We have

$$C_{\mathrm{AM}}(a_1, \ldots, a_m) = \mathrm{AM}_{\mathrm{all}}, \qquad C_{\mathrm{HM}}(a_1, \ldots, a_m) = \mathrm{HM}_{\mathrm{all}}\,.$$

Proof.

DEFINES $\mathrm{AM}(a,b) := (a+b)/2$ and $\mathrm{HM}(a,b) := 2ab/(a+b)$ (Definition A.46)
$a := (a_1, \ldots, a_m)$
$a_L := (a_1, \ldots, a_{m/2})$
$a_R := (a_{m/2+1}, \ldots, a_m)$
$1/a := (1/a_1, \ldots, 1/a_m)$

(L1) $\mathrm{AM}(\mathrm{AM}_{\mathrm{all}}(a_L), \mathrm{AM}_{\mathrm{all}}(a_R)) = \mathrm{AM}_{\mathrm{all}}(a)$
[AM (the proof's block), $\mathrm{AM}_{\mathrm{all}}$ (the statement): $\frac{1}{2}\left(\frac{2}{m}\sum_{i \leq m/2} a_i + \frac{2}{m}\sum_{i > m/2} a_i\right) = \frac{1}{m}\sum_{i \leq m} a_i$]

(L2) $\forall k \geq 1 :\ C_{\mathrm{AM}}(a) = \mathrm{AM}(C_{\mathrm{AM}}(a_L), C_{\mathrm{AM}}(a_R))$
[$M = \mathrm{AM}$, $C_L = C_R$, $C_R = C_{\mathrm{AM}}$ at depth $k-1$ (C_{AM}, the statement)]

(L3) $\forall k \geq 1 :\ [\forall b \in (0,\infty)^{m/2} :\ C_{\mathrm{AM}}(b) = \mathrm{AM}_{\mathrm{all}}(b)] \Rightarrow$
$C_{\mathrm{AM}}(a) = \mathrm{AM}(\mathrm{AM}_{\mathrm{all}}(a_L), \mathrm{AM}_{\mathrm{all}}(a_R))$
[(L2); the hypothesis at $b := a_L$ and at $b := a_R$]

(L4) $\Rightarrow\ \forall k \geq 1 :$ [the hypothesis of (L3)] $\Rightarrow\ C_{\mathrm{AM}}(a) = \mathrm{AM}_{\mathrm{all}}(a)$
[(L3), (L1)]

(L5) $k = 0 :\ C_{\mathrm{AM}}(a) = a_1$
[$\mathcal{C}_0 = \{a_1 \mapsto a_1\}$ (the statement)]

(L6) $k = 0 :\ a_1 = \mathrm{AM}_{\mathrm{all}}(a)$
[$\mathrm{AM}_{\mathrm{all}} = (1/m)\sum_i a_i$ at $m = 1$ (the statement)]

(L7) $k = 0 :\ C_{\mathrm{AM}}(a) = \mathrm{AM}_{\mathrm{all}}(a)$
[(L5), (L6)]

(L8) $\Rightarrow\ \forall k \geq 0 :\ C_{\mathrm{AM}}(a) = \mathrm{AM}_{\mathrm{all}}(a)$
[induction on k: (L7) at $k = 0$; (L4) from $k-1$ to k]

(L9) $\forall x, y > 0 :\ \mathrm{HM}(x,y) = 1/\,\mathrm{AM}(1/x, 1/y)$
[$2xy/(x+y) = 1/((1/x + 1/y)/2)$]

(L10) $\forall k \geq 1:\ C_{\mathrm{HM}}(a) = \mathrm{HM}(C_{\mathrm{HM}}(a_L), C_{\mathrm{HM}}(a_R))$

[C_{HM} (the statement)]

(L11) $\forall k \geq 1:\ [\forall b \in (0,\infty)^{m/2}:\ C_{\mathrm{HM}}(b) = 1/C_{\mathrm{AM}}(1/b)] \Rightarrow$
$C_{\mathrm{HM}}(a) = \mathrm{HM}(1/C_{\mathrm{AM}}(1/a_L), 1/C_{\mathrm{AM}}(1/a_R))$

[(L10); the hypothesis at $b := a_L$ and at $b := a_R$]

(L12) $\forall b \in (0,\infty)^{m/2}:\ C_{\mathrm{AM}}(b) > 0$

[C_{AM} (the statement); Fact A.41, item 9: $\min(a,b) \leq (a+b)/2$, at each node of C_{AM}]

(L13) $\mathrm{HM}(1/C_{\mathrm{AM}}(1/a_L), 1/C_{\mathrm{AM}}(1/a_R)) = 1/\mathrm{AM}(C_{\mathrm{AM}}(1/a_L), C_{\mathrm{AM}}(1/a_R))$

[(L9) at $x := 1/C_{\mathrm{AM}}(1/a_L)$, $y := 1/C_{\mathrm{AM}}(1/a_R)$; (L12)]

(L14) $\mathrm{AM}(C_{\mathrm{AM}}(1/a_L), C_{\mathrm{AM}}(1/a_R)) = C_{\mathrm{AM}}(1/a)$

[$(1/a)_L = 1/a_L$, $(1/a)_R = 1/a_R$ by (L2) at $1/a$]

(L15) $\Rightarrow\ \forall k \geq 1:$ [the hypothesis of (L11)] $\Rightarrow\ C_{\mathrm{HM}}(a) = 1/C_{\mathrm{AM}}(1/a)$

[(L11), (L13), (L14)]

(L16) $k = 0:\ C_{\mathrm{HM}}(a) = a_1$

[$\mathcal{C}_0 = \{a_1 \mapsto a_1\}$ (the statement) at a]

(L17) $k = 0:\ a_1 = 1/C_{\mathrm{AM}}(1/a)$

[$\mathcal{C}_0 = \{a_1 \mapsto a_1\}$ (the statement) at $1/a$]

(L18) $k = 0:\ C_{\mathrm{HM}}(a) = 1/C_{\mathrm{AM}}(1/a)$

[(L16), (L17)]

(L19) $\Rightarrow\ \forall k \geq 0:\ C_{\mathrm{HM}}(a) = 1/C_{\mathrm{AM}}(1/a)$

[induction on k: (L18) at $k = 0$; (L15) from $k-1$ to k]

(L20) $\Rightarrow\ \forall k \geq 0:\ C_{\mathrm{HM}}(a) = 1/\mathrm{AM}_{\mathrm{all}}(1/a)$

[(L19); (L8) at $1/a$]

(L21) $1/\mathrm{AM}_{\mathrm{all}}(1/a) = m/\sum_i a_i^{-1}$

[$\mathrm{AM}_{\mathrm{all}}$ (the statement)]

(L22) $m/\sum_i a_i^{-1} = \mathrm{HM}_{\mathrm{all}}(a)$

[$\mathrm{HM}_{\mathrm{all}}$ (the statement)]

(L23) $\Rightarrow\ \forall k \geq 0:\ C_{\mathrm{HM}}(a) = \mathrm{HM}_{\mathrm{all}}(a)$

[(L20), (L21), (L22)]

(L24) $\Rightarrow$ the statement

[(L8), (L23)]

□

Lemma C.2 (Mixed means [to table])**.** *Every composition of the two means lies between the harmonic and the arithmetic mean over all values. Let:*

- $k \geq 0$.

Define:

- $m := 2^k$;
- $\mathcal{C}_k$, *that of Definition A.46.*

Let:

- $a_1, \ldots, a_m > 0$;
- $C \in \mathcal{C}_k$.

Define:

- $\mathrm{AM}_{\mathrm{all}} := (1/m)\sum_i a_i$, *the arithmetic mean over all values (Definition A.46);*
- $\mathrm{HM}_{\mathrm{all}} := m/\sum_i a_i^{-1}$, *the harmonic mean over all values (Definition A.46).*

We have

$$\mathrm{HM}_{\mathrm{all}} \leq C(a_1, \ldots, a_m) \leq \mathrm{AM}_{\mathrm{all}}\,.$$

Proof.

DEFINES $\mathrm{AM}(a,b) := (a+b)/2$ and $\mathrm{HM}(a,b) := 2ab/(a+b)$ (Definition A.46)
$C_{\mathrm{AM}} \in \mathcal{C}_k$, with $M = \mathrm{AM}$ and $C_L = C_R = C_{\mathrm{AM}}$ at every level (Definition A.46)
$C_{\mathrm{HM}} \in \mathcal{C}_k$, with $M = \mathrm{HM}$ and $C_L = C_R = C_{\mathrm{HM}}$ at every level (Definition A.46)
$a := (a_1, \ldots, a_m)$
$a_L := (a_1, \ldots, a_{m/2})$
$a_R := (a_{m/2+1}, \ldots, a_m)$
$1/a := (1/a_1, \ldots, 1/a_m)$

DEFINES $M \in \{\mathrm{AM}, \mathrm{HM}\}$, C_L and $C_R \in \mathcal{C}_{k-1}$ with $C = M(C_L, C_R)$ at $k \geq 1$ (Definition A.46, the compositions)

(L1) $\partial_a \mathrm{AM}(a,b) = \frac{1}{2}$
[$\mathrm{AM}(a,b) = (a+b)/2$ (the proof's block)]

(L2) $\partial_b \mathrm{AM}(a,b) = \frac{1}{2}$
[$\mathrm{AM}(a,b) = (a+b)/2$ (the proof's block)]

(L3) $\Rightarrow\ \partial_a \mathrm{AM}(a,b),\ \partial_b \mathrm{AM}(a,b) > 0$
[(L1), (L2)]

(L4) $\partial_a \mathrm{HM}(a,b) = 2b^2/(a+b)^2$
[$\mathrm{HM}(a,b) = 2ab/(a+b)$ (the proof's block)]

(L5) $\partial_b \mathrm{HM}(a,b) = 2a^2/(a+b)^2$
[$\mathrm{HM}(a,b) = 2ab/(a+b)$ (the proof's block)]

(L6) $\Rightarrow\ \partial_a \mathrm{HM}(a,b),\ \partial_b \mathrm{HM}(a,b) > 0$
[(L4), (L5); $a, b > 0$ (Definition A.46)]

(L7) $\Rightarrow\ \forall M \in \{\mathrm{AM}, \mathrm{HM}\}\ \forall 0 < x \leq x',\ 0 < y \leq y' :\ M(x,y) \leq M(x',y')$
[(L3), (L6)]

(L8) $\mathrm{AM}(a,b) - \mathrm{HM}(a,b) = (a-b)^2/(2(a+b))$
[AM, HM (the proof's block): $(a+b)/2 - 2ab/(a+b) = ((a+b)^2 - 4ab)/(2(a+b))$]

(L9) $\Rightarrow\ \mathrm{AM}(a,b) - \mathrm{HM}(a,b) \geq 0$
[(L8); $a, b > 0$ (Definition A.46)]

(L10) $\forall k \geq 1\ \forall C \in \mathcal{C}_k\ \exists M \in \{\mathrm{AM}, \mathrm{HM}\}\ \exists C_L, C_R \in \mathcal{C}_{k-1} :\ C(a) = M(C_L(a_L), C_R(a_R))$
[$\mathcal{C}_k$ (the statement)]

(L11) $\forall k \geq 1\ \forall C \in \mathcal{C}_k :\ [C_L(a_L) \leq C_{\mathrm{AM}}(a_L),\ C_R(a_R) \leq C_{\mathrm{AM}}(a_R)] \Rightarrow C(a) \leq M(C_{\mathrm{AM}}(a_L), C_{\mathrm{AM}}(a_R))$
[(L7), (L10)]

(L12) $M(C_{\mathrm{AM}}(a_L), C_{\mathrm{AM}}(a_R)) \leq \mathrm{AM}(C_{\mathrm{AM}}(a_L), C_{\mathrm{AM}}(a_R))$
[HM $\leq$ AM (L9) if $M = \mathrm{HM}$, equality if $M = \mathrm{AM}$]

(L13) $\mathrm{AM}(C_{\mathrm{AM}}(a_L), C_{\mathrm{AM}}(a_R)) = C_{\mathrm{AM}}(a)$
[Lemma C.1, (L2)]

(L14) $\Rightarrow\ M(C_{\mathrm{AM}}(a_L), C_{\mathrm{AM}}(a_R)) \leq C_{\mathrm{AM}}(a)$
[(L12), (L13)]

(L15) $k = 0 :\ \forall C \in \mathcal{C}_0 :\ C(a) = a_1$
[$\mathcal{C}_0 = \{a_1 \mapsto a_1\}$ at $k = 0$ (Lemma C.1)]

(L16) $k = 0 :\ a_1 = C_{\mathrm{AM}}(a)$
[$\mathcal{C}_0 = \{C_{\mathrm{AM}}\}$ at $k = 0$ (Lemma C.1)]

(L17) $k = 0 :\ \forall C \in \mathcal{C}_0 :\ C(a) = C_{\mathrm{AM}}(a)$
[(L15), (L16)]

(L18) $\Rightarrow\ \forall k \geq 0\ \forall C \in \mathcal{C}_k :\ C(a) \leq C_{\mathrm{AM}}(a)$
[induction on k: (L17) at $k = 0$; (L11) at C_L, C_R with the claim at $k-1$ as its hypothesis, and (L14), from $k-1$ to k]

(L19) $\forall k \geq 0 :\ C_{\mathrm{AM}}(a) = \mathrm{AM}_{\mathrm{all}}(a)$
[Lemma C.1]

(L20) $\Rightarrow\ \forall k \geq 0\ \forall C \in \mathcal{C}_k :\ C(a) \leq \mathrm{AM}_{\mathrm{all}}(a)$

[(L18), (L19)]

(L21) $\forall k \geq 1\ \forall C \in \mathcal{C}_k :\ [C_L(a_L) \geq C_{\mathrm{HM}}(a_L),\ C_R(a_R) \geq C_{\mathrm{HM}}(a_R)] \Rightarrow C(a) \geq M(C_{\mathrm{HM}}(a_L), C_{\mathrm{HM}}(a_R))$

[(L7), (L10)]

(L22) $M(C_{\mathrm{HM}}(a_L), C_{\mathrm{HM}}(a_R)) \geq \mathrm{HM}(C_{\mathrm{HM}}(a_L), C_{\mathrm{HM}}(a_R))$

[AM $\geq$ HM (L9) if $M = \mathrm{AM}$, equality if $M = \mathrm{HM}$]

(L23) $\mathrm{HM}(C_{\mathrm{HM}}(a_L), C_{\mathrm{HM}}(a_R)) = C_{\mathrm{HM}}(a)$

[Lemma C.1, (L10)]

(L24) $\Rightarrow\ M(C_{\mathrm{HM}}(a_L), C_{\mathrm{HM}}(a_R)) \geq C_{\mathrm{HM}}(a)$

[(L22), (L23)]

(L25) $k = 0 :\ \forall C \in \mathcal{C}_0 :\ C(a) = a_1$

[$\mathcal{C}_0 = \{a_1 \mapsto a_1\}$ at $k = 0$ (Lemma C.1)]

(L26) $k = 0 :\ a_1 = C_{\mathrm{HM}}(a)$

[$\mathcal{C}_0 = \{C_{\mathrm{HM}}\}$ at $k = 0$ (Lemma C.1)]

(L27) $k = 0 :\ \forall C \in \mathcal{C}_0 :\ C(a) = C_{\mathrm{HM}}(a)$

[(L25), (L26)]

(L28) $\Rightarrow\ \forall k \geq 0\ \forall C \in \mathcal{C}_k :\ C(a) \geq C_{\mathrm{HM}}(a)$

[induction on k: (L27) at $k = 0$; (L21) with (L24) from $k - 1$ to k]

(L29) $\forall k \geq 0 :\ C_{\mathrm{HM}}(a) = \mathrm{HM}_{\mathrm{all}}(a)$

[Lemma C.1]

(L30) $\Rightarrow\ \forall k \geq 0\ \forall C \in \mathcal{C}_k :\ C(a) \geq \mathrm{HM}_{\mathrm{all}}(a)$

[(L28), (L29)]

(L31) $\Rightarrow$ the statement

[(L20), (L30)]

□

D Proofs of the tree

Structure. This appendix proves the statements of Section 3.2. Section D.1 states the child's diagonals as means; Section D.2 the Gram form; Section D.3 the exact structure of the diagonals.

The conventions of the proof appendices. A statement the body keeps is restated by its number and title, with the display it proves; its algorithms and its dependency graph stay in Section 3.2. A statement placed here carries its proof. A line of a proof is cited from anywhere in the report as "(Lk)" of the statement it proves.

How each statement is verified. Table 15 lists how each fact placed here is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Fact D.1	✓				
Fact D.2	✓				
Fact D.3	✓				
Lemma D.4	✓				
Lemma D.5	✓				
Lemma D.6	✓				
Lemma D.7	✓				
Lemma D.8	✓				
Prop. D.9	✓				
Lemma D.10			✓		
Lemma D.11	✓		✓		

Table 15: Appendix D: its facts, and how each lemma and proposition is verified.

D.1 The child's diagonals as means

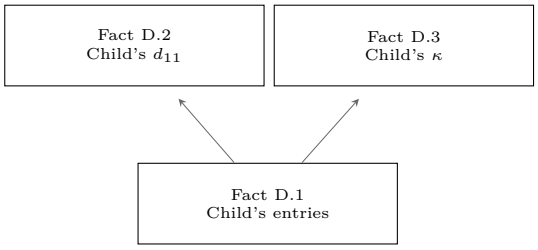


Figure 42: Dependencies, Section D.1.

Fact D.1 (A child's entries [to table])**.** The split of a diagonal d returns, from the pair $d(\psi)$, $d(-\psi)$, the arithmetic mean as the child's first entry and the half-difference, turned by the conjugate root, as its second. Let:

- $m \geq 2$, a power of two;
- $d \in \mathcal{R}_m$, the input of split_{sa} (Algorithm 3) at lines 16 and 30 of ffsamp (Algorithm 6);
- $\psi \in \mathbb{C}$ with $\psi^m = -1$.

Define:

- $a = d(\psi)$;
- $b = d(-\psi)$;
- $\text{AM}(a, b) = (a + b)/2$;
- (d_0, d_1), the values of split_{sa} (Algorithm 3) at d and ψ.

Assume:

(A1) $a > 0$;

(A2) $b > 0$.

Then the child's two entries are:

1. $d_0 = \text{AM}(a, b)$;
2. $d_1 = ((a - b)/2)\ \text{conj}\,\psi$;
3. $|d_1| = |a - b|/2$. [derived]

Proof. (L1) $d_0 = (a + b)/2$

[split_{sa} (Algorithm 3), line 5, at $(a, b) := (d(\psi), d(-\psi))$]

(L2) $(a + b)/2 = \text{AM}(a, b)$

[$\text{AM}(a, b)$ (the statement)]

(L3) $\Rightarrow$ $d_0 = \text{AM}(a, b)$

[(L1), (L2)]

(L4) $\Rightarrow$ item 1

[(L3)]

(L5) $d_1 = ((a - b)/2)\ \text{conj}\,\psi$

[split_{sa} (Algorithm 3), line 7]

(L6) $\Rightarrow$ item 2

[(L5)]

(L7) $|\text{conj}\,\psi| = 1$

[Fact A.42, item 1; Fact A.41, item 1: $|\text{conj}\,x| = |x|$]

(L8) $a - b \in \mathbb{R}$

[$a, b > 0$ (assumptions A1, A2)]

(L9) $\Rightarrow$ $|d_1| = |a-b|/2$

[(L5), (L7), (L8); Fact A.41, item 1: $|xy| = |x||y|$]

(L10) $\Rightarrow$ item 3

[(L9)]

□ (items 1, 2 and 3)

Fact D.2 (A child's second diagonal [to table])**.** The second diagonal of the child's Gram matrix is the harmonic mean of the parent's pair. Let:

- $m \geq 2$, a power of two;
- $d \in \mathcal{R}_m$;
- $\psi \in \mathbb{C}$ with $\psi^m = -1$.

Define:

- $a = d(\psi)$;
- $b = d(-\psi)$;
- (d_0, d_1), the values of split_{sa} (Algorithm 3) at d and ψ;
- $d_{11} = d_0 - |d_1|^2/d_0$, the second diagonal LDL† (Algorithm 5) returns at $(g_{00}, g_{01}, g_{11}) := (d_0, d_1, d_0)$, the child's Gram matrix [L0: `sign_sampler.c:1284-1285`] [L0: `fxp/sign_fxsampler.c:304-305`] (ffsamp (Algorithm 6), lines 16 and 30), line 19;
- $\text{HM}(a, b) = 2ab/(a+b)$.

Assume:

(A1) $a > 0$;

(A2) $b > 0$.

Then

$$d_{11} = \text{HM}(a, b). \qquad \text{[derived]}$$

Proof. (L1) $d_{11} = d_0 - |d_1|^2/d_0$

[d_{11} (the statement)]

(L2) $d_0 = (a+b)/2$

[Fact D.1, item 1, and its $\text{AM}(a,b) = (a+b)/2$ (Definition A.46); $a, b > 0$ (assumptions A1, A2)]

(L3) $|d_1| = |a-b|/2$

[Fact D.1, item 3; $a, b > 0$ (assumptions A1, A2)]

(L4) $a + b > 0$

[$a, b > 0$ (assumptions A1, A2)]

(L5) $d_0 > 0$

[(L2), (L4)]

(L6) $d_0^2 - |d_1|^2 = ((a+b)^2 - (a-b)^2)/4$

[(L2), (L3)]

(L7) $((a+b)^2 - (a-b)^2)/4 = ab$

[expand]

(L8) $d_{11} = (d_0^2 - |d_1|^2)/d_0$

[(L1), (L5)]

(L9) $\Rightarrow$ $d_{11} = ab/d_0$

[(L6), (L7), (L8)]

(L10) $ab/d_0 = 2ab/(a+b)$

[(L2), (L4)]

(L11) $2ab/(a+b) = \text{HM}(a, b)$

[$\text{HM}(a, b)$ (the statement)]

(L12) $\Rightarrow$ $d_{11} = \text{HM}(a, b)$

[(L9), (L10), (L11)]

(L13) $\Rightarrow$ the statement

[(L12)]

□

Fact D.3 (A child's κ [to table])**.** At the child, κ of the LDL subtraction $d_0 - |d_1|^2/d_0$ is a function of the parent's pair. Let:

- $m \geq 2$, a power of two;
- $d \in \mathcal{R}_m$;
- $\psi \in \mathbb{C}$ with $\psi^m = -1$.

Define:

- $a := d(\psi)$;
- $b := d(-\psi)$;
- $d_0 := (a+b)/2$ (Fact D.1, item 1, with its $\mathrm{AM}(a,b) = (a+b)/2$);
- $d_1 := ((a-b)/2)\ \mathrm{conj}\,\psi$ (Fact D.1, item 2);
- $\kappa := |d_1|^2/(d_0^2 - |d_1|^2)$ (LDL† (Algorithm 5), line 15, at $(g_{00}, g_{01}, g_{11}) := (d_0, d_1, d_0)$: $g_{11} - |g_{01}|^2/g_{00} = d_0 - |d_1|^2/d_0$).

Assume:

(A1) $a > 0$;

(A2) $b > 0$.

Then

$$\kappa = (a-b)^2/(4ab).$$

Proof. (L1) $d_0 = (a+b)/2$

[d_0 (the statement; Fact D.1, item 1); $a, b > 0$ (assumptions A1, A2)]

(L2) $|d_1| = |a-b|/2$

[$d_1 = ((a-b)/2)\ \mathrm{conj}\,\psi$ (the statement; Fact D.1, item 2); $|xy| = |x||y|$, $|\mathrm{conj}\,x| = |x|$ (Fact A.41, item 1); $|\psi| = 1$ (Fact A.42, item 1)]

(L3) $(a+b)^2 - (a-b)^2 = 4ab$

[expand]

(L4) $d_0^2 - |d_1|^2 = ab$

[(L1), (L2), (L3)]

(L5) $|d_1|^2 = (a-b)^2/4$

[(L2)]

(L6) $ab > 0$

[$a, b > 0$ (assumptions A1, A2)]

(L7) $\Rightarrow$ $\kappa = (a-b)^2/(4ab)$

[κ (the statement); (L4), (L5), (L6)]

(L8) $\Rightarrow$ the statement

[(L7)]

□

D.2 The Gram form

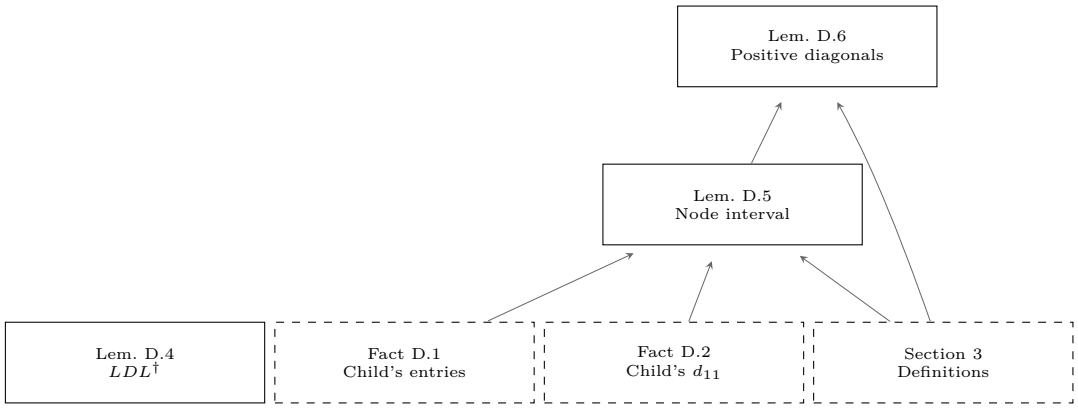


Figure 43: Dependencies, Section D.2.

Lemma D.4 (The $LDL^\dagger$ decomposition of a Gram matrix [to table])**.** *The decomposition the $LDL^\dagger$ step computes over $\mathbb{R}$ reproduces the Gram matrix. Let:*

- $g_{00}, g_{11} \in \mathbb{R}$;
- $g_{01} \in \mathbb{C}$.

Define:

- $\mathcal{G} := \begin{pmatrix} g_{00} & g_{01} \\ \operatorname{conj} g_{01} & g_{11} \end{pmatrix}$ *and* $l_{10} := \operatorname{conj} g_{01}/g_{00}$ *(Definition A.17);*
- $d_{00} := g_{00}$ *and* $d_{11} := g_{11} - |g_{01}|^2/g_{00}$ *(Definition A.17);*
- *zo, that of* LDL† *(Algorithm 5), line 15;*
- $L = \begin{pmatrix} 1 & 0 \\ l_{10} & 1 \end{pmatrix}$;
- $D = \operatorname{diag}(d_{00}, d_{11})$;
- $L^\dagger = \operatorname{conj} L^{\mathsf{T}}$.

Assume:

(A1) $g_{00} > 0$.

Then the factors satisfy:

1. $d_{00} = g_{00}$;
2. $d_{00} \operatorname{conj}(l_{10}) = g_{01}$;
3. $l_{10} d_{00} = \operatorname{conj}(g_{01})$;
4. $l_{10} d_{00} \operatorname{conj}(l_{10}) = zo$;
5. $zo + d_{11} = g_{11}$;
6. $\mathcal{G} = LDL^\dagger$.

Proof. (L1) $d_{00} = g_{00}$

[d_{00} (Definition A.17)]

(L2) $\Rightarrow$ item 1

[(L1)]

(L3) $l_{10} = \operatorname{conj}(g_{01})/g_{00}$

[l_{10} (Definition A.17); $g_{00} > 0$ (assumption A1)]

(L4) $\operatorname{conj}(l_{10}) = g_{01}/g_{00}$

[(L3); $\operatorname{conj} xy = \operatorname{conj} x \operatorname{conj} y$ (Fact A.41, item 13) at $(x, y) := (\operatorname{conj}(g_{01}), 1/g_{00})$; $g_{00} \in \mathbb{R}$ (the statement)]

(L5) $\Rightarrow$ $d_{00}\,\mathrm{conj}(l_{10}) = g_{01}$

[(L1), (L4)]

(L6) $\Rightarrow$ item 2

[(L5)]

(L7) $l_{10}d_{00} = \mathrm{conj}(d_{00}\,\mathrm{conj}(l_{10}))$

[Fact A.41, item 13: $\mathrm{conj}\,xy = \mathrm{conj}\,x\ \mathrm{conj}\,y$; $d_{00} \in \mathbb{R}$ (L1)]

(L8) $\Rightarrow$ $l_{10}d_{00} = \mathrm{conj}(g_{01})$

[(L5), (L7)]

(L9) $\Rightarrow$ item 3

[(L8)]

(L10) $l_{10}\,\mathrm{conj}(l_{10}) = |g_{01}|^2/g_{00}^2$

[(L3), (L4); Fact A.41, item 1: $x\,\mathrm{conj}\,x = |x|^2$]

(L11) $\Rightarrow$ $l_{10}d_{00}\,\mathrm{conj}(l_{10}) = |g_{01}|^2/g_{00}$

[(L1), (L10)]

(L12) $|g_{01}|^2/g_{00} = zo$

[zo (LDL† (Algorithm 5), line 15)]

(L13) $\Rightarrow$ $l_{10}d_{00}\,\mathrm{conj}(l_{10}) = zo$

[(L11), (L12)]

(L14) $\Rightarrow$ item 4

[(L13)]

(L15) $zo + d_{11} = g_{11}$

[d_{11} (Definition A.17); (L12)]

(L16) $\Rightarrow$ item 5

[(L15)]

(L17) $LDL^\dagger = \begin{pmatrix} d_{00} & d_{00}\,\mathrm{conj}(l_{10}) \\ l_{10}d_{00} & l_{10}d_{00}\,\mathrm{conj}(l_{10}) + d_{11} \end{pmatrix}$

[L, D, $L^\dagger$ (the statement); $(LDL^\dagger)_{ij} = \sum_k L_{ik}\,d_k\,\mathrm{conj}(L_{jk})$, the matrix product]

(L18) $\Rightarrow$ $LDL^\dagger = \mathcal{G}$

[(L17); items 1 to 5; $\mathcal{G}$ (the statement)]

(L19) $\Rightarrow$ item 6

[(L18)]

□ (items 1 to 6)

Lemma D.5 (An interval for every node's diagonals [to table])**.** *On a Gram matrix, an interval of positive reals that holds the values of the root's first diagonal and Schur complement holds the values of the two diagonals of every node of its tree. Let:*

- $\mathcal{G} \in \mathrm{Gram}_n$ *(Definition A.14);*
- $I \subseteq (0, \infty)$*, an interval.*

Define:

- $T := \mathrm{ffLDL}^\dagger(\mathcal{G})$ *(Definition A.20);*
- $\forall \nu \in \mathrm{Sub}(T):\ (g^\nu_{jk})_{j,k\in\{0,1\}} := \mathcal{G}_\nu$ *(Definition A.32);*
- $\forall \nu \in \mathrm{Sub}(T):\ d^\nu_{11} := g^\nu_{11} - |g^\nu_{01}|^2/g^\nu_{00}$.

Assume:

(A1) $\forall \psi:\ g^T_{00}(\psi) \in I$;

(A2) $\forall \psi:\ d^T_{11}(\psi) \in I$.

Then the two diagonals lie in I:

1. $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi:\ g^\nu_{00}(\psi) \in I$;
2. $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi:\ d^\nu_{11}(\psi) \in I$.

Proof.

DEFINES g^ν_{01}, g^ν_{11}, $\nu \in \mathrm{Sub}(T)$, the g_{01} and g_{11} of $\mathcal{G}_\nu$ (Definition A.32)

DEFINES $d^\nu_{00} := g^\nu_{00}$, $\nu \in \mathrm{Sub}(T)$, the g_{00} of $\mathcal{G}_\nu$ (Definitions A.17 and A.32)

DEFINES $\mu^\nu(\psi)$, $l^\nu_{10}(\psi)$, $zo^\nu(\psi)$, those of LDL† (Algorithm 5), lines 11 to 19, at $\mathcal{G}_\nu(\psi)$

DEFINES $L^\nu(\psi) := \begin{pmatrix} 1 & 0 \\ l_{10} & 1 \end{pmatrix}$ and $D^\nu(\psi) := \mathrm{diag}(d_{00}, d_{11})$ (Lemma D.4)

DEFINES l_{10}, d_{00} and d_{11}, those of $\mathcal{G}_\nu(\psi)$ (Definition A.17)

Proof of items 1 and 2.

(L1) $\forall a, b > 0 :\ \mathrm{AM}(a,b) \in [\min(a,b), \max(a,b)]$

[Fact A.41, item 9; Definition A.46]

(L2) $\forall a, b > 0 :\ \mathrm{HM}(a,b) \in [\min(a,b), \max(a,b)]$

[Fact A.41, item 9; Definition A.46]

(L3) $\forall a, b \in I :\ [\min(a,b), \max(a,b)] \subseteq I$

[I, an interval (the statement)]

(L4) $\forall a \in I :\ a > 0$

[$I \subseteq (0, \infty)$ (the statement)]

(L5) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall (T', d') \in \{(T_{00}, d^\nu_{00}), (T_{11}, d^\nu_{11})\} :\ \mathcal{G}_{T'} = \mathcal{G}_{d'}$

[$\mathcal{G}_{T_{00}} = \mathcal{G}_{d_{00}}$, $\mathcal{G}_{T_{11}} = \mathcal{G}_{d_{11}}$ (Definition A.32); d^ν_{00} (the proof's block); d^ν_{11} (the statement)]

Lemma D.4, item 1 $\forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall \psi,\ \psi^m = -1,\ g^\nu_{00}(\psi) \in I$	This proof

(I1)

g_{00}, g_{01}, g_{11}	$g^\nu_{00}(\psi), g^\nu_{01}(\psi), g^\nu_{11}(\psi)$ (the statement; the proof's block)
d_{00}	$d^\nu_{00}(\psi)$ (the proof's block)
μ, l_{10}, zo, d_{11}	$\mu^\nu(\psi), l^\nu_{10}(\psi), zo^\nu(\psi), d^\nu_{11}(\psi)$ (the proof's block; the statement)
$\mathcal{G}, L, D, L^\dagger$	$\mathcal{G}_\nu(\psi), L^\nu(\psi), D^\nu(\psi), L^\nu(\psi)^\dagger$ (the proof's block)
$g_{00}, g_{11} \in \mathbb{R}$	$g^\nu_{00}(\psi)$, $g^\nu_{11}(\psi)$ (Definition A.17)
$g_{01} \in \mathbb{C}$	$g^\nu_{01}(\psi)$ (Definition A.17)

Assumption A1	(L4) at $a := g^\nu_{00}(\psi)$

Its conclusion: $d_{00} = g_{00}$

(L6) $\forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall \psi,\ \psi^m = -1 :\ [g^\nu_{00}(\psi) \in I] \Rightarrow\ d^\nu_{00}(\psi) = g^\nu_{00}(\psi)$

[(I1)]

(L7) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4$
$\forall (T', d) \in \{(T_{00}, g^\nu_{00}), (T_{11}, d^\nu_{11})\}\ \forall \psi,\ \psi^m = -1 :$
$[d(\psi), d(-\psi) \in I] \Rightarrow\ \mathcal{G}_{T'}(\psi^2) = \mathcal{G}_d(\psi^2)$

[(L5); (L6) at ψ and $-\psi$; $\mathcal{G}_d$ (Definition A.23); Definition A.20, items 3 and 4; split (Algorithm 2), lines 5 and 7]

Fact D.1, item 1	This proof
$\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall (T', d) \in \{(T_{00}, g_{00}^{\nu}), (T_{11}, d_{11}^{\nu})\}\ \forall \psi,\ \psi^m = -1,\ d(\psi), d(-\psi) \in I$	

Shared: m (the scope), d (the scope), ψ (the scope)

a	$d(\psi)$
b	$d(-\psi)$
$\mathrm{AM}(a, b)$	$\mathrm{AM}(d(\psi), d(-\psi))$ (Definition A.46)
(I2) (d_0, d_1)	$(g_{00}^{T'}(\psi^2), g_{01}^{T'}(\psi^2))$ ((L7); $g_{00}^{T'}$, the statement; $g_{01}^{T'}$, the proof's block)
$m \geq 2$	$m \geq 4$, a power of two (the scope)
$m \in \{2^j : j \in \mathbb{Z}_{\geq 0}\}$	$\mathcal{T}_m$ (Definition A.18)
$d \in \mathcal{R}_m$	g_{00}^{ν}, d_{11}^{ν} (Definition A.17)
$\psi \in \mathbb{C}$	The scope
$\psi^m = -1$	The scope
Assumption A1	(L4) at $a := d(\psi)$
Assumption A2	(L4) at $a := d(-\psi)$

Its conclusion: $d_0 = \mathrm{AM}(a, b)$

(L8) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4$
$\forall (T', d) \in \{(T_{00}, g_{00}^{\nu}), (T_{11}, d_{11}^{\nu})\}\ \forall \psi,\ \psi^m = -1 :$
$[d(\psi), d(-\psi) \in I] \Rightarrow\ g_{00}^{T'}(\psi^2) = \mathrm{AM}(d(\psi), d(-\psi))$

[(I2)]

Fact D.2 $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall (T', d) \in \{(T_{00}, g_{00}^{\nu}), (T_{11}, d_{11}^{\nu})\}\ \forall \psi,\ \psi^m = -1,\ d(\psi), d(-\psi) \in I$	This proof

Shared: m (the scope), d (the scope), ψ (the scope)

a	$d(\psi)$
b	$d(-\psi)$
(d_0, d_1)	$(g_{00}^{T'}(\psi^2), g_{01}^{T'}(\psi^2))$ ((L7); $g_{00}^{T'}$, the statement; $g_{01}^{T'}$, the proof's block)
(I3) d_{11}	$d_{11}^{T'}(\psi^2)$ ((L7); $d_{11}^{T'}$, the statement)
$\mathrm{HM}(a, b)$	$\mathrm{HM}(d(\psi), d(-\psi))$ (Definition A.46)
$m \geq 2$	$m \geq 4$, a power of two (the scope)
$m \in \{2^j : j \in \mathbb{Z}_{\geq 0}\}$	$\mathcal{T}_m$ (Definition A.18)
$d \in \mathcal{R}_m$	g_{00}^{ν}, d_{11}^{ν} (Definition A.17)
$\psi \in \mathbb{C}$	The scope
$\psi^m = -1$	The scope
Assumption A1	(L4) at $a := d(\psi)$
Assumption A2	(L4) at $a := d(-\psi)$

Its conclusion: $d_{11} = \mathrm{HM}(a, b)$

(L9) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4$
$\forall (T', d) \in \{(T_{00}, g_{00}^{\nu}), (T_{11}, d_{11}^{\nu})\}\ \forall \psi,\ \psi^m = -1 :$
$[d(\psi), d(-\psi) \in I] \Rightarrow\ d_{11}^{T'}(\psi^2) = \mathrm{HM}(d(\psi), d(-\psi))$

[(I3)]

(L10) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4$
$\forall (T', d) \in \{(T_{00}, g_{00}^{\nu}), (T_{11}, d_{11}^{\nu})\}\ \forall \psi,\ \psi^m = -1 :$
$[d(\psi), d(-\psi) \in I] \Rightarrow\ g_{00}^{T'}(\psi^2) \in [\min(d(\psi), d(-\psi)),\ \max(d(\psi), d(-\psi))]$

[(L8); (L1) at $(a, b) := (d(\psi), d(-\psi))$, $a, b > 0$ by (L4)]

(L11) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4$
$\forall (T', d) \in \{(T_{00}, g^\nu_{00}), (T_{11}, d^\nu_{11})\}\ \forall \psi,\ \psi^m = -1 :$
$[d(\psi), d(-\psi) \in I] \Rightarrow\ d^{T'}_{11}(\psi^2) \in [\min(d(\psi), d(-\psi)),\ \max(d(\psi), d(-\psi))]$
[(L9); (L2) at $(a, b) := (d(\psi), d(-\psi))$, $a, b > 0$ by (L4)]

(L12) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4 :$
$[\forall \psi :\ g^\nu_{00}(\psi) \in I \wedge d^\nu_{11}(\psi) \in I] \Rightarrow\ \forall T' \in \{T_{00}, T_{11}\}\ \forall \psi',\ \psi'^{m/2} = -1 :\ g^{T'}_{00}(\psi') \in I$
[(L3), (L10); Fact A.43, item 5: $\{\psi^2 : \psi \in \Psi_m\} = Z_{m/2}$]

(L13) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4 :$
$[\forall \psi :\ g^\nu_{00}(\psi) \in I \wedge d^\nu_{11}(\psi) \in I] \Rightarrow\ \forall T' \in \{T_{00}, T_{11}\}\ \forall \psi',\ \psi'^{m/2} = -1 :\ d^{T'}_{11}(\psi') \in I$
[(L3), (L11); Fact A.43, item 5: $\{\psi^2 : \psi \in \Psi_m\} = Z_{m/2}$]

(L14) $\forall \psi :\ g^T_{00}(\psi) \in I$
[assumption A1]

(L15) $\forall \psi :\ d^T_{11}(\psi) \in I$
[assumption A2]

(L16) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ g^\nu_{00}(\psi) \in I$
[induction on the depth from the root: the base (L14), (L15), the step (L12), (L13)]

(L17) $\Rightarrow$ item 1
[(L16)]

(L18) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d^\nu_{11}(\psi) \in I$
[induction on the depth from the root: the base (L14), (L15), the step (L12), (L13)]

(L19) $\Rightarrow$ item 2
[(L18)]

□ (items 1 and 2)

Lemma D.6 (Positive diagonals of the $LDL^\dagger$ tree [to table])**.** *On a Gram matrix, the values of the first diagonal and the Schur complement are positive at every node of its tree. Let:*

- $h \geq 1$;
- $\mathcal{G} \in \mathrm{Gram}_n$ *(Definition A.14) at* $n := 2^h$.

Define:

- $T := \mathrm{ffLDL}^\dagger(\mathcal{G})$ *(Definition A.20);*
- $\forall \nu \in \mathrm{Sub}(T) :\ (g^\nu_{jk})_{j,k \in \{0,1\}} := \mathcal{G}_\nu$ *(Definition A.32);*
- $\forall \nu \in \mathrm{Sub}(T) :\ d^\nu_{11} := g^\nu_{11} - |g^\nu_{01}|^2 / g^\nu_{00}$.

Then the two diagonals are positive:

1. $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ g^\nu_{00}(\psi) > 0$;
2. $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d^\nu_{11}(\psi) > 0$.

Proof. Proof of items 1 and 2.

(L1) $\forall \psi :\ g_{00}(\psi) > 0$
[$\mathcal{G} \in \mathrm{Gram}_n$ (Definition A.14)]

(L2) $\forall \psi :\ g_{00}(\psi) g_{11}(\psi) - |g_{01}(\psi)|^2 > 0$
[$\mathcal{G} \in \mathrm{Gram}_n$ (Definition A.14)]

(L3) $\forall \psi :\ d^T_{11}(\psi) = (g_{00}(\psi) g_{11}(\psi) - |g_{01}(\psi)|^2) / g_{00}(\psi)$
[$d_{11}(\psi) := g_{11}(\psi) - |g_{01}(\psi)|^2 / g_{00}(\psi)$ (Definition A.17); $\mathcal{G}_T = \mathcal{G}$ (Definition A.32); $T = \mathrm{ffLDL}^\dagger(\mathcal{G})$ (the statement)]

(L4) $\Rightarrow\ \forall \psi :\ d^T_{11}(\psi) > 0$
[(L1), (L2), (L3)]

(L5) $\forall \psi :\ g^T_{00}(\psi) > 0$
[(L1); $g^T_{00} = g_{00}$ ($\mathcal{G}_T = \mathcal{G}$, Definition A.32)]

	Lemma D.5 at $I := (0, \infty)$	This proof
	Shared: $\mathcal{G},\ T,\ g_{00}^{\nu}, d_{11}^{\nu}$	
	I	$(0, \infty)$ (the scope)
(I1)	Assumption A1 Assumption A2	(L5) (L4)
	Its item 1: $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ g_{00}^{\nu}(\psi) \in I$	
	Its item 2: $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d_{11}^{\nu}(\psi) \in I$	

(L6) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ g_{00}^{\nu}(\psi) > 0$

[item 1 of (I1)]

(L7) $\Rightarrow$ item 1

[(L6)]

(L8) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d_{11}^{\nu}(\psi) > 0$

[item 2 of (I1)]

(L9) $\Rightarrow$ item 2

[(L8)]

□ (items 1 and 2)

D.3 Exact structure of the diagonals

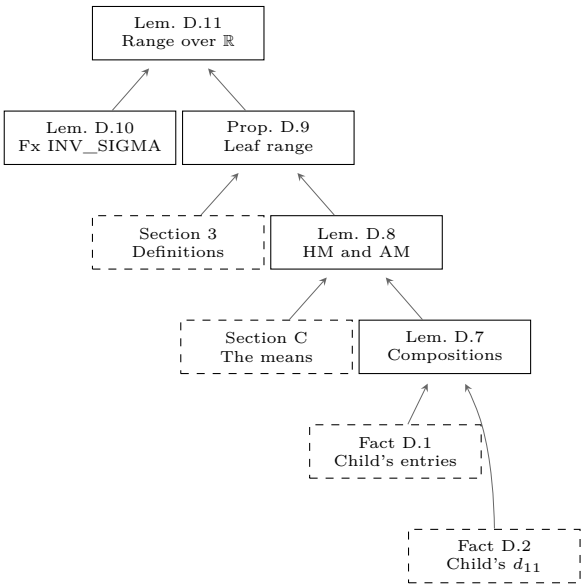


Figure 44: Dependencies, Section D.3.

Fact A.33 (*The key's Gram determinant [to table]*) [to statement].

The NTRU equation makes the root's Gram determinant q^2, which fixes the second diagonal $d_{11} = g_{11} - |g_{01}|^2/g_{00}$ and $\kappa = |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$. Let:

- $\psi \in \mathbb{C}$ *with* $\psi^n = -1$, *a root of* $x^n + 1$.

Define:

- $g_{00} = |f(\psi)|^2 + |g(\psi)|^2$;
- $g_{11} = |F(\psi)|^2 + |G(\psi)|^2$;
- $g_{01} = g(\psi)\,\mathrm{conj}\,G(\psi) + f(\psi)\,\mathrm{conj}\,F(\psi)$ *[LO: sign_core.c: 112-120] [LO: fxp/sign_fxcore.c: 177-193]* (ffSampling$^{\mathcal{F}}$ *(Algorithm 10), line 4);*
- $d_{11} = g_{11} - |g_{01}|^2/g_{00}$ *at the root node* (LDL† *(Algorithm 5), line 19);*

- $\kappa = |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$ *at the root node (*LDL† *(Algorithm 5), line 15);*
- $\kappa_{\text{root}} = \max_\psi \kappa$.

Then the NTRU equation, the determinant, the first diagonal's sign, the second diagonal, κ *and* κ_{root} *are:*

1. $fG - gF = q$ *in* $\mathcal{R}_n$ *[L0: kgen.c: 57-59];*
2. $g_{00}g_{11} - |g_{01}|^2 = q^2$*;*
3. $g_{00} > 0$*;*
4. $d_{11} = q^2/g_{00}$*;*
5. $\kappa = |g_{01}|^2/q^2$*;*
6. $\kappa_{\text{root}} = \max_\psi |g_{01}|^2/q^2$.

Proof. Proof of item 1.

(L1) $fG - gF = q$ in $\mathcal{R}_n$

[keygen (Algorithm 11), line 3 [L0: kgen.c:57-59]]

(L2) $\Rightarrow$ item 1

[(L1)]

□ (item 1)

Proof of item 2.

(L3) $g_{00}g_{11} - |g_{01}|^2 = (|f(\psi)|^2 + |g(\psi)|^2)(|F(\psi)|^2 + |G(\psi)|^2) - |g(\psi)\operatorname{conj} G(\psi) + f(\psi)\operatorname{conj} F(\psi)|^2$

[g_{00}, g_{01}, g_{11} (the statement)]

(L4) $|g(\psi)\operatorname{conj} G(\psi) + f(\psi)\operatorname{conj} F(\psi)|^2$
$= |g(\psi)\operatorname{conj} G(\psi)|^2 + |f(\psi)\operatorname{conj} F(\psi)|^2 + 2\operatorname{Re}(g(\psi)\operatorname{conj} G(\psi)\ \operatorname{conj} f(\psi)\operatorname{conj} F(\psi))$

[Fact A.41, item 33: $|x+y|^2 = |x|^2 + |y|^2 + 2\operatorname{Re}(x \operatorname{conj} y)$, at $x := g(\psi)\operatorname{conj} G(\psi)$, $y := f(\psi)\operatorname{conj} F(\psi)$]

(L5) $g(\psi)\operatorname{conj} G(\psi)\ \operatorname{conj} f(\psi)\operatorname{conj} F(\psi) = \operatorname{conj} f(\psi)G(\psi)\ \operatorname{conj} g(\psi)F(\psi)$

[Fact A.41, item 13: $\operatorname{conj} xy = \operatorname{conj} x\ \operatorname{conj} y$; item 35: $\operatorname{conj}\operatorname{conj} x = x$]

(L6) $\operatorname{Re}(g(\psi)\operatorname{conj} G(\psi)\ \operatorname{conj} f(\psi)\operatorname{conj} F(\psi)) = \operatorname{Re}(f(\psi)G(\psi)\ \operatorname{conj} g(\psi)F(\psi))$

[(L5); Fact A.41, item 36: $\operatorname{Re}\operatorname{conj} x = \operatorname{Re} x$]

(L7) $|g(\psi)\operatorname{conj} G(\psi)|^2 + |f(\psi)\operatorname{conj} F(\psi)|^2 = |g(\psi)|^2|G(\psi)|^2 + |f(\psi)|^2|F(\psi)|^2$

[Fact A.41, item 1: $|xy| = |x||y|$, $|\operatorname{conj} x| = |x|$]

(L8) $\Rightarrow$ $|g(\psi)\operatorname{conj} G(\psi) + f(\psi)\operatorname{conj} F(\psi)|^2$
$= |g(\psi)|^2|G(\psi)|^2 + |f(\psi)|^2|F(\psi)|^2 + 2\operatorname{Re}(f(\psi)G(\psi)\ \operatorname{conj} g(\psi)F(\psi))$

[(L4), (L6), (L7)]

(L9) $|f(\psi)G(\psi) - g(\psi)F(\psi)|^2 = |f(\psi)G(\psi)|^2 + |g(\psi)F(\psi)|^2 - 2\operatorname{Re}(f(\psi)G(\psi)\ \operatorname{conj} g(\psi)F(\psi))$

[Fact A.41, item 34: $|x-y|^2 = |x|^2 + |y|^2 - 2\operatorname{Re}(x \operatorname{conj} y)$, at $x := f(\psi)G(\psi)$, $y := g(\psi)F(\psi)$]

(L10) $|f(\psi)G(\psi)|^2 + |g(\psi)F(\psi)|^2 = |f(\psi)|^2|G(\psi)|^2 + |g(\psi)|^2|F(\psi)|^2$

[Fact A.41, item 1: $|xy| = |x||y|$]

(L11) $\Rightarrow$ $|f(\psi)G(\psi) - g(\psi)F(\psi)|^2$
$= |f(\psi)|^2|G(\psi)|^2 + |g(\psi)|^2|F(\psi)|^2 - 2\operatorname{Re}(f(\psi)G(\psi)\ \operatorname{conj} g(\psi)F(\psi))$

[(L9), (L10)]

(L12) $\Rightarrow$ $g_{00}g_{11} - |g_{01}|^2 = |f(\psi)G(\psi) - g(\psi)F(\psi)|^2$

[(L3), (L8), (L11); expand]

(L13) $(fG - gF)(\psi) = f(\psi)G(\psi) - g(\psi)F(\psi)$

[$(f+g)(\psi) = f(\psi) + g(\psi)$ (Fact A.42, item 6, at $m := n$); $(fg)(\psi) = f(\psi)g(\psi)$ (Fact A.42, item 7, at $m := n$)]

(L14) $(fG - gF)(\psi) = q$

[(L1); $c(\psi) = c$ (Fact A.42, item 8, at $m := n$) at $c := q$]

(L15) $\Rightarrow$ $|f(\psi)G(\psi) - g(\psi)F(\psi)|^2 = q^2$

[(L13), (L14); Fact A.41, item 1: $|a+ib|^2 = a^2+b^2$ at $(a,b) := (q,0)$]

(L16) $\Rightarrow$ $g_{00}g_{11} - |g_{01}|^2 = q^2$

[(L12), (L15)]

(L17) $\Rightarrow$ item 2

[(L16)]

□ (item 2)

Proof of item 3.

(L18) $g_{00} \geq 0$

[$g_{00} = |f(\psi)|^2 + |g(\psi)|^2$ (the statement)]

(L19) $g_{00}g_{11} = q^2 + |g_{01}|^2$

[item 2]

(L20) $q^2 + |g_{01}|^2 > 0$

[$q = 12289$ (Definition A.13)]

(L21) $\Rightarrow$ $g_{00} > 0$

[(L18), (L19), (L20)]

(L22) $\Rightarrow$ item 3

[(L21)]

□ (item 3)

Proof of item 4.

(L23) $d_{11} = (g_{00}g_{11} - |g_{01}|^2)/g_{00}$

[d_{11} (the statement); item 3]

(L24) $\Rightarrow$ $d_{11} = q^2/g_{00}$

[(L23); item 2]

(L25) $\Rightarrow$ item 4

[(L24)]

□ (item 4)

Proof of item 5.

(L26) $\kappa = |g_{01}|^2/q^2$

[κ (the statement); item 2]

(L27) $\Rightarrow$ item 5

[(L26)]

□ (item 5)

Proof of item 6.

(L28) $\kappa_{\text{root}} = \max_\psi \kappa$

[κ_{root} (the statement)]

(L29) $\Rightarrow$ $\kappa_{\text{root}} = \max_\psi |g_{01}|^2/q^2$

[(L28); item 5, $\forall\psi$]

(L30) $\Rightarrow$ item 6

[(L29)]

□ (item 6)

Lemma D.7 (Leaf diagonals as compositions of means [to table])**.** *Below a diagonal w with $\forall\psi,\ \psi^n = -1 :\ w(\psi) > 0$, each leaf diagonal of the tree is a composition of arithmetic and harmonic means of the values $w(\psi)$, $\psi^{n/2} = i$, and such compositions of positive values are positive. Let:*

- $h \geq 2$;

- $w \in \mathcal{R}_n$ *at* $n := 2^h$.

Define:

- *The means*
  - $\mathcal{C}_k$, *that of Definition A.46;*
  - $a_L = (a_1, \dots, a_{2^{k-1}})$ *and* $a_R = (a_{2^{k-1}+1}, \dots, a_{2^k})$, *for* $k \geq 1$ *and* $a \in (0,\infty)^{2^k}$;
- *The roots*
  - $\Psi_j(\omega) = \{\psi \in \mathbb{C} : \psi^{2^j} = \omega\}$, *for* $j \leq h-1$ *and* $\omega^{n/2^j} = -1$;
  - $\omega_2 = e^{i\pi/2}$;
  - $a_w = (w(\psi))_{\psi \in \Psi_{h-1}(\omega_2)}$;
- *The tree*
  - $\mathcal{G}_w$, *that of Definition A.23 at* $d := w$;
  - $T_w = \text{ffLDL}^\dagger(\mathcal{G}_w)$ *(Definition A.20 at* $\mathcal{G} := \mathcal{G}_w$*);*
- *The diagonals*
  - d_i, $i \in I(T_w)$, *the leaf diagonals of* T_w *(Definition A.19);*
  - d^ν_{00} *and* d^ν_{11}, *the diagonals of* LDL† *(Algorithm 5) at* $\mathcal{G}_\nu$, $\nu \in \text{Sub}(T_w)$ *(Definition A.32);*
  - $E_w(0) = \{w\}$ *and* $E_w(j) = \{d^\nu_{00}, d^\nu_{11} : \nu \in \text{Sub}(T_w) \cap \mathcal{T}_{n/2^j}\}$, *for* $1 \leq j \leq h-1$;
- *The compositions*
  - $Q_w(j)$, *for* $j \leq h-1$: $\forall p \in E_w(j)\ \forall \omega,\ \omega^{n/2^j} = -1\ \exists C \in \mathcal{C}_j\ \exists b$, *an ordering of* $(w(\psi))_{\psi \in \Psi_j(\omega)}$: $p(\omega) = C(b)$.

Assume:

(A1) $\forall \psi,\ \psi^n = -1 :\ w(\psi) > 0$.

Then the compositions are positive and the leaf diagonals are compositions:

1. $\forall k \geq 0\ \forall C \in \mathcal{C}_k\ \forall a \in (0,\infty)^{2^k} :\ C(a) > 0$;
2. $\forall i \in I(T_w)\ \exists C \in \mathcal{C}_{h-1}\ \exists b$, *an ordering of* $a_w :\ d_i = C(b)$.

Proof. Proof of item 1.

(L1) $\forall x, y > 0 :\ \text{AM}(x,y) > 0$

[AM (Definition A.46)]

(L2) $\forall x, y > 0 :\ \text{HM}(x,y) > 0$

[HM (Definition A.46)]

(L3) $\forall C \in \mathcal{C}_0\ \forall a \in (0,\infty) :\ C(a) > 0$

[$\mathcal{C}_0 = \{a_1 \mapsto a_1\}$ (Definition A.46)]

(L4) $\forall k \geq 1\ \forall C \in \mathcal{C}_k\ \exists M \in \{\text{AM}, \text{HM}\}\ \exists C_L, C_R \in \mathcal{C}_{k-1}\ \forall a \in (0,\infty)^{2^k} :\ C(a) = M(C_L(a_L), C_R(a_R))$

[$\mathcal{C}_k$ (Definition A.46); a_L, a_R (the statement)]

(L5) $\forall k \geq 1 :\ [\forall C' \in \mathcal{C}_{k-1}\ \forall a' \in (0,\infty)^{2^{k-1}} :\ C'(a') > 0] \Rightarrow\ \forall C \in \mathcal{C}_k\ \forall a \in (0,\infty)^{2^k} :\ C(a) > 0$

[(L1), (L2), (L4)]

(L6) $\Rightarrow\ \forall k \geq 0\ \forall C \in \mathcal{C}_k\ \forall a \in (0,\infty)^{2^k} :\ C(a) > 0$

[induction on k: (L3) the base, (L5) the step]

(L7) $\Rightarrow$ item 1

[(L6)]

□ (item 1)

Proof of item 2.

(L8) $Q_w(0)$

[$\forall \omega,\ \omega^n = -1$: $C := (a_1 \mapsto a_1) \in \mathcal{C}_0$, $b := (w(\omega))$; $\Psi_0(\omega) = \{\omega\}$, $E_w(0)$ (the statement)]

(L9) $\forall j \leq h-2\ \forall \nu' \in \text{Sub}(T_w) \cap \mathcal{T}_{n/2^{j+1}}\ \exists p \in E_w(j) :\ \mathcal{G}_{\nu'} = \mathcal{G}_p$

[$\mathcal{G}_{\nu_{00}} = \mathcal{G}_{d^\nu_{00}}$, $\mathcal{G}_{\nu_{11}} = \mathcal{G}_{d^\nu_{11}}$ (Definition A.32) at every node $\nu = \text{node}(l_{10};\ \nu_{00}, \nu_{11})$ of $T_w = \text{ffLDL}^\dagger(\mathcal{G}_w)$ (the statement); Sub, depth (Definition A.18); $E_w(j)$ (the statement)]

(L10) $\forall j \leq h-2\ \forall \omega',\ \omega'^{n/2^{j+1}} = -1\ \forall \psi',\ \psi'^2 = \omega' :\ (\pm\psi')^{n/2^j} = -1$

[$(\pm\psi')^{n/2^j} = (\psi'^2)^{n/2^{j+1}}$, $n/2^j$ even at $j \leq h-1$]

	Lemma D.4, item 1 at $\mathcal{G}_{\nu'}(\omega')$	This proof
(I1)	g_{00}, g_{01}, g_{11}	$g_{00}^{\nu'}(\omega'), g_{01}^{\nu'}(\omega'), g_{11}^{\nu'}(\omega')$ (Definition A.20)
	d_{00}	$d_{00}^{\nu'}(\omega')$ (Definition A.20)
	l_{10}, zo, d_{11}	$l_{10}^{\nu'}(\omega'), zo^{\nu'}(\omega'), d_{11}^{\nu'}(\omega')$
	$\mathcal{G}, L, D, L^\dagger$	$\mathcal{G}_{\nu'}(\omega'), L^{\nu'}(\omega'), D^{\nu'}(\omega'), L^{\nu'}(\omega')^\dagger$
	$g_{00}, g_{11} \in \mathbb{R}$	$g_{00}^{\nu'}(\omega'),\ g_{11}^{\nu'}(\omega')$ (Definition A.17)
	$g_{01} \in \mathbb{C}$	$g_{01}^{\nu'}(\omega')$ (Definition A.17)
	Assumption A1	$g_{00}^{\nu'}(\omega') = \mathrm{AM}(p(\psi'), p(-\psi'))$ (Fact D.1, item 1; Definition A.20, item 3); (L1) at $p(\pm\psi') > 0$
	Its item 1: $d_{00} = g_{00}$	

(L11) $\forall j \le h-2\ \forall \nu',\ \mathcal{G}_{\nu'} = \mathcal{G}_p,\ p \in E_w(j)\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega',\ p(\pm\psi') > 0 :\ d_{00}^{\nu'}(\omega') = \mathrm{AM}(p(\psi'), p(-\psi'))$

[Fact D.1, item 1, at $m := n/2^j$, $d := p$, $\psi := \psi'$, by (L10); (I1); Definition A.20, items 3 and 4]

(L12) $\forall j \le h-2\ \forall \nu',\ \mathcal{G}_{\nu'} = \mathcal{G}_p,\ p \in E_w(j)\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega',\ p(\pm\psi') > 0 :\ d_{11}^{\nu'}(\omega') = \mathrm{HM}(p(\psi'), p(-\psi'))$

[Fact D.2 at $m := n/2^j$, $d := p$, $\psi := \psi'$, by (L10); Definition A.20, items 3 and 4]

(L13) $\forall j \le h-2\ \forall \omega',\ \omega'^{n/2^{j+1}} = -1\ \forall \psi',\ \psi'^2 = \omega'\ \forall z \in \mathbb{C} :\ z^2 = \omega' \iff z \in \{\psi', -\psi'\}$

[Fact A.43, item 4, at $(\omega, \psi') := (\omega', \psi')$, $\psi' \ne 0$ by $\psi'^{n/2^j} = -1$, (L10)]

(L14) $\forall j \le h-2\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega' :\ \Psi_{j+1}(\omega') = \Psi_j(\psi') \cup \Psi_j(-\psi')$

[(L13) at $z := \psi^{2^j}$; Ψ_j (the statement)]

(L15) $\forall j \le h-2\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega' :\ \psi' \ne -\psi'$

[$|\psi'| = 1$ (Fact A.42, item 1, by (L10))]

(L16) $\forall j \le h-2\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega' :\ \Psi_j(\psi') \cap \Psi_j(-\psi') = \emptyset$

[(L15); Ψ_j (the statement)]

(L17) $\forall j \le h-2 :\ Q_w(j) \Rightarrow\ \forall p \in E_w(j)\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega' :$
$p(\pm\psi') = C_\pm(b_\pm),\ b_\pm$ an ordering of $(w(\psi))_{\psi \in \Psi_j(\pm\psi')}$

[$Q_w(j)$ at $\omega := \pm\psi'$, by (L10)]

(L18) $\forall j \le h-2 :\ Q_w(j) \Rightarrow\ \forall p \in E_w(j)\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega' :\ C_\pm \in \mathcal{C}_j$

[$Q_w(j)$ at $\omega := \pm\psi'$, by (L10)]

(L19) $\forall j \le h-2 :\ Q_w(j) \Rightarrow\ \forall p \in E_w(j)\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega' :\ p(\pm\psi') > 0$

[(L17), (L18); (L6) at $a := b_\pm$, positive by assumption A1]

(L20) $\forall j \le h-2 :\ Q_w(j) \Rightarrow\ \forall p \in E_w(j)\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega' :$
(b_+, b_-) an ordering of $(w(\psi))_{\psi \in \Psi_{j+1}(\omega')}$

[(L17); (L14), (L16)]

(L21) $\forall j \le h-2 :\ Q_w(j) \Rightarrow\ \forall p \in E_w(j)\ \forall \omega'\ \forall \psi',\ \psi'^2 = \omega'\ \forall M \in \{\mathrm{AM}, \mathrm{HM}\} :$
$\exists C \in \mathcal{C}_{j+1} :\ M(C_+(b_+), C_-(b_-)) = C((b_+, b_-))$

[(L18); $\mathcal{C}_k$ (Definition A.46) at $k := j+1$; a_L, a_R (the statement) at $a := (b_+, b_-)$]

(L22) $\forall j \le h-2 :\ Q_w(j) \Rightarrow\ Q_w(j+1)$

[(L9), (L11), (L12), (L17), (L19); (L20), (L21)]

(L23) $\Rightarrow\ Q_w(h-1)$

[induction on j: (L8) the base, (L22) the step]

(L24) $\forall i \in I(T_w)\ \exists \nu \in \mathrm{Sub}(T_w) \cap \mathcal{T}_2\ \exists p \in \{d_{00}^\nu, d_{11}^\nu\} :\ d_i = p(\omega_2)$

[d_i (Definition A.19); the leaf diagonals of a node of degree 2 (Definition A.18); Definition A.20, items 1 and 2, at $\mathcal{G}_\nu(\omega_2)$]

(L25) $\Rightarrow\ \forall i \in I(T_w)\ \exists C \in \mathcal{C}_{h-1}\ \exists b,$ an ordering of $a_w :\ d_i = C(b)$

[(L23) at $\omega := \omega_2$, $\omega_2^2 = -1$; (L24); $E_w(h-1)$, a_w (the statement)]

(L26) $\Rightarrow$ item 2

[(L25)]

□ (item 2)

Lemma D.8 (Leaf diagonals between the harmonic and arithmetic means [to table])**.** *Below a diagonal w with $\forall \psi,\ \psi^n = -1 :\ w(\psi) > 0$, each leaf diagonal of the tree lies between the harmonic and the arithmetic mean of the values $w(\psi_k)$, $k < n/2$, ψ_k the roots with positive imaginary part.*
Let:

- $h \geq 2$;
- $w \in \mathcal{R}_n$ *at* $n := 2^h$.

Define:

- $\psi_k = e^{i\pi(2k+1)/n}$, $k < n/2$ *(Definition A.32 at* $m := n$*);*
- $\mathrm{AM}_\psi(w) = \mathrm{AM}_{\mathrm{all}}((w(\psi_k))_{k<n/2})$ *and* $\mathrm{HM}_\psi(w) = \mathrm{HM}_{\mathrm{all}}((w(\psi_k))_{k<n/2})$ *(Definition A.46);*
- $T_w = \mathrm{ffLDL}^\dagger(\mathcal{G}_w)$ *and* $\mathcal{G}_w$*, those of Lemma D.7;*
- d_i, $i \in I(T_w)$*, the leaf diagonals of* T_w *(Definition A.19);*
- $\mathcal{C}_k$*, that of Definition A.46;*
- $\Psi_j(\omega) = \{\psi \in \mathbb{C} : \psi^{2^j} = \omega\}$*, for* $j \leq h-1$ *and* $\omega^{n/2^j} = -1$ *(Lemma D.7);*
- $\omega_2 = e^{i\pi/2}$ *and* $a_w = (w(\psi))_{\psi \in \Psi_{h-1}(\omega_2)}$ *(Lemma D.7).*

Assume:
(A1) $\forall \psi,\ \psi^n = -1 :\ w(\psi) > 0$.
Then

$$\forall i \in I(T_w) :\quad \mathrm{HM}_\psi(w) \leq d_i \leq \mathrm{AM}_\psi(w).$$

Proof. (I1)

Lemma D.7, item 2	This proof
Shared: $h, w,\ T_w, d_i, \mathcal{C}_k,\ \Psi_j, \omega_2, a_w$ Shared: assumption A1	
Its conclusion: $\forall i \in I(T_w)\ \exists C \in \mathcal{C}_{h-1}\ \exists b,$ an ordering of $a_w :\ d_i = C(b)$	

$\forall i \in I(T_w)\ \exists C \in \mathcal{C}_{h-1}\ \exists b,$ an ordering of $a_w :\ d_i = C(b)$ [(I1)]

(L2) $\forall m \geq 1\ \forall a \in (0,\infty)^m\ \forall b,$ an ordering of $a :\ \mathrm{AM}_{\mathrm{all}}(b) = \mathrm{AM}_{\mathrm{all}}(a)$ [$\mathrm{AM}_{\mathrm{all}}$ (Definition A.46)]

(L3) $\forall m \geq 1\ \forall a \in (0,\infty)^m\ \forall b,$ an ordering of $a :\ \mathrm{HM}_{\mathrm{all}}(b) = \mathrm{HM}_{\mathrm{all}}(a)$ [$\mathrm{HM}_{\mathrm{all}}$ (Definition A.46)]

Lemma C.2 at every $i \in I(T_w)$	This proof
Shared: $\mathcal{C}_k$, $\mathrm{AM}_{\mathrm{all}}$, $\mathrm{HM}_{\mathrm{all}}$ (Definition A.46)	
(I2) k	$h-1$ (the statement)
m	2^{h-1}
C	C (L1)
$(a_1, \ldots, a_m)$	b (L1)
$k \geq 0$	$h \geq 2$ (the statement)
$C \in \mathcal{C}_k$	(L1)
$a_1, \ldots, a_m > 0$	b, an ordering of a_w (L1); a_w (the statement); assumption A1
Its conclusion: $\mathrm{HM}_{\mathrm{all}} \leq C(a_1, \ldots, a_m) \leq \mathrm{AM}_{\mathrm{all}}$	

(L4) $\forall i \in I(T_w) :\ \mathrm{HM}_{\mathrm{all}}(a_w) \leq d_i$ [(L1), (L3); (I2)]

(L5) $\forall i \in I(T_w) :\ d_i \leq \mathrm{AM}_{\mathrm{all}}(a_w)$ [(L1), (L2); (I2)]

(L6) $\forall \psi,\ \psi^n = -1 :\ w(\operatorname{conj}\psi) = w(\psi)$ [Fact A.42, item 2: $w(\operatorname{conj}\psi) = \operatorname{conj} w(\psi)$; $w(\psi) \in \mathbb{R}$ (assumption A1)]

(L7) $\forall g :\ [\forall \psi :\ g(\operatorname{conj}\psi) = g(\psi)] \Rightarrow\ \sum_{\psi \in \Psi_{h-1}(\omega_2)} g(\psi) = \sum_{k<n/2} g(\psi_k),\ |\Psi_{h-1}(\omega_2)| = n/2$ [Fact A.43, item 7, at $m := n$; $\Psi_{h-1}(\omega_2) = \{\psi : \psi^{n/2} = i\}$ (Ψ_j, ω_2, the statement)]

(L8) $\mathrm{AM}_{\mathrm{all}}(a_w) = \mathrm{AM}_\psi(w)$
[(L7) at $g := w$, by (L6); $\mathrm{AM}_{\mathrm{all}}$ (Definition A.46); a_w, AM_ψ (the statement)]

(L9) $\mathrm{HM}_{\mathrm{all}}(a_w) = \mathrm{HM}_\psi(w)$
[(L7) at $g := 1/w$, by (L6); $\mathrm{HM}_{\mathrm{all}}$ (Definition A.46); a_w, HM_ψ (the statement)]

(L10) $\Rightarrow\ \forall i \in I(T_w):\ \mathrm{HM}_\psi(w) \le d_i$
[(L4), (L9)]

(L11) $\Rightarrow\ \forall i \in I(T_w):\ \mathrm{HM}_\psi(w) \le d_i \le \mathrm{AM}_\psi(w)$
[(L10); (L5), (L8)]

(L12) $\Rightarrow$ the statement
[(L11)]

□

Proposition D.9 (The range of the leaf diagonals [to table])**.** *On a key the key generation accepts, every leaf diagonal lies between* $q^2/16822$ *and* 16822*. Define:*

- d_i, $i \le N$, *the leaf diagonals of* T *(Definition A.19).*

Then

$$\forall i \le N: \quad d_i \in [q^2/16822,\ 16822].$$

Proof.

DEFINES
h: $n = 2^h$; T_{00}, T_{11}: $T = \mathrm{node}(l_{10};\ T_{00}, T_{11})$
$d_{00}, d_{11} \in \mathcal{R}_n$, the root node's diagonals: LDL† (Algorithm 5) at $\mathcal{G}(\psi)$, $\psi^n = -1$
$\psi_k := e^{i\pi(2k+1)/n}$, $k < n/2$ (Definition A.32 at $m := n$)
$(w, d_w, T_w) \in \{(g_{00}, d_{00}, T_{00}),\ (q^2/g_{00}, d_{11}, T_{11})\}$, w a function on $\{\psi : \psi^n = -1\}$
$\mathrm{AM}_\psi(w) := \mathrm{AM}_{\mathrm{all}}((w(\psi_k))_{k<n/2})$, $\mathrm{HM}_\psi(w) := \mathrm{HM}_{\mathrm{all}}((w(\psi_k))_{k<n/2})$
(Definition A.46; Fact A.34)

(L1) $\forall \psi,\ \psi^n = -1:\ g_{00}(\psi) > 0$
[Fact A.33, item 3]

(I1)

Lemma D.4 $\forall \psi,\ \psi^n = -1$	This proof
g_{00}, g_{01}, g_{11}	$g_{00}(\psi), g_{01}(\psi), g_{11}(\psi)$ (the proof's block)
d_{00}	$d_{00}(\psi)$ (the proof's block)
μ, l_{10}, zo, d_{11}	$\mu(\psi), l_{10}(\psi), zo(\psi), d_{11}(\psi)$
$\mathcal{G}, L, D, L^\dagger$	$\mathcal{G}(\psi), L(\psi), D(\psi), L(\psi)^\dagger$
$g_{00}, g_{11} \in \mathbb{R}$	$g_{00}(\psi)$, $g_{11}(\psi)$ (Definition A.17)
$g_{01} \in \mathbb{C}$	$g_{01}(\psi)$ (Definition A.17)
Assumption A1	(L1)
Its item 1: $d_{00} = g_{00}$	

(L2) $\forall \psi:\ d_{00}(\psi) = g_{00}(\psi)$
[item 1 of (I1)]

(L3) $\forall \psi:\ d_{11}(\psi) = q^2/g_{00}(\psi)$
[Fact A.33, item 4]

(L4) $\forall w\ \forall \psi:\ w(\psi) > 0$
[(L1); w (the proof's block)]

(L5) $\forall w\ \forall \psi:\ d_w(\psi) = w(\psi)$
[(L2), (L3); d_w (the proof's block)]

(L6) $h \ge 2$
[$n = 2^h$ (the proof's block); $n \in \{512, 1024\}$ (Fact A.34)]

(L7) $\forall w:\ T_w = \mathrm{ffLDL}^\dagger(\mathcal{G}_{d_w})$
[T_w (the proof's block); Definition A.20, items 5, 6 and 7]

(L8) $\forall w\ \forall \psi,\ \psi^n = -1:\ d_w(\psi) > 0$
[(L4), (L5)]

	Lemma D.8 at every w of the proof's block	This proof
	Shared: h, T_w (L7), d_i, ψ_k, $\mathcal{C}_k$ (Definition A.46)	
	w	d_w (the proof's block)
	$\mathrm{AM}_\psi(w)$	$\mathrm{AM}_\psi(d_w)$ (the proof's block)
(I2)	$\mathrm{HM}_\psi(w)$	$\mathrm{HM}_\psi(d_w)$ (the proof's block)
	Ψ_j, ω_2, a_w	$\Psi_j, \omega_2, a_{d_w}$
	$h \geq 2$	(L6)
	$w \in \mathcal{R}_n$	$d_w \in \mathcal{R}_n$ (the proof's block)
	Assumption A1	(L8)
	Its conclusion: $\forall i \in I(T_w) :\ \mathrm{HM}_\psi(w) \leq d_i \leq \mathrm{AM}_\psi(w)$	

(L9) $\forall w\ \forall i \in I(T_w) :\ \mathrm{HM}_\psi(d_w) \leq d_i \leq \mathrm{AM}_\psi(d_w)$

[(I2)]

(L10) $\forall w :\ \mathrm{AM}_\psi(d_w) = \mathrm{AM}_\psi(w)$

[(L5); AM_ψ (the proof's block)]

(L11) $\forall w :\ \mathrm{HM}_\psi(d_w) = \mathrm{HM}_\psi(w)$

[(L5); HM_ψ (the proof's block)]

(L12) $\forall w\ \forall i \in I(T_w) :\ \mathrm{HM}_\psi(w) \leq d_i \leq \mathrm{AM}_\psi(w)$

[(L9), (L10), (L11)]

(L13) $\forall m \geq 1\ \forall a \in (0,\infty)^m :\ \mathrm{HM}_{\mathrm{all}}(a) = 1/\,\mathrm{AM}_{\mathrm{all}}((1/a_i)_i)$

[$\mathrm{HM}_{\mathrm{all}}$, $\mathrm{AM}_{\mathrm{all}}$ (Definition A.46)]

(L14) $\forall m \geq 1\ \forall a \in (0,\infty)^m\ \forall c > 0 :\ \mathrm{AM}_{\mathrm{all}}((ca_i)_i) = c\ \mathrm{AM}_{\mathrm{all}}(a)$

[$\mathrm{AM}_{\mathrm{all}}$ (Definition A.46)]

(L15) $\mathrm{HM}_\psi(g_{00}) = q^2/\,\mathrm{AM}_\psi(q^2/g_{00})$

[(L13) at $a := (g_{00}(\psi_k))_k$; (L14) at $c := q^2$, $a := (1/g_{00}(\psi_k))_k$; (L1); AM_ψ, HM_ψ (the proof's block)]

(L16) $\mathrm{HM}_\psi(q^2/g_{00}) = q^2/\,\mathrm{AM}_\psi(g_{00})$

[(L13) at $a := (q^2/g_{00}(\psi_k))_k$; (L14) at $c := 1/q^2$, $a := (g_{00}(\psi_k))_k$; (L1); AM_ψ, HM_ψ (the proof's block)]

(L17) $\mathrm{AM}_\psi(g_{00}) \leq 16822$

[Fact A.34]

(L18) $\mathrm{AM}_\psi(q^2/g_{00}) < (0.999 \cdot 1.17)^2 q$

[Fact A.34]

(L19) $(0.999 \cdot 1.17)^2 q < 16822$

[Fact A.34: $(0.999 \cdot 1.17)^2 q = 16788.7841$]

(L20) $\Rightarrow\ \mathrm{AM}_\psi(q^2/g_{00}) < 16822$

[(L18), (L19)]

(L21) $\forall x, y > 0 :\ x \leq y \Rightarrow\ q^2/y \leq q^2/x$

[Fact A.41, item 5: $t \mapsto 1/t$ nonincreasing on $(0,\infty)$]

(L22) $\mathrm{AM}_\psi(q^2/g_{00}) > 0$

[(L4); $\mathrm{AM}_{\mathrm{all}}$ (Definition A.46)]

(L23) $q^2/16822 \leq q^2/\,\mathrm{AM}_\psi(q^2/g_{00})$

[(L20), (L21), (L22)]

(L24) $\Rightarrow\ q^2/16822 \leq \mathrm{HM}_\psi(g_{00})$

[(L23), (L15)]

(L25) $\Rightarrow\ \forall i \in I(T_{00}) :\ q^2/16822 \leq d_i$

[(L24); (L12) at $w := g_{00}$]

(L26) $\forall i \in I(T_{00}) :\ d_i \leq 16822$

[(L12) at $w := g_{00}$; (L17)]

(L27) $\mathrm{AM}_\psi(g_{00}) > 0$

[(L4); $\mathrm{AM}_{\mathrm{all}}$ (Definition A.46)]

(L28) $q^2/16822 \leq q^2/\,\mathrm{AM}_\psi(g_{00})$

[(L17), (L21), (L27)]

(L29) $\Rightarrow$ $q^2/16822 \le \mathrm{HM}_\psi(q^2/g_{00})$

[(L28), (L16)]

(L30) $\Rightarrow$ $\forall i \in I(T_{11}):\ q^2/16822 \le d_i$

[(L29); (L12) at $w := q^2/g_{00}$]

(L31) $\forall i \in I(T_{11}):\ d_i \le 16822$

[(L12) at $w := q^2/g_{00}$; (L20)]

(L32) $I(T_{00}) \cup I(T_{11}) = \{1, \ldots, N\}$

[Fact A.31, item 2]

(L33) $\Rightarrow$ $\forall i \le N:\ d_i \in [q^2/16822,\ 16822]$

[(L25), (L26), (L30), (L31), (L32)]

(L34) $\Rightarrow$ the statement

[(L33)]

□

Lemma D.10 (The fixed-point signer's stored word `INV_SIGMA` [to table])**.** *For the fixed-point signer, the stored inverse standard deviation is $1/s$ within one rounding of its realization. Let:*

- *The signer be the fixed-point signer at $(u, \zeta) = (0, 2^{-64})$ (Definition A.4, item 8).*

Define:

- `INV_SIGMA`*, the number of the signer's stored word at* $\log_2 n$*:* `FXP_INV_SIGMA` *of* ***fxp/*** *[L0: fxp/fxp_consts.h:2058-2070];*
- $c_n = 1/s$.

Measured:

- $(\texttt{INV_SIGMA} - \zeta)\, s \le 1 + u$ *for the fixed-point signer at its (u, ζ), at $n = 512$ and $n = 1024$ [gate: verify/gates/sampler/invsigma_fx.py];*
- $(\texttt{INV_SIGMA} + \zeta)\, s \ge 1 - u$ *for the fixed-point signer at its (u, ζ), at $n = 512$ and $n = 1024$ [gate: verify/gates/sampler/invsigma_fx.py].*

Then

$$\texttt{INV_SIGMA}\ \mathcal{I}\left(u^{\pm}, \zeta^{\pm}\right)\ c_n.$$

Proof. (L1) $s > 0$

[$s = 1.17\sqrt{q}\,\sigma_{\min}$ (Definition A.25); the stored word $\sigma_{\min} > 0$ [L0: fxp/fxp_consts.h:2073-2084]]

(L2) $\texttt{INV_SIGMA} - c_n \le u c_n + \zeta$

[the first measured row, divided by $s > 0$ ((L1)); $c_n = 1/s$ (the statement)]

(L3) $c_n - \texttt{INV_SIGMA} \le u c_n + \zeta$

[the second measured row, divided by $s > 0$ ((L1)); $c_n = 1/s$ (the statement)]

(L4) $\Rightarrow$ $\exists\, u_\circ, \zeta_\circ \in \mathbb{R},\ |u_\circ| \le u,\ |\zeta_\circ| \le \zeta:\ \texttt{INV_SIGMA} = c_n(1 + u_\circ) + \zeta_\circ$

[(L2), (L3) at $u_\circ := \max(-u, \min(u, (\texttt{INV_SIGMA} - c_n)/c_n))$, $\zeta_\circ := \texttt{INV_SIGMA} - c_n(1 + u_\circ)$, $c_n > 0$ by (L1)]

(L5) $\Rightarrow$ the statement

[(L4); Definition A.10]

□

Lemma D.11 (The range of the leaf standard deviations over $\mathbb{R}$ [to table])**.** *On a key the key generation accepts, every leaf standard deviation over $\mathbb{R}$ lies strictly between $\sigma_{\min}$ and $1.17^2\sigma_{\min}$, for the fixed-point signer's stored constants. Let:*

- *The signer be the fixed-point signer at $(u, \zeta) = (0, 2^{-64})$ (Definition A.4, item 8).*

Define:

- `INV_SIGMA`*, the number of the signer's stored word at* $\log_2 n$*:* `FXP_INV_SIGMA` *of* ***fxp/*** *[L0: fxp/fxp_consts.h:2058-2070];*

- $c_n = 1/s$;
- d_i, $i \le N$, *the leaf diagonals of* T *(Definition A.19);*
- $\sigma_i := 1/(\sqrt{d_i}\, c_n)$, *the standard deviation of the leaf* i *over* $\mathbb{R}$*: lines 1 and 3 of* deepest *(Algorithm 7) over* $\mathbb{R}$*, at* $\texttt{INV_SIGMA} = c_n$.

Measured:

- $\sqrt{16822}\,\sigma_{\min}(\texttt{INV_SIGMA} + \zeta)/(1-u) < 1$ *for the fixed-point signer at its* (u, ζ)*, at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/sampler/leafsigma_fx.py];*
- $\sqrt{q^2/16822} \cdot 1.17^2\sigma_{\min}(\texttt{INV_SIGMA} - \zeta)/(1+u) > 1$ *for the fixed-point signer at its* (u, ζ)*, at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/sampler/leafsigma_fx.py].*

We have

1. $\forall i \le N :\ \sigma_i > \sigma_{\min}$;
2. $\forall i \le N :\ \sigma_i < 1.17^2\sigma_{\min}$.

Proof. (L1) $\forall i \le N :\ d_i \in [q^2/16822,\ 16822]$

[Proposition D.9]

(L2) $q^2/16822 > 0$

[expand]

(L3) $\texttt{INV_SIGMA}\ \mathcal{I}\,(u^{\pm}, \zeta^{\pm})\ c_n$

[Lemma D.10 at the signer and n]

(L4) $c_n, \sigma_{\min} > 0$

[$c_n = 1/s$ (the statement); $s = 1.17\sqrt{q}\,\sigma_{\min}$ (Definition A.25); the stored word [L0: fxp/fxp_consts.h:2073-2084]]

(L5) $c_n \le (\texttt{INV_SIGMA} + \zeta)/(1-u)$

[(L3), (L4); $u < 1$ (the statement)]

(L6) $c_n \ge (\texttt{INV_SIGMA} - \zeta)/(1+u)$

[(L3), (L4)]

(L7) $\forall i \le N :\ \sqrt{d_i} \le \sqrt{16822}$

[(L1); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L8) $\forall i \le N :\ \sqrt{d_i} \ge \sqrt{q^2/16822}$

[(L1), (L2); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L9) $\forall i \le N :\ \sqrt{d_i}\, c_n \sigma_{\min} < 1$

[(L4), (L5), (L7); the first measured row; $\forall a, a', b, b' \in \mathbb{R},\ 0 \le a \le a',\ 0 \le b \le b' :\ ab \le a'b'$ (Fact A.41, item 8)]

(L10) $\forall i \le N :\ \sigma_i > \sigma_{\min}$

[(L4), (L9); σ_i (the statement)]

(L11) $\forall i \le N :\ \sqrt{d_i}\, c_n \cdot 1.17^2\sigma_{\min} > 1$

[(L2), (L4), (L6), (L8); the second measured row; $\forall a, a', b, b' \in \mathbb{R},\ 0 \le a \le a',\ 0 \le b \le b' :\ ab \le a'b'$ (Fact A.41, item 8)]

(L12) $\forall i \le N :\ \sigma_i < 1.17^2\sigma_{\min}$

[(L4), (L11); σ_i (the statement)]

(L13) $\Rightarrow$ item 1

[(L10)]

(L14) $\Rightarrow$ item 2

[(L12)]

$\square$ (items 1 and 2)

E Proofs of the Rényi divergence argument

This appendix proves the statements of Sections 4.2 and 4.3. The proofs follow the conventions of Appendix D. Section E.1 proves the Rényi divergence of two leaf Gaussians in closed form; Section E.2 proves the bound on the normalizer ratio Φ; Section E.3 proves the composition on the tail-cut event; Section E.4 proves probability preservation; Section E.5 proves the product bound on a leaf's Rényi divergence.

How each statement is verified. Table 16 lists how each fact, lemma and corollary placed here is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma E.1	✓				
Lemma E.2	✓				
Fact E.4	✓				
Lemma E.5	✓				
Lemma E.6	✓				
Lemma E.7	✓				
Lemma E.8	✓				
Lemma E.9	✓				
Lemma E.10	✓				
Lemma E.11	✓				
Lemma E.12	✓				
Cor. E.13	✓				
Cor. E.14	✓				
Lemma E.15	✓				
Lemma E.16	✓				
Lemma E.17	✓				
Lemma E.18	✓				L1: DRS14, Lem. 2.13
Lemma E.20	✓				
Cor. E.21	✓				

Table 16: Appendix E: its facts, and how each lemma and corollary is verified.

E.1 The divergence at one leaf

This subsection proves Lemma 4.1.

Lemma E.1 (The weighted sum of two squares [to table])**.** *A weighted sum of two squares completes to one square at the weighted mean. Let:*

- $A, B, c, c' \in \mathbb{R}$.

Define:

- $m = (Ac + Bc')/(A + B)$.

Assume:

(A1) $A + B \neq 0$.

Then the square completes:

$$\forall x \in \mathbb{R}: \quad A(x-c)^2 + B(x-c')^2 = (A+B)(x-m)^2 + \frac{AB}{A+B}(c-c')^2.$$

Proof. (L1) $\forall x \in \mathbb{R}: \ A(x-c)^2 + B(x-c')^2 = (A+B)x^2 - 2(Ac+Bc')x + Ac^2 + Bc'^2$ [expand]

(L2) $\forall x \in \mathbb{R}: \ (A+B)(x-m)^2 = (A+B)x^2 - 2(Ac+Bc')x + \frac{(Ac+Bc')^2}{A+B}$ [$m = (Ac+Bc')/(A+B)$ (the statement); $A+B \neq 0$ (assumption A1); expand]

(L3) $(A+B)(Ac^2+Bc'^2) - (Ac+Bc')^2 = AB(c-c')^2$ [expand]

(L4) $\forall x \in \mathbb{R}:\ A(x-c)^2 + B(x-c')^2 - (A+B)(x-m)^2 = Ac^2 + Bc'^2 - \frac{(Ac+Bc')^2}{A+B}$
[(L1), (L2)]

(L5) $Ac^2 + Bc'^2 - \frac{(Ac+Bc')^2}{A+B} = \frac{AB}{A+B}(c-c')^2$
[(L3) divided by $A+B \neq 0$ (assumption A1)]

(L6) $\Rightarrow$ the statement
[(L4), (L5)]
□

Lemma 4.1 (*The Rényi divergence of two leaf Gaussians in closed form [to table]*) [to statement].
The Rényi divergence of two leaf Gaussians at the order α is a closed form in a merged standard deviation s'' and a merged center m. Define:

- $G_1 = D_{\mathbb{Z},s_1,c}$ *and* $G_2 = D_{\mathbb{Z},s_2,c'}$, *the* $D_{\mathbb{Z},s,c}$ *of Definition A.2 at* $s := s_1$ *and at* $(s,c) := (s_2, c')$;
- $A = \alpha/s_1^2$;
- $B = (1-\alpha)/s_2^2$;
- $m = (Ac + Bc')/(A+B)$ *(Lemma E.1);*
- $s'' = (A+B)^{-1/2}$.

Assume:
(A1) $s_1^2 < s_2^2\,\alpha/(\alpha-1)$.
Then

$$R_\alpha(G_1 \| G_2)^{\alpha-1} = \frac{\rho_{s'',m}(\mathbb{Z})\ \exp\left(\alpha(\alpha-1)(c-c')^2 s''^2/(2s_1^2 s_2^2)\right)}{\rho_{s_1,c}(\mathbb{Z})^\alpha\ \rho_{s_2,c'}(\mathbb{Z})^{1-\alpha}}.$$

Proof. (L1) $\forall z \in \mathbb{Z}:\ G_1(z)^\alpha G_2(z)^{1-\alpha} = \frac{\rho_{s_1,c}(z)^\alpha\ \rho_{s_2,c'}(z)^{1-\alpha}}{\rho_{s_1,c}(\mathbb{Z})^\alpha\ \rho_{s_2,c'}(\mathbb{Z})^{1-\alpha}}$
[$D_{\mathbb{Z},s,c}(z) = \rho_{s,c}(z)/\rho_{s,c}(\mathbb{Z})$ (Definition A.2, item 2), at $(s,c) := (s_1,c)$ and at $(s,c) := (s_2,c')$]

(L2) $\forall z \in \mathbb{Z}:\ \rho_{s_1,c}(z)^\alpha\ \rho_{s_2,c'}(z)^{1-\alpha} = \exp(-\frac{1}{2}(A(z-c)^2 + B(z-c')^2))$
[Definition A.2, item 1, at $(s,c) := (s_1,c)$ and at (s_2,c'), raised to the powers α and $1-\alpha$; A, B (the statement)]

(L3) $A + B = \frac{\alpha s_2^2 - (\alpha-1)s_1^2}{s_1^2 s_2^2}$
[A, B (the statement); expand]

(L4) $A + B > 0$
[(L3); assumption A1 multiplied by $(\alpha-1)/(s_1^2 s_2^2) > 0$]

Lemma E.1 at every $z \in \mathbb{Z}$	This proof
Shared: $A, B, c, c',\ m$	
x	z
(I1) $A, B, c, c' \in \mathbb{R}$	A, B, G_1, G_2 (the statement); Definition A.2
$x \in \mathbb{R}$	$z \in \mathbb{Z}$
Assumption A1	(L4)
Its conclusion: $\forall x \in \mathbb{R}:\ A(x-c)^2 + B(x-c')^2 = (A+B)(x-m)^2 + \frac{AB}{A+B}(c-c')^2$	

(L5) $\forall z \in \mathbb{Z}:\ \exp(-\frac{1}{2}(A(z-c)^2 + B(z-c')^2)) = \exp(-\frac{1}{2}(A+B)(z-m)^2)\exp(-\frac{1}{2}\frac{AB}{A+B}(c-c')^2)$
[(I1); Fact A.41, item 12: $e^x e^y = e^{x+y}$]

(L6) $-\frac{AB}{A+B} = \frac{\alpha(\alpha-1)s''^2}{s_1^2 s_2^2}$
[A, B (the statement); expand; $1/(A+B) = s''^2$ (the statement; (L4))]

(L7) $\forall z \in \mathbb{Z}:\ \exp(-\frac{1}{2}(A+B)(z-m)^2) = \rho_{s'',m}(z)$
[$1/(A+B) = s''^2$ (the statement; (L4)); Definition A.2, item 1, at $(s,c) := (s'',m)$]

(L8) $\Rightarrow$ the statement
[(L1), (L2), (L5), (L6), (L7) summed over $z \in \mathbb{Z}$; $\rho_{s,c}$ (Definition A.2) at $(s,c) := (s'',m)$; Definition A.3, item 2, at $(X,\mu,\nu) := (\mathbb{Z}, G_1, G_2)$; $G_2 > 0$ on $\mathbb{Z}$ ($D_{\mathbb{Z},s,c} \in (0,1]$, Definition A.2, at $(s,c) := (s_2,c')$)]
□

E.2 The normalizer ratio to second order

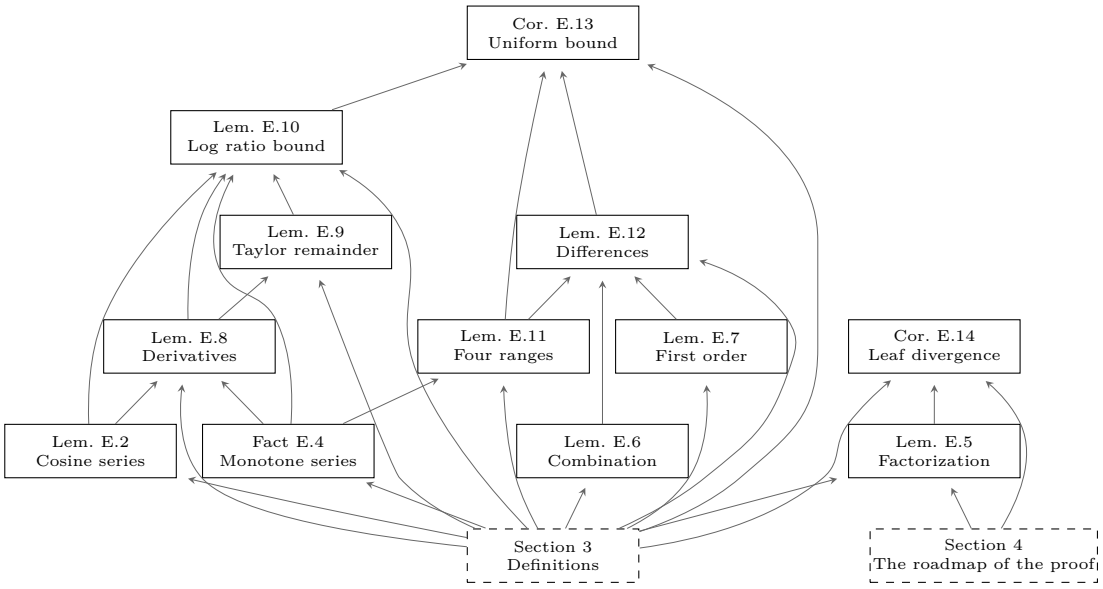


Figure 45: Dependencies, Section E.2.

This subsection proves the bound on the normalizer ratio Φ. Lemma E.2 states the series of the deviation; Lemma E.5 the factorization of the leaf divergence; Lemma E.10 the bound on $\ln \Phi$; Corollary E.13 the uniform bound over the four ranges.

The series of the normalizer deviation (Definition A.38). Let $s > 0$ be a standard deviation, and $j \in \{0, 1, 2, 3, 4\}$ an index. The **series** of the normalizer deviation $d(s, c)$ (Definition A.29) at s is $\varepsilon_j(s) := 2 \sum_{k \geq 1} (2\pi k)^j e^{-2\pi^2 s^2 k^2}$.

The normalizer ratio Φ, its differences and the remainder form Q (Definition A.39). Let $s > 0$ be a standard deviation, $c' \in \mathbb{R}$ a center, and $v = (v_s, v_c) \in \mathbb{R}^2$ a vector. Let $\delta > -1$ with $\alpha + (1 - \alpha)(1 + \delta)^2 > 0$ be a relative perturbation, and $\Delta \in \mathbb{R}$ a shift. Define $s_1 := s(1 + \delta)$, $s_2 := s$, $c := c' + \Delta$, $s'' := s(1 + \delta)\theta_\alpha(\delta)^{1/2}$ and $m := c' + \alpha\theta_\alpha(\delta)\Delta$, the s'' and m of Lemma 4.1 at (s_1, s_2, c, c'). The **normalizer ratio** at (s, δ, c', Δ) is $\Phi(s, \delta, c', \Delta) := (1 + d(s'', m))\,(1 + d(s_1, c))^{-\alpha}\,(1 + d(s_2, c'))^{\alpha - 1}$, with d that of Definition A.29. The **first difference** is $v_1 := (s_1, c) - (s_2, c')$, and the **second difference** is $v'' := (s'', m) - (s_2, c')$. Define $s_- := \min(s, s_1, s'')$ and $s_+ := \max(s, s_1, s'')$. The **remainder form** is $Q(v) := \left(s_+^2 \varepsilon_4(s_-) + \varepsilon_2(s_-)\right) v_s^2 + 2 s_+ \varepsilon_3(s_-) |v_s| |v_c| + \varepsilon_2(s_-) v_c^2$.

The uniform bound $\bar{\phi}_{\mathrm{u}}$ over the four ranges (Definition A.40). Let $s_{\mathrm{lo}} > 0$ and $s_{\mathrm{hi}} \geq s_{\mathrm{lo}}$ be standard deviations, $\bar{\delta} \in [0, 1)$ with $(1 + \bar{\delta})^2 < \alpha/(\alpha - 1)$ a relative bound, and $\bar{\Delta} \geq 0$ a shift bound. Define:

- The **four ranges** are the standard deviation's $[s_{\mathrm{lo}}, s_{\mathrm{hi}}]$, the ratio's $[-\bar{\delta}, \bar{\delta}]$, the center's $\mathbb{R}$ and the center shift's $[-\bar{\Delta}, \bar{\Delta}]$.
- $r_- := (1 - \bar{\delta})\,\theta_\alpha(-\bar{\delta})^{1/2}$ and $r_+ := (1 + \bar{\delta})\,\theta_\alpha(\bar{\delta})^{1/2}$.
- $\underline{s} := s_{\mathrm{lo}} r_-$ and $\overline{s} := s_{\mathrm{hi}} r_+$.
- $\varepsilon_j^\circ := \varepsilon_j(\underline{s})$.
- $g(\delta) := (1 + \delta)(2 + \delta)\,\theta_\alpha(\delta)/(\theta_\alpha(\delta)^{1/2} + 1) - 1$.
- $a_s := (\alpha - 1)\,\bar{\delta}\,\max\left(|g(-\bar{\delta})|, |g(\bar{\delta})|\right)$ and $a_c := \alpha(\alpha - 1)(2\bar{\delta} + \bar{\delta}^2)\,\theta_\alpha(\bar{\delta})\,\bar{\Delta}$.
- $b_s := \max(1 - r_-,\ r_+ - 1)$ and $b_c := \alpha\,\theta_\alpha(\bar{\delta})\,\bar{\Delta}$.
- $\bar{Q}(x, y) := (\overline{s}^2 \varepsilon_4^\circ + \varepsilon_2^\circ)\,x^2 + 2\overline{s}\,\varepsilon_3^\circ\,xy + \varepsilon_2^\circ y^2$ for $x, y \geq 0$.

- The **uniform bound** is $\bar{\phi}_{\mathrm{u}} := \alpha(\varepsilon_0^\circ)^2/(1-\varepsilon_0^\circ) + \overline{s}\,\varepsilon_2^\circ\, s_{\mathrm{hi}} a_s + \varepsilon_1^\circ a_c + (\bar{Q}(s_{\mathrm{hi}} b_s, b_c) + \alpha\bar{Q}(s_{\mathrm{hi}}\bar{\delta}, \bar{\Delta}))/2$.

Lemma E.2 (The cosine series of the deviation [to table])**.** *The normalizer's deviation is a cosine series in the center with Gaussian weights, and is at most the first series at the standard deviation. Define:*

- $d(s,c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\,s) - 1$ *for* $s > 0$ *and* $c \in \mathbb{R}$ *(Definition A.29);*
- $\varepsilon_0(s) := 2\sum_{k\geq 1} e^{-2\pi^2 s^2 k^2}$ *(Definition A.38).*

Then the deviation is the series and is bounded:

1. $\forall s > 0\ \forall c \in \mathbb{R}:\ d(s,c) = 2\sum_{k\geq 1} e^{-2\pi^2 s^2 k^2}\cos(2\pi k c)$; *[derived]*
2. $\forall s > 0\ \forall c \in \mathbb{R}:\ |d(s,c)| \leq \varepsilon_0(s)$. *[derived]*

Proof. Proof of item 1.

(L1) $\rho_{s,c}(\mathbb{Z}) = \sqrt{2\pi}\,s\sum_{k\in\mathbb{Z}} e^{-2\pi^2 s^2 k^2} e^{-2\pi i k c}$
[Fact A.45, item 6 (Poisson summation) at $x \mapsto e^{-(x-c)^2/(2s^2)}$]

(L2) $\forall \phi \in \mathbb{R}:\ e^{-i\phi} + e^{i\phi} = 2\cos\phi$
[Fact A.41, item 12: $\operatorname{conj} e^{i\phi} = e^{-i\phi}$, $e^{i\phi} = \cos\phi + i\sin\phi$; item 1: $x + \operatorname{conj} x = 2\operatorname{Re} x$]

(L3) $\sum_{k\in\mathbb{Z}} e^{-2\pi^2 s^2 k^2} e^{-2\pi i k c} = 1 + 2\sum_{k\geq 1} e^{-2\pi^2 s^2 k^2}\cos(2\pi k c)$
[the terms k and $-k$ by (L2) at $\phi := 2\pi k c$; the term $k = 0$]

(L4) $\Rightarrow$ item 1
[(L1), (L3); $d(s,c)$ (Definition A.29)]

□ (item 1)

Proof of item 2.

(L5) $|d(s,c)| \leq 2\sum_{k\geq 1} e^{-2\pi^2 s^2 k^2}|\cos(2\pi k c)|$
[item 1; $|\sum x_k| \leq \sum |x_k|$ (Fact A.41, item 1)]

(L6) $\Rightarrow$ item 2
[(L5); $|\cos\phi| \leq 1$ (Fact A.41, item 12); $\varepsilon_0(s)$ (Definition A.38)]

□ (item 2)

Corollary E.3 ([MP11, Lem. 2.8] at $\Lambda = \mathbb{Z}$ [to table])**.** *Where the first series is at most ϵ, a discrete Gaussian's offset from its center has the continuous Gaussian's moment-generating function within the factor $(1+\epsilon)/(1-\epsilon)$. Let:*

- $s > 0$;
- $c \in \mathbb{R}$;
- $\ell \in \mathbb{R}$;
- $\epsilon \in (0,1)$.

Define:

- $\varepsilon_0(s) := 2\sum_{k\geq 1} e^{-2\pi^2 s^2 k^2}$ *(Definition A.38);*
- $d(s,c') := \rho_{s,c'}(\mathbb{Z})/(\sqrt{2\pi}\,s) - 1$ *for* $c' \in \mathbb{R}$ *(Definition A.29);*
- $M_{s,c}(\ell) := \sum_{z\in\mathbb{Z}} e^{\ell(z-c)} D_{\mathbb{Z},s,c}(z)$ *(Lemma B.4).*

Assume:

(A1) $\varepsilon_0(s) \leq \epsilon$.

Then [L1: MP12, Lem. 2.8] the moment-generating function is bounded:

$$M_{s,c}(\ell) \leq \frac{1+\epsilon}{1-\epsilon}\, e^{\ell^2 s^2/2}.$$

The citation [MP12, Lem. 2.8] is read at $\Lambda = \mathbb{Z}$, their $(s,t) := (\sqrt{2\pi}\,s, \ell/(2\pi))$, their $x := z - c$ for $z \leftarrow D_{\mathbb{Z},s,c}$, their $s \geq \eta_\epsilon(\mathbb{Z})$ read as $\varepsilon_0(s) \leq \epsilon$.

Proof. (I1)

Lemma E.2, item 2 at every $c' \in \mathbb{R}$	This proof
Shared: s, d (Definition A.29), ε_0 (Definition A.38)	
c	c'
$s > 0$	The statement
$c \in \mathbb{R}$	The scope
Its item 2: $\lvert d(s,c)\rvert \le \varepsilon_0(s)$	
$\forall c' \in \mathbb{R}:\ \lvert d(s,c')\rvert \le \varepsilon_0(s)$	

[(I1)]

(L2) $\forall c' \in \mathbb{R}:\ \rho_{s,c'}(\mathbb{Z}) = \sqrt{2\pi}\, s\,(1 + d(s,c'))$

[$d(s,c')$ (the statement); $\sqrt{2\pi}\, s > 0$ ($s > 0$, the statement)]

(L3) $\forall c' \in \mathbb{R}:\ d(s,c') \in [-\epsilon, \epsilon]$

[(L1); assumption A1]

(L4) $\forall c' \in \mathbb{R}:\ \rho_{s,c'}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\, s, (1+\epsilon)\sqrt{2\pi}\, s]$

[(L2), (L3); $\sqrt{2\pi}\, s > 0$ ($s > 0$, the statement); Fact A.41, item 26]

Lemma B.4, item 2	This proof
Shared: s, c, ℓ, ϵ, $M_{s,c}$	
Shared: $s > 0$, $c \in \mathbb{R}$, $\ell \in \mathbb{R}$	
(I2) $\epsilon \in [0,1)$	$\epsilon \in (0,1)$ (the statement)
Assumption A1	(L4)
Its item 2: $M_{s,c}(\ell) \le \frac{1+\epsilon}{1-\epsilon}\, e^{\ell^2 s^2/2}$	

(L5) $\Rightarrow$ the statement

[(I2)]

□

Fact E.4 (Monotonicity of the series [to table])**.** Each series is nonincreasing in the standard deviation. Then

$$\forall j \in \{0,\dots,4\}\ \forall s' \ge s > 0:\quad \varepsilon_j(s') \le \varepsilon_j(s). \qquad \text{[derived]}$$

Proof. (L1) $\forall k \ge 1:\ e^{-2\pi^2 s'^2 k^2} \le e^{-2\pi^2 s^2 k^2}$

[$s' \ge s$, $s > 0$ (the quantifier); $t \mapsto t^2$ nondecreasing on $[0,\infty)$ and exp increasing (Fact A.41, item 5)]

(L2) $\forall k \ge 1\ \forall j \in \{0,\dots,4\}:\ (2\pi k)^j > 0$

[$2\pi k > 0$ (Definition A.38, $k \ge 1$)]

(L3) $\forall k \ge 1\ \forall j \in \{0,\dots,4\}:\ (2\pi k)^j e^{-2\pi^2 s'^2 k^2} \le (2\pi k)^j e^{-2\pi^2 s^2 k^2}$

[(L1), (L2); Fact A.41, item 26: $ca \le cb$ at $c := (2\pi k)^j$]

(L4) $\forall j \in \{0,\dots,4\}:\ \sum_{k\ge1}(2\pi k)^j e^{-2\pi^2 s'^2 k^2} \le \sum_{k\ge1}(2\pi k)^j e^{-2\pi^2 s^2 k^2}$

[(L3); $(2\pi k)^j e^{-2\pi^2 s'^2 k^2} \ge 0$ by (L2) and $e^t > 0$ (Fact A.41, item 12); Fact A.45, item 9, at $Y := \mathbb{Z}_{>0}$]

(L5) $\forall j \in \{0,\dots,4\}:\ \varepsilon_j(s') \le \varepsilon_j(s)$

[(L4); ε_j (Definition A.38); Fact A.41, item 26, at $c := 2$]

(L6) $\Rightarrow$ the statement

[(L5)]

□

Lemma E.5 (Factorization of the leaf divergence [to table])**.** *At a ratio of standard deviations and a center shift, the leaf divergence is a closed-form factor times* Φ*. Define:*

- $s_1 := s(1+\delta)$, $s_2 := s$, $c := c' + \Delta$ *and* $\theta_\alpha(\delta) := 1/(\alpha + (1-\alpha)(1+\delta)^2)$ *(Definition A.39);*
- $s'' := s(1+\delta)\theta_\alpha(\delta)^{1/2}$ *and* $m := c' + \alpha\theta_\alpha(\delta)\Delta$ *(Definition A.39);*

- Φ, *the normalizer ratio of Definition A.39;*
- $d(s,c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\,s) - 1$ *for* $s > 0$ *and* $c \in \mathbb{R}$ *(Definition A.29);*
- $D_{\mathbb{Z},s,c}(z) := \rho_{s,c}(z)/\rho_{s,c}(\mathbb{Z})$ *for* $z \in \mathbb{Z}$ *(Definition A.2).*

Then

$$\forall \alpha > 1\ \forall s > 0\ \forall \delta > -1,\ \alpha + (1-\alpha)(1+\delta)^2 > 0\ \forall c', \Delta \in \mathbb{R}:$$

$$R_\alpha(D_{\mathbb{Z},s_1,c} \,\|\, D_{\mathbb{Z},s_2,c'})^{\alpha-1} = \frac{s''}{s_1^{\alpha} s_2^{1-\alpha}} \exp\left(\frac{\alpha(\alpha-1)\Delta^2\theta_\alpha(\delta)}{2s^2}\right)\Phi(s,\delta,c',\Delta). \qquad \textit{[derived]}$$

Proof.

DEFINES $\alpha > 1$, $s > 0$, $\delta > -1$ with $\alpha + (1-\alpha)(1+\delta)^2 > 0$, $c' \in \mathbb{R}$ and $\Delta \in \mathbb{R}$, those the statement quantifies

(L1) $\forall (\sigma,\gamma) \in \{(s'',m),(s_1,c),(s_2,c')\}:\ \rho_{\sigma,\gamma}(\mathbb{Z}) = \sqrt{2\pi}\,\sigma\,(1+d(\sigma,\gamma))$

[d (Definition A.29)]

(L2) $(\alpha-1)(1+\delta)^2 < \alpha$

[$\alpha + (1-\alpha)(1+\delta)^2 > 0$ (the statement)]

(L3) $\Rightarrow\ s_1^2 < s_2^2\,\alpha/(\alpha-1)$

[(L2); $s_1 = s(1+\delta)$, $s_2 = s$ (Definition A.39); $\alpha - 1 > 0$ (the proof's block)]

(L4) $\alpha/s_1^2 + (1-\alpha)/s_2^2 = 1/(s^2(1+\delta)^2\theta_\alpha(\delta))$

[s_1, s_2, $\theta_\alpha(\delta)$ (Definition A.39); expand]

(L5) $\Rightarrow\ 1/(\alpha/s_1^2 + (1-\alpha)/s_2^2) = s''^2$

[(L4); $s'' = s(1+\delta)\theta_\alpha(\delta)^{1/2}$ (Definition A.39)]

(L6) $\frac{\alpha c/s_1^2 + (1-\alpha)c'/s_2^2}{\alpha/s_1^2 + (1-\alpha)/s_2^2} = c' + \alpha\theta_\alpha(\delta)\Delta$

[(L4); $c = c' + \Delta$, $s_1 = s(1+\delta)$, $\theta_\alpha(\delta)$ (Definition A.39); expand]

Lemma 4.1 at (s_1,s_2,c,c')	This proof
Shared: α, s_1, s_2, c, c'	
(I1) s''	s'' (L5)
(I1) m	m (L6); $m = c' + \alpha\theta_\alpha(\delta)\Delta$ (Definition A.39)
Assumption A1	(L3)
Its conclusion: $R_\alpha(D_{\mathbb{Z},s_1,c} \,\|\, D_{\mathbb{Z},s_2,c'})^{\alpha-1} = \frac{\rho_{s'',m}(\mathbb{Z})\,\exp\left(\alpha(\alpha-1)(c-c')^2 s''^2/(2s_1^2 s_2^2)\right)}{\rho_{s_1,c}(\mathbb{Z})^{\alpha}\,\rho_{s_2,c'}(\mathbb{Z})^{1-\alpha}}$	

(L7) $R_\alpha(D_{\mathbb{Z},s_1,c} \,\|\, D_{\mathbb{Z},s_2,c'})^{\alpha-1} = \frac{\sqrt{2\pi}\,s''(1+d(s'',m))\exp(\alpha(\alpha-1)\Delta^2 s''^2/(2s_1^2 s_2^2))}{(\sqrt{2\pi}\,s_1)^{\alpha}(1+d(s_1,c))^{\alpha}(\sqrt{2\pi}\,s_2)^{1-\alpha}(1+d(s_2,c'))^{1-\alpha}}$

[(I1); $c - c' = \Delta$ (the statement); (L1) for its three normalizers]

(L8) $(\sqrt{2\pi})^{1-\alpha-(1-\alpha)} = 1$

[$1 - \alpha - (1-\alpha) = 0$]

(L9) $\frac{s''^2}{s_1^2 s_2^2} = \frac{\theta_\alpha(\delta)}{s^2}$

[$s''^2 = s_1^2\theta_\alpha(\delta)$ and $s_2 = s$ (Definition A.39)]

(L10) $\Rightarrow$ the statement

[(L7), (L8), (L9); Φ (Definition A.39)]

□

Lemma E.6 (The linear combination of the two differences [to table])**.** *The linear combination* $v'' - \alpha v_1$ *of the two differences is explicit in* δ, $\theta_\alpha(\delta)$ *and* Δ*. Define:*

- $\theta_\alpha(\delta) := 1/(\alpha + (1-\alpha)(1+\delta)^2)$ *and* $s'' := s(1+\delta)\theta_\alpha(\delta)^{1/2}$ *(Definition A.39);*
- $m := c' + \alpha\theta_\alpha(\delta)\Delta$, $v_1 := (s_1,c) - (s_2,c')$ *and* $v'' := (s'',m) - (s_2,c')$ *(Definition A.39);*
- s_1, s_2 *and* c*, those of Definition A.39.*

Then

$$\forall \alpha > 1\ \forall s > 0\ \forall \delta > -1,\ \alpha + (1-\alpha)(1+\delta)^2 > 0\ \forall c', \Delta \in \mathbb{R}:$$

$$v'' - \alpha v_1 = \left(s\left((1+\delta)\theta_\alpha(\delta)^{1/2} - 1 - \alpha\delta\right),\ \alpha\Delta(\theta_\alpha(\delta) - 1)\right). \qquad \textit{[derived]}$$

Proof.
DEFINES $\alpha > 1$, $s > 0$, $\delta > -1$ with $\alpha + (1-\alpha)(1+\delta)^2 > 0$, $c' \in \mathbb{R}$ and $\Delta \in \mathbb{R}$, those the statement quantifies

(L1) $s'' - s - \alpha\delta s = s((1+\delta)\theta_\alpha(\delta)^{1/2} - 1 - \alpha\delta)$
[$s'' = s(1+\delta)\theta_\alpha(\delta)^{1/2}$ (Definition A.39)]

(L2) $m - c' - \alpha\Delta = \alpha\Delta(\theta_\alpha(\delta) - 1)$
[$m = c' + \alpha\theta_\alpha(\delta)\Delta$ (Definition A.39)]

(L3) $\Rightarrow$ the statement
[(L1), (L2); $v_1 = (s_1, c) - (s_2, c')$, $v'' = (s'', m) - (s_2, c')$, $s_1 = s(1+\delta)$, $s_2 = s$, $c = c' + \Delta$ (Definition A.39)]

□

Lemma E.7 (The first order of θ_α [to table])**.** *The deviation of $\theta_\alpha(\delta)$ from 1 is a multiple of $2\delta + \delta^2$.*

$$\forall \alpha > 1\ \forall \delta > -1,\ \alpha + (1-\alpha)(1+\delta)^2 > 0 : \quad \theta_\alpha(\delta) - 1 = (\alpha - 1)(2\delta + \delta^2)\,\theta_\alpha(\delta). \qquad \textit{[derived]}$$

Proof.
DEFINES $\alpha > 1$ and $\delta > -1$ with $\alpha + (1-\alpha)(1+\delta)^2 > 0$, those the statement quantifies

(L1) $\theta_\alpha(\delta) - 1 = \theta_\alpha(\delta)(1 - 1/\theta_\alpha(\delta))$
[$\theta_\alpha(\delta) \neq 0$ ($\theta_\alpha(\delta) = 1/(\alpha + (1-\alpha)(1+\delta)^2)$, Definition A.39); expand]

(L2) $1/\theta_\alpha(\delta) = \alpha + (1-\alpha)(1+\delta)^2$
[$\theta_\alpha(\delta)$ (Definition A.39)]

(L3) $\Rightarrow$ $\theta_\alpha(\delta) - 1 = \theta_\alpha(\delta)(1 - \alpha - (1-\alpha)(1+\delta)^2)$
[(L1), (L2)]

(L4) $1 - \alpha - (1-\alpha)(1+\delta)^2 = (\alpha - 1)((1+\delta)^2 - 1)$
[expand]

(L5) $(1+\delta)^2 - 1 = 2\delta + \delta^2$
[expand]

(L6) $\Rightarrow$ the statement
[(L3), (L4), (L5)]

□

Lemma E.8 (Partial derivatives of the deviation [to table])**.** *Above a floor of the standard deviation, each partial derivative of the normalizer's deviation up to order two is at most a series of the floor.*
Let:
- $\sigma_{\mathrm{lo}} > 0$.

Define:
- $d(s, c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\, s) - 1$ *for* $s > 0$ *and* $c \in \mathbb{R}$ *(Definition A.29).*

Then at every (σ, γ) with $\sigma \geq \sigma_{\mathrm{lo}}$ the partial derivatives satisfy:

1. $|\partial_\gamma d| \leq \varepsilon_1(\sigma_{\mathrm{lo}})$;
2. $|\partial_\sigma d| \leq \sigma\varepsilon_2(\sigma_{\mathrm{lo}})$;
3. $|\partial_\gamma^2 d| \leq \varepsilon_2(\sigma_{\mathrm{lo}})$;
4. $|\partial_\sigma \partial_\gamma d| \leq \sigma\varepsilon_3(\sigma_{\mathrm{lo}})$;
5. $|\partial_\sigma^2 d| \leq \sigma^2\varepsilon_4(\sigma_{\mathrm{lo}}) + \varepsilon_2(\sigma_{\mathrm{lo}})$.

Proof.
DEFINES $\forall k \geq 1 :\ a_k := e^{-2\pi^2\sigma^2k^2}$ and $\phi_k := 2\pi k\gamma$, at the point (σ, γ) of the line

	Lemma E.2, item 1 at every (σ, γ) with $\sigma > 0$ and $\gamma \in \mathbb{R}$	This proof
	Shared: d (Definition A.29)	
(I1)	s	σ
	c	γ
	$s > 0$	The scope
	$c \in \mathbb{R}$	The scope
	Its item 1: $d(s,c) = 2\sum_{k\geq 1} e^{-2\pi^2 s^2 k^2} \cos(2\pi k c)$	

(L1) $\forall(\sigma,\gamma),\ \sigma > 0:\ \partial_\gamma d = -2\sum_{k\geq 1}(2\pi k) a_k \sin\phi_k$
[(I1), differentiated termwise; a_k, ϕ_k (the proof's block)]

(L2) $\forall(\sigma,\gamma),\ \sigma > 0:\ \partial_\sigma d = -2\sum_{k\geq 1}\sigma(2\pi k)^2 a_k \cos\phi_k$
[(I1), differentiated termwise; a_k, ϕ_k (the proof's block)]

(L3) $\forall(\sigma,\gamma),\ \sigma > 0:\ \partial_\gamma^2 d = -2\sum_{k\geq 1}(2\pi k)^2 a_k \cos\phi_k$
[(L1), differentiated termwise]

(L4) $\forall(\sigma,\gamma),\ \sigma > 0:\ \partial_\sigma\partial_\gamma d = 2\sum_{k\geq 1}\sigma(2\pi k)^3 a_k \sin\phi_k$
[(L1), differentiated termwise]

(L5) $\forall(\sigma,\gamma),\ \sigma > 0:\ \partial_\sigma^2 d = 2\sum_{k\geq 1}(\sigma^2(2\pi k)^4 - (2\pi k)^2) a_k \cos\phi_k$
[(L2), differentiated termwise]

(L6) $\forall\phi \in \mathbb{R}:\ |\cos\phi| \leq 1$
[Fact A.41, item 12]

(L7) $\forall\phi \in \mathbb{R}:\ |\sin\phi| \leq 1$
[Fact A.41, item 12]

(L8) $\forall(\sigma,\gamma),\ \sigma \geq \sigma_{\mathrm{lo}}:\ |\partial_\gamma d| \leq \varepsilon_1(\sigma_{\mathrm{lo}})$
[(L1), (L7); Fact A.41, item 1; ε_j (Definition A.38); Fact E.4 at $\sigma \geq \sigma_{\mathrm{lo}}$]

(L9) $\Rightarrow$ item 1
[(L8)]

(L10) $\forall(\sigma,\gamma),\ \sigma \geq \sigma_{\mathrm{lo}}:\ |\partial_\sigma d| \leq \sigma\varepsilon_2(\sigma_{\mathrm{lo}})$
[(L2), (L6); Fact A.41, item 1; ε_j (Definition A.38); Fact E.4 at $\sigma \geq \sigma_{\mathrm{lo}}$]

(L11) $\Rightarrow$ item 2
[(L10)]

(L12) $\forall(\sigma,\gamma),\ \sigma \geq \sigma_{\mathrm{lo}}:\ |\partial_\gamma^2 d| \leq \varepsilon_2(\sigma_{\mathrm{lo}})$
[(L3), (L6); Fact A.41, item 1; ε_j (Definition A.38); Fact E.4 at $\sigma \geq \sigma_{\mathrm{lo}}$]

(L13) $\Rightarrow$ item 3
[(L12)]

(L14) $\forall(\sigma,\gamma),\ \sigma \geq \sigma_{\mathrm{lo}}:\ |\partial_\sigma\partial_\gamma d| \leq \sigma\varepsilon_3(\sigma_{\mathrm{lo}})$
[(L4), (L7); Fact A.41, item 1; ε_j (Definition A.38); Fact E.4 at $\sigma \geq \sigma_{\mathrm{lo}}$]

(L15) $\Rightarrow$ item 4
[(L14)]

(L16) $\forall(\sigma,\gamma),\ \sigma \geq \sigma_{\mathrm{lo}}:\ |\partial_\sigma^2 d| \leq \sigma^2\varepsilon_4(\sigma_{\mathrm{lo}}) + \varepsilon_2(\sigma_{\mathrm{lo}})$
[(L5), (L6); Fact A.41, item 1; ε_j (Definition A.38); Fact E.4 at $\sigma \geq \sigma_{\mathrm{lo}}$]

(L17) $\Rightarrow$ item 5
[(L16)]

□ (items 1 to 5)

Lemma E.9 (The second-order remainder of the deviation [to table])**.** *Along a segment whose standard deviations stay inside $[s_-, s_+]$, the normalizer's deviation departs from its tangent by at most half the quadratic form Q. Let:*

- $s > 0$*;*
- $\delta > -1$ *with* $\alpha + (1-\alpha)(1+\delta)^2 > 0$*;*

- $c', \Delta \in \mathbb{R}$.

Define:

- *The leaf parameters*
  - $\theta_\alpha(\delta) := 1/(\alpha + (1-\alpha)(1+\delta)^2)$ *and* $s_1 := s(1+\delta)$ *(Definition A.39);*
  - $s_2 := s$ *(Definition A.39);*
  - $s'' := s(1+\delta)\theta_\alpha(\delta)^{1/2}$, $s_- := \min(s, s_1, s'')$ *and* $s_+ := \max(s, s_1, s'')$ *(Definition A.39);*
- *The components*
  - v_s *and* v_c*, the components of* $v \in \mathbb{R}^2$*;*
- *The normalizer*
  - $d(s,c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\, s) - 1$ *for* $s > 0$ *and* $c \in \mathbb{R}$ *(Definition A.29);*
  - $d_2 = d(s_2, c')$*;*
- *The remainder form*
  - Q*, the remainder form of Definition A.39;*
  - $V = \{v \in \mathbb{R}^2 : \forall r \in [0,1] :\ s_2 + r v_s \in [s_-, s_+]\}$*;*
  - $\forall v \in \mathbb{R}^2 :\ \mathrm{Rm}(v) = d((s_2, c') + v) - d_2 - \nabla d(s_2, c') \cdot v$.

Then

$$\forall v \in V : \quad |\mathrm{Rm}(v)| \le Q(v)/2.$$

Proof.

DEFINES $\forall v \in V\ \forall r \in [0,1] :\ g_v(r) := d((s_2, c') + rv)$

(L1) $s_1 > 0$

[$s_1 = s(1+\delta)$ (Definition A.39); $s > 0$, $\delta > -1$ (the statement); $\prod_k c_k > 0$ at $c_k > 0$ (Fact A.41, items 12 and 28)]

(L2) $s'' > 0$

[$s'' = s(1+\delta)\theta_\alpha(\delta)^{1/2}$, $\theta_\alpha(\delta) = 1/(\alpha + (1-\alpha)(1+\delta)^2)$ (Definition A.39); $\alpha + (1-\alpha)(1+\delta)^2 > 0$ (the statement); (L1); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28); $\prod_k c_k > 0$ at $c_k > 0$ (Fact A.41, items 12 and 28)]

(L3) $s_- > 0$

[$s_- = \min(s, s_1, s'')$ (Definition A.39); $s > 0$ (the statement); (L1), (L2)]

(L4) $\forall v \in V\ \forall r \in [0,1] :\ g_v''(r) = v^\top \nabla^2 d((s_2, c') + rv)\, v$

[g_v (the proof's block); differentiate twice]

Lemma E.8 at every $v \in V$ and $r \in [0,1]$	This proof
Shared: d (Definition A.29)	
σ_{lo}	s_- (the statement)
(σ, γ)	$(s_2 + r v_s, c' + r v_c)$
$\sigma_{\mathrm{lo}} > 0$	(L3)
$\sigma \ge \sigma_{\mathrm{lo}}$	$s_2 + r v_s \in [s_-, s_+]$ ($v \in V$, the scope; V, the statement)
$\gamma \in \mathbb{R}$	$c' \in \mathbb{R}$ (the statement); $v \in \mathbb{R}^2$, $r \in [0,1]$ (the scope)
Its item 1: $\lvert\partial_\gamma d\rvert \le \varepsilon_1(\sigma_{\mathrm{lo}})$	
Its item 2: $\lvert\partial_\sigma d\rvert \le \sigma\varepsilon_2(\sigma_{\mathrm{lo}})$	
Its item 3: $\lvert\partial_\gamma^2 d\rvert \le \varepsilon_2(\sigma_{\mathrm{lo}})$	
Its item 4: $\lvert\partial_\sigma\partial_\gamma d\rvert \le \sigma\varepsilon_3(\sigma_{\mathrm{lo}})$	
Its item 5: $\lvert\partial_\sigma^2 d\rvert \le \sigma^2\varepsilon_4(\sigma_{\mathrm{lo}}) + \varepsilon_2(\sigma_{\mathrm{lo}})$	

(I1)

(L5) $\forall v \in V\ \forall r \in [0,1] :\ |g_v''(r)| \le Q(v)$

[(L4); (I1); Q (Definition A.39); Fact A.41, item 1]

(L6) $\forall v \in V :\ g_v'(0) = \nabla d(s_2, c') \cdot v$

[g_v (the proof's block); Fact A.41, item 19, at g_v]

(L7) $\forall v \in V :\ g_v(1) - g_v(0) - g_v'(0) = \mathrm{Rm}(v)$

[(L6); g_v (the proof's block); Rm (the statement)]

(L8) $\Rightarrow$ $\forall v \in V:\ |\mathrm{Rm}(v)| \le Q(v)/2$

[Fact A.41, item 11, at $g := g_v$, $M := Q(v)$; (L5); (L7)]

(L9) $\Rightarrow$ the statement

[(L8)]

□

Lemma E.10 (Bound on the logarithm of the normalizer ratio [to table])**.** *The logarithm of $\Phi(s, \delta, c', \Delta)$ is at most the normalizers' second-order term plus the first-order terms of $v'' - \alpha v_1$. Let:*

- $s > 0$;
- $\delta > -1$ *with* $\alpha + (1-\alpha)(1+\delta)^2 > 0$;
- $c', \Delta \in \mathbb{R}$.

Define:

- *The leaf parameters*
  - $\theta_\alpha(\delta) := 1/(\alpha + (1-\alpha)(1+\delta)^2)$ *(Definition A.39);*
  - $s_1 := s(1+\delta)$, $s_2 := s$ *and* $c := c' + \Delta$ *(Definition A.39 at $(\alpha, s, \delta, c', \Delta)$);*
  - $s'' := s(1+\delta)\theta_\alpha(\delta)^{1/2}$ *and* $m := c' + \alpha\theta_\alpha(\delta)\Delta$ *(Definition A.39);*
- *The components*
  - v_s *and* v_c*, the components of* $v \in \mathbb{R}^2$*;*
- *The differences*
  - $v_1 := (s_1, c) - (s_2, c')$ *and* $v'' := (s'', m) - (s_2, c')$ *(Definition A.39);*
- *The remainder form*
  - $s_- := \min(s, s_1, s'')$ *and* $s_+ := \max(s, s_1, s'')$ *(Definition A.39);*
- *The normalizer*
  - $d(s, c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\, s) - 1$ *for* $s > 0$ *and* $c \in \mathbb{R}$ *(Definition A.29);*
  - $\epsilon_0 = \varepsilon_0(s_-)$*;*
- *The normalizer ratio*
  - Φ*, the normalizer ratio, and* Q*, the remainder form, those of Definition A.39.*

Assume:

(A1) $\epsilon_0 < 1$.

Then

$$|\ln \Phi(s, \delta, c', \Delta)| \le \frac{\alpha\epsilon_0^2}{1-\epsilon_0} + s_+\varepsilon_2(s_-)|v''_s - \alpha v_{1,s}| + \varepsilon_1(s_-)|v''_c - \alpha v_{1,c}| + \frac{Q(v'') + \alpha Q(v_1)}{2}.$$

Proof.

DEFINES
$d'' := d(s'', m)$
$d_1 := d(s_1, c)$
$d_2 := d(s_2, c')$
$V = \{v \in \mathbb{R}^2 : \forall r \in [0,1]:\ s_2 + r v_s \in [s_-, s_+]\}$ (Lemma E.9)
$\mathrm{Rm}(v) = d((s_2, c') + v) - d_2 - \nabla d(s_2, c') \cdot v$, $d_2 = d(s_2, c')$ (Lemma E.9)

(L1) $s'' \ge s_-$

[$s_- = \min(s, s_1, s'')$ (Definition A.39)]

(L2) $s_1 \ge s_-$

[$s_- = \min(s, s_1, s'')$ (Definition A.39)]

(L3) $s_2 \ge s_-$

[$s_2 = s$ and $s_- = \min(s, s_1, s'')$ (Definition A.39)]

(L4) $s_1 > 0$

[$s_1 = s(1+\delta)$ (Definition A.39); $s > 0$, $\delta > -1$ (the statement); $\prod_k c_k > 0$ at $c_k > 0$ (Fact A.41, items 12 and 28)]

(L5) $s'' > 0$

[$s'' = s(1+\delta)\theta_\alpha(\delta)^{1/2}$, $\theta_\alpha(\delta) = 1/(\alpha + (1-\alpha)(1+\delta)^2)$ (Definition A.39); $\alpha + (1-\alpha)(1+\delta)^2 > 0$ (the statement); (L4); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28); $\prod_k c_k > 0$ at $c_k > 0$ (Fact A.41, items 12 and 28)]

(L6) $s_2 > 0$

[$s_2 = s$ (Definition A.39); $s > 0$ (the statement)]

(L7) $s_- > 0$

[$s_- = \min(s, s_1, s'')$ (Definition A.39); $s > 0$ (the statement); (L4), (L5)]

Lemma E.2, item 2	This proof
Shared: d (Definition A.29), ε_0 (Definition A.38)	
(I1) (s, c) $s > 0$ $c \in \mathbb{R}$	(s'', m) (Definition A.39) (L5) $m = c' + \alpha\theta_\alpha(\delta)\Delta$ (Definition A.39); $c', \Delta \in \mathbb{R}$ (the statement)
Its item 2: $\lvert d(s,c)\rvert \le \varepsilon_0(s)$	

(L8) $|d''| \le \epsilon_0$

[(I1); Fact E.4 at (L1); ϵ_0 (the statement)]

Lemma E.2, item 2	This proof
Shared: d (Definition A.29), ε_0 (Definition A.38)	
(I2) (s, c) $s > 0$ $c \in \mathbb{R}$	(s_1, c) (Definition A.39) (L4) $c = c' + \Delta$ (Definition A.39); $c', \Delta \in \mathbb{R}$ (the statement)
Its item 2: $\lvert d(s,c)\rvert \le \varepsilon_0(s)$	

(L9) $|d_1| \le \epsilon_0$

[(I2); Fact E.4 at (L2); ϵ_0 (the statement)]

Lemma E.2, item 2	This proof
Shared: d (Definition A.29), ε_0 (Definition A.38)	
(I3) (s, c) $s > 0$ $c \in \mathbb{R}$	(s_2, c') (Definition A.39) (L6) $c' \in \mathbb{R}$ (the statement)
Its item 2: $\lvert d(s,c)\rvert \le \varepsilon_0(s)$	

(L10) $|d_2| \le \epsilon_0$

[(I3); Fact E.4 at (L3); ϵ_0 (the statement)]

(L11) $1 + d'' > 0$

[(L8); $\epsilon_0 < 1$ (assumption A1)]

(L12) $1 + d_1 > 0$

[(L9); $\epsilon_0 < 1$ (assumption A1)]

(L13) $1 + d_2 > 0$

[(L10); $\epsilon_0 < 1$ (assumption A1)]

(L14) $\ln \Phi = \ln(1 + d'') - \alpha \ln(1 + d_1) + (\alpha - 1)\ln(1 + d_2)$

[Φ (Definition A.39); (L11), (L12), (L13)]

(L15) $|\ln \Phi - (d'' - \alpha d_1 + (\alpha - 1)d_2)| \le \frac{(1+\alpha+(\alpha-1))\epsilon_0^2}{2(1-\epsilon_0)}$

[(L14); Fact A.41, item 15, at $\epsilon := \epsilon_0$ and $x := d''$, d_1, d_2 by (L8), (L9), (L10), $\epsilon_0 < 1$ (assumption A1); $|x + y| \le |x| + |y|$ (Fact A.41, item 1)]

(L16) $(1 + \alpha + (\alpha - 1))/2 = \alpha$

[expand]

(L17) $\Rightarrow$ $|\ln \Phi - (d'' - \alpha d_1 + (\alpha - 1)d_2)| \le \frac{\alpha\epsilon_0^2}{1-\epsilon_0}$

[(L15), (L16)]

(L18) $v'' \in V$

[$(s'', m) = (s_2, c') + v''$ (Definition A.39); $s_2, s'' \in [s_-, s_+]$ (Definition A.39); V (the proof's block)]

(L19) $v_1 \in V$

[$(s_1, c) = (s_2, c') + v_1$ (Definition A.39); $s_2, s_1 \in [s_-, s_+]$ (Definition A.39); V (the proof's block)]

(L20) $d'' - \alpha d_1 + (\alpha - 1) d_2 = \nabla d(s_2, c') \cdot (v'' - \alpha v_1) + \mathrm{Rm}(v'') - \alpha\,\mathrm{Rm}(v_1)$

[Rm (the proof's block) at v'' and v_1; $(s'', m) = (s_2, c') + v''$, $(s_1, c) = (s_2, c') + v_1$ (Definition A.39); collect]

Lemma E.8	This proof
Shared: d (Definition A.29)	
σ_{lo}	s_- (the statement)
(σ, γ)	(s_2, c')
(I4) $\sigma_{\mathrm{lo}} > 0$	(L7)
$\sigma \geq \sigma_{\mathrm{lo}}$	(L3)
$\gamma \in \mathbb{R}$	$c' \in \mathbb{R}$ (the statement)
Its item 1: $\lvert\partial_\gamma d\rvert \leq \varepsilon_1(\sigma_{\mathrm{lo}})$	
Its item 2: $\lvert\partial_\sigma d\rvert \leq \sigma\varepsilon_2(\sigma_{\mathrm{lo}})$	

(L21) $\forall w \in \mathbb{R}^2 :\ \lvert\nabla d(s_2, c') \cdot w\rvert \leq s_+\varepsilon_2(s_-)\lvert w_s\rvert + \varepsilon_1(s_-)\lvert w_c\rvert$

[(I4); $s_2 \in [s_-, s_+]$ (Definition A.39)]

Lemma E.9 at v'' and at v_1	This proof
Shared: $\alpha,\ s,\ \delta,\ c',\ \Delta,\ s_2, s_-, s_+, Q$ (Definition A.39), d (Definition A.29), d_2, V, Rm (the proof's block)	
(I5) Shared: $\alpha > 1,\ s > 0,\ \delta > -1,\ \alpha + (1-\alpha)(1+\delta)^2 > 0,\ c', \Delta \in \mathbb{R}$	
v	v'', v_1 (Definition A.39)
$v \in V$	(L18) at v''; (L19) at v_1
Its conclusion: $\forall v \in V :\ \lvert\mathrm{Rm}(v)\rvert \leq Q(v)/2$	

(L22) $\lvert\mathrm{Rm}(v'') - \alpha\,\mathrm{Rm}(v_1)\rvert \leq \frac{1}{2}(Q(v'') + \alpha Q(v_1))$

[(I5); Fact A.41, item 1]

(L23) $\Rightarrow$ the statement

[(L17), (L20), (L21) at $w := v'' - \alpha v_1$, (L22); Fact A.41, item 1]

□

Lemma E.11 (The standard deviations over the four ranges [to table])**.** *Over the four ranges of the standard deviation, the ratio, the center and the center shift, $\theta_\alpha(\delta) \in [\theta_\alpha(-\bar\delta), \theta_\alpha(\bar\delta)]$, and the standard deviations of the leaf stay between $\underline{s}$ and $\overline{s}$. Let:*

- $s_{\mathrm{lo}}, s_{\mathrm{hi}}$ *with* $0 < s_{\mathrm{lo}} \leq s_{\mathrm{hi}}$;
- $\bar\delta \in [0, 1)$;
- $s \in [s_{\mathrm{lo}}, s_{\mathrm{hi}}]$;
- $\delta \in [-\bar\delta, \bar\delta]$.

Define:

- *The leaf parameters*
  - $\theta_\alpha(\delta) := 1/(\alpha + (1-\alpha)(1+\delta)^2)$ *and* $s_1 := s(1+\delta)$ *(Definition A.39);*
  - $s'' := s(1+\delta)\theta_\alpha(\delta)^{1/2}$, $s_- := \min(s, s_1, s'')$ *and* $s_+ := \max(s, s_1, s'')$ *(Definition A.39);*
- *The ranges*
  - $r_- := (1-\bar\delta)\,\theta_\alpha(-\bar\delta)^{1/2}$, $r_+ := (1+\bar\delta)\,\theta_\alpha(\bar\delta)^{1/2}$ *and* $\underline{s} := s_{\mathrm{lo}} r_-$ *(Definition A.40);*
  - $\overline{s} := s_{\mathrm{hi}} r_+$ *and* $\varepsilon_j^\circ := \varepsilon_j(\underline{s})$, $j \leq 4$ *(Definition A.40).*

Assume:

(A1) $(1+\bar\delta)^2 < \alpha/(\alpha-1)$;

(A2) $\varepsilon_0^\circ < 1$.

Then the factor, the standard deviations and the normalizers' deviations satisfy:

1. $1+\delta > 0$;
2. $\alpha + (1-\alpha)(1+\delta)^2 > 0$;
3. $\theta_\alpha(-\bar{\delta}) > 0$;
4. $\theta_\alpha(\delta) \in [\theta_\alpha(-\bar{\delta}), \theta_\alpha(\bar{\delta})]$;
5. $1 \in [r_-, r_+]$;
6. $(1+\delta)\theta_\alpha(\delta)^{1/2} \in [r_-, r_+]$;
7. $s'' \in [\underline{s}, \overline{s}]$;
8. $[s_-, s_+] \subseteq [\underline{s}, \overline{s}]$;
9. $\forall j \le 4 :\ \varepsilon_j(s_-) \le \varepsilon_j^\circ$;
10. $\varepsilon_0(s_-) < 1$.

Proof. (L1) $1 - \bar{\delta} > 0$
[$\bar{\delta} \in [0,1)$ (the statement)]

(L2) $\forall \delta,\ |\delta| \le \bar{\delta} :\ 1 - \bar{\delta} \le 1 + \delta$
[$-\bar{\delta} \le \delta$ (the statement)]

(L3) $\Rightarrow\ 1 + \delta > 0$
[(L1), (L2) at δ]

(L4) $\Rightarrow$ item 1
[(L3)]

(L5) $\forall \delta,\ |\delta| \le \bar{\delta} :\ 1 + \delta \le 1 + \bar{\delta}$
[$\delta \le \bar{\delta}$ (the statement)]

(L6) $\forall \delta,\ |\delta| \le \bar{\delta} :\ (1 - \bar{\delta})^2 \le (1 + \delta)^2$
[(L1), (L2); $x \mapsto x^2$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L7) $\forall \delta,\ |\delta| \le \bar{\delta} :\ (1 + \delta)^2 \le (1 + \bar{\delta})^2$
[(L1), (L2), (L5); $x \mapsto x^2$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L8) $\alpha + (1-\alpha)(1+\bar{\delta})^2 > 0$
[$(1+\bar{\delta})^2 < \alpha/(\alpha-1)$ (assumption A1), multiplied by $\alpha - 1 > 0$]

(L9) $\forall x \le x' :\ \alpha - (\alpha-1)x' \le \alpha - (\alpha-1)x$
[$\alpha - 1 > 0$ (the statement)]

(L10) $\forall \delta,\ |\delta| \le \bar{\delta} :\ \alpha + (1-\alpha)(1+\bar{\delta})^2 \le \alpha + (1-\alpha)(1+\delta)^2$
[(L7); (L9) at $x := (1+\delta)^2$, $x' := (1+\bar{\delta})^2$]

(L11) $\Rightarrow\ \alpha + (1-\alpha)(1+\delta)^2 > 0$
[(L8), (L10) at δ]

(L12) $\Rightarrow$ item 2
[(L11)]

(L13) $\forall \delta,\ |\delta| \le \bar{\delta} :\ \alpha + (1-\alpha)(1+\delta)^2 \le \alpha + (1-\alpha)(1-\bar{\delta})^2$
[(L6); (L9) at $x := (1-\bar{\delta})^2$, $x' := (1+\delta)^2$]

(L14) $\theta_\alpha(-\bar{\delta}) > 0$
[(L8), (L10), (L13) at $\delta := 0$; $1/\theta_\alpha(\delta) = \alpha + (1-\alpha)(1+\delta)^2$ (Definition A.39)]

(L15) $\Rightarrow$ item 3
[(L14)]

(L16) $\forall \delta,\ |\delta| \le \bar{\delta} :\ \theta_\alpha(-\bar{\delta}) \le \theta_\alpha(\delta)$
[(L8), (L10), (L13); $1/\theta_\alpha(\delta) = \alpha + (1-\alpha)(1+\delta)^2$ (Definition A.39); $x \mapsto 1/x$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L17) $\forall \delta,\ |\delta| \le \bar{\delta}:\ \theta_\alpha(\delta) \le \theta_\alpha(\bar{\delta})$
[(L8), (L10); $1/\theta_\alpha(\delta) = \alpha + (1-\alpha)(1+\delta)^2$ (Definition A.39); $x \mapsto 1/x$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L18) $\Rightarrow\ \theta_\alpha(\delta) \in [\theta_\alpha(-\bar{\delta}), \theta_\alpha(\bar{\delta})]$
[(L16), (L17) at δ]

(L19) $\Rightarrow$ item 4
[(L18)]

(L20) $\theta_\alpha(0) = 1$
[$\theta_\alpha(\delta)$ (Definition A.39) at $\delta = 0$]

(L21) $\theta_\alpha(-\bar{\delta}) \le 1$
[(L16) at $\delta := 0$; (L20)]

(L22) $1 \le \theta_\alpha(\bar{\delta})$
[(L17) at $\delta := 0$; (L20)]

(L23) $r_- \le 1$
[(L1), (L21); $1 - \bar{\delta} \le 1$ (the statement); r_- (Definition A.40); Fact A.41, items 5 and 8]

(L24) $1 \le r_+$
[(L22); $1 + \bar{\delta} \ge 1$ ($\bar{\delta} \in [0,1)$, the statement); r_+ (Definition A.40); Fact A.41, items 5 and 8]

(L25) $\Rightarrow\ 1 \in [r_-, r_+]$
[(L23), (L24)]

(L26) $\Rightarrow$ item 5
[(L25)]

(L27) $\forall \delta,\ |\delta| \le \bar{\delta}:\ (1+\delta)\theta_\alpha(\delta)^{1/2} \in [r_-, r_+]$
[(L1), (L2), (L5), (L14), (L16), (L17); r_-, r_+ (Definition A.40); Fact A.41, items 5 and 8]

(L28) $\Rightarrow$ item 6
[(L27)]

(L29) $s_1 \in [s_{\mathrm{lo}}(1-\bar{\delta}),\ s_{\mathrm{hi}}(1+\bar{\delta})]$
[$s_1 = s(1+\delta)$ (Definition A.39); $s \in [s_{\mathrm{lo}}, s_{\mathrm{hi}}]$ (the statement); (L1), (L2), (L5)]

(L30) $s'' \in [\underline{s}, \overline{s}]$
[$s'' = s(1+\delta)\theta_\alpha(\delta)^{1/2}$ (Definition A.39); $s \in [s_{\mathrm{lo}}, s_{\mathrm{hi}}]$ (the statement); (L27); $\underline{s} = s_{\mathrm{lo}} r_-$, $\overline{s} = s_{\mathrm{hi}} r_+$ (Definition A.40)]

(L31) $\Rightarrow$ item 7
[(L30)]

(L32) $r_- \le 1 - \bar{\delta}$
[$r_- = (1-\bar{\delta})\theta_\alpha(-\bar{\delta})^{1/2}$ (Definition A.40); (L1), (L21)]

(L33) $1 + \bar{\delta} \le r_+$
[$r_+ = (1+\bar{\delta})\theta_\alpha(\bar{\delta})^{1/2}$ (Definition A.40); (L22)]

(L34) $\underline{s} \le s_-$
[$s_- = \min(s, s_1, s'')$ (Definition A.39); $s \ge s_{\mathrm{lo}}$ (the statement); (L23), (L29), (L30), (L32); $\underline{s} = s_{\mathrm{lo}} r_-$ (Definition A.40)]

(L35) $s_+ \le \overline{s}$
[$s_+ = \max(s, s_1, s'')$ (Definition A.39); $s \le s_{\mathrm{hi}}$ (the statement); (L24), (L29), (L30), (L33); $\overline{s} = s_{\mathrm{hi}} r_+$ (Definition A.40)]

(L36) $\Rightarrow\ [s_-, s_+] \subseteq [\underline{s}, \overline{s}]$
[(L34), (L35); $s_- \le s_+$ (Definition A.39)]

(L37) $\Rightarrow$ item 8
[(L36)]

(L38) $\forall j \le 4:\ \varepsilon_j(s_-) \le \varepsilon_j^\circ$
[Fact E.4 at $s_- \ge \underline{s}$ (L34); $\varepsilon_j^\circ = \varepsilon_j(\underline{s})$ (Definition A.40)]

(L39) $\Rightarrow$ item 9
[(L38)]

(L40) $\varepsilon_0(s_-) < 1$

[(L38) at $j = 0$; $\varepsilon_0^\circ < 1$ (assumption A2)]

(L41) $\Rightarrow$ item 10

[(L40)]

□ (items 1 to 10)

Lemma E.12 (The differences over the four ranges [to table])**.** *Over the four ranges of the standard deviation, the ratio, the center and the center shift, the leaf's two differences v_1, v'' and $v'' - \alpha v_1$ are at most the constants of Definition A.40. Let:*

- $s_{\text{lo}}, s_{\text{hi}}$ *with* $0 < s_{\text{lo}} \le s_{\text{hi}}$;
- $\bar{\delta} \in [0, 1)$;
- $\bar{\Delta} \in \mathbb{R}$;
- $s \in [s_{\text{lo}}, s_{\text{hi}}]$;
- $\delta \in [-\bar{\delta}, \bar{\delta}]$;
- $c' \in \mathbb{R}$;
- $\Delta \in [-\bar{\Delta}, \bar{\Delta}]$.

Define:

- *The leaf parameters*
  - $\theta_\alpha(\delta) := 1/(\alpha + (1-\alpha)(1+\delta)^2)$ *and* $s_1 := s(1+\delta)$ *(Definition A.39);*
  - $s'' := s(1+\delta)\theta_\alpha(\delta)^{1/2}$, $s_- := \min(s, s_1, s'')$ *and* $s_+ := \max(s, s_1, s'')$ *(Definition A.39);*
- *The ranges*
  - $r_- := (1-\bar{\delta})\,\theta_\alpha(-\bar{\delta})^{1/2}$, $r_+ := (1+\bar{\delta})\,\theta_\alpha(\bar{\delta})^{1/2}$ *and* $\underline{s} := s_{\text{lo}} r_-$ *(Definition A.40);*
  - $\overline{s} := s_{\text{hi}} r_+$, $\varepsilon_j^\circ := \varepsilon_j(\underline{s})$, $j \le 4$, *and* $b_s := \max(1 - r_-,\ r_+ - 1)$ *(Definition A.40);*
- *The difference bounds*
  - $g(\delta) := (1+\delta)(2+\delta)\,\theta_\alpha(\delta)/(\theta_\alpha(\delta)^{1/2} + 1) - 1$ *and* $b_c := \alpha\,\theta_\alpha(\bar{\delta})\,\bar{\Delta}$ *(Definition A.40);*
  - $a_s := (\alpha - 1)\,\bar{\delta}\,\max\left(|g(-\bar{\delta})|, |g(\bar{\delta})|\right)$ *(Definition A.40);*
  - $a_c := \alpha(\alpha-1)(2\bar{\delta} + \bar{\delta}^2)\,\theta_\alpha(\bar{\delta})\,\bar{\Delta}$ *(Definition A.40);*
- *The differences*
  - $v_1 := (s_1, c' + \Delta) - (s, c') =: (v_{1,s}, v_{1,c})$ *(Definition A.39 at* $(s_2, c) := (s, c' + \Delta)$*);*
  - $v'' := (s'', m) - (s, c') =: (v''_s, v''_c)$, *with* $m := c' + \alpha\theta_\alpha(\delta)\Delta$ *(Definition A.39 at* $(s_2, c) := (s, c' + \Delta)$*).*

Assume:

(A1) $(1+\bar{\delta})^2 < \alpha/(\alpha - 1)$;

(A2) $\varepsilon_0^\circ < 1$.

Then the differences and $v'' - \alpha v_1$ satisfy:

1. $|v_{1,s}| \le s_{\text{hi}}\bar{\delta}$;
2. $|v_{1,c}| \le \bar{\Delta}$;
3. $|v''_s| \le s_{\text{hi}} b_s$;
4. $|v''_c| \le b_c$;
5. $|v''_s - \alpha v_{1,s}| \le s_{\text{hi}} a_s$;
6. $|v''_c - \alpha v_{1,c}| \le a_c$.

Proof. (L1) $1 - \bar{\delta} > 0$

[$\bar{\delta} \in [0, 1)$ (the statement)]

(L2) $\forall \delta,\ |\delta| \le \bar{\delta}:\ 1 - \bar{\delta} \le 1 + \delta$

[$-\bar{\delta} \le \delta$ (the statement)]

(L3) $\forall \delta,\ |\delta| \le \bar{\delta}:\ 1 + \delta \le 1 + \bar{\delta}$

[$\delta \le \bar{\delta}$ (the statement)]

(L4) $\theta_\alpha(0) = 1$

[$\theta_\alpha(\delta)$ (Definition A.39) at $\delta = 0$]

Lemma E.11 at the statement's objects	This proof
Shared: $\alpha,\ s_{\mathrm{lo}}, s_{\mathrm{hi}},\ \bar\delta,\ s,\ \delta,\ \theta_\alpha(\delta),\ r_-, r_+,\ \underline{s}, \overline{s}, \varepsilon_j^\circ,\ s_1, s'', s_-, s_+$	
Shared: $\alpha > 1,\ s_{\mathrm{lo}} > 0,\ s_{\mathrm{lo}} \le s_{\mathrm{hi}},\ \bar\delta \in [0, 1),\ s \in [s_{\mathrm{lo}}, s_{\mathrm{hi}}],\ \delta \in [-\bar\delta, \bar\delta]$	
Shared: assumptions A1, A2	
(I1) Its item 1: $1 + \delta > 0$	
(I1) Its item 2: $\alpha + (1-\alpha)(1+\delta)^2 > 0$	
(I1) Its item 3: $\theta_\alpha(-\bar\delta) > 0$	
(I1) Its item 4: $\theta_\alpha(\delta) \in [\theta_\alpha(-\bar\delta), \theta_\alpha(\bar\delta)]$	
(I1) Its item 5: $1 \in [r_-, r_+]$	
(I1) Its item 6: $(1+\delta)\theta_\alpha(\delta)^{1/2} \in [r_-, r_+]$	

(L5) $1 + \delta > 0$

[item 1 of (I1)]

(L6) $\alpha + (1-\alpha)(1+\delta)^2 > 0$

[item 2 of (I1)]

(L7) $\theta_\alpha(-\bar\delta) > 0$

[item 3 of (I1)]

(L8) $\theta_\alpha(\delta) \in [\theta_\alpha(-\bar\delta), \theta_\alpha(\bar\delta)]$

[item 4 of (I1)]

(L9) $1 \in [r_-, r_+]$

[item 5 of (I1)]

(L10) $(1+\delta)\theta_\alpha(\delta)^{1/2} \in [r_-, r_+]$

[item 6 of (I1)]

(L11) $\theta_\alpha(\delta) > 0$

[(L7), (L8)]

(L12) $s > 0$

[$s \in [s_{\mathrm{lo}}, s_{\mathrm{hi}}]$ (the statement); $s_{\mathrm{lo}} > 0$ (the statement)]

(L13) $|v_{1,s}| \le s_{\mathrm{hi}}\bar\delta$

[$v_1 = (s_1, c) - (s_2, c')$, $s_1 = s(1+\delta)$, $s_2 = s$ (Definition A.39); $|\delta| \le \bar\delta$, $s \le s_{\mathrm{hi}}$ (the statement)]

(L14) $\Rightarrow$ item 1

[(L13)]

(L15) $|v_{1,c}| \le \bar\Delta$

[$v_1 = (s_1, c) - (s_2, c')$, $c = c' + \Delta$ (Definition A.39); $|\Delta| \le \bar\Delta$ (the statement)]

(L16) $\Rightarrow$ item 2

[(L15)]

(L17) $|v''_s| = s\,|(1+\delta)\theta_\alpha(\delta)^{1/2} - 1|$

[$v'' = (s'', m) - (s_2, c')$, $s_2 = s$, $s'' = s(1+\delta)\theta_\alpha(\delta)^{1/2}$ (Definition A.39)]

(L18) $|(1+\delta)\theta_\alpha(\delta)^{1/2} - 1| \le b_s$

[(L9), (L10); $b_s = \max(1 - r_-, r_+ - 1)$ (Definition A.40)]

(L19) $\Rightarrow$ $|v''_s| \le s_{\mathrm{hi}} b_s$

[(L17), (L18); $s \le s_{\mathrm{hi}}$ (the statement)]

(L20) $\Rightarrow$ item 3

[(L19)]

(L21) $|v''_c| = \alpha\theta_\alpha(\delta)|\Delta|$

[$v''_c = m - c'$, $m - c' = \alpha\theta_\alpha(\delta)\Delta$ (Definition A.39); (L11)]

(L22) $\Rightarrow$ $|v''_c| \le b_c$

[(L21); (L8); $|\Delta| \le \bar\Delta$ (the statement); $b_c = \alpha\theta_\alpha(\bar\delta)\bar\Delta$ (Definition A.40)]

(L23) $\Rightarrow$ item 4

[(L22)]

(L24) $\forall t > 0:\ t^{1/2} - 1 = (t-1)/(t^{1/2}+1)$

[expand]

Lemma E.6	This proof
Shared: $\alpha,\ s,\ \delta,\ c',\ \Delta,\ \theta_\alpha(\delta),\ s'',\ m$ (Definition A.39), $v_1,\ v''$	
Shared: $\alpha > 1,\ c', \Delta \in \mathbb{R}$	
(I2)	
$s > 0$	(L12)
$\delta > -1$	(L5)
$\alpha + (1-\alpha)(1+\delta)^2 > 0$	(L6)
Its conclusion: $v'' - \alpha v_1 = \left(s\left((1+\delta)\theta_\alpha(\delta)^{1/2} - 1 - \alpha\delta\right),\ \alpha\Delta(\theta_\alpha(\delta) - 1)\right)$	

(L25) $v'' - \alpha v_1 = \left(s\left((1+\delta)\theta_\alpha(\delta)^{1/2} - 1 - \alpha\delta\right),\ \alpha\Delta(\theta_\alpha(\delta) - 1)\right)$

[(I2)]

Lemma E.7	This proof
Shared: $\alpha,\ \delta$	
(I3)	
$\delta > -1$	(L5)
$\alpha + (1-\alpha)(1+\delta)^2 > 0$	(L6)
Its conclusion: $\theta_\alpha(\delta) - 1 = (\alpha - 1)(2\delta + \delta^2)\,\theta_\alpha(\delta)$	

(L26) $\theta_\alpha(\delta) - 1 = (\alpha - 1)(2\delta + \delta^2)\,\theta_\alpha(\delta)$

[(I3)]

(L27) $v_s'' - \alpha v_{1,s} = (\alpha - 1)\,\delta\, s\, g(\delta)$

[(L25); (L24) at $t := \theta_\alpha(\delta)$; (L26); g (Definition A.40); expand]

(L28) $\forall \delta \in [-\bar\delta, \bar\delta]:\ (1+\delta)(2+\delta) > 0$

[(L1), (L2)]

(L29) $\forall \delta, \delta' \in [-\bar\delta, \bar\delta],\ \delta \le \delta':\ (1+\delta)(2+\delta) \le (1+\delta')(2+\delta')$

[(L1), (L2); Fact A.41, item 8]

(L30) $\forall \delta, \delta' \in [-\bar\delta, \bar\delta],\ \delta \le \delta':\ \theta_\alpha(\delta) \le \theta_\alpha(\delta')$

[$\theta_\alpha(\delta) = 1/(\alpha + (1-\alpha)(1+\delta)^2)$ (Definition A.39); (L1), (L2); $\alpha > 1$ (Definition A.40); (L6); Fact A.41, item 5]

(L31) $\forall t > 0:\ t/(t^{1/2}+1) > 0$

[$t > 0$]

(L32) $\forall t > 0:\ t/(t^{1/2}+1) = t^{1/2} - 1 + 1/(t^{1/2}+1)$

[multiply by $t^{1/2} + 1 > 0$; expand]

(L33) $\forall t > 0:\ \frac{d}{dt}\left(t/(t^{1/2}+1)\right) = \frac{1}{2}t^{-1/2}\left(1 - (t^{1/2}+1)^{-2}\right)$

[(L32); differentiate]

(L34) $\forall t > 0:\ \frac{1}{2}t^{-1/2}\left(1 - (t^{1/2}+1)^{-2}\right) \ge 0$

[$t^{1/2} + 1 \ge 1$ ($t \mapsto t^{1/2}$ nondecreasing on $[0,\infty)$, Fact A.41, item 5); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L35) $\forall t, t' > 0,\ t \le t':\ t/(t^{1/2}+1) \le t'/(t'^{1/2}+1)$

[(L33), (L34); Fact A.41, item 5: a nonnegative derivative on an interval, nondecreasing there]

(L36) $\Rightarrow\ \forall \delta, \delta' \in [-\bar\delta, \bar\delta],\ \delta \le \delta':\ g(\delta) \le g(\delta')$

[(L28) to (L35); Fact A.41, item 8; g (Definition A.40)]

(L37) $g(0) = 0$

[g (Definition A.40); (L4)]

(L38) $\forall \delta \in [0, \bar\delta]:\ 0 \le g(\delta)$

[(L36), (L37)]

(L39) $\forall \delta \in [0, \bar\delta]:\ g(\delta) \le g(\bar\delta)$

[(L36)]

(L40) $\forall \delta \in [-\bar{\delta}, 0] :\ g(-\bar{\delta}) \le g(\delta)$

[(L36)]

(L41) $\forall \delta \in [-\bar{\delta}, 0] :\ g(\delta) \le 0$

[(L36), (L37)]

(L42) $\Rightarrow\ |v_s'' - \alpha v_{1,s}| \le s_{\text{hi}} a_s$

[(L27), (L38) to (L41); $s \le s_{\text{hi}}$, $|\delta| \le \bar{\delta}$ (the statement); a_s (Definition A.40)]

(L43) $\Rightarrow$ item 5

[(L42)]

(L44) $\forall \delta,\ |\delta| \le \bar{\delta} :\ |2\delta + \delta^2| = |\delta|(2 + \delta)$

[$2 + \delta > 0$ ((L1), (L2))]

(L45) $\forall \delta,\ |\delta| \le \bar{\delta} :\ |\delta|(2 + \delta) \le 2\bar{\delta} + \bar{\delta}^2$

[$|\delta| \le \bar{\delta}$; (L3)]

(L46) $|v_c'' - \alpha v_{1,c}| = \alpha |\Delta|\, (\alpha - 1) |2\delta + \delta^2|\, \theta_\alpha(\delta)$

[(L25), (L26); (L11); $\alpha > 1$ (the statement); $|xy| = |x||y|$ (Fact A.41, item 1)]

(L47) $\Rightarrow\ |v_c'' - \alpha v_{1,c}| \le a_c$

[(L46), (L44), (L45); (L8); $|\Delta| \le \bar{\Delta}$ (the statement); a_c (Definition A.40)]

(L48) $\Rightarrow$ item 6

[(L47)]

□ (items 1 to 6)

Corollary E.13 (The uniform bound over the four ranges [to table])**.** *Over the four ranges of the standard deviation, the ratio, the center and the center shift,* $|\ln \Phi|$ *is at most* $\bar{\phi}_{\text{u}}$*. Let:*

- $s_{\text{lo}}, s_{\text{hi}}$ *with* $0 < s_{\text{lo}} \le s_{\text{hi}}$*;*
- $\bar{\delta} \in [0, 1)$*;*
- $\bar{\Delta} \ge 0$.

Define:

- $r_- := (1 - \bar{\delta})\, \theta_\alpha(-\bar{\delta})^{1/2}$, $r_+ := (1 + \bar{\delta})\, \theta_\alpha(\bar{\delta})^{1/2}$ *and* $\underline{s} := s_{\text{lo}} r_-$ *(Definition A.40);*
- $\overline{s} := s_{\text{hi}} r_+$ *and* $\varepsilon_0^\circ := \varepsilon_0(\underline{s})$ *(Definition A.40);*
- $\bar{\phi}_{\text{u}}$*, that of Definition A.40;*
- ε_0*, that of Definition A.38;*
- Φ*, that of Definition A.39.*

Assume:

(A1) $(1 + \bar{\delta})^2 < \alpha/(\alpha - 1)$*;*

(A2) $\varepsilon_0^\circ < 1$.

Then

$$\forall s \in [s_{\text{lo}}, s_{\text{hi}}]\ \forall \delta \in [-\bar{\delta}, \bar{\delta}]\ \forall c' \in \mathbb{R}\ \forall \Delta \in [-\bar{\Delta}, \bar{\Delta}] :\quad |\ln \Phi(s, \delta, c', \Delta)| \le \bar{\phi}_{\text{u}}.$$

Proof.

DEFINES $s \in [s_{\text{lo}}, s_{\text{hi}}]$, $\delta \in [-\bar{\delta}, \bar{\delta}]$, $c' \in \mathbb{R}$ and $\Delta \in [-\bar{\Delta}, \bar{\Delta}]$, the four values the statement quantifies

Lemma E.11 at $(\alpha, s, \delta, c', \Delta)$	This proof
Shared: α, $s_{\text{lo}}, s_{\text{hi}}$, $\bar{\delta}$, s, δ, $\underline{s}, \overline{s}, \varepsilon_j^\circ, r_-, r_+$ (Definition A.40), $\theta_\alpha(\delta), s_1, s'', s_-, s_+$ (Definition A.39)	
Shared: $\alpha > 1$, $s_{\text{lo}} > 0$, $s_{\text{lo}} \le s_{\text{hi}}$, $\bar{\delta} \in [0, 1)$	
Shared: assumptions A1, A2	
(I1) Its item 1: $1 + \delta > 0$	
Its item 2: $\alpha + (1 - \alpha)(1 + \delta)^2 > 0$	
Its item 8: $[s_-, s_+] \subseteq [\underline{s}, \overline{s}]$	
Its item 9: $\forall j \le 4 :\ \varepsilon_j(s_-) \le \varepsilon_j^\circ$	
Its item 10: $\varepsilon_0(s_-) < 1$	

(L1) $1+\delta>0$

[item 1 of (I1)]

(L2) $\alpha+(1-\alpha)(1+\delta)^2>0$

[item 2 of (I1)]

(L3) $[s_-,s_+]\subseteq[\underline{s},\overline{s}]$

[item 8 of (I1)]

(L4) $\forall j\le 4:\ \varepsilon_j(s_-)\le\varepsilon_j^\circ$

[item 9 of (I1)]

(L5) $\varepsilon_0(s_-)<1$

[item 10 of (I1)]

Lemma E.12 at $(\alpha,s,\delta,c',\Delta)$	This proof
Shared: $\alpha,\ s_{\mathrm{lo}},s_{\mathrm{hi}},\ \bar\delta,\ \bar\Delta,\ s,\ \delta,\ c',\ \Delta,\ \underline{s},\overline{s},\varepsilon_j^\circ,r_-,r_+,b_s,b_c,a_s,a_c,g$ (Definition A.40), $\theta_\alpha(\delta),s_1,s'',s_-,s_+,v_1,v''$ (Definition A.39) Shared: $\alpha>1,\ s_{\mathrm{lo}}>0,\ s_{\mathrm{lo}}\le s_{\mathrm{hi}},\ \bar\delta\in[0,1)$ Shared: assumptions A1, A2	
$\bar\Delta\in\mathbb{R}$	$\bar\Delta\ge 0$ (the statement)

(I2)

Its item 1: $\lvert v_{1,s}\rvert\le s_{\mathrm{hi}}\bar\delta$
Its item 2: $\lvert v_{1,c}\rvert\le\bar\Delta$
Its item 3: $\lvert v_s''\rvert\le s_{\mathrm{hi}}b_s$
Its item 4: $\lvert v_c''\rvert\le b_c$
Its item 5: $\lvert v_s''-\alpha v_{1,s}\rvert\le s_{\mathrm{hi}}a_s$
Its item 6: $\lvert v_c''-\alpha v_{1,c}\rvert\le a_c$

(L6) $|v_{1,s}|\le s_{\mathrm{hi}}\bar\delta$

[item 1 of (I2)]

(L7) $|v_{1,c}|\le\bar\Delta$

[item 2 of (I2)]

(L8) $|v_s''|\le s_{\mathrm{hi}}b_s$

[item 3 of (I2)]

(L9) $|v_c''|\le b_c$

[item 4 of (I2)]

(L10) $|v_s''-\alpha v_{1,s}|\le s_{\mathrm{hi}}a_s$

[item 5 of (I2)]

(L11) $|v_c''-\alpha v_{1,c}|\le a_c$

[item 6 of (I2)]

(L12) $s>0$

[$s\in[s_{\mathrm{lo}},s_{\mathrm{hi}}]$ (the proof's block); $s_{\mathrm{lo}}>0$ (the statement)]

(L13) $\forall 0\le\sigma\le\sigma'\ \forall j\in\{2,3,4\}\ \forall 0\le e_j\le e_j'\ \forall 0\le x\le x'\ \forall 0\le y\le y':$
$(\sigma^2e_4+e_2)x^2+2\sigma e_3xy+e_2y^2\le(\sigma'^2e_4'+e_2')x'^2+2\sigma'e_3'x'y'+e_2'y'^2$

[the coefficients and terms of Q nonnegative (Definition A.39); Fact A.41, item 8]

(L14) $Q(v_1)\le\bar Q(s_{\mathrm{hi}}\bar\delta,\bar\Delta)$

[(L13); (L3), (L4); (L6), (L7); $\bar Q$ (Definition A.40)]

(L15) $Q(v'')\le\bar Q(s_{\mathrm{hi}}b_s,b_c)$

[(L13); (L3), (L4); (L8), (L9); $\bar Q$ (Definition A.40)]

(L16) $\forall x,x'\in[0,1),\ x<x':\ x^2/(1-x)<x'^2/(1-x')$

[Fact A.41, items 5 and 8]

	Lemma E.10 at $(\alpha, s, \delta, c', \Delta)$	This proof
	Shared: $\alpha,\ s,\ \delta,\ c',\ \Delta,\ \Phi,\ s_1, s_2, c, s'', m, v_1, v'', s_-, s_+, Q$ (Definition A.39), d (Definition A.29)	
(I3)	ϵ_0	$\varepsilon_0(s_-)$ (Definition A.39)
	$s > 0$	(L12)
	$\delta > -1$	(L1)
	$\alpha + (1-\alpha)(1+\delta)^2 > 0$	(L2)
	$c', \Delta \in \mathbb{R}$	The proof's block
	$(v_s, v_c) \in \mathbb{R}^2$	Definition A.39
	Assumption A1	(L5)
	Its conclusion: $\lvert\ln \Phi(s,\delta,c',\Delta)\rvert \le \frac{\alpha\epsilon_0^2}{1-\epsilon_0} + s_+\varepsilon_2(s_-)\lvert v_s'' - \alpha v_{1,s}\rvert + \varepsilon_1(s_-)\lvert v_c'' - \alpha v_{1,c}\rvert + \frac{Q(v'')+\alpha Q(v_1)}{2}$	

(L17) $|\ln \Phi| \le \frac{\alpha\varepsilon_0(s_-)^2}{1-\varepsilon_0(s_-)} + s_+\varepsilon_2(s_-)|v_s'' - \alpha v_{1,s}| + \varepsilon_1(s_-)|v_c'' - \alpha v_{1,c}| + \frac{Q(v'')+\alpha Q(v_1)}{2}$

[(I3)]

(L18) $\frac{\alpha\varepsilon_0(s_-)^2}{1-\varepsilon_0(s_-)} \le \frac{\alpha(\varepsilon_0^\circ)^2}{1-\varepsilon_0^\circ}$

[(L16); (L4) at $j := 0$; (L5); assumption A2]

(L19) $s_+\varepsilon_2(s_-)|v_s'' - \alpha v_{1,s}| \le \overline{s}\,\varepsilon_2^\circ\, s_{\mathrm{hi}} a_s$

[(L3), (L4), (L10); Fact A.41, item 8]

(L20) $\varepsilon_1(s_-)|v_c'' - \alpha v_{1,c}| \le \varepsilon_1^\circ a_c$

[(L4), (L11); Fact A.41, item 8]

(L21) $|\ln \Phi| \le \bar{\phi}_{\mathrm{u}}$

[(L17), (L18), (L19), (L20), (L14), (L15); $\bar{\phi}_{\mathrm{u}}$ (Definition A.40)]

(L22) $\Rightarrow$ the statement

[(L21); s, δ, c', Δ (the proof's block)]

□

Corollary E.14 (Leaf divergence bound [to table])**.** *At a pair of leaves, the divergence is at most e^{ϕ_0} times the closed-form factor, once $|\ln \Phi(s_2, \delta, c', c - c')| \le \phi_0$. Let:*

- $s_1 > 0$*, the first standard deviation of Lemma 4.1;*
- $s_2 > 0$*, its second standard deviation;*
- $c \in \mathbb{R}$*, its first center;*
- $c' \in \mathbb{R}$*, its second center;*
- $\phi_0 \in \mathbb{R}$*.*

Define:

- $s'' := (\alpha/s_1^2 + (1-\alpha)/s_2^2)^{-1/2}$*,* $G_1 := D_{\mathbb{Z}, s_1, c}$ *and* $G_2 := D_{\mathbb{Z}, s_2, c'}$ *(Lemma 4.1 at* $A := \alpha/s_1^2$ *and* $B := (1-\alpha)/s_2^2$*);*
- $\delta := s_1/s_2 - 1$*;*
- $\Phi(s_2, \delta, c', c - c')$*, the value of* Φ *of Definition A.39.*

Assume:

(A1) $s_1^2 < s_2^2\,\alpha/(\alpha - 1)$*;*

(A2) $|\ln \Phi(s_2, \delta, c', c - c')| \le \phi_0$*.*

Then

$$R_\alpha(G_1 \| G_2)^{\alpha-1} \le e^{\phi_0}\, \frac{s''}{s_1^\alpha s_2^{1-\alpha}}\, \exp\left(\frac{\alpha(\alpha-1)(c-c')^2 s''^2}{2 s_1^2 s_2^2}\right).$$

Proof. (L1) $\theta_\alpha(\delta)/s_2^2 = s''^2/(s_1^2 s_2^2)$

[$s''^2 = s_1^2\theta_\alpha(\delta)$ (Definition A.39) at $s := s_2$]

(L2) $s_1^2 < s_2^2\alpha/(\alpha-1) \iff \alpha + (1-\alpha)(1+\delta)^2 > 0$

[$\delta := s_1/s_2 - 1$; multiply by $(\alpha-1)/s_2^2 > 0$]

(L3) $\delta > -1$

[$\delta = s_1/s_2 - 1$ (the statement); $s_1, s_2 > 0$ (the statement)]

	Lemma E.5	This proof
	Shared: $\alpha,\ c',\ \delta,\ s'', \Phi$ (Definition A.39)	
(I1)	s	s_2
	Δ	$c - c'$
	$D_{\mathbb{Z},s_1,c}$	G_1 (Lemma 4.1)
	$D_{\mathbb{Z},s_2,c'}$	G_2 (Lemma 4.1)
	$s > 0$	$s_2 > 0$ (the statement)
	$\delta > -1$	(L3)
	$\alpha + (1-\alpha)(1+\delta)^2 > 0$	(L2); assumption A1
	Its conclusion: $R_\alpha(D_{\mathbb{Z},s_1,c} \,\|\, D_{\mathbb{Z},s_2,c'})^{\alpha-1} = \frac{s''}{s_1^\alpha s_2^{1-\alpha}} \exp\left(\frac{\alpha(\alpha-1)\Delta^2\theta_\alpha(\delta)}{2s^2}\right) \Phi(s,\delta,c',\Delta)$	

(L4) $R_\alpha(G_1 \| G_2)^{\alpha-1} = \frac{s''}{s_1^\alpha s_2^{1-\alpha}} \exp\left(\frac{\alpha(\alpha-1)(c-c')^2 s''^2}{2s_1^2 s_2^2}\right) \Phi(s_2,\delta,c',c-c')$

[(I1); (L1)]

(L5) $\Phi(s_2,\delta,c',c-c') \le e^{\phi_0}$

[$|\ln \Phi(s_2,\delta,c',c-c')| \le \phi_0$ (assumption A2); exp increasing (Fact A.41, item 5)]

(L6) $s_1, s_2, s'' > 0$

[$s_1, s_2 > 0$ (the statement); $s'' = (A+B)^{-1/2}$ (Lemma 4.1); Fact A.41, item 12]

(L7) $\frac{s''}{s_1^\alpha s_2^{1-\alpha}} \exp\left(\frac{\alpha(\alpha-1)(c-c')^2 s''^2}{2s_1^2 s_2^2}\right) > 0$

[(L6); $e^t > 0$ (Fact A.41, item 12); Fact A.41, item 8]

(L8) $\Rightarrow$ the statement

[(L4), (L5), (L7)]

□

E.3 Composition along the samples

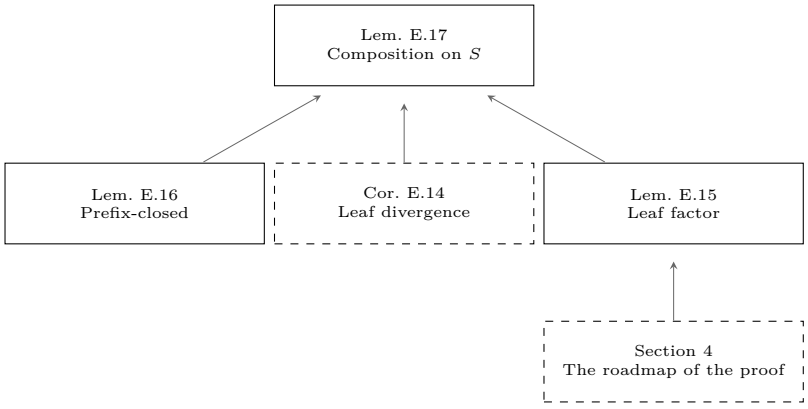


Figure 46: Dependencies, Section E.3.

Lemma E.15 (The closed-form factor at a leaf [to table])**.** *At a leaf, the closed-form factor depends on δ_i and Δ_i/σ_i only. Let:*

- $N \in \mathbb{Z}_{\ge 0}$;
- $i \le N$;
- $z_{<i} \in \mathbb{Z}^{i-1}$.

Define:

- $\sigma_i,\ \widetilde{\sigma}_i =: \sigma_i(1+\delta_i)$ *and* $\Delta_i := \widetilde{t}_i - t_i$ *at* $z_{<i}$ *(Definition A.27);*
- $s'' := (\alpha/\widetilde{\sigma}_i^2 + (1-\alpha)/\sigma_i^2)^{-1/2}$ *(Lemma 4.1 at* $s_1 := \widetilde{\sigma}_i,\ s_2 := \sigma_i$*).*

Assume:

(A1) $\widetilde{\sigma}_i^2 < \sigma_i^2\, \alpha/(\alpha-1)$.

Then the exponent and the factor are:

1. $\dfrac{\alpha(\alpha-1)\Delta_i^2 s''^2}{2\widetilde{\sigma}_i^2\sigma_i^2} = \dfrac{\alpha(\alpha-1)\Delta_i^2\theta_\alpha(\delta_i)}{2\sigma_i^2}$;

2. $\dfrac{s''}{\widetilde{\sigma}_i^{\alpha}\sigma_i^{1-\alpha}} = \theta_\alpha(\delta_i)^{1/2}(1+\delta_i)^{1-\alpha}$.

Proof. (L1) $1/s''^2 = \alpha/\widetilde{\sigma}_i^2 + (1-\alpha)/\sigma_i^2$
[s'' (Lemma 4.1) at $s_1 = \widetilde{\sigma}_i$, $s_2 = \sigma_i$, its $A + B > 0$ by assumption A1]

(L2) $\alpha/\widetilde{\sigma}_i^2 + (1-\alpha)/\sigma_i^2 = (\alpha + (1-\alpha)(1+\delta_i)^2)/(\sigma_i^2(1+\delta_i)^2)$
[$\widetilde{\sigma}_i = \sigma_i(1+\delta_i)$ (the statement); expand]

(L3) $\Rightarrow$ $s''^2 = \sigma_i^2(1+\delta_i)^2\theta_\alpha(\delta_i)$
[(L1), (L2); θ_α (the statement)]

(L4) $\Rightarrow$ $\frac{s''^2}{\widetilde{\sigma}_i^2\sigma_i^2} = \frac{\theta_\alpha(\delta_i)}{\sigma_i^2}$
[(L3); $\widetilde{\sigma}_i = \sigma_i(1+\delta_i)$ (the statement)]

(L5) $\Rightarrow$ item 1
[(L4) multiplied by $\alpha(\alpha-1)\Delta_i^2/2$]

(L6) $s'' = \sigma_i(1+\delta_i)\theta_\alpha(\delta_i)^{1/2}$
[(L3); $s'' > 0$ (Lemma 4.1); $\sigma_i(1+\delta_i) = \widetilde{\sigma}_i$, $\widetilde{\sigma}_i > 0$ (Definition A.27)]

(L7) $\sigma_i\,\sigma_i^{-\alpha}\,\sigma_i^{\alpha-1} = 1$
[add the exponents: $1-\alpha+\alpha-1=0$]

(L8) $(1+\delta_i)\,(1+\delta_i)^{-\alpha} = (1+\delta_i)^{1-\alpha}$
[add the exponents]

(L9) $\frac{s''}{\widetilde{\sigma}_i^{\alpha}\sigma_i^{1-\alpha}} = \frac{\sigma_i(1+\delta_i)\theta_\alpha(\delta_i)^{1/2}}{\sigma_i^{\alpha}(1+\delta_i)^{\alpha}\sigma_i^{1-\alpha}}$
[(L6); $\widetilde{\sigma}_i = \sigma_i(1+\delta_i)$ (the statement)]

(L10) $\Rightarrow$ item 2
[(L7), (L8), (L9)]

□ (items 1 and 2)

Lemma E.16 (Composition on a prefix-closed event [to table])**.** *On a prefix-closed event, the Rényi divergence of two measures on it, to the power $\alpha-1$, is at most the supremum of the product of the per-leaf bounds. Let:*

- $N \in \mathbb{Z}_{\geq 0}$ *(Definition A.1);*
- $P_i(\cdot \mid z_{<i})$ *and* $Q_i(\cdot \mid z_{<i})$*, probability measures on $\mathbb{Z}$ for $i \leq N$ and $z_{<i} \in \mathbb{Z}^{i-1}$;*
- $G_k \subseteq \mathbb{Z}^k$*, $k \leq N$;*
- $g_i : \mathbb{Z}^{i-1} \to (0,\infty)$*, $i \leq N$.*

Define:

- $P(z) := \prod_{i\leq N} P_i(z_i \mid z_{<i})$ *for $z \in \mathbb{Z}^N$;*
- $Q(z) := \prod_{i\leq N} Q_i(z_i \mid z_{<i})$ *for $z \in \mathbb{Z}^N$.*

Assume:

(A1) $\forall i \leq N\ \forall z_{<i} \in \mathbb{Z}^{i-1}\ \forall x \in \mathbb{Z}:\ Q_i(x \mid z_{<i}) > 0$*;*

(A2) $\forall k \in \{1,\dots,N\}\ \forall z_{\leq k} \in G_k:\ z_{<k} \in G_{k-1}$*;*

(A3) $\forall i \leq N\ \forall z_{<i} \in G_{i-1}:\ \sum_{x\in\mathbb{Z},\ (z_{<i},x)\in G_i} P_i(x \mid z_{<i})^{\alpha}\, Q_i(x \mid z_{<i})^{1-\alpha} \leq g_i(z_{<i})$.

Then the Rényi divergence on G_N to the power $\alpha-1$, in $[0,\infty]$, is at most the supremum of the product:

$$\sum_{z\in G_N} P(z)^{\alpha} Q(z)^{1-\alpha} \leq \sup_{z\in G_N} \prod_{i\leq N} g_i(z_{<i}).$$

Proof.

DEFINES $\forall k \le N\ \forall z_{\le k} \in \mathbb{Z}^k :\ P(z_{\le k}) := \prod_{i \le k} P_i(z_i \mid z_{<i})$
$\forall k \le N\ \forall z_{\le k} \in \mathbb{Z}^k :\ Q(z_{\le k}) := \prod_{i \le k} Q_i(z_i \mid z_{<i})$
$\forall k \le N\ \forall z_{\le k} \in \mathbb{Z}^k :\ g_{\le k}(z_{\le k}) := \prod_{i \le k} g_i(z_{<i})$
$\forall k \le N :\ \Sigma_k := \sum_{z_{\le k} \in G_k} P(z_{\le k})^\alpha Q(z_{\le k})^{1-\alpha} / g_{\le k}(z_{\le k}) \in [0, \infty]$

(L1) $\forall k \le N\ \forall z_{\le k} \in \mathbb{Z}^k :\ Q(z_{\le k}) > 0$

[$Q(z_{\le k})$ (the proof's block); assumption A1]

(L2) $\forall k \le N\ \forall z_{\le k} \in \mathbb{Z}^k :\ g_{\le k}(z_{\le k}) > 0$

[$g_{\le k}$ (the proof's block); $g_i > 0$ (the statement)]

(L3) $\forall k \in \{1, \dots, N\}\ \forall z_{\le k} \in \mathbb{Z}^k :\ \frac{P(z_{\le k})^\alpha Q(z_{\le k})^{1-\alpha}}{g_{\le k}(z_{\le k})} = \frac{P(z_{<k})^\alpha Q(z_{<k})^{1-\alpha}}{g_{\le k-1}(z_{<k})} \cdot \frac{P_k(z_k|z_{<k})^\alpha\, Q_k(z_k|z_{<k})^{1-\alpha}}{g_k(z_{<k})}$

[$P(z_{\le k})$, $Q(z_{\le k})$, $g_{\le k}$ (the proof's block), each the product at $k-1$ times its factor at k; (L1), (L2); expand]

(L4) $\forall\, 1 \le k \le N :\ \Sigma_k = \sum_{z_{<k} \in G_{k-1}} \sum_{x \in \mathbb{Z},\ (z_{<k}, x) \in G_k} \frac{P(z_{<k},x)^\alpha Q(z_{<k},x)^{1-\alpha}}{g_{\le k}(z_{<k},x)}$

[Σ_k (the proof's block); assumption A2; Fact A.45, item 11, at $Y := \mathbb{Z}^{k-1}$, $Y' := \mathbb{Z}$]

(L5) $\forall\, 1 \le k \le N :\ \Sigma_k = \sum_{z_{<k} \in G_{k-1}} \frac{P(z_{<k})^\alpha Q(z_{<k})^{1-\alpha}}{g_{\le k-1}(z_{<k})} \sum_{x \in \mathbb{Z},\ (z_{<k}, x) \in G_k} \frac{P_k(x|z_{<k})^\alpha\, Q_k(x|z_{<k})^{1-\alpha}}{g_k(z_{<k})}$

[(L4), (L3) at $z_{\le k} := (z_{<k}, x)$; Fact A.45, item 9: $\sum_y a f(y) = a \sum_y f(y)$]

(L6) $\forall k \in \{1, \dots, N\}\ \forall z_{<k} \in G_{k-1} :\ \sum_{x \in \mathbb{Z},\ (z_{<k}, x) \in G_k} \frac{P_k(x|z_{<k})^\alpha\, Q_k(x|z_{<k})^{1-\alpha}}{g_k(z_{<k})} \le 1$

[assumption A3 at $i := k$, divided by $g_k(z_{<k}) > 0$ (the statement)]

(L7) $\forall k \in \{1, \dots, N\} :\ \Sigma_k \le \sum_{z_{<k} \in G_{k-1}} \frac{P(z_{<k})^\alpha Q(z_{<k})^{1-\alpha}}{g_{\le k-1}(z_{<k})}$

[(L5), (L6); the outer terms in $[0, \infty)$ by (L1), (L2); Fact A.45, item 9]

(L8) $\Rightarrow\ \forall k \in \{1, \dots, N\} :\ \Sigma_k \le \Sigma_{k-1}$

[(L7); Σ_{k-1} (the proof's block)]

(L9) $\Sigma_0 \le 1$

[Σ_0 (the proof's block): $G_0 \subseteq \mathbb{Z}^0$, one point; P, Q, $g_{\le 0}$ at it: empty products, 1]

(L10) $\Rightarrow\ \Sigma_N \le 1$

[induction on k: (L9) the base at $k = 0$, (L8) the step from $k-1$ to k]

(L11) $\forall z \in G_N :\ P(z)^\alpha Q(z)^{1-\alpha} \le \left(\sup_{z' \in G_N} g_{\le N}(z')\right) \frac{P(z)^\alpha Q(z)^{1-\alpha}}{g_{\le N}(z)}$

[(L2); $g_{\le N}(z) \le \sup_{G_N} g_{\le N}$ (Fact A.41, item 20); $P(z) = P(z_{\le N})$, $Q(z) = Q(z_{\le N})$ (the statement; the proof's block)]

(L12) $\sum_{z \in G_N} P(z)^\alpha Q(z)^{1-\alpha} \le \left(\sup_{z' \in G_N} g_{\le N}(z')\right) \sum_{z \in G_N} \frac{P(z)^\alpha Q(z)^{1-\alpha}}{g_{\le N}(z)}$

[(L11) summed over $z \in G_N$ (Fact A.45, item 9)]

(L13) $\sum_{z \in G_N} P(z)^\alpha Q(z)^{1-\alpha} \le \left(\sup_{z' \in G_N} \prod_{i \le N} g_i(z'_{<i})\right) \Sigma_N$

[(L12); Σ_N, $g_{\le N}(z) = \prod_{i \le N} g_i(z_{<i})$ (the proof's block)]

(L14) $\Rightarrow$ the statement

[(L13), (L10); (L2)]

□

Lemma E.17 (Composition on the tail-cut event [to table])**.** *On the tail-cut event, the Rényi divergence of the computed measure from the ideal measure, to the power $\alpha - 1$, is at most a product of per-leaf factors. Let:*

- $N \in \mathbb{Z}_{\ge 0}$;
- $\bar\delta$, $\bar\theta_\alpha$, W_α, $\bar\phi \in \mathbb{R}$.

Define:

- $P_D(z) := \prod_{i \le N} D_{\mathbb{Z}, \widetilde\sigma_i(z_{<i}), \widetilde t_i(z_{<i})}(z_i)$ *for* $z \in \mathbb{Z}^N$ *(Definition A.28);*
- Q, *the measure of* ffSampling$^{\mathbb{R}}$ *(Definition A.25);*
- σ_i, δ_i *with* $\widetilde\sigma_i =: \sigma_i(1 + \delta_i)$, *and* Δ_i, *the leaf parameters (Definition A.27);*
- $\bar W_S := \sup_{z \in S} \sum_{i \le N} \Delta_i(z_{<i})^2 / \sigma_i(z_{<i})^2$ *(Definition A.27);*
- Φ, *the normalizer ratio of Definition A.39;*

- $\Phi_{\alpha,i} := \Phi(\sigma_i, \delta_i, t_i, \Delta_i)$.

Assume:

(A1) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ |\delta_i| \le \bar{\delta}$;

(A2) $\bar{\delta} < (\alpha/(\alpha-1))^{1/2} - 1$;

(A3) $\bar{\theta}_\alpha \ge 0$;

(A4) $\forall \delta > -1,\ |\delta| \le \bar{\delta} :\ \theta_\alpha(\delta) \le \bar{\theta}_\alpha$;

(A5) $W_\alpha > 0$;

(A6) $\forall \delta > -1,\ |\delta| \le \bar{\delta} :\ \theta_\alpha(\delta)^{1/2}(1+\delta)^{1-\alpha} \le W_\alpha$;

(A7) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ |\ln \Phi_{\alpha,i}| \le \bar{\phi}$.

Then the Rényi divergence on the tail-cut event to the power $\alpha - 1$ is bounded:

$$\sum_{z \in S} P_D(z)^\alpha Q(z)^{1-\alpha} \le (e^{\bar{\phi}} W_\alpha)^N \exp(\alpha(\alpha-1)\bar{\theta}_\alpha \bar{W}_S/2).$$

Proof.

DEFINES $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1},\ Q(z_{<i}) > 0 :\ Q_i(\,\cdot \mid z_{<i}) := Q(\,\cdot \mid z_{<i})$
$g_i(z_{<i}) := e^{\bar{\phi}} W_\alpha \exp(\alpha(\alpha-1)\bar{\theta}_\alpha \Delta_i^2/(2\sigma_i^2))$
$\forall k \le N :\ S_{\le k} := \{z_{\le k} : z \in S\}$ ($S_{<i}$ of the statement at $i := k+1$)
$s'' = (\alpha/\widetilde{\sigma}_i^2 + (1-\alpha)/\sigma_i^2)^{-1/2}$ (Lemma 4.1 at $s_1 := \widetilde{\sigma}_i$, $s_2 := \sigma_i$)

(L1) $\forall i\ \forall z_{<i} \in S_{<i} :\ \widetilde{\sigma}_i^2 < \sigma_i^2 \frac{\alpha}{\alpha-1}$
[$\widetilde{\sigma}_i = \sigma_i(1+\delta_i)$ (the statement); $|\delta_i| \le \bar{\delta}$ (assumption A1); $\bar{\delta} < (\alpha/(\alpha-1))^{1/2} - 1$ (assumption A2)]

(L2) $\forall i\ \forall z_{<i} :\ \widetilde{D}_i = D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$
[$\widetilde{D}_i$, P_D (Definition A.28)]

(L3) $\forall i\ \forall z_{<i} :\ Q_i|_{z_{<i}} = D_{\mathbb{Z},\sigma_i,t_i}$
[Q_i (the proof's block); Q (Definition A.25, item 2)]

(L4) $\forall i\ \forall z_{<i} :\ \delta_i > -1$
[δ_i (the statement); $\widetilde{\sigma}_i > 0$ ($\widetilde{D}_i$, Definition A.28); $\sigma_i > 0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2)]

(I1)

Corollary E.14 at every $i \le N$ and $z_{<i} \in S_{<i}$	This proof
Shared: $\alpha,\ s''$	
Shared: $\alpha > 1,\ \phi_0 \in \mathbb{R}$	
s_1	$\widetilde{\sigma}_i$
s_2	σ_i
c	$\widetilde{t}_i$
c'	t_i
G_1	$\widetilde{D}_i$ (L2)
G_2	$Q_i\|_{z_{<i}}$ (L3)
ϕ_0	$\bar{\phi}$ (the statement)
Φ	$\Phi_{\alpha,i}$ (the statement)
$s_1, s_2 > 0$	$\widetilde{\sigma}_i > 0$ ($\widetilde{D}_i$, Definition A.28); $\sigma_i > 0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2)
$c, c' \in \mathbb{R}$	$\widetilde{t}_i$, t_i (Definition A.25)
$\delta > -1$	(L4)
$\Delta \in \mathbb{R}$	Δ_i (Definition A.27)
Assumption A1	(L1)
Assumption A2	Assumption A7
Its conclusion: $R_\alpha(G_1\|G_2)^{\alpha-1} \le e^{\phi_0} \frac{s''}{s_1^\alpha s_2^{1-\alpha}} \exp\left(\frac{\alpha(\alpha-1)(c-c')^2 s''^2}{2 s_1^2 s_2^2}\right)$	

(L5) $\forall i\ \forall z_{<i} \in S_{<i} :\ R_\alpha(\widetilde{D}_i\|Q_i|_{z_{<i}})^{\alpha-1} \le e^{\bar{\phi}} \frac{s''}{\widetilde{\sigma}_i^\alpha \sigma_i^{1-\alpha}} \exp\left(\frac{\alpha(\alpha-1)(\widetilde{t}_i - t_i)^2 s''^2}{2\widetilde{\sigma}_i^2 \sigma_i^2}\right)$
[(I1)]

(L6) $\Rightarrow\ \forall i\ \forall z_{<i} \in S_{<i} :\ R_\alpha(\widetilde{D}_i\|Q_i|_{z_{<i}})^{\alpha-1} \le e^{\bar{\phi}} \frac{s''}{\widetilde{\sigma}_i^\alpha \sigma_i^{1-\alpha}} \exp\left(\frac{\alpha(\alpha-1)\Delta_i^2 s''^2}{2\widetilde{\sigma}_i^2 \sigma_i^2}\right)$

[(L5); Δ_i (the statement)]

Lemma E.15 at every $i \le N$ and $z_{<i} \in S_{<i}$	This proof
Shared: $\alpha,\ \sigma_i, \widetilde{\sigma}_i, \delta_i, \Delta_i,\ \theta_\alpha,\ s''$	
Shared: $N \in \mathbb{Z}_{\ge 0},\ \alpha > 1$	
$i \le N,\ z_{<i} \in \mathbb{Z}^{i-1}$	The scope
Assumption A1	(L1)
Its item 1: $\frac{\alpha(\alpha-1)\Delta_i^2 s''^2}{2\widetilde{\sigma}_i^2\sigma_i^2} = \frac{\alpha(\alpha-1)\Delta_i^2\theta_\alpha(\delta_i)}{2\sigma_i^2}$	
Its item 2: $\frac{s''}{\widetilde{\sigma}_i^\alpha \sigma_i^{1-\alpha}} = \theta_\alpha(\delta_i)^{1/2}(1+\delta_i)^{1-\alpha}$	

(I2)

(L7) $\forall i\ \forall z_{<i} \in S_{<i}:\ \frac{s''}{\widetilde{\sigma}_i^\alpha \sigma_i^{1-\alpha}} = \theta_\alpha(\delta_i)^{1/2}(1+\delta_i)^{1-\alpha}$

[item 2 of (I2)]

(L8) $\forall i\ \forall z_{<i} \in S_{<i}:\ \frac{\alpha(\alpha-1)\Delta_i^2 s''^2}{2\widetilde{\sigma}_i^2\sigma_i^2} = \frac{\alpha(\alpha-1)\Delta_i^2\theta_\alpha(\delta_i)}{2\sigma_i^2}$

[item 1 of (I2)]

(L9) $\forall i\ \forall z_{<i} \in S_{<i}:\ \theta_\alpha(\delta_i)^{1/2}(1+\delta_i)^{1-\alpha} \le W_\alpha$

[$|\delta_i| \le \bar{\delta}$ (assumption A1); $\delta_i > -1$ ($\widetilde{\sigma}_i = \sigma_i(1+\delta_i)$, $\widetilde{\sigma}_i, \sigma_i > 0$, Definition A.25); W_α (assumption A6)]

(L10) $\forall i\ \forall z_{<i} \in S_{<i}:\ \theta_\alpha(\delta_i) \le \bar{\theta}_\alpha$

[$|\delta_i| \le \bar{\delta}$ (assumption A1); $\delta_i > -1$ ($\widetilde{\sigma}_i = \sigma_i(1+\delta_i)$, $\widetilde{\sigma}_i, \sigma_i > 0$, Definition A.25); $\bar{\theta}_\alpha$ (assumption A4)]

(L11) $\Rightarrow\ \forall i\ \forall z_{<i} \in S_{<i}:\ R_\alpha(\widetilde{D}_i \| Q_i|_{z_{<i}})^{\alpha-1} \le g_i(z_{<i})$

[(L6) to (L10); $x \mapsto e^x$ nondecreasing (Fact A.41, item 5); g_i (the proof's block)]

(L12) $\forall i\ \forall z_{<i}:\ \sum_{z_i} \widetilde{D}_i^\alpha Q_i^{1-\alpha} = R_\alpha(\widetilde{D}_i \| Q_i)^{\alpha-1}$

[Definition A.3, item 2, at $(X, \mu, \nu) := (\mathbb{Z}, \widetilde{D}_i, Q_i)$; $Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2); Q_i (the proof's block)]

(L13) $\forall i\ \forall z_{<i}:\ g_i(z_{<i}) > 0$

[g_i (the proof's block); $W_\alpha > 0$ (assumption A5); $e^t > 0$ (Fact A.41, item 12)]

(L14) $\Rightarrow\ \forall i\ \forall z_{<i} \in S_{<i}:\ \sum_{x \in \mathbb{Z},\ (z_{<i},x) \in S_{\le i}} \widetilde{D}_i(x)^\alpha\, Q_i(x \mid z_{<i})^{1-\alpha} \le g_i(z_{<i})$

[(L11), (L12); $\widetilde{D}_i(x)^\alpha Q_i(x \mid z_{<i})^{1-\alpha} \ge 0$ ($\widetilde{D}_i$, Q_i probability measures); the sum over a subset of $\mathbb{Z}$ (Fact A.45, item 9); $S_{<i} = S_{\le i-1}$ (the proof's block)]

(L15) $\forall k \in \{1, \dots, N\}\ \forall z_{\le k} \in S_{\le k}:\ z_{<k} \in S_{\le k-1}$

[$S_{\le k}$ (the proof's block)]

Lemma E.16 at N	This proof
Shared: $Q_i(\cdot \mid z_{<i}),\ g_i$	
Shared: $\alpha > 1,\ N \in \mathbb{Z}_{\ge 0}$	
$P_i(\cdot \mid z_{<i})$	$\widetilde{D}_i$ (L2)
G_k	$S_{\le k}$ (the proof's block)
$P_i(\cdot \mid z_{<i}), Q_i(\cdot \mid z_{<i}) : \mathbb{Z} \to [0,1],\ \sum_{x \in \mathbb{Z}} P_i(x \mid z_{<i}) = 1,\ \sum_{x \in \mathbb{Z}} Q_i(x \mid z_{<i}) = 1$	$\widetilde{D}_i$ (Definition A.28); $Q_i(\cdot \mid z_{<i})$ (the proof's block)
$G_k \subseteq \mathbb{Z}^k$	$S_{\le k}$ (the proof's block)
$g_i : \mathbb{Z}^{i-1} \to (0, \infty)$	(L13)
$(P, Q) := (P_D, Q)$	Definitions A.28, A.25; Fact A.45, item 1
$G_N = S$	$S_{\le k}$ (the proof's block) at $k := N$
Assumption A1	$Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
Assumption A2	(L15)
Assumption A3	(L14)
Its conclusion: $\sum_{z \in G_N} P(z)^\alpha Q(z)^{1-\alpha} \le \sup_{z \in G_N} \prod_{i \le N} g_i(z_{<i})$	

(I3)

(L16) $\sum_{z \in S} P_D(z)^\alpha Q(z)^{1-\alpha} \le \sup_S \prod_i g_i$

[(I3)]

(L17) $\prod_i g_i = (e^{\bar\phi} W_\alpha)^N \exp\left(\frac{\alpha(\alpha-1)\bar\theta_\alpha}{2} \sum_i \frac{\Delta_i^2}{\sigma_i^2}\right)$

[g_i (the proof's block); Fact A.41, item 12: $e^x e^y = e^{x+y}$]

(L18) $\Rightarrow$ $\sup_S \prod_i g_i = (e^{\bar\phi} W_\alpha)^N \exp(\alpha(\alpha-1)\bar\theta_\alpha \bar W_S/2)$

[(L17); $\bar W_S$ (the statement); $\bar\theta_\alpha \geq 0$ (assumption A3); $x \mapsto e^x$ nondecreasing (Fact A.41, item 5)]

(L19) $\Rightarrow$ the statement

[(L16), (L18)]

□

E.4 Probability preservation

Lemma E.18 (A leaf's tail mass [to table])**.** *A leaf's mass beyond τ standard deviations is at most a Gaussian tail factor times the normalizers' ratio. Let:*

- $s > 0$;
- $t \in \mathbb{R}$;
- $z \leftarrow D_{\mathbb{Z},s,t}$.

Define:

- $\rho_s(y) = e^{-y^2/(2s^2)}$;
- $\forall c \in \mathbb{R}:\ \rho_{s,c}(\mathbb{Z}) = \sum_{x\in\mathbb{Z}} \rho_{s,c}(x)$ *(Definition A.2);*
- $\rho_s(\mathbb{Z}) = \rho_{s,0}(\mathbb{Z})$ *(Definition A.2).*

Then the tail is bounded:

1. $$\Pr[|z-t| > \tau s] \leq \frac{\rho_s(\mathbb{Z})}{\rho_{s,t}(\mathbb{Z})}\, \tau\, e^{(1-\tau^2)/2}. \qquad \textit{[L1: DRS14, Lem. 2.13]}$$

2. *Let $\epsilon \in [0,1)$. Assume:*

   (A1) $\forall c \in \mathbb{R}:\ \rho_{s,c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}s, (1+\epsilon)\sqrt{2\pi}s]$.

   Then
   $$\Pr[|z-t| > \tau s] \leq \frac{1+\epsilon}{1-\epsilon}\, \tau\, e^{(1-\tau^2)/2}.$$

[DRS14, Lem. 2.13] read for item 1	*This statement*
n	1
L	$\mathbb{Z}/(\sqrt{2\pi}\, s)$ *(the statement)*
c	$-t/(\sqrt{2\pi}\, s)$ *(the statement)*
y	$(z-t)/(\sqrt{2\pi}\, s)$
t	τ
(I1) $\rho(L+c)$	$\rho_{s,t}(\mathbb{Z})$ *(their $\rho(x) = e^{-\pi x^2}$; Definition A.2)*
$\rho(L)$	$\rho_s(\mathbb{Z})$ *(their $\rho(x) = e^{-\pi x^2}$; Definition A.2)*
$\Pr_{y\sim D_{L+c}}[\|\|y\\| \geq t\sqrt{n/(2\pi)}]$	$\Pr[\|z-t\| \geq \tau s]$
$e^{-\frac{n}{2}(t^2 - 2\log t - 1)}$	$\tau\, e^{(1-\tau^2)/2}$
L an n-dimensional lattice, $c \in \mathbb{R}^n$	*$s > 0$, $t \in \mathbb{R}$ (the statement)*
$t \geq 1$	$\tau > 1$ *(the statement)*
Its conclusion: $\Pr[\|z-t\| \geq \tau s] \leq \frac{\rho_s(\mathbb{Z})}{\rho_{s,t}(\mathbb{Z})}\, \tau\, e^{(1-\tau^2)/2}$	

Proof. Proof of item 1.

(L1) $\forall y \in \mathbb{R}:\ -\frac{y^2}{2s^2} = \frac{1-\tau^2}{2} - \frac{y^2}{2\tau^2 s^2} - \frac{(\tau^2-1)(y^2-\tau^2 s^2)}{2\tau^2 s^2}$

[expand]

(L2) $\forall y,\ |y| > \tau s:\ (\tau^2-1)(y^2-\tau^2 s^2)/(2\tau^2 s^2) \geq 0$

[$\tau > 1$ (the statement); $y^2 > \tau^2 s^2$ ($|y| > \tau s$, the line's quantifier; Fact A.41, item 5); Fact A.41, item 8]

(L3) $\Rightarrow\ \forall y,\ |y| > \tau s:\ \rho_s(y) \leq e^{(1-\tau^2)/2}\,\rho_{\tau s}(y)$

[(L1), (L2); $x \mapsto e^x$ nondecreasing (Fact A.41, item 5)]

(L4) $\Rightarrow\ \sum_{x\in\mathbb{Z},\ |x-t|>\tau s} \rho_{s,t}(x) \leq e^{(1-\tau^2)/2}\,\rho_{\tau s,t}(\mathbb{Z})$

[(L3) termwise at $y := x - t$; Definition A.2, item 1, at $(s,c) := (s,t)$, $(s,0)$, $(\tau s,t)$ and $(\tau s,0)$; $\rho_{\tau s,t}(x) \geq 0$ (Fact A.41, item 12) off the tail; the sums converge (Fact A.45, item 6)]

(L5) $\forall s' > 0\ \forall c \in \mathbb{R}:\ \rho_{s',c}(\mathbb{Z}) = \sqrt{2\pi}\,s' \sum_{k\in\mathbb{Z}} e^{-2\pi^2 s'^2 k^2} \cos(2\pi k c)$

[Fact A.45, item 6 (Mathlib's `Complex.tsum_exp_neg_quadratic`)]

(L6) $\Rightarrow\ \rho_{\tau s,t}(\mathbb{Z}) \leq \rho_{\tau s}(\mathbb{Z})$

[(L5) at $s' := \tau s$, $c := t$ and $c := 0$; $\rho_{\tau s}$ (Definition A.2); $\cos \leq 1$ and $e^{-2\pi^2 s'^2 k^2} > 0$ (Fact A.41, item 12)]

(L7) $\rho_{\tau s}(\mathbb{Z}) = \sqrt{2\pi}\,\tau s \sum_{k\in\mathbb{Z}} e^{-2\pi^2\tau^2 s^2 k^2}$

[(L5) at $c := 0$, $s' := \tau s$; $\rho_{\tau s}$ (Definition A.2); $\cos 0 = 1$ (Fact A.41, item 12, at $\theta := 0$)]

(L8) $\rho_s(\mathbb{Z}) = \sqrt{2\pi}\,s \sum_{k\in\mathbb{Z}} e^{-2\pi^2 s^2 k^2}$

[(L5) at $c := 0$, $s' := s$; $\rho_s(\mathbb{Z}) = \rho_{s,0}(\mathbb{Z})$ (the statement); $\cos 0 = 1$ (Fact A.41, item 12, at $\theta := 0$)]

(L9) $\Rightarrow\ \rho_{\tau s}(\mathbb{Z}) \leq \tau\,\rho_s(\mathbb{Z})$

[(L7), (L8); $\tau > 1 \Rightarrow\ e^{-2\pi^2\tau^2 s^2 k^2} \leq e^{-2\pi^2 s^2 k^2}$ (Fact A.41, item 5), termwise]

(L10) $\Pr[|z-t| > \tau s] = \frac{1}{\rho_{s,t}(\mathbb{Z})} \sum_{x\in\mathbb{Z},\ |x-t|>\tau s} \rho_{s,t}(x)$

[Definition A.2, item 2, at $c := t$]

(L11) $\rho_{s,t}(\mathbb{Z}) > 0$

[$\rho_{s,t}(\mathbb{Z}) = \sum_{x\in\mathbb{Z}} \rho_{s,t}(x)$ (the statement, at $c := t$); $\rho_{s,t}(x) = e^{-(x-t)^2/(2s^2)}$ (Definition A.2, item 1, at $c := t$); Fact A.41, item 12]

(L12) $\Rightarrow\ \Pr[|z-t| > \tau s] \leq \frac{e^{(1-\tau^2)/2}\,\rho_{\tau s,t}(\mathbb{Z})}{\rho_{s,t}(\mathbb{Z})}$

[(L10), (L4); (L11)]

(L13) $\Rightarrow\ \Pr[|z-t| > \tau s] \leq \frac{e^{(1-\tau^2)/2}\,\rho_{\tau s}(\mathbb{Z})}{\rho_{s,t}(\mathbb{Z})}$

[(L12), (L6); (L11)]

(L14) $e^{(1-\tau^2)/2}/\rho_{s,t}(\mathbb{Z}) > 0$

[(L11); Fact A.41, item 12]

(L15) $\Rightarrow$ item 1

[(L13), (L9); (L14)]

□ (item 1)

Proof of item 2.

(L16) $\Pr[|z-t| > \tau s] \leq \frac{\rho_s(\mathbb{Z})}{\rho_{s,t}(\mathbb{Z})}\,\tau\,e^{(1-\tau^2)/2}$

[item 1]

(L17) $\rho_s(\mathbb{Z}) \leq (1+\epsilon)\sqrt{2\pi}\,s$

[assumption A1 at $c := 0$; $\rho_s(\mathbb{Z}) = \rho_{s,0}(\mathbb{Z})$ (the statement)]

(L18) $\rho_{s,t}(\mathbb{Z}) \geq (1-\epsilon)\sqrt{2\pi}\,s$

[assumption A1 at $c := t$]

(L19) $(1-\epsilon)\sqrt{2\pi}\,s > 0$

[$\epsilon < 1$, $s > 0$ (the statement); Fact A.41, item 8]

(L20) $\Rightarrow\ \frac{\rho_s(\mathbb{Z})}{\rho_{s,t}(\mathbb{Z})} \leq \frac{1+\epsilon}{1-\epsilon}$

[(L17), (L18); (L19)]

(L21) $\tau\,e^{(1-\tau^2)/2} > 0$

[$\tau > 1$ (the statement); Fact A.41, item 12; Fact A.41, item 8]

(L22) $\Rightarrow$ item 2

[(L16), (L20); (L21)]

□ (item 2)

Corollary E.19 ([Ban93, Lem. (1.5)(ii)] at $n = 1$ [to table])**.** *A leaf's mass beyond τ standard deviations is at most twice the Gaussian tail factor times the normalizers' ratio. Let:*

- $s > 0$;
- $t \in \mathbb{R}$;
- $z \leftarrow D_{\mathbb{Z},s,t}$.

Define:

- $\rho_s(y) = e^{-y^2/(2s^2)}$;
- $\forall c \in \mathbb{R}:\ \rho_{s,c}(\mathbb{Z}) = \sum_{x\in\mathbb{Z}} \rho_{s,c}(x)$ *(Definition A.2);*
- $\rho_s(\mathbb{Z}) = \rho_{s,0}(\mathbb{Z})$ *(Definition A.2).*

Then [L1: Ban93, Lem. (1.5)(ii)] the tail is bounded:

$$\Pr[|z - t| > \tau s] \le 2\,\frac{\rho_s(\mathbb{Z})}{\rho_{s,t}(\mathbb{Z})}\,\tau\, e^{(1-\tau^2)/2}.$$

The citation [Ban93, Lem. (1.5)(ii)] is read at $n = 1$, $L := \mathbb{Z}/(\sqrt{2\pi}\,s)$, $u := -t/(\sqrt{2\pi}\,s)$, $c := \tau/\sqrt{2\pi}$, their $\rho(x) = e^{-\pi x^2}$, their $c \ge (2\pi)^{-1/2}$ at $\tau > 1$, and their open ball B'_1, whose event $|x| \ge c$ contains ours.

Proof.

(I1)	
Lemma E.18, item 1	This proof
Shared: s, t, z, $\rho_s(\mathbb{Z})$, $\rho_{s,t}(\mathbb{Z})$ Shared: $\tau > 1$, $s > 0$, $t \in \mathbb{R}$, $z \leftarrow D_{\mathbb{Z},s,t}$	
Its item 1: $\Pr[\lvert z-t\rvert > \tau s] \le \frac{\rho_s(\mathbb{Z})}{\rho_{s,t}(\mathbb{Z})}\,\tau\, e^{(1-\tau^2)/2}$	
$\Pr[\lvert z-t\rvert > \tau s] \le \frac{\rho_s(\mathbb{Z})}{\rho_{s,t}(\mathbb{Z})}\,\tau\, e^{(1-\tau^2)/2}$	

[(I1)]

(L2) $\rho_s(\mathbb{Z}), \rho_{s,t}(\mathbb{Z}) > 0$

[Definition A.2, item 2, at $c := 0$ and $c := t$; $\rho_s(\mathbb{Z}) = \rho_{s,0}(\mathbb{Z})$ (the statement)]

(L3) $\tau\, e^{(1-\tau^2)/2} > 0$

[$\tau > 1$ (the statement); Fact A.41, item 12; Fact A.41, item 8]

(L4) $1 \le 2$

[subtract]

(L5) $\Rightarrow$ the statement

[(L1), (L4); (L2), (L3); Fact A.41, item 8; Fact A.41, item 26]

□

Lemma E.20 (Ideal mass of the tail [to table])**.** *The tail S^c is covered by the leaves' tails, and each leaf's tail is small under the normalizer bounds. Let:*

- $\epsilon \in [0, 1)$.

Define:

- $P_D(z) := \prod_{i\le N} D_{\mathbb{Z},\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}(z_i)$ *for $z \in \mathbb{Z}^N$ (Definition A.28).*

Assume:

(A1) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ \widetilde{\sigma}_i > 0$;

(A2) $\forall i \le N\ \forall z_{<i}\ \forall c \in \mathbb{R}:\ \rho_{\widetilde{\sigma}_i,c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\widetilde{\sigma}_i]$.

Then the complement's cover, each leaf's tail and the complement's mass are bounded:

1. *Let P be a probability measure on $\mathbb{Z}^N$. Then $P(S^c) \le \sum_{i=1}^N \Pr_P[|z_i - \widetilde{t}_i| > \tau\,\widetilde{\sigma}_i]$;*
2. *$\forall i \le N\ \forall z_{<i}:\ \Pr_{P_D}[|z_i - \widetilde{t}_i| > \tau\,\widetilde{\sigma}_i \mid z_{<i}] \le \frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$;*
3. *$P_D(S^c) \le N\,\dfrac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$.*

Proof. Proof of item 1.

(L1) $S^c \subseteq \bigcup_{i \le N} \{z \in \mathbb{Z}^N : |z_i - \widetilde{t}_i(z_{<i})| > \tau\, \widetilde{\sigma}_i(z_{<i})\}$

[S (Definition A.26)]

(L2) $\Rightarrow\ P(S^c) \le \sum_{i=1}^{N} \Pr_P[|z_i - \widetilde{t}_i| > \tau\, \widetilde{\sigma}_i]$

[(L1); Fact A.45, item 5]

(L3) $\Rightarrow$ item 1

[(L2)]

□ (item 1)

Proof of item 2.

(L4) $\forall i \le N\ \forall z_{<i} :\ \Pr_{P_D}[\cdot \mid z_{<i}] = D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$

[P_D (Definition A.28)]

Lemma E.18, item 2 at every $i \le N$ and $z_{<i}$	This proof
Shared: $\tau,\ \epsilon$	
Shared: $\tau > 1,\ \epsilon \in [0,1)$	
s	$\widetilde{\sigma}_i(z_{<i})$ (the statement)
t	$\widetilde{t}_i(z_{<i})$ (the statement)
(I1) z	z_i (L4)
$\rho_{s,c}(\mathbb{Z})$	$\rho_{\widetilde{\sigma}_i,c}(\mathbb{Z})$ (the statement)
$s > 0$	Assumption A1
$t \in \mathbb{R}$	$\widetilde{t}_i$ (Definition A.25)
$z \leftarrow D_{\mathbb{Z},s,t}$	(L4)
Assumption A1	Assumption A2
Its conclusion: $\Pr[\lvert z - t\rvert > \tau s] \le \frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$	

(L5) $\forall i \le N\ \forall z_{<i} :\ \Pr_{P_D}[|z_i - \widetilde{t}_i| > \tau\, \widetilde{\sigma}_i \,|\, z_{<i}] \le \frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$

[(I1)]

(L6) $\Rightarrow$ item 2

[(L5)]

□ (item 2)

Proof of item 3.

Lemma E.20, item 1	This proof
(I2) P	P_D
$P : \mathbb{Z}^N \to [0,1],\ \sum_{x \in \mathbb{Z}^N} P(x) = 1$	P_D (Definition A.28)
Its item 1: $P(S^c) \le \sum_{i=1}^{N} \Pr_P[\lvert z_i - \widetilde{t}_i\rvert > \tau\, \widetilde{\sigma}_i]$	

(L7) $P_D(S^c) \le \sum_{i=1}^{N} \Pr_{P_D}[|z_i - \widetilde{t}_i| > \tau\, \widetilde{\sigma}_i]$

[(I2)]

(L8) $\forall i \le N :\ \Pr_{P_D}[|z_i - \widetilde{t}_i| > \tau\, \widetilde{\sigma}_i] = \mathbb{E}_{P_D}[\Pr_{P_D}[|z_i - \widetilde{t}_i| > \tau\, \widetilde{\sigma}_i \,|\, z_{<i}]]$

[Fact A.45, item 1]

(L9) $\forall i \le N :\ \mathbb{E}_{P_D}[\Pr_{P_D}[|z_i - \widetilde{t}_i| > \tau\, \widetilde{\sigma}_i \,|\, z_{<i}]] \le \frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$

[item 2 at every $z_{<i}$; $\mathbb{E}_{P_D}[1] = 1$ (P_D a probability measure)]

(L10) $\Rightarrow$ item 3

[(L7), (L8), (L9); the sum of the N leaves]

□ (item 3)

Corollary E.21 (The signer's tail mass [to table])**.** *Under the signer in $\mathcal{F}$, the tail S^c of the tail-cut event has mass at most N times one leaf's tail bound. Let:*

- $\epsilon \in [0,1)$.

Define:

- $S^c := \mathbb{Z}^N \setminus S$ *(Definition A.26 at τ).*

Let:

- $\epsilon_{\text{hi}} \geq 0$ *with* $\forall i \leq N\ \forall z_{<i}\ \forall z_i \notin C_i :\ \widetilde{B}_i(z_i) \leq (1+\epsilon_{\text{hi}})\,\widetilde{D}_i(z_i)$ *(Definition A.28).*

Assume:

(A1) $\forall i \leq N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i > 0$;

(A2) $\forall i \leq N\ \forall z_{<i}\ \forall c \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_i,c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$.

Then

$$P(S^c) \leq N\,(1+\epsilon_{\text{hi}})\,\frac{1+\epsilon}{1-\epsilon}\,\tau\,e^{(1-\tau^2)/2}.$$

Proof. (L1) $\forall i\ \forall\, z_{<i}\ \forall z_i \notin C_i :\ \widetilde{B}_i(z_i) \leq (1+\epsilon_{\text{hi}})\widetilde{D}_i(z_i)$

[ϵ_{hi} (the statement)]

(L2) $\forall i \leq N\ \forall\, z_{<i} \in \mathbb{Z}^{i-1} :\ C_i \subseteq \mathcal{Z}_i$

[assumption A1; C_i (Definition A.26); $\mathcal{Z}_i$ (Definition A.28)]

(L3) $\Rightarrow\ \forall i \leq N\ \forall z_{<i}\ \forall z_i \in \mathcal{Z}_i^c :\ \widetilde{B}_i(z_i) \leq (1+\epsilon_{\text{hi}})\,\widetilde{D}_i(z_i)$

[(L1), (L2)]

(L4) $\Rightarrow\ \forall i \leq N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \leq (1+\epsilon_{\text{hi}})\,\widetilde{D}_i(\mathcal{Z}_i^c)$

[(L3); Fact A.45, item 9, at $f := \widetilde{B}_i$, $g := (1+\epsilon_{\text{hi}})\widetilde{D}_i$ on $\mathcal{Z}_i^c$]

(L5) $\forall i \leq N\ \forall z_{<i} :\ \widetilde{D}_i(\mathcal{Z}_i^c) = \Pr_{z\leftarrow\widetilde{D}_i}[|z-\widetilde{t}_i| > \tau\,\widetilde{\sigma}_i]$

[$\widetilde{D}_i$, $\mathcal{Z}_i$ (Definition A.28)]

Lemma E.18, item 2 at every $i \leq N$ and $z_{<i}$, at τ	This proof
Shared: $\epsilon \in [0,1)$	
s, t	$\widetilde{\sigma}_i, \widetilde{t}_i$ (Definition A.25)
z	$z_i \leftarrow \widetilde{D}_i$ (Definition A.28)
(I1) $\rho_{s,c}(\mathbb{Z})$	$\rho_{\widetilde{\sigma}_i,c}(\mathbb{Z})$ (assumption A2)
$s > 0$	Assumption A1
$t \in \mathbb{R}$	$\widetilde{t}_i$ (Definition A.25)
$z \leftarrow D_{\mathbb{Z},s,t}$	$\widetilde{D}_i = D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$ (Definition A.28)
Assumption A1	Assumption A2
Its conclusion: $\Pr[\lvert z-t\rvert > \tau s] \leq \frac{1+\epsilon}{1-\epsilon}\,\tau\,e^{(1-\tau^2)/2}$	

(L6) $\Rightarrow\ \forall i \leq N\ \forall z_{<i} :\ \widetilde{D}_i(\mathcal{Z}_i^c) \leq \frac{1+\epsilon}{1-\epsilon}\,\tau\,e^{(1-\tau^2)/2}$

[(L5); (I1)]

(L7) $\Rightarrow\ \forall i \leq N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \leq (1+\epsilon_{\text{hi}})\,\frac{1+\epsilon}{1-\epsilon}\,\tau\,e^{(1-\tau^2)/2}$

[(L4), (L6); $\epsilon_{\text{hi}} \geq 0$ (the statement); Fact A.41, item 26, at $c := 1+\epsilon_{\text{hi}}$]

Lemma E.20, item 1 at P	This proof
Shared: ϵ, S^c Shared: $\epsilon \in [0,1)$	
(I2) $P : \mathbb{Z}^N \to [0,1],\ \sum_{z\in\mathbb{Z}^N} P(z) = 1$	The signer's output measure P (the statement)
Assumption A1 Assumption A2	Assumption A1 Assumption A2
Its conclusion: $P(S^c) \leq \sum_{i=1}^N \Pr_P[\lvert z_i - \widetilde{t}_i\rvert > \tau\,\widetilde{\sigma}_i]$	

(L8) $P(S^c) \leq \sum_{i=1}^N \Pr_P[|z_i - \widetilde{t}_i| > \tau\,\widetilde{\sigma}_i]$

[(I2)]

(L9) $\forall i \leq N :\ \Pr_P[|z_i - \widetilde{t}_i| > \tau\,\widetilde{\sigma}_i] = \mathbb{E}_P[\widetilde{B}_i(\mathcal{Z}_i^c)]$

[Fact A.45, item 1; $\widetilde{B}_i$, $\mathcal{Z}_i$ (Definition A.28)]

(L10) $\Rightarrow\ \forall i \leq N :\ \mathbb{E}_P[\widetilde{B}_i(\mathcal{Z}_i^c)] \leq (1+\epsilon_{\text{hi}})\,\frac{1+\epsilon}{1-\epsilon}\,\tau\,e^{(1-\tau^2)/2}$

[(L7) at every $z_{<i}$; $\mathbb{E}_P[1] = 1$ (P a probability measure)]

(L11) $\Rightarrow$ $P(S^c) \le N\,(1+\epsilon_{\text{hi}})\,\frac{1+\epsilon}{1-\epsilon}\,\tau\,e^{(1-\tau^2)/2}$

[(L8), (L9), (L10); the sum of the N leaves]

(L12) $\Rightarrow$ the statement

[(L11)]

□

Theorem 4.3 (*Probability preservation [to table]*) [to statement].

On the tail-cut event, the divergence of the computed from the ideal measure is at most Π *up to the event's masses, and every event keeps a mass under the ideal measure. Let:*

- $\bar\delta,\ \bar\theta_\alpha,\ W_\alpha,\ \bar\phi \in \mathbb{R}$.

Define:

- *The probability measures*
  - Q, *the measure of* ffSampling$^{\mathbb{R}}$ *(Definition A.25);*
  - $P_D(z) := \prod_{i\le N} D_{\mathbb{Z},\widetilde\sigma_i(z_{<i}),\widetilde t_i(z_{<i})}(z_i)$ *for* $z \in \mathbb{Z}^N$ *(Definition A.28);*
- *The tail-cut event*
  - $S := \{\, z \in \mathbb{Z}^N : \forall i \le N\ |z_i - \widetilde t_i(z_{<i})| \le \tau\,\widetilde\sigma_i(z_{<i}) \,\}$, *the tail-cut event (Definition A.26);*
  - $S_{<i} := \{\, z_{<i} : z \in S \,\}$ *and* $Q_S(A) := Q(A\cap S)/Q(S)$ *(Definition A.26);*
- *The conditional probability measures*
  - $(P_D)_S(A) := P_D(A\cap S)/P_D(S)$ *for* $A \subseteq \mathbb{Z}^N$;
- *The normalizer ratio*
  - Φ, *the normalizer ratio of Definition A.39;*
  - $\Phi_{\alpha,i} := \Phi(\sigma_i, \delta_i, t_i, \Delta_i)$;
- *The terms*
  - $\bar W_S := \sup_{z\in S} \sum_{i\le N} \Delta_i(z_{<i})^2/\sigma_i(z_{<i})^2$ *(Lemma E.17);*
  - $\Pi := \left[(e^{\bar\phi}W_\alpha)^N \exp(\alpha(\alpha-1)\bar\theta_\alpha \bar W_S/2)\right]^{1/(\alpha-1)}$.

Assume:

(A1) $P_D(S) > 0$;
(A2) $Q(S) > 0$;
(A3) $\bar\delta \ge \max_{i\le N} \sup_{z_{<i}\in S_{<i}} |\delta_i(z_{<i})|$;
(A4) $\bar\delta < (\alpha/(\alpha-1))^{1/2} - 1$;
(A5) $\bar\theta_\alpha \ge 0$;
(A6) $\forall \delta > -1,\ |\delta| \le \bar\delta :\ \theta_\alpha(\delta) \le \bar\theta_\alpha$;
(A7) $W_\alpha > 0$;
(A8) $\forall \delta > -1,\ |\delta| \le \bar\delta :\ \theta_\alpha(\delta)^{1/2}(1+\delta)^{1-\alpha} \le W_\alpha$;
(A9) $\bar\phi \ge \max_{i\le N} \sup_{z_{<i}\in S_{<i}} |\ln \Phi_{\alpha,i}(z_{<i})|$.

Then the conditioned measures' divergence and every event's ideal mass are bounded:

1. $R_\alpha((P_D)_S \,\|\, Q_S) \le Q(S)\,P_D(S)^{-\alpha/(\alpha-1)}\,\Pi$;
2. $\forall A \subseteq \mathbb{Z}^N,\ P_D(A) \ge P_D(S^c) :\quad Q(A) \ge (P_D(A) - P_D(S^c))^{\alpha/(\alpha-1)}/\Pi$.

Proof. Proof of item 1.

	Fact A.45, item 10	This proof
	Shared: α	
	X	$\mathbb{Z}^N$ (the statement)
	μ	P_D (the statement)
	ν	Q (the statement)
	B	S (the statement)
	μ_B	$(P_D)_S$ (the statement)
(I1)	ν_B	Q_S (the statement)
	α	α (the statement)
	X countable	$\mathbb{Z}^N$ countable (Fact A.41, item 17)
	$\mu, \nu : X \to [0,1]$, $\sum_{x\in X} \mu(x) = 1$, $\sum_{x\in X} \nu(x) = 1$	P_D (Definition A.28), Q (Definition A.25)
	$B \subseteq X$	S (Definition A.26)
	$\mu(B) > 0$	Assumption A1
	$\nu(B) > 0$	Assumption A2
	Its conclusion: $R_\alpha(\mu_B \,\|\, \nu_B)^{\alpha-1} = \nu(B)^{\alpha-1}\mu(B)^{-\alpha} \sum_{x\in B} \mu(x)^\alpha \, \nu(x)^{1-\alpha}$	

(L1) $R_\alpha((P_D)_S \| Q_S)^{\alpha-1} = Q(S)^{\alpha-1} P_D(S)^{-\alpha} \sum_{x\in S} P_D(x)^\alpha \, Q(x)^{1-\alpha}$

[(I1)]

(L2) $\forall i \le N \ \forall z_{<i} \in S_{<i} : \ |\delta_i(z_{<i})| \le \bar{\delta}$

[assumption A3; $a \le \max A$, $a \le \sup A$ (Fact A.41, item 20)]

(L3) $\forall i \le N \ \forall z_{<i} \in S_{<i} : \ |\ln \Phi_{\alpha,i}(z_{<i})| \le \bar{\phi}$

[assumption A9; $a \le \max A$, $a \le \sup A$ (Fact A.41, item 20)]

	Lemma E.17	This proof
	Shared: α, N, $\bar{\delta}, \bar{\theta}_\alpha, W_\alpha, \bar{\phi}$, P_D, Q, $\sigma_i, \delta_i, \Delta_i$ (Definition A.27), $\bar{W}_S$, $\Phi_{\alpha,i}$ Shared: $\alpha > 1$, $\tau > 1$, $\bar{\delta}, \bar{\theta}_\alpha, W_\alpha, \bar{\phi} \in \mathbb{R}$	
	$N \in \mathbb{Z}_{\ge 0}$	$N := 2n$, $n \in \{512, 1024\}$ (the statement)
	$\widetilde{\sigma}_i =: \sigma_i(1+\delta_i)$	δ_i (Definition A.27)
(I2)	Assumption A1	(L2)
	Assumption A2	Assumption A4
	Assumption A3	Assumption A5
	Assumption A4	Assumption A6
	Assumption A5	Assumption A7
	Assumption A6	Assumption A8
	Assumption A7	(L3)
	Its conclusion: $\sum_{z\in S} P_D(z)^\alpha Q(z)^{1-\alpha} \le (e^{\bar{\phi}} W_\alpha)^N \exp(\alpha(\alpha-1)\bar{\theta}_\alpha \bar{W}_S/2)$	

(L4) $\sum_{z\in S} P_D(z)^\alpha Q(z)^{1-\alpha} \le (e^{\bar{\phi}} W_\alpha)^N \exp(\alpha(\alpha-1)\bar{\theta}_\alpha \bar{W}_S/2)$

[(I2)]

(L5) $\Rightarrow \ R_\alpha((P_D)_S \| Q_S)^{\alpha-1} \le Q(S)^{\alpha-1} P_D(S)^{-\alpha} \, \Pi^{\alpha-1}$

[(L1), (L4); Π (the statement)]

(L6) $\Rightarrow$ item 1

[(L5); $x \mapsto x^{1/(\alpha-1)}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

□ (item 1)

Proof of item 2.

	[LSS14, Lem. 4.1] at every $A \subseteq \mathbb{Z}^N$	This proof
	α	α
	X	$\mathbb{Z}^N$
	P_1	$(P_D)_S$ (the statement)
	Q_1	Q_S (the statement)
	A	$A \cap S$
	$R_\alpha(P_1 \| Q_1)$	$R_\alpha((P_D)_S \| Q_S)$ (Definition A.3)
(I3)	$\alpha \in (1, \infty]$	$\alpha > 1$ (the statement)
	P_1, Q_1 discrete distributions on X, $\mathrm{Supp}(P_1) \subseteq \mathrm{Supp}(Q_1)$	P_D, Q conditioned on S (Definition A.3; assumptions A1, A2); $\mathrm{Supp}((P_D)_S) \subseteq S$ ($(P_D)_S$, the statement); $S \subseteq \mathrm{Supp}(Q_S)$ (Q_S, the statement; $Q > 0$ on $\mathbb{Z}^N$, Fact A.45, item 2, at $\mu := Q$; $Q_i > 0$ on $\mathbb{Z}$, Definition A.25, item 2)
	$A \subseteq X$	$A \cap S \subseteq \mathbb{Z}^N$ (Fact A.41, item 17)

Its conclusion: $Q_1(A) \geq P_1(A)^{\alpha/(\alpha-1)} / R_\alpha(P_1 \| Q_1)$

(L7) $\forall A:\ Q_S(A \cap S) \geq (P_D)_S(A \cap S)^{\alpha/(\alpha-1)} / R_\alpha((P_D)_S \| Q_S)$

[(I3)]

(L8) $\forall A:\ Q(A \cap S) = Q(S)\, Q_S(A \cap S)$

[Q_S (the statement); $(A \cap S) \cap S = A \cap S$ (Fact A.41, item 17: $A \cap S \subseteq S$)]

(L9) $\forall A:\ Q(S)\, Q_S(A \cap S) \geq \frac{Q(S)\,(P_D)_S(A \cap S)^{\alpha/(\alpha-1)}}{Q(S)\, P_D(S)^{-\alpha/(\alpha-1)}\, \Pi}$

[(L7); item 1]

(L10) $\forall A:\ \frac{Q(S)\,(P_D)_S(A \cap S)^{\alpha/(\alpha-1)}}{Q(S)\, P_D(S)^{-\alpha/(\alpha-1)}\, \Pi} = \frac{P_D(A \cap S)^{\alpha/(\alpha-1)}}{\Pi}$

[$(P_D)_S(A \cap S) = P_D(A \cap S)/P_D(S)$ ($(P_D)_S$, the statement; $(A \cap S) \cap S = A \cap S$, Fact A.41, item 17: $A \cap S \subseteq S$); collect]

(L11) $\Rightarrow\ \forall A:\ Q(A \cap S) \geq P_D(A \cap S)^{\alpha/(\alpha-1)} / \Pi$

[(L8), (L9), (L10)]

(L12) $\forall A:\ Q(A) \geq Q(A \cap S)$

[Q a probability measure (the statement); Fact A.45, item 12, at $A \cap S \subseteq A$ (Fact A.41, item 17)]

(L13) $\forall A:\ P_D(A \cap S) \geq P_D(A) - P_D(S^c)$

[$A \subseteq (A \cap S) \cup S^c$ (Fact A.41, item 17); Fact A.45, item 5]

(L14) $\forall A,\ P_D(A) \geq P_D(S^c):\ P_D(A) - P_D(S^c) \geq 0$

[the item's quantifier]

(L15) $\Rightarrow$ item 2

[(L11), (L12), (L13), (L14); $x \mapsto x^{\alpha/(\alpha-1)}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

□ (item 2)

E.5 The base sampler's divergence at a leaf

This subsection proves Proposition 4.2.

Proposition 4.2 (*The product bound on a leaf's Rényi divergence [to table]*) [to statement].

The leaf's Rényi divergence on a set from the ideal measure, to the power $\alpha - 1$, is at most a product of two leaf divergences. Let:

- $\mathcal{Y} \subseteq \mathbb{Z}$;
- $i \leq N$;
- $z_{<i} \in \mathbb{Z}^{i-1}$.

Define:

- $\widetilde{B} := B^{\mathcal{F}}_{\widetilde{\sigma}_i(z_{<i}), \widetilde{t}_i(z_{<i})}$ *and* $\widetilde{D} := D_{\mathbb{Z}, \widetilde{\sigma}_i(z_{<i}), \widetilde{t}_i(z_{<i})}$ *at* $z_{<i}$ *(Definition A.28);*
- $R^{\mathcal{Y}}_a(\widetilde{B} \,\|\, \widetilde{D}) := \left(\sum_{x \in \mathcal{Y}} \widetilde{B}(x)^a\, \widetilde{D}(x)^{1-a}\right)^{1/(a-1)}$ *for* $a > 1$ *(Definition A.28);*
- $Q = D_{\mathbb{Z}, \sigma_i, t_i}$ *at* $z_{<i}$*, the ideal measure at the parameters over* $\mathbb{R}$ *(Definition A.25, item 2).*

Assume:
(A1) $\sum_{z\in\mathcal{Y}} \widetilde{B}^{2\alpha}\widetilde{D}^{1-2\alpha} < \infty$;
(A2) $\sum_{z\in\mathbb{Z}} \widetilde{D}^{2\alpha-1}Q^{2-2\alpha} < \infty$.
Then

$$\sum_{z\in\mathcal{Y}} \widetilde{B}(z)^{\alpha}Q(z)^{1-\alpha} \le R_{2\alpha}^{\mathcal{Y}}(\widetilde{B}\,\|\,\widetilde{D})^{(2\alpha-1)/2}\, R_{2\alpha-1}(\widetilde{D}\,\|\,Q)^{\alpha-1}.$$

Proof. (L1) $\forall z\in\mathbb{Z}:\ \widetilde{D}(z) > 0$
[$\widetilde{D} = D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$ (Definition A.28)]
(L2) $\forall z\in\mathbb{Z}:\ \widetilde{B}^{\alpha}Q^{1-\alpha} = (\widetilde{B}/\widetilde{D})^{\alpha}\widetilde{D}^{1/2}\cdot\widetilde{D}^{\alpha-1/2}Q^{1-\alpha}$
[(L1); add the exponents of $\widetilde{D}$]
(L3) $\sum_{z\in\mathcal{Y}} \widetilde{D}^{2\alpha-1}Q^{2-2\alpha} \le \sum_{z\in\mathbb{Z}} \widetilde{D}^{2\alpha-1}Q^{2-2\alpha}$
[$\mathcal{Y}\subseteq\mathbb{Z}$ (the statement); $\widetilde{D}^{2\alpha-1}Q^{2-2\alpha}\ge 0$ ($\widetilde{D}$, Q probability measures); Fact A.45, item 9]
(L4) $\sum_{z\in\mathcal{Y}} \widetilde{B}^{\alpha}Q^{1-\alpha} \le \left[\sum_{z\in\mathcal{Y}}(\widetilde{B}/\widetilde{D})^{2\alpha}\widetilde{D}\right]^{1/2}\left[\sum_{z\in\mathcal{Y}}\widetilde{D}^{2\alpha-1}Q^{2-2\alpha}\right]^{1/2}$
[(L2); Fact A.41, item 4, over $z\in\mathcal{Y}$ at $X_z := (\widetilde{B}/\widetilde{D})^{\alpha}\widetilde{D}^{1/2}$, $Y_z := \widetilde{D}^{\alpha-1/2}Q^{1-\alpha}$; the two sums finite (assumptions A1, A2; (L3))]
(L5) $\sum_{z\in\mathcal{Y}}(\widetilde{B}/\widetilde{D})^{2\alpha}\widetilde{D} = \sum_{z\in\mathcal{Y}}\widetilde{B}^{2\alpha}\widetilde{D}^{1-2\alpha}$
[(L1); add the exponents of $\widetilde{D}$]
(L6) $\sum_{z\in\mathcal{Y}}\widetilde{B}^{2\alpha}\widetilde{D}^{1-2\alpha} = R_{2\alpha}^{\mathcal{Y}}(\widetilde{B}\|\widetilde{D})^{2\alpha-1}$
[$R_{2\alpha}^{\mathcal{Y}}$ (Definition A.28)]
(L7) $\sum_{z\in\mathbb{Z}}\widetilde{D}^{2\alpha-1}Q^{2-2\alpha} = R_{2\alpha-1}(\widetilde{D}\|Q)^{2\alpha-2}$
[Definition A.3, item 2, at $(X,\alpha,\mu,\nu) := (\mathbb{Z}, 2\alpha-1, \widetilde{D}, Q)$; $Q>0$ on $\mathbb{Z}$ (Definition A.25, item 2)]
(L8) $\Rightarrow$ the statement
[(L3) to (L7); $x\mapsto\sqrt{x}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]
□

F Proofs of the theorem

Structure. This appendix proves Theorems F.4 and 1.1. Lemma F.1 states the bound at one leaf; Lemma F.2 the composition along the samples; Lemma F.3 the conditioning on S'; Theorem F.4 the divergence on a sub-event of the tail-cut event; Corollary F.5 the four leading terms of $\ln R$.

How each statement is verified. Table 17 lists how each statement placed here is verified; the dependency graph of the appendix is Figure 118, in Appendix M.6.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma F.1	✓				
Lemma F.2	✓				
Lemma F.3	✓				
Thm. F.4	✓				
Cor. F.5	✓				

Table 17: Appendix F: how each lemma, corollary and theorem is verified.

Lemma F.1 (One leaf's conditional Rényi divergence [to table])**.** *At a leaf of a prefix in S', the computed measure's Rényi divergence on $\mathcal{Z}_i$ from the ideal measure, to the power $\alpha-1$, is at most g_i. Define:*

- $Q_i := D_{\mathbb{Z},\sigma_i,t_i}$ *for $i\le N$ and every $z_{<i}$, the conditional probability measure of Definition A.25, item 2;*

- $\widetilde{B}_i := B^{\mathcal{F}}_{\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}$ *(Definition A.28 at $C_i := \emptyset$);*
- $\mathcal{Z}_i := (|\cdot - \widetilde{t}_i|/\widetilde{\sigma}_i)^{-1}([0,\tau]) \subseteq \mathbb{Z}$ *(Definition A.28 at $C_i := \emptyset$);*
- $\bar{\rho}_B := \max_{i\le N} \sup_{z_{<i}\in S_{<i}} R^{\mathcal{Z}_i}_{2\alpha}(\widetilde{B}_i \,\|\, \widetilde{D}_i)$, *with* $\widetilde{D}_i := D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$ *(Definition A.28 at $C_i := \emptyset$);*
- $\bar{W}_{\alpha_L} > 0$ *with* $\forall \delta > -1,\ |\delta| \le \bar{\delta} :\ \theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \le \bar{W}_{\alpha_L}$ *(Definition A.30);*
- $\bar{\theta}_{\alpha_L} \ge 0$ *with* $\forall \delta > -1,\ |\delta| \le \bar{\delta} :\ \theta_{\alpha_L}(\delta) \le \bar{\theta}_{\alpha_L}$ *(Definition A.30);*
- $B_i := e^{\bar{\phi}}\, \bar{W}_{\alpha_L} \exp(\alpha_L(\alpha_L-1)\bar{\theta}_{\alpha_L}\Delta_i^2/(2\sigma_i^2))$ *for $i \le N$ and every $z_{<i}$;*
- $g_i := \bar{\rho}_B^{\alpha_L/2} B_i^{1/2}$.

Assume:

(A1) $(1+\bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$;

(A2) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i > 0$.

Then

$$\forall i \le N\ \forall\, z_{<i} \in S'_{<i} :\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i}(\widetilde{B}_i/Q_i)^\alpha \,|\, z_{<i}] \le g_i.$$

Proof.

DEFINES $\widetilde{D}_i := D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$ (Definition A.28)
DEFINES $S_{<i} := \{\, z_{<i} : z \in S \,\}$ (Definition A.26)
DEFINES $\Phi_{\alpha_L,i} := (1+d(s_i'',m_i))(1+d(\widetilde{\sigma}_i,\widetilde{t}_i))^{-\alpha_L}(1+d(\sigma_i,t_i))^{\alpha_L-1}$ (Definition A.29)
DEFINES $d(s,c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\, s) - 1$ (Definition A.29)
DEFINES $s_i'' := \sigma_i(1+\delta_i)\,\theta_{\alpha_L}(\delta_i)^{1/2}$ and $m_i := t_i + \alpha_L\theta_{\alpha_L}(\delta_i)\,\Delta_i$ (Definition A.29)
DEFINES $\theta_{\alpha_L}(\delta) := 1/(\alpha_L + (1-\alpha_L)(1+\delta)^2)$ (Definition A.30)

(L1) $\forall i :\ \widetilde{D}_i = D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$
[$\widetilde{D}_i$ (the proof's block; Definition A.28)]

(L2) $\forall i \le N :\ S'_{<i} \subseteq S_{<i}$
[$S' \subseteq S$ (Definition A.26); $S'_{<i}$, $S_{<i}$ (Definition A.26)]

(L3) $\forall i\ \forall\, z_{<i} \in S'_{<i} :\ |\delta_i| \le \bar{\delta}$
[$\bar{\delta}$ (Definition A.27)]

(L4) $\forall i\ \forall\, z_{<i} \in \mathbb{Z}^{i-1} :\ 1 + \delta_i = \widetilde{\sigma}_i/\sigma_i$
[δ_i (Definition A.27); $\sigma_i > 0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2); divide by σ_i]

(L5) $\forall i\ \forall\, z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i/\sigma_i > 0$
[$\widetilde{\sigma}_i > 0$ (assumption A2); $\sigma_i > 0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28) at $(y,a) := (\sigma_i, -1)$; $\prod_k c_k > 0$ at $c_k > 0$ (Fact A.41, items 12 and 28)]

(L6) $\Rightarrow\ \forall i\ \forall\, z_{<i} \in \mathbb{Z}^{i-1} :\ \delta_i > -1$
[(L4), (L5)]

(L7) $\forall i\ \forall\, z_{<i} \in S'_{<i} :\ (1+\delta_i)^2 < \alpha_L/(\alpha_L - 1)$
[$|1+\delta_i| \le 1 + \bar{\delta}$ ((L3); Fact A.41, item 1); $t \mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5); assumption A1]

(L8) $\forall i\ \forall\, z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i^2 = \sigma_i^2(1+\delta_i)^2$
[δ_i (Definition A.27); expand]

(L9) $\forall i\ \forall\, z_{<i} \in \mathbb{Z}^{i-1} :\ \sigma_i^2 > 0$
[$\sigma_i > 0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28)]

(L10) $\forall i\ \forall\, z_{<i} \in S'_{<i} :\ \widetilde{\sigma}_i^2 < \sigma_i^2\,\alpha_L/(\alpha_L - 1)$
[(L8); (L7) multiplied by $\sigma_i^2 > 0$ ((L9); Fact A.41, item 26)]

(L11) $\forall i\ \forall\, z_{<i} \in S'_{<i} :\ |\ln \Phi_{\alpha_L,i}| \le \bar{\phi}$
[$\bar{\phi}$ (Definition A.29)]

	Corollary E.14 at order α_L, at every $i \le N$ and $z_{<i} \in S'_{<i}$	This proof
	α	α_L (the statement)
	s_1	$\widetilde{\sigma}_i$
	s_2	σ_i
	c	$\widetilde{t}_i$
	c'	t_i
	G_1	$\widetilde{D}_i$ (L1)
	G_2	Q_i (the statement)
	ϕ_0	$\bar{\phi}$ (Definition A.29)
	s''	s''_i (Definition A.39 at $s := \sigma_i$, $\delta := \delta_i$; Definition A.29)
(I1)	Φ	$\Phi_{\alpha_L,i}$ (Definition A.39 at $s := \sigma_i$, $\delta := \delta_i$, $\Delta := \Delta_i$; Definition A.29)
	$\alpha > 1$	$\alpha_L > 1$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement)
	$s_1, s_2 > 0$	Assumption A2; $\sigma_i > 0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2)
	$c, c' \in \mathbb{R}$	$\widetilde{t}_i$, t_i (Definition A.25)
	$\delta > -1$	(L6)
	$\Delta \in \mathbb{R}$	Δ_i (Definition A.27)
	$\phi_0 \in \mathbb{R}$	$\bar{\phi}$ (Definition A.29)
	Assumption A1	(L10)
	Assumption A2	(L11)
	Its conclusion: $R_\alpha(G_1\|G_2)^{\alpha-1} \le e^{\phi_0} \frac{s''}{s_1^\alpha s_2^{1-\alpha}} \exp\left(\frac{\alpha(\alpha-1)(c-c')^2 s''^2}{2 s_1^2 s_2^2}\right)$	

(L12) $\forall i\ \forall z_{<i} \in S'_{<i}:\ R_{\alpha_L}(\widetilde{D}_i\|Q_i)^{\alpha_L-1} \le e^{\bar{\phi}} \frac{s''_i}{\widetilde{\sigma}_i^{\alpha_L}\sigma_i^{1-\alpha_L}} \exp\left(\frac{\alpha_L(\alpha_L-1)(\widetilde{t}_i-t_i)^2 s''^2_i}{2\widetilde{\sigma}_i^2\sigma_i^2}\right)$

[(I1)]

(L13) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \frac{s''_i}{\widetilde{\sigma}_i^{\alpha_L}\sigma_i^{1-\alpha_L}} = \theta_{\alpha_L}(\delta_i)^{1/2}(1+\delta_i)^{1-\alpha_L}$

[s''_i, $\theta_{\alpha_L}(\delta_i)$ (Definition A.29); δ_i (Definition A.27); expand]

(L14) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \frac{(\widetilde{t}_i-t_i)^2 s''^2_i}{\widetilde{\sigma}_i^2\sigma_i^2} = \frac{\theta_{\alpha_L}(\delta_i)\Delta_i^2}{\sigma_i^2}$

[s''_i, $\theta_{\alpha_L}(\delta_i)$ (Definition A.29); δ_i, Δ_i (Definition A.27); expand]

(L15) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \theta_{\alpha_L}(\delta_i) > 0$

[$\theta_{\alpha_L}(\delta_i)$ (Definition A.29); (L7); $\alpha_L > 1$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement)]

(L16) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \theta_{\alpha_L}(\delta_i)^{1/2}(1+\delta_i)^{1-\alpha_L} \in [0, \bar{W}_{\alpha_L}]$

[(L3), (L6), (L15); $\bar{W}_{\alpha_L}$ (Definition A.30); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28)]

(L17) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \theta_{\alpha_L}(\delta_i) \le \bar{\theta}_{\alpha_L}$

[(L3), (L6); $\bar{\theta}_{\alpha_L}$ (Definition A.30)]

(L18) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \frac{s''_i}{\widetilde{\sigma}_i^{\alpha_L}\sigma_i^{1-\alpha_L}} \in [0, \bar{W}_{\alpha_L}]$

[(L13), (L16)]

(L19) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \alpha_L(\alpha_L-1)\Delta_i^2/(2\sigma_i^2) \ge 0$

[$\alpha_L > 1$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement); $\sigma_i > 0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2); $\Delta_i^2 \ge 0$ (Fact A.41, item 13); $ab \le a'b'$ at $(a, a', b, b') := (0, \alpha_L(\alpha_L-1), 0, \Delta_i^2/(2\sigma_i^2))$ (Fact A.41, item 8)]

(L20) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \frac{\alpha_L(\alpha_L-1)(\widetilde{t}_i-t_i)^2 s''^2_i}{2\widetilde{\sigma}_i^2\sigma_i^2} \le \alpha_L(\alpha_L-1)\bar{\theta}_{\alpha_L}\Delta_i^2/(2\sigma_i^2)$

[(L14); (L17) multiplied by $\alpha_L(\alpha_L-1)\Delta_i^2/(2\sigma_i^2) \ge 0$ ((L19); Fact A.41, item 26)]

(L21) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \exp\left(\frac{\alpha_L(\alpha_L-1)(\widetilde{t}_i-t_i)^2 s''^2_i}{2\widetilde{\sigma}_i^2\sigma_i^2}\right) \le \exp(\alpha_L(\alpha_L-1)\bar{\theta}_{\alpha_L}\Delta_i^2/(2\sigma_i^2))$

[(L20); exp increasing on $\mathbb{R}$ (Fact A.41, item 5)]

(L22) $\forall i\ \forall z_{<i} \in S'_{<i}:\ e^{\bar{\phi}} \frac{s''_i}{\widetilde{\sigma}_i^{\alpha_L}\sigma_i^{1-\alpha_L}} \exp\left(\frac{\alpha_L(\alpha_L-1)(\widetilde{t}_i-t_i)^2 s''^2_i}{2\widetilde{\sigma}_i^2\sigma_i^2}\right) \le B_i$

[B_i (the statement); (L18), (L21); $e^t > 0$ (Fact A.41, item 12); $ab \le a'b'$ (Fact A.41, item 8); $e^{\bar{\phi}} > 0$ (Fact A.41, item 12); $ca \le cb$ (Fact A.41, item 26)]

(L23) $\Rightarrow\ \forall i\ \forall z_{<i} \in S'_{<i}:\ R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha_L - 1} \le B_i$

[(L12), (L22)]

Proposition 4.2 at every $i \le N$ and $z_{<i} \in S'_{<i}$	This proof
Shared: $n \in \{512, 1024\},\ N := 2n,\ \alpha > 1$	
α	α (the statement)
$2\alpha - 1$	α_L (the statement)
$\mathcal{Y}$	$\mathcal{Z}_i$ (Definition A.28)
$\widetilde{B}$	$\widetilde{B}_i$ (the statement)
$\widetilde{D}$	$\widetilde{D}_i$ (L1)
Q	Q_i (the statement)
$\mathcal{Y} \subseteq \mathbb{Z}$	$\mathcal{Z}_i$ (Definition A.28)
$i \le N,\ z_{<i} \in \mathbb{Z}^{i-1}$	The scope
Assumption A1	$\mathcal{Z}_i$ finite (Definition A.28)
Assumption A2	(L23)
Its conclusion: $\sum_{z \in \mathcal{Y}} \widetilde{B}(z)^\alpha Q(z)^{1-\alpha} \le R^{\mathcal{Y}}_{2\alpha}(\widetilde{B} \,\|\, \widetilde{D})^{(2\alpha-1)/2}\, R_{2\alpha-1}(\widetilde{D} \,\|\, Q)^{\alpha-1}$	

(I2)

(L24) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \sum_{z \in \mathcal{Z}_i} \widetilde{B}_i(z)^\alpha Q_i(z)^{1-\alpha} \le R^{\mathcal{Z}_i}_{2\alpha}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2}\, R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1}$

[(I2)]

Fact A.45, item 3 at every $i \le N$ and $z_{<i} \in \mathbb{Z}^{i-1}$	This proof
Shared: $N,\ i,\ \alpha$	
μ	Q (Definition A.25)
p	$z_{<i}$
ν	$\widetilde{B}_i$ (the statement)
Y	$\mathcal{Z}_i$ (the statement)
$\mu_i(\cdot \mid p)$	Q_i (the statement)
$N \ge 1$	$N := 2n,\ n \in \{512, 1024\}$ (the statement)
$\mu : \mathbb{Z}^N \to [0,1],\ \sum_{z \in \mathbb{Z}^N} \mu(z) = 1$	Q (Definition A.25)
$i \le N,\ p \in \mathbb{Z}^{i-1}$	The scope
$\mu(p) > 0$	Fact A.45, item 2, at $\mu := Q$; $Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
$\nu : \mathbb{Z} \to [0,1],\ \sum_{x \in \mathbb{Z}} \nu(x) = 1$	$\widetilde{B}_i$ (Definition A.28)
$Y \subseteq \mathbb{Z}$	$\mathcal{Z}_i$ (Definition A.28)
$\forall x \in Y:\ \mu_i(x \mid p) > 0$	$Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
Its conclusion: $\mathbb{E}_\mu[\mathbf{1}_Y (\nu/\mu_i(\cdot \mid p))^\alpha \mid p] = \sum_{x \in Y} \nu(x)^\alpha\, \mu_i(x \mid p)^{1-\alpha}$	

(I3)

(L25) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i} (\widetilde{B}_i/Q_i)^\alpha \mid z_{<i}] = \sum_{x \in \mathcal{Z}_i} \widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha}$

[(I3)]

(L26) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i} (\widetilde{B}_i/Q_i)^\alpha \mid z_{<i}] \le R^{\mathcal{Z}_i}_{2\alpha}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2}\, R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1}$

[(L24), (L25)]

(L27) $\forall i\ \forall z_{<i} \in S'_{<i}:\ R^{\mathcal{Z}_i}_{2\alpha}(\widetilde{B}_i \| \widetilde{D}_i) \le \bar{\rho}_B$

[(L2); $\bar{\rho}_B$ (Definition A.28 at $C_i := \emptyset$); $a \le \max A$ and $a \le \sup A$ (Fact A.41, item 20)]

(L28) $\forall i\ \forall z_{<i} \in S'_{<i}:\ R^{\mathcal{Z}_i}_{2\alpha}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2} \le \bar{\rho}_B^{\alpha_L/2}$

[(L27); $t \mapsto t^p$ nondecreasing on $[0,\infty)$ at $p := \alpha_L/2$ (Fact A.41, item 5); $R^{\mathcal{Z}_i}_{2\alpha}(\widetilde{B}_i \| \widetilde{D}_i) \ge 0$ ($R^{\mathcal{Y}}_a$, Definition A.28); $\alpha_L/2 > 0$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement)]

(L29) $\forall i\ \forall z_{<i} \in S'_{<i}:\ R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1} = (R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha_L - 1})^{1/2}$

[$\alpha_L - 1 = 2(\alpha - 1)$ ($\alpha_L = 2\alpha - 1$, the statement); $(y^a)^b = y^{ab}$ at $y > 0$ (Fact A.41, items 12, 28 and 30); $R_{\alpha_L}(\widetilde{D}_i \| Q_i) \in (0, \infty]$ (R_α, Definition A.3) at $(\alpha, \mu, \nu) := (\alpha_L, \widetilde{D}_i, Q_i)$; $Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)]

(L30) $\forall i\ \forall z_{<i} \in S'_{<i}:\ (R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha_L - 1})^{1/2} \le B_i^{1/2}$

[(L23); $x \mapsto \sqrt{x}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5); $R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha_L - 1} \ge 0$ (R_α, Definition A.3)]

(L31) $\forall i\ \forall z_{<i} \in S'_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2}\, R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1} \le \bar{\rho}_B^{\alpha_L/2} B_i^{1/2}$
[(L28), (L29), (L30); $ab \le a'b'$ (Fact A.41, item 8); $R_{2\alpha}^{\mathcal{Z}_i}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2} \ge 0$ ($R_a^{\mathcal{Y}}$, Definition A.28); $R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1} \ge 0$ (R_α, Definition A.3)]

(L32) $\Rightarrow\ \forall i\ \forall z_{<i} \in S'_{<i}:\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i}(\widetilde{B}_i/Q_i)^\alpha \,|\, z_{<i}] \le g_i$
[(L26), (L31); g_i (the statement)]

(L33) $\Rightarrow$ the statement
[(L32)]

□

Lemma F.2 (The Rényi divergence on S' [to table])**.** *On a sub-event of the tail-cut event, the Rényi divergence on it of the computed measure from the ideal measure, to the power $\alpha-1$, is at most $R^{\alpha-1}$ once every leaf's Rényi divergence on $\mathcal{Z}_i$, to the power $\alpha-1$, is at most g_i. Define:*

- $Q_i := D_{\mathbb{Z},\sigma_i,t_i}$ *for $i \le N$ and every $z_{<i}$ (Definition A.25, item 2);*
- $\widetilde{B}_i := B^{\mathcal{F}}_{\widetilde{\sigma}_i(z_{<i}),\widetilde{t}_i(z_{<i})}$ *(Definition A.28 at $C_i := \emptyset$);*
- $\mathcal{Z}_i := (|\cdot - \widetilde{t}_i|/\widetilde{\sigma}_i)^{-1}([0,\tau]) \subseteq \mathbb{Z}$ *(Definition A.28 at $C_i := \emptyset$);*
- $\bar{\rho}_B := \max_{i\le N} \sup_{z_{<i}\in S_{<i}} R_{2\alpha}^{\mathcal{Z}_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)$*, with $\widetilde{D}_i := D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$ (Definition A.28 at $C_i := \emptyset$);*
- $g_i := \bar{\rho}_B^{\alpha_L/2} B_i^{1/2}$ *(Lemma F.1).*

Assume:

(A1) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ \widetilde{\sigma}_i > 0$;

(A2) $\bar{\rho}_B > 0$;

(A3) $\forall i \le N\ \forall z_{<i} \in S'_{<i}:\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i}(\widetilde{B}_i/Q_i)^\alpha \,|\, z_{<i}] \le g_i$.

Then

$$\sum_{z\in S'} P(z)^\alpha Q(z)^{1-\alpha} \le R^{\alpha-1}.$$

Proof.

DEFINES $G_k := \{z_{\le k} : z \in S'\}$, $k \le N$

DEFINES $B_i := e^{\bar{\phi}} \bar{W}_{\alpha_L} \exp(\alpha_L(\alpha_L-1)\bar{\theta}_{\alpha_L}\Delta_i^2/(2\sigma_i^2))$ (Lemma F.1)

DEFINES $\bar{W}_{\alpha_L} > 0$ with $\forall \delta > -1,\ |\delta| \le \bar{\delta}:\ \theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \le \bar{W}_{\alpha_L}$ (Definition A.30)

DEFINES $\bar{\theta}_{\alpha_L} \ge 0$ with $\forall \delta > -1,\ |\delta| \le \bar{\delta}:\ \theta_{\alpha_L}(\delta) \le \bar{\theta}_{\alpha_L}$ (Definition A.30)

DEFINES $\bar{W}_{S'} := \sup_{z\in S'} \sum_{i\le N} \Delta_i(z_{<i})^2/\sigma_i(z_{<i})^2$ (Definition A.27)

(L1) $\forall i\ \forall z_{<i}:\ P_i|_{z_{<i}} = \widetilde{B}_i$
[$\widetilde{B}_i$ (the statement; Definition A.28)]

(L2) $\forall i\ \forall z_{<i}:\ Q_i|_{z_{<i}} = Q_i$
[Q_i (Definition A.25, item 2)]

(L3) $\forall k \in \{1,\dots,N\}\ \forall z_{\le k} \in G_k:\ z_{<k} \in G_{k-1}$
[G_k (the proof's block)]

Fact A.45, item 3 at every $i \le N$ and $z_{<i} \in \mathbb{Z}^{i-1}$	This proof
Shared: $N,\ i,\ \alpha$	
μ	Q (Definition A.25)
p	$z_{<i}$
ν	$\widetilde{B}_i$ (the statement)
Y	$\mathcal{Z}_i$ (the statement)
$\mu_i(\cdot \mid p)$	Q_i (L2)
(I1) $N \ge 1$	$N := 2n,\ n \in \{512, 1024\}$ (the statement)
$\mu : \mathbb{Z}^N \to [0,1],\ \sum_{z \in \mathbb{Z}^N} \mu(z) = 1$	Q (Definition A.25)
$i \le N,\ p \in \mathbb{Z}^{i-1}$	The scope
$\mu(p) > 0$	Fact A.45, item 2, at $\mu := Q$; (L2); $Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
$\nu : \mathbb{Z} \to [0,1],\ \sum_{x \in \mathbb{Z}} \nu(x) = 1$	$\widetilde{B}_i$ (Definition A.28)
$Y \subseteq \mathbb{Z}$	$\mathcal{Z}_i$ (Definition A.28)
$\forall x \in Y :\ \mu_i(x \mid p) > 0$	$Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
Its conclusion: $\mathbb{E}_\mu[\mathbf{1}_Y(\nu/\mu_i(\cdot \mid p))^\alpha \mid p] = \sum_{x \in Y} \nu(x)^\alpha \mu_i(x \mid p)^{1-\alpha}$	

(L4) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i}(\widetilde{B}_i/Q_i)^\alpha \mid z_{<i}] = \sum_{x \in \mathcal{Z}_i} \widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha}$

[(I1)]

(L5) $\forall i \le N\ \forall z_{<i} \in G_{i-1} :\ \{x \in \mathbb{Z} : (z_{<i}, x) \in G_i\} \subseteq \mathcal{Z}_i$

[G_k (the proof's block); S (Definition A.26); $\mathcal{Z}_i$ (Definition A.28); $\widetilde{\sigma}_i > 0$ (assumption A1)]

(L6) $\forall i \le N\ \forall z_{<i} \in G_{i-1} :\ \sum_{x \in \mathbb{Z},\ (z_{<i},x) \in G_i} \widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha} \le g_i$

[assumption A3 on $G_{i-1} \subseteq S'_{<i}$ (G_k, the proof's block; $S'_{<i}$, Definition A.26); (L4); (L5); $\widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha} \ge 0$ ($\widetilde{B}_i$, Q_i probability measures)]

(L7) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ B_i > 0$

[B_i (the proof's block; Lemma F.1); $e^t > 0$ (Fact A.41, item 12); $\bar{W}_{\alpha_L} > 0$ (Definition A.30); $\prod_k c_k > 0$ at $c_k > 0$ (Fact A.41, items 12 and 28)]

(L8) $\Rightarrow\ \forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ g_i > 0$

[g_i (Lemma F.1); $\bar{\rho}_B > 0$ (assumption A2); (L7); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28); $\prod_k c_k > 0$ at $c_k > 0$ (Fact A.41, items 12 and 28)]

Lemma E.16 at N	This proof
Shared: $\alpha,\ G_k,\ g_i$	
$P_i(\cdot \mid z_{<i})$	$\widetilde{B}_i$ (L1)
$Q_i(\cdot \mid z_{<i})$	Q_i (L2)
$N \in \mathbb{Z}_{\ge 0}$	$N := 2n,\ n \in \{512, 1024\}$ (the statement)
$P_i(\cdot \mid z_{<i}), Q_i(\cdot \mid z_{<i}) : \mathbb{Z} \to [0,1],\ \sum_{x \in \mathbb{Z}} P_i(x \mid z_{<i}) = 1,\ \sum_{x \in \mathbb{Z}} Q_i(x \mid z_{<i}) = 1$	$\widetilde{B}_i$ (Definition A.28); Q_i (Definition A.25, item 2)
(I2) $G_k \subseteq \mathbb{Z}^k$	G_k (the proof's block)
$g_i : \mathbb{Z}^{i-1} \to (0, \infty)$	(L8)
$(P, Q) := (P, Q)$	(L1), (L2) (Fact A.45, item 1)
$G_N = S'$	G_k (the proof's block) at $k := N$
Assumption A1	$Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
Assumption A2	(L3)
Assumption A3	(L6)
Its conclusion: $\sum_{z \in G_N} P(z)^\alpha Q(z)^{1-\alpha} \le \sup_{z \in G_N} \prod_{i \le N} g_i(z_{<i})$	

(L9) $\sum_{z \in S'} P(z)^\alpha Q(z)^{1-\alpha} \le \sup_{S'} \prod_i g_i$

[(I2)]

(L10) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ g_i = \bar{\rho}_B^{\alpha_L/2} (e^{\bar{\phi}}\, \bar{W}_{\alpha_L})^{1/2} \exp(\alpha_L(\alpha_L - 1)\bar{\theta}_{\alpha_L} \Delta_i^2/(4\sigma_i^2))$

[g_i, B_i (Lemma F.1); $\sqrt{ab} = \sqrt{a}\sqrt{b}$ at $a, b \ge 0$ (Fact A.41, item 13); $(e^x)^{1/2} = e^{x/2}$ (Fact A.41, items 12, 28 and 30)]

(L11) $\forall z \in \mathbb{Z}^N :\ \prod_{i\le N} g_i = (\bar\rho_B^{\alpha_L/2}(e^{\bar\phi}\,\bar W_{\alpha_L})^{1/2})^N \exp(\alpha_L(\alpha_L-1)\bar\theta_{\alpha_L}(\sum_{i\le N}\Delta_i^2/\sigma_i^2)/4)$

[(L10); $e^x e^y = e^{x+y}$ (Fact A.41, item 12); collect]

(L12) $\alpha_L(\alpha_L-1)/4 = \alpha_L(\alpha-1)/2$

[$\alpha_L = 2\alpha - 1$ (the statement); expand]

(L13) $\forall z \in S' :\ \sum_{i\le N}\Delta_i^2/\sigma_i^2 \le \bar W_{S'}$

[$\bar W_{S'}$ (Definition A.27); $a \le \sup A$ (Fact A.41, item 20)]

(L14) $\forall z \in S' :\ \prod_{i\le N} g_i \le (\bar\rho_B^{\alpha_L/2}(e^{\bar\phi}\,\bar W_{\alpha_L})^{1/2})^N \exp(\alpha_L(\alpha-1)\bar\theta_{\alpha_L}\bar W_{S'}/2)$

[(L11), (L12), (L13); $\bar\theta_{\alpha_L} \ge 0$ (Definition A.30); $\alpha_L(\alpha-1) > 0$ ($\alpha_L = 2\alpha-1$, $\alpha > 1$, the statement); $ca \le cb$ (Fact A.41, item 26); exp increasing on $\mathbb{R}$ (Fact A.41, item 5); $\bar\rho_B^{\alpha_L/2}(e^{\bar\phi}\,\bar W_{\alpha_L})^{1/2} > 0$ (assumption A2; $\bar W_{\alpha_L} > 0$, Definition A.30; $y^a > 0$ at $y > 0$, Fact A.41, items 12 and 28)]

(L15) $\Rightarrow\ \sup_{S'}\prod_{i\le N} g_i \le (\bar\rho_B^{\alpha_L/2}(e^{\bar\phi}\,\bar W_{\alpha_L})^{1/2})^N \exp(\alpha_L(\alpha-1)\bar\theta_{\alpha_L}\bar W_{S'}/2)$

[(L14); Fact A.41, item 20]

(L16) $\Rightarrow\ \sum_{z\in S'} P(z)^\alpha Q(z)^{1-\alpha} \le (\bar\rho_B^{\alpha_L/2}(e^{\bar\phi}\,\bar W_{\alpha_L})^{1/2})^N \exp(\alpha_L(\alpha-1)\bar\theta_{\alpha_L}\bar W_{S'}/2)$

[(L9), (L15)]

(L17) $\Rightarrow\ \sum_{z\in S'} P^\alpha Q^{1-\alpha} \le R^{\alpha-1}$

[(L16); R (Definition A.30); multiply the exponents]

(L18) $\Rightarrow$ the statement

[(L17)]

□

Lemma F.3 (Divergence of the conditioned measures [to table])**.** *Conditioning two probability measures on an event keeps the divergence within their Rényi divergence on it, times* $(1 - P(S'^c))^{-\alpha/(\alpha-1)}$*. Let:*

- $\alpha > 1$*, an order;*
- $N \in \mathbb{Z}_{>0}$*;*
- P*, a probability measure on* $\mathbb{Z}^N$*;*
- Q*, a probability measure on* $\mathbb{Z}^N$*;*
- $S' \subseteq \mathbb{Z}^N$*;*
- $R' \ge 0$*.*

Define:

- $S'^c := \mathbb{Z}^N \setminus S'$*;*
- $P_{S'}(A) := P(A \cap S')/P(S')$ *for* $A \subseteq \mathbb{Z}^N$*;*
- $Q_{S'}(A) := Q(A \cap S')/Q(S')$*.*

Assume:

(A1) $P(S') > 0$*;*

(A2) $Q(S') > 0$*;*

(A3) $\sum_{z\in S'} P(z)^\alpha Q(z)^{1-\alpha} \le R'^{\alpha-1}$*.*

Then

$$R_\alpha(P_{S'} \,\|\, Q_{S'}) \le R' \,(1 - P(S'^c))^{-\alpha/(\alpha-1)}.$$

Proof. (L1) $R_\alpha(P_{S'}\|Q_{S'})^{\alpha-1} = Q(S')^{\alpha-1}P(S')^{-\alpha}\sum_{z\in S'} P^\alpha Q^{1-\alpha}$

[Fact A.45, item 10, at $(\mu,\nu,B) := (P,Q,S')$; $P(S'), Q(S') > 0$ (assumptions A1, A2)]

(L2) $\Rightarrow\ R_\alpha(P_{S'}\|Q_{S'})^{\alpha-1} \le Q(S')^{\alpha-1}P(S')^{-\alpha}R'^{\alpha-1}$

[(L1); assumption A3 multiplied by $Q(S')^{\alpha-1}P(S')^{-\alpha} \ge 0$]

(L3) $\Rightarrow\ R_\alpha(P_{S'}\|Q_{S'}) \le R' \,(1 - P(S'^c))^{-\alpha/(\alpha-1)}$

[$(\alpha-1)$-th root at $R' \ge 0$ (the statement); $Q(S') \le 1$ (Q, the statement; Fact A.45, item 12); $P(S') \ge 1 - P(S'^c)$ (Fact A.45, item 5)]

(L4) $\Rightarrow$ the statement

[(L3)]

□

Theorem F.4 (The divergence on a sub-event of the tail-cut event [to table])**.** *The signer in $\mathcal{F}$ stays within the factor R of the signer over $\mathbb{R}$ on a sub-event of the tail-cut event. Define:*

- $S'^c := \mathbb{Z}^N \setminus S'$ *(Definition A.26);*
- $P_{S'}(A) := P(A \cap S')/P(S')$ *for* $A \subseteq \mathbb{Z}^N$*;*
- $Q_{S'}(A) := Q(A \cap S')/Q(S')$*;*
- $\bar{\rho}_B := \max_{i \le N} \sup_{z_{<i} \in S_{<i}} R_{2\alpha}^{\mathcal{Z}_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)$*, with* $\widetilde{D}_i := D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$ *(Definition A.28 at* $C_i := \emptyset$*).*

Assume:

(A1) $(1+\bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$*;*
(A2) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i > 0$*;*
(A3) $\bar{\rho}_B > 0$*;*
(A4) $P(S') > 0$*;*
(A5) $Q(S') > 0$*.*

Then

$$R_\alpha(P_{S'} \,\|\, Q_{S'}) \le R\,(1 - P(S'^c))^{-\alpha/(\alpha-1)}.$$

Proof.

DEFINES $S'_{<i} := \{\, z_{<i} : z \in S' \,\}$ for $i \le N$ (Definition A.26)
DEFINES $Q_i := D_{\mathbb{Z},\sigma_i,t_i}$ for $i \le N$ and every $z_{<i}$ (Definition A.25, item 2)
DEFINES $\widetilde{B}_i := B^{\mathcal{F}}_{\widetilde{\sigma}_i(z_{\lesssim i}),\widetilde{t}_i(z_{<i})}$ (Definition A.28)
DEFINES $\mathcal{Z}_i := (|\cdot - \widetilde{t}_i|/\widetilde{\sigma}_i)^{-1}([0,\tau]) \subseteq \mathbb{Z}$ (Definition A.28)
DEFINES $B_i := e^{\bar{\phi}}\, \bar{W}_{\alpha_L} \exp(\alpha_L(\alpha_L - 1)\bar{\theta}_{\alpha_L}\Delta_i^2/(2\sigma_i^2))$ (Lemma F.1)
DEFINES $g_i := \bar{\rho}_B^{-\alpha_L/2} B_i^{1/2}$ (Lemma F.1)

	Lemma F.1 at every $i \le N$ and $z_{<i} \in S'_{<i}$	This proof
(I1)	Shared: $\alpha,\ \tau,\ \bar{\phi},\ S',\ S'_{<i},\ Q_i,\ \widetilde{B}_i,\ \mathcal{Z}_i,\ \bar{\rho}_B,\ \bar{W}_{\alpha_L}$ (Definition A.30), $\bar{\theta}_{\alpha_L}$ (Definition A.30), $B_i,\ g_i$ Shared: $n \in \{512, 1024\},\ N := 2n,\ \alpha > 1,\ \tau > 1,\ S' \subseteq S,\ \alpha_L := 2\alpha - 1$ Shared: assumptions A1, A2	
	Its conclusion: $\mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i}(\widetilde{B}_i/Q_i)^\alpha \,|\, z_{<i}] \le g_i$	
(L1)	$\forall i \le N\ \forall z_{<i} \in S'_{<i} :\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i}(\widetilde{B}_i/Q_i)^\alpha \,|\, z_{<i}] \le g_i$	[(I1)]

	Lemma F.2	This proof
(I2)	Shared: $\alpha,\ \tau,\ \bar{\phi},\ S',\ P,\ Q,\ R,\ \bar{\rho}_B,\ Q_i,\ \widetilde{B}_i,\ \mathcal{Z}_i,\ g_i$ Shared: $n \in \{512, 1024\},\ N := 2n,\ \alpha > 1,\ \tau > 1,\ S' \subseteq S,\ \alpha_L := 2\alpha - 1$	
	Assumption A1 Assumption A2 Assumption A3	Assumption A2 Assumption A3 (L1)
	Its conclusion: $\sum_{z \in S'} P(z)^\alpha Q(z)^{1-\alpha} \le R^{\alpha-1}$	
(L2)	$\sum_{z \in S'} P(z)^\alpha Q(z)^{1-\alpha} \le R^{\alpha-1}$	[(I2)]
(L3)	$R \ge 0$	[R, $\bar{\rho}_B$, $\bar{W}_{\alpha_L}$ (Definition A.30); Fact A.41, items 5 and 12]

	Lemma F.3	This proof
	Shared: α, N, P, Q, S', S'^c, $P_{S'}$, $Q_{S'}$	
(I3)	R' $N \in \mathbb{Z}_{>0}$ $P, Q : \mathbb{Z}^N \to [0,1]$, $\sum_{z\in\mathbb{Z}^N} P(z) = 1$, $\sum_{z\in\mathbb{Z}^N} Q(z) = 1$ $S' \subseteq \mathbb{Z}^N$ $R' \geq 0$	R (the statement) $N := 2n$, $n \in \{512, 1024\}$ (the statement) P, Q (Definition A.25) S' (Definition A.26) (L3)
	Assumption A1 Assumption A2 Assumption A3	Assumption A4 Assumption A5 (L2)
	Its conclusion: $R_\alpha(P_{S'} \,\|\, Q_{S'}) \leq R' \,(1 - P(S'^c))^{-\alpha/(\alpha-1)}$	

(L4) $R_\alpha(P_{S'} \| Q_{S'}) \leq R\,(1 - P(S'^c))^{-\alpha/(\alpha-1)}$

[(I3)]

(L5) $\Rightarrow$ the statement

[(L4)]

□

Corollary F.5 (The four leading terms of the divergence factor [to table])**.** *At the admissible choices $\bar{W}_{\alpha_L}(\bar{\delta})$ and $\bar{\theta}_{\alpha_L}(\bar{\delta})$, $\ln R$ is the base sampler's term, the normalizer term, $N\alpha_L\bar{\delta}^2$ up to a remainder, and the center term. Let:*

- $N \in \mathbb{Z}_{>0}$;
- $\bar{\rho}_B > 0$;
- $\bar{\phi} \in \mathbb{R}$;
- $\bar{W}_{S'} \in \mathbb{R}$;
- $\bar{\delta} \geq 0$.

Define:

- $a := \alpha_L - 1$;
- $\bar{x} := 2\bar{\delta} + \bar{\delta}^2$;
- $r := \left((a\bar{x})^3/(1 - a\bar{x}) + a\bar{x}^3/(1 - \bar{x})\right)/6$;
- $\bar{W}_{\alpha_L}(\bar{\delta}) := \exp\left(a(a+1)\bar{\delta}^2(1 + \bar{\delta}/2)^2 + r\right)$;
- $\bar{\theta}_{\alpha_L}(\bar{\delta}) := 1/(1 - a\bar{x})$;
- $\theta_{\alpha_L}(\delta) := 1/(\alpha_L + (1 - \alpha_L)(1 + \delta)^2)$ *(Definition A.30)*;
- $R := R_B R_\sigma R_t$, *with* $R_B := \bar{\rho}_B^{-\alpha_L N/(2(\alpha-1))}$ *(Definition A.30)*;
- $R_\sigma := (e^{\bar{\phi}}\,\bar{W}_{\alpha_L}(\bar{\delta}))^{N/(2(\alpha-1))}$ *and* $R_t := \exp(\alpha_L\,\bar{\theta}_{\alpha_L}(\bar{\delta})\,\bar{W}_{S'}/2)$ *(Definition A.30 at* $\bar{W}_{\alpha_L} := \bar{W}_{\alpha_L}(\bar{\delta})$ *and* $\bar{\theta}_{\alpha_L} := \bar{\theta}_{\alpha_L}(\bar{\delta})$*).*

Assume:

(A1) $a\bar{x} < 1$;

(A2) $\bar{x} < 1$.

Then $\bar{\theta}_{\alpha_L}(\bar{\delta})$ and $\bar{W}_{\alpha_L}(\bar{\delta})$ are admissible in Definition A.30, and $\ln R$ is the sum of the four terms:

1. $\forall \delta > -1,\ |\delta| \leq \bar{\delta}:\ \theta_{\alpha_L}(\delta) \leq \bar{\theta}_{\alpha_L}(\bar{\delta})$;
2. $\forall \delta > -1,\ |\delta| \leq \bar{\delta}:\ \theta_{\alpha_L}(\delta)^{1/2}(1 + \delta)^{1-\alpha_L} \leq \bar{W}_{\alpha_L}(\bar{\delta})$;
3. $\ln R = \frac{N}{\alpha-1}\left(\frac{\alpha_L}{2}\ln\bar{\rho}_B + \frac{\bar{\phi}}{2}\right) + N\alpha_L\bar{\delta}^2(1 + \bar{\delta}/2)^2 + \frac{N}{2(\alpha-1)}\,r + \frac{\alpha_L}{2}\,\bar{\theta}_{\alpha_L}(\bar{\delta})\bar{W}_{S'}$.

Proof.

DEFINES $D := \{\delta \in \mathbb{R} : \delta > -1,\ |\delta| \leq \bar{\delta}\}$

DEFINES $x(\delta) := 2\delta + \delta^2$ for $\delta \in D$

Proof of item 1.

(L1) $\forall \delta \in D:\ (1+\delta)^2 = 1 + x(\delta)$

[x (the proof's block); expand]

(L2) $\forall \delta \in D:\ \alpha_L + (1-\alpha_L)(1+\delta)^2 = 1 - a\,x(\delta)$

[(L1); a (the statement); expand]

(L3) $\forall \delta \in D:\ |x(\delta)| \le 2|\delta| + \delta^2$

[x (the proof's block); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$]

(L4) $\forall \delta \in D:\ 2|\delta| + \delta^2 \le \bar{x}$

[$|\delta| \le \bar{\delta}$ (D, the proof's block); $t \mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5); $\bar{x}$ (the statement)]

(L5) $\Rightarrow\ \forall \delta \in D:\ |x(\delta)| \le \bar{x}$

[(L3), (L4)]

(L6) $a > 0$

[$a = 2\alpha - 2$ (α_L, a, the statement); $\alpha > 1$ (the statement)]

(L7) $\forall \delta \in D:\ a\,x(\delta) \le a\bar{x}$

[(L5), (L6); Fact A.41, item 26]

(L8) $1 - a\bar{x} > 0$

[assumption A1]

(L9) $\forall \delta \in D:\ 1 - a\,x(\delta) \ge 1 - a\bar{x}$

[(L7)]

(L10) $\Rightarrow\ \forall \delta \in D:\ 1 - a\,x(\delta) > 0$

[(L8), (L9)]

(L11) $\Rightarrow\ \forall \delta \in D:\ \theta_{\alpha_L}(\delta) = 1/(1 - a\,x(\delta))$

[θ_{α_L} (Definition A.30); (L2), (L10)]

(L12) $\Rightarrow\ \forall \delta \in D:\ \theta_{\alpha_L}(\delta) \le \bar{\theta}_{\alpha_L}(\bar{\delta})$

[(L11), (L9), (L8); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5); $\bar{\theta}_{\alpha_L}(\bar{\delta})$ (the statement)]

(L13) $\Rightarrow$ item 1

[(L12); D (the proof's block)]

□ (item 1)

Proof of item 2.

(L14) $\forall \delta \in D:\ \theta_{\alpha_L}(\delta) > 0$

[(L11), (L10)]

(L15) $\forall \delta \in D:\ 1 + \delta > 0$

[$\delta > -1$ (D, the proof's block)]

(L16) $\forall \delta \in D:\ \ln\left(\theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L}\right) = \frac{1}{2}\left(-\ln(1 - a\,x(\delta)) - a\ln(1 + x(\delta))\right)$

[(L11), (L14), (L15), (L1); $1 - \alpha_L = -a$ (a, the statement); $\ln(st) = \ln s + \ln t$ at $s, t > 0$ (Fact A.41, item 29); $\ln(y^b) = b \ln y$ at $y > 0$ (Fact A.41, item 12)]

(L17) $\forall \delta \in D:\ |a\,x(\delta)| < 1$

[(L5), (L6); assumption A1]

(L18) $\forall \delta \in D:\ |x(\delta)| < 1$

[(L5); assumption A2]

(I1)

Fact A.41, item 31 at every $\delta \in D$	This proof
y	$-a\,x(\delta)$ (the statement; the proof's block)
$y \in (-1, 1)$	(L17)
Its conclusion: $\ln(1+y) = \sum_{k\ge1}(-1)^{k+1}y^k/k$	

(L19) $\forall \delta \in D:\ \ln(1 + (-a\,x(\delta))) = \sum_{k\ge1}(-1)^{k+1}(-a\,x(\delta))^k/k$

[(I1)]

(L20) $\forall \delta \in D:\ -\ln(1 - a\,x(\delta)) = \sum_{k\ge1}(a\,x(\delta))^k/k$

[(L19); expand]

	Fact A.41, item 31 at every $\delta \in D$	This proof
(I2)	y $y \in (-1,1)$	$x(\delta)$ (the proof's block) (L18)
	Its conclusion: $\ln(1+y) = \sum_{k\geq 1}(-1)^{k+1}y^k/k$	

(L21) $\forall \delta \in D:\ \ln(1+x(\delta)) = \sum_{k\geq 1}(-1)^{k+1}x(\delta)^k/k$

[(I2)]

(L22) $\forall \delta \in D:\ -a\ln(1+x(\delta)) = \sum_{k\geq 1}(-1)^k a\,x(\delta)^k/k$

[(L21); expand]

(L23) $\forall \delta \in D:\ \sum_{k\geq 1}(a\,x(\delta))^k/k + \sum_{k\geq 1}(-1)^k a\,x(\delta)^k/k = (a\,x(\delta) - a\,x(\delta)) + (a^2x(\delta)^2/2 + a\,x(\delta)^2/2) + \sum_{k\geq 3}(a^k + (-1)^k a)\,x(\delta)^k/k$

[(L17), (L18), (L20), (L22); expand]

(L24) $\forall \delta \in D:\ (a\,x(\delta) - a\,x(\delta)) + (a^2x(\delta)^2/2 + a\,x(\delta)^2/2) = \frac{a(a+1)}{2}\,x(\delta)^2$

[expand]

(L25) $\Rightarrow\ \forall \delta \in D:\ -\ln(1-a\,x(\delta)) - a\ln(1+x(\delta)) = \frac{a(a+1)}{2}\,x(\delta)^2 + \sum_{k\geq 3}(a^k + (-1)^k a)\,x(\delta)^k/k$

[(L20), (L22), (L23), (L24)]

(L26) $\forall \delta \in D:\ \sum_{k\geq 3}(a^k + (-1)^k a)\,x(\delta)^k/k \leq \frac{1}{3}\sum_{k\geq 3}\left((a|x(\delta)|)^k + a|x(\delta)|^k\right)$

[(L6); at $k \geq 3$: $(a^k + (-1)^k a)\,x(\delta)^k/k \leq (a^k + a)|x(\delta)|^k/3$ (Fact A.41, item 1)]

	Fact A.41, item 32 at every $\delta \in D$	This proof
(I3)	p $p \in [0,1)$	$a|x(\delta)|$ (the statement; the proof's block) (L17), (L6)
	Its conclusion: $\sum_{k\geq 3} p^k = p^3/(1-p)$	

(L27) $\forall \delta \in D:\ \sum_{k\geq 3}(a|x(\delta)|)^k = (a|x(\delta)|)^3/(1-a|x(\delta)|)$

[(I3)]

	Fact A.41, item 32 at every $\delta \in D$	This proof
(I4)	p $p \in [0,1)$	$|x(\delta)|$ (the proof's block) (L18)
	Its conclusion: $\sum_{k\geq 3} p^k = p^3/(1-p)$	

(L28) $\forall \delta \in D:\ \sum_{k\geq 3}|x(\delta)|^k = |x(\delta)|^3/(1-|x(\delta)|)$

[(I4)]

(L29) $\forall \delta \in D:\ (a|x(\delta)|)^3/(1-a|x(\delta)|) \leq (a\bar{x})^3/(1-a\bar{x})$

[(L5), (L6), (L8); $t \mapsto t^3$ nondecreasing on $[0,\infty)$, $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5); Fact A.41, item 8]

(L30) $\forall \delta \in D:\ a|x(\delta)|^3/(1-|x(\delta)|) \leq a\bar{x}^3/(1-\bar{x})$

[(L5), (L6); assumption A2; $t \mapsto t^3$ nondecreasing on $[0,\infty)$, $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5); Fact A.41, item 8]

(L31) $\Rightarrow\ \forall \delta \in D:\ \sum_{k\geq 3}(a^k + (-1)^k a)\,x(\delta)^k/k \leq 2r$

[(L26), (L27), (L28), (L29), (L30); r (the statement)]

(L32) $\forall \delta \in D:\ x(\delta)^2 \leq \bar{x}^2$

[(L5); $t \mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L33) $\Rightarrow\ \forall \delta \in D:\ \ln\left(\theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L}\right) \leq \frac{1}{2}\left(\frac{a(a+1)}{2}\,\bar{x}^2 + 2r\right)$

[(L16), (L25), (L31), (L32); $a(a+1) > 0$ (L6)]

(L34) $\bar{x}^2 = 4\bar{\delta}^2(1+\bar{\delta}/2)^2$

[$\bar{x}$ (the statement); expand]

(L35) $\frac{1}{2}\left(\frac{a(a+1)}{2}\,\bar{x}^2 + 2r\right) = a(a+1)\bar{\delta}^2(1+\bar{\delta}/2)^2 + r$

[(L34); expand]

(L36) $a(a+1)\bar{\delta}^2(1+\bar{\delta}/2)^2 + r = \ln \bar{W}_{\alpha_L}(\bar{\delta})$

[$\bar{W}_{\alpha_L}(\bar{\delta})$ (the statement); $\ln e^t = t$ (Fact A.41, item 30)]

(L37) $\Rightarrow\ \forall\delta\in D:\ \ln\left(\theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L}\right)\le\ln\bar{W}_{\alpha_L}(\bar{\delta})$

[(L33), (L35), (L36)]

(L38) $\Rightarrow\ \forall\delta\in D:\ \theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L}\le\bar{W}_{\alpha_L}(\bar{\delta})$

[(L37); exp increasing on $\mathbb{R}$ (Fact A.41, item 5); $e^{\ln y}=y$ at $y>0$ (Fact A.41, item 28), (L14), (L15)]

(L39) $\Rightarrow$ item 2

[(L38); D (the proof's block)]

□ (item 2)

Proof of item 3.

(L40) $\bar{\theta}_{\alpha_L}(\bar{\delta})>0$

[(L8); $\bar{\theta}_{\alpha_L}(\bar{\delta})$ (the statement)]

(L41) $\bar{W}_{\alpha_L}(\bar{\delta})>0$

[$\bar{W}_{\alpha_L}(\bar{\delta})$ (the statement); $e^t>0$ (Fact A.41, item 12)]

(I5)

Definition A.30	This proof
Shared: $\alpha,\ \alpha_L,\ N,\ \bar{\rho}_B,\ \bar{\phi},\ \bar{W}_{S'},\ \bar{\delta},\ \theta_{\alpha_L},\ R_B,\ R_\sigma,\ R_t,\ R$	
Shared: $N\in\mathbb{Z}_{>0},\ \alpha>1,\ \alpha_L:=2\alpha-1$	
$\bar{\theta}_{\alpha_L}$	$\bar{\theta}_{\alpha_L}(\bar{\delta})$ (the statement)
$\bar{W}_{\alpha_L}$	$\bar{W}_{\alpha_L}(\bar{\delta})$ (the statement)
$\bar{\theta}_{\alpha_L}\ge 0$	(L40)
$\forall\delta>-1,\ \lvert\delta\rvert\le\bar{\delta}:\ \theta_{\alpha_L}(\delta)\le\bar{\theta}_{\alpha_L}$	(L13)
$\bar{W}_{\alpha_L}>0$	(L41)
$\forall\delta>-1,\ \lvert\delta\rvert\le\bar{\delta}:$ $\theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L}\le\bar{W}_{\alpha_L}$	(L39)
Its conclusion: $R:=R_BR_\sigma R_t$	

(L42) $R=R_BR_\sigma R_t$

[(I5)]

(L43) $\ln R=\ln R_B+\ln R_\sigma+\ln R_t$

[(L42); $R_B,R_\sigma,R_t>0$ ($\bar{\rho}_B>0$, $\bar{W}_{\alpha_L}(\bar{\delta})>0$, the statement; Fact A.41, item 12); $\ln(st)=\ln s+\ln t$ (Fact A.41, item 29)]

(L44) $\ln R_B=\frac{\alpha_L N}{2(\alpha-1)}\ln\bar{\rho}_B$

[R_B (Definition A.30); $\bar{\rho}_B>0$ (the statement); $\ln(y^b)=b\ln y$ (Fact A.41, item 12)]

(L45) $\ln R_\sigma=\frac{N}{2(\alpha-1)}\left(\bar{\phi}+\ln\bar{W}_{\alpha_L}(\bar{\delta})\right)$

[R_σ (Definition A.30); $\ln(y^b)=b\ln y$ (Fact A.41, item 12); $\ln(st)=\ln s+\ln t$ (Fact A.41, item 29); $\ln e^t=t$ (Fact A.41, item 30)]

(L46) $\ln R_t=\frac{\alpha_L}{2}\bar{\theta}_{\alpha_L}(\bar{\delta})\bar{W}_{S'}$

[R_t (Definition A.30) at $\bar{\theta}_{\alpha_L}:=\bar{\theta}_{\alpha_L}(\bar{\delta})$; α_L (the statement); $\ln e^t=t$ (Fact A.41, item 30)]

(L47) $a(a+1)=(\alpha_L-1)\alpha_L$

[a, α_L (the statement)]

(L48) $\frac{N}{2(\alpha-1)}\,a(a+1)\bar{\delta}^2(1+\bar{\delta}/2)^2=N\alpha_L\bar{\delta}^2(1+\bar{\delta}/2)^2$

[(L47); α_L (the statement); expand]

(L49) $\frac{N}{2(\alpha-1)}\ln\bar{W}_{\alpha_L}(\bar{\delta})=N\alpha_L\bar{\delta}^2(1+\bar{\delta}/2)^2+\frac{N}{2(\alpha-1)}\,r$

[(L36), (L48)]

(L50) $\Rightarrow\ \ln R=\frac{N}{\alpha-1}\left(\frac{\alpha_L}{2}\ln\bar{\rho}_B+\frac{\bar{\phi}}{2}\right)+N\alpha_L\bar{\delta}^2(1+\bar{\delta}/2)^2+\frac{N}{2(\alpha-1)}\,r+\frac{\alpha_L}{2}\,\bar{\theta}_{\alpha_L}(\bar{\delta})\bar{W}_{S'}$

[(L43), (L44), (L45), (L46), (L49); α_L (the statement)]

(L51) $\Rightarrow$ item 3

[(L50)]

□ (item 3)

The terms at a Falcon-type signer. At a Falcon-type signer, $\bar{\delta}$ and $\bar{W}_{S'}$ are bounded by Lemma 4.7, item 2, and Lemma 4.9, item 3, $\bar{\delta}$ of the order of u and ζ and $\bar{W}_{S'}$ of the order of their squares; the term in $\bar{\rho}_B$ is the base sampler's (Corollary 4.10, precondition 1). At the fixed-point signer, the four terms at the tail's W^{tail} and the corollary's terms are Table 35 (Appendix I.7).

Theorem 1.1 (*The divergence bound with four explicit terms [to table]*) [to statement].

The signer in $\mathcal{F}$ stays within the factor R of the signer over $\mathbb{R}$ on a sub-event of the tail-cut event, $\ln R$ the sum of four explicit terms. Define:

- $S := \{\, z \in \mathbb{Z}^N : \forall i \le N \ |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$, *the tail-cut event.*

Let:

- $S' \subseteq S$, *an event.*

Define:

- *The sub-event*
  - $S'^c := \mathbb{Z}^N \setminus S'$;
- *The prefix sets*
  - $S_{<i} := \{\, z_{<i} : z \in S \,\}$ *for* $i \le N$;
- *The conditional probability measures*
  - $P_{S'}(A) := P(A \cap S')/P(S')$ *for* $A \subseteq \mathbb{Z}^N$;
  - $Q_{S'}(A) := Q(A \cap S')/Q(S')$;
- *The leaf measures*
  - $\widetilde{B}_i(A) := P(z_i \in A \mid z_{<i})$ *for* $i \le N$, $z_{<i} \in S_{<i}$ *and* $A \subseteq \mathbb{Z}$, *the base sampler's conditional probability measure at leaf* i;
  - $\widetilde{D}_i := D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$, *the discrete Gaussian at the computed parameters;*
- *The tail cut*
  - $\mathcal{Z}_i := \{\, z_i \in \mathbb{Z} : |z_i - \widetilde{t}_i| \le \tau\, \widetilde{\sigma}_i \,\}$;
- *The moments*
  - $\bar{\rho}_B := \max_{i \le N} \ \sup_{z_{<i} \in S_{<i}} \left(\sum_{z_i \in \mathcal{Z}_i} \widetilde{B}_i(z_i)^{2\alpha}\, \widetilde{D}_i(z_i)^{1-2\alpha} \right)^{1/(2\alpha-1)}$;
- *The terms*
  - $\bar{x} := 2\bar{\delta} + \bar{\delta}^2$;
  - $r := \left(((\alpha_L - 1)\bar{x})^3/(1 - (\alpha_L - 1)\bar{x}) + (\alpha_L - 1)\bar{x}^3/(1 - \bar{x}) \right)/6$;
  - $\bar{\theta}_{\alpha_L}(\bar{\delta}) := 1/(1 - (\alpha_L - 1)\bar{x})$;
  - $R := \exp\left(\frac{N}{\alpha - 1} \left(\frac{\alpha_L}{2} \ln \bar{\rho}_B + \frac{\bar{\phi}}{2} \right) + N\alpha_L \bar{\delta}^2 (1 + \bar{\delta}/2)^2 + \frac{N}{2(\alpha-1)}\, r + \frac{\alpha_L}{2}\, \bar{\theta}_{\alpha_L}(\bar{\delta}) \bar{W}_{S'} \right)$.

Assume:

(A1) $(1 + \bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$;
(A2) $\bar{x} < 1$;
(A3) $\forall i \le N \ \forall z_{<i} \in \mathbb{Z}^{i-1} : \ \widetilde{\sigma}_i > 0$;
(A4) $\bar{\rho}_B > 0$;
(A5) $P(S') > 0$;
(A6) $Q(S') > 0$.

Then

$$R_\alpha(P_{S'} \,\|\, Q_{S'}) \le R\,(1 - P(S'^c))^{-\alpha/(\alpha-1)}.$$

Proof.

DEFINES $\bar{W}_{\alpha_L}(\bar{\delta}) := \exp(a(a+1)\bar{\delta}^2(1 + \bar{\delta}/2)^2 + r)$, $a := \alpha_L - 1$ (Corollary F.5)
DEFINES $\theta_{\alpha_L}(\delta) := 1/(\alpha_L + (1 - \alpha_L)(1 + \delta)^2)$ (Definition A.30)
DEFINES R_{full}, that of Definition A.30 at the statement's α, $\bar{\phi}$ and S', $\bar{W}_{\alpha_L} := \bar{W}_{\alpha_L}(\bar{\delta})$ and $\bar{\theta}_{\alpha_L} := \bar{\theta}_{\alpha_L}(\bar{\delta})$

(L1) $S' \ne \emptyset$

[assumption A5; $P(\emptyset) = 0$ (Fact A.45, item 12)]

(L2) $\alpha_L - 1 = 2\alpha - 2$

[α_L (the statement)]

(L3) $2\alpha - 2 > 0$

[$\alpha > 1$ (the statement)]

(L4) $(\alpha_L - 1)(1 + \bar{\delta})^2 < \alpha_L$

[assumption A1, multiplied by $\alpha_L - 1 > 0$ ((L2), (L3))]

(L5) $(1 + \bar{\delta})^2 = 1 + \bar{x}$

[$\bar{x}$ (the statement); expand]

(L6) $\Rightarrow\ (\alpha_L - 1)(1 + \bar{x}) < \alpha_L$

[(L4), (L5)]

(L7) $\Rightarrow\ (\alpha_L - 1)\bar{x} < 1$

[(L6); expand; subtract]

(L8) $N \in \mathbb{Z}_{>0}$

[$N := 2n$ (the statement); $n \in \{512, 1024\}$ (Definition A.25)]

(L9) $\bar{\delta} \geq 0$

[(L1); $\bar{\delta}$ (the statement; Definition A.27); $S'_{<i}$ (Definition A.26); $|x| \geq 0$ (Fact A.41, item 1); $a \leq \max A$, $a \leq \sup A$ (Fact A.41, item 20)]

(L10) $\bar{W}_{S'} \in \mathbb{R}$

[(L1); $\bar{W}_{S'}$ (the statement; Definition A.27); $S' \subseteq S$ (Definition A.26); S (Definition A.26)]

Corollary F.5	This proof
Shared: $\alpha,\ N,\ \bar{\rho}_B,\ \bar{\phi},\ \bar{W}_{S'},\ \bar{\delta},\ \bar{x},\ r,\ \bar{W}_{\alpha_L}(\bar{\delta}),\ \bar{\theta}_{\alpha_L}(\bar{\delta}),\ \theta_{\alpha_L}$	
Shared: $\alpha > 1,\ \alpha_L := 2\alpha - 1,\ \bar{\phi} \in \mathbb{R}$	
a	$\alpha_L - 1$ (the statement)
R	R_{full} (the proof's block)
$N \in \mathbb{Z}_{>0}$	(L8)
$\bar{\rho}_B > 0$	Assumption A4
(I1) $\bar{W}_{S'} \in \mathbb{R}$	(L10)
$\bar{\delta} \geq 0$	(L9)
Assumption A1	(L7)
Assumption A2	Assumption A2
Its item 1: $\forall \delta > -1,\ \lvert\delta\rvert \leq \bar{\delta} :\ \theta_{\alpha_L}(\delta) \leq \bar{\theta}_{\alpha_L}(\bar{\delta})$	
Its item 2: $\forall \delta > -1,\ \lvert\delta\rvert \leq \bar{\delta} :\ \theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \leq \bar{W}_{\alpha_L}(\bar{\delta})$	
Its item 3: $\ln R = \frac{N}{\alpha-1}\left(\frac{\alpha_L}{2}\ln\bar{\rho}_B + \frac{\bar{\phi}}{2}\right) + N\alpha_L\bar{\delta}^2(1+\bar{\delta}/2)^2 + \frac{N}{2(\alpha-1)}r + \frac{\alpha_L}{2}\bar{\theta}_{\alpha_L}(\bar{\delta})\bar{W}_{S'}$	

(L11) $\forall \delta > -1,\ \lvert\delta\rvert \leq \bar{\delta} :\ \theta_{\alpha_L}(\delta) \leq \bar{\theta}_{\alpha_L}(\bar{\delta})$

[item 1 of (I1)]

(L12) $\forall \delta > -1,\ \lvert\delta\rvert \leq \bar{\delta} :\ \theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \leq \bar{W}_{\alpha_L}(\bar{\delta})$

[item 2 of (I1)]

(L13) $\bar{\theta}_{\alpha_L}(\bar{\delta}) > 0$

[(L7); $\bar{\theta}_{\alpha_L}(\bar{\delta})$ (the statement)]

(L14) $\bar{W}_{\alpha_L}(\bar{\delta}) > 0$

[$\bar{W}_{\alpha_L}(\bar{\delta})$ (the proof's block); $e^t > 0$ (Fact A.41, item 12)]

(L15) $\ln R_{\text{full}} = \frac{N}{\alpha-1}\left(\frac{\alpha_L}{2}\ln\bar{\rho}_B + \frac{\bar{\phi}}{2}\right) + N\alpha_L\bar{\delta}^2(1+\bar{\delta}/2)^2 + \frac{N}{2(\alpha-1)}r + \frac{\alpha_L}{2}\bar{\theta}_{\alpha_L}(\bar{\delta})\bar{W}_{S'}$

[item 3 of (I1)]

(L16) $R_{\text{full}} > 0$

[assumption A4, (L14); R_{full} (the proof's block); R, R_B, R_σ, R_t (Definition A.30); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28); $e^t > 0$ (Fact A.41, item 12)]

(L17) $R_{\text{full}} = e^{\ln R_{\text{full}}}$

[(L16); $e^{\ln y} = y$ at $y > 0$ (Fact A.41, item 28)]

(L18) $\Rightarrow\ R_{\text{full}} = R$

[(L17), (L15); R (the statement)]

	Theorem F.4	This proof
	Shared: $\alpha,\ \tau,\ \bar{\phi},\ S',\ P,\ Q,\ S'^c,\ P_{S'},\ Q_{S'},\ \bar{\rho}_B$	
	Shared: $n \in \{512, 1024\},\ N := 2n,\ \alpha > 1,\ \tau > 1,\ S' \subseteq S,\ \alpha_L := 2\alpha - 1$	
	$\bar{W}_{\alpha_L}$	$\bar{W}_{\alpha_L}(\bar{\delta})$ (the proof's block)
	$\bar{\theta}_{\alpha_L}$	$\bar{\theta}_{\alpha_L}(\bar{\delta})$ (the statement)
	R	R (L18)
	$\bar{\theta}_{\alpha_L} \geq 0$	(L13)
	$\forall \delta > -1,\ \lvert\delta\rvert \leq \bar{\delta}:\ \theta_{\alpha_L}(\delta) \leq \bar{\theta}_{\alpha_L}$	(L11)
(I2)	$\bar{W}_{\alpha_L} > 0$	(L14)
	$\forall \delta > -1,\ \lvert\delta\rvert \leq \bar{\delta}:$ $\theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \leq \bar{W}_{\alpha_L}$	(L12)
	Assumption A1	Assumption A1
	Assumption A2	Assumption A3
	Assumption A3	Assumption A4
	Assumption A4	Assumption A5
	Assumption A5	Assumption A6
	Its conclusion: $R_\alpha(P_{S'} \,\|\, Q_{S'}) \leq R\,(1 - P(S'^c))^{-\alpha/(\alpha-1)}$	

(L19) $R_\alpha(P_{S'} \| Q_{S'}) \leq R\,(1 - P(S'^c))^{-\alpha/(\alpha-1)}$

[(I2)]

(L20) $\Rightarrow$ the statement

[(L19)]

□

Theorem 4.4 (*The divergence bound with fringe sets* [to table]) [to statement].

Where the fringe sets are not empty, the signer in $\mathcal{F}$ stays within the factor R of the signer over $\mathbb{R}$ on the core class of a sub-event of the tail-cut event, and a fringe leaf costs κ_C in a class's Rényi divergence to the power $\alpha - 1$ and $\bar{p}_C$ in mass. Define:

- $\mathcal{K}(z) := \{\, i \leq N : z_i \in C_i(z_{<i}) \,\}$ *(Definition A.26);*
- $S'_k := \{\, z \in S' : |\mathcal{K}(z)| = k \,\}$ *for $k \leq N$ (Definition A.26);*
- $R_\alpha^{S'_k}(P \,\|\, Q)$, *that of Definition A.28 at $\mathcal{Y} := S'_k$;*
- $P_{S'_0}(A) := P(A \cap S'_0)/P(S'_0)$ *(Definition A.26);*
- $Q_{S'_0}(A) := Q(A \cap S'_0)/Q(S'_0)$ *(Definition A.26);*
- $\bar{W}_{\alpha_L} > 0$ *with* $\forall \delta > -1,\ |\delta| \leq \bar{\delta}:\ \theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \leq \bar{W}_{\alpha_L}$ *(Definition A.30);*
- $\bar{\theta}_{\alpha_L} \geq 0$ *with* $\forall \delta > -1,\ |\delta| \leq \bar{\delta}:\ \theta_{\alpha_L}(\delta) \leq \bar{\theta}_{\alpha_L}$ *(Definition A.30).*

Assume:

(A1) $(1 + \bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$;

(A2) $\forall i \leq N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ \widetilde{\sigma}_i > 0$;

(A3) $\bar{\rho}_B > 0$.

Then the core class keeps the factor R, and the classes and the fringe leaves' masses are bounded:

1. *Assume:*

   (A4) $P(S'_0) > 0$;

   (A5) $Q(S'_0) > 0$.

   Then $R_\alpha(P_{S'_0} \,\|\, Q_{S'_0}) \leq R\,(1 - P((S'_0)^c))^{-\alpha/(\alpha-1)}$;

2. $\forall k \leq N:\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \leq \binom{N}{k} \kappa_C^k\, R^{\alpha-1}$;

3. $\forall I \subseteq \{1, \ldots, N\}:\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \leq \bar{p}_C^{|I|}$.

Proof.

DEFINES $B_i := e^{\bar\phi}\,\bar W_{\alpha_L}\exp(\alpha_L(\alpha_L-1)\bar\theta_{\alpha_L}\Delta_i^2/(2\sigma_i^2))$

DEFINES $g_i := \bar\rho_B^{\alpha_L/2}B_i^{1/2}$

DEFINES $G_k := \{z_{\le k} : z\in S_0'\}$, $k\le N$

DEFINES $G_k^I := \{z_{\le k} : z\in S',\ \mathcal{K}(z)=I\}$, $I\subseteq\{1,\dots,N\}$, $k\le N$

DEFINES $g_i^{I,\kappa'} := \kappa' g_i$ at $i\in I$, $g_i^{I,\kappa'} := g_i$ at $i\notin I$, $I\subseteq\{1,\dots,N\}$, $\kappa'>\kappa_C$

Proof of item 1.

(L1) $\forall i\ \forall\, z_{<i}:\ P_i|_{z_{<i}} = \widetilde B_i$

[$\widetilde B_i$ (the statement; Definition A.28)]

(L2) $\forall i:\ \widetilde D_i = D_{\mathbb{Z},\widetilde\sigma_i,\widetilde t_i}$

[$\widetilde D_i$ (the statement; Definition A.28)]

(L3) $\forall i\ \forall\, z_{<i}:\ Q_i|_{z_{<i}} = Q_i$

[Q_i (Definition A.25, item 2)]

(L4) $\forall i\le N:\ S'_{<i}\subseteq S_{<i}$

[$S'\subseteq S$ (Definition A.26); $S'_{<i}$, $S_{<i}$ (Definition A.26)]

(L5) $\forall i\ \forall\, z_{<i}\in S'_{<i}:\ |\delta_i|\le\bar\delta$

[$\bar\delta$ (Definition A.27)]

(L6) $\forall i\ \forall\, z_{<i}\in\mathbb{Z}^{i-1}:\ 1+\delta_i = \widetilde\sigma_i/\sigma_i$

[δ_i (Definition A.27); $\sigma_i>0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2); divide by σ_i]

(L7) $\forall i\ \forall\, z_{<i}\in\mathbb{Z}^{i-1}:\ \widetilde\sigma_i/\sigma_i>0$

[$\widetilde\sigma_i>0$ (assumption A2); $\sigma_i>0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2); $y^a>0$ at $y>0$ (Fact A.41, items 12 and 28) at $(y,a):=(\sigma_i,-1)$; $\prod_k c_k>0$ at $c_k>0$ (Fact A.41, items 12 and 28)]

(L8) $\Rightarrow\ \forall i\ \forall\, z_{<i}\in\mathbb{Z}^{i-1}:\ \delta_i>-1$

[(L6), (L7)]

(L9) $\forall i\ \forall\, z_{<i}\in S'_{<i}:\ (1+\delta_i)^2<\alpha_L/(\alpha_L-1)$

[$|1+\delta_i|\le 1+\bar\delta$ ((L5); Fact A.41, item 1); $t\mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5); assumption A1]

(L10) $\forall i\ \forall\, z_{<i}\in\mathbb{Z}^{i-1}:\ \widetilde\sigma_i^2=\sigma_i^2(1+\delta_i)^2$

[δ_i (Definition A.27); expand]

(L11) $\forall i\ \forall\, z_{<i}\in\mathbb{Z}^{i-1}:\ \sigma_i^2>0$

[$\sigma_i>0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2); $y^a>0$ at $y>0$ (Fact A.41, items 12 and 28)]

(L12) $\forall i\ \forall\, z_{<i}\in S'_{<i}:\ \widetilde\sigma_i^2<\sigma_i^2\,\alpha_L/(\alpha_L-1)$

[(L10); (L9) multiplied by $\sigma_i^2>0$ ((L11); Fact A.41, item 26)]

(L13) $\forall i\ \forall\, z_{<i}\in S'_{<i}:\ |\ln\Phi_{\alpha_L,i}|\le\bar\phi$

[$\bar\phi$ (Definition A.29)]

	Corollary E.14 at order α_L, at every $i \le N$ and $z_{<i} \in S'_{<i}$	This proof
	α	α_L (the statement)
	s_1	$\widetilde{\sigma}_i$
	s_2	σ_i
	c	$\widetilde{t}_i$
	c'	t_i
	G_1	$\widetilde{D}_i$ (L2)
	G_2	Q_i (L3)
	ϕ_0	$\bar{\phi}$ (Definition A.29)
	s''	s''_i (Definition A.39 at $s := \sigma_i$, $\delta := \delta_i$; Definition A.29)
(I1)	Φ	$\Phi_{\alpha_L,i}$ (Definition A.39 at $s := \sigma_i$, $\delta := \delta_i$, $\Delta := \Delta_i$; Definition A.29)
	$\alpha > 1$	$\alpha_L > 1$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement)
	$s_1, s_2 > 0$	Assumption A2; $\sigma_i > 0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2)
	$c, c' \in \mathbb{R}$	$\widetilde{t}_i$, t_i (Definition A.25)
	$\delta > -1$	(L8)
	$\Delta \in \mathbb{R}$	Δ_i (Definition A.27)
	$\phi_0 \in \mathbb{R}$	$\bar{\phi}$ (Definition A.29)
	Assumption A1	(L12)
	Assumption A2	(L13)

Its conclusion: $R_\alpha(G_1\|G_2)^{\alpha-1} \le e^{\phi_0} \frac{s''}{s_1^\alpha s_2^{1-\alpha}} \exp\left(\frac{\alpha(\alpha-1)(c-c')^2 s'^2}{2s_1^2 s_2^2}\right)$

(L14) $\forall i \; \forall z_{<i} \in S'_{<i} : \; R_{\alpha_L}(\widetilde{D}_i\|Q_i)^{\alpha_L-1} \le e^{\bar{\phi}} \frac{s''_i}{\widetilde{\sigma}_i^{\alpha_L}\sigma_i^{1-\alpha_L}} \exp\left(\frac{\alpha_L(\alpha_L-1)(\widetilde{t}_i-t_i)^2 s''^2_i}{2\widetilde{\sigma}_i^2\sigma_i^2}\right)$

[(I1)]

(L15) $\forall i \; \forall z_{<i} \in S'_{<i} : \; \frac{s''_i}{\widetilde{\sigma}_i^{\alpha_L}\sigma_i^{1-\alpha_L}} = \theta_{\alpha_L}(\delta_i)^{1/2}(1+\delta_i)^{1-\alpha_L}$

[s''_i, $\theta_{\alpha_L}(\delta_i)$ (Definition A.29); δ_i (Definition A.27); expand]

(L16) $\forall i \; \forall z_{<i} \in S'_{<i} : \; \frac{(\widetilde{t}_i-t_i)^2 s''^2_i}{\widetilde{\sigma}_i^2\sigma_i^2} = \frac{\theta_{\alpha_L}(\delta_i)\Delta_i^2}{\sigma_i^2}$

[s''_i, $\theta_{\alpha_L}(\delta_i)$ (Definition A.29); δ_i, Δ_i (Definition A.27); expand]

(L17) $\forall i \; \forall z_{<i} \in S'_{<i} : \; \theta_{\alpha_L}(\delta_i) > 0$

[$\theta_{\alpha_L}(\delta_i)$ (Definition A.29); (L9); $\alpha_L > 1$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement)]

(L18) $\forall i \; \forall z_{<i} \in S'_{<i} : \; \theta_{\alpha_L}(\delta_i)^{1/2}(1+\delta_i)^{1-\alpha_L} \in [0, \bar{W}_{\alpha_L}]$

[(L5), (L8), (L17); $\bar{W}_{\alpha_L}$ (Definition A.30); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28)]

(L19) $\forall i \; \forall z_{<i} \in S'_{<i} : \; \theta_{\alpha_L}(\delta_i) \le \bar{\theta}_{\alpha_L}$

[(L5), (L8); $\bar{\theta}_{\alpha_L}$ (Definition A.30)]

(L20) $\forall i \; \forall z_{<i} \in S'_{<i} : \; \frac{s''_i}{\widetilde{\sigma}_i^{\alpha_L}\sigma_i^{1-\alpha_L}} \in [0, \bar{W}_{\alpha_L}]$

[(L15), (L18)]

(L21) $\forall i \; \forall z_{<i} \in S'_{<i} : \; \alpha_L(\alpha_L-1)\Delta_i^2/(2\sigma_i^2) \ge 0$

[$\alpha_L > 1$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement); $\sigma_i > 0$ ($D_{\mathbb{Z},\sigma_i,t_i}$, Definition A.25, item 2); $\Delta_i^2 \ge 0$ (Fact A.41, item 13); $ab \le a'b'$ at $(a, a', b, b') := (0, \alpha_L(\alpha_L-1), 0, \Delta_i^2/(2\sigma_i^2))$ (Fact A.41, item 8)]

(L22) $\forall i \; \forall z_{<i} \in S'_{<i} : \; \frac{\alpha_L(\alpha_L-1)(\widetilde{t}_i-t_i)^2 s''^2_i}{2\widetilde{\sigma}_i^2\sigma_i^2} \le \alpha_L(\alpha_L-1)\bar{\theta}_{\alpha_L}\Delta_i^2/(2\sigma_i^2)$

[(L16); (L19) multiplied by $\alpha_L(\alpha_L-1)\Delta_i^2/(2\sigma_i^2) \ge 0$ ((L21); Fact A.41, item 26)]

(L23) $\forall i \; \forall z_{<i} \in S'_{<i} : \; \exp\left(\frac{\alpha_L(\alpha_L-1)(\widetilde{t}_i-t_i)^2 s''^2_i}{2\widetilde{\sigma}_i^2\sigma_i^2}\right) \le \exp(\alpha_L(\alpha_L-1)\bar{\theta}_{\alpha_L}\Delta_i^2/(2\sigma_i^2))$

[(L22); exp increasing on $\mathbb{R}$ (Fact A.41, item 5)]

(L24) $\forall i \; \forall z_{<i} \in S'_{<i} : \; e^{\bar{\phi}} \frac{s''_i}{\widetilde{\sigma}_i^{\alpha_L}\sigma_i^{1-\alpha_L}} \exp\left(\frac{\alpha_L(\alpha_L-1)(\widetilde{t}_i-t_i)^2 s''^2_i}{2\widetilde{\sigma}_i^2\sigma_i^2}\right) \le B_i$

[B_i (the proof's block); (L20), (L23); $e^t > 0$ (Fact A.41, item 12); $ab \le a'b'$ (Fact A.41, item 8); $e^{\bar{\phi}} > 0$ (Fact A.41, item 12); $ca \le cb$ (Fact A.41, item 26)]

(L25) $\Rightarrow\ \forall i\ \forall z_{<i} \in S'_{<i}:\ R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha_L - 1} \le B_i$

[(L14), (L24)]

Proposition 4.2 at every $i \le N$ and $z_{<i} \in S'_{<i}$	This proof
Shared: $n \in \{512, 1024\},\ N := 2n,\ \alpha > 1$	
α	α (the statement)
$2\alpha - 1$	α_L (the statement)
$\mathcal{Y}$	$\mathcal{Z}_i \setminus C_i$ (Definitions A.26, A.28)
$\widetilde{B}$	$\widetilde{B}_i$ (the statement)
(I2) $\widetilde{D}$	$\widetilde{D}_i$ (L2)
Q	Q_i (L3)
$\mathcal{Y} \subseteq \mathbb{Z}$	$\mathcal{Z}_i \setminus C_i$ (Definitions A.26, A.28)
$i \le N,\ z_{<i} \in \mathbb{Z}^{i-1}$	The scope
Assumption A1	$\mathcal{Z}_i \setminus C_i$ finite ($\mathcal{Z}_i$, Definition A.28)
Assumption A2	(L25)
Its conclusion: $\sum_{z \in \mathcal{Y}} \widetilde{B}(z)^\alpha Q(z)^{1-\alpha} \le R_{2\alpha}^{\mathcal{Y}}(\widetilde{B} \,\|\, \widetilde{D})^{(2\alpha-1)/2}\, R_{2\alpha-1}(\widetilde{D} \,\|\, Q)^{\alpha-1}$	

(L26) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \sum_{z \in \mathcal{Z}_i \setminus C_i} \widetilde{B}_i(z)^\alpha Q_i(z)^{1-\alpha} \le R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2}\, R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1}$

[(I2)]

Fact A.45, item 3 at every $i \le N$ and $z_{<i} \in \mathbb{Z}^{i-1}$	This proof
Shared: $N,\ i,\ \alpha$	
μ	Q (Definition A.25)
p	$z_{<i}$
ν	$\widetilde{B}_i$ (the statement)
Y	$\mathcal{Z}_i \setminus C_i$ (Definitions A.26, A.28)
$\mu_i(\cdot \mid p)$	Q_i (L3)
(I3) $N \ge 1$	$N := 2n$, $n \in \{512, 1024\}$ (the statement)
$\mu : \mathbb{Z}^N \to [0,1],\ \sum_{z \in \mathbb{Z}^N} \mu(z) = 1$	Q (Definition A.25)
$i \le N,\ p \in \mathbb{Z}^{i-1}$	The scope
$\mu(p) > 0$	Fact A.45, item 2, at $\mu := Q$; (L3); $Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
$\nu : \mathbb{Z} \to [0,1],\ \sum_{x \in \mathbb{Z}} \nu(x) = 1$	$\widetilde{B}_i$ (Definition A.28)
$Y \subseteq \mathbb{Z}$	$\mathcal{Z}_i \setminus C_i$ (Definitions A.26, A.28)
$\forall x \in Y:\ \mu_i(x \mid p) > 0$	$Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
Its conclusion: $\mathbb{E}_\mu[\mathbf{1}_Y (\nu/\mu_i(\cdot \mid p))^\alpha \,|\, p] = \sum_{x \in Y} \nu(x)^\alpha\, \mu_i(x \mid p)^{1-\alpha}$	

(L27) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i \setminus C_i} (\widetilde{B}_i / Q_i)^\alpha \,|\, z_{<i}] = \sum_{x \in \mathcal{Z}_i \setminus C_i} \widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha}$

[(I3)]

(L28) $\forall i\ \forall z_{<i} \in S'_{<i}:\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i \setminus C_i} (\widetilde{B}_i / Q_i)^\alpha \,|\, z_{<i}] \le R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2}\, R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1}$

[(L26), (L27)]

(L29) $\forall i\ \forall z_{<i} \in S'_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \| \widetilde{D}_i) \le \bar{\rho}_B$

[(L4); $\bar{\rho}_B$ (Definition A.28); $a \le \max A$ and $a \le \sup A$ (Fact A.41, item 20)]

(L30) $\forall i\ \forall z_{<i} \in S'_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2} \le \bar{\rho}_B^{\alpha_L/2}$

[(L29); $t \mapsto t^p$ nondecreasing on $[0,\infty)$ at $p := \alpha_L/2$ (Fact A.41, item 5); $R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \| \widetilde{D}_i) \ge 0$ ($R_a^{\mathcal{Y}}$, Definition A.28); $\alpha_L/2 > 0$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement)]

(L31) $\forall i\ \forall z_{<i} \in S'_{<i}:\ R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1} = (R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha_L - 1})^{1/2}$

[$\alpha_L - 1 = 2(\alpha - 1)$ ($\alpha_L = 2\alpha - 1$, the statement); $(y^a)^b = y^{ab}$ at $y > 0$ (Fact A.41, items 12, 28 and 30); $R_{\alpha_L}(\widetilde{D}_i \| Q_i) \in (0, \infty]$ (R_α, Definition A.3) at $(\alpha, \mu, \nu) := (\alpha_L, \widetilde{D}_i, Q_i)$; $Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)]

(L32) $\forall i\ \forall z_{<i} \in S'_{<i}:\ (R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha_L - 1})^{1/2} \le B_i^{1/2}$

[(L25); $x \mapsto \sqrt{x}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5); $R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha_L - 1} \ge 0$ (R_α, Definition A.3)]

(L33) $\forall i\ \forall z_{<i} \in S'_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2}\, R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1} \le \bar{\rho}_B^{\alpha_L/2} B_i^{1/2}$
[(L30), (L31), (L32); $ab \le a'b'$ (Fact A.41, item 8); $R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \| \widetilde{D}_i)^{\alpha_L/2} \ge 0$ ($R_a^{\mathcal{Y}}$, Definition A.28); $R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1} \ge 0$ (R_α, Definition A.3)]

(L34) $\Rightarrow\ \forall i\ \forall z_{<i} \in S'_{<i}:\ \mathbb{E}_Q[\mathbf{1}_{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i/Q_i)^\alpha \mid z_{<i}] \le g_i$
[(L28), (L33); g_i (the proof's block)]

(L35) $\forall k \in \{1, \dots, N\}\ \forall z_{\le k} \in G_k:\ z_{<k} \in G_{k-1}$
[G_k (the proof's block)]

(L36) $\forall i \le N\ \forall z_{<i} \in G_{i-1}:\ \{x \in \mathbb{Z} : (z_{<i}, x) \in G_i\} \subseteq \mathcal{Z}_i \setminus C_i$
[G_k (the proof's block); S'_0, S (Definition A.26); $\mathcal{Z}_i$ (Definition A.28); $\widetilde{\sigma}_i > 0$ (assumption A2)]

(L37) $\forall i \le N\ \forall z_{<i} \in G_{i-1}:\ \sum_{x \in \mathbb{Z},\ (z_{<i},x) \in G_i} \widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha} \le g_i$
[(L34) on $G_{i-1} \subseteq S'_{<i}$ (G_k, the proof's block; S'_0, $S'_{<i}$, Definition A.26); (L27); (L36); $\widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha} \ge 0$ ($\widetilde{B}_i$, Q_i probability measures)]

(L38) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ B_i > 0$
[B_i (the proof's block); $e^t > 0$ (Fact A.41, item 12); $\bar{W}_{\alpha_L} > 0$ (Definition A.30); $\prod_k c_k > 0$ at $c_k > 0$ (Fact A.41, items 12 and 28)]

(L39) $\Rightarrow\ \forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ g_i > 0$
[g_i (the proof's block); $\bar{\rho}_B > 0$ (assumption A3); (L38); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28); $\prod_k c_k > 0$ at $c_k > 0$ (Fact A.41, items 12 and 28)]

(I4)

Lemma E.16 at N	This proof
Shared: α, G_k, g_i	
$P_i(\cdot \mid z_{<i})$	$\widetilde{B}_i$ (L1)
$Q_i(\cdot \mid z_{<i})$	Q_i (L3)
$N \in \mathbb{Z}_{\ge 0}$	$N := 2n$, $n \in \{512, 1024\}$ (the statement)
$P_i(\cdot \mid z_{<i}), Q_i(\cdot \mid z_{<i}) : \mathbb{Z} \to [0,1]$, $\sum_{x \in \mathbb{Z}} P_i(x \mid z_{<i}) = 1$, $\sum_{x \in \mathbb{Z}} Q_i(x \mid z_{<i}) = 1$	$\widetilde{B}_i$ (Definition A.28); Q_i (Definition A.25, item 2)
$G_k \subseteq \mathbb{Z}^k$	G_k (the proof's block)
$g_i : \mathbb{Z}^{i-1} \to (0, \infty)$	(L39)
$(P, Q) := (P, Q)$	(L1), (L3) (Fact A.45, item 1)
$G_N = S'_0$	G_k (the proof's block) at $k := N$
Assumption A1	$Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
Assumption A2	(L35)
Assumption A3	(L37)
Its conclusion: $\sum_{z \in G_N} P(z)^\alpha Q(z)^{1-\alpha} \le \sup_{z \in G_N} \prod_{i \le N} g_i(z_{<i})$	

(L40) $\sum_{z \in S'_0} P(z)^\alpha Q(z)^{1-\alpha} \le \sup_{S'_0} \prod_i g_i$
[(I4)]

(L41) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ g_i = \bar{\rho}_B^{\alpha_L/2} (e^{\bar{\phi}}\, \bar{W}_{\alpha_L})^{1/2} \exp(\alpha_L(\alpha_L - 1)\bar{\theta}_{\alpha_L} \Delta_i^2/(4\sigma_i^2))$
[g_i, B_i (the proof's block); $\sqrt{ab} = \sqrt{a}\sqrt{b}$ at $a, b \ge 0$ (Fact A.41, item 13); $(e^x)^{1/2} = e^{x/2}$ (Fact A.41, items 12, 28 and 30)]

(L42) $\forall z \in \mathbb{Z}^N:\ \prod_{i \le N} g_i = (\bar{\rho}_B^{\alpha_L/2} (e^{\bar{\phi}}\, \bar{W}_{\alpha_L})^{1/2})^N \exp(\alpha_L(\alpha_L - 1)\bar{\theta}_{\alpha_L} (\sum_{i \le N} \Delta_i^2/\sigma_i^2)/4)$
[(L41); $e^x e^y = e^{x+y}$ (Fact A.41, item 12); collect]

(L43) $\alpha_L(\alpha_L - 1)/4 = \alpha_L(\alpha - 1)/2$
[$\alpha_L = 2\alpha - 1$ (the statement); expand]

(L44) $\forall z \in S'_0:\ \sum_{i \le N} \Delta_i^2/\sigma_i^2 \le \bar{W}_{S'}$
[$\bar{W}_{S'}$ (Definition A.27) on $S'_0 \subseteq S'$ (S'_0, Definition A.26); $a \le \sup A$ (Fact A.41, item 20)]

(L45) $\forall z \in S'_0:\ \prod_{i \le N} g_i \le (\bar{\rho}_B^{\alpha_L/2} (e^{\bar{\phi}}\, \bar{W}_{\alpha_L})^{1/2})^N \exp(\alpha_L(\alpha - 1)\bar{\theta}_{\alpha_L} \bar{W}_{S'}/2)$
[(L42), (L43), (L44); $\bar{\theta}_{\alpha_L} \ge 0$ (Definition A.30); $\alpha_L(\alpha - 1) > 0$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement); $ca \le cb$ (Fact A.41, item 26); exp increasing on $\mathbb{R}$ (Fact A.41, item 5); $\bar{\rho}_B^{\alpha_L/2} (e^{\bar{\phi}}\, \bar{W}_{\alpha_L})^{1/2} > 0$ (assumption A3; $\bar{W}_{\alpha_L} > 0$, Definition A.30; $y^a > 0$ at $y > 0$, Fact A.41, items 12 and 28)]

(L46) $\Rightarrow\ \sup_{S'_0} \prod_{i \le N} g_i \le (\bar{\rho}_B^{\alpha_L/2} (e^{\bar{\phi}}\, \bar{W}_{\alpha_L})^{1/2})^N \exp(\alpha_L(\alpha - 1)\bar{\theta}_{\alpha_L} \bar{W}_{S'}/2)$

[(L45); Fact A.41, item 20]

(L47) $\Rightarrow$ $\sum_{z\in S'_0} P(z)^\alpha Q(z)^{1-\alpha} \le (\bar\rho_B^{\alpha_L/2}(e^{\bar\phi}\,\bar W_{\alpha_L})^{1/2})^N \exp(\alpha_L(\alpha-1)\bar\theta_{\alpha_L}\bar W_{S'}/2)$

[(L40), (L46)]

(L48) $\Rightarrow$ $\sum_{z\in S'_0} P^\alpha Q^{1-\alpha} \le R^{\alpha-1}$

[(L47); R (Definition A.30); multiply the exponents]

Fact A.45, item 10	This proof
Shared: α	
X	$\mathbb{Z}^N$ (the statement)
μ	P (the statement)
ν	Q (the statement)
B	S'_0 (the statement)
μ_B	$P_{S'_0}$ (the statement)
(I5) ν_B	$Q_{S'_0}$ (the statement)
α	α (the statement)
X countable	$\mathbb{Z}^N$ countable (Fact A.41, item 17)
$\mu,\nu : X \to [0,1]$, $\sum_{x\in X}\mu(x) = 1$, $\sum_{x\in X}\nu(x) = 1$	P, Q (Definition A.25)
$B \subseteq X$	S'_0 (Definition A.26)
$\mu(B) > 0$	Assumption A4
$\nu(B) > 0$	Assumption A5
Its conclusion: $R_\alpha(\mu_B \,\|\, \nu_B)^{\alpha-1} = \nu(B)^{\alpha-1}\mu(B)^{-\alpha}\sum_{x\in B}\mu(x)^\alpha\,\nu(x)^{1-\alpha}$	

(L49) $R_\alpha(P_{S'_0}\|Q_{S'_0})^{\alpha-1} = Q(S'_0)^{\alpha-1}P(S'_0)^{-\alpha}\sum_{x\in S'_0} P(x)^\alpha\,Q(x)^{1-\alpha}$

[(I5)]

(L50) $\Rightarrow$ $R_\alpha(P_{S'_0}\|Q_{S'_0})^{\alpha-1} \le Q(S'_0)^{\alpha-1}P(S'_0)^{-\alpha}R^{\alpha-1}$

[(L49); (L48) multiplied by $Q(S'_0)^{\alpha-1}P(S'_0)^{-\alpha} \ge 0$]

(L51) $\Rightarrow$ $R_\alpha(P_{S'_0}\|Q_{S'_0}) \le R\,(1-P((S'_0)^c))^{-\alpha/(\alpha-1)}$

[$(\alpha-1)$-th root; $Q(S'_0) \le 1$ (Q, Definition A.25; Fact A.45, item 12); $P(S'_0) \ge 1 - P((S'_0)^c)$ (Fact A.45, item 5)]

(L52) $\Rightarrow$ item 1

[(L51)]

□ (item 1)

Proof of item 2.

(L53) $\forall i:\ Q_i^{1-\alpha} \ge 0$

[$Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2); Fact A.41, item 12]

(L54) $\forall i \le N\ \forall\, z_{<i} \in S'_{<i}:\ \sum_{z_i\in C_i}\widetilde B_i^\alpha Q_i^{1-\alpha} \le \bar U^\alpha \sum_{z_i\in C_i}\widetilde D_i^\alpha Q_i^{1-\alpha}$

[$\widetilde B_i \le \bar U\,\widetilde D_i$ on C_i ($\bar U$, Definition A.28) at $z_{<i} \in S_{<i}$, (L4); $x \mapsto x^\alpha$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5); (L53)]

(L55) $\forall i \le N\ \forall\, z_{<i} \in S'_{<i}:\ \sum_{z_i\in C_i}\widetilde D_i^\alpha Q_i^{1-\alpha} \le R_\alpha(\widetilde D_i\|Q_i)^{\alpha-1}$

[$C_i \subseteq \mathbb{Z}$ (Definition A.28); $\widetilde D_i^\alpha Q_i^{1-\alpha} \ge 0$ ($\widetilde D_i$, Q_i probability measures); Fact A.45, item 9; Definition A.3, item 2, at $(X,\mu,\nu) := (\mathbb{Z}, \widetilde D_i, Q_i)$; $Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)]

Fact A.45, item 8 at every $i \le N$ and $z_{<i} \in S'_{<i}$	This proof
a	α (the statement)
μ	$\widetilde D_i$ (L2)
ν	Q_i (L3)
(I6) $\mu,\nu : \mathbb{Z} \to [0,1]$, $\sum_{x\in\mathbb{Z}}\mu(x) = 1$, $\sum_{x\in\mathbb{Z}}\nu(x) = 1$	$\widetilde D_i$ (Definition A.28), Q_i (Definition A.25, item 2)
$\forall z \in \mathbb{Z}:\ \nu(z) > 0$	$Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
$a > 1$	$\alpha > 1$ (the statement)
Its conclusion: $R_a(\mu \,\|\, \nu) \le R_{2a-1}(\mu \,\|\, \nu)$	

(L56) $\forall i \le N\ \forall z_{<i} \in S'_{<i}:\ R_\alpha(\widetilde{D}_i \,\|\, Q_i) \le R_{2\alpha-1}(\widetilde{D}_i \,\|\, Q_i)$

[(I6)]

(L57) $\forall i \le N\ \forall z_{<i} \in S'_{<i}:\ R_\alpha(\widetilde{D}_i \| Q_i)^{\alpha-1} \le R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1}$

[(L56); $2\alpha - 1 = \alpha_L$ (α_L, the statement); $t \mapsto t^{\alpha-1}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L58) $\forall i \le N\ \forall z_{<i} \in S'_{<i}:\ R_{\alpha_L}(\widetilde{D}_i \| Q_i)^{\alpha-1} \le B_i^{1/2}$

[(L31), (L32)]

(L59) $\Rightarrow\ \forall i \le N\ \forall z_{<i} \in S'_{<i}:\ \sum_{z_i \in C_i} \widetilde{D}_i^\alpha Q_i^{1-\alpha} \le B_i^{1/2}$

[(L55), (L57), (L58)]

(L60) $\Rightarrow\ \forall i \le N\ \forall z_{<i} \in S'_{<i}:\ \sum_{z_i \in C_i} \widetilde{B}_i^\alpha Q_i^{1-\alpha} \le \bar{U}^\alpha B_i^{1/2}$

[(L54), (L59)]

(L61) $\bar{U}^\alpha B_i^{1/2} = \kappa_C\, g_i$

[κ_C (Definition A.28); g_i (the proof's block)]

(L62) $\Rightarrow\ \forall i \le N\ \forall z_{<i} \in S'_{<i}:\ \sum_{z_i \in C_i} \widetilde{B}_i^\alpha Q_i^{1-\alpha} \le \kappa_C\, g_i$

[(L60), (L61)]

(L63) $\forall I \subseteq \{1,\dots,N\}\ \forall k \in \{1,\dots,N\}\ \forall z_{\le k} \in G_k^I:\ z_{<k} \in G_{k-1}^I$

[G_k^I (the proof's block)]

(L64) $\forall I\ \forall i \le N,\ i \notin I\ \forall z_{<i} \in G_{i-1}^I:\ \{x \in \mathbb{Z} : (z_{<i}, x) \in G_i^I\} \subseteq \mathcal{Z}_i \setminus C_i$

[G_k^I (the proof's block); S, $\mathcal{K}$ (Definition A.26); $\mathcal{Z}_i$ (Definition A.28); $\widetilde{\sigma}_i > 0$ (assumption A2)]

(L65) $\forall I\ \forall i \in I\ \forall z_{<i} \in G_{i-1}^I:\ \{x \in \mathbb{Z} : (z_{<i}, x) \in G_i^I\} \subseteq C_i$

[G_k^I (the proof's block); $\mathcal{K}$ (Definition A.26)]

(L66) $\forall I\ \forall i \le N,\ i \notin I\ \forall z_{<i} \in G_{i-1}^I:\ \sum_{x \in \mathbb{Z},\ (z_{<i},x) \in G_i^I} \widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha} \le g_i$

[(L34) on $G_{i-1}^I \subseteq S'_{<i}$ (G_k^I, the proof's block; $S'_{<i}$, Definition A.26); (L27); (L64); $\widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha} \ge 0$ ($\widetilde{B}_i$, Q_i probability measures)]

(L67) $\forall I\ \forall i \in I\ \forall z_{<i} \in G_{i-1}^I:\ \sum_{x \in \mathbb{Z},\ (z_{<i},x) \in G_i^I} \widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha} \le \kappa_C\, g_i$

[(L62) on $G_{i-1}^I \subseteq S'_{<i}$ (G_k^I, the proof's block; $S'_{<i}$, Definition A.26); (L65); $\widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha} \ge 0$ ($\widetilde{B}_i$, Q_i probability measures)]

(L68) $\forall \kappa' > \kappa_C:\ \kappa' > 0$

[$\kappa_C \ge 0$ (κ_C, Definition A.28)]

(L69) $\forall \kappa' > \kappa_C\ \forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ \kappa_C\, g_i \le \kappa'\, g_i$

[(L39); Fact A.41, item 26]

(L70) $\forall I\ \forall \kappa' > \kappa_C\ \forall i \le N\ \forall z_{<i} \in G_{i-1}^I:\ \sum_{x \in \mathbb{Z},\ (z_{<i},x) \in G_i^I} \widetilde{B}_i(x)^\alpha Q_i(x)^{1-\alpha} \le g_i^{I,\kappa'}$

[(L66), (L67), (L69); $g_i^{I,\kappa'}$ (the proof's block)]

(L71) $\forall I\ \forall \kappa' > \kappa_C\ \forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}:\ g_i^{I,\kappa'} > 0$

[$g_i^{I,\kappa'}$ (the proof's block); (L39), (L68); Fact A.41, item 8]

Lemma E.16 at N, at every $I \subseteq \{1,\dots,N\}$ and $\kappa' > \kappa_C$	This proof
Shared: α	
$P_i(\cdot \mid z_{<i})$	$\widetilde{B}_i$ (L1)
$Q_i(\cdot \mid z_{<i})$	Q_i (L3)
G_k	G_k^I (the proof's block)
g_i	$g_i^{I,\kappa'}$ (the proof's block)
$N \in \mathbb{Z}_{\geq 0}$	$N := 2n$, $n \in \{512, 1024\}$ (the statement)
(I7) $P_i(\cdot \mid z_{<i}), Q_i(\cdot \mid z_{<i}) : \mathbb{Z} \to [0,1]$, $\sum_{x\in\mathbb{Z}} P_i(x \mid z_{<i}) = 1$, $\sum_{x\in\mathbb{Z}} Q_i(x \mid z_{<i}) = 1$	$\widetilde{B}_i$ (Definition A.28); Q_i (Definition A.25, item 2)
$G_k \subseteq \mathbb{Z}^k$	G_k^I (the proof's block)
$g_i : \mathbb{Z}^{i-1} \to (0,\infty)$	(L71)
$(P,Q) := (P,Q)$	(L1), (L3) (Fact A.45, item 1)
Assumption A1	$Q_i > 0$ on $\mathbb{Z}$ (Definition A.25, item 2)
Assumption A2	(L63)
Assumption A3	(L70)
Its conclusion: $\sum_{z\in G_N} P(z)^\alpha Q(z)^{1-\alpha} \leq \sup_{z\in G_N} \prod_{i\leq N} g_i(z_{<i})$	

(L72) $\forall I\ \forall \kappa' > \kappa_C :\ \sum_{z\in G_N^I} P(z)^\alpha Q(z)^{1-\alpha} \leq \sup_{z\in G_N^I} \prod_{i\leq N} g_i^{I,\kappa'}(z_{<i})$

[(I7)]

(L73) $\forall I\ \forall \kappa' > \kappa_C\ \forall z \in G_N^I :\ \prod_{i\leq N} g_i^{I,\kappa'}(z_{<i}) = \kappa'^{|I|} \prod_{i\leq N} g_i(z_{<i})$

[$g_i^{I,\kappa'}$ (the proof's block); collect]

(L74) $\sup_{S'} \prod_i g_i \leq R^{\alpha-1}$

[g_i, B_i (the proof's block); $\sum_i \Delta_i^2/\sigma_i^2 \leq \bar{W}_{S'}$ on S' ($\bar{W}_{S'}$, Definition A.27); $\bar{\theta}_{\alpha_L} \geq 0$ (Definition A.30); exp increasing (Fact A.41, item 5); R (Definition A.30); multiply the exponents]

(L75) $\forall I\ \forall \kappa' > \kappa_C :\ \sum_{z\in S',\ \mathcal{K}(z)=I} P(z)^\alpha Q(z)^{1-\alpha} \leq R^{\alpha-1}\kappa'^{|I|}$

[(L72), (L73), (L74), (L68); G_N^I (the proof's block); $a \leq \sup A$ (Fact A.41, item 20)]

Fact A.41, item 18 at every $I \subseteq \{1,\dots,N\}$	This proof
k	$\lvert I\rvert$
A	$R^{\alpha-1}$ (the statement)
(I8) c	κ_C (Definition A.28)
x	$\sum_{z\in S',\ \mathcal{K}(z)=I} P(z)^\alpha Q(z)^{1-\alpha}$
$k \in \mathbb{Z}_{\geq 0}$	$\lvert I\rvert$ (the scope)
$A, c, x \in \mathbb{R}$	R (Definition A.30); κ_C (Definition A.28); (L75)
$\forall c' > c :\ x \leq Ac'^k$	(L75)
Its conclusion: $x \leq Ac^k$	

(L76) $\forall I \subseteq \{1,\dots,N\} :\ \sum_{z\in S',\ \mathcal{K}(z)=I} P(z)^\alpha Q(z)^{1-\alpha} \leq R^{\alpha-1}\kappa_C^{|I|}$

[(I8)]

(L77) $\forall k \leq N :\ S'_k = \bigcup_{I\subseteq\{1,\dots,N\},\ |I|=k} \{z \in S' : \mathcal{K}(z) = I\}$

[S'_k, $\mathcal{K}$ (Definition A.26)]

(L78) $\forall k \leq N :\ \sum_{z\in S'_k} P^\alpha Q^{1-\alpha} = \sum_{I\subseteq\{1,\dots,N\},\ |I|=k} \sum_{z\in S',\ \mathcal{K}(z)=I} P(z)^\alpha Q(z)^{1-\alpha}$

[(L77); $\mathcal{K}$, a function on S' (Definition A.26); Fact A.45, item 9]

(L79) $\forall k \leq N :\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \leq \binom{N}{k} \kappa_C^k R^{\alpha-1}$

[(L78), (L76); $\sum_{I\subseteq\{1,\dots,N\},\ |I|=k} 1 = \binom{N}{k}$; $R_\alpha^{S'_k}(P \,\|\, Q)$ (Definition A.28)]

(L80) $\Rightarrow$ item 2

[(L79)]

□ (item 2)

Proof of item 3.

(L81) $\forall I \subseteq \{1,\dots,N\}:\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$
[$\Pr_P[z_i \in C_i \mid z_{<i}] = \widetilde{B}_i(C_i)$, $\widetilde{B}_i(C_i) \le \bar{p}_C$ at $z_{<i} \in S_{<i}$ (Definition A.28) and $z \in S' \Rightarrow\ z_{<i} \in S'_{<i}$ ($S'_{<i}$, Definition A.26), (L4); the $|I|$ conditionals along $z_1,\dots,z_N$ (Fact A.45, item 1)]

(L82) $\Rightarrow$ item 3

[(L81)]

□ (item 3)

G Proofs of Section 4.5

Structure. This appendix proves the statements of Section 4.5. Section G.1 states the rounding factors; Section G.2 the tree map and the output measures; Section G.3 the elementary bounds; Section G.4 the computed diagonals; Section G.5 the centers; Section G.6 the base sampler under $\mathcal{F}$. The proofs follow the conventions of Appendix D.

How each statement is verified. Table 18 lists the definitions and facts placed here, Table 19 how each statement placed here is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Fact G.5	✓				
Def. G.6	✓				
Fact G.7	✓				
Fact G.8	✓				
Def. G.9	✓				
Fact G.12	✓				
Fact G.50	✓				
Fact G.66	✓				

Table 18: Appendix G: its definitions and facts.

Table 19: Appendix G: how each lemma, proposition, corollary and theorem is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma G.1	✓				
Lemma G.2	✓				
Lemma G.3	✓				
Lemma G.4	✓				
Lemma G.10	✓				
Lemma G.11	✓				
Lemma G.13	✓				
Lemma G.14	✓		✓		
Prop. G.15	✓				
Lemma G.16	✓				
Lemma G.17	✓				
Lemma G.18	✓				
Prop. G.19	✓				
Lemma G.20	✓				
Lemma G.21	✓				
Lemma G.22	✓				
Lemma G.23	✓				
Lemma G.24	✓				
Lemma G.25	✓				
Lemma G.26	✓				
Lemma G.27	✓				
Lemma G.28	✓				

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma G.29	✓				
Lemma G.30	✓				
Lemma G.31	✓				
Lemma G.32	✓				
Lemma G.33	✓				
Lemma G.34	✓				
Lemma G.35	✓				
Cor. G.36	✓				
Lemma G.37	✓				
Prop. G.38	✓				
Lemma G.39	✓				
Lemma G.40	✓				
Cor. G.41	✓				
Lemma G.42	✓				
Cor. G.43	✓				
Lemma G.44	✓				
Lemma G.45	✓				
Lemma G.46	✓				
Lemma G.47	✓				
Prop. G.48	✓				
Lemma G.49	✓				
Lemma G.51	✓				
Lemma G.52	✓				
Lemma G.53	✓				
Lemma G.54	✓				
Lemma G.55	✓				
Lemma G.56	✓				
Lemma G.57	✓				
Lemma G.58	✓				
Thm. G.59	✓				
Lemma G.60	✓				
Lemma G.61	✓				
Cor. G.62	✓				
Lemma G.63	✓				
Lemma G.64	✓				
Lemma G.65	✓				
Lemma G.67	✓				
Lemma G.68	✓				
Lemma G.69	✓				
Lemma G.70	✓				
Lemma G.71	✓				
Lemma G.72	✓				
Lemma G.73	✓				
Lemma G.74	✓				
Cor. G.75	✓				
Lemma G.76	✓				
Lemma G.77	✓				
Lemma G.78	✓				
Lemma G.79	✓				
Lemma G.80	✓				

G.1 The relative form and the rounding factors

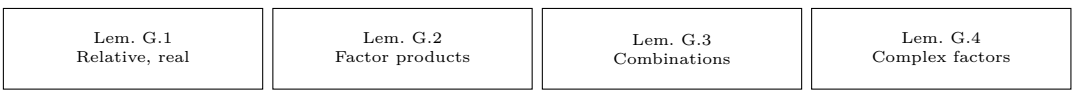


Figure 47: Dependencies, Section G.1.

Structure. Lemma G.1 states the relative form of a real modulus bound; Lemma G.2 the products of rounding factors; Lemma G.3 their nonnegative combinations; Lemma G.4 the products of complex factors. The four hold for the pair (u, ζ) of any realization.

Lemma G.1 (The relative form of a real modulus bound [to table])**.** *A real value within c times the modulus of its reference is the reference times a factor within c of 1. Let:*

- $c \geq 0$;
- $x, p \in \mathbb{R}$.

Define:

- $\delta(p, x) := (p - x)/x$ *for* $x \neq 0$, *and* $\delta(p, 0) := 0$.

Assume:

(A1) $|p - x| \leq c|x|$.

Then the factor is bounded and yields p:

1. $|\delta(p, x)| \leq c$;
2. $p = x(1 + \delta(p, x))$.

Proof. (L1) $x = 0 \Rightarrow |p| \leq 0$
[assumption A1 at $x = 0$]

(L2) $x = 0 \Rightarrow p = 0$
[(L1)]

(L3) $x = 0 \Rightarrow |\delta(p, x)| = 0$
[$\delta(p, 0) = 0$ (the statement)]

(L4) $x = 0 \Rightarrow |\delta(p, x)| \leq c$
[(L3); $c \geq 0$ (the statement)]

(L5) $x = 0 \Rightarrow x(1 + \delta(p, x)) = 0$
[$x = 0$]

(L6) $x = 0 \Rightarrow x(1 + \delta(p, x)) = p$
[(L2), (L5)]

(L7) $x \neq 0 \Rightarrow |\delta(p, x)| = |p - x|/|x|$
[$\delta(p, x) = (p - x)/x$ (the statement); Fact A.41, item 1: $|xy| = |x||y|$]

(L8) $x \neq 0 \Rightarrow |\delta(p, x)| \leq c$
[(L7); assumption A1]

(L9) $x \neq 0 \Rightarrow x(1 + \delta(p, x)) = x + (p - x)$
[$\delta(p, x) = (p - x)/x$ (the statement)]

(L10) $x + (p - x) = p$
[expand]

(L11) $\Rightarrow |\delta(p, x)| \leq c$
[(L4), (L8)]

(L12) $\Rightarrow$ item 1
[(L11)]

(L13) $\Rightarrow p = x(1 + \delta(p, x))$
[(L6), (L9), (L10)]

(L14) $\Rightarrow$ item 2
[(L13)]

□ (items 1 and 2)

Lemma G.2 (Products of rounding factors [to table])**.** *A product of k factors, each within u of 1, lies between the k-th powers of $1 - u$ and $1 + u$, so it is within $(1 + u)^k - 1$ of 1. Let:*

- $u \in [0, 1]$;
- $k \in \mathbb{Z}_{\geq 0}$ *(Definition A.1);*

- $t_1, \dots, t_k \in \mathbb{R}$.

Define:

- $P := \prod_{j=1}^{k}(1+t_j)$;
- $p_k := (1+u)^k - 1$;
- $p'_k := 1-(1-u)^k$.

Assume:

(A1) $\forall j \le k:\ |t_j| \le u$.

Then the product lies in the interval and within p_k of 1:

1. $P \in [(1-u)^k, (1+u)^k]$;
2. $p'_k \le p_k$;
3. $|P-1| \le p_k$.

Proof.

DEFINES $P_i := \prod_{j=1}^{i}(1+t_j)$, $i \in \{0, \dots, k\}$

Proof of item 1.

(L1) $1-u \ge 0$

[$u \le 1$ (the statement)]

(L2) $\forall j \le k:\ 1+t_j \ge 1-u$

[assumption A1]

(L3) $\forall j \le k:\ 1+t_j \le 1+u$

[assumption A1]

(L4) $P_0 \in [(1-u)^0, (1+u)^0]$

[$P_0 = 1$ (the proof's block): the empty product]

(L5) $\forall i < k:\ P_{i+1} = P_i(1+t_{i+1})$

[P_i (the proof's block)]

(L6) $\forall i < k:\ [P_i \ge (1-u)^i] \Rightarrow\ P_i(1+t_{i+1}) \ge (1-u)^{i+1}$

[(L1), (L2) at $j = i+1$; Fact A.41, item 8, at $(a, a', b, b') := ((1-u)^i, P_i, 1-u, 1+t_{i+1})$]

(L7) $\forall i < k:\ [0 \le P_i \le (1+u)^i] \Rightarrow\ P_i(1+t_{i+1}) \le (1+u)^{i+1}$

[(L1), (L2), (L3) at $j = i+1$; Fact A.41, item 8, at $(a, a', b, b') := (P_i, (1+u)^i, 1+t_{i+1}, 1+u)$]

(L8) $\Rightarrow\ \forall i < k:\ [P_i \in [(1-u)^i, (1+u)^i]] \Rightarrow\ P_{i+1} \in [(1-u)^{i+1}, (1+u)^{i+1}]$

[(L1), (L5), (L6), (L7)]

(L9) $\Rightarrow\ P \in [(1-u)^k, (1+u)^k]$

[induction on i: base (L4), step (L8), at $i = k$; $P = P_k$ (the statement)]

(L10) $\Rightarrow$ item 1

[(L9)]

□ (item 1)

Proof of item 2.

(L11) $(1+u)^k + (1-u)^k = 2\sum_{i \le k,\ 2|i} \binom{k}{i} u^i$

[the binomial expansions of $(1 \pm u)^k$]

(L12) $2\sum_{i \le k,\ 2|i} \binom{k}{i} u^i \ge 2$

[$\binom{k}{0} u^0 = 1$; the other terms nonnegative at $u \ge 0$ (the statement)]

(L13) $p_k - p'_k = (1+u)^k + (1-u)^k - 2$

[p_k, p'_k (the statement)]

(L14) $\Rightarrow\ p_k - p'_k \ge 0$

[(L11), (L12), (L13)]

(L15) $\Rightarrow$ item 2

[(L14)]

□ (item 2)

Proof of item 3.

(L16) $P - 1 \in [-p'_k, p_k]$

[item 1; p_k, p'_k (the statement)]

(L17) $\Rightarrow$ $|P - 1| \le \max(p_k, p'_k)$

[(L16)]

(L18) $\Rightarrow$ $|P - 1| \le p_k$

[(L17); item 2]

(L19) $\Rightarrow$ item 3

[(L18)]

□ (item 3)

Lemma G.3 (Nonnegative combinations of rounding-factor products [to table])**.** *A nonnegative combination of values in $[(1-u)^k, (1+u)^k]$ lies between the two powers times the sum of the weights. Let:*

- $u \in \mathbb{R}$;
- $k \in \mathbb{Z}_{\ge 0}$;
- $m \in \mathbb{Z}_{\ge 0}$;
- $a_1, \dots, a_m \ge 0$;
- $P_1, \dots, P_m \in [(1-u)^k, (1+u)^k]$.

Define:

- $A := \sum_{j=1}^{m} a_j$.

Then

$$\sum_{j=1}^{m} a_j P_j \in [(1-u)^k A,\ (1+u)^k A].$$

Proof. (L1) $\forall j \le m:\ a_j P_j \ge a_j (1-u)^k$

[$a_j \ge 0$, $P_j \in [(1-u)^k, (1+u)^k]$ (the statement); Fact A.41, item 8]

(L2) $\forall j \le m:\ a_j P_j \le a_j (1+u)^k$

[$a_j \ge 0$, $P_j \in [(1-u)^k, (1+u)^k]$ (the statement); Fact A.41, item 8]

(L3) $\Rightarrow$ $\sum_{j=1}^{m} a_j P_j \in [(1-u)^k A,\ (1+u)^k A]$

[(L1), (L2) summed over $j \le m$; A (the statement)]

(L4) $\Rightarrow$ the statement

[(L3)]

□

Lemma G.4 (Products of complex factors [to table])**.** *A product of complex factors, each within c_j of 1, is within the product of the $1 + c_j$ less one of 1. Let:*

- $k \in \mathbb{Z}_{\ge 0}$;
- $\delta_1, \dots, \delta_k \in \mathbb{C}$;
- $c_1, \dots, c_k \ge 0$.

Assume:

(A1) $\forall j \le k:\ |\delta_j| \le c_j$.

Then

$$\left|\prod_{j=1}^{k} (1+\delta_j) - 1\right| \le \prod_{j=1}^{k} (1+c_j) - 1.$$

Proof.

DEFINES $X_j := \prod_{i \le j} (1+\delta_i)$, $j \in \{0, \dots, k\}$

DEFINES $C_j := \prod_{i \le j} (1+c_i)$, $j \in \{0, \dots, k\}$

(L1) $X_0 = 1$

[X_j (the proof's block): the empty product]

(L2) $C_0 = 1$

[C_j (the proof's block): the empty product]

(L3) $\forall j \le k:\ X_j - 1 = (1+\delta_j)(X_{j-1} - 1) + \delta_j$

[$X_j = (1+\delta_j)X_{j-1}$ (the proof's block); expand]

(L4) $\Rightarrow\ \forall j \le k:\ |X_j - 1| \le |1+\delta_j||X_{j-1} - 1| + |\delta_j|$

[(L3); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$]

(L5) $\forall j \le k:\ |1+\delta_j| \le 1 + c_j$

[Fact A.41, item 1: $|x+y| \le |x| + |y|$; assumption A1]

(L6) $\Rightarrow\ \forall j \le k:\ |X_j - 1| \le (1+c_j)|X_{j-1} - 1| + c_j$

[(L4), (L5); assumption A1]

(L7) $\forall j \le k:\ 1 + c_j \ge 0$

[$c_j \ge 0$ (the statement)]

(L8) $\forall j \le k:\ [|X_{j-1} - 1| \le C_{j-1} - 1] \Rightarrow\ |X_j - 1| \le (1+c_j)(C_{j-1} - 1) + c_j$

[(L6), (L7)]

(L9) $\forall j \le k:\ (1+c_j)(C_{j-1} - 1) + c_j = C_j - 1$

[expand; $C_j = (1+c_j)C_{j-1}$ (the proof's block)]

(L10) $|X_0 - 1| = 0$

[(L1)]

(L11) $C_0 - 1 = 0$

[(L2)]

(L12) $\Rightarrow\ |X_k - 1| \le C_k - 1$

[induction on j: base (L10), (L11), step (L8), (L9); X_k, C_k (the proof's block)]

(L13) $\Rightarrow$ the statement

[(L12)]

□

G.2 The tree map and the output measures

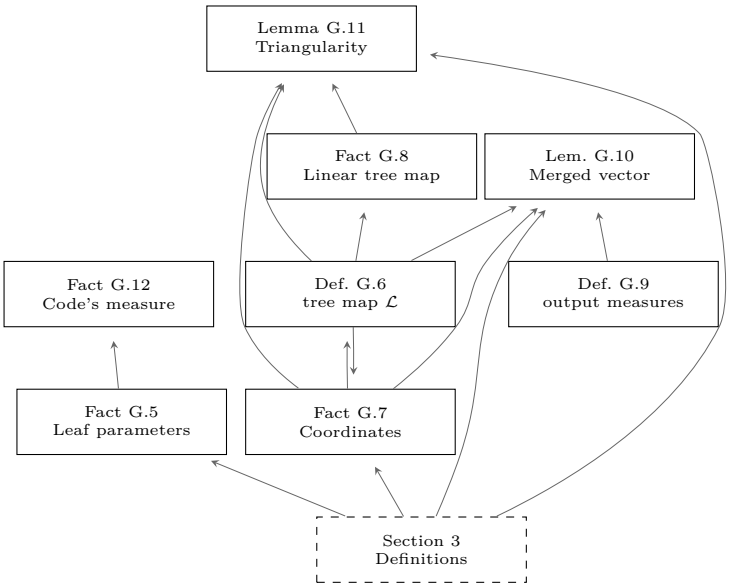


Figure 48: Dependencies, Section G.2.

Fact G.5 states the code's leaf parameters over $\mathbb{R}$; Fact G.12 the output measure of the code's recursion.

Fact G.5 (The code's leaf parameters over $\mathbb{R}$ [to table])**.** At every position and for all samples before it, the leaf parameters the code's recursion computes over $\mathbb{R}$ from a Gram matrix are those the sampler computes on the tree of that matrix. Let:

- $\mathcal{G} \in \mathrm{Gram}_n$ (Definition A.14);
- $t \in \mathcal{R}_n \times \mathcal{R}_n$;
- $s > 0$, the standard deviation parameter of ffSampling (Definition A.21).

Define, at the positions i of the sampling order of Definition A.19:

- $T := \mathrm{ffLDL}^\dagger(\mathcal{G})$ (Definition A.20);
- $(\sigma_i, c_i)(z_{<i})$, $i \le N$, $z \in \mathbb{Z}^N$: the leaf parameters ffSampling (Definition A.21) computes at (t, T) with the samples $z_{<i}$, Definition A.21, items 1 and 2;
- $(\sigma'_i, c'_i)(z_{<i})$, $i \le N$, $z \in \mathbb{Z}^N$: those ffsamp (Algorithm 6) computes at $(t, \mathcal{G}, 0)$ over $\mathbb{R}$ with the samples $z_{<i}$, deepest (Algorithm 7), lines 1 to 18.

Assume:

(A1) `INV_SIGMA` $= 1/s$ in ffsamp (Algorithm 6) over $\mathbb{R}$.

Then

$$\forall z \in \mathbb{Z}^N \ \forall i \le N: \quad (\sigma'_i, c'_i)(z_{<i}) = (\sigma_i, c_i)(z_{<i}). \qquad \text{[derived]}$$

Proof.

DEFINES $\mathcal{G}_\nu$, $\nu \in \mathrm{Sub}(T)$: that of Definition A.32

DEFINES $\mathcal{P}(m)$, $m \in \{2, 4, \ldots, n\}$: $\forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m \ \forall t' \in \mathcal{R}_m^2 \ \forall z \ \forall i \in I(\nu)$, the leaf parameter at i of ffsamp$(t', \mathcal{G}_\nu, 0)$ over $\mathbb{R}$ equals that of ffSampling(t', ν)

DEFINES $(t_0, t_1) := t'$, (l_{10}, d_{00}, d_{11}), z_1, tb_0 at a call: those of ffSampling (Definition A.21) at (t', ν)

DEFINES $(l'_{10}, d'_{00}, d'_{11}) := \mathrm{LDL}^\dagger(\mathcal{G}_\nu)$, z'_1: those of ffsamp (Algorithm 6) at $(t', \mathcal{G}_\nu, 0)$, lines 4, 1

DEFINES $tb'_0 := t_0 + (t_1 - z'_1)\, l'_{10}$: that of ffsamp (Algorithm 6) at $(t', \mathcal{G}_\nu, 0)$, line 26

(L1) $\forall \nu \in \mathrm{Sub}(T): \ (l'_{10}, d'_{00}, d'_{11}) = (l_{10}, d_{00}, d_{11})$
[ffsamp (Algorithm 6), line 4, and Definition A.20, item 1: $\mathrm{LDL}^\dagger$ (Algorithm 5) at $\mathcal{G}_\nu$ over $\mathbb{R}$]

(L2) $\forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_2, \ I(\nu) = \{a, \ldots, a+3\}$:

$$(\sigma'_i, c'_i)_{i=a}^{a+3} = \left((s/\sqrt{d'_{11}}, \ \mathrm{Re}\, t_1), \ (s/\sqrt{d'_{11}}, \ \mathrm{Im}\, t_1), \ (s/\sqrt{d'_{00}}, \ \mathrm{Re}\, tb'_0), \ (s/\sqrt{d'_{00}}, \ \mathrm{Im}\, tb'_0)\right)$$

[deepest (Algorithm 7), lines 1 to 18; `INV_SIGMA` $= 1/s$ (assumption A1); $I(R(\nu)) = \{a, a+1\}$, $I(L(\nu)) = \{a+2, a+3\}$ (Definition A.19)]

(L3) $\forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_2, \ I(\nu) = \{a, \ldots, a+3\}$:

$$(\sigma_i, c_i)_{i=a}^{a+3} = \left((s/\sqrt{d_{11}}, \ \mathrm{Re}\, t_1), \ (s/\sqrt{d_{11}}, \ \mathrm{Im}\, t_1), \ (s/\sqrt{d_{00}}, \ \mathrm{Re}\, tb_0), \ (s/\sqrt{d_{00}}, \ \mathrm{Im}\, tb_0)\right)$$

[Definition A.21, items 1 and 2, at $T_{11} := d_{11}$, $T_{00} := d_{00}$ (Definition A.20, item 2) and $t_{T_{11}} = t_1$, $t_{T_{00}} = tb_0$ (Definition A.21, items 7 to 11); $I(R(\nu)) = \{a, a+1\}$, $I(L(\nu)) = \{a+2, a+3\}$ (Definition A.19)]

(L4) $\forall \nu \in \mathrm{Sub}(T): \ z'_1 = z_1$
[both the samples $(z_i)_{i \in I(R(\nu))}$: deepest (Algorithm 7), line 1, and Definition A.21, item 4, at $m = 2$; merge of them in both at $m \ge 4$]

(L5) $\forall \nu \in \mathrm{Sub}(T): \ tb'_0 = tb_0$
[(L1), (L4); tb'_0, tb_0 (the proof's block)]

(L6) $\Rightarrow \ \mathcal{P}(2)$
[(L1), (L2), (L3), (L5)]

(L7) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m, \ m \ge 4: \ \mathcal{G}_{T_{11}} = \mathcal{G}_{d_{11}}$
[Definition A.32; (L1)]

(L8) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m, \ m \ge 4: \ \mathcal{G}_{T_{00}} = \mathcal{G}_{d_{00}}$
[Definition A.32; (L1)]

(L9) $\forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall t' :$
$\mathrm{ffsamp}(t', \mathcal{G}_\nu, 0)$ calls $\mathrm{ffsamp}(\mathrm{split}(t_1), \mathcal{G}_{d_{11}}, 0)$, then $\mathrm{ffsamp}(\mathrm{split}(tb'_0), \mathcal{G}_{d_{00}}, 0)$
[ffsamp (Algorithm 6), lines 17 to 34]

(L10) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall t' :$
$\mathrm{ffSampling}(t', \nu)$ calls $\mathrm{ffSampling}(\mathrm{split}(t_1), T_{11})$, then $\mathrm{ffSampling}(\mathrm{split}(tb_0), T_{00})$
[Definition A.21, items 13 to 18]

(L11) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m :\ I(\nu) = I(T_{11}) \sqcup I(T_{00})$
[Definition A.19]

(L12) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m :\ \max I(T_{11}) < \min I(T_{00})$
[Definition A.19]

(L13) $\Rightarrow\ \forall m \in \{4, 8, \ldots, n\} :\ \mathcal{P}(m/2) \Rightarrow\ \mathcal{P}(m)$
[(L5), (L7) to (L12)]

(L14) $\Rightarrow\ \mathcal{P}(n)$
[induction on m: base (L6), step (L13)]

(L15) $\Rightarrow\ \forall z\ \forall i \leq N :\ (\sigma'_i, c'_i)(z_{<i}) = (\sigma_i, c_i)(z_{<i})$
[(L14) at $\nu := T$, $t' := t$; $\mathcal{G}_T = \mathcal{G}$ (Definition A.32); $I(T) = \{1, \ldots, N\}$ (Definition A.19)]

(L16) $\Rightarrow$ the statement
[(L15)]

□

Definition G.6 (Node factor, tree map, coordinates and matrices [to table])**.** The node factor, the tree map, the coordinates and the matrices read a pair of polynomials along the tree. Let:

- $T \in \mathcal{T}_n$;
- $\nu = \mathrm{node}(l_{10};\ \cdot, \cdot) \in \mathrm{Sub}(T) \cap \mathcal{T}_m$;
- $x = (x_0, x_1) \in \mathcal{R}_m^2$;
- $T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}$, $m' = 2^{h'}$;
- $i \in I(T')$;
- $b \in \mathbb{R}^{I(T')}$.

Define:

- The split
  - $\forall a \in \mathcal{R}_m,\ m \geq 4 :\ \mathrm{split}(a) := (a_0, a_1)$ (Definition A.15);
  - $a_0 := \sum_{i<m/2} a_{[2i]} x^i$ and $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i$ (Definition A.15);
- The node factor
  - $L_\nu := \begin{pmatrix} 1 & 0 \\ l_{10} & 1 \end{pmatrix}$;
  - $xL_\nu := (x_0 + x_1 l_{10},\ x_1)$;
- The tree map
  -
$$\begin{aligned}
&\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ x \in \mathcal{R}_2 :\ x\mathcal{L}_d := x,\\
&\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}),\ x \in \mathcal{R}_2^2 :\ x\mathcal{L}_\nu := (x_1,\ x_0 + x_1 l_{10}),\\
&\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathcal{T}_m,\ m \geq 4,\ x \in \mathcal{R}_m^2 :\\
&\qquad x\mathcal{L}_\nu := (\mathrm{split}((xL_\nu)_1)\mathcal{L}_{T_{11}},\ \mathrm{split}((xL_\nu)_0)\mathcal{L}_{T_{00}})\,;
\end{aligned}$$
  - $\forall v \leq n :\ (x\mathcal{L}_T)_{2v-1} := \mathrm{Re}\,(x\mathcal{L}_T)_v$;
  - $\forall v \leq n :\ (x\mathcal{L}_T)_{2v} := \mathrm{Im}\,(x\mathcal{L}_T)_v$;
- The coordinates
  - $a := \min I(T')$;
  - $\ell_i := \lceil (i - a + 1)/2 \rceil \in \{1, \ldots, m'\}$;
  - $q_i := i - a - 2\ell_i + 2 \in \{0, 1\}$;
  - $(c_{i,1}, \ldots, c_{i,h'}) \in \{0,1\}^{h'}$, by $\ell_i - 1 = \sum_{k=1}^{h'} (1 - c_{i,k}) 2^{h'-k}$;

  - $p_i := 2^{h'-1} q_i + \sum_{k=2}^{h'} 2^{k-2} c_{i,k} \in \{0, \dots, m'-1\}$;
  - $\forall x = (x_0, x_1) \in \mathcal{R}^2_{m'} :\ x_i := (x_{c_{i,1}})_{[p_i]}$;
  - $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\}\ \forall x \in \mathcal{R}_2 :\ x_j := x_{[0]}$;
  - $x_{j+1} := x_{[1]}$ for the same d and x;
  - $x^{(b)} \in \mathcal{R}^2_{m'}$, the element with $(x^{(b)}_i)_{i \in I(T')} = b$ (Fact G.7, item 4);
  - $e^{(j)} := x^{(b)}$ at $b_j = 1$ and $b_i = 0$ for $i \neq j$;
- The matrices
  - $\forall j, i \in I(T') :\ (\mathcal{L}_{T'})_{ji} := (e^{(j)} \mathcal{L}_{T'})_i$;
  - d_i, $i \leq N$, the leaf diagonals of T (Definition A.19);
  - $D := \mathrm{diag}(d_1, \dots, d_N)$.

```
noncomputable def coeffAt {N : Nat} (f : Fin N -> Real) (p : Nat) : Real :=
  if hp : p < N then f <p, hp> else 0

def tmEll (t : Nat) : Nat := (t + 1 + 1) / 2

def tmQ (t : Nat) : Nat := t + 2 - 2 * tmEll t

def tmC (h t k : Nat) : Nat := 1 - (tmEll t - 1) / 2 ^ (h - k) % 2

def tmP (h t : Nat) : Nat := 2 ^ (h - 1) * tmQ t + Sum j in range (h - 1), 2 ^ j * tmC h t (j +
    2)

def tmCF (h t k : Nat) : Fin 2 := <tmC h t k, by unfold tmC; omega>

noncomputable def tmCoord (h : Nat) (x : Fin 2 -> Fin (2 ^ h) -> Real) (t : Nat) : Real :=
  coeffAt (x (tmCF h t 1)) (tmP h t)

noncomputable def rco {k : Nat} (T : FTree k) (x : SlotVec k x SlotVec k) (i : Nat) : Real :=
  if i % 2 = 0 then ((T.coords x).getD (i / 2) 0).re else ((T.coords x).getD (i / 2) 0).im

noncomputable def rzc {k : Nat} (T : FTree k) (x : SlotVec k x SlotVec k) (i : Nat) : Real :=
  if i % 2 = 0 then ((T.zcoords x).getD (i / 2) 0).re else ((T.zcoords x).getD (i / 2) 0).im

noncomputable def Lmat {k : Nat} (T : FTree k) (i j : Nat) : Real := rco T (unrz T (basisR j)) i

noncomputable def coords : {k : Nat} -> FTree k -> SlotVec k x SlotVec k -> List Complex
  | _, base _ _ l10, x => [x.2 0, x.1 0 + x.2 0 * l10]
  | _, node psi l10 T0 T1, x => T1.coords (splitV psi x.2) ++ T0.coords (splitV psi (x.1 + x.2
      * l10))

noncomputable def unrz {k : Nat} (T : FTree k) (r : Nat -> Real) : SlotVec k x SlotVec k :=
  unzc T (fun j => <r (2 * j), r (2 * j + 1)>)

noncomputable def basisR (j : Nat) : Nat -> Real := fun m => if m = j then 1 else 0

noncomputable def omega (m : Nat) : Complex := Complex.exp (((Real.pi / (2 * m) : Real) :
    Complex) * Complex.I)

noncomputable def zcoords : {k : Nat} -> FTree k -> SlotVec k x SlotVec k -> List Complex
  | _, base _ _ _, z => [z.2 0, z.1 0]
  | _, node psi _ T0 T1, z => T1.zcoords (splitV psi z.2) ++ T0.zcoords (splitV psi z.1)
```

Figure 49: The Lean declarations carrying Definition G.6: `coeffAt`, `tmEll`, `tmQ`, `tmC`, `tmP`, `tmCF`, `tmCoord`, `FTree.rco`, `FTree.rzc`, `FTree.Lmat`, `FTree.coords`, `FTree.unrz`, `FTree.basisR`, `omega`, `FTree.zcoords` (`DefsFacts.lean`, `Ldl.lean`, `Parseval.lean`, `TreeRec.lean`); with `SlotVec`, `FTree` of Figure 21; with `splitV` of Figure 26; Lean's symbols in ASCII.

Fact G.7 (The tree's coordinates [to table])**.** Along the tree, the real coordinates of a pair are the coefficients of its split halves, and they form a linear bijection. Let:

- $T \in \mathcal{T}_n$ (Definition A.18).

Define:

- $\mathrm{split}(a) := (a_0, a_1)$ for $a \in \mathcal{R}_m$, $m \geq 4$ (Definition A.15);
- $a_0 := \sum_{i<m/2} a_{[2i]} x^i$ and $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i$ (Definition A.15).

Then the coordinates satisfy:

1. $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T),\ I(\nu) = \{a, \dots, a+3\}\ \forall x \in \mathcal{R}_2^2 : (x_a, x_{a+1}, x_{a+2}, x_{a+3}) = ((x_1)_{[0]}, (x_1)_{[1]}, (x_0)_{[0]}, (x_0)_{[1]})$;
2. $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall x \in \mathcal{R}_m^2$:
$$(x_i)_{i \in I(T_{11})} = ((\mathrm{split}(x_1))_i)_{i \in I(T_{11})};$$
3. $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall x \in \mathcal{R}_m^2$:
$$(x_i)_{i \in I(T_{00})} = ((\mathrm{split}(x_0))_i)_{i \in I(T_{00})};$$
4. $\forall m' \in \{2, 4, \dots, n\}\ \forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'} : x \mapsto (x_i)_{i \in I(T')}$ is an $\mathbb{R}$-linear bijection $\mathcal{R}_{m'}^2 \to \mathbb{R}^{I(T')}$.

Proof.

DEFINES $\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m$, $x \in \mathcal{R}_m^2$: those of items 1 to 3, with $(T_{00}, T_{11}) = (d_{00}, d_{11})$ at $m = 2$

DEFINES $a := \min I(\nu)$ in items 1 to 3; $a := \min I(T')$ in item 4

DEFINES h' with $m = 2^{h'}$ in items 1 to 3; with $m' = 2^{h'}$ in item 4

DEFINES ℓ_i, q_i, $c_{i,k}$, p_i: the coordinates of Definition G.6 at $T' := \nu$ in items 1 to 3, at T' in item 4

DEFINES ℓ'_i, q'_i, $c'_{i,k}$, p'_i: those of Definition G.6 at $T' := T_{11}$ and at $T' := T_{00}$

DEFINES $a'_i := \min I(T_{11})$ for $i \in I(T_{11})$; $a'_i := \min I(T_{00})$ for $i \in I(T_{00})$

Proof of items 1 to 3.

(L1) $m = 2 :\ (\ell_i, q_i, c_{i,1})_{i=a}^{a+3} = ((1,0,1), (1,1,1), (2,0,0), (2,1,0))$

[$\ell_i - 1 = 1 - c_{i,1}$ (Definition G.6 at $h' = 1$)]

(L2) $m = 2 :\ \forall i \in I(\nu) :\ p_i = q_i$

[Definition G.6 at $h' = 1$]

(L3) $\Rightarrow\ m = 2 :\ (x_a, x_{a+1}, x_{a+2}, x_{a+3}) = ((x_1)_{[0]}, (x_1)_{[1]}, (x_0)_{[0]}, (x_0)_{[1]})$

[(L1), (L2); $x_i := (x_{c_{i,1}})_{[p_i]}$ (Definition G.6)]

(L4) $m \geq 4\ \forall i \in I(T_{11}) :\ \ell_i = \ell'_i$

[$I(T_{11}) = \{a, \dots, a+m-1\}$ (Definition A.19), before $I(T_{00})$ (Definition A.19); ℓ_i, ℓ'_i (the proof's block)]

(L5) $m \geq 4\ \forall i \in I(T_{11}) \sqcup I(T_{00}) :\ \ell'_i - 1 < 2^{h'-1}$

[$\ell'_i - 1 = \sum_{k=1}^{h'-1} (1 - c'_{i,k}) 2^{h'-1-k}$, $c'_{i,k} \in \{0,1\}$ (Definition G.6 at $T' := T_{11}, T_{00}$); Fact A.41, item 7]

(L6) $m \geq 4\ \forall i \in I(T_{00}) :\ \ell_i - 1 = 2^{h'-1} + \ell'_i - 1$

[$I(T_{00}) = \{a+m, \dots, a+2m-1\}$ (Definition A.19); ℓ_i, ℓ'_i (the proof's block)]

(L7) $m \geq 4\ \forall i \in I(\nu) :\ \ell_i - 1 = 2^{h'-1}(1 - c_{i,1}) + \sum_{k=2}^{h'} (1 - c_{i,k}) 2^{h'-k}$

[$\ell_i - 1 = \sum_{k=1}^{h'} (1 - c_{i,k}) 2^{h'-k}$ (Definition G.6), the term $k = 1$ apart]

(L8) $m \geq 4\ \forall i \in I(\nu) :\ \sum_{k=2}^{h'} (1 - c_{i,k}) 2^{h'-k} < 2^{h'-1}$

[$c_{i,k} \in \{0,1\}$ (Definition G.6); Fact A.41, item 7]

(L9) $\Rightarrow\ m \geq 4\ \forall i \in I(T_{11}) :\ c_{i,1} = 1$

[(L4), (L5), (L7), (L8); $c_{i,1} \in \{0,1\}$ (Definition G.6)]

(L10) $\Rightarrow\ m \geq 4\ \forall i \in I(T_{00}) :\ c_{i,1} = 0$

[(L6), (L7), (L8); $c_{i,1} \in \{0,1\}$ (Definition G.6)]

(L11) $\Rightarrow$ $m \geq 4\ \forall i \in I(T_{11}) \sqcup I(T_{00}) :\ \sum_{k=2}^{h'}(1-c_{i,k})2^{h'-k} = \ell'_i - 1$

[(L4), (L6), (L7), (L9), (L10)]

(L12) $\Rightarrow$ $m \geq 4\ \forall i \in I(T_{11}) \sqcup I(T_{00}) :\ (c'_{i,1}, \ldots, c'_{i,h'-1}) = (c_{i,2}, \ldots, c_{i,h'})$

[(L11); $\ell'_i - 1 = \sum_{k=1}^{h'-1}(1-c'_{i,k})2^{h'-1-k}$ (Definition G.6 at $T' := T_{11}, T_{00}$): the binary digits of $\ell'_i - 1$]

(L13) $m \geq 4\ \forall i \in I(T_{11}) \sqcup I(T_{00}) :\ a'_i - a \in \{0, m\}$

[a'_i (the proof's block); $\min I(T_{11}) = a$, $\min I(T_{00}) = a + m$ (Definition A.19)]

(L14) $\Rightarrow$ $m \geq 4\ \forall i \in I(T_{11}) \sqcup I(T_{00}) :\ q'_i = q_i$

[(L13); $i - a = 2(\ell_i - 1) + q_i$, $i - a'_i = 2(\ell'_i - 1) + q'_i$, $q_i, q'_i \in \{0,1\}$ (Definition G.6); m even]

(L15) $\Rightarrow$ $m \geq 4\ \forall i \in I(T_{11}) \sqcup I(T_{00}) :\ p_i = 2p'_i + c_{i,2}$

[(L12), (L14); $p_i = 2^{h'-1}q_i + \sum_{k=2}^{h'} 2^{k-2}c_{i,k}$, $p'_i = 2^{h'-2}q'_i + \sum_{k=2}^{h'-1} 2^{k-2}c'_{i,k}$ (Definition G.6)]

(L16) $\forall f \in \mathcal{R}_m\ \forall c \in \{0,1\}\ \forall p' < m/2 :\ (f_c)_{[p']} = f_{[2p'+c]}$

[$f = f_0(x^2) + x f_1(x^2)$ (split (Algorithm 2), Postcondition)]

(L17) $m \geq 4\ \forall i \in I(T_{11}) \sqcup I(T_{00}) :\ x_i = (x_{c_{i,1}})_{[2p'_i + c_{i,2}]}$

[$x_i := (x_{c_{i,1}})_{[p_i]}$ (Definition G.6); (L15)]

(L18) $\Rightarrow$ $m \geq 4\ \forall i \in I(T_{11}) \sqcup I(T_{00}) :\ x_i = ((x_{c_{i,1}})_{c_{i,2}})_{[p'_i]}$

[(L17); (L16) at $(f, c, p') := (x_{c_{i,1}}, c_{i,2}, p'_i)$]

(L19) $\Rightarrow$ $m \geq 4\ \forall i \in I(T_{11}) \sqcup I(T_{00}) :\ x_i = (\mathrm{split}(x_{c_{i,1}}))_i$

[(L18); (L12); $(\mathrm{split}(x_{c_{i,1}}))_i = ((\mathrm{split}(x_{c_{i,1}}))_{c'_{i,1}})_{[p'_i]}$ (Definition G.6) at T_{11}, T_{00}]

(L20) $\Rightarrow$ item 1

[(L3) at $m = 2$]

(L21) $\Rightarrow$ item 2

[(L9), (L19) at $m \geq 4$]

(L22) $\Rightarrow$ item 3

[(L10), (L19) at $m \geq 4$]

□ (items 1 to 3)

Proof of item 4.

(L23) $\forall i \in I(T') :\ i - a = 2(\ell_i - 1) + q_i$

[Definition G.6]

(L24) $\forall i \in I(T') :\ \ell_i - 1 = \sum_{k=1}^{h'}(1-c_{i,k})2^{h'-k}$

[Definition G.6]

(L25) $\Rightarrow$ $i \mapsto (c_{i,1}, \ldots, c_{i,h'}, q_i)$ is a bijection $I(T') \to \{0,1\}^{h'+1}$

[(L23), (L24): the binary digits of $i - a \in \{0, \ldots, 2m' - 1\}$]

(L26) $(c_{i,2}, \ldots, c_{i,h'}, q_i) \mapsto p_i$ is a bijection $\{0,1\}^{h'} \to \{0, \ldots, m' - 1\}$

[$p_i = 2^{h'-1}q_i + \sum_{k=2}^{h'} 2^{k-2}c_{i,k}$ (Definition G.6): the binary digits of p_i]

(L27) $\Rightarrow$ $i \mapsto (c_{i,1}, p_i)$ is a bijection $I(T') \to \{0,1\} \times \{0, \ldots, m' - 1\}$

[(L25), (L26)]

(L28) $\forall c \in \{0,1\}\ \forall p < m' :\ x \mapsto (x_c)_{[p]}$ is $\mathbb{R}$-linear

[$\mathcal{R}_{m'}$ an $\mathbb{R}$-vector space with the coefficients as coordinates (Definition A.1)]

(L29) $\Rightarrow$ item 4

[(L27), (L28); $x_i = (x_{c_{i,1}})_{[p_i]}$ (Definition G.6)]

□ (item 4)

Fact G.8 (Linearity of the tree map [to table])**.** The tree map of every subtree is $\mathbb{R}$-linear. Let:

- $T \in \mathcal{T}_n$ (Definition A.18).

Then the tree map is linear:

$$\forall m' \in \{2, 4, \ldots, n\}\ \forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}\ \forall x, y \in \mathcal{R}_{m'}^2\ \forall c \in \mathbb{R} :\ (x + cy)\mathcal{L}_{T'} = x\mathcal{L}_{T'} + c\, y\mathcal{L}_{T'}.$$

Proof. (L1) $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T)\ \forall x :\ x\mathcal{L}_\nu = (x_1,\ x_0 + x_1 l_{10})$

[Definition G.6]

(L2) $\Rightarrow$ $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T)\ \forall x, y\ \forall c:\ (x + cy)\mathcal{L}_\nu = x\mathcal{L}_\nu + c\, y\mathcal{L}_\nu$

[(L1); $\mathcal{R}_2$ an $\mathbb{R}$-algebra (Definition A.1)]

(L3) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall x:\ x\mathcal{L}_\nu = (\mathrm{split}(x_1)\mathcal{L}_{T_{11}},\ \mathrm{split}(x_0 + x_1 l_{10})\mathcal{L}_{T_{00}})$

[Definition G.6]

(L4) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:$
$[\forall T' \in \{T_{00}, T_{11}\}:\ y \mapsto y\mathcal{L}_{T'}\ \mathbb{R}\text{-linear}] \Rightarrow\ \forall x, y\ \forall c:\ (x + cy)\mathcal{L}_\nu = x\mathcal{L}_\nu + c\, y\mathcal{L}_\nu$

[(L3); Fact A.42, item 4; $\mathcal{R}_m$ an $\mathbb{R}$-algebra (Definition A.1)]

(L5) $\Rightarrow$ the statement

[induction on the depth from the leaves: base (L2), step (L4)]

□

Definition G.9 (Samples, leaf product and output measures [to table])**.** The sampler's samples at a subtree have a leaf product and an output measure. Let:

- $T \in \mathcal{T}_n$;
- $t \in \mathcal{R}_n^2$;
- $s > 0$;
- $T' \in \mathrm{Sub}(T)$;
- t', a center at T';
- $A \subseteq \mathbb{Z}^{I(T')}$.

Define:

- $(\sigma_i, c_i) := (\sigma_i, c_i)(t, z_{<i})$, $i \leq N$, the leaf parameters of ffSampling(t, T) (Definition A.21, items 1 to 3);
- z_i, $i \leq N$, the samples of ffSampling(t, T) (Definition A.21, item 3);
- $z := (z_i)_{i \leq N} \in \mathbb{Z}^N$;
- $z_{T'} := (z_i)_{i \in I(T')}$;
- $t_{T'}$, the center of the call of ffSampling (Definition A.21) at T' (items 6, 7, 10, 13, 17);
- $\varrho_{T'}(t_{T'}, z_{T'}) := \prod_{i \in I(T')} \rho_{\sigma_i, c_i}(z_i)$;
- $Q_{T', t'}(A) := \Pr[z_{T'} \in A]$ at $t_{T'} = t'$.

```
noncomputable def FTree.Qset {k : Nat} (s : Real) (T : FTree k) (t : SlotVec k x SlotVec k)
    (A : Finset (SlotVec k x SlotVec k)) : Real :=
  Sum z in A, T.outputProb s t z

noncomputable def outputProb (s : Real) : {k : Nat} -> FTree k -> SlotVec k x SlotVec k
    -> SlotVec k x SlotVec k -> Real
  | _, base d0 d1 l10, t, z =>
      rho (s / Real.sqrt d1) ((t.2 0).re - (z.2 0).re) / rhoZ (s / Real.sqrt d1) (t.2 0).re
        * (rho (s / Real.sqrt d1) ((t.2 0).im - (z.2 0).im) / rhoZ (s / Real.sqrt d1) (t.2
            0).im)
        * (rho (s / Real.sqrt d0) ((t.1 0 + (t.2 0 - z.2 0) * l10).re - (z.1 0).re)
              / rhoZ (s / Real.sqrt d0) (t.1 0 + (t.2 0 - z.2 0) * l10).re
            * (rho (s / Real.sqrt d0) ((t.1 0 + (t.2 0 - z.2 0) * l10).im - (z.1 0).im)
              / rhoZ (s / Real.sqrt d0) (t.1 0 + (t.2 0 - z.2 0) * l10).im))
  | _, node psi l10 T0 T1, t, z =>
      outputProb s T1 (splitV psi t.2) (splitV psi z.2)
        * outputProb s T0 (splitV psi (t.1 + (t.2 - z.2) * l10)) (splitV psi z.1)
```

Figure 50: The Lean declarations carrying Definition G.9: `FTree.Qset`, `FTree.outputProb` (`Integrality.lean`, `Output.lean`); with `SlotVec`, `FTree` of Figure 21; with `splitV` of Figure 26; with `rhoZ`, `rho` of Figure 27; Lean's symbols in ASCII.

Lemma G.10 (The merged vector in the tree's coordinates [to table])**.** *Down the tree, the sampler's merged values split into the children's, and at the root they are the sample in the tree's coordinates. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $t \in \mathcal{R}_n^2$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*.*

Define:

- $\forall T' \in \mathrm{Sub}(T):\ \hat{z}_{T'}$*, that of* ffSampling *(Definition A.21) at* (t, T) *with the leaf samples* z *(Definition G.9);*
- $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ z_0, z_1$*, those of* ffSampling *(Definition A.21) at* (t, T) *with the leaf samples* z *(Definition G.9);*
- $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathcal{T}_2:\ z_0 := \hat{z}_{T_{00}},\ z_1 := \hat{z}_{T_{11}}$*;*
- $\forall T' \in \mathrm{Sub}(T):\ z_{T'} := (z_i)_{i \in I(T')}$ *(Definition G.9);*
- $\forall T' \in \mathrm{Sub}(T):\ I(T')$*, that of Definition A.19;*
- $\forall a \in \mathcal{R}_m,\ m \geq 4:\ \mathrm{split}(a) := (a_0, a_1)$ *(Definition A.15);*
- $a_0 := \sum_{i<m/2} a_{[2i]} x^i$ *and* $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i$ *(Definition A.15);*
- $x^{(z)} \in \mathcal{R}_n^2$*, the element with* $(x_i^{(z)})_{i \leq N} = z$ *(Definition G.6);*
- x_i*, the coordinate of* x *at* i *(Definition G.6).*

Then the merged values split, and the root's are the sample:

1. $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ \hat{z}_{T_{11}} = \mathrm{split}(z_1)$*;*
2. $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ \hat{z}_{T_{00}} = \mathrm{split}(z_0)$*;*
3. $((\hat{z}_T)_i)_{i \leq N} = z$*;*
4. $\hat{z}_T = x^{(z)}$*.*

Proof. Proof of items 1 and 2.

(L1) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ \hat{z}_{T_{11}} = \mathrm{split}(z_1)$
[Definition A.21, item 15: $z_1 = \mathrm{merge}(\hat{z}_{T_{11}})$; $\mathrm{split}(\mathrm{merge}(y)) = y$ (Fact A.42, item 5)]

(L2) $\Rightarrow$ item 1
[(L1)]

(L3) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ \hat{z}_{T_{00}} = \mathrm{split}(z_0)$
[Definition A.21, item 19: $z_0 = \mathrm{merge}(\hat{z}_{T_{00}})$; $\mathrm{split}(\mathrm{merge}(y)) = y$ (Fact A.42, item 5)]

(L4) $\Rightarrow$ item 2
[(L3)]

□ (items 1 and 2)

Proof of items 3 and 4.

(L5) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\}:\ \hat{z}_d = z_j + i z_{j+1}$
[Definition A.21, item 4]

(L6) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\}:\ ((\hat{z}_d)_i)_{i \in I(d)} = (z_j, z_{j+1})$
[(L5); Definition G.6: $x_j = x_{[0]}$, $x_{j+1} = x_{[1]}$ on $\mathcal{R}_2$]

(L7) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T):\ \hat{z}_\nu = (z_0, z_1)$
[Definition A.21, item 12 at $m = 2$, item 20 at $m \geq 4$]

(L8) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T):\ [\forall T' \in \{T_{00}, T_{11}\}:\ ((\hat{z}_{T'})_i)_{i \in I(T')} = z_{T'}] \Rightarrow ((\hat{z}_\nu)_i)_{i \in I(\nu)} = z_\nu$
[(L1), (L3), (L7); Fact G.7, items 1 to 3; $z_{T'}$ (Definition G.9)]

(L9) $\Rightarrow\ ((\hat{z}_T)_i)_{i \leq N} = z$
[induction on the depth from the leaves: base (L6), step (L8); $I(T) = \{1, \ldots, N\}$ (Definition A.19)]

(L10) $\Rightarrow$ item 3
[(L9)]

(L11) $\Rightarrow$ $\hat{z}_T = x^{(z)}$

[(L9); $x^{(z)}$ (Definition G.6); Fact G.7, item 4]

(L12) $\Rightarrow$ item 4

[(L11)]

□ (items 3 and 4)

Lemma G.11 (Triangularity of the tree map [to table])**.** *Each real coordinate of the tree map is the input's coordinate at the same position plus a combination of the input's coordinates at the earlier positions. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18).*

Define:

- $\mathcal{L}_T$*, the tree map at* T*, and* x_i*, the coordinate of* x *at* i *(Definition G.6);*
- $(x\mathcal{L}_T)_{2v-1} := \mathrm{Re}\,(x\mathcal{L}_T)_v$ *and* $(x\mathcal{L}_T)_{2v} := \mathrm{Im}\,(x\mathcal{L}_T)_v$ *for* $v \le n$ *(Definition G.6);*
- $\forall j, i \le N:\ e^{(j)}_i := [i = j]$*,* $e^{(j)} \in \mathcal{R}_n^2$ *(Definition G.6);*
- $\forall j, i \le N:\ (\mathcal{L}_T)_{ji} := (e^{(j)}\mathcal{L}_T)_i$ *(Definition G.6).*

Then

$$\forall x \in \mathcal{R}_n \times \mathcal{R}_n\ \forall i \le N: \quad (x\mathcal{L}_T)_i = x_i + \sum_{j<i} x_j (\mathcal{L}_T)_{ji}.$$

Proof.

DEFINES $\mathrm{Sub}(d) = \{d\}$, $d \in \mathbb{R}$, and $\mathrm{Sub}(\nu) = \{\nu\} \cup \mathrm{Sub}(L(\nu)) \cup \mathrm{Sub}(R(\nu))$ (Definition A.18)

DEFINES $I(T')$, $T' \in \mathrm{Sub}(T)$, that of Definition A.19

DEFINES $\mathcal{L}_{T'}$, $(x\mathcal{L}_{T'})_i$ and $(\mathcal{L}_{T'})_{ji}$, $T' \in \mathrm{Sub}(T)$, those of Definition G.6

DEFINES $L_\nu := \begin{pmatrix} 1 & 0 \\ l_{10} & 1 \end{pmatrix}$, $\nu \in \mathrm{Sub}(T)$ (Definition G.6)

(L1) $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T)\ \forall x \in \mathcal{R}_2^2:\ x\mathcal{L}_\nu = (x_1,\ x_0 + x_1 l_{10})$

[Definition G.6]

(L2) $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T),\ a = \min I(\nu)\ \forall x \in \mathcal{R}_2^2:\ (x_a, x_{a+1}, x_{a+2}, x_{a+3}) = ((x_1)_{[0]}, (x_1)_{[1]}, (x_0)_{[0]}, (x_0)_{[1]})$

[Fact G.7, item 1]

(L3) $\forall l_{10} \in \mathcal{R}_2:\ x_1 \mapsto x_1 l_{10}$ is $\mathbb{R}$-linear on $\mathcal{R}_2$

[$\mathcal{R}_2$ an $\mathbb{R}$-algebra (Definition A.1)]

(L4) $\Rightarrow$ $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T),\ a = \min I(\nu)\ \forall x\ \forall i \in \{a, a+1\}:\ (x\mathcal{L}_\nu)_i = x_i$

[(L1), (L2)]

(L5) $\Rightarrow$ $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T),\ a = \min I(\nu)\ \forall x\ \forall i \in \{a+2, a+3\}:\ (x\mathcal{L}_\nu)_i = x_i + \sum_{j \in \{a, a+1\}} x_j (\mathcal{L}_\nu)_{ji}$

[(L1), (L2), (L3); $(\mathcal{L}_\nu)_{ji}$ (the proof's block)]

(L6) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \ge 4\ \forall x \in \mathcal{R}_m^2:$
$x\mathcal{L}_\nu = (\mathrm{split}(x_1)\mathcal{L}_{T_{11}},\ \mathrm{split}(x_0 + x_1 l_{10})\mathcal{L}_{T_{00}})$

[Definition G.6: $xL_\nu = (x_0 + x_1 l_{10},\ x_1)$]

(L7) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \ge 4\ \forall x:\ \mathrm{split}(x_0 + x_1 l_{10}) = \mathrm{split}(x_0) + \mathrm{split}(x_1 l_{10})$

[Fact A.42, item 4]

(L8) $\forall T' \in \{T_{00}, T_{11}\}:\ y \mapsto y\mathcal{L}_{T'}$ is $\mathbb{R}$-linear

[Fact G.8 at T']

(L9) $\Rightarrow$ $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \ge 4\ \forall x:$
$x\mathcal{L}_\nu = (\mathrm{split}(x_1)\mathcal{L}_{T_{11}},\ \mathrm{split}(x_0)\mathcal{L}_{T_{00}} + \mathrm{split}(x_1 l_{10})\mathcal{L}_{T_{00}})$

[(L6), (L7), (L8)]

(L10) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \ge 4\ \forall x:\ ((\mathrm{split}(x_1))_i)_{i \in I(T_{11})} = (x_i)_{i \in I(T_{11})}$

[Fact G.7, item 2]

(L11) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall x:\ ((\mathrm{split}(x_0))_i)_{i \in I(T_{00})} = (x_i)_{i \in I(T_{00})}$
[Fact G.7, item 3]

(L12) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:$

$$\Big[\forall T' \in \{T_{00}, T_{11}\}\ \forall y\ \forall i \in I(T'):\ (y\mathcal{L}_{T'})_i = y_i + \sum_{j \in I(T'),\ j<i} y_j (\mathcal{L}_{T'})_{ji}\Big] \Rightarrow$$

$$\forall x\ \forall i \in I(T_{11}):\ (\mathrm{split}(x_1)\mathcal{L}_{T_{11}})_i = x_i + \sum_{j \in I(T_{11}),\ j<i} x_j (\mathcal{L}_{T_{11}})_{ji}$$

[the bracket at $T' := T_{11}$, $y := \mathrm{split}(x_1)$; (L10)]

(L13) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:$

$$[\text{the bracket of (L12)}] \Rightarrow\ \forall x\ \forall i \in I(T_{00}):\ (\mathrm{split}(x_0)\mathcal{L}_{T_{00}})_i = x_i + \sum_{j \in I(T_{00}),\ j<i} x_j (\mathcal{L}_{T_{00}})_{ji}$$

[the bracket at $T' := T_{00}$, $y := \mathrm{split}(x_0)$; (L11)]

(L14) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ x_1 \mapsto (x_j)_{j \in I(T_{11})}$ is a bijection $\mathcal{R}_m \to \mathbb{R}^{I(T_{11})}$
[(L10); Fact A.42, item 4: $\mathrm{merge}(\mathrm{split}(f)) = f$; Fact G.7, item 4, at T_{11}]

(L15) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ x_1 \mapsto \mathrm{split}(x_1 l_{10})\mathcal{L}_{T_{00}}$ is $\mathbb{R}$-linear
[(L3); Fact A.42, item 4; (L8) at $T' := T_{00}$]

(L16) $\Rightarrow\ \forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall x\ \forall i \in I(T_{00}):\ (\mathrm{split}(x_1 l_{10})\mathcal{L}_{T_{00}})_i = \sum_{j \in I(T_{11})} x_j (\mathcal{L}_\nu)_{ji}$
[(L9), (L14), (L15); $(\mathcal{L}_\nu)_{ji} = (e^{(j)}\mathcal{L}_\nu)_i$ (Definition G.6)]

(L17) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall i, j \in I(T_{11}):\ (\mathcal{L}_\nu)_{ji} = (\mathcal{L}_{T_{11}})_{ji}$
[(L9), (L10); $(\mathcal{L}_\nu)_{ji}$ (Definition G.6)]

(L18) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall i, j \in I(T_{00}):\ (\mathcal{L}_\nu)_{ji} = (\mathcal{L}_{T_{00}})_{ji}$
[(L9), (L11); $(\mathcal{L}_\nu)_{ji}$ (Definition G.6)]

(L19) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m:\ \forall i \in I(T_{11})\ \forall i' \in I(T_{00}):\ i < i'$
[Definition A.19]

(L20) $\Rightarrow\ \forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ [\text{the bracket of (L12)}] \Rightarrow\ \forall x\ \forall i \in I(\nu):\ (x\mathcal{L}_\nu)_i = x_i + \sum_{j \in I(\nu),\ j<i} x_j (\mathcal{L}_\nu)_{ji}$
[(L9), (L12), (L13), (L16), (L17), (L18), (L19)]

(L21) $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T),\ a = \min I(\nu)\ \forall x\ \forall i \in I(\nu):\ (x\mathcal{L}_\nu)_i = x_i + \sum_{j \in I(\nu),\ j<i} x_j (\mathcal{L}_\nu)_{ji}$
[(L4), (L5), each also at $x := e^{(j)}$; $(\mathcal{L}_\nu)_{ji} = (e^{(j)}\mathcal{L}_\nu)_i$ (Definition G.6); $I(\nu) = \{a, \ldots, a+3\}$ (Definition A.19)]

(L22) $\Rightarrow\ \forall x \in \mathcal{R}_n \times \mathcal{R}_n\ \forall i \leq N:\ (x\mathcal{L}_T)_i = x_i + \sum_{j<i} x_j (\mathcal{L}_T)_{ji}$
[induction on the depth from the leaves: base (L21), step (L20); $I(T) = \{1, \ldots, N\}$ (Definition A.19)]

(L23) $\Rightarrow$ the statement
[(L22)]

□

Fact G.12 (The output measure of the code's recursion [to table])**.** Over $\mathbb{R}$, the code's recursion outputs each sample vector with the probability the sampler outputs it on the tree of the same Gram matrix. Let:

- $\mathcal{G} \in \mathrm{Gram}_n$ (Definition A.14);
- $t \in \mathcal{R}_n^2$;
- $s > 0$, the standard deviation parameter of ffSampling (Definition A.21).

Define:

- $Q'_{\mathcal{G},t}(A) := \Pr[\mathrm{ffsamp}(t, \mathcal{G}) \in A]$ for $A \subseteq \mathbb{Z}^N$ (Definition A.23 at $(\mathcal{G}, t, s)$).

Assume:

(A1) `INV_SIGMA` $= 1/s$ in ffsamp (Algorithm 6) over $\mathbb{R}$.

Then

$$\forall z \in \mathbb{Z}^N : \quad Q'_{\mathcal{G},t}(\{z\}) = \Pr[\text{ffSampling}(t, \text{ffLDL}^\dagger(\mathcal{G})) = z] \text{ over } \mathbb{R}.$$

Proof.

DEFINES (σ_i, c_i), (σ'_i, c'_i), $i \le N$: those of Fact G.5

(L1) $\forall z :\ \Pr[\text{ffsamp}(t, \mathcal{G}, 0) = z] = \prod_{i \le N} D_{\mathbb{Z}, \sigma'_i, c'_i}(z_i)$
[Fact A.45, item 1, over $z_1, \ldots, z_N$; $z_i \leftarrow D_{\mathbb{Z}, \sigma'_i, c'_i}$ (deepest (Algorithm 7), lines 1 to 18, over $\mathbb{R}$)]

(L2) $\forall z :\ \Pr[\text{ffSampling}(t, \text{ffLDL}^\dagger(\mathcal{G})) = z] = \prod_{i \le N} D_{\mathbb{Z}, \sigma_i, c_i}(z_i)$
[Fact A.45, item 1; $z_i \leftarrow D_{\mathbb{Z}, \sigma_i, c_i}$ (Definition A.21, item 3)]

(L3) $\forall z\ \forall i \le N :\ (\sigma'_i, c'_i) = (\sigma_i, c_i)$
[Fact G.5 at $(\mathcal{G}, t, s)$; $\texttt{INV_SIGMA} = 1/s$ (assumption A1)]

(L4) $\Rightarrow\ \forall z :\ \Pr[\text{ffsamp}(t, \mathcal{G}, 0) = z] = \Pr[\text{ffSampling}(t, \text{ffLDL}^\dagger(\mathcal{G})) = z]$
[(L1), (L2), (L3)]

(L5) $\forall z :\ Q'_{\mathcal{G},t}(\{z\}) = \Pr[\text{ffsamp}(t, \mathcal{G}, 0) = z]$
[$Q'_{\mathcal{G},t}$, ffsamp (Definition A.23, at $\texttt{INV_SIGMA} := 1/s$: assumption A1)]

(L6) $\Rightarrow$ the statement
[(L4), (L5)]

□

G.3 Elementary bounds under a realization

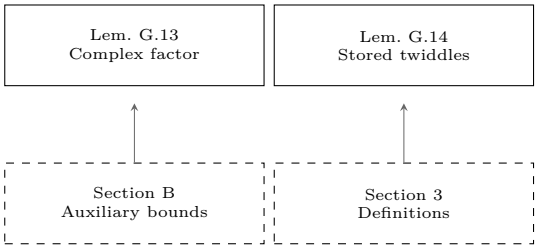


Figure 51: Dependencies, Section G.3.

Structure. This subsection states the constants c and k of each routine of $\text{ffSampling}^{\mathcal{F}}$. Table 20 lists the constants; Lemma G.14 states the perturbation of the stored twiddles; Section G.3.1 the two-norm in FFT form; Section G.3.2 the split and the merge; Section G.3.3 the center update and the leaf standard deviation; Section G.3.4 the Gram matrix; Section G.3.5 the $LDL^\dagger$ step. Every operation of the sampler returns, on a value x of $C_{\mathcal{F}}$, a value $\widetilde{x}$ with $\widetilde{x}\ \mathcal{I}\ (c^{\pm}, (k\zeta)^{\pm})\ x$.

k_B	$\sqrt{2}(3+2u)$	Complex product
c_{split}	$(1+u)\left(1+u+\sqrt{2}\zeta\right)\left(1+\sqrt{2}u(2+u)\right)-1$	Split
k_D	$\frac{\sqrt{2}}{2}\left(1+u+\sqrt{2}\zeta\right)\left(1+\sqrt{2}u(2+u)\right)+k_B$	Split
c_{merge}	$u+(1+u)\left(\left(1+u+\sqrt{2}\zeta\right)\left(1+\sqrt{2}u(2+u)\right)-1\right)$	Merge
k_E	$2\sqrt{2}\left((3+2u)(1+u)+1\right)$	Merge
e_0	$(1+u)\left(1+\sqrt{2}u(2+u)\right)-1$	Center update
k_I	$\left(\sqrt{2}\lvert l_{10}\rvert\left(1+\sqrt{2}u(2+u)\right)+k_B\right)(1+u)+\sqrt{2}$	Center update
k_J	$\left(\lvert c_n\rvert+\sqrt{\tilde{d}_{11}}\right)(1+u)^2+(1+u)\zeta+1$	Leaf standard deviation
R_{h-1}	$(1+c_{\text{merge}})^{h-1}-1$	FFT image
A_{j+1}	$\sqrt{2}(1+c_{\text{merge}})A_j+k_E\zeta\sqrt{P},\ A_0=0$	FFT image
k_H	$4(1+u)^2+2(1+u)+1$	Gram diagonal
k'_H	$\sqrt{2}\left(2(3+2u)(1+u)+1\right)$	Gram off-diagonal

Table 20: The constants of the bounds of Section G.3.

A pair of factors read as one. Lemma G.13 reads a pair of components scaled by two factors near 1 as one factor, the form the proofs below take.

Lemma G.13 (Two real scalings as one complex factor [to table])**.** *Scaling the real and the imaginary part of a complex value by two real factors, each within c of 1, multiplies the value by one complex factor within c of 1. Let:*

- $c \in \mathbb{R}$;
- $x \in \mathbb{C}$, *written* $x =: x_r + ix_i$ *with* $x_r, x_i \in \mathbb{R}$;
- $P_1, P_2 \in \mathbb{R}$.

Assume:

(A1) $|P_1 - 1| \le c$;

(A2) $|P_2 - 1| \le c$.

Then

$$\exists\, \delta \in \mathbb{C},\ |\delta| \le c: \quad x_r P_1 + i x_i P_2 = x(1+\delta).$$

Proof. (L1) $x_r P_1 + i x_i P_2 - x = x_r(P_1 - 1) + i x_i (P_2 - 1)$

[$x = x_r + ix_i$ (the statement); expand]

(L2) $\Rightarrow\ |x_r P_1 + i x_i P_2 - x|^2 = x_r^2 (P_1-1)^2 + x_i^2 (P_2-1)^2$

[(L1); Fact A.41, item 1: $|a+ib|^2 = a^2+b^2$]

(L3) $x_r^2(P_1-1)^2 + x_i^2(P_2-1)^2 \le c^2(x_r^2 + x_i^2)$

[assumptions A1, A2; Fact A.41, item 5: $t \mapsto t^2$ nondecreasing on $[0,\infty)$]

(L4) $c^2(x_r^2 + x_i^2) = c^2|x|^2$

[Fact A.41, item 1: $|a+ib|^2 = a^2+b^2$]

(L5) $\Rightarrow\ |x_r P_1 + i x_i P_2 - x| \le c|x|$

[(L2), (L3), (L4); Fact A.41, item 5: $t \mapsto \sqrt{t}$ nondecreasing]

Lemma B.1	This proof
Shared: x, c	
Shared: $x \in \mathbb{C}$	
(I1) p	$x_r P_1 + i x_i P_2$
$c \ge 0$	Assumption A1
$p \in \mathbb{C}$	$x_r, x_i, P_1, P_2 \in \mathbb{R}$ (the statement)
$\lvert p - x\rvert \le c\lvert x\rvert$	(L5)
Its conclusion: $\lvert\delta(p,x)\rvert \le c,\ p = x(1+\delta(p,x))$	

(L6) $\Rightarrow\ \exists\,\delta\in\mathbb{C},\ |\delta|\le c:\ x_rP_1+ix_iP_2=x(1+\delta)$

[(I1)]

(L7) $\Rightarrow$ the statement

[(L6)]

□

Lemma G.14 (Perturbation of the stored twiddles [to table])**.** *Each stored root of unity is the root rounded once per component, so it lies within the realization's rounding of the root: the fixed-point signer meets Definition A.8, item 1. Let:*

- $k\in\{1,\dots,2^{10}-1\}$.

Define:

- $\forall j<10:\ k_j:=\lfloor k/2^j\rfloor \bmod 2$;
- $\mathrm{rev}_{10}(k):=\sum_{j<10}k_j2^{9-j}$;
- $\psi_k:=\exp(i\pi\,\mathrm{rev}_{10}(k)/1024)$;
- $\tilde{\psi}_k:=\mathtt{GM}[k]$, *the stored root [L0: fxp/fxp_consts.h:6].*

Measured:

- $\tilde{\psi}_k$ *in* `fxp/`, *the 2048 words [L0: fxp/gen_consts.py:145], equal the core's [gate: fxp/gate_c_functions_vs_core].*

Then

$$\tilde{\psi}_k\ \mathcal{I}\left(u^{\pm}+\sqrt{2}\zeta^{\pm},0\right)\ \psi_k.$$

Proof.

DEFINES $c_k:=\cos(\pi\,\mathrm{rev}_{10}(k)/1024)$
DEFINES $s_k:=\sin(\pi\,\mathrm{rev}_{10}(k)/1024)$
COMPUTES $\widetilde{c}_k:=\mathrm{Re}\,\widetilde{\psi}_k$
COMPUTES $\widetilde{s}_k:=\mathrm{Im}\,\widetilde{\psi}_k$

(L1) $\psi_k=c_k+is_k$

[ψ_k (the statement); Fact A.41, item 12: $e^{i\theta}=\cos\theta+i\sin\theta$]

(L2) $\widetilde{c}_k=\mathrm{RN}(c_k)$

[at $\mathcal{F}_{\mathrm{fx}}$, the statement's measured row, the word nearest to c_k [L0: fxp/gen_consts.py:145]]

(L3) $\widetilde{s}_k=\mathrm{RN}(s_k)$

[at $\mathcal{F}_{\mathrm{fx}}$, the statement's measured row, the word nearest to s_k [L0: fxp/gen_consts.py:145]]

(L4) $\Rightarrow\ \exists\,u_c,\zeta_c\in\mathbb{R},\ |u_c|\le u,\ |\zeta_c|\le\zeta:\ \widetilde{c}_k=c_k(1+u_c)+\zeta_c$

[(L2); Definition A.4: $\mathrm{fl}(c)=c(1+u_\circ)+\zeta_\circ$ for a stored constant c]

(L5) $\Rightarrow\ \exists\,u_s,\zeta_s\in\mathbb{R},\ |u_s|\le u,\ |\zeta_s|\le\zeta:\ \widetilde{s}_k=s_k(1+u_s)+\zeta_s$

[(L3); Definition A.4: $\mathrm{fl}(c)=c(1+u_\circ)+\zeta_\circ$ for a stored constant c]

(L6) $|\psi_k|=1$

[(L1); Fact A.41, item 12: $\cos^2\theta+\sin^2\theta=1$; Fact A.41, item 1: $|a+ib|^2=a^2+b^2$]

Lemma B.2, item 4	This proof
Shared: u,ζ	
a	ψ_k
$\tilde{a}$	$\widetilde{\psi}_k$
(I1) $a\in\mathbb{C}$	(L1)
$\lvert a\rvert=1$	(L6)
$\tilde{a}\in C_{\mathcal{F}}$	(L2), (L3); $\widetilde{c}_k$, $\widetilde{s}_k$ (the proof's block)
$\tilde{a}_r\ \mathcal{I}\,(u^{\pm},\zeta^{\pm})\ a_r$	(L1), (L4); $\widetilde{c}_k$ (the proof's block)
$\tilde{a}_i\ \mathcal{I}\,(u^{\pm},\zeta^{\pm})\ a_i$	(L1), (L5); $\widetilde{s}_k$ (the proof's block)
Its item 4: $\tilde{a}\ \mathcal{I}\left(u^{\pm}+\sqrt{2}\,\zeta^{\pm},0\right)\ a$	

(L7) $\Rightarrow\ \widetilde{\psi}_k\ \mathcal{I}\left(u^{\pm}+\sqrt{2}\,\zeta^{\pm},0\right)\ \psi_k$

[(I1)]

(L8) $\Rightarrow$ the statement

[(L7)]

□

G.3.1 The two-norm in FFT form

Proposition G.15 (Parseval's identity [to table])**.** *The squared coefficient norm of a real polynomial f is $2/n$ times the sum of $|f(\psi_k)|^2$ over the roots ψ_k of x^n+1 with positive imaginary part. Let:*

- $n = 2^h$ *with* $h \geq 1$*;*
- $f = \sum_{p<n} f_{[p]} x^p \in \mathbb{R}[x]/(x^n+1)$.

Define:

- $f(\psi) := \sum_{p<n} f_{[p]} \psi^p$, $\psi \in \mathbb{C}$*;*
- $\{\psi_k : k < n/2\} = \{\psi \in \mathbb{C} : \psi^n = -1,\ \operatorname{Im}\psi > 0\}$.

Then

$$\sum_{p<n} f_{[p]}^2 = \frac{2}{n} \sum_{k<n/2} |f(\psi_k)|^2.$$

Proof.

DEFINES $\omega := e^{i\pi/n}$

DEFINES $\xi_j := \omega^{2j+1}$, $j < n$

(L1) $\omega^n = e^{i\pi}$

[ω (the proof's block); Fact A.41, item 12: $e^x e^y = e^{x+y}$]

(L2) $e^{i\pi} = -1$

[Fact A.41, item 12]

(L3) $\forall j < n :\ \xi_j^n = -1$

[Fact A.43, item 1, at $m := n$; ξ_j (the proof's block)]

(L4) $\forall m,\ 0 < |m| < n :\ \omega^{2m} = e^{2\pi i m/n}$

[ω (the proof's block); Fact A.41, item 12: $e^x e^y = e^{x+y}$]

(L5) $\forall m,\ 0 < |m| < n :\ e^{2\pi i m/n} \neq 1$

[$m/n \notin \mathbb{Z}$; Fact A.41, item 12: $e^{i\theta} = \cos\theta + i\sin\theta$]

(L6) $\forall m :\ (\omega^{2m})^n = 1$

[$(\omega^{2m})^n = (\omega^n)^{2m}$; (L1), (L2)]

(L7) $\forall m,\ 0 < |m| < n :\ \sum_{j<n} \xi_j^m = \omega^m \sum_{j<n} (\omega^{2m})^j$

[ξ_j (the proof's block)]

(L8) $\forall m,\ 0 < |m| < n :\ \omega^m \sum_{j<n} (\omega^{2m})^j = 0$

[Fact A.41, item 7, at $\omega^{2m} \neq 1$ (L4), (L5); (L6)]

(L9) $\forall j < n :\ |f(\xi_j)|^2 = \sum_{p,p'<n} f_{[p]} f_{[p']} \xi_j^p \operatorname{conj} \xi_j^{p'}$

[Fact A.41, item 1: $x \operatorname{conj} x = |x|^2$; $f_{[p]} \in \mathbb{R}$]

(L10) $\forall j < n :\ \operatorname{conj} \xi_j = \xi_j^{-1}$

[(L3); Fact A.42, item 1: $\psi \operatorname{conj} \psi = 1$]

(L11) $\Rightarrow\ \sum_{j<n} |f(\xi_j)|^2 = \sum_{p,p'<n} f_{[p]} f_{[p']} \sum_{j<n} \xi_j^{p-p'}$

[(L9), (L10)]

(L12) $\forall p < n :\ \sum_{j<n} \xi_j^{p-p} = n$

[$\xi_j^0 = 1$]

(L13) $\Rightarrow\ \sum_{j<n} |f(\xi_j)|^2 = n \sum_{p<n} f_{[p]}^2$

[(L11); (L7), (L8) at $m := p - p' \neq 0$; (L12) at $p = p'$]

(L14) $\forall \psi,\ \psi^n = -1 :\ |f(\operatorname{conj}\psi)| = |f(\psi)|$

[Fact A.42, item 2; Fact A.41, item 1: $|\operatorname{conj} x| = |x|$]

(L15) $\Rightarrow\ \sum_{p<n} f_{[p]}^2 = \frac{2}{n} \sum_{k<n/2} |f(\psi_k)|^2$

[(L13); Fact A.43, item 6, at $m := n$, $g := |f|^2$, invariant by (L14); $Z_n = \{\xi_j : j < n\}$ (Fact A.43, item 1)]

(L16) $\Rightarrow$ the statement

[(L15)]

□

G.3.2 The split and the merge

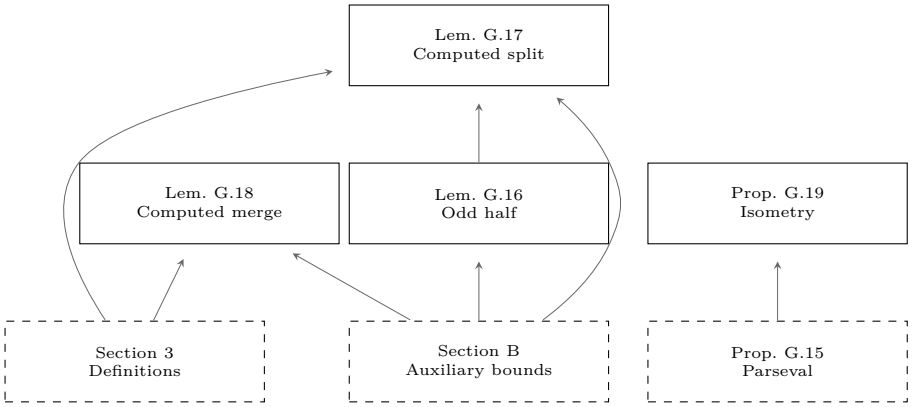


Figure 52: Dependencies, Section G.3.2.

Structure. Lemma G.16 states the computed odd half of the split; Lemma G.17 the computed split; Lemma G.18 the computed merge; Proposition G.19 the isometry of the split and the merge.

Lemma G.16 (The computed odd half of the split [to table])**.** *The odd half the split computes at a pair, with a stored twiddle near the root, is the odd half over* $\mathbb{R}$ *times a factor within* c_{split} *of* 1*, plus a term in* ζ*. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $a, b \in C_{\mathcal{F}}$*;*
- $\psi \in \mathbb{C}$*;*
- $\widetilde{\psi} \in C_{\mathcal{F}}$*.*

Define:

- $f_1 := ((a-b)/2)\ \mathrm{conj}(\psi)$*, that of* split *(Algorithm 2), line 7;*
- $\widetilde{p} := (a \ominus b) \otimes \mathrm{conj}(\widetilde{\psi}) \in C_{\mathcal{F}}$*;*
- $\widetilde{f_1} := \mathrm{fl}(\widetilde{p}/2) \in C_{\mathcal{F}}$*, the value* split *(Algorithm 2) computes at line 6;*
- $k_B := \sqrt{2}(3 + 2u)$*;*
- $c_{\text{split}} := (1+u)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1$*;*
- $k_D := (\sqrt{2}/2)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) + k_B$*.*

Assume:

(A1) $|\psi| = 1$*;*

(A2) $|\widetilde{\psi} - \psi| \le u + \sqrt{2}\,\zeta$*.*

Then

$$\exists\, \delta_1, e_1 \in \mathbb{C},\ |\delta_1| \le c_{\text{split}},\ |e_1| \le k_D\,\zeta : \quad \widetilde{f_1} = f_1(1+\delta_1) + e_1.$$

Proof.

DEFINES $e_1 := \frac{e_a}{2}\ \mathrm{conj}(\psi)(1+\mathrm{conj}\,\delta_c)(1+\delta_b) + e_b/2 + \zeta_\circ$, e_a, δ_c, δ_b, e_b, $\zeta_\circ$ those of (L1) to (L8)

	Lemma B.2, item 2	This proof
(I1)	Shared: $u, \zeta,\ a, b$ Shared: $a, b \in C_{\mathcal{F}}$	
	Its item 2: $(a \ominus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\,\zeta^{\pm}\right)\ (a-b)$	

(L1) $\exists\, \delta_a, e_a \in \mathbb{C},\ |\delta_a| \le u,\ |e_a| \le \sqrt{2}\,\zeta :\ a \ominus b = (a-b)(1+\delta_a) + e_a$

[(I1)]

Lemma B.1	This proof
p	$\widetilde{\psi}$
x	ψ
c	$u + \sqrt{2}\,\zeta$
(I2) $c \ge 0$	$u, \zeta \ge 0$ (Definition A.4)
$x \in \mathbb{C}$	$\psi \in \mathbb{C}$ (the statement)
$p \in \mathbb{C}$	$\widetilde{\psi} \in C_{\mathcal{F}}$ (the statement); Definition A.8
$\lvert p - x\rvert \le c\lvert x\rvert$	Assumptions A1, A2
Its conclusion: $\lvert\delta(p,x)\rvert \le c,\ p = x(1+\delta(p,x))$	

(L2) $\exists\, \delta_c \in \mathbb{C},\ |\delta_c| \le u + \sqrt{2}\,\zeta :\ \widetilde{\psi} = \psi(1+\delta_c)$

[(I2)]

(L3) $\operatorname{conj}(\widetilde{\psi}) = \operatorname{conj}(\psi)(1 + \operatorname{conj}\delta_c)$

[(L2); Fact A.41, item 13: $\operatorname{conj} xy = \operatorname{conj} x \operatorname{conj} y$, $\operatorname{conj} x + y = \operatorname{conj} x + \operatorname{conj} y$]

(L4) $|\operatorname{conj}\delta_c| = |\delta_c|$

[Fact A.41, item 1]

Lemma B.2, item 3	This proof
Shared: $u, \zeta,\ k_B$	
a	$a \ominus b$
(I3) b	$\operatorname{conj}(\widetilde{\psi})$
$a \in C_{\mathcal{F}}$	$a, b \in C_{\mathcal{F}}$ (the statement); Definition A.8
$b \in C_{\mathcal{F}}$	$\widetilde{\psi} \in C_{\mathcal{F}}$ (the statement); Definition A.4, item 7: $\mathrm{fl}(\operatorname{conj} x) = \operatorname{conj} x$
Its item 3: $(a \otimes b)\ \mathcal{I}\left((\sqrt{2}\,u(2+u))^{\pm}, k_B\,\zeta^{\pm}\right)\ ab$	

(L5) $\exists\, \delta_b, e_b \in \mathbb{C},\ |\delta_b| \le \sqrt{2}u(2+u),\ |e_b| \le k_B\,\zeta :\ \widetilde{p} = (a \ominus b)\ \operatorname{conj}(\widetilde{\psi})(1+\delta_b) + e_b$

[(I3); $\widetilde{p}$ (the statement)]

(L6) $\exists\, \zeta_\circ \in \mathbb{C},\ |\operatorname{Re}\zeta_\circ|, |\operatorname{Im}\zeta_\circ| \le \zeta/2 :\ \widetilde{f_1} = \widetilde{p}/2 + \zeta_\circ$

[Definition A.4, item 3, at each part of $\widetilde{p}$]

(L7) $|\zeta_\circ| \le \zeta$

[(L6); Fact A.41, item 1: $|x+y| \le |x| + |y|$ at $(x,y) := (\operatorname{Re}\zeta_\circ, i\operatorname{Im}\zeta_\circ)$]

(L8) $\Rightarrow\ \widetilde{f_1} = \frac{a \ominus b}{2}\ \operatorname{conj}(\widetilde{\psi})(1+\delta_b) + (e_b/2 + \zeta_\circ)$

[(L5), (L6)]

(L9) $|e_b/2 + \zeta_\circ| \le (k_B/2 + 1)\,\zeta$

[(L5), (L7); Fact A.41, item 1: $|x+y| \le |x| + |y|$]

(L10) $k_B \ge 2$

[$k_B = \sqrt{2}(3+2u)$ (the statement); $u \ge 0$ (Definition A.4)]

(L11) $\Rightarrow\ |e_b/2 + \zeta_\circ| \le k_B\,\zeta$

[(L9), (L10)]

(L12) $\Rightarrow\ \widetilde{f_1} = f_1(1+\delta_a)(1+\operatorname{conj}\delta_c)(1+\delta_b) + e_1$

[e_1 (the proof's block); (L1), (L3), (L8); f_1 (the statement)]

Lemma G.4	This proof
k	3
$(\delta_1, \delta_2, \delta_3)$	$(\delta_a, \operatorname{conj}\delta_c, \delta_b)$
(c_1, c_2, c_3)	$(u, u+\sqrt{2}\,\zeta, \sqrt{2}\,u(2+u))$
(I4) $\delta_1, \delta_2, \delta_3 \in \mathbb{C}$	(L1), (L2), (L5)
$c_1, c_2, c_3 \geq 0$	$u, \zeta \geq 0$ (Definition A.4)
Assumption A1	(L1), (L2), (L4), (L5)
Its conclusion: $\lvert\prod_{j=1}^{k}(1+\delta_j)-1\rvert \leq \prod_{j=1}^{k}(1+c_j)-1$	

(L13) $\lvert(1+\delta_a)(1+\operatorname{conj}\delta_c)(1+\delta_b)-1\rvert \leq c_{\text{split}}$

[(I4); c_{split} (the statement)]

(L14) $\lvert e_1\rvert \leq \frac{\sqrt{2}}{2}\,\zeta\,(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}u(2+u)) + k_B\,\zeta$

[(L12); Fact A.41, item 1: $\lvert x+y\rvert \leq \lvert x\rvert + \lvert y\rvert$, $\lvert xy\rvert = \lvert x\rvert\lvert y\rvert$, $\lvert\operatorname{conj} x\rvert = \lvert x\rvert$; $\lvert\psi\rvert = 1$ (assumption A1); (L1), (L2), (L4), (L5), (L11)]

(L15) $\frac{\sqrt{2}}{2}\,\zeta\,(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}u(2+u)) + k_B\,\zeta = k_D\,\zeta$

[k_D (the statement)]

(L16) $\Rightarrow\ \exists\,\delta_1, e_1 \in \mathbb{C},\ \lvert\delta_1\rvert \leq c_{\text{split}},\ \lvert e_1\rvert \leq k_D\,\zeta:\ \tilde{f}_1 = f_1(1+\delta_1) + e_1$

[(L12), (L13), (L14), (L15) at $\delta_1 := (1+\delta_a)(1+\operatorname{conj}\delta_c)(1+\delta_b)-1$]

(L17) $\Rightarrow$ the statement

[(L16)]

□

Lemma G.17 (The computed split's perturbation [to table])**.** *At a pair, the split's two computed halves are within c_{split} of the halves over $\mathbb{R}$ in the pair norm, plus a term in ζ. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *$a, b \in C_{\mathcal{F}}$;*
- *$\psi \in \mathbb{C}$;*
- *$\tilde{\psi} \in C_{\mathcal{F}}$.*

Define:

- $f_0 := \frac{a+b}{2}$;
- $f_1 := \frac{a-b}{2}\operatorname{conj}(\psi)$;
- $\tilde{f}_0 := \operatorname{fl}\left(\frac{a \oplus b}{2}\right)$;
- $\tilde{p} := (a \ominus b) \otimes \operatorname{conj}(\tilde{\psi})$;
- $\tilde{f}_1 := \operatorname{fl}\left(\frac{\tilde{p}}{2}\right)$;
- $c_{\text{split}} := (1+u)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1$ *(Lemma G.16);*
- $k_B := \sqrt{2}(3+2u)$ *(Lemma G.16);*
- $k_D := (\sqrt{2}/2)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) + k_B$ *(Lemma G.16).*

Assume:

(A1) $\lvert\psi\rvert = 1$;

(A2) $\tilde{\psi}\ \mathcal{I}\left(u^{\pm} + \sqrt{2}\zeta^{\pm}, 0\right)\ \psi$.

Then

$$(\tilde{f}_0, \tilde{f}_1)\ \mathcal{N}\left(c_{\text{split}}, \left(\frac{\sqrt{2}}{2} + k_D\right)\zeta\right)\ (f_0, f_1).$$

Proof. (I1)

Lemma B.3	This proof
Shared: $u, \zeta,\ a, b,\ f_0, \tilde{f}_0$	
Shared: $a, b \in C_{\mathcal{F}}$	
Its conclusion: $\exists\,\delta_0, e_0 \in \mathbb{C},\ \lvert\delta_0\rvert \leq u,\ \lvert e_0\rvert \leq (\sqrt{2}/2)\,\zeta:\ \tilde{f}_0 = f_0(1+\delta_0) + e_0$	

$\exists\, \delta_0, e_0 \in \mathbb{C},\ |\delta_0| \le u,\ |e_0| \le (\sqrt{2}/2)\,\zeta :\ \widetilde{f_0} = f_0(1+\delta_0) + e_0$

[(I1)]

(L2) $|\widetilde{\psi} - \psi| \le u + \sqrt{2}\,\zeta$

[assumption A2; Definition A.10 at $|\psi| = 1$ (assumption A1)]

Lemma G.16	This proof
Shared: $\mathcal{F}, (u,\zeta),\ a, b, \psi, \tilde{\psi},\ f_1, \tilde{p}, \tilde{f}_1,\ c_{\text{split}}, k_B, k_D$ Shared: $a, b \in C_{\mathcal{F}},\ \psi \in \mathbb{C},\ \tilde{\psi} \in C_{\mathcal{F}}$ Shared: assumption A1	
Assumption A2	(L2)
Its conclusion: $\exists\, \delta_1, e_1 \in \mathbb{C},\ \lvert\delta_1\rvert \le c_{\text{split}},\ \lvert e_1\rvert \le k_D\,\zeta :\ \tilde{f}_1 = f_1(1+\delta_1) + e_1$	

(I2)

(L3) $\exists\, \delta_1, e_1 \in \mathbb{C},\ |\delta_1| \le c_{\text{split}},\ |e_1| \le k_D\,\zeta :\ \widetilde{f_1} = f_1(1+\delta_1) + e_1$

[(I2)]

(L4) $1 + u + \sqrt{2}\,\zeta \ge 1 + u$

[$\zeta \ge 0$ (Definition A.4)]

(L5) $1 + \sqrt{2}u(2+u) \ge 1$

[$u \ge 0$ (Definition A.4)]

(L6) $(1+u)^2 - 1 \le c_{\text{split}}$

[(L4), (L5); c_{split} (Lemma G.16); Fact A.41, item 8]

(L7) $(1+u)^2 - 1 = 2u + u^2$

[expand]

(L8) $2u + u^2 \ge u$

[$u \ge 0$ (Definition A.4)]

(L9) $\Rightarrow\ u \le c_{\text{split}}$

[(L6), (L7), (L8)]

(L10) $\|(\widetilde{f_0}, \widetilde{f_1}) - (f_0, f_1)\| \le \|(f_0\delta_0, f_1\delta_1)\| + \|(e_0, e_1)\|$

[(L1), (L3); Fact A.41, item 3: $\|X + Y\| \le \|X\| + \|Y\|$]

(L11) $\|(f_0\delta_0, f_1\delta_1)\| \le c_{\text{split}}\|(f_0, f_1)\|$

[(L1), (L3), (L9); $\|(X,Y)\|^2 := \|X\|^2 + \|Y\|^2$ (Fact A.41, its lead); Fact A.41, item 1: $|xy| = |x||y|$]

(L12) $\|(e_0, e_1)\| \le |e_0| + |e_1|$

[Fact A.41, item 3: $\|(x,y)\| \le |x| + |y|$]

(L13) $|e_0| + |e_1| \le (\sqrt{2}/2 + k_D)\,\zeta$

[(L1), (L3)]

(L14) $\Rightarrow\ \|(\widetilde{f_0}, \widetilde{f_1}) - (f_0, f_1)\| \le c_{\text{split}}\|(f_0, f_1)\| + (\sqrt{2}/2 + k_D)\,\zeta$

[(L10), (L11), (L12), (L13)]

(L15) $\Rightarrow\ (\widetilde{f_0}, \widetilde{f_1})\ \mathcal{N}\left(c_{\text{split}}, (\sqrt{2}/2 + k_D)\,\zeta\right)\ (f_0, f_1)$

[(L14); Definition A.11 with the pair norm]

(L16) $\Rightarrow$ the statement

[(L15)]

□

Lemma G.18 (The computed merge's perturbation [to table])**.** *At a pair, the merge's two computed values are within* c_{merge} *of the values over* $\mathbb{R}$ *in the pair norm, plus a term in* ζ*. Let:*

- $\mathcal{F}$ *be a realization at* (u,ζ) *(Definition A.4);*
- $f_0, f_1 \in C_{\mathcal{F}}$*;*
- $\psi \in \mathbb{C}$*;*
- $\tilde{\psi} \in C_{\mathcal{F}}$*.*

Define:

- $a := f_0 + \psi f_1$*;*
- $b := f_0 - \psi f_1$*;*

- $\tilde{a} := f_0 \oplus f_1 \otimes \tilde{\psi}$;
- $\tilde{b} := f_0 \ominus f_1 \otimes \tilde{\psi}$;
- $c_{\text{merge}} := u + (1+u)\left(\left(1 + u + \sqrt{2}\zeta\right)\left(1 + \sqrt{2}u(2+u)\right) - 1\right)$;
- $k_E := 2\sqrt{2}\,((3+2u)(1+u)+1)$.

Assume:
(A1) $|\psi| = 1$;
(A2) $\tilde{\psi}\ \mathcal{I}\left(u^{\pm} + \sqrt{2}\zeta^{\pm}, 0\right)\ \psi$.
Then

$$(\tilde{a}, \tilde{b})\ \mathcal{N}\left(c_{\text{merge}}, k_E\zeta\right)\ (a, b).$$

Proof.
DEFINES $e := (1 + u + \sqrt{2}\,\zeta)(1 + \sqrt{2}\,u(2+u)) - 1$
COMPUTES $\widetilde{m} := f_1 \otimes \widetilde{\psi}$ (merge (Algorithm 4), line 4)

	Lemma B.1	This proof
	p	$\tilde{\psi}$
	x	ψ
	c	$u + \sqrt{2}\,\zeta$
(I1)	$c \geq 0$	$u, \zeta \geq 0$ (Definition A.4)
	$x \in \mathbb{C}$	$\psi \in \mathbb{C}$ (the statement)
	$p \in \mathbb{C}$	$\tilde{\psi} \in C_{\mathcal{F}}$ (the statement); Definition A.8
	$\lvert p - x\rvert \leq c\lvert x\rvert$	Assumptions A1, A2; Definition A.10
	Its conclusion: $\lvert\delta(p,x)\rvert \leq c,\ p = x(1+\delta(p,x))$	

(L1) $\exists\,\delta_c \in \mathbb{C},\ |\delta_c| \leq u + \sqrt{2}\,\zeta :\ \widetilde{\psi} = \psi(1+\delta_c)$
[(I1)]

	Lemma B.2, item 3	This proof
	Shared: u, ζ	
(I2)	a	f_1
	b	$\tilde{\psi}$
	$a, b \in C_{\mathcal{F}}$	$f_1, \tilde{\psi} \in C_{\mathcal{F}}$ (the statement)
	Its item 3: $(a \otimes b)\ \mathcal{I}\left((\sqrt{2}\,u(2+u))^{\pm}, k_B\,\zeta^{\pm}\right)\ ab$	

(L2) $\exists\,\delta_b, e_b \in \mathbb{C},\ |\delta_b| \leq \sqrt{2}u(2+u),\ |e_b| \leq k_B\,\zeta :\ \widetilde{m} = f_1\widetilde{\psi}(1+\delta_b) + e_b$
[(I2)]

(L3) $\Rightarrow\ \widetilde{m} = f_1\psi(1+\delta_c)(1+\delta_b) + e_b$
[(L1), (L2)]

	Lemma G.4	This proof
	k	2
	(δ_1, δ_2)	(δ_c, δ_b)
	(c_1, c_2)	$(u + \sqrt{2}\,\zeta, \sqrt{2}\,u(2+u))$
(I3)	$\delta_1, \delta_2 \in \mathbb{C}$	(L1), (L2)
	$c_1, c_2 \geq 0$	$u, \zeta \geq 0$ (Definition A.4)
	Assumption A1	(L1), (L2)
	Its conclusion: $\lvert\prod_{j=1}^{k}(1+\delta_j) - 1\rvert \leq \prod_{j=1}^{k}(1+c_j) - 1$	

(L4) $|(1+\delta_c)(1+\delta_b) - 1| \leq e$
[(I3); e (the proof's block)]

(L5) $\Rightarrow\ \exists\,e' \in \mathbb{C},\ |e'| \leq e :\ \widetilde{m} = f_1\psi(1+e') + e_b$
[(L3), (L4) at $e' := (1+\delta_c)(1+\delta_b) - 1$]

Lemma B.2, item 1	This proof
Shared: u, ζ	
a (I4) b $a, b \in C_{\mathcal{F}}$	f_0 $\widetilde{m}$ $f_0, f_1, \tilde{\psi} \in C_{\mathcal{F}}$ (the statement); $\widetilde{m}$ (the proof's block); Definition A.8
Its item 1: $(a \oplus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\,\zeta^{\pm}\right)\ (a+b)$	

(L6) $\exists\, t_+, e_+ \in \mathbb{C},\ |t_+| \le u,\ |e_+| \le \sqrt{2}\,\zeta :\ \widetilde{a} = (f_0 + \widetilde{m})(1+t_+) + e_+$
[(I4)]

Lemma B.2, item 2	This proof
Shared: u, ζ	
a (I5) b $a, b \in C_{\mathcal{F}}$	f_0 $\widetilde{m}$ $f_0, f_1, \tilde{\psi} \in C_{\mathcal{F}}$ (the statement); $\widetilde{m}$ (the proof's block); Definition A.8
Its item 2: $(a \ominus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\,\zeta^{\pm}\right)\ (a-b)$	

(L7) $\exists\, t_-, e_- \in \mathbb{C},\ |t_-| \le u,\ |e_-| \le \sqrt{2}\,\zeta :\ \widetilde{b} = (f_0 - \widetilde{m})(1+t_-) + e_-$
[(I5)]

(L8) $\Rightarrow\ \widetilde{a} - a = a\,t_+ + f_1\psi e'(1+t_+) + (e_b(1+t_+) + e_+)$
[(L5), (L6); $a = f_0 + f_1\psi$ (the statement); expand]

(L9) $\Rightarrow\ \widetilde{b} - b = b\,t_- - f_1\psi e'(1+t_-) + (-e_b(1+t_-) + e_-)$
[(L5), (L7); $b = f_0 - f_1\psi$ (the statement); expand]

(L10) $\forall s \in \{+,-\} :\ |1+t_s| \le 1+u$
[(L6), (L7); Fact A.41, item 1: $|x+y| \le |x| + |y|$]

(L11) $|e_b(1+t_+) + e_+| \le k_B\,\zeta(1+u) + \sqrt{2}\,\zeta$
[Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$; (L2), (L6), (L10)]

(L12) $|-e_b(1+t_-) + e_-| \le k_B\,\zeta(1+u) + \sqrt{2}\,\zeta$
[Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$; (L2), (L7), (L10)]

(L13) $k_B\,\zeta(1+u) + \sqrt{2}\,\zeta = \sqrt{2}((3+2u)(1+u)+1)\,\zeta$
[$k_B = \sqrt{2}(3+2u)$ (Lemma B.2)]

(L14) $\|(a\,t_+,\ b\,t_-)\| \le u\,\|(a,b)\|$
[$|t_\pm| \le u$ ((L6), (L7)); $\|(X,Y)\|^2 := \|X\|^2 + \|Y\|^2$ (Fact A.41, its lead); Fact A.41, item 1: $|xy| = |x||y|$]

(L15) $\|(f_1\psi e'(1+t_+),\ -f_1\psi e'(1+t_-))\| \le \sqrt{2}\,|f_1||e'|(1+u)$
[Fact A.41, item 3: $\|(x,y)\| \le \sqrt{2}\max(|x|,|y|)$; item 1: $|xy| = |x||y|$; $|\psi| = 1$ (assumption A1); (L10)]

(L16) $\|(e_b(1+t_+) + e_+,\ -e_b(1+t_-) + e_-)\| \le k_E\,\zeta$
[(L11), (L12), (L13); Fact A.41, item 3: $\|(x,y)\| \le |x| + |y|$; k_E (the statement)]

(L17) $\Rightarrow\ \|(\widetilde{a},\widetilde{b}) - (a,b)\| \le u\|(a,b)\| + \sqrt{2}|f_1||e'|(1+u) + k_E\,\zeta$
[(L8), (L9); Fact A.41, item 3: $\|X+Y\| \le \|X\| + \|Y\|$; (L14), (L15), (L16)]

(L18) $\|(a,b)\|^2 = 2(|f_0|^2 + |f_1|^2)$
[a, b (the statement); Fact A.41, item 2, at $(x,y) := (f_0, \psi f_1)$; $|\psi| = 1$ (assumption A1)]

(L19) $\Rightarrow\ \sqrt{2}|f_1| \le \|(a,b)\|$
[(L18); Fact A.41, item 13: $t^{2j} \ge 0$ at $(t,j) := (|f_0|, 1)$; Fact A.41, item 5: $t \mapsto \sqrt{t}$ nondecreasing]

(L20) $\Rightarrow\ \|(\widetilde{a},\widetilde{b}) - (a,b)\| \le (u + (1+u)e)\|(a,b)\| + k_E\,\zeta$
[(L17), (L19); $|e'| \le e$ (L5)]

(L21) $u + (1+u)e = c_{\text{merge}}$
[e (the proof's block); c_{merge} (the statement)]

(L22) $\Rightarrow\ (\widetilde{a},\widetilde{b})\ \mathcal{N}\left(c_{\text{merge}}, k_E\,\zeta\right)\ (a,b)$
[(L20), (L21); Definition A.11 with the pair norm]

(L23) $\Rightarrow$ the statement

[(L22)]

□

Proposition G.19 (Isometry of the split and the merge [to table])**.** *The split of a polynomial into its two halves keeps the coefficient norm, and so does the merge. Let:*

- $m \geq 4$;
- $f \in \mathcal{R}_m$;
- $g_0, g_1 \in \mathcal{R}_{m/2}$.

Define:

- $\operatorname{split}(a) := (a_0, a_1)$ *for* $a \in \mathcal{R}_m$, $m \geq 4$ *(Definition A.15);*
- $a_0 := \sum_{i<m/2} a_{[2i]} x^i$ *and* $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i$ *(Definition A.15);*
- $\operatorname{merge}(f_0, f_1) := f_0(x^2) + x f_1(x^2)$ *(Definition A.15);*
- $\|h\| := \left(\sum_{p<k} h_{[p]}^2\right)^{1/2}$, $h \in \mathcal{R}_k$;
- $\|(h_0, h_1)\| := \left(\|h_0\|^2 + \|h_1\|^2\right)^{1/2}$, $h_0, h_1 \in \mathcal{R}_{m/2}$.

Then the two norms are equal at both maps:

1. $\|\operatorname{split}(f)\| = \|f\|$;
2. $\|\operatorname{merge}(g_0, g_1)\| = \|(g_0, g_1)\|$.

Proof.

DEFINES $\Psi_k := \{\psi \in \mathbb{C} : \psi^k = -1,\ \operatorname{Im}\psi > 0\}$, $k \in \{m/2, m\}$

DEFINES $Z_{m/2} := \{\omega \in \mathbb{C} : \omega^{m/2} = -1\}$

DEFINES $f_0 \in \mathcal{R}_{m/2}$ by $f_0(\psi^2) = (f(\psi) + f(-\psi))/2$, $\psi \in \Psi_m$, that of split (Algorithm 2), lines 1 to 5

DEFINES $f_1 \in \mathcal{R}_{m/2}$ by $f_1(\psi^2) = ((f(\psi) - f(-\psi))/2)\ \operatorname{conj}\psi$, $\psi \in \Psi_m$, that of split (Algorithm 2), line 7

Proof of item 1.

(L1) $\forall \psi \in \Psi_m :\ |f_0(\psi^2)|^2 + |f_1(\psi^2)|^2 = \frac{1}{4}(|f(\psi) + f(-\psi)|^2 + |f(\psi) - f(-\psi)|^2)$

[f_0, f_1 (the proof's block); Fact A.42, item 1: $|\psi| = 1$; Fact A.41, item 1: $|xy| = |x||y|$, $|\operatorname{conj} x| = |x|$]

(L2) $\Rightarrow\ \forall \psi \in \Psi_m :\ |f_0(\psi^2)|^2 + |f_1(\psi^2)|^2 = \frac{1}{2}(|f(\psi)|^2 + |f(-\psi)|^2)$

[(L1); Fact A.41, item 2]

(L3) $-\Psi_m = \operatorname{conj}\Psi_m$

[Fact A.43, item 3, at m; Ψ_m (the proof's block), Fact A.43, item 2]

(L4) $\Rightarrow\ \sum_{\psi\in\Psi_m} |f(-\psi)|^2 = \sum_{\psi\in\Psi_m} |f(\psi)|^2$

[(L3); Fact A.42, item 2: $f(\operatorname{conj}\psi) = \operatorname{conj} f(\psi)$; Fact A.41, item 1: $|\operatorname{conj} x| = |x|$]

(L5) $\Rightarrow\ \sum_{\psi\in\Psi_m} (|f_0(\psi^2)|^2 + |f_1(\psi^2)|^2) = \sum_{\psi\in\Psi_m} |f(\psi)|^2$

[(L2), (L4)]

(L6) $\psi \mapsto \psi^2$ is a bijection $\Psi_m \to Z_{m/2}$

[Fact A.43, item 5, at $m \geq 4$; $Z_{m/2}$ (the proof's block)]

(L7) $\Rightarrow\ \forall j \in \{0, 1\} :\ \sum_{\psi\in\Psi_m} |f_j(\psi^2)|^2 = \sum_{\omega\in Z_{m/2}} |f_j(\omega)|^2$

[(L6)]

(L8) $\forall j \in \{0, 1\} :\ \sum_{\omega\in Z_{m/2}} |f_j(\omega)|^2 = 2\sum_{\omega\in\Psi_{m/2}} |f_j(\omega)|^2$

[Fact A.43, item 6, at $m/2$, $g := |f_j|^2$, invariant by Fact A.42, item 2, and Fact A.41, item 1: $|\operatorname{conj} x| = |x|$; $\Psi_{m/2}$ (the statement), Fact A.43, item 2]

	Proposition G.15	This proof
	Shared: f	
(I1)	n $\{\psi_k : k < n/2\}$ $n \in \{2^h : h \in \mathbb{Z}_{>0}\}$ $f \in \mathbb{R}[x]/(x^n+1)$ $\{\psi_k : k < n/2\} =$ $\{\psi \in \mathbb{C} : \psi^n = -1,\ \mathrm{Im}\,\psi > 0\}$	m Ψ_m $m \geq 4$, $f \in \mathcal{R}_m$ (the statement); Definition A.1 $f \in \mathcal{R}_m$ (the statement); Definition A.1 Ψ_m (the proof's block)
	Its conclusion: $\sum_{p<n} f_{[p]}^2 = \frac{2}{n}\sum_{k<n/2}\lvert f(\psi_k)\rvert^2$	

(L9) $\|f\|^2 = \frac{2}{m}\sum_{\psi\in\Psi_m}|f(\psi)|^2$

[(I1); $\|h\|$ (the statement)]

	Proposition G.15 at every $j \in \{0,1\}$	This proof
	n f $\{\psi_k : k < n/2\}$ $n \in \{2^h : h \in \mathbb{Z}_{>0}\}$ $f \in \mathbb{R}[x]/(x^n+1)$ $\{\psi_k : k < n/2\} =$ $\{\psi \in \mathbb{C} : \psi^n = -1,\ \mathrm{Im}\,\psi > 0\}$	$m/2$ f_j $\Psi_{m/2}$ $m \geq 4$, $f \in \mathcal{R}_m$ (the statement); Definition A.1 $f_j \in \mathcal{R}_{m/2}$ (the proof's block); Definition A.1 $\Psi_{m/2}$ (the proof's block)
(I2)	Its conclusion: $\sum_{p<n} f_{[p]}^2 = \frac{2}{n}\sum_{k<n/2}\lvert f(\psi_k)\rvert^2$	

(L10) $\forall j \in \{0,1\}:\ \|f_j\|^2 = \frac{4}{m}\sum_{\omega\in\Psi_{m/2}}|f_j(\omega)|^2$

[(I2); $\|h\|$ (the statement)]

(L11) $\forall \psi \in \mathbb{C},\ \psi^m = -1:\ f(\psi) = a_0(\psi^2) + \psi\, a_1(\psi^2)$

[merge(split(f)) $= f$ (Fact A.42, item 4); split$(f) = (a_0, a_1)$ at $a := f$ (the statement); merge (the statement); Fact A.42, items 6 and 7]

(L12) $\forall \psi \in \Psi_m:\ f(-\psi) = a_0(\psi^2) - \psi\, a_1(\psi^2)$

[(L11) at $-\psi$; $(-\psi)^m = \psi^m$ and $(-\psi)^2 = \psi^2$ at m even ($m \geq 4$, the statement); Ψ_m (the proof's block)]

(L13) $\forall \psi \in \Psi_m:\ a_0(\psi^2) = f_0(\psi^2)$

[(L11), (L12); f_0 (the proof's block)]

(L14) $\forall \psi \in \Psi_m:\ a_1(\psi^2) = f_1(\psi^2)$

[(L11), (L12); f_1 (the proof's block); $\psi\,\mathrm{conj}\,\psi = 1$ (Fact A.42, item 1)]

(L15) $\mathrm{split}(f) = (f_0, f_1)$

[(L13), (L14); (L6); split$(f) = (a_0, a_1)$ at $a := f$ (the statement); f_0, f_1 (the proof's block)]

(L16) $\Rightarrow\ \|\mathrm{split}(f)\|^2 = \frac{2}{m}\sum_{\psi\in\Psi_m}(|f_0(\psi^2)|^2 + |f_1(\psi^2)|^2)$

[(L15); $\|(h_0, h_1)\|$ (the statement); (L7), (L8), (L10)]

(L17) $\Rightarrow\ \|\mathrm{split}(f)\|^2 = \|f\|^2$

[(L5), (L9), (L16)]

(L18) $\Rightarrow\ \|\mathrm{split}(f)\| = \|f\|$

[(L17)]

(L19) $\Rightarrow$ item 1

[(L18)]

□ (item 1)

Proof of item 2.

(L20) $\mathrm{split}(\mathrm{merge}(g_0, g_1)) = (g_0, g_1)$

[Fact A.42, item 5, at $(f_0, f_1) := (g_0, g_1)$]

Proposition G.19, item 1	This proof
Shared: m	
f	$\mathrm{merge}(g_0, g_1)$
$f \in \mathcal{R}_m$	$g_0, g_1 \in \mathcal{R}_{m/2}$ (the statement); Definition A.15
Its item 1: $\|\mathrm{split}(f)\| = \|f\|$	

(I3)

(L21) $\Rightarrow$ $\|\mathrm{merge}(g_0, g_1)\| = \|(g_0, g_1)\|$ [(I3); (L20)]

(L22) $\Rightarrow$ item 2 [(L21)]

□ (item 2)

G.3.3 The center update and the leaf standard deviation

Structure. Lemma G.20 states the computed center update; Lemma G.21 the computed $1/\sigma$ at a leaf.

Lemma G.20 (The computed center update's perturbation [to table])**.** *The center update a node computes is within u of the update over $\mathbb{R}$, plus a term in the size of the correction and in ζ. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *$t_0, t_1, z_1, l_{10} \in C_{\mathcal{F}}$.*

Define:

- *$tb_0 := t_0 + (t_1 - z_1) l_{10}$, that of* ffsamp *(Algorithm 6), line 26;*
- *$\tilde{tb}_0 := t_0 \oplus (t_1 \ominus z_1) \otimes l_{10}$, the value* ffsamp *(Algorithm 6) computes;*
- *$k_B := \sqrt{2}(3 + 2u)$;*
- *$e_0 := (1 + u)\left(1 + \sqrt{2}u(2 + u)\right) - 1$;*
- *$k_I := \left(\sqrt{2}|l_{10}|\left(1 + \sqrt{2}u(2 + u)\right) + k_B\right)(1 + u) + \sqrt{2}$.*

Then

$$\tilde{tb}_0 \, \mathcal{N}\left(u, (1 + u)|t_1 - z_1||l_{10}|e_0 + k_I\zeta\right) tb_0.$$

Proof. (I1)

Lemma B.2, item 2	This proof
Shared: u, ζ	
a	t_1
b	z_1
$a, b \in C_{\mathcal{F}}$	$t_1, z_1 \in C_{\mathcal{F}}$ (the statement)
Its item 2: $(a \ominus b)\, \mathcal{I}\left(u^{\pm}, \sqrt{2}\,\zeta^{\pm}\right)(a - b)$	
$\exists\, \delta_1, e_1 \in \mathbb{C},\ \|\delta_1| \le u,\ \|e_1| \le \sqrt{2}\,\zeta :\ t_1 \ominus z_1 = (t_1 - z_1)(1 + \delta_1) + e_1$ [(I1)]	

Lemma B.2, item 3	This proof
Shared: $u, \zeta,\ k_B$	
a	$t_1 \ominus z_1$
b	l_{10}
$a, b \in C_{\mathcal{F}}$	$t_1, z_1, l_{10} \in C_{\mathcal{F}}$ (the statement); Definition A.8
Its item 3: $(a \otimes b)\, \mathcal{I}\left((\sqrt{2}\,u(2 + u))^{\pm}, k_B\,\zeta^{\pm}\right) ab$	
(L2) $\exists\, \delta_2, e_2 \in \mathbb{C},\ \|\delta_2| \le \sqrt{2}u(2 + u),\ \|e_2| \le k_B\,\zeta :\ (t_1 \ominus z_1) \otimes l_{10} = (t_1 \ominus z_1)\, l_{10}(1 + \delta_2) + e_2$ [(I2)]	

(L3) $\Rightarrow$ $(t_1 \ominus z_1) \otimes l_{10} = (t_1 - z_1)\, l_{10}(1 + \delta_1)(1 + \delta_2) + e_1 l_{10}(1 + \delta_2) + e_2$ [(L1), (L2)]

	Lemma B.2, item 1	This proof
	Shared: u, ζ	
(I3)	a	t_0
	b	$(t_1 \ominus z_1) \otimes l_{10}$
	$a, b \in C_{\mathcal{F}}$	$t_0, t_1, z_1, l_{10} \in C_{\mathcal{F}}$ (the statement); Definition A.8
	Its item 1: $(a \oplus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\,\zeta^{\pm}\right)\ (a+b)$	

(L4) $\exists\, \delta_3, e_3 \in \mathbb{C},\ |\delta_3| \le u,\ |e_3| \le \sqrt{2}\,\zeta :\ \widetilde{tb}_0 = (t_0 + (t_1 \ominus z_1) \otimes l_{10})(1+\delta_3) + e_3$

[(I3)]

(L5) $\Rightarrow\ \widetilde{tb}_0 - tb_0 = tb_0\,\delta_3 + (t_1 - z_1)\,l_{10}((1+\delta_1)(1+\delta_2)-1)(1+\delta_3) + ((e_1 l_{10}(1+\delta_2)+e_2)(1+\delta_3)+e_3)$

[(L3), (L4); $tb_0 = t_0 + (t_1 - z_1)\,l_{10}$ (the statement); expand]

(L6) $|tb_0\,\delta_3| \le u\,|tb_0|$

[(L4); Fact A.41, item 1: $|xy| = |x||y|$]

	Lemma G.4	This proof
	Shared: δ_1 (L1), δ_2 (L2)	
(I4)	k	2
	(c_1, c_2)	$(u, \sqrt{2}\,u(2+u))$
	$\delta_1, \delta_2 \in \mathbb{C}$	(L1), (L2)
	$c_1, c_2 \ge 0$	$u \ge 0$ (Definition A.4)
	Assumption A1	(L1), (L2)
	Its conclusion: $\lvert\prod_{j=1}^{k}(1+\delta_j) - 1\rvert \le \prod_{j=1}^{k}(1+c_j) - 1$	

(L7) $|(1+\delta_1)(1+\delta_2) - 1| \le e_0$

[(I4); e_0 (the statement)]

(L8) $\Rightarrow\ |(t_1 - z_1)\,l_{10}((1+\delta_1)(1+\delta_2)-1)(1+\delta_3)| \le (1+u)|t_1 - z_1||l_{10}|\,e_0$

[(L7); Fact A.41, item 1: $|xy| = |x||y|$, $|x+y| \le |x| + |y|$; (L4)]

(L9) $|(e_1 l_{10}(1+\delta_2) + e_2)(1+\delta_3) + e_3| \le k_I\,\zeta$

[Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$; (L1), (L2), (L4); k_I (the statement)]

(L10) $\Rightarrow\ |\widetilde{tb}_0 - tb_0| \le u|tb_0| + (1+u)|t_1 - z_1||l_{10}|\,e_0 + k_I\,\zeta$

[(L5); Fact A.41, item 1: $|x+y| \le |x| + |y|$; (L6), (L8), (L9)]

(L11) $\Rightarrow\ \widetilde{tb}_0\ \mathcal{N}\left(u, (1+u)|t_1 - z_1||l_{10}|\,e_0 + k_I\,\zeta\right)\ tb_0$

[(L10); Definition A.11]

(L12) $\Rightarrow$ the statement

[(L11)]

□

Lemma G.21 (The computed inverse leaf standard deviation [to table])**.** *At a leaf, the inverse standard deviation the code computes from a perturbed diagonal is the one over $\mathbb{R}$ times a factor set by the perturbation and three roundings, plus a term in ζ. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *$d_{11} \ge 0$;*
- *$\delta_d \in \mathbb{R}$;*
- *$c_n \in \mathbb{R}$.*

Define:

- $\texttt{isigma} := \sqrt{d_{11}}\,c_n$;
- $\tilde{d}_{11} := d_{11}(1+\delta_d)$;
- $\widetilde{\texttt{isigma}} := \mathrm{fl}\left(\mathrm{fl}\left(\sqrt{\tilde{d}_{11}}\right) \cdot \texttt{INV_SIGMA}[\log_2 n]\right)$;
- $k_J := \left(|c_n| + \sqrt{\tilde{d}_{11}}\right)(1+u)^2 + (1+u)\zeta + 1.$

Assume:

(A1) $u \le 1$;
(A2) $\texttt{INV_SIGMA}[\log_2 n]\ \mathcal{I}\,(u^{\pm}, \zeta^{\pm})\ c_n$;
(A3) $|\delta_d| \le 1$.
Then

$$\widetilde{\texttt{isigma}}\ \mathcal{I}\left(\sqrt{1 \pm |\delta_d|}\,(1 \pm u)^3 - 1, k_J \zeta^{\pm}\right)\ \texttt{isigma}.$$

Proof.

COMPUTES $\widetilde{r} := \mathrm{fl}(\sqrt{\widetilde{d}_{11}})$ (deepest (Algorithm 7), line 1)

(L1) $1 + \delta_d \ge 0$

[$|\delta_d| \le 1$ (assumption A3)]

(L2) $\widetilde{d}_{11} \ge 0$

[$\widetilde{d}_{11} = d_{11}(1+\delta_d)$, $d_{11} \ge 0$ (the statement); (L1)]

(L3) $\exists\, u_r, \zeta_r \in \mathbb{R},\ |u_r| \le u,\ |\zeta_r| \le \zeta :\ \widetilde{r} = \sqrt{\widetilde{d}_{11}}(1+u_r) + \zeta_r$

[Definition A.4 for $\sqrt{}$ at $\widetilde{d}_{11}$; (L2)]

(L4) $\exists\, u_{\texttt{INV}}, \zeta_{\texttt{INV}} \in \mathbb{R},\ |u_{\texttt{INV}}| \le u,\ |\zeta_{\texttt{INV}}| \le \zeta :\ \texttt{INV_SIGMA}[\log_2 n] = c_n(1+u_{\texttt{INV}}) + \zeta_{\texttt{INV}}$

[assumption A2; Definition A.10]

(L5) $\exists\, u_{\texttt{isigma}}, \zeta_{\texttt{isigma}} \in \mathbb{R},\ |u_{\texttt{isigma}}| \le u,\ |\zeta_{\texttt{isigma}}| \le \zeta :\ \widetilde{\texttt{isigma}} = \widetilde{r} \cdot \texttt{INV_SIGMA}[\log_2 n]\,(1 + u_{\texttt{isigma}}) + \zeta_{\texttt{isigma}}$

[Definition A.4 for $\times$]

(L6) $\sqrt{\widetilde{d}_{11}} = \sqrt{d_{11}}\,(1+\delta_d)^{1/2}$

[$\widetilde{d}_{11} = d_{11}(1+\delta_d)$ (the statement); (L1); Fact A.41, item 13: $\sqrt{ab} = \sqrt{a}\sqrt{b}$ at $a, b \ge 0$]

(L7) $\Rightarrow\ \widetilde{\texttt{isigma}} = \texttt{isigma}\,(1+\delta_d)^{1/2}(1+u_r)(1+u_{\texttt{INV}})(1+u_{\texttt{isigma}}) + E, \quad E := (\zeta_r c_n(1+u_{\texttt{INV}}) + \sqrt{\widetilde{d}_{11}}(1+u_r)\zeta_{\texttt{INV}} + \zeta_r\zeta_{\texttt{INV}})(1+u_{\texttt{isigma}}) + \zeta_{\texttt{isigma}}$

[(L3), (L4), (L5), (L6); $\texttt{isigma} = \sqrt{d_{11}}\,c_n$ (the statement); expand]

(L8) $|E| \le ((|c_n| + \sqrt{\widetilde{d}_{11}})(1+u)^2 + \zeta(1+u) + 1)\zeta$

[(L7); (L3), (L4), (L5); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$]

(L9) $((|c_n| + \sqrt{\widetilde{d}_{11}})(1+u)^2 + \zeta(1+u) + 1)\zeta = k_J\,\zeta$

[k_J (the statement)]

(I1)

Lemma G.2, item 1	This proof
Shared: u	
k	3
(t_1, t_2, t_3)	$(u_r, u_{\texttt{INV}}, u_{\texttt{isigma}})$
$u \in [0, 1]$	$u \ge 0$ (Definition A.4); assumption A1
$t_1, t_2, t_3 \in \mathbb{R}$	(L3), (L4), (L5)
Assumption A1	(L3), (L4), (L5)
Its item 1: $P \in [(1-u)^k, (1+u)^k]$	

(L10) $(1+u_r)(1+u_{\texttt{INV}})(1+u_{\texttt{isigma}}) \in [(1-u)^3, (1+u)^3]$

[(I1)]

(L11) $1 + \delta_d \in [1 - |\delta_d|,\ 1 + |\delta_d|]$

[Fact A.41, item 1: $|\mathrm{Re}\,x| \le |x|$ at $x := \delta_d$]

(L12) $\Rightarrow\ (1+\delta_d)^{1/2} \in [(1-|\delta_d|)^{1/2},\ (1+|\delta_d|)^{1/2}]$

[(L11); $|\delta_d| \le 1$ (assumption A3); Fact A.41, item 5: $t \mapsto \sqrt{t}$ nondecreasing]

(L13) $\Rightarrow\ (1+\delta_d)^{1/2}(1+u_r)(1+u_{\texttt{INV}})(1+u_{\texttt{isigma}}) - 1 \in [(1-|\delta_d|)^{1/2}(1-u)^3 - 1,\ (1+|\delta_d|)^{1/2}(1+u)^3 - 1]$

[(L10), (L12); Fact A.41, item 8]

(L14) $\Rightarrow\ \widetilde{\texttt{isigma}}\ \mathcal{I}\left((1 \pm |\delta_d|)^{1/2}(1 \pm u)^3 - 1, (k_J\,\zeta)^{\pm}\right)\ \texttt{isigma}$

[(L7), (L8), (L9), (L13); Definition A.10; Definition A.9]

(L15) $\Rightarrow$ the statement

[(L14)]

□

G.3.4 The Gram matrix

Structure. Algorithm 13 describes Gram; Lemma G.22 states its computed diagonals; Lemma G.23 its computed off-diagonal entry.

Algorithm 13 Gram(B), the Gram matrix in FFT form [L0: `sign_fpoly.c:2625-2652`] [L0: `fxp/sign_fxpoly.c:243-275`]

Input: $B = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix}$ over $\mathcal{R}_n$; $\forall \psi:\ b_{jk} = b_{jk,r} + i b_{jk,i} \in C_{\mathcal{F}}$
Output (code): $\forall \psi:\ \widetilde{g}_{00}, \widetilde{g}_{11} \in \mathcal{F},\ \widetilde{g}_{01} \in C_{\mathcal{F}}$
Output (idealized): $\forall \psi:\ g_{00} = |b_{00}|^2 + |b_{01}|^2,\ g_{01} = b_{00} \operatorname{conj} b_{10} + b_{01} \operatorname{conj} b_{11},\ g_{11} = |b_{10}|^2 + |b_{11}|^2$
Postcondition: $BB^\dagger = \begin{pmatrix} g_{00} & g_{01} \\ \operatorname{conj} g_{01} & g_{11} \end{pmatrix}$
In the proofs: $\widetilde{s}_j,\ s_j,\ j \le 3,\ \widetilde{u},\ u,\ \widetilde{v},\ v$

1: **for all** $\psi,\ \psi^n = -1$ **do**
2: $\quad \widetilde{s}_0 \leftarrow \mathrm{fl}(\mathrm{fl}(b_{00,r}^2) + \mathrm{fl}(b_{00,i}^2))$
3: $\quad s_0 \leftarrow b_{00,r}^2 + b_{00,i}^2$
4: $\quad \widetilde{s}_1 \leftarrow \mathrm{fl}(\mathrm{fl}(b_{01,r}^2) + \mathrm{fl}(b_{01,i}^2))$
5: $\quad s_1 \leftarrow b_{01,r}^2 + b_{01,i}^2$
6: $\quad \widetilde{g}_{00} \leftarrow \mathrm{fl}(\widetilde{s}_0 + \widetilde{s}_1)$
7: $\quad g_{00} \leftarrow s_0 + s_1$
8: $\quad \widetilde{u} \leftarrow b_{00} \otimes \operatorname{conj} b_{10}$
9: $\quad u \leftarrow b_{00} \operatorname{conj} b_{10}$
10: $\quad \widetilde{v} \leftarrow b_{01} \otimes \operatorname{conj} b_{11}$
11: $\quad v \leftarrow b_{01} \operatorname{conj} b_{11}$
12: $\quad \widetilde{g}_{01} \leftarrow \widetilde{u} \oplus \widetilde{v}$
13: $\quad g_{01} \leftarrow u + v$
14: $\quad \widetilde{s}_2 \leftarrow \mathrm{fl}(\mathrm{fl}(b_{10,r}^2) + \mathrm{fl}(b_{10,i}^2))$
15: $\quad s_2 \leftarrow b_{10,r}^2 + b_{10,i}^2$
16: $\quad \widetilde{s}_3 \leftarrow \mathrm{fl}(\mathrm{fl}(b_{11,r}^2) + \mathrm{fl}(b_{11,i}^2))$
17: $\quad s_3 \leftarrow b_{11,r}^2 + b_{11,i}^2$
18: $\quad \widetilde{g}_{11} \leftarrow \mathrm{fl}(\widetilde{s}_2 + \widetilde{s}_3)$
19: $\quad g_{11} \leftarrow s_2 + s_3$
20: **end for**
21: **return** $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$
22: **return** (g_{00}, g_{01}, g_{11})

Lemma G.22 (The computed Gram diagonals [to table])**.** *Each diagonal entry the code computes is the sum of squares over $\mathbb{R}$ times a factor within $(1+u)^3 - 1$ of 1, plus a term in ζ. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *$b_{00}, b_{01}, b_{10}, b_{11} \in C_{\mathcal{F}}$.*

Define:

- *$g_{00} := |b_{00}|^2 + |b_{01}|^2$;*
- *$g_{11} := |b_{10}|^2 + |b_{11}|^2$;*
- *$\tilde{g}_{00}$ and $\tilde{g}_{11}$, the values Gram (Algorithm 13) computes at lines 2 to 6 and at line 18;*

- $k_H := 4(1+u)^2 + 2(1+u) + 1$.

Assume:

(A1) $u \le 1$.

Then the two diagonals satisfy:

1. $\tilde{g}_{00}\ \mathcal{I}\left(((1+u)^3-1)^{\pm}, k_H\zeta^{\pm}\right)\ g_{00}$;
2. $\tilde{g}_{11}\ \mathcal{I}\left(((1+u)^3-1)^{\pm}, k_H\zeta^{\pm}\right)\ g_{11}$.

Proof.

DEFINES $(b_0, b_1, \tilde{s}_a, \tilde{s}_b, g, \tilde{g})$: either $(b_{00}, b_{01}, \tilde{s}_0, \tilde{s}_1, g_{00}, \tilde{g}_{00})$ or $(b_{10}, b_{11}, \tilde{s}_2, \tilde{s}_3, g_{11}, \tilde{g}_{11})$, with $\tilde{s}_0$ to $\tilde{s}_3$ those of Gram (Algorithm 13), lines 2 to 18

DEFINES $b_j =: b_{j,r} + ib_{j,i}$, $b_{j,r}, b_{j,i} \in \mathcal{F}$, $j \in \{0,1\}$

DEFINES $(\beta_1, \beta_2, \beta_3, \beta_4) := (b_{0,r}, b_{0,i}, b_{1,r}, b_{1,i})$

Proof of items 1 and 2.

(L1) $\forall j \le 4\ \exists\, u_{\beta_j}, \zeta_{\beta_j} \in \mathbb{R},\ |u_{\beta_j}| \le u,\ |\zeta_{\beta_j}| \le \zeta :\ \mathrm{fl}(\beta_j^2) = \beta_j^2(1+u_{\beta_j}) + \zeta_{\beta_j}$
[Definition A.4 for $\times$, at each β_j]

(L2) $\exists\, u_{s_a}, \zeta_{s_a} \in \mathbb{R},\ |u_{s_a}| \le u,\ |\zeta_{s_a}| \le \zeta :\ \tilde{s}_a = (\mathrm{fl}(\beta_1^2) + \mathrm{fl}(\beta_2^2))(1+u_{s_a}) + \zeta_{s_a}$
[Definition A.4 for $+$]

(L3) $\exists\, u_{s_b}, \zeta_{s_b} \in \mathbb{R},\ |u_{s_b}| \le u,\ |\zeta_{s_b}| \le \zeta :\ \tilde{s}_b = (\mathrm{fl}(\beta_3^2) + \mathrm{fl}(\beta_4^2))(1+u_{s_b}) + \zeta_{s_b}$
[Definition A.4 for $+$]

(L4) $\exists\, u_g, \zeta_g \in \mathbb{R},\ |u_g| \le u,\ |\zeta_g| \le \zeta :\ \tilde{g} = (\tilde{s}_a + \tilde{s}_b)(1+u_g) + \zeta_g$
[Definition A.4 for $+$]

(L5) $\Rightarrow\ \tilde{g} = \sum_{j=1}^4 \beta_j^2 P_j + E$, $(P_1, P_2, P_3, P_4) := ((1+u_{\beta_1})(1+u_{s_a})(1+u_g), (1+u_{\beta_2})(1+u_{s_a})(1+u_g), (1+u_{\beta_3})(1+u_{s_b})(1+u_g), (1+u_{\beta_4})(1+u_{s_b})(1+u_g))$, $E := ((\zeta_{\beta_1} + \zeta_{\beta_2})(1+u_{s_a}) + \zeta_{s_a} + (\zeta_{\beta_3} + \zeta_{\beta_4})(1+u_{s_b}) + \zeta_{s_b})(1+u_g) + \zeta_g$
[(L1) to (L4); expand]

(L6) $|E| \le (4(1+u)^2 + 2(1+u) + 1)\zeta$
[(L5); (L1) to (L4); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$]

(L7) $(4(1+u)^2 + 2(1+u) + 1)\zeta = k_H\,\zeta$
[k_H (the statement)]

(I1)

Lemma G.2, item 1 at every $j \le 4$	This proof
Shared: u	
k	3
(t_1, t_2, t_3)	$(u_{\beta_j}, u_{s_a}, u_g),\ j \le 2;\ (u_{\beta_j}, u_{s_b}, u_g),\ j \ge 3$
$u \in [0,1]$	$u \ge 0$ (Definition A.4); assumption A1
$t_1, t_2, t_3 \in \mathbb{R}$	(L1) to (L4)
Assumption A1	(L1) to (L4)
Its item 1: $P \in [(1-u)^k, (1+u)^k]$	

(L8) $\forall j \le 4 :\ P_j \in [(1-u)^3, (1+u)^3]$
[(I1); (L5)]

(L9) $\sum_{j=1}^4 \beta_j^2 = g$
[g (the proof's block); g_{00}, g_{11} (the statement); Fact A.41, item 1: $|a+ib|^2 = a^2 + b^2$]

	Lemma G.3	This proof
	Shared: $u,\ P_1, \dots, P_4$ (L5)	
(I2)	k	3
	m	4
	$(a_1, \dots, a_4)$	$(\beta_1^2, \dots, \beta_4^2)$
	$u \in \mathbb{R}$	$u \geq 0$ (Definition A.4)
	$a_1, \dots, a_4 \geq 0$	$\beta_j \in \mathbb{R}$ (the proof's block); Fact A.41, item 13: $t^{2j} \geq 0$
	$P_1, \dots, P_4 \in [(1-u)^k, (1+u)^k]$	(L8)
	Its conclusion: $\sum_{j=1}^m a_j P_j \in [(1-u)^k A,\ (1+u)^k A]$	
(L10)	$\Rightarrow\ \widetilde{g} - E \in [(1-u)^3 g,\ (1+u)^3 g]$	
		[(I2); (L5), (L9)]

	Lemma G.2, item 2	This proof
	Shared: u	
(I3)	k	3
	(t_1, t_2, t_3)	$(u_{\beta_1}, u_{s_a}, u_g)$
	$u \in [0, 1]$	$u \geq 0$ (Definition A.4); assumption A1
	$t_1, t_2, t_3 \in \mathbb{R}$	(L1), (L2), (L4)
	Assumption A1	(L1), (L2), (L4)
	Its item 2: $p'_k \leq p_k$	
(L11)	$\Rightarrow\ \lvert\widetilde{g} - E - g\rvert \leq ((1+u)^3 - 1)g$	
		[(L10); (I3)]

	Lemma G.1, items 1 and 2	This proof
(I4)	p	$\widetilde{g} - E$
	x	g
	c	$(1+u)^3 - 1$
	$c \geq 0$	$u \geq 0$ (Definition A.4)
	$x, p \in \mathbb{R}$	(L5), (L9)
	Assumption A1	(L9), (L11)
	Its item 1: $\lvert\delta(p, x)\rvert \leq c$	
	Its item 2: $p = x(1 + \delta(p, x))$	
(L12)	$\Rightarrow\ \exists\, \delta \in \mathbb{R},\ \lvert\delta\rvert \leq (1+u)^3 - 1 :\ \widetilde{g} = g(1+\delta) + E$	
		[(I4)]
(L13)	$\Rightarrow\ \widetilde{g}\ \mathcal{I}\left(((1+u)^3 - 1)^{\pm}, (k_H\, \zeta)^{\pm}\right) g$	
		[(L6), (L7), (L12); Definition A.10 at $(u_\circ, \zeta_\circ) := (\delta, E)$; Definition A.9]
(L14)	$\Rightarrow$ item 1	
		[(L13) at $(b_0, b_1) := (b_{00}, b_{01})$; $(\widetilde{s}_a, \widetilde{s}_b, g, \widetilde{g})$ (the proof's block)]
(L15)	$\Rightarrow$ item 2	
		[(L13) at $(b_0, b_1) := (b_{10}, b_{11})$; $(\widetilde{s}_a, \widetilde{s}_b, g, \widetilde{g})$ (the proof's block)]
		□ (items 1 and 2)

Lemma G.23 (The computed Gram off-diagonal entry [to table])**.** *The off-diagonal entry the code computes is within u of the one over $\mathbb{R}$, plus a term in the diagonals' geometric mean and in ζ. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *$b_{00}, b_{01}, b_{10}, b_{11} \in C_{\mathcal{F}}$.*

Define:

- *$g_{00} := \lvert b_{00}\rvert^2 + \lvert b_{01}\rvert^2$;*

- $g_{11} := |b_{10}|^2 + |b_{11}|^2$;
- $g_{01} := b_{00}\,\mathrm{conj}(b_{10}) + b_{01}\,\mathrm{conj}(b_{11})$;
- $\tilde{g}_{01}$, *the value* Gram *(Algorithm 13) computes at lines 8 to 12;*
- $k'_H := \sqrt{2}\,(2(3+2u)(1+u)+1)$.

Then

$$\tilde{g}_{01}\,\mathcal{N}\left(u, (1+u)\sqrt{2}u(2+u)\sqrt{g_{00}g_{11}} + k'_H\zeta\right) g_{01}.$$

Proof.

(I1)

Lemma B.2, item 3	This proof
Shared: u, ζ	
a	b_{00}
b	$\mathrm{conj}(b_{10})$
$a, b \in C_{\mathcal{F}}$	$b_{00}, b_{10} \in C_{\mathcal{F}}$ (the statement); Definition A.4, item 7
Its item 3: $(a \otimes b)\ \mathcal{I}\left((\sqrt{2}\,u(2+u))^{\pm}, k_B\,\zeta^{\pm}\right)\ ab$	

(I1) $\exists\,\delta_1, e_1 \in \mathbb{C},\ |\delta_1| \le \sqrt{2}u(2+u),\ |e_1| \le k_B\,\zeta:\ b_{00} \otimes \mathrm{conj}(b_{10}) = b_{00}\,\mathrm{conj}(b_{10})(1+\delta_1) + e_1$ [(I1)]

Lemma B.2, item 3	This proof
Shared: u, ζ	
a	b_{01}
b	$\mathrm{conj}(b_{11})$
$a, b \in C_{\mathcal{F}}$	$b_{01}, b_{11} \in C_{\mathcal{F}}$ (the statement); Definition A.4, item 7
Its item 3: $(a \otimes b)\ \mathcal{I}\left((\sqrt{2}\,u(2+u))^{\pm}, k_B\,\zeta^{\pm}\right)\ ab$	

(I2) $\exists\,\delta_2, e_2 \in \mathbb{C},\ |\delta_2| \le \sqrt{2}u(2+u),\ |e_2| \le k_B\,\zeta:\ b_{01} \otimes \mathrm{conj}(b_{11}) = b_{01}\,\mathrm{conj}(b_{11})(1+\delta_2) + e_2$ [(I2)]

Lemma B.2, item 1	This proof
Shared: u, ζ	
a	$b_{00} \otimes \mathrm{conj}(b_{10})$
b	$b_{01} \otimes \mathrm{conj}(b_{11})$
$a, b \in C_{\mathcal{F}}$	$b_{00}, b_{01}, b_{10}, b_{11} \in C_{\mathcal{F}}$ (the statement); Definition A.4, item 7; Definition A.8
Its item 1: $(a \oplus b)\ \mathcal{I}\left(u^{\pm}, \sqrt{2}\,\zeta^{\pm}\right)\ (a+b)$	

(I3) $\exists\,\delta_3, e_3 \in \mathbb{C},\ |\delta_3| \le u,\ |e_3| \le \sqrt{2}\,\zeta:\ \tilde{g}_{01} = (b_{00} \otimes \mathrm{conj}(b_{10}) + b_{01} \otimes \mathrm{conj}(b_{11}))(1+\delta_3) + e_3$ [(I3)]

(L4) $\Rightarrow\ \tilde{g}_{01} - g_{01} = g_{01}\delta_3 + (b_{00}\,\mathrm{conj}(b_{10})\delta_1 + b_{01}\,\mathrm{conj}(b_{11})\delta_2)(1+\delta_3) + ((e_1+e_2)(1+\delta_3) + e_3)$
[(L1), (L2), (L3); g_{01} (the statement); expand]

(L5) $\Rightarrow\ |\tilde{g}_{01} - g_{01}| \le u|g_{01}| + (1+u)\sqrt{2}u(2+u)(|b_{00}||b_{10}| + |b_{01}||b_{11}|) + (2k_B(1+u) + \sqrt{2})\,\zeta$
[(L4); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$, $|\mathrm{conj}\,x| = |x|$; (L1), (L2), (L3)]

(L6) $|b_{00}||b_{10}| + |b_{01}||b_{11}| \le \sqrt{g_{00}g_{11}}$
[Fact A.41, item 4; g_{00}, g_{11} (the statement)]

(L7) $2k_B(1+u) + \sqrt{2} = k'_H$
[k_B (Lemma B.2); k'_H (the statement)]

(L8) $\Rightarrow\ |\tilde{g}_{01} - g_{01}| \le u|g_{01}| + (1+u)\sqrt{2}u(2+u)\sqrt{g_{00}g_{11}} + k'_H\,\zeta$
[(L5), (L6), (L7)]

(L9) $\Rightarrow\ \tilde{g}_{01}\,\mathcal{N}\left(u, (1+u)\sqrt{2}\,u(2+u)\sqrt{g_{00}g_{11}} + k'_H\,\zeta\right) g_{01}$
[(L8); Definition A.11]

(L10) $\Rightarrow$ the statement
[(L9)]

□

G.3.5 The $LDL^\dagger$ step

Structure. Lemma G.24 states the computed $LDL^\dagger$ step; Lemma G.25 its computed second diagonal.

Lemma G.24 (The computed $LDL^\dagger$ step [to table])**.** *The $LDL^\dagger$ step's computed quotient and factor are within two roundings of the ones over $\mathbb{R}$ and the computed Schur product within four; each plus a term in ζ. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *$g_{00} \in \mathcal{F}$;*
- *$g_{01} = g_{01,r} + i g_{01,i} \in C_{\mathcal{F}}$.*

Define:

- *μ, l_{10} and zo, those of* LDL† *(Algorithm 5), lines 11 to 15, over $\mathbb{R}$;*
- *$\widetilde{\mu}$, $\widetilde{l_{10}}$ and $\widetilde{zo}$, the values* LDL† *(Algorithm 5) computes in $\mathcal{F}$, lines 2 to 14;*
- *$k_\mu := \sqrt{2}\,(|g_{01}|(1+u)+1)$;*
- *$k_{zo} := \sqrt{2}\,|g_{01}|^2(1+u)^3 + \sqrt{2}\,|g_{01}|(1+u)^2 + 2(1+u) + 1$.*

Assume:

(A1) $u \le 1$;

(A2) $g_{00} > 0$.

Then the three computed values deviate as follows:

1. $\exists\, \delta, e \in \mathbb{C},\ |\delta| \le (1+u)^2 - 1,\ |e| \le k_\mu\, \zeta:\quad \widetilde{\mu} = \mu(1+\delta) + e$;
2. $\exists\, \delta', e' \in \mathbb{C},\ |\delta'| \le (1+u)^2 - 1,\ |e'| \le k_\mu\, \zeta:\quad \widetilde{l_{10}} = l_{10}(1+\delta') + e'$;
3. $\exists\, \delta_{zo}, E_{zo} \in \mathbb{R},\ |\delta_{zo}| \le (1+u)^4 - 1,\ |E_{zo}| \le k_{zo}\, \zeta:\quad \widetilde{zo} = zo(1+\delta_{zo}) + E_{zo}$.

Proof.

DEFINES	$\mu =: \mu_r + i\mu_i$, $\mu_r, \mu_i \in \mathbb{R}$
COMPUTES	$\widetilde{\mu} =: \widetilde{\mu}_r + i\widetilde{\mu}_i$ (LDL† (Algorithm 5), the lines of $\widetilde{\mu}$)
COMPUTES	$\widetilde{\iota}$ at $\mathcal{F} \neq \mathcal{F}_{\mathrm{fx}}$ (LDL†, line 2)
DEFINES	$\widetilde{\iota} := 1/g_{00}$ at $\mathcal{F} = \mathcal{F}_{\mathrm{fx}}$
DEFINES	$e := (g_{01,r}\zeta_\iota(1+u_{\mu_r}) + \zeta_{\mu_r}) + i\,(g_{01,i}\zeta_\iota(1+u_{\mu_i}) + \zeta_{\mu_i})$, u_ι, u_{μ_r}, u_{μ_i}, ζ_ι, ζ_{μ_r}, ζ_{μ_i} those of (L1) to (L3)

Proof of item 1.

(L1) $\exists\, u_\iota, \zeta_\iota \in \mathbb{R},\ |u_\iota| \le u,\ |\zeta_\iota| \le \zeta:\ \widetilde{\iota} = (1/g_{00})(1+u_\iota) + \zeta_\iota$
[at $\mathcal{F} \neq \mathcal{F}_{\mathrm{fx}}$, Definition A.4 for / (LDL†, line 2); at $\mathcal{F} = \mathcal{F}_{\mathrm{fx}}$, $(u_\iota, \zeta_\iota) := (0,0)$ and $\widetilde{\iota} = 1/g_{00}$ (the proof's block)]

(L2) $\exists\, u_{\mu_r}, \zeta_{\mu_r} \in \mathbb{R},\ |u_{\mu_r}| \le u,\ |\zeta_{\mu_r}| \le \zeta:\ \widetilde{\mu}_r = g_{01,r}\widetilde{\iota}(1+u_{\mu_r}) + \zeta_{\mu_r}$
[at $\mathcal{F} \neq \mathcal{F}_{\mathrm{fx}}$, Definition A.4 for $\times$; at $\mathcal{F} = \mathcal{F}_{\mathrm{fx}}$, Definition A.4 for / (LDL†, line 7) and $g_{01,r}/g_{00} = g_{01,r}\widetilde{\iota}$ (the proof's block)]

(L3) $\exists\, u_{\mu_i}, \zeta_{\mu_i} \in \mathbb{R},\ |u_{\mu_i}| \le u,\ |\zeta_{\mu_i}| \le \zeta:\ \widetilde{\mu}_i = g_{01,i}\widetilde{\iota}(1+u_{\mu_i}) + \zeta_{\mu_i}$
[at $\mathcal{F} \neq \mathcal{F}_{\mathrm{fx}}$, Definition A.4 for $\times$; at $\mathcal{F} = \mathcal{F}_{\mathrm{fx}}$, Definition A.4 for / (LDL†, line 8) and $g_{01,i}/g_{00} = g_{01,i}\widetilde{\iota}$ (the proof's block)]

(L4) $\Rightarrow\ \widetilde{\mu} = \mu_r(1+u_\iota)(1+u_{\mu_r}) + i\,\mu_i(1+u_\iota)(1+u_{\mu_i}) + e$
[e (the proof's block); (L1), (L2), (L3); $\mu = g_{01}/g_{00}$ (LDL† (Algorithm 5), line 11)]

(L5) $|\mathrm{Re}\, e| \le (|g_{01}|(1+u)+1)\,\zeta$
[(L4); (L1), (L2); Fact A.41, item 1: $|\mathrm{Re}\, x| \le |x|$ at $x := g_{01}$, $|x+y| \le |x| + |y|$, $|xy| = |x||y|$]

(L6) $|\mathrm{Im}\, e| \le (|g_{01}|(1+u)+1)\,\zeta$
[(L4); (L1), (L3); Fact A.41, item 1: $|\mathrm{Im}\, x| \le |x|$ at $x := g_{01}$, $|x+y| \le |x| + |y|$, $|xy| = |x||y|$]

(L7) $\Rightarrow\ |e| \le k_\mu\,\zeta$

[(L5), (L6); Fact A.41, item 1: $|a+ib|^2 = a^2+b^2$; k_μ (the statement)]

(L8) $|\widetilde{\mu} - e - \mu|^2 = \mu_r^2((1+u_\iota)(1+u_{\mu_r})-1)^2 + \mu_i^2((1+u_\iota)(1+u_{\mu_i})-1)^2$

[(L4); Fact A.41, item 1: $|a+ib|^2 = a^2+b^2$]

Lemma G.2, item 3 at every $s \in \{r,i\}$	This proof
Shared: u	
k	2
(t_1,t_2)	(u_ι, u_{μ_s})
$u \in [0,1]$	$u \ge 0$ (Definition A.4); assumption A1
$t_1,t_2 \in \mathbb{R}$	(L1), (L2), (L3)
Assumption A1	(L1), (L2), (L3)
Its item 3: $\lvert P-1\rvert \le p_k$	

(I1)

(L9) $\Rightarrow\ |\widetilde{\mu} - e - \mu| \le ((1+u)^2-1)|\mu|$

[(L8); (I1); Fact A.41, item 5: $t \mapsto \sqrt{t}$ nondecreasing]

Lemma B.1	This proof
p	$\widetilde{\mu} - e$
x	μ
c	$(1+u)^2-1$
$c \ge 0$	$u \ge 0$ (Definition A.4)
$x,p \in \mathbb{C}$	μ, $\widetilde{\mu}$, e (the proof's block)
$\lvert p-x\rvert \le c\lvert x\rvert$	(L9)
Its conclusion: $\lvert\delta(p,x)\rvert \le c,\ p = x(1+\delta(p,x))$	

(I2)

(L10) $\Rightarrow\ \exists\,\delta\in\mathbb{C},\ |\delta| \le (1+u)^2-1:\ \widetilde{\mu} = \mu(1+\delta)+e$

[(I2); (L7)]

(L11) $\Rightarrow$ item 1

[(L10)]

□ (item 1)

Proof of item 2.

(L12) $\widetilde{l}_{10} = \operatorname{conj}\widetilde{\mu}$

[LDL† (Algorithm 5), line 12; Definition A.4, item 7]

(L13) $\Rightarrow\ \widetilde{l}_{10} = \operatorname{conj}\mu\,(1+\operatorname{conj}\delta) + \operatorname{conj} e$

[(L10), (L12); Fact A.41, item 13: $\operatorname{conj}x+y = \operatorname{conj}x + \operatorname{conj}y$, $\operatorname{conj}xy = \operatorname{conj}x\,\operatorname{conj}y$]

(L14) $l_{10} = \operatorname{conj}\mu$

[LDL† (Algorithm 5), line 13]

(L15) $|\operatorname{conj}\delta| = |\delta|$

[Fact A.41, item 1: $|\operatorname{conj}x| = |x|$]

(L16) $|\operatorname{conj} e| = |e|$

[Fact A.41, item 1: $|\operatorname{conj}x| = |x|$]

(L17) $\Rightarrow\ \exists\,\delta',e'\in\mathbb{C},\ |\delta'| \le (1+u)^2-1,\ |e'| \le k_\mu\,\zeta:\ \widetilde{l}_{10} = l_{10}(1+\delta') + e'$

[(L13) to (L16) at $(\delta',e') := (\operatorname{conj}\delta, \operatorname{conj} e)$; (L7), (L10)]

(L18) $\Rightarrow$ item 2

[(L17)]

□ (item 2)

Proof of item 3.

(L19) $\exists\,u_{zo,r},\zeta_{zo,r}\in\mathbb{R},\ |u_{zo,r}| \le u,\ |\zeta_{zo,r}| \le \zeta:\ \operatorname{fl}(\widetilde{\mu}_r\, g_{01,r}) = \widetilde{\mu}_r g_{01,r}(1+u_{zo,r}) + \zeta_{zo,r}$

[Definition A.4 for $\times$]

(L20) $\exists\,u_{zo,i},\zeta_{zo,i}\in\mathbb{R},\ |u_{zo,i}| \le u,\ |\zeta_{zo,i}| \le \zeta:\ \operatorname{fl}(\widetilde{\mu}_i\, g_{01,i}) = \widetilde{\mu}_i g_{01,i}(1+u_{zo,i}) + \zeta_{zo,i}$

[Definition A.4 for $\times$]

(L21) $\exists\, u_{zo}, \zeta_{zo} \in \mathbb{R},\ |u_{zo}| \le u,\ |\zeta_{zo}| \le \zeta :\ \widetilde{zo} = (\mathrm{fl}(\widetilde{\mu}_r\, g_{01,r}) + \mathrm{fl}(\widetilde{\mu}_i\, g_{01,i}))(1 + u_{zo}) + \zeta_{zo}$
[Definition A.4 for $+$]

(L22) $\mu_r g_{01,r} = g_{01,r}^2 / g_{00}$
[$\mu = g_{01}/g_{00}$ (LDL† (Algorithm 5), line 11); μ_r (the proof's block); $g_{00} \in \mathbb{R}$ (Definition A.14)]

(L23) $\mu_i g_{01,i} = g_{01,i}^2 / g_{00}$
[$\mu = g_{01}/g_{00}$ (LDL† (Algorithm 5), line 11); μ_i (the proof's block); $g_{00} \in \mathbb{R}$ (Definition A.14)]

(L24) $\Rightarrow\ \widetilde{zo} = \frac{g_{01,r}^2}{g_{00}} P_1 + \frac{g_{01,i}^2}{g_{00}} P_2 + E_{zo}, \quad (P_1, P_2) := ((1+u_\iota)(1+u_{\mu_r})(1+u_{zo,r})(1+u_{zo}), (1+u_\iota)(1+u_{\mu_i})(1+u_{zo,i})(1+u_{zo})),\ E_{zo} := (\mathrm{Re}(e) g_{01,r}(1+u_{zo,r}) + \zeta_{zo,r} + \mathrm{Im}(e) g_{01,i}(1+u_{zo,i}) + \zeta_{zo,i})(1+u_{zo}) + \zeta_{zo}$
[(L4), (L19) to (L23); expand]

(L25) $|g_{01,r}| + |g_{01,i}| \le \sqrt{2}|g_{01}|$
[Fact A.41, item 4, at $X := (|g_{01,r}|, |g_{01,i}|)$, $Y := (1,1)$]

(L26) $|E_{zo}| \le k_{zo}\, \zeta$
[(L24), (L5), (L6), (L25); (L1) to (L3), (L19) to (L21); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$; k_{zo} (the statement)]

(I3)

Lemma G.2, item 1 at every $s \in \{r, i\}$	This proof
Shared: u	
k	4
(t_1, t_2, t_3, t_4)	$(u_\iota, u_{\mu_s}, u_{zo,s}, u_{zo})$
$u \in [0, 1]$	$u \ge 0$ (Definition A.4); assumption A1
$t_1, \ldots, t_4 \in \mathbb{R}$	(L1) to (L3), (L19) to (L21)
Assumption A1	(L1) to (L3), (L19) to (L21)
Its item 1: $P \in [(1-u)^k, (1+u)^k]$	

(L27) $P_1 \in [(1-u)^4, (1+u)^4]$
[(I3) at $s = r$; (L24)]

(L28) $P_2 \in [(1-u)^4, (1+u)^4]$
[(I3) at $s = i$; (L24)]

(L29) $\frac{g_{01,r}^2}{g_{00}} + \frac{g_{01,i}^2}{g_{00}} = zo$
[$zo = |g_{01}|^2 / g_{00}$ (LDL† (Algorithm 5), line 15; Lemma D.4, item 4)]

(I4)

Lemma G.3	This proof
Shared: $u,\ P_1, P_2$ (L24)	
k	4
m	2
(a_1, a_2)	$(g_{01,r}^2/g_{00}, g_{01,i}^2/g_{00})$
$u \in \mathbb{R}$	$u \ge 0$ (Definition A.4)
$a_1, a_2 \ge 0$	Assumption A2; Fact A.41, item 13: $t^{2j} \ge 0$
$P_1, P_2 \in [(1-u)^k, (1+u)^k]$	(L27), (L28)
Its conclusion: $\sum_{j=1}^m a_j P_j \in [(1-u)^k A,\ (1+u)^k A]$	

(L30) $\Rightarrow\ \widetilde{zo} - E_{zo} \in [zo\,(1-u)^4,\ zo\,(1+u)^4]$
[(I4); (L24), (L29)]

	Lemma G.2, item 2	This proof
	Shared: u	
(I5)	k	4
	(t_1, t_2, t_3, t_4)	$(u_\iota, u_{\mu_r}, u_{zo,r}, u_{zo})$
	$u \in [0, 1]$	$u \geq 0$ (Definition A.4); assumption A1
	$t_1, \ldots, t_4 \in \mathbb{R}$	(L1), (L2), (L19), (L21)
	Assumption A1	(L1), (L2), (L19), (L21)
	Its item 2: $p'_k \leq p_k$	
(L31)	$\lvert\widetilde{zo} - E_{zo} - zo\rvert \leq ((1+u)^4 - 1)zo$	
		[(L30); (I5)]

	Lemma G.1, items 1 and 2	This proof
(I6)	p	$\widetilde{zo} - E_{zo}$
	x	zo
	c	$(1+u)^4 - 1$
	$c \geq 0$	$u \geq 0$ (Definition A.4)
	$x, p \in \mathbb{R}$	(L24), (L29)
	Assumption A1	(L29), (L31); assumption A2
	Its item 1: $\lvert\delta(p, x)\rvert \leq c$	
	Its item 2: $p = x(1 + \delta(p, x))$	
(L32)	$\Rightarrow\ \exists\, \delta_{zo} \in \mathbb{R},\ \lvert\delta_{zo}\rvert \leq (1+u)^4 - 1 :\ \widetilde{zo} = zo(1+\delta_{zo}) + E_{zo}$	
		[(I6); (L26)]
(L33)	$\Rightarrow$ item 3	
		[(L32)]
		□ (item 3)

Lemma G.25 (The computed second diagonal of the $LDL^\dagger$ step [to table])**.** *The $LDL^\dagger$ step's computed second diagonal is within one rounding of the one over $\mathbb{R}$ plus the computed Schur product's deviation scaled by κ, plus a term in ζ. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *$g_{00}, g_{11} \in \mathcal{F}$;*
- *$g_{01} \in C_{\mathcal{F}}$.*

Define:

- *zo and d_{11}, those of* LDL† *(Algorithm 5), lines 15 and 19, over $\mathbb{R}$;*
- *$\widetilde{zo}$ and $\widetilde{d}_{11}$, the values* LDL† *(Algorithm 5) computes in $\mathcal{F}$, lines 14 and 18;*
- *$k_{zo} := \sqrt{2}\,|g_{01}|^2(1+u)^3 + \sqrt{2}\,|g_{01}|(1+u)^2 + 2(1+u) + 1$ (Lemma G.24);*
- *$\kappa := |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$.*

Assume:

(A1) $u \leq 1$;

(A2) $g_{00} > 0$;

(A3) $g_{00}g_{11} > |g_{01}|^2$.

Then the computed second diagonal deviates as follows:

$$\exists\, E \in \mathbb{R},\ |E| \leq (u + \kappa((1+u)^4 - 1)(1+u))|d_{11}| + (k_{zo}(1+u) + 1)\,\zeta :\quad \widetilde{d}_{11} = d_{11} + E.$$

Proof. (I1)

Lemma G.24, item 3	This proof

Shared: $\mathcal{F}, (u, \zeta),\ g_{00}, g_{01},\ zo, \widetilde{zo},\ k_{zo}$
Shared: $g_{00} \in \mathcal{F},\ g_{01} \in C_{\mathcal{F}}$
Shared: assumptions A1, A2

Its conclusion: $\exists\, \delta_{zo}, E_{zo} \in \mathbb{R},\ |\delta_{zo}| \le (1+u)^4 - 1,\ |E_{zo}| \le k_{zo}\,\zeta :\ \widetilde{zo} = zo(1+\delta_{zo}) + E_{zo}$

$\exists\, \delta_{zo}, E_{zo} \in \mathbb{R},\ |\delta_{zo}| \le (1+u)^4 - 1,\ |E_{zo}| \le k_{zo}\,\zeta :\ \widetilde{zo} = zo(1+\delta_{zo}) + E_{zo}$

[(I1)]

(L2) $\exists\, u_{d_{11}}, \zeta_{d_{11}} \in \mathbb{R},\ |u_{d_{11}}| \le u,\ |\zeta_{d_{11}}| \le \zeta :\ \widetilde{d}_{11} = (g_{11} - \widetilde{zo})(1+u_{d_{11}}) + \zeta_{d_{11}}$

[Definition A.4 for $-$]

(L3) $\Rightarrow\ \widetilde{d}_{11} = (g_{11} - zo(1+\delta_{zo}) - E_{zo})(1+u_{d_{11}}) + \zeta_{d_{11}}$

[(L2), (L1)]

(L4) $\Rightarrow\ \widetilde{d}_{11} = (d_{11} - zo\,\delta_{zo} - E_{zo})(1+u_{d_{11}}) + \zeta_{d_{11}}$

[(L3); $d_{11} = g_{11} - zo$ (LDL† (Algorithm 5), line 19)]

(L5) $\Rightarrow\ \widetilde{d}_{11} - d_{11} = d_{11}u_{d_{11}} - zo\,\delta_{zo}(1+u_{d_{11}}) - E_{zo}(1+u_{d_{11}}) + \zeta_{d_{11}}$

[(L4); expand]

(L6) $zo \ge 0$

[$zo = |g_{01}|^2/g_{00}$ (LDL† (Algorithm 5), line 15); $g_{00} > 0$ (assumption A2)]

(L7) $\Rightarrow\ |\widetilde{d}_{11} - d_{11}| \le u|d_{11}| + zo\,((1+u)^4 - 1)(1+u) + (k_{zo}(1+u) + 1)\,\zeta$

[(L5); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$; (L1), (L2), (L6)]

(L8) $d_{11} = (g_{00}g_{11} - |g_{01}|^2)/g_{00}$

[$d_{11} = g_{11} - zo$, $zo = |g_{01}|^2/g_{00}$ (LDL† (Algorithm 5), lines 15 and 19)]

(L9) $zo = \kappa\, d_{11}$

[$zo = |g_{01}|^2/g_{00}$ (LDL† (Algorithm 5), line 15); (L8); κ (the statement); assumption A3]

(L10) $d_{11} > 0$

[(L8); assumption A3; $g_{00} > 0$ (assumption A2)]

(L11) $\Rightarrow\ \exists\, E \in \mathbb{R},\ |E| \le (u + \kappa((1+u)^4 - 1)(1+u))|d_{11}| + (k_{zo}(1+u) + 1)\,\zeta :\ \widetilde{d}_{11} = d_{11} + E$

[(L7), (L9), (L10) at $E := \widetilde{d}_{11} - d_{11}$]

(L12) $\Rightarrow$ the statement

[(L11)]

□

G.4 The computed diagonals

Structure. This subsection proves the bounds on the computed diagonals. Figure 53 describes their relative deviation χ; Section G.4.1 states one node and the recursion; Section G.4.2 the root node; Section G.4.3 the leaf standard deviation and l_{10}.

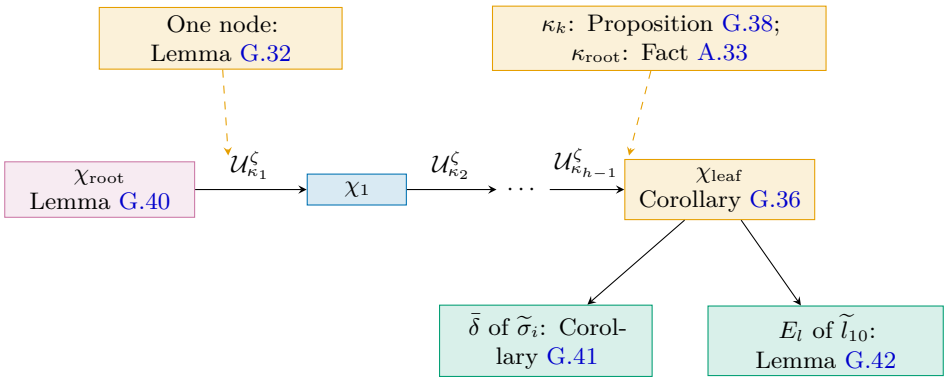


Figure 53: Section G.4: the relative deviation χ of the computed diagonals, from the root node to the leaves, and the two quantities the rest of the report takes from it.

G.4.1 One node and the recursion

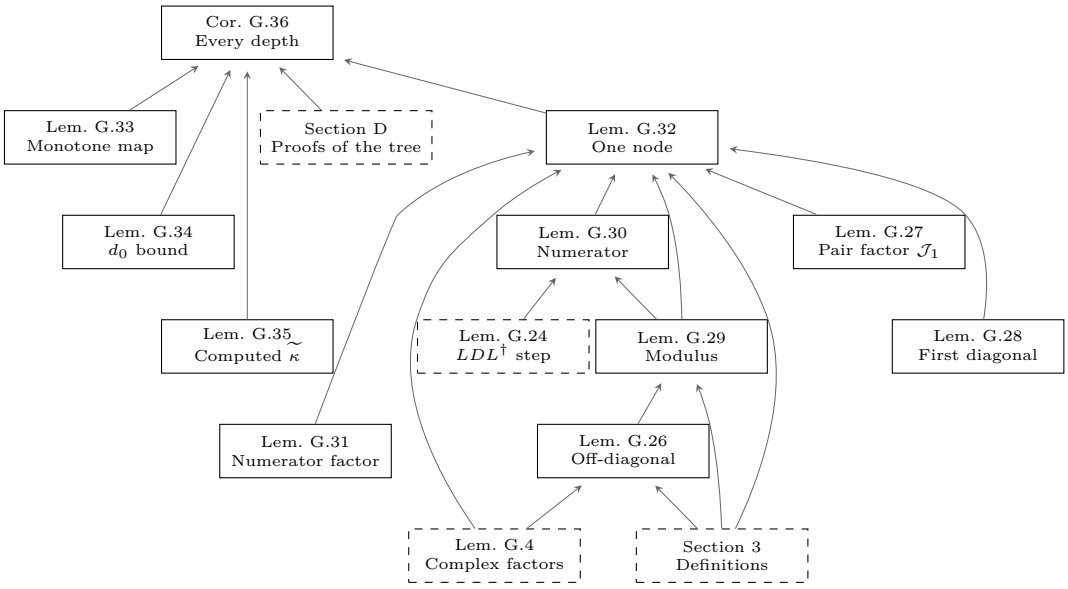


Figure 54: Dependencies, Section G.4.1.

Structure. Lemmas G.26 to G.31 state the steps at one node; Lemma G.32 the computed diagonals at one node; Lemma G.33 the monotonicity of the bound map; Lemma G.35 the computed pair's $\widetilde{\kappa}$; Corollary G.36 the computed diagonals at every depth.

Lemma G.26 (A child's computed off-diagonal [to table])**.** *At a pair of real computed values, the off-diagonal the self-adjoint split computes is the half-difference over $\mathbb{R}$ times the conjugate root, times a factor within c_{sa} of 1, plus a term in ζ. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *$\psi \in \mathbb{C}$;*
- *$\widetilde{\psi} \in C_{\mathcal{F}}$;*
- *$\widetilde{a}, \widetilde{b} \in \mathcal{F}$.*

Define:

- *$\widetilde{d}_1$, the value $\mathrm{split}_{\mathrm{sa}}$ (Algorithm 3) computes in $\mathcal{F}$ from $(f(\psi), f(-\psi)) := (\widetilde{a}, \widetilde{b})$ at line 6, with $\widetilde{s} := \widetilde{\psi}$;*
- *$c_{\mathrm{sa}} := (1+u)^2(1+u+\sqrt{2}\,\zeta) - 1$;*
- *$k_{\mathrm{sa}} := (1+u)(1+u+\sqrt{2}\,\zeta)/2 + \sqrt{2}$.*

Assume:

(A1) $|\psi| = 1$;

(A2) $|\widetilde{\psi} - \psi| \le u + \sqrt{2}\,\zeta$.

Then

$$\exists\, \delta_{\mathrm{sa}}, e_{\mathrm{sa}} \in \mathbb{C},\ |\delta_{\mathrm{sa}}| \le c_{\mathrm{sa}},\ |e_{\mathrm{sa}}| \le k_{\mathrm{sa}}\zeta : \quad \widetilde{d}_1 = \tfrac{\widetilde{a}-\widetilde{b}}{2}\,\mathrm{conj}(\psi)(1+\delta_{\mathrm{sa}}) + e_{\mathrm{sa}}.$$

Proof.

COMPUTES $\widetilde{h} := \mathrm{fl}((\widetilde{a} \ominus \widetilde{b})/2) \in \mathcal{F}$ ($\mathrm{split}_{\mathrm{sa}}$ (Algorithm 3), line 6)
DEFINES $e_p := \zeta_r + i\zeta_i$, ζ_r, ζ_i those of (L3)
DEFINES $\delta_{\mathrm{sa}} := (1+u_\circ)(1+\mathrm{conj}\,\delta_c)(1+\delta_p) - 1$, $u_\circ$, δ_c, δ_p those of (L1), (L2), (L4)
DEFINES $e_{\mathrm{sa}} := \frac{\zeta_\circ}{2}\,\mathrm{conj}(\psi)(1+\mathrm{conj}\,\delta_c)(1+\delta_p) + e_p$, $\zeta_\circ$ that of (L1)

(L1) $\exists\, u_\circ, \zeta_\circ \in \mathbb{R},\ |u_\circ| \le u,\ |\zeta_\circ| \le \zeta :\ \widetilde{h} = \frac{(\widetilde{a}-\widetilde{b})(1+u_\circ)+\zeta_\circ}{2}$

[Definition A.4, item 4, at $\circ := -$]

	Lemma B.1	This proof
	p	$\widetilde{\psi}$
	x	ψ
	c	$u + \sqrt{2}\,\zeta$
(I1)	$c \geq 0$	$u, \zeta \geq 0$ (Definition A.4)
	$x \in \mathbb{C}$	$\psi \in \mathbb{C}$ (the statement)
	$p \in \mathbb{C}$	$\widetilde{\psi} \in C_{\mathcal{F}}$ (the statement); Definition A.8
	$\lvert p - x\rvert \leq c\lvert x\rvert$	Assumptions A1, A2
	Its conclusion: $\lvert\delta(p,x)\rvert \leq c,\ p = x(1+\delta(p,x))$	

(L2) $\exists\, \delta_c \in \mathbb{C},\ |\delta_c| \leq u + \sqrt{2}\,\zeta :\ \widetilde{\psi} = \psi(1+\delta_c)$

[(I1)]

(L3) $\exists\, u_r, u_i, \zeta_r, \zeta_i \in \mathbb{R},\ |u_\cdot| \leq u,\ |\zeta_\cdot| \leq \zeta :\ \widetilde{d}_1 = \widetilde{h}\,\mathrm{Re}\,\mathrm{conj}\,\widetilde{\psi}(1+u_r) + \zeta_r + i(\widetilde{h}\,\mathrm{Im}\,\mathrm{conj}\,\widetilde{\psi}(1+u_i) + \zeta_i)$

[$\widetilde{h} \otimes \mathrm{conj}\,\widetilde{\psi} = \mathrm{fl}(\widetilde{h}\,\mathrm{Re}\,\mathrm{conj}\,\widetilde{\psi}) + i\,\mathrm{fl}(\widetilde{h}\,\mathrm{Im}\,\mathrm{conj}\,\widetilde{\psi})$ (Definition A.8); Definition A.4, items 1 and 7]

	Lemma G.13	This proof
	c	u
	x	$\widetilde{h}\,\mathrm{conj}\,\widetilde{\psi}$
	(x_r, x_i)	$(\widetilde{h}\,\mathrm{Re}\,\mathrm{conj}\,\widetilde{\psi}, \widetilde{h}\,\mathrm{Im}\,\mathrm{conj}\,\widetilde{\psi})$
	(P_1, P_2)	$(1+u_r, 1+u_i)$
	$c \in \mathbb{R}$	$u \geq 0$ (Definition A.4)
(I2)	$x \in \mathbb{C}$	$\widetilde{\psi} \in C_{\mathcal{F}}$ (the statement); $\widetilde{h} \in \mathcal{F}$ (the proof's block)
	$x_r, x_i \in \mathbb{R}$	$\widetilde{h} \in \mathcal{F}$ (the proof's block)
	$P_1, P_2 \in \mathbb{R}$	(L3)
	Assumption A1	(L3)
	Assumption A2	(L3)
	Its conclusion: $\exists\,\delta \in \mathbb{C},\ \lvert\delta\rvert \leq c :\ x_r P_1 + i x_i P_2 = x(1+\delta)$	

(L4) $\Rightarrow\ \exists\, \delta_p \in \mathbb{C},\ |\delta_p| \leq u :\ \widetilde{d}_1 = \widetilde{h}\ \mathrm{conj}\,\widetilde{\psi}(1+\delta_p) + e_p$

[e_p (the proof's block); (L3); (I2)]

(L5) $|e_p| \leq \sqrt{2}\,\zeta$

[(L3); Fact A.41, item 1: $|a+ib|^2 = a^2 + b^2$]

(L6) $\Rightarrow\ \widetilde{d}_1 = \frac{\widetilde{a}-\widetilde{b}}{2}\,\mathrm{conj}(\psi)(1+\delta_{\mathrm{sa}}) + e_{\mathrm{sa}}$

[δ_{sa}, e_{sa} (the proof's block); (L1), (L2), (L4); expand]

	Lemma G.4	This proof
	k	3
	$(\delta_1, \delta_2, \delta_3)$	$(u_\circ, \mathrm{conj}\,\delta_c, \delta_p)$
	(c_1, c_2, c_3)	$(u, u + \sqrt{2}\,\zeta, u)$
(I3)	$\delta_1, \delta_2, \delta_3 \in \mathbb{C}$	(L1), (L2), (L4)
	$c_1, c_2, c_3 \geq 0$	$u, \zeta \geq 0$ (Definition A.4)
	Assumption A1	(L1), (L2), (L4); $\lvert\mathrm{conj}\,\delta_c\rvert = \lvert\delta_c\rvert$ (Fact A.41, item 1)
	Its conclusion: $\lvert\prod_{j=1}^k (1+\delta_j) - 1\rvert \leq \prod_{j=1}^k (1+c_j) - 1$	

(L7) $|\delta_{\mathrm{sa}}| \leq c_{\mathrm{sa}}$

[(L6); (I3); δ_{sa} (the proof's block); c_{sa} (the statement)]

(L8) $|e_{\mathrm{sa}}| \leq \frac{\zeta}{2}(1 + u + \sqrt{2}\,\zeta)(1+u) + \sqrt{2}\,\zeta$

[(L6); Fact A.41, item 1: $|x+y| \leq |x| + |y|$, $|xy| = |x||y|$, $|\mathrm{conj}\,x| = |x|$; $|\psi| = 1$ (assumption A1); (L1), (L2), (L4), (L5)]

(L9) $\frac{\zeta}{2}(1 + u + \sqrt{2}\,\zeta)(1+u) + \sqrt{2}\,\zeta = k_{\mathrm{sa}}\zeta$

[k_{sa} (the statement)]

(L10) $\Rightarrow\ \exists\, \delta_{\mathrm{sa}}, e_{\mathrm{sa}} \in \mathbb{C},\ |\delta_{\mathrm{sa}}| \leq c_{\mathrm{sa}},\ |e_{\mathrm{sa}}| \leq k_{\mathrm{sa}}\zeta :\ \widetilde{d}_1 = \frac{\widetilde{a}-\widetilde{b}}{2}\,\mathrm{conj}(\psi)(1+\delta_{\mathrm{sa}}) + e_{\mathrm{sa}}$

[(L6) to (L9)]

(L11) $\Rightarrow$ the statement

[(L10)]

□

Lemma G.27 (The pair factor $\mathcal{J}_1$ [to table])**.** *Perturbing a positive pair by relative amounts at most χ multiplies the ratio of its harmonic-mean numerator to the harmonic mean by a factor near 1. Let:*

- $a, b > 0$;
- $\chi \in [0, 1)$;
- $\omega_a, \omega_b \in \mathbb{R}$.

Define:

- $\widetilde{a} := a(1 + \omega_a)$;
- $\widetilde{b} := b(1 + \omega_b)$;
- $\widetilde{A} := (\widetilde{a} + \widetilde{b})/2$;
- $w := a/(a + b)$;
- $\mathrm{HM}(a, b) := 2ab/(a + b)$ *(Definition A.46)*;
- $\mathcal{J}_1 := \dfrac{(1 + \omega_a)(1 + \omega_b)}{1 + w\omega_a + (1 - w)\omega_b}$.

Assume:

(A1) $|\omega_a| \le \chi$;

(A2) $|\omega_b| \le \chi$.

Then the ratio is $\mathcal{J}_1$ and $\mathcal{J}_1$ lies in the interval:

1. $\dfrac{\widetilde{a}\widetilde{b}/\widetilde{A}}{\mathrm{HM}(a, b)} = \mathcal{J}_1$;

2. $\mathcal{J}_1 \in \left[1 - \chi,\ 1 + \dfrac{\chi + \chi^2}{1 - \chi}\right]$.

Proof.

DEFINES $A := (a + b)/2$

DEFINES $N := (1 - w)\omega_a + w\omega_b + \omega_a\omega_b$

DEFINES $W := 1 + w\omega_a + (1 - w)\omega_b$

Proof of item 1.

(L1) $\widetilde{a}\widetilde{b}/(ab) = (1 + \omega_a)(1 + \omega_b)$

[$\widetilde{a}$, $\widetilde{b}$ (the statement)]

(L2) $\widetilde{A}/A = W$

[$\widetilde{A}$, w (the statement); A, W (the proof's block)]

(L3) $\mathrm{HM}(a, b) = ab/A$

[HM (the statement); A (the proof's block)]

(L4) $\Rightarrow$ $\dfrac{\widetilde{a}\widetilde{b}/\widetilde{A}}{\mathrm{HM}(a,b)} = \dfrac{\widetilde{a}\widetilde{b}/(ab)}{\widetilde{A}/A}$

[(L3)]

(L5) $\dfrac{\widetilde{a}\widetilde{b}/(ab)}{\widetilde{A}/A} = \mathcal{J}_1$

[(L1), (L2); $\mathcal{J}_1$ (the statement)]

(L6) $\Rightarrow$ $\dfrac{\widetilde{a}\widetilde{b}/\widetilde{A}}{\mathrm{HM}(a,b)} = \mathcal{J}_1$

[(L4), (L5)]

(L7) $\Rightarrow$ item 1

[(L6)]

□ (item 1)

Proof of item 2.

(L8) $(1+\omega_a)(1+\omega_b) - W = N$
[N, W (the proof's block); expand]

(L9) $\Rightarrow\ \mathcal{J}_1 = 1 + N/W$
[(L8); $\mathcal{J}_1$ (the statement); W (the proof's block)]

(L10) $w \in [0,1]$
[w (the statement); $a, b > 0$ (the statement)]

(L11) $N \geq -\chi - \chi^2$
[(L10); N (the proof's block); assumptions A1, A2]

(L12) $N \leq \chi + \chi^2$
[(L10); N (the proof's block); assumptions A1, A2]

(L13) $W \geq 1 - \chi$
[(L10); W (the proof's block); assumptions A1, A2]

(L14) $\Rightarrow\ \mathcal{J}_1 \leq 1 + \frac{\chi+\chi^2}{1-\chi}$
[(L9), (L11) to (L13); $\chi < 1$ (the statement)]

(L15) $(a+b)(w\omega_a + (1-w)\omega_b) = a\omega_a + b\omega_b$
[w (the statement)]

(L16) $(a+b)((1+\omega_a)(1+\omega_b) - (1-\chi)W) = a(1+\omega_a)(\chi+\omega_b) + b(1+\omega_b)(\chi+\omega_a)$
[(L15); W (the proof's block); expand]

(L17) $\forall c \in \{a, b\}:\ 1 + \omega_c \geq 1 - \chi$
[assumptions A1, A2]

(L18) $1 - \chi > 0$
[$\chi < 1$ (the statement)]

(L19) $\forall c \in \{a, b\}:\ \chi + \omega_c \geq 0$
[assumptions A1, A2]

(L20) $a(1+\omega_a)(\chi+\omega_b) \geq 0$
[$a > 0$ (the statement); (L17), (L18), (L19); Fact A.41, item 8]

(L21) $b(1+\omega_b)(\chi+\omega_a) \geq 0$
[$b > 0$ (the statement); (L17), (L18), (L19); Fact A.41, item 8]

(L22) $\Rightarrow\ (1-\chi)W \leq (1+\omega_a)(1+\omega_b)$
[(L16), (L20), (L21); $a + b > 0$ (the statement)]

(L23) $\Rightarrow\ 1 - \chi \leq \mathcal{J}_1$
[(L13), (L18), (L22); $\mathcal{J}_1$ (the statement)]

(L24) $\Rightarrow\ \mathcal{J}_1 \in \left[1-\chi,\ 1+\frac{\chi+\chi^2}{1-\chi}\right]$
[(L14), (L23)]

(L25) $\Rightarrow$ item 2
[(L24)]

□ (item 2)

Lemma G.28 (The child's computed first diagonal [to table])**.** *At a perturbed pair, the first diagonal the self-adjoint split computes is the pair's mean within u_0. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $d_{\mathrm{lo}} > 0$*;*
- $a, b \in [d_{\mathrm{lo}}, \infty)$*;*
- $\widetilde{\psi} \in C_{\mathcal{F}}$*;*
- $\chi \in [0, 1)$*;*
- $\omega_a, \omega_b \in \mathbb{R}$.

Define:

- $\widetilde{a} := a(1+\omega_a)$;
- $\widetilde{b} := b(1+\omega_b)$;
- $\widetilde{d_0}$, *the value* $\mathrm{split}_{\mathrm{sa}}$ *(Algorithm 3) computes in* $\mathcal{F}$ *from* $(f(\psi), f(-\psi)) := (\widetilde{a}, \widetilde{b})$ *at line 4, with* $\widetilde{s} := \widetilde{\psi}$;
- $\widetilde{A} := (\widetilde{a} + \widetilde{b})/2$;
- $m_1 := d_{\mathrm{lo}}(1-\chi)(1-u)$;
- $u_0 := (1+u)(1+\zeta/(2m_1)) - 1$.

Assume:

(A1) $\widetilde{a}, \widetilde{b} \in \mathcal{F}$;

(A2) $u < 1$;

(A3) $|\omega_a| \le \chi$;

(A4) $|\omega_b| \le \chi$.

Then

$$\exists\, u_{d_0} \in \mathbb{R},\ |u_{d_0}| \le u_0 : \quad \widetilde{d_0} = \widetilde{A}(1+u_{d_0}).$$

Proof.

DEFINES $u_{d_0} := (1+u_s)(1+\zeta_s/(2\widetilde{A}(1+u_s))) - 1$, u_s, ζ_s those of (L1), its denominator positive by (L4) to (L6)

(L1) $\exists\, u_s, \zeta_s \in \mathbb{R},\ |u_s| \le u,\ |\zeta_s| \le \zeta :\ \widetilde{d_0} = \widetilde{A}(1+u_s) + \zeta_s/2$

[Definition A.4, item 4, at $\circ := +$ [L0: `sign_fpoly.c:2350-2362`]; $\widetilde{a}, \widetilde{b} \in \mathcal{F}$ (assumption A1); $\widetilde{A}$ (the statement)]

(L2) $\widetilde{a} \ge d_{\mathrm{lo}}(1-\chi)$

[$a \ge d_{\mathrm{lo}}$ (the statement); $|\omega_a| \le \chi$ (assumption A3)]

(L3) $\widetilde{b} \ge d_{\mathrm{lo}}(1-\chi)$

[$b \ge d_{\mathrm{lo}}$ (the statement); $|\omega_b| \le \chi$ (assumption A4)]

(L4) $\widetilde{A}(1+u_s) \ge d_{\mathrm{lo}}(1-\chi)(1-u)$

[(L1), (L2), (L3); $\widetilde{A}$ (the statement)]

(L5) $d_{\mathrm{lo}}(1-\chi)(1-u) = m_1$

[m_1 (the statement)]

(L6) $m_1 > 0$

[$m_1 = d_{\mathrm{lo}}(1-\chi)(1-u)$ (the statement); $d_{\mathrm{lo}} > 0$, $\chi < 1$, $u < 1$ (assumption A2)]

(L7) $\Rightarrow\ \widetilde{d_0} = \widetilde{A}(1+u_{d_0})$

[u_{d_0} (the proof's block); (L1), (L4), (L5), (L6)]

(I1)

Lemma G.4	This proof
k	2
(δ_1, δ_2)	$(u_s, \zeta_s/(2\widetilde{A}(1+u_s)))$
(c_1, c_2)	$(u, \zeta/(2m_1))$
$\delta_1, \delta_2 \in \mathbb{C}$	(L1), (L4), (L5), (L6)
$c_1, c_2 \ge 0$	$u, \zeta \ge 0$ (Definition A.4); (L6)
Assumption A1	(L1), (L4), (L5), (L6)
Its conclusion: $\lvert\prod_{j=1}^{k}(1+\delta_j) - 1\rvert \le \prod_{j=1}^{k}(1+c_j) - 1$	

(L8) $\Rightarrow\ |u_{d_0}| \le (1+u)(1+\zeta/(2m_1)) - 1$

[(L7); (I1)]

(L9) $(1+u)(1+\zeta/(2m_1)) - 1 = u_0$

[u_0 (the statement)]

(L10) $\Rightarrow\ \exists\, u_{d_0} \in \mathbb{R},\ |u_{d_0}| \le u_0 :\ \widetilde{d_0} = \widetilde{A}(1+u_{d_0})$

[(L7), (L8), (L9)]

(L11) $\Rightarrow$ the statement

[(L10)]

□

Lemma G.29 (The modulus of the child's computed off-diagonal [to table])**.** *At a perturbed pair, the off-diagonal the self-adjoint split computes has squared modulus within the split's bounds of the pair's squared half-difference and modulus at most M_2. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$*;*
- $a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$*;*
- $\psi \in \mathbb{C}$*;*
- $\widetilde{\psi} \in C_{\mathcal{F}}$*;*
- $\chi \in [0, 1)$*;*
- $\omega_a, \omega_b \in \mathbb{R}$.

Define:

- $\widetilde{a} := a(1 + \omega_a)$*;*
- $\widetilde{b} := b(1 + \omega_b)$*;*
- $\widetilde{d}_1$*, the value* $\mathrm{split}_{\mathrm{sa}}$ *(Algorithm 3) computes in* $\mathcal{F}$ *from* $(f(\psi), f(-\psi)) := (\widetilde{a}, \widetilde{b})$ *at line 6, with* $\widetilde{s} := \widetilde{\psi}$*;*
- $\widetilde{D} := |\widetilde{a} - \widetilde{b}|/2$*;*
- $c_{\mathrm{sa}} := (1 + u)^2(1 + u + \sqrt{2}\,\zeta) - 1$ *(Lemma G.26);*
- $k_{\mathrm{sa}} := (1 + u)(1 + u + \sqrt{2}\,\zeta)/2 + \sqrt{2}$ *(Lemma G.26);*
- $M_1 := d_{\mathrm{hi}}(1 + \chi)/2$*;*
- $M_2 := M_1(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta$*;*
- $\mathcal{H} := 2\widetilde{D}(1 + c_{\mathrm{sa}})k_{\mathrm{sa}}\zeta + (k_{\mathrm{sa}}\zeta)^2$.

Assume:

(A1) $\widetilde{a}, \widetilde{b} \in \mathcal{F}$*;*
(A2) $|\omega_a| \le \chi$*;*
(A3) $|\omega_b| \le \chi$*;*
(A4) $|\psi| = 1$*;*
(A5) $|\widetilde{\psi} - \psi| \le u + \sqrt{2}\,\zeta$.

Then the child's computed off-diagonal satisfies:

1. $\big||\widetilde{d}_1|^2 - \widetilde{D}^2\big| \le \widetilde{D}^2((1 + c_{\mathrm{sa}})^2 - 1) + \mathcal{H}$*;*
2. $|\widetilde{d}_1| \le M_2$.

Proof.

DEFINES $c := c_{\mathrm{sa}}$

Proof of item 1.

Lemma G.26	This proof
Shared: $\mathcal{F}, (u, \zeta),\ \psi, \widetilde{\psi}, \widetilde{a}, \widetilde{b},\ \widetilde{d}_1,\ c_{\mathrm{sa}}, k_{\mathrm{sa}}$ Shared: $\psi \in \mathbb{C},\ \widetilde{\psi} \in C_{\mathcal{F}}$	
(I1) $\widetilde{a}, \widetilde{b} \in \mathcal{F}$	Assumption A1
Assumption A1 Assumption A2	Assumption A4 Assumption A5
Its conclusion: $\exists\, \delta_{\mathrm{sa}}, e_{\mathrm{sa}} \in \mathbb{C},\ \lvert\delta_{\mathrm{sa}}\rvert \le c_{\mathrm{sa}},\ \lvert e_{\mathrm{sa}}\rvert \le k_{\mathrm{sa}}\zeta :\ \widetilde{d}_1 = \frac{\widetilde{a}-\widetilde{b}}{2}\,\mathrm{conj}(\psi)(1 + \delta_{\mathrm{sa}}) + e_{\mathrm{sa}}$	

(L1) $\exists\, \delta_{\mathrm{sa}}, e_{\mathrm{sa}} \in \mathbb{C},\ |\delta_{\mathrm{sa}}| \le c,\ |e_{\mathrm{sa}}| \le k_{\mathrm{sa}}\zeta :\ \widetilde{d}_1 = \frac{\widetilde{a}-\widetilde{b}}{2}\,\mathrm{conj}(\psi)(1 + \delta_{\mathrm{sa}}) + e_{\mathrm{sa}}$
[(I1)]

(L2) $|\widetilde{d}_1| \le \widetilde{D}(1 + c) + k_{\mathrm{sa}}\zeta$
[(L1); Fact A.41, item 1: $|x + y| \le |x| + |y|$, $|xy| = |x||y|$; $|\psi| = 1$ (assumption A4); $\widetilde{D}$ (the statement)]

(L3) $|\widetilde{d}_1| \ge \widetilde{D}(1 - c) - k_{\mathrm{sa}}\zeta$
[(L1); Fact A.41, item 1: $||x| - |y|| \le |x - y|$]

(L4) $|\widetilde{d}_1|^2 - \widetilde{D}^2 \le \widetilde{D}^2((1+c)^2-1) + \mathcal{H}$

[(L2); Fact A.41, item 5: $t \mapsto t^2$ nondecreasing on $[0,\infty)$; $\mathcal{H}$ (the statement)]

(L5) $\widetilde{D}(1-c) \ge k_{\mathrm{sa}}\zeta \Rightarrow\ \widetilde{D}^2 - |\widetilde{d}_1|^2 \le \widetilde{D}^2(2c-c^2) + 2\widetilde{D}(1-c)k_{\mathrm{sa}}\zeta$

[(L3); Fact A.41, item 5: $t \mapsto t^2$ nondecreasing on $[0,\infty)$]

(L6) $2c - c^2 \le 2c + c^2$

[Fact A.41, item 13: $t^{2j} \ge 0$ at $(t,j) := (c,1)$]

(L7) $c, \widetilde{D}, k_{\mathrm{sa}}\zeta \ge 0$

[c_{sa}, k_{sa} (Lemma G.26); $u, \zeta \ge 0$ (Definition A.4); $\widetilde{D}$ (the statement)]

(L8) $1 - c \le 1 + c$

[(L7)]

(L9) $\widetilde{D}^2(2c-c^2) + 2\widetilde{D}(1-c)k_{\mathrm{sa}}\zeta \le \widetilde{D}^2((1+c)^2-1) + \mathcal{H}$

[(L6), (L8); (L7); $\mathcal{H}$ (the statement)]

(L10) $\Rightarrow\ \widetilde{D}(1-c) \ge k_{\mathrm{sa}}\zeta \Rightarrow\ \widetilde{D}^2 - |\widetilde{d}_1|^2 \le \widetilde{D}^2((1+c)^2-1) + \mathcal{H}$

[(L5), (L9)]

(L11) $c < 1/2 \Rightarrow\ 1 - c > 1/2$

[subtract]

(L12) $\widetilde{D}(1-c) < k_{\mathrm{sa}}\zeta,\ c < 1/2 \Rightarrow\ \widetilde{D} < 2k_{\mathrm{sa}}\zeta$

[(L11)]

(L13) $\widetilde{D}^2 - |\widetilde{d}_1|^2 \le \widetilde{D}^2$

[Fact A.41, item 13: $t^{2j} \ge 0$ at $(t,j) := (|\widetilde{d}_1|, 1)$]

(L14) $\widetilde{D}(1-c) < k_{\mathrm{sa}}\zeta,\ c < 1/2 \Rightarrow\ \widetilde{D}^2 \le 2\widetilde{D}k_{\mathrm{sa}}\zeta$

[(L12); (L7)]

(L15) $2\widetilde{D}k_{\mathrm{sa}}\zeta \le \mathcal{H}$

[$\mathcal{H}$ (the statement); (L7)]

(L16) $\Rightarrow\ \widetilde{D}(1-c) < k_{\mathrm{sa}}\zeta,\ c < 1/2 \Rightarrow\ \widetilde{D}^2 - |\widetilde{d}_1|^2 \le \mathcal{H}$

[(L13), (L14), (L15)]

(L17) $c \ge 1/2 \Rightarrow\ (1+c)^2 - 1 \ge 5/4$

[Fact A.41, item 5: $t \mapsto t^2$ nondecreasing on $[0,\infty)$, at $1 + c \ge 3/2$]

(L18) $c \ge 1/2 \Rightarrow\ \widetilde{D}^2 \le \widetilde{D}^2((1+c)^2-1)$

[(L17); $\widetilde{D}^2 \ge 0$ (Fact A.41, item 13)]

(L19) $\Rightarrow\ c \ge 1/2 \Rightarrow\ \widetilde{D}^2 - |\widetilde{d}_1|^2 \le \widetilde{D}^2((1+c)^2-1)$

[(L13), (L18)]

(L20) $\mathcal{H}, \widetilde{D}^2((1+c)^2-1) \ge 0$

[$\mathcal{H}$ (the statement); (L7); Fact A.41, items 13 and 8]

(L21) $\Rightarrow\ \big||\widetilde{d}_1|^2 - \widetilde{D}^2\big| \le \widetilde{D}^2((1+c_{\mathrm{sa}})^2-1) + \mathcal{H}$

[(L4), (L10), (L16), (L19), the three cases covering every $(\widetilde{D}, c)$; (L20)]

(L22) $\Rightarrow$ item 1

[(L21)]

□ (item 1)

Proof of item 2.

(L23) $\widetilde{a} \le d_{\mathrm{hi}}(1+\chi)$

[$a \le d_{\mathrm{hi}}$ (the statement); $|\omega_a| \le \chi$ (assumption A2)]

(L24) $\widetilde{b} \le d_{\mathrm{hi}}(1+\chi)$

[$b \le d_{\mathrm{hi}}$ (the statement); $|\omega_b| \le \chi$ (assumption A3)]

(L25) $\widetilde{a}, \widetilde{b} > 0$

[$\widetilde{a}$, $\widetilde{b}$ (the statement); $a, b \ge d_{\mathrm{lo}}$, $d_{\mathrm{lo}} > 0$ (the statement); $|\omega_a|, |\omega_b| \le \chi$ (assumptions A2, A3); $\chi < 1$ (the statement)]

(L26) $\widetilde{D} \le \max(\widetilde{a}, \widetilde{b})/2$

[$\widetilde{D}$ (the statement); (L25)]

(L27) $\Rightarrow$ $\widetilde{D} \le M_1$

[(L23), (L24), (L26); M_1 (the statement)]

(L28) $\Rightarrow$ $|\widetilde{d}_1| \le M_2$

[(L2), (L27); M_2 (the statement)]

(L29) $\Rightarrow$ item 2

[(L28)]

□ (item 2)

Lemma G.30 (The child's computed numerator [to table])**.** *At a perturbed pair, the numerator of the child's second diagonal is the pair's product times a factor near* 1*. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$*;*
- $a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$*;*
- $\psi \in \mathbb{C}$*;*
- $\widetilde{\psi} \in C_{\mathcal{F}}$*;*
- $\chi \in [0, 1)$*;*
- $\omega_a, \omega_b \in \mathbb{R}$*;*
- $u_{d_0} \in \mathbb{R}$*.*

Define:

- *The perturbed pair*
  - $\widetilde{a} := a(1 + \omega_a)$*;*
  - $\widetilde{b} := b(1 + \omega_b)$*;*
- *The node bounds*
  - $c_{\mathrm{sa}} := (1 + u)^2(1 + u + \sqrt{2}\,\zeta) - 1$ *(Lemma G.26);*
  - $k_{\mathrm{sa}} := (1 + u)(1 + u + \sqrt{2}\,\zeta)/2 + \sqrt{2}$ *(Lemma G.26);*
  - $\widetilde{A} := (\widetilde{a} + \widetilde{b})/2$ *(Lemma G.28);*
  - $u_0 := (1 + u)(1 + \zeta/(2d_{\mathrm{lo}}(1 - \chi)(1 - u))) - 1$ *(Lemma G.28 at* $m_1 := d_{\mathrm{lo}}(1 - \chi)(1 - u)$*);*
  - $\widetilde{D} := |\widetilde{a} - \widetilde{b}|/2$ *(Lemma G.29);*
  - $M_1 := d_{\mathrm{hi}}(1 + \chi)/2$ *(Lemma G.29);*
  - $M_2 := M_1(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta$ *(Lemma G.29);*
  - $\bar{k}_{zo} := \sqrt{2}\,M_2^2(1 + u)^3 + \sqrt{2}\,M_2(1 + u)^2 + 2(1 + u) + 1$*;*
- *The computed values*
  - $(\widetilde{d}_0, \widetilde{d}_1)$*, the values* $\mathrm{split}_{\mathrm{sa}}$ *(Algorithm 3) computes in* $\mathcal{F}$ *from* $(f(\psi), f(-\psi)) := (\widetilde{a}, \widetilde{b})$ *at lines 4, 6, with* $\widetilde{s} := \widetilde{\psi}$*;*
  - $\widetilde{zo}$*, the value* $\mathrm{LDL}^{\dagger}$ *(Algorithm 5) computes in* $\mathcal{F}$ *at line 14 on* $(g_{00}, g_{01}, g_{11}) := (\widetilde{d}_0, \widetilde{d}_1, \widetilde{d}_0)$*;*
- *The terms*
  - $\widetilde{\kappa} := (\widetilde{a} - \widetilde{b})^2/(4\widetilde{a}\widetilde{b})$*.*

Assume:

(A1) $\widetilde{a}, \widetilde{b} \in \mathcal{F}$*;*
(A2) $u < 1$*;*
(A3) $|\omega_a| \le \chi$*;*
(A4) $|\omega_b| \le \chi$*;*
(A5) $|\psi| = 1$*;*
(A6) $|\widetilde{\psi} - \psi| \le u + \sqrt{2}\,\zeta$*;*
(A7) $u_0 < 1$*;*
(A8) $|u_{d_0}| \le u_0$*;*
(A9) $\widetilde{d}_0 = \widetilde{A}(1 + u_{d_0})$*.*

Then the child's computed values satisfy:

1. $\exists\, \delta_{zo}, E_{zo} \in \mathbb{R},\ |\delta_{zo}| \le (1 + u)^4 - 1,\ |E_{zo}| \le \bar{k}_{zo}\zeta :\ \widetilde{zo}\,\widetilde{d}_0 = |\widetilde{d}_1|^2(1 + \delta_{zo}) + E_{zo}\widetilde{d}_0$*;*

2. Define, at the δ_{zo}, E_{zo} of item 1:

- $\mathcal{M} := (|\widetilde{d}_1|^2 - \widetilde{D}^2)(1+\delta_{zo}) + E_{zo}\widetilde{d}_0$.

Then $(\widetilde{d}_0 - \widetilde{zo})\,\widetilde{d}_0 = \widetilde{a}\widetilde{b}\left((1+u_{d_0})^2 + \widetilde{\kappa}\left((1+u_{d_0})^2 - 1 - \delta_{zo}\right) - \mathcal{M}/(\widetilde{a}\widetilde{b})\right)$.

Proof.

DEFINES $k'_{zo} := \sqrt{2}\,|\widetilde{d}_1|^2(1+u)^3 + \sqrt{2}\,|\widetilde{d}_1|(1+u)^2 + 2(1+u) + 1$, the k_{zo} of Lemma G.24 at $|g_{01}| := |\widetilde{d}_1|$

Proof of item 1.

(L1) $\widetilde{a} \geq d_{\text{lo}}(1-\chi)$

[$a \geq d_{\text{lo}}$ (the statement); $|\omega_a| \leq \chi$ (assumption A3)]

(L2) $\widetilde{b} \geq d_{\text{lo}}(1-\chi)$

[$b \geq d_{\text{lo}}$ (the statement); $|\omega_b| \leq \chi$ (assumption A4)]

(L3) $\widetilde{d}_0 > 0$

[$\widetilde{d}_0 = \widetilde{A}(1+u_{d_0})$, $|u_{d_0}| \leq u_0$ (assumptions A9, A8); $u_0 < 1$ (assumption A7); $\widetilde{A} > 0$ by (L1), (L2), $d_{\text{lo}} > 0$, $\chi < 1$ (the statement)]

Lemma G.24, item 3	This proof
Shared: $\mathcal{F}$, $\widetilde{zo}$	
g_{00}, g_{01}	$\widetilde{d}_0, \widetilde{d}_1$ (the statement)
zo	$\frac{\widetilde{d}_1\overline{\widetilde{d}_1}}{\widetilde{d}_0}$ (LDL† (Algorithm 5), line 15)
k_{zo}	k'_{zo} (the proof's block)
(I1) E_{zo}	E'_{zo}
$\mathcal{F}$ realization at (u,ζ)	The statement
$g_{00} \in \mathcal{F}$	$\widetilde{d}_0$ (the statement)
$g_{01} \in C_{\mathcal{F}}$	$\widetilde{d}_1$ (the statement)
Assumption A1	$u < 1$ (assumption A2)
Assumption A2	(L3)
Its conclusion: $\exists\,\delta_{zo}, E_{zo} \in \mathbb{R},\ \|\delta_{zo}\| \leq (1+u)^4 - 1,\ \|E_{zo}\| \leq k_{zo}\,\zeta :\ \widetilde{zo} = zo(1+\delta_{zo}) + E_{zo}$	

(L4) $\exists\,\delta_{zo}, E'_{zo} \in \mathbb{R},\ |\delta_{zo}| \leq (1+u)^4 - 1,\ |E'_{zo}| \leq k'_{zo}\zeta :\ \widetilde{zo} = \frac{|\widetilde{d}_1|^2}{\widetilde{d}_0}(1+\delta_{zo}) + E'_{zo}$

[(I1)]

Lemma G.29, item 2	This proof
Shared: $\mathcal{F}$, $d_{\text{lo}}, d_{\text{hi}}$, a, b, $\psi, \widetilde{\psi}$, χ, ω_a, ω_b, $\widetilde{a}, \widetilde{b}, \widetilde{d}_1$, $\widetilde{D}, M_2$	
Shared: $d_{\text{lo}}, d_{\text{hi}} > 0$, $a, b \in [d_{\text{lo}}, d_{\text{hi}}]$, $\psi \in \mathbb{C}$, $\widetilde{\psi} \in C_{\mathcal{F}}$, $\chi \in [0,1)$, $\omega_a, \omega_b \in \mathbb{R}$	
$\mathcal{F}$ realization at (u,ζ)	The statement
(I2) Assumption A1	Assumption A1
Assumption A2	Assumption A3
Assumption A3	Assumption A4
Assumption A4	Assumption A5
Assumption A5	Assumption A6
Its conclusion: $\|\widetilde{d}_1\| \leq M_2$	

(L5) $|\widetilde{d}_1| \leq M_2$

[(I2)]

(L6) $k'_{zo} \leq \bar{k}_{zo}$

[(L5); k'_{zo} (the proof's block); $\bar{k}_{zo}$ (the statement); Fact A.41, item 5: $t \mapsto t^p$ nondecreasing on $[0,\infty)$]

(L7) $\Rightarrow\ \exists\,\delta_{zo}, E_{zo} \in \mathbb{R},\ |\delta_{zo}| \leq (1+u)^4 - 1,\ |E_{zo}| \leq \bar{k}_{zo}\zeta :\ \widetilde{zo}\,\widetilde{d}_0 = |\widetilde{d}_1|^2(1+\delta_{zo}) + E_{zo}\widetilde{d}_0$

[(L4), (L6) at $E_{zo} := E'_{zo}$; multiply by $\widetilde{d}_0$]

(L8) $\Rightarrow$ item 1

[(L7)]

□ (item 1)

Proof of item 2.

(L9) $\forall x, y \in \mathbb{R}:\ (x+y)^2 - (x-y)^2 = 4xy$

[expand]

(L10) $\widetilde{A}^2 = \widetilde{a}\widetilde{b} + \widetilde{D}^2$

[$\widetilde{A}$, $\widetilde{D}$ (the statement); (L9) at $(x, y) := (\widetilde{a}, \widetilde{b})$]

(L11) $\widetilde{D}^2 = \widetilde{\kappa}\,\widetilde{a}\widetilde{b}$

[$\widetilde{\kappa}$, $\widetilde{D}$ (the statement)]

(L12) $(\widetilde{d_0} - \widetilde{zo})\widetilde{d_0} = \widetilde{A}^2(1+u_{d_0})^2 - |\widetilde{d_1}|^2(1+\delta_{zo}) - E_{zo}\widetilde{d_0}$

[assumption A9; item 1]

(L13) $\Rightarrow\ (\widetilde{d_0} - \widetilde{zo})\widetilde{d_0} = \widetilde{a}\widetilde{b}(1+u_{d_0})^2 + \widetilde{D}^2((1+u_{d_0})^2 - 1 - \delta_{zo}) - \mathcal{M}$

[(L10), (L12); $\mathcal{M}$ (the statement)]

(L14) $\Rightarrow\ (\widetilde{d_0} - \widetilde{zo})\widetilde{d_0} = \widetilde{a}\widetilde{b}\left((1+u_{d_0})^2 + \widetilde{\kappa}\left((1+u_{d_0})^2 - 1 - \delta_{zo}\right) - \mathcal{M}/(\widetilde{a}\widetilde{b})\right)$

[(L11), (L13); $\widetilde{a}\widetilde{b} > 0$ by (L1), (L2)]

(L15) $\Rightarrow$ item 2

[(L14)]

□ (item 2)

Lemma G.31 (The factor of the computed numerator [to table])**.** *At a perturbed pair, the factor that multiplies the pair's product in the computed numerator of the second diagonal is within a bound set by u_0, the pair's $\widetilde{\kappa}$ and a term in ζ of 1. Let:*

- $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$;
- $u, \zeta \geq 0$;
- $\chi \in [0, 1)$;
- $\widetilde{a}, \widetilde{b} > 0$;
- $\widetilde{d_0} \in \mathbb{R}$;
- $\widetilde{d_1} \in \mathbb{C}$;
- $u_{d_0}, \delta_{zo}, E_{zo} \in \mathbb{R}$.

Define:

- *The node bounds*
  - $c_{\mathrm{sa}} := (1+u)^2(1+u+\sqrt{2}\,\zeta) - 1$ *(Lemma G.26);*
  - $k_{\mathrm{sa}} := (1+u)(1+u+\sqrt{2}\,\zeta)/2 + \sqrt{2}$ *(Lemma G.26);*
  - $\widetilde{A} := (\widetilde{a} + \widetilde{b})/2$ *(Lemma G.28);*
  - $u_0 := (1+u)(1+\zeta/(2d_{\mathrm{lo}}(1-\chi)(1-u))) - 1$ *(Lemma G.28 at $m_1 := d_{\mathrm{lo}}(1-\chi)(1-u)$);*
  - $\widetilde{D} := |\widetilde{a} - \widetilde{b}|/2$ *(Lemma G.29);*
  - $M_1 := d_{\mathrm{hi}}(1+\chi)/2$ *(Lemma G.29);*
  - $M_2 := M_1(1+c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta$ *(Lemma G.29);*
  - $\mathcal{H} := 2\widetilde{D}(1+c_{\mathrm{sa}})k_{\mathrm{sa}}\zeta + (k_{\mathrm{sa}}\zeta)^2$ *(Lemma G.29);*
  - $\bar{k}_{zo} := \sqrt{2}\,M_2^2(1+u)^3 + \sqrt{2}\,M_2(1+u)^2 + 2(1+u) + 1$ *(Lemma G.30);*
- *The terms*
  - $\widetilde{\kappa} := (\widetilde{a} - \widetilde{b})^2/(4\widetilde{a}\widetilde{b})$ *(Lemma G.30);*
  - $r' := (1+c_{\mathrm{sa}})^2(1+u)^4 - 1$;
  - $\mathcal{Q} := \left(2(1+c_{\mathrm{sa}})k_{\mathrm{sa}}\zeta(1+u)^4 + \bar{k}_{zo}\,\zeta\,(1+u_0)\right)/(d_{\mathrm{lo}}(1-\chi)) + (k_{\mathrm{sa}}\zeta)^2(1+u)^4/(d_{\mathrm{lo}}(1-\chi))^2$;
  - $\mathcal{M} := (|\widetilde{d_1}|^2 - \widetilde{D}^2)(1+\delta_{zo}) + E_{zo}\widetilde{d_0}$.

Assume:

(A1) $\widetilde{a} \geq d_{\mathrm{lo}}(1-\chi)$;

(A2) $\widetilde{b} \geq d_{\mathrm{lo}}(1-\chi)$;

(A3) $u_0 < 1$;

(A4) $|u_{d_0}| \le u_0$;
(A5) $\widetilde{d}_0 = \widetilde{A}(1+u_{d_0})$;
(A6) $||\widetilde{d}_1|^2 - \widetilde{D}^2| \le \widetilde{D}^2((1+c_{\mathrm{sa}})^2-1) + \mathcal{H}$;
(A7) $|\delta_{zo}| \le (1+u)^4 - 1$;
(A8) $|E_{zo}| \le \bar{k}_{zo}\zeta$.
Then

$$|(1+u_{d_0})^2 + \widetilde{\kappa}\left((1+u_{d_0})^2 - 1 - \delta_{zo}\right) - \mathcal{M}/(\widetilde{a}\widetilde{b}) - 1| \le (1+\widetilde{\kappa})((1+u_0)^2-1) + \widetilde{\kappa}r' + \mathcal{Q}.$$

Proof. (L1) $\widetilde{a}\widetilde{b} \ge d_{\mathrm{lo}}(1-\chi)\widetilde{A}$
[$\widetilde{a}, \widetilde{b} \ge d_{\mathrm{lo}}(1-\chi)$ (assumptions A1, A2); Fact A.41, item 8: its second clause, its (m,s,t) set to $(d_{\mathrm{lo}}(1-\chi), \widetilde{a}, \widetilde{b})$]

(L2) $\widetilde{D} \le \widetilde{A}$
[$\widetilde{D}$, $\widetilde{A}$ (the statement); Fact A.41, item 1: $|x-y| \le |x| + |y|$; $\widetilde{a}, \widetilde{b} > 0$ (the statement)]

(L3) $\widetilde{A} > 0$
[$\widetilde{A}$ (the statement); $\widetilde{a}, \widetilde{b} > 0$ (the statement)]

(L4) $\widetilde{d}_0 \ge \widetilde{A}(1-u_0)$
[$\widetilde{d}_0 = \widetilde{A}(1+u_{d_0})$, $|u_{d_0}| \le u_0$ (assumptions A4, A5); (L3)]

(L5) $\widetilde{d}_0 \le \widetilde{A}(1+u_0)$
[$\widetilde{d}_0 = \widetilde{A}(1+u_{d_0})$, $|u_{d_0}| \le u_0$ (assumptions A4, A5); (L3)]

(L6) $\widetilde{d}_0 \ge 0$
[(L4); $u_0 < 1$ (assumption A3)]

(L7) $||M \le (\widetilde{D}^2((1+c_{\mathrm{sa}})^2-1) + \mathcal{H})(1+u)^4 + \bar{k}_{zo}\,\zeta\,\widetilde{d}_0$
[$\mathcal{M}$ (the statement); assumptions A6, A7, A8; (L6); Fact A.41, item 1]

(L8) $\widetilde{D}/(\widetilde{a}\widetilde{b}) \le 1/(d_{\mathrm{lo}}(1-\chi))$
[(L1), (L2)]

(L9) $\widetilde{A}/(\widetilde{a}\widetilde{b}) \le 1/(d_{\mathrm{lo}}(1-\chi))$
[(L1)]

(L10) $1/(\widetilde{a}\widetilde{b}) \le 1/(d_{\mathrm{lo}}(1-\chi))^2$
[$\widetilde{a}, \widetilde{b} \ge d_{\mathrm{lo}}(1-\chi)$ (assumptions A1, A2)]

(L11) $\widetilde{D}^2/(\widetilde{a}\widetilde{b}) = \widetilde{\kappa}$
[$\widetilde{D}$, $\widetilde{\kappa}$ (the statement)]

(L12) $\Rightarrow$ $||M/(\widetilde{a}\widetilde{b}) \le \widetilde{\kappa}((1+c_{\mathrm{sa}})^2-1)(1+u)^4 + \mathcal{Q}$
[(L5), (L7) to (L11); $\mathcal{H}$ (the statement); $\mathcal{Q}$ (the statement)]

(I1)

Lemma G.4	This proof
k	2
(δ_1, δ_2)	(u_{d_0}, u_{d_0})
(c_1, c_2)	(u_0, u_0)
$\delta_1, \delta_2 \in \mathbb{C}$	$u_{d_0} \in \mathbb{R}$ (the statement)
$c_1, c_2 \ge 0$	Assumption A4
Assumption A1	Assumption A4
Its conclusion: $\lvert\prod_{j=1}^k (1+\delta_j) - 1\rvert \le \prod_{j=1}^k (1+c_j) - 1$	

(L13) $|(1+u_{d_0})^2 - 1| \le (1+u_0)^2 - 1$
[(I1)]

(L14) $|(1+u_{d_0})^2 - 1 - \delta_{zo}| \le (1+u_0)^2 - 1 + (1+u)^4 - 1$
[(L13); $|\delta_{zo}| \le (1+u)^4 - 1$ (assumption A7); Fact A.41, item 1: $|x+y| \le |x| + |y|$]

(L15) $\widetilde{\kappa} \ge 0$
[$\widetilde{\kappa}$ (the statement); $\widetilde{a}, \widetilde{b} > 0$ (the statement); Fact A.41, items 13 and 8]

(L16) $|(1+u_{d_0})^2 + \widetilde{\kappa}((1+u_{d_0})^2 - 1 - \delta_{zo}) - \mathcal{M}/(\widetilde{a}\widetilde{b}) - 1| \le |(1+u_{d_0})^2 - 1| + \widetilde{\kappa}|(1+u_{d_0})^2 - 1 - \delta_{zo}| + ||M/(\widetilde{a}\widetilde{b})$
[Fact A.41, item 1: $|x+y| \le |x| + |y|$; (L15)]

(L17) $\Rightarrow$ $|(1+u_{d_0})^2+\widetilde{\kappa}((1+u_{d_0})^2-1-\delta_{zo})-\mathcal{M}/(\widetilde{a}\widetilde{b})-1| \le (1+\widetilde{\kappa})((1+u_0)^2-1)+\widetilde{\kappa}((1+u)^4-1+((1+c_{\mathrm{sa}})^2-1)(1+u)^4)+\mathcal{Q}$

[(L12), (L13), (L14), (L16)]

(L18) $(1+u)^4-1+((1+c_{\mathrm{sa}})^2-1)(1+u)^4 = r'$

[collect; r' (the statement)]

(L19) $\Rightarrow$ $|(1+u_{d_0})^2+\widetilde{\kappa}((1+u_{d_0})^2-1-\delta_{zo})-\mathcal{M}/(\widetilde{a}\widetilde{b})-1| \le (1+\widetilde{\kappa})((1+u_0)^2-1)+\widetilde{\kappa}r'+\mathcal{Q}$

[(L17), (L18)]

(L20) $\Rightarrow$ the statement

[(L19)]

□

Lemma G.32 (The computed diagonals at one node [to table])**.** *At one node, a pair perturbed by relative amounts at most χ bounds the child's computed first diagonal within $(1+\chi)(1+u_0)-1$ of the pair's arithmetic mean and the child's computed second diagonal within c_H of its harmonic mean. Let:*

- $\mathcal{F}$ *be a realization at* (u,ζ) *(Definition A.4);*
- $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$*;*
- $a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$*;*
- $\psi \in \mathbb{C}$*;*
- $\tilde{\psi} \in C_{\mathcal{F}}$*;*
- $\chi \in [0,1)$*;*
- $\omega_a, \omega_b \in \mathbb{R}$.

Define:

- $\tilde{a} := a(1+\omega_a)$*;*
- $\tilde{b} := b(1+\omega_b)$*;*
- $(\tilde{d}_0, \tilde{d}_1)$*, the values* $\mathrm{split}_{\mathrm{sa}}$ *(Algorithm 3) computes in* $\mathcal{F}$ *from* $(f(\psi), f(-\psi)) := (\tilde{a}, \tilde{b})$ *at lines 4, 6, with* $\tilde{s} := \tilde{\psi}$*;*
- $\tilde{d}_{11}$*, the output of* $\mathrm{LDL}^{\dagger}$ *(Algorithm 5) in* $\mathcal{F}$ *at* $(g_{00}, g_{01}, g_{11}) := (\tilde{d}_0, \tilde{d}_1, \tilde{d}_0)$*, line 18;*
- $\tilde{\kappa} := (\tilde{a}-\tilde{b})^2/(4\tilde{a}\tilde{b})$*;*
- $m_1 := d_{\mathrm{lo}}(1-\chi)(1-u)$*;*
- $u_0 := (1+u)\,(1+\zeta/(2m_1)) - 1$*;*
- $c_{\mathrm{sa}} := (1+u)^2(1+u+\sqrt{2}\,\zeta) - 1$*;*
- $k_{\mathrm{sa}} := (1+u)(1+u+\sqrt{2}\,\zeta)/2 + \sqrt{2}$*;*
- $M_1 := d_{\mathrm{hi}}(1+\chi)/2$*;*
- $M_2 := M_1(1+c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta$*;*
- $\bar{k}_{zo} := \sqrt{2}\,M_2^2(1+u)^3 + \sqrt{2}\,M_2(1+u)^2 + 2(1+u) + 1$*;*
- $r' := (1+c_{\mathrm{sa}})^2(1+u)^4 - 1$*;*
- $\mathcal{Q} := \dfrac{2(1+c_{\mathrm{sa}})k_{\mathrm{sa}}\zeta(1+u)^4 + \bar{k}_{zo}\,\zeta\,(1+u_0)}{d_{\mathrm{lo}}(1-\chi)} + \dfrac{(k_{\mathrm{sa}}\zeta)^2(1+u)^4}{(d_{\mathrm{lo}}(1-\chi))^2}$*;*
- $c_H := \left(1+\dfrac{\chi+\chi^2}{1-\chi}\right)(1+(1+\tilde{\kappa})((1+u_0)^2-1)+\tilde{\kappa}r'+\mathcal{Q})\left(1+\dfrac{u+u_0}{1-u_0}\right) - 1 + \dfrac{\zeta}{d_{\mathrm{lo}}}$.

Assume:

(A1) $\tilde{a}, \tilde{b} \in \mathcal{F}$*;*
(A2) $u < 1$*;*
(A3) $|\omega_a| \le \chi$*;*
(A4) $|\omega_b| \le \chi$*;*
(A5) $|\psi| = 1$*;*
(A6) $|\tilde{\psi} - \psi| \le u + \sqrt{2}\,\zeta$*;*
(A7) $u_0 < 1$.

Then the child's two computed diagonals satisfy:

7838 1. $\tilde{d}_0 \mathcal{I}\left(((1+\chi)(1+u_0)-1)^{\pm}, 0\right)$ $\mathrm{AM}(a,b)$;

7839 2. $\tilde{d}_{11} \mathcal{I}\left(c_H^{\pm}, 0\right)$ $\mathrm{HM}(a,b)$.

7840 *Proof.*

DEFINES $\widetilde{A} := (\widetilde{a}+\widetilde{b})/2$

DEFINES $A := (a+b)/2$

DEFINES $w := a/(a+b)$

DEFINES $\mathcal{J}_1 := \dfrac{(1+\omega_a)(1+\omega_b)}{1+w\omega_a+(1-w)\omega_b}$

7841 DEFINES $\mathcal{J}_2 := (1+u_{d_0})^2 + \widetilde{\kappa}((1+u_{d_0})^2 - 1 - \delta_{zo}) - \mathcal{M}/(\widetilde{a}\widetilde{b})$, δ_{zo} that of (L10), u_{d_0} that of (L1)

DEFINES $\widetilde{D} := |\widetilde{a}-\widetilde{b}|/2$

DEFINES $\mathcal{M} := (|\widetilde{d}_1|^2 - \widetilde{D}^2)(1+\delta_{zo}) + E_{zo}\widetilde{d}_0$, δ_{zo}, E_{zo} those of (L10)

DEFINES $\mathcal{H} := 2\widetilde{D}(1+c_{\mathrm{sa}})k_{\mathrm{sa}}\zeta + (k_{\mathrm{sa}}\zeta)^2$

7842 *Proof of item 1.*

Lemma G.28	This proof
Shared: $\mathcal{F}$, d_{lo}, a,b, $\widetilde{\psi}$, χ, ω_a,ω_b, $\widetilde{a},\widetilde{b},\widetilde{d}_0$, $\widetilde{A}$, m_1,u_0	
Shared: $d_{\mathrm{lo}}>0$, $\widetilde{\psi}\in C_{\mathcal{F}}$, $\chi\in[0,1)$, $\omega_a,\omega_b\in\mathbb{R}$	
7843 (I1) Shared: assumptions A1, A2, A3, A4	
$\mathcal{F}$ realization at (u,ζ)	The statement
$a,b\in[d_{\mathrm{lo}},\infty)$	$a,b\in[d_{\mathrm{lo}},d_{\mathrm{hi}}]$ (the statement)
Its conclusion: $\exists\, u_{d_0}\in\mathbb{R},\ \lvert u_{d_0}\rvert\le u_0:\ \widetilde{d}_0=\widetilde{A}(1+u_{d_0})$	

7844 (L1) $\exists\, u_{d_0}\in\mathbb{R},\ |u_{d_0}|\le u_0:\ \widetilde{d}_0=\widetilde{A}(1+u_{d_0})$

7845 [(I1)]

7846 (L2) $w\in(0,1)$

7847 [w (the proof's block); $a,b>0$ (the statement)]

7848 (L3) $\widetilde{A}/A = 1+w\omega_a+(1-w)\omega_b$

7849 [$\widetilde{A}$, A, w (the proof's block)]

7850 (L4) $1+w\omega_a+(1-w)\omega_b\in[1-\chi,1+\chi]$

7851 [(L2); assumptions A3, A4]

7852 (L5) $\Rightarrow\ \widetilde{d}_0 = \mathrm{AM}(a,b)(1+e_A),\quad e_A := (1+w\omega_a+(1-w)\omega_b)(1+u_{d_0})-1$

7853 [(L1), (L3); $A=\mathrm{AM}(a,b)$ (Definition A.46)]

Lemma G.4	This proof
k	2
δ_1	$w\omega_a+(1-w)\omega_b$ (L4)
δ_2	u_{d_0} (L1)
c_1,c_2	χ,u_0 (the statement)
7854 (I2) $k\in\mathbb{Z}_{\ge0}$	$2\in\mathbb{Z}_{\ge0}$
$\delta_1,\delta_2\in\mathbb{C}$	(L4), (L1)
$c_1,c_2\ge0$	$\chi\in[0,1)$ (the statement); u_0, m_1 (the statement); $u,\zeta\ge0$ (Definition A.4); $u<1$ (assumption A2)
Assumption A1	(L4), (L1)
Its conclusion: $\lvert\prod_{j=1}^k(1+\delta_j)-1\rvert\le\prod_{j=1}^k(1+c_j)-1$	

7855 (L6) $|(1+w\omega_a+(1-w)\omega_b)(1+u_{d_0})-1|\le(1+\chi)(1+u_0)-1$

7856 [(I2)]

7857 (L7) $\Rightarrow\ |e_A|\le(1+\chi)(1+u_0)-1$

7858 [(L6); e_A (L5)]

(L8) $\Rightarrow$ $\tilde{d}_0\, \mathcal{I}\left(((1+\chi)(1+u_0)-1)^{\pm}, 0\right)\ \mathrm{AM}(a,b)$

[(L5), (L7); Definition A.10; Definition A.9]

(L9) $\Rightarrow$ item 1

[(L8)]

□ (item 1)

Proof of item 2.

Lemma G.30 at the u_{d_0} of (L1)	This proof
Shared: $\mathcal{F},\ d_{\mathrm{lo}}, d_{\mathrm{hi}},\ a, b,\ \psi, \widetilde{\psi},\ \chi,\ \omega_a, \omega_b,\ u_{d_0}$(L1), $\widetilde{a}, \widetilde{b}, \widetilde{d}_0, \widetilde{d}_1,\ \widetilde{\kappa}, \bar{k}_{zo},\ \mathcal{M}$	
Shared: $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0,\ a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}],\ \psi \in \mathbb{C},\ \widetilde{\psi} \in C_{\mathcal{F}},\ \chi \in [0,1),\ \omega_a, \omega_b \in \mathbb{R}$	
Shared: assumptions A1, A2, A3, A4, A5, A7	
$\widetilde{zo}$	$\widetilde{zo}$ (LDL† (Algorithm 5), line 14)
$\widetilde{A}, u_0$	$\widetilde{A}, u_0$ (the proof's block; the statement)
$\widetilde{D}, M_2$	$\widetilde{D}, M_2$ (the proof's block; the statement)
(I3) $\mathcal{F}$ realization at (u, ζ)	The statement
$u_{d_0} \in \mathbb{R}$	(L1)
Assumption A6	Assumption A6
Assumption A8	(L1)
Assumption A9	(L1)
Its item 1: $\exists\, \delta_{zo}, E_{zo} \in \mathbb{R},\ \lvert\delta_{zo}\rvert \le (1+u)^4 - 1,\ \lvert E_{zo}\rvert \le \bar{k}_{zo}\zeta :\ \widetilde{zo}\, \widetilde{d}_0 = \lvert\widetilde{d}_1\rvert^2(1+\delta_{zo}) + E_{zo}\widetilde{d}_0$	
Its item 2: $(\widetilde{d}_0 - \widetilde{zo})\, \widetilde{d}_0 = \widetilde{a}\widetilde{b}\left((1+u_{d_0})^2 + \widetilde{\kappa}\left((1+u_{d_0})^2 - 1 - \delta_{zo}\right) - \mathcal{M}/(\widetilde{a}\widetilde{b})\right)$	

(L10) $\exists\, \delta_{zo}, E_{zo} \in \mathbb{R},\ \lvert\delta_{zo}\rvert \le (1+u)^4 - 1,\ \lvert E_{zo}\rvert \le \bar{k}_{zo}\zeta :\ \widetilde{zo}\, \widetilde{d}_0 = \lvert\widetilde{d}_1\rvert^2(1+\delta_{zo}) + E_{zo}\widetilde{d}_0$

[item 1 of (I3)]

(L11) $(\widetilde{d}_0 - \widetilde{zo})\, \widetilde{d}_0 = \widetilde{a}\widetilde{b}\left((1+u_{d_0})^2 + \widetilde{\kappa}\left((1+u_{d_0})^2 - 1 - \delta_{zo}\right) - \mathcal{M}/(\widetilde{a}\widetilde{b})\right)$

[item 2 of (I3)]

(L12) $\exists\, \delta_{zo}, E_{zo} \in \mathbb{R},\ \lvert\delta_{zo}\rvert \le (1+u)^4 - 1,\ \lvert E_{zo}\rvert \le \bar{k}_{zo}\zeta :\ (\widetilde{d}_0 - \widetilde{zo})\, \widetilde{d}_0 = \widetilde{a}\widetilde{b}\, \mathcal{J}_2$

[(L10), (L11); $\mathcal{J}_2$, $\mathcal{M}$ (the proof's block)]

(L13) $\widetilde{a} \ge d_{\mathrm{lo}}(1-\chi)$

[$a \ge d_{\mathrm{lo}}$ (the statement); $\lvert\omega_a\rvert \le \chi$ (assumption A3)]

(L14) $\widetilde{b} \ge d_{\mathrm{lo}}(1-\chi)$

[$b \ge d_{\mathrm{lo}}$ (the statement); $\lvert\omega_b\rvert \le \chi$ (assumption A4)]

Lemma G.29, item 1	This proof
Shared: $\mathcal{F},\ d_{\mathrm{lo}}, d_{\mathrm{hi}},\ a, b,\ \psi, \widetilde{\psi},\ \chi,\ \omega_a, \omega_b,\ \widetilde{a}, \widetilde{b}, \widetilde{d}_1,\ \widetilde{D}, \mathcal{H},\ c_{\mathrm{sa}}, k_{\mathrm{sa}}, M_1, M_2$	
Shared: $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0,\ a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}],\ \psi \in \mathbb{C},\ \widetilde{\psi} \in C_{\mathcal{F}},\ \chi \in [0,1),\ \omega_a, \omega_b \in \mathbb{R}$	
$\mathcal{F}$ realization at (u, ζ)	The statement
(I4) Assumption A1	Assumption A1
Assumption A2	Assumption A3
Assumption A3	Assumption A4
Assumption A4	Assumption A5
Assumption A5	Assumption A6
Its conclusion: $\left\lvert\lvert\widetilde{d}_1\rvert^2 - \widetilde{D}^2\right\rvert \le \widetilde{D}^2((1+c_{\mathrm{sa}})^2 - 1) + \mathcal{H}$	

(L15) $\left\lvert\lvert\widetilde{d}_1\rvert^2 - \widetilde{D}^2\right\rvert \le \widetilde{D}^2((1+c_{\mathrm{sa}})^2 - 1) + \mathcal{H}$

[(I4)]

	Lemma G.31 at the u_{d_0} of (L1) and the δ_{zo}, E_{zo} of (L10)	This proof
	Shared: $d_{\mathrm{lo}}, d_{\mathrm{hi}},\ u, \zeta,\ \chi,\ \widetilde{a}, \widetilde{b}, \widetilde{d}_0, \widetilde{d}_1,\ \widetilde{\kappa}, \bar{k}_{zo}, r', \mathcal{Q},\ \mathcal{M}$	
	Shared: $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0,\ \chi \in [0, 1)$	
	$u_{d_0}, \delta_{zo}, E_{zo}$	$u_{d_0}, \delta_{zo}, E_{zo}$ (L1), (L10)
	$\widetilde{A}, u_0$	$\widetilde{A}, u_0$ (the proof's block; the statement)
	$\widetilde{D}, c_{\mathrm{sa}}, k_{\mathrm{sa}}, M_2, \mathcal{H}$	$\widetilde{D}, c_{\mathrm{sa}}, k_{\mathrm{sa}}, M_2, \mathcal{H}$ (the proof's block; the statement)
	$u, \zeta \geq 0$	Definition A.4
	$\widetilde{a}, \widetilde{b} > 0$	(L13), (L14); $d_{\mathrm{lo}} > 0$, $\chi < 1$ (the statement)
	$\widetilde{d}_0 \in \mathbb{R}$	$\widetilde{d}_0$ (the statement)
(I5)	$\widetilde{d}_1 \in \mathbb{C}$	$\widetilde{d}_1$ (the statement)
	$u_{d_0}, \delta_{zo}, E_{zo} \in \mathbb{R}$	(L1), (L10)
	Assumption A1	(L13)
	Assumption A2	(L14)
	Assumption A3	Assumption A7
	Assumption A4	(L1)
	Assumption A5	(L1)
	Assumption A6	(L15)
	Assumption A7	(L10)
	Assumption A8	(L10)

Its conclusion:
$|(1+u_{d_0})^2 + \widetilde{\kappa}\left((1+u_{d_0})^2 - 1 - \delta_{zo}\right) - \mathcal{M}/(\widetilde{a}\widetilde{b}) - 1| \leq (1+\widetilde{\kappa})((1+u_0)^2 - 1) + \widetilde{\kappa} r' + \mathcal{Q}$

(L16) $|(1+u_{d_0})^2 + \widetilde{\kappa}\left((1+u_{d_0})^2 - 1 - \delta_{zo}\right) - \mathcal{M}/(\widetilde{a}\widetilde{b}) - 1| \leq (1+\widetilde{\kappa})((1+u_0)^2 - 1) + \widetilde{\kappa} r' + \mathcal{Q}$
[(I5)]

(L17) $|\mathcal{J}_2 - 1| \leq (1+\widetilde{\kappa})((1+u_0)^2 - 1) + \widetilde{\kappa} r' + \mathcal{Q}$
[(L16); $\mathcal{J}_2$ (the proof's block)]

(L18) $\exists\, u_{d_{11}}, \zeta_{d_{11}} \in \mathbb{R},\ |u_{d_{11}}| \leq u,\ |\zeta_{d_{11}}| \leq \zeta :\ \widetilde{d}_{11} = (\widetilde{d}_0 - \widetilde{zo})(1+u_{d_{11}}) + \zeta_{d_{11}}$
[Definition A.4, item 1, for $-$ (LDL† (Algorithm 5), line 18)]

(L19) $|u_{d_{11}} - u_{d_0}| \leq u + u_0$
[(L1), (L18); Fact A.41, item 1: $|x-y| \leq |x| + |y|$]

(L20) $|1 + u_{d_0}| \geq 1 - u_0$
[(L1); Fact A.41, item 1: $||x| - |y|| \leq |x-y|$]

(L21) $1 - u_0 > 0$
[$u_0 < 1$ (assumption A7)]

(L22) $\frac{1+u_{d_{11}}}{1+u_{d_0}} - 1 = \frac{u_{d_{11}} - u_{d_0}}{1+u_{d_0}}$
[$1 + u_{d_0} \neq 0$ ((L20), (L21)); expand]

(L23) $|\frac{1+u_{d_{11}}}{1+u_{d_0}} - 1| = \frac{|u_{d_{11}} - u_{d_0}|}{|1+u_{d_0}|}$
[(L22); Fact A.41, item 1: $|xy| = |x||y|$]

(L24) $\frac{|u_{d_{11}} - u_{d_0}|}{|1+u_{d_0}|} \leq \frac{u+u_0}{1-u_0}$
[(L19), (L20), (L21)]

(L25) $\Rightarrow\ |\frac{1+u_{d_{11}}}{1+u_{d_0}} - 1| \leq \frac{u+u_0}{1-u_0}$
[(L23), (L24)]

	Lemma G.27	This proof
	Shared: $a, b,\ \chi,\ \omega_a, \omega_b,\ \widetilde{a}, \widetilde{b},\ \widetilde{A}, w, \mathcal{J}_1,\ \mathrm{HM}(a,b)$ (Definition A.46) Shared: $\chi \in [0,1),\ \omega_a, \omega_b \in \mathbb{R}$	
	$a, b > 0$	$a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}],\ d_{\mathrm{lo}} > 0$ (the statement)
(I6)	Assumption A1 Assumption A2	Assumption A3 Assumption A4
	Its item 1: $\dfrac{\widetilde{a}\widetilde{b}/\widetilde{A}}{\mathrm{HM}(a,b)} = \mathcal{J}_1$	
	Its item 2: $\mathcal{J}_1 \in \left[1-\chi,\ 1+\dfrac{\chi+\chi^2}{1-\chi}\right]$	

(L26) $\dfrac{\widetilde{a}\widetilde{b}/\widetilde{A}}{\mathrm{HM}(a,b)} = \mathcal{J}_1$

[item 1 of (I6)]

(L27) $\mathcal{J}_1 \in \left[1-\chi,\ 1+\dfrac{\chi+\chi^2}{1-\chi}\right]$

[item 2 of (I6)]

(L28) $\widetilde{a}\widetilde{b}/\widetilde{A} = \mathrm{HM}(a,b)\,\mathcal{J}_1$

[(L26); multiply by $\mathrm{HM}(a,b)$]

(L29) $\Rightarrow\ \widetilde{d}_{11} = \mathrm{HM}(a,b)\,\mathcal{J}_1\mathcal{J}_2\frac{1+u_{d_{11}}}{1+u_{d_0}} + \zeta_{d_{11}}$

[(L1), (L12), (L18), (L28)]

(L30) $\chi \le (\chi+\chi^2)/(1-\chi)$

[$\chi \in [0,1)$ (the statement)]

(L31) $|\mathcal{J}_1 - 1| \le \frac{\chi+\chi^2}{1-\chi}$

[(L27), (L30)]

(L32) $\mathrm{HM}(a,b) \ge d_{\mathrm{lo}}$

[$a, b \ge d_{\mathrm{lo}}$ (the statement); Fact A.41, item 9]

(L33) $|\zeta_{d_{11}}|/\mathrm{HM}(a,b) \le \zeta/d_{\mathrm{lo}}$

[(L18), (L32)]

(L34) $\Rightarrow\ \widetilde{d}_{11} = \mathrm{HM}(a,b)(1+e_H), \quad e_H := \mathcal{J}_1\mathcal{J}_2\frac{1+u_{d_{11}}}{1+u_{d_0}} - 1 + \zeta_{d_{11}}/\mathrm{HM}(a,b)$

[(L29), (L32)]

	Lemma G.4	This proof
	k	3
	δ_1	$\mathcal{J}_1 - 1$ (L31)
	δ_2	$\mathcal{J}_2 - 1$ (L17)
	δ_3	$\frac{1+u_{d_{11}}}{1+u_{d_0}} - 1$ (L25)
(I7)	c_1, c_2, c_3	$\frac{\chi+\chi^2}{1-\chi}, (1+\widetilde{\kappa})((1+u_0)^2-1)+\widetilde{\kappa}r'+\mathcal{Q}, \frac{u+u_0}{1-u_0}$ (the statement)
	$k \in \mathbb{Z}_{\ge 0}$	$3 \in \mathbb{Z}_{\ge 0}$
	$\delta_1, \delta_2, \delta_3 \in \mathbb{C}$	(L31), (L17), (L25)
	$c_1, c_2, c_3 \ge 0$	$\chi \in [0,1)$ (the statement); $\widetilde{\kappa}$, u_0, r', $\mathcal{Q}$ (the statement); $u_0 < 1$ (assumption A7)
	Assumption A1	(L31), (L17), (L25)
	Its conclusion: $\lvert\prod_{j=1}^k(1+\delta_j)-1\rvert \le \prod_{j=1}^k(1+c_j)-1$	

(L35) $|\mathcal{J}_1\mathcal{J}_2\frac{1+u_{d_{11}}}{1+u_{d_0}} - 1| \le \left(1+\frac{\chi+\chi^2}{1-\chi}\right)\left(1+(1+\widetilde{\kappa})((1+u_0)^2-1)+\widetilde{\kappa}r'+\mathcal{Q}\right)\left(1+\frac{u+u_0}{1-u_0}\right) - 1$

[(I7)]

(L36) $\Rightarrow\ |e_H| \le c_H$

[(L34), (L35), (L33); Fact A.41, item 1: $|x+y| \le |x|+|y|$; c_H (the statement)]

(L37) $\Rightarrow\ \tilde{d}_{11}\ \mathcal{I}\left(c_H^{\pm}, 0\right)\mathrm{HM}(a,b)$

[(L34), (L36); Definition A.10; Definition A.9]

(L38) $\Rightarrow$ item 2

[(L37)]

□ (item 2)

Lemma G.33 (Monotonicity of the bound map [to table])**.** *The bound of Lemma G.32 on the second diagonal grows with the pair's relative bound χ and with κ. Let:*

- $u \in [0, 1)$*;*
- $\zeta \geq 0$*;*
- $d_{\text{lo}}, d_{\text{hi}} > 0$*;*
- $\chi, \chi', \kappa, \kappa' \in \mathbb{R}$*.*

Define:

- $c_{\text{sa}} := (1+u)^2(1+u+\sqrt{2}\,\zeta) - 1$*;*
- $k_{\text{sa}} := (1+u)(1+u+\sqrt{2}\,\zeta)/2 + \sqrt{2}$*;*
- $r' := (1+c_{\text{sa}})^2(1+u)^4 - 1$*;*
- $\forall \chi \in [0,1):\ u_0(\chi) := (1+u)\left(1 + \dfrac{\zeta}{2d_{\text{lo}}(1-\chi)(1-u)}\right) - 1$*;*
- $\forall \chi \in [0,1):\ M_2(\chi) := d_{\text{hi}}(1+\chi)(1+c_{\text{sa}})/2 + k_{\text{sa}}\zeta$*;*
- $\forall \chi \in [0,1):\ \bar{k}_{zo}(\chi) := \sqrt{2}\,M_2(\chi)^2(1+u)^3 + \sqrt{2}\,M_2(\chi)(1+u)^2 + 2(1+u) + 1$*;*
- $\forall \chi \in [0,1):\ \mathcal{Q}(\chi) := \dfrac{2(1+c_{\text{sa}})k_{\text{sa}}\zeta(1+u)^4 + \bar{k}_{zo}(\chi)\,\zeta\,(1+u_0(\chi))}{d_{\text{lo}}(1-\chi)} + \dfrac{(k_{\text{sa}}\zeta)^2(1+u)^4}{(d_{\text{lo}}(1-\chi))^2}$*;*
- $\forall \chi \in [0,1)\ \forall \kappa \in \mathbb{R}:\ \mathcal{U}^{\zeta}_{\kappa}(\chi) := \left(1 + \dfrac{\chi+\chi^2}{1-\chi}\right)$ *;*

  $\cdot \left(1 + (1+\kappa)((1+u_0(\chi))^2 - 1) + \kappa r' + \mathcal{Q}(\chi)\right)\left(1 + \dfrac{u+u_0(\chi)}{1-u_0(\chi)}\right) - 1 + \dfrac{\zeta}{d_{\text{lo}}}$
- $\mathcal{A} := \{\chi \in [0,1) : u_0(\chi) < 1\}$*.*

Assume:

(A1) $\chi' \in \mathcal{A}$*;*
(A2) $\chi \geq 0$*;*
(A3) $\chi \leq \chi'$*;*
(A4) $\kappa \geq 0$*;*
(A5) $\kappa \leq \kappa'$*.*

Then

$$\mathcal{U}^{\zeta}_{\kappa}(\chi) \leq \mathcal{U}^{\zeta}_{\kappa'}(\chi').$$

Proof.

DEFINES $\phi_1(\chi) := 1 + \frac{\chi+\chi^2}{1-\chi}$
DEFINES $\phi_2(\chi,\kappa) := 1 + (1+\kappa)((1+u_0(\chi))^2 - 1) + \kappa r' + \mathcal{Q}(\chi)$
DEFINES $\phi_3(\chi) := 1 + \frac{u+u_0(\chi)}{1-u_0(\chi)}$

(L1) $\mathcal{U}^{\zeta}_{\kappa}(\chi) = \phi_1(\chi)\phi_2(\chi,\kappa)\phi_3(\chi) - 1 + \zeta/d_{\text{lo}}$

[$\mathcal{U}^{\zeta}_{\kappa}$ (the statement); ϕ_1, ϕ_2, ϕ_3 (the proof's block)]

(L2) $1 - \chi' > 0$

[$\chi' \in \mathcal{A}$ (assumption A1)]

(L3) $1 - \chi' \leq 1 - \chi$

[$\chi \leq \chi'$ (assumption A3)]

(L4) $c_{\text{sa}} \geq 0$

[c_{sa} (the statement); $u, \zeta \geq 0$ (the statement)]

(L5) $k_{\text{sa}} \geq 0$

[k_{sa} (the statement); $u, \zeta \geq 0$ (the statement)]

(L6) $r' \geq 0$

[r' (the statement); (L4)]

(L7) $u_0(\chi) \geq 0$

[u_0 (the statement); (L2), (L3); $u, \zeta \geq 0$, $d_{\text{lo}} > 0$ (the statement)]

(L8) $u_0(\chi) \leq u_0(\chi')$

[u_0 (the statement); (L2), (L3); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5); $u, \zeta \geq 0$, $d_{\text{lo}} > 0$ (the statement)]

(L9) $M_2(\chi) \geq 0$

[M_2 (the statement); $\chi \geq 0$ (assumption A2); (L4), (L5); $d_{\text{hi}}, \zeta \geq 0$ (the statement)]

(L10) $M_2(\chi) \leq M_2(\chi')$

[M_2 (the statement); $\chi \leq \chi'$ (assumption A3); (L4); $d_{\text{hi}} > 0$ (the statement)]

(L11) $\bar{k}_{zo}(\chi) \leq \bar{k}_{zo}(\chi')$

[$\bar{k}_{zo}$ (the statement); (L9), (L10); $t \mapsto t^2$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L12) $\mathcal{Q}(\chi) \geq 0$

[$\mathcal{Q}$ (the statement); (L2), (L3), (L4), (L5), (L7), (L9); $d_{\text{lo}} > 0$ (the statement)]

(L13) $\mathcal{Q}(\chi) \leq \mathcal{Q}(\chi')$

[$\mathcal{Q}$ (the statement); (L2) to (L8), (L11); $d_{\text{lo}} > 0$ (the statement); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5); Fact A.41, item 8]

(L14) $\chi + \chi^2 \geq 0$

[$\chi \geq 0$ (assumption A2)]

(L15) $\chi + \chi^2 \leq \chi' + \chi'^2$

[$0 \leq \chi$, $\chi \leq \chi'$ (assumptions A2, A3); Fact A.41, item 5]

(L16) $\phi_1(\chi) \geq 0$

[ϕ_1 (the proof's block); (L2), (L3), (L14)]

(L17) $\phi_1(\chi) \leq \phi_1(\chi')$

[ϕ_1 (the proof's block); (L2), (L3), (L15); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5); Fact A.41, item 8]

(L18) $(1 + u_0(\chi))^2 - 1 \geq 0$

[(L7); Fact A.41, item 5]

(L19) $(1 + u_0(\chi))^2 - 1 \leq (1 + u_0(\chi'))^2 - 1$

[(L7), (L8); Fact A.41, item 5]

(L20) $\phi_2(\chi, \kappa) \geq 0$

[ϕ_2 (the proof's block); (L6), (L12), (L18); $\kappa \geq 0$ (assumption A4)]

(L21) $\phi_2(\chi, \kappa) \leq \phi_2(\chi', \kappa')$

[ϕ_2 (the proof's block); (L6), (L13), (L18), (L19); $\kappa \geq 0$, $\kappa \leq \kappa'$ (assumptions A4, A5); Fact A.41, item 8]

(L22) $\forall x \in [0, 1) : \ \frac{u+x}{1-x} = \frac{1+u}{1-x} - 1$

[expand]

(L23) $\phi_3(\chi) \geq 0$

[ϕ_3 (the proof's block); (L7), (L8); $u_0(\chi') < 1$ (assumption A1; $\mathcal{A}$, the statement)]

(L24) $\phi_3(\chi) \leq \phi_3(\chi')$

[ϕ_3 (the proof's block); (L7), (L8), (L22); $u_0(\chi') < 1$ (assumption A1; $\mathcal{A}$, the statement); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L25) $\Rightarrow \ \mathcal{U}^{\zeta}_{\kappa}(\chi) \leq \mathcal{U}^{\zeta}_{\kappa'}(\chi')$

[(L1), (L16), (L17), (L20), (L21), (L23), (L24); Fact A.41, item 8, twice]

(L26) $\Rightarrow$ the statement

[(L25)]

□

Lemma G.34 (The first diagonal's bound under the bound map [to table])**.** *The bound of Lemma G.32 on the first diagonal is below the bound map at every $\kappa \geq 0$. Let:*

- $u \in [0, 1)$;
- $\zeta \geq 0$;
- $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$;
- $\chi, \kappa \in \mathbb{R}$.

Define:

- $u_0(\chi) := (1 + u)(1 + \zeta/(2d_{\mathrm{lo}}(1 - \chi)(1 - u))) - 1$ *(Lemma G.33);*
- $\mathcal{A} := \{\chi \in [0, 1) : u_0(\chi) < 1\}$ *(Lemma G.33);*
- $c_{\mathrm{sa}} := (1 + u)^2(1 + u + \sqrt{2}\,\zeta) - 1$ *(Lemma G.33);*
- $k_{\mathrm{sa}} := (1 + u)(1 + u + \sqrt{2}\,\zeta)/2 + \sqrt{2}$ *(Lemma G.33);*
- $M_2(\chi) := d_{\mathrm{hi}}(1 + \chi)(1 + c_{\mathrm{sa}})/2 + k_{\mathrm{sa}}\zeta$ *(Lemma G.33);*
- $r' := (1 + c_{\mathrm{sa}})^2(1 + u)^4 - 1$ *(Lemma G.33);*
- $\bar{k}_{zo}(\chi) := \sqrt{2}\,M_2(\chi)^2(1 + u)^3 + \sqrt{2}\,M_2(\chi)(1 + u)^2 + 2(1 + u) + 1$ *(Lemma G.33);*
- $\mathcal{U}^{\zeta}_{\kappa}(\chi)$ *and* $\mathcal{Q}(\chi)$*, those of Lemma G.33 at* $(u, \zeta, d_{\mathrm{lo}}, d_{\mathrm{hi}})$.

Assume:

(A1) $\chi \in \mathcal{A}$;

(A2) $\kappa \geq 0$.

Then

$$(1 + \chi)(1 + u_0(\chi)) - 1 \leq \mathcal{U}^{\zeta}_{\kappa}(\chi).$$

Proof. (L1) $d_{\mathrm{lo}}(1 - \chi) > 0$
[$d_{\mathrm{lo}} > 0$ (the statement); $\chi < 1$ (assumption A1; $\mathcal{A}$, the statement)]

(L2) $d_{\mathrm{lo}}(1 - \chi)(1 - u) > 0$
[(L1); $u < 1$ (the statement)]

(L3) $c_{\mathrm{sa}} \geq 0$
[c_{sa} (the statement); $u, \zeta \geq 0$ (the statement)]

(L4) $k_{\mathrm{sa}} \geq 0$
[k_{sa} (the statement); $u, \zeta \geq 0$ (the statement)]

(L5) $\bar{k}_{zo}(\chi) \geq 0$
[$\bar{k}_{zo}$ (the statement); $u \geq 0$ (the statement)]

(L6) $\frac{\chi + \chi^2}{1 - \chi} - \chi = \frac{2\chi^2}{1 - \chi}$
[expand]

(L7) $1 + \chi \leq 1 + \frac{\chi + \chi^2}{1 - \chi}$
[(L6); $\chi \in [0, 1)$ (assumption A1; $\mathcal{A}$, the statement)]

(L8) $u_0(\chi) \geq u$
[u_0 (the statement); $\zeta \geq 0$ (the statement); (L2)]

(L9) $u \geq 0$
[$u \in [0, 1)$ (the statement)]

(L10) $(1 + u_0(\chi))^2 - 1 - u_0(\chi) = u_0(\chi) + u_0(\chi)^2$
[expand]

(L11) $\Rightarrow$ $(1 + u_0(\chi))^2 - 1 \geq u_0(\chi)$
[(L8), (L9), (L10)]

(L12) $r' \geq 0$
[r' (the statement); (L3)]

(L13) $\mathcal{Q}(\chi) \geq 0$
[$\mathcal{Q}$ (the statement); (L1), (L3), (L4), (L5); $\zeta \geq 0$ (the statement)]

(L14) $1 + u_0(\chi) \leq 1 + (1 + \kappa)((1 + u_0(\chi))^2 - 1) + \kappa r' + \mathcal{Q}(\chi)$
[(L11), (L12), (L13); $\kappa \geq 0$ (assumption A2)]

(L15) $1 \leq 1 + \frac{u + u_0(\chi)}{1 - u_0(\chi)}$
[$u_0(\chi) < 1$ (assumption A1; $\mathcal{A}$, the statement); (L8), (L9)]

(L16) $\Rightarrow$ $(1 + \chi)(1 + u_0(\chi)) - 1 \leq \mathcal{U}^{\zeta}_{\kappa}(\chi)$
[(L7), (L14), (L15), each side nonnegative by $\chi \in [0, 1)$ (assumption A1) and $\kappa \geq 0$ (assumption A2);

Fact A.41, item 8, twice; $\zeta/d_{\text{lo}} \geq 0$ (the statement); $\mathcal{U}_\kappa^\zeta$ (the statement)]

(L17) $\Rightarrow$ the statement

[(L16)]

□

Lemma G.35 (The computed pair's $\widetilde{\kappa}$ [to table])**.** *Perturbing a positive pair by relative amounts at most χ scales κ at the pair's child by at most ϑ, plus $(\vartheta-1)/2$. Let:*

- $a, b > 0$;
- $\chi \in [0, 1)$;
- $\omega_a, \omega_b \in \mathbb{R}$.

Define:

- $\widetilde{a} := a(1+\omega_a)$;
- $\widetilde{b} := b(1+\omega_b)$;
- $\kappa := (a-b)^2/(4ab)$;
- $\widetilde{\kappa} := (\widetilde{a}-\widetilde{b})^2/(4\widetilde{a}\widetilde{b})$;
- $\vartheta := (1+\chi)/(1-\chi)$.

Assume:

(A1) $|\omega_a| \leq \chi$;

(A2) $|\omega_b| \leq \chi$.

Then

$$\widetilde{\kappa} \leq \vartheta\kappa + (\vartheta-1)/2.$$

Proof. (L1) $\forall x, y > 0 : \frac{(x-y)^2}{4xy} = \frac{x/y+y/x-2}{4}$

[expand]

(L2) $\widetilde{a}/\widetilde{b} = (a/b)(1+\omega_a)/(1+\omega_b)$

[$\widetilde{a}$, $\widetilde{b}$ (the statement)]

(L3) $1+\omega_a \leq 1+\chi$

[$|\omega_a| \leq \chi$ (assumption A1)]

(L4) $1+\omega_b \geq 1-\chi$

[$|\omega_b| \leq \chi$ (assumption A2)]

(L5) $1-\chi > 0$

[$\chi < 1$ (the statement)]

(L6) $(1+\omega_a)/(1+\omega_b) \leq \vartheta$

[(L3), (L4), (L5); ϑ (the statement)]

(L7) $\Rightarrow$ $\widetilde{a}/\widetilde{b} \leq \vartheta\, a/b$

[(L2), (L6); $a/b > 0$ (the statement)]

(L8) $1+\omega_b \leq 1+\chi$

[$|\omega_b| \leq \chi$ (assumption A2)]

(L9) $1+\omega_a \geq 1-\chi$

[$|\omega_a| \leq \chi$ (assumption A1)]

(L10) $(1+\omega_b)/(1+\omega_a) \leq \vartheta$

[(L8), (L9), (L5); ϑ (the statement)]

(L11) $\widetilde{b}/\widetilde{a} = (b/a)(1+\omega_b)/(1+\omega_a)$

[$\widetilde{a}$, $\widetilde{b}$ (the statement)]

(L12) $\Rightarrow$ $\widetilde{b}/\widetilde{a} \leq \vartheta\, b/a$

[(L11), (L10); $b/a > 0$ (the statement)]

(L13) $\Rightarrow$ $\widetilde{\kappa} \leq \frac{\vartheta(a/b+b/a)-2}{4}$

[(L1) at $(\widetilde{a}, \widetilde{b})$; (L7), (L12); $\widetilde{\kappa}$ (the statement)]

(L14) $\frac{\vartheta(a/b+b/a)-2}{4} = \vartheta\kappa + (\vartheta-1)/2$

[(L1) at (a, b); κ (the statement)]

(L15) $\Rightarrow$ $\widetilde{\kappa} \le \vartheta\kappa + (\vartheta - 1)/2$

[(L13), (L14)]

(L16) $\Rightarrow$ the statement

[(L15)]

□

Corollary G.36 (The computed diagonals at every depth [to table])**.** *Down the tree, each depth's computed diagonals are within the bound map's iterate of the ones over* $\mathbb{R}$*, starting from the root node's bound. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $h \ge 1$*;*
- $\mathcal{G} \in \mathrm{Gram}_n$ *(Definition A.14) at* $n := 2^h$*;*
- $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$*;*
- $\forall k \in \{1, \dots, h-1\} : \ \kappa_k \in \mathbb{R}$*;*
- $\chi_0 \in [0, 1)$.

Define:

- *The tree*
  - $T :=$ ffLDL$^\dagger(\mathcal{G})$ *(Definition A.20);*
  - $\forall \nu \in \mathrm{Sub}(T) : \ \mathcal{G}_\nu$*, that of Definition A.32;*
  - $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi : \ (g_{00}, g_{01}, g_{11})$*, the entries of* $\mathcal{G}_\nu(\psi)$ *(Definition A.14);*
  - $\kappa_\nu(\psi) := |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$*;*
- *The diagonals*
  - $d^\nu_{00}(\psi) := g_{00}$*;*
  - $d^\nu_{11}(\psi) := g_{11} - |g_{01}|^2/g_{00}$ *(*LDL† *(Algorithm 5), lines 15, 19);*
  - $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}$*:* $\widetilde{d}^\nu_j$*, the diagonal* ffLDL† *computes in* $\mathcal{F}$ *at* ν *in place of* d^ν_j*;*
- *The node bounds*
  - $u_0(\chi) := (1+u)(1 + \zeta/(2d_{\mathrm{lo}}(1-\chi)(1-u))) - 1$ *(Lemma G.32);*
  - $\mathcal{U}^\zeta_\kappa(\chi)$*, that of Lemma G.33 at* $(u, \zeta, d_{\mathrm{lo}}, d_{\mathrm{hi}})$*, the bound* c_H *of Lemma G.32 at* $\widetilde{\kappa} := \kappa$ *and* χ*;*
  - $\mathcal{A} := \{\chi \in [0, 1) : u_0(\chi) < 1\}$ *(Lemma G.32);*
- *The error chain*
  - $\chi^\zeta_0 := \chi_0$*;*
  - $\forall k \in \{1, \dots, h-1\} : \ \vartheta_{k-1} := (1 + \chi^\zeta_{k-1})/(1 - \chi^\zeta_{k-1})$*;*
  - $\forall k \in \{1, \dots, h-1\} : \ \hat{\kappa}_k := \vartheta_{k-1}\kappa_k + (\vartheta_{k-1} - 1)/2$*;*
  - $\forall k \in \{1, \dots, h-1\} : \ \chi^\zeta_k := \mathcal{U}^\zeta_{\hat{\kappa}_k}(\chi^\zeta_{k-1})$*, by induction on* k*;*
  - $\chi_{\mathrm{leaf}} := \max_{\nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1} \ \max_{j \in \{00,11\}} \ \max_\psi |\widetilde{d}^\nu_j(\psi)/d^\nu_j(\psi) - 1|$.

Assume:

(A1) $u < 1$*;*
(A2) $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi : \ d^\nu_j(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$*;*
(A3) $\forall k \in \{1, \dots, h-1\}\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = k\ \forall \psi : \ \kappa_\nu(\psi) \le \kappa_k$*;*
(A4) $\forall j \in \{00, 11\}\ \forall \psi : \ \widetilde{d}^T_j(\psi)\ \mathcal{I}\left(\chi^\pm_0, 0\right) d^T_j(\psi)$*;*
(A5) $\forall \psi : \ |\widetilde{\psi} - \psi| \le u + \sqrt{2}\,\zeta$*,* $\widetilde{\psi} \in C_{\mathcal{F}}$ *the stored root of* ψ*;*
(A6) $\forall k \in \{0, \dots, h-1\} : \ \chi^\zeta_k \in \mathcal{A}$.

Then every depth's computed diagonals are within its bound, the leaves' within the last, and no iterate exceeds the last:

1. $\forall k \in \{0, \dots, h-1\}\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = k\ \forall j \in \{00, 11\}\ \forall \psi : \ \widetilde{d}^\nu_j(\psi)\ \mathcal{I}\left((\chi^\zeta_k)^\pm, 0\right) d^\nu_j(\psi)$*;*

2. $\chi_{\mathrm{leaf}} \le \chi^\zeta_{h-1}$*;*

3. $\forall k \in \{0, \dots, h-1\}: \ \chi^{\zeta}_k \le \chi^{\zeta}_{h-1}$.

Proof.

DEFINES $k \in \{1, \dots, h-1\}$

DEFINES $\nu \in \mathrm{Sub}(T)$ at depth k, the child T_{jj} of its parent π, $j \in \{00, 11\}$ (Definition A.32)

DEFINES ψ, a root of π's ring

DEFINES $a := d^{\pi}_j(\psi)$

DEFINES $b := d^{\pi}_j(-\psi)$

DEFINES $\widetilde{a} := \widetilde{d}^{\pi}_j(\psi)$

DEFINES $\widetilde{b} := \widetilde{d}^{\pi}_j(-\psi)$

DEFINES $\omega_a := \widetilde{a}/a - 1$

DEFINES $\omega_b := \widetilde{b}/b - 1$

DEFINES $\mathcal{B}_{k-1}$: $|\omega_a| \le \chi^{\zeta}_{k-1}$ and $|\omega_b| \le \chi^{\zeta}_{k-1}$

DEFINES $\widetilde{\kappa} := (\widetilde{a} - \widetilde{b})^2/(4\widetilde{a}\widetilde{b})$

Proof of item 1.

Fact D.1, item 1	This proof
Shared: $\psi,\ a, b,\ \mathrm{AM}(a,b)$ (Definition A.46)	
m	2^{h-k+1} (π at depth $k-1$, the proof's block; Definition A.32)
d	d^{π}_j (the statement)
d_0	$d^{\nu}_{00}(\psi^2)$ (Definition A.32; Definition A.20, items 3, 5)
d_1	$g^{\nu}_{01}(\psi^2)$ (Definition A.32)
$m \ge 2$	π at depth $k-1 \le h-2$ (the proof's block)
(I1) $m \in \{2^j : j \in \mathbb{Z}_{\ge 0}\}$	$m := 2^{h-k+1}$ (the rows above)
$d \in \mathcal{R}_m$	d^{π}_j (the statement)
$\psi \in \mathbb{C}$	ψ, a root of π's ring (the proof's block)
$\psi^m = -1$	ψ, a root of π's ring (the proof's block)
Assumption A1	Assumption A2 at a, b (the proof's block); $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$ (the statement)
Assumption A2	Assumption A2 at a, b (the proof's block); $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$ (the statement)
Its conclusion: $d_0 = \mathrm{AM}(a,b)$	
(L1) $d^{\nu}_{00}(\psi^2) = \mathrm{AM}(a,b)$	

[(I1)]

	Fact D.2	This proof
	Shared: $\psi,\ a, b,\ \mathrm{HM}(a,b)$ (Definition A.46)	
	m	2^{h-k+1} (π at depth $k-1$, the proof's block; Definition A.32)
	d	d^{π}_{j} (the statement)
	d_0	$d^{\nu}_{00}(\psi^2)$ (Definition A.32; Definition A.20, items 3, 5)
	d_1	$g^{\nu}_{01}(\psi^2)$ (Definition A.32)
	d_{11}	$d^{\nu}_{11}(\psi^2)$ (the statement; Definition A.32; Definition A.20, items 4, 6)
(I2)	$m \geq 2$	π at depth $k-1 \leq h-2$ (the proof's block)
	$m \in \{2^j : j \in \mathbb{Z}_{\geq 0}\}$	$m := 2^{h-k+1}$ (the rows above)
	$d \in \mathcal{R}_m$	d^{π}_{j} (the statement)
	$\psi \in \mathbb{C}$	ψ, a root of π's ring (the proof's block)
	$\psi^m = -1$	ψ, a root of π's ring (the proof's block)
	Assumption A1	Assumption A2 at a, b (the proof's block); $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$ (the statement)
	Assumption A2	Assumption A2 at a, b (the proof's block); $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$ (the statement)
	Its conclusion: $d_{11} = \mathrm{HM}(a,b)$	
(L2)	$d^{\nu}_{11}(\psi^2) = \mathrm{HM}(a,b)$	
		[(I2)]

	Lemma G.32 at $\chi := \chi^{\zeta}_{k-1}$, under $\mathcal{B}_{k-1}$	This proof
	Shared: $\mathcal{F},\ d_{\mathrm{lo}}, d_{\mathrm{hi}},\ a, b,\ \psi,\ \omega_a, \omega_b,\ \widetilde{a}, \widetilde{b},\ \widetilde{\kappa}$	
	$\widetilde{\psi}$	$\widetilde{\psi}$ (assumption A5)
	χ	χ^{ζ}_{k-1} (the statement)
	$\widetilde{d}_0$	$\widetilde{d}^{\nu}_{00}(\psi^2)$ (the statement; Definition A.20, items 3, 5)
	$\widetilde{d}_{11}$	$\widetilde{d}^{\nu}_{11}(\psi^2)$ (the statement; Definition A.20, items 4, 6)
	c_H	$\mathcal{U}^{\zeta}_{\kappa}(\chi^{\zeta}_{k-1})$ (the statement)
	u_0	$u_0(\chi^{\zeta}_{k-1})$ (the statement)
	$\mathcal{F}$ realization at (u,ζ)	The statement
	$a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$	Assumption A2
	$\psi \in \mathbb{C}$	ψ, a root of π's ring (the proof's block)
(I3)	$\widetilde{\psi} \in C_{\mathcal{F}}$	Assumption A5
	$\chi \in [0,1)$	Assumption A6; $\mathcal{A}$ (the statement)
	$\omega_a, \omega_b \in \mathbb{R}$	ω_a, ω_b (the proof's block)
	Assumption A1	$\widetilde{a}$, $\widetilde{b}$ (the proof's block); $\widetilde{d}^{\pi}_{j}$, computed in $\mathcal{F}$ (the statement)
	Assumption A2	Assumption A1
	Assumption A3	$\mathcal{B}_{k-1}$ (the scope; the proof's block)
	Assumption A4	$\mathcal{B}_{k-1}$ (the scope; the proof's block)
	Assumption A5	ψ, a root of π's ring (the proof's block)
	Assumption A6	Assumption A5
	Assumption A7	Assumption A6; $\mathcal{A}$ (the statement)
	Its item 1: $\tilde{d}_0\ \mathcal{I}\left(((1+\chi)(1+u_0)-1)^{\pm}, 0\right)\ \mathrm{AM}(a,b)$	
	Its item 2: $\tilde{d}_{11}\ \mathcal{I}\left(c_H^{\pm}, 0\right)\ \mathrm{HM}(a,b)$	
(L3)	$\mathcal{B}_{k-1} \Rightarrow\ \widetilde{d}^{\nu}_{00}(\psi^2)\ \mathcal{I}\left(\left((1+\chi^{\zeta}_{k-1})(1+u_0(\chi^{\zeta}_{k-1}))-1\right)^{\pm}, 0\right)\ \mathrm{AM}(a,b)$	
		[item 1 of (I3)]
(L4)	$\mathcal{B}_{k-1} \Rightarrow\ \widetilde{d}^{\nu}_{11}(\psi^2)\ \mathcal{I}\left(\mathcal{U}^{\zeta}_{\kappa}(\chi^{\zeta}_{k-1})^{\pm}, 0\right)\ \mathrm{HM}(a,b)$	
		[item 2 of (I3)]

8178 (L5) $\mathcal{B}_{k-1} \Rightarrow\ |\widetilde{d}^{\nu}_{00}(\psi^2)/d^{\nu}_{00}(\psi^2) - 1| \le (1 + \chi^{\zeta}_{k-1})(1 + u_0(\chi^{\zeta}_{k-1})) - 1$

8179 [(L3), (L1); Definition A.10; Definition A.9]

8180 (L6) $\mathcal{B}_{k-1} \Rightarrow\ |\widetilde{d}^{\nu}_{11}(\psi^2)/d^{\nu}_{11}(\psi^2) - 1| \le \mathcal{U}^{\zeta}_{\kappa}(\chi^{\zeta}_{k-1})$

8181 [(L4), (L2); Definition A.10; Definition A.9]

Fact D.3	This proof
Shared: $\psi,\ a, b$	
m	2^{h-k+1} (π at depth $k-1$, the proof's block; Definition A.32)
d	d^{π}_{j} (the statement)
d_0	$d^{\nu}_{00}(\psi^2)$ (Definition A.32; Definition A.20, items 3, 5)
d_1	$g^{\nu}_{01}(\psi^2)$ (Definition A.32)
κ	$\kappa_{\nu}(\psi^2)$ (the statement; $\mathcal{G}_{\nu}(\psi^2)$, Definition A.32; Definition A.20, items 3, 4)
(I4) $m \ge 2$	π at depth $k-1 \le h-2$ (the proof's block)
$m \in \{2^j : j \in \mathbb{Z}_{\ge 0}\}$	$m := 2^{h-k+1}$ (the rows above)
$d \in \mathcal{R}_m$	d^{π}_{j} (the statement)
$\psi \in \mathbb{C}$	ψ, a root of π's ring (the proof's block)
$\psi^m = -1$	ψ, a root of π's ring (the proof's block)
Assumption A1	Assumption A2 at a, b (the proof's block); $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$ (the statement)
Assumption A2	Assumption A2 at a, b (the proof's block); $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$ (the statement)
Its conclusion: $\kappa = (a-b)^2/(4ab)$	

8183 (L7) $\kappa_{\nu}(\psi^2) = (a-b)^2/(4ab)$

8184 [(I4)]

Lemma G.35 at $\chi := \chi^{\zeta}_{k-1}$, under $\mathcal{B}_{k-1}$	This proof
Shared: $a, b,\ \omega_a, \omega_b,\ \widetilde{a}, \widetilde{b},\ \widetilde{\kappa}$	
χ	χ^{ζ}_{k-1} (the statement)
κ	$\kappa_{\nu}(\psi^2)$ (L7)
ϑ	ϑ_{k-1} (the statement)
(I5) $a, b > 0$	Assumption A2 at a, b (the proof's block); $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$ (the statement)
$\chi \in [0, 1)$	Assumption A6; $\mathcal{A}$ (the statement)
$\omega_a, \omega_b \in \mathbb{R}$	ω_a, ω_b (the proof's block)
Assumption A1	$\mathcal{B}_{k-1}$ (the scope; the proof's block)
Assumption A2	$\mathcal{B}_{k-1}$ (the scope; the proof's block)
Its conclusion: $\widetilde{\kappa} \le \vartheta\kappa + (\vartheta - 1)/2$	

8186 (L8) $\mathcal{B}_{k-1} \Rightarrow\ \widetilde{\kappa} \le \vartheta_{k-1}\kappa_{\nu}(\psi^2) + (\vartheta_{k-1} - 1)/2$

8187 [(I5)]

8188 (L9) $\vartheta_{k-1} \ge 1$

8189 [ϑ_{k-1} (the statement); $\chi^{\zeta}_{k-1} \in [0, 1)$ (assumption A6; $\mathcal{A}$, the statement)]

8190 (L10) $\kappa_{\nu}(\psi^2) \ge 0$

8191 [(L7); $a, b > 0$ (assumption A2)]

8192 (L11) $\kappa_{\nu}(\psi^2) \le \kappa_k$

8193 [assumption A3]

8194 (L12) $\hat{\kappa}_k \ge 0$

8195 [$\hat{\kappa}_k$ (the statement); (L9), (L10), (L11)]

8196 (L13) $\mathcal{B}_{k-1} \Rightarrow\ \widetilde{\kappa} \le \hat{\kappa}_k$

8197 [(L8), (L9), (L11); $\hat{\kappa}_k$ (the statement)]

	Lemma G.34	This proof
	Shared: $u, \zeta,\ d_{\mathrm{lo}}, d_{\mathrm{hi}},\ \mathcal{U}_\kappa^\zeta(\chi), u_0(\chi), \mathcal{A}$	
	χ	χ_{k-1}^ζ (the statement)
	κ	$\hat{\kappa}_k$ (the statement)
(I6)	$u \in [0,1)$	$u \geq 0$ (Definition A.4); assumption A1
	$\zeta \geq 0$	Definition A.4
	$\chi, \kappa \in \mathbb{R}$	χ_{k-1}^ζ, $\hat{\kappa}_k$ (the statement)
	Assumption A1	Assumption A6
	Assumption A2	(L12)
	Its conclusion: $(1+\chi)(1+u_0(\chi)) - 1 \leq \mathcal{U}_\kappa^\zeta(\chi)$	

(L14) $(1+\chi_{k-1}^\zeta)(1+u_0(\chi_{k-1}^\zeta)) - 1 \leq \mathcal{U}_{\hat{\kappa}_k}^\zeta(\chi_{k-1}^\zeta)$

[(I6)]

(L15) $\mathcal{U}_{\hat{\kappa}_k}^\zeta(\chi_{k-1}^\zeta) = \chi_k^\zeta$

[χ_k^ζ (the statement)]

(L16) $\mathcal{B}_{k-1} \Rightarrow\ \widetilde{a}, \widetilde{b} > 0$

[ω_a, ω_b, $\mathcal{B}_{k-1}$ (the proof's block); $a, b \geq d_{\mathrm{lo}}$, $d_{\mathrm{lo}} > 0$ (assumption A2); $\chi_{k-1}^\zeta < 1$ (assumption A6; $\mathcal{A}$, the statement)]

(L17) $\mathcal{B}_{k-1} \Rightarrow\ \widetilde{\kappa} \geq 0$

[$\widetilde{\kappa}$ (the proof's block); (L16)]

	Lemma G.33 under $\mathcal{B}_{k-1}$	This proof
	Shared: $u, \zeta,\ d_{\mathrm{lo}}, d_{\mathrm{hi}},\ \mathcal{U}_\kappa^\zeta(\chi), u_0(\chi), \mathcal{A}$	
	χ, χ'	$\chi_{k-1}^\zeta, \chi_{k-1}^\zeta$ (the statement)
	κ, κ'	$\widetilde{\kappa}, \hat{\kappa}_k$ (the proof's block; the statement)
	$u \in [0,1)$	$u \geq 0$ (Definition A.4); assumption A1
	$\zeta \geq 0$	Definition A.4
(I7)	$\chi, \chi', \kappa, \kappa' \in \mathbb{R}$	χ_{k-1}^ζ, $\hat{\kappa}_k$ (the statement); $\widetilde{\kappa}$ (the proof's block)
	Assumption A1	Assumption A6
	Assumption A2	Assumption A6; $\mathcal{A}$ (the statement)
	Assumption A3	$\chi = \chi'$ (the rows above)
	Assumption A4	(L17)
	Assumption A5	(L13)
	Its conclusion: $\mathcal{U}_\kappa^\zeta(\chi) \leq \mathcal{U}_{\kappa'}^\zeta(\chi')$	

(L18) $\mathcal{B}_{k-1} \Rightarrow\ \mathcal{U}_\kappa^\zeta(\chi_{k-1}^\zeta) \leq \mathcal{U}_{\hat{\kappa}_k}^\zeta(\chi_{k-1}^\zeta)$

[(I7)]

(L19) $k = 0 :\ \forall j\ \forall \psi :\ |\widetilde{d}_j^T(\psi)/d_j^T(\psi) - 1| \leq \chi_0^\zeta$

[assumption A4 at the root node; $\chi_0^\zeta = \chi_0$ (the statement); Definition A.10]

(L20) $[\forall j\ \forall \psi :\ \widetilde{d}_j^\pi(\psi)\ \mathcal{I}\left((\chi_{k-1}^\zeta)^\pm, 0\right) d_j^\pi(\psi)] \Rightarrow\ \mathcal{B}_{k-1}$

[ω_a, ω_b, $\mathcal{B}_{k-1}$ (the proof's block); Definition A.10]

(L21) $\Rightarrow\ \forall j\ \forall \psi :\ \widetilde{d}_j^\nu(\psi^2)\ \mathcal{I}\left((\chi_k^\zeta)^\pm, 0\right) d_j^\nu(\psi^2)$

[(L20); (L5), (L14), (L15) at $j = 00$; (L6), (L15), (L18) at $j = 11$; Definition A.10]

(L22) $\{\psi^2 : \psi \text{ a root of } \pi\text{'s ring}\} = \{\text{the roots of } \nu\text{'s ring}\}$

[Fact A.43, item 5]

(L23) $\Rightarrow$ item 1

[induction on k: the base (L19), the step (L20), (L21), (L22)]

□ (item 1)

Proof of item 2.

Corollary G.36, item 1 at every $\nu \in \mathrm{Sub}(T)$ with $\mathrm{depth}(\nu) = h-1$, $j \in \{00, 11\}$ and ψ	This proof
Shared: $T,\ d_j^\nu, \widetilde{d}_j^\nu,\ \chi_k^\zeta$	
k	$h-1$
$k \in \{0, \dots, h-1\}$	$h \geq 1$ (the statement)
Its item 1: $\forall k \in \{0, \dots, h-1\}\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = k\ \forall j \in \{00, 11\}\ \forall \psi :\ \widetilde{d}_j^\nu(\psi)\ \mathcal{I}\left((\chi_k^\zeta)^\pm, 0\right)\ d_j^\nu(\psi)$	

(I8)

(L24) $\chi_{\mathrm{leaf}} \leq \chi_{h-1}^\zeta$

[(I8); Definition A.10; χ_{leaf} (the statement)]

(L25) $\Rightarrow$ item 2

[(L24)]

□ (item 2)

Proof of item 3.

(L26) $\forall k \in \{1, \dots, h-1\} :\ \chi_{k-1}^\zeta \in [0, 1)$

[assumption A6; $\mathcal{A}$ (the statement)]

(L27) $\forall k \in \{1, \dots, h-1\} :\ u_0(\chi_{k-1}^\zeta) \geq 0$

[(L26); u_0, m_1 (Lemma G.32); u, ζ (Definition A.4); d_{lo} (the statement); assumption A1]

(L28) $\forall k \in \{1, \dots, h-1\} :\ (1 + \chi_{k-1}^\zeta)(1 + u_0(\chi_{k-1}^\zeta)) - 1 = \chi_{k-1}^\zeta + u_0(\chi_{k-1}^\zeta)(1 + \chi_{k-1}^\zeta)$

[expand]

(L29) $\Rightarrow\ \forall k \in \{1, \dots, h-1\} :\ \chi_{k-1}^\zeta \leq (1 + \chi_{k-1}^\zeta)(1 + u_0(\chi_{k-1}^\zeta)) - 1$

[(L26), (L27), (L28); Fact A.41, item 8]

(L30) $\Rightarrow\ \forall k \in \{1, \dots, h-1\} :\ \chi_{k-1}^\zeta \leq \chi_k^\zeta$

[(L29), (L14), (L15)]

(L31) $\chi_{h-1}^\zeta \leq \chi_{h-1}^\zeta$

[expand]

(L32) $\Rightarrow\ \forall k \in \{0, \dots, h-1\} :\ \chi_k^\zeta \leq \chi_{h-1}^\zeta$

[induction on $h-1-k$: the base (L31), the step (L30)]

(L33) $\Rightarrow$ item 3

[(L32)]

□ (item 3)

G.4.2 κ and the root node

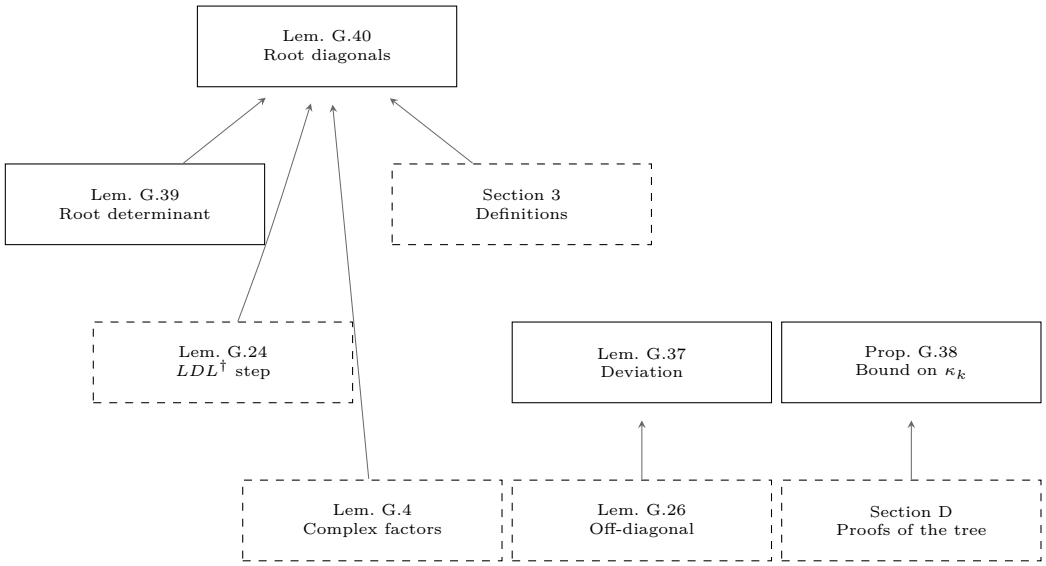


Figure 55: Dependencies, Section G.4.2.

Structure. Lemma G.37 states the deviation of a child's computed off-diagonal; Proposition G.38 the bound on κ_k; Lemma G.40 the computed diagonals at the root node.

Lemma G.37 (Deviation of a child's computed off-diagonal [to table])**.** *A pair perturbed by relative amounts at most χ bounds the computed off-diagonal within a relative part of the one over $\mathbb{R}$, a part proportional to χ and a term in ζ. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $a, b > 0$*;*
- $\psi \in \mathbb{C}$*;*
- $\widetilde{\psi} \in C_{\mathcal{F}}$*;*
- $\chi \in \mathbb{R}$*;*
- $\omega_a, \omega_b \in \mathbb{R}$*.*

Define:

- $\widetilde{a} := a(1+\omega_a)$*;*
- $\widetilde{b} := b(1+\omega_b)$*;*
- $d_0 := (a+b)/2$*;*
- $d_1 := \frac{a-b}{2}\,\mathrm{conj}(\psi)$*;*
- $\widetilde{d}_1$*, the value* $\mathrm{split}_{\mathrm{sa}}$ *(Algorithm 3) computes in* $\mathcal{F}$ *from* $(f(\psi), f(-\psi)) := (\widetilde{a}, \widetilde{b})$ *at line 6, with* $\widetilde{s} := \widetilde{\psi}$*;*
- $c_{\mathrm{sa}} := (1+u)^2(1+u+\sqrt{2}\,\zeta) - 1$ *(Lemma G.26);*
- $k_{\mathrm{sa}} := (1+u)(1+u+\sqrt{2}\,\zeta)/2 + \sqrt{2}$ *(Lemma G.26).*

Assume:

(A1) $|\omega_a| \le \chi$*;*
(A2) $|\omega_b| \le \chi$*;*
(A3) $\widetilde{a}, \widetilde{b} \in \mathcal{F}$*;*
(A4) $|\psi| = 1$*;*
(A5) $|\widetilde{\psi} - \psi| \le u + \sqrt{2}\,\zeta$*.*

Then

$$|\widetilde{d}_1 - d_1| \le c_{\mathrm{sa}}|d_1| + \chi\, d_0(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta.$$

Proof. (L1) $(\widetilde{a} - \widetilde{b}) - (a-b) = a\omega_a - b\omega_b$
[$\widetilde{a}$, $\widetilde{b}$ (the statement)]

(L2) $|a\omega_a - b\omega_b| \le \chi(a+b)$

[assumptions A1, A2; Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$; $a, b > 0$ (the statement)]

(L3) $\chi(a+b) = 2\chi d_0$

[d_0 (the statement)]

Lemma G.26	This proof
Shared: $\mathcal{F}, (u, \zeta),\ \psi, \widetilde{\psi}, \widetilde{a}, \widetilde{b},\ \widetilde{d}_1,\ c_{\text{sa}}, k_{\text{sa}}$ Shared: $\psi \in \mathbb{C},\ \widetilde{\psi} \in C_{\mathcal{F}}$ (I1) Shared: assumptions A4, A5	
$\widetilde{a}, \widetilde{b} \in \mathcal{F}$	Assumption A3
Its conclusion: $\exists\, \delta_{\text{sa}}, e_{\text{sa}} \in \mathbb{C},\ \lvert\delta_{\text{sa}}\rvert \le c_{\text{sa}},\ \lvert e_{\text{sa}}\rvert \le k_{\text{sa}}\zeta :\ \widetilde{d}_1 = \frac{\widetilde{a}-\widetilde{b}}{2}\operatorname{conj}(\psi)(1+\delta_{\text{sa}}) + e_{\text{sa}}$	

(L4) $\exists\, \delta_{\text{sa}}, e_{\text{sa}} \in \mathbb{C},\ |\delta_{\text{sa}}| \le c_{\text{sa}},\ |e_{\text{sa}}| \le k_{\text{sa}}\zeta :\ \widetilde{d}_1 = \frac{\widetilde{a}-\widetilde{b}}{2}\operatorname{conj}(\psi)(1+\delta_{\text{sa}}) + e_{\text{sa}}$

[(I1)]

(L5) $\Rightarrow\ \widetilde{d}_1 - d_1 = \frac{(\widetilde{a}-\widetilde{b})-(a-b)}{2}\operatorname{conj}(\psi)(1+\delta_{\text{sa}}) + d_1\delta_{\text{sa}} + e_{\text{sa}}$

[(L4); d_1 (the statement); expand]

(L6) $\Rightarrow\ |\widetilde{d}_1 - d_1| \le c_{\text{sa}}|d_1| + \chi\, d_0(1+c_{\text{sa}}) + k_{\text{sa}}\zeta$

[(L1) to (L5); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$, $|\operatorname{conj} x| = |x|$; $|\psi| = 1$ (assumption A4)]

(L7) $\Rightarrow$ the statement

[(L6)]

□

Proposition G.38 (The bound on κ_k [to table])**.** *At a depth, κ_k is bounded by the spread of the diagonals one depth above. Let:*

- $h \ge 1$;
- $\mathcal{G} \in \text{Gram}_n$ *(Definition A.14) at* $n := 2^h$;
- $k \in \{1, \dots, h-1\}$.

Define:

- $T :=$ ffLDL$^\dagger(\mathcal{G})$ *(Definition A.20);*
- $\mathcal{G}_\nu$, $\nu \in \text{Sub}(T)$, *that of Definition A.32;*
- (g_{00}, g_{01}, g_{11}), *the entries of* $\mathcal{G}_\nu(\psi)$, ψ *a root of* ν*'s ring (Definition A.14);*
- $d^\nu_{00}(\psi) := g_{00}$;
- $d^\nu_{11}(\psi) := g_{11} - |g_{01}|^2/g_{00}$ *(*LDL† *(Algorithm 5), lines 15, 19);*
- $\kappa_\nu(\psi) := |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$;
- $\varsigma_k := \max_{\pi \in \text{Sub}(T),\ \text{depth}(\pi)=k-1}\ \max_{j \in \{00,11\}}\ \max_\psi d^\pi_j(\psi)/\min_\psi d^\pi_j(\psi)$;
- $\kappa_k := \max_{\nu \in \text{Sub}(T),\ \text{depth}(\nu)=k}\ \max_\psi \kappa_\nu(\psi)$.

Then

$$\kappa_k \le (\varsigma_k - 1)^2/(4\varsigma_k).$$

Proof.

DEFINES $\nu \in \text{Sub}(T)$ at depth k, the child T_{jj} of its parent π, $j \in \{00, 11\}$ (Definition A.32)

DEFINES ψ, a root of π's ring

DEFINES $a := d^\pi_j(\psi)$

DEFINES $b := d^\pi_j(-\psi)$

DEFINES $\rho := \max(a,b)/\min(a,b)$

	Lemma D.6	This proof
	Shared: $\mathcal{G},\ T$	
	Shared: $h \geq 1,\ n := 2^h,\ \mathcal{G} \in \mathrm{Gram}_n$	
(I1)	g^ν_{00}, d^ν_{11}	d^ν_{00}, d^ν_{11} (the statement)
	Its item 1: $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ g^\nu_{00}(\psi) > 0$	
	Its item 2: $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d^\nu_{11}(\psi) > 0$	

(L1) $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d^\nu_{00}(\psi) > 0$

[item 1 of (I1)]

(L2) $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d^\nu_{11}(\psi) > 0$

[item 2 of (I1)]

(L3) $a, b > 0$

[(L1), (L2) at π and $\pm\psi$; a, b (the proof's block)]

	Fact D.3	This proof
	Shared: $\psi,\ a, b$	
	m	2^{h-k+1} (π at depth $k-1$, the proof's block; Definition A.32)
	d	d^π_j (the statement)
	(d_0, d_1)	$(g^\nu_{00}(\psi^2), g^\nu_{01}(\psi^2))$ (Definition A.32; Definition A.20, items 3, 4)
	κ	$\kappa_\nu(\psi^2)$ (the statement; $\mathcal{G}_\nu(\psi^2)$, Definition A.32; Definition A.20, items 3, 4)
(I2)	$m \geq 2$	π at depth $k-1 \leq h-2$ (the proof's block; the statement)
	$m \in \{2^j : j \in \mathbb{Z}_{\geq 0}\}$	$m := 2^{h-k+1}$ (the rows above)
	$d \in \mathcal{R}_m$	d^π_j (the statement)
	$\psi \in \mathbb{C}$	ψ, a root of π's ring (the proof's block)
	$\psi^m = -1$	ψ, a root of π's ring (the proof's block)
	Assumption A1	(L3)
	Assumption A2	(L3)
	Its conclusion: $\kappa = (a-b)^2/(4ab)$	

(L4) $\kappa_\nu(\psi^2) = (a-b)^2/(4ab)$

[(I2)]

(L5) $(a-b)^2/(4ab) = (\rho-1)^2/(4\rho)$

[ρ (the proof's block); divide the numerator and the denominator by $\min(a,b)^2$]

(L6) $(\rho-1)^2/(4\rho) = (\rho + 1/\rho - 2)/4$

[expand]

(L7) $\rho \geq 1$

[ρ (the proof's block); (L3)]

(L8) $\rho \leq \varsigma_k$

[ρ (the proof's block); ς_k (the statement)]

(L9) $\Rightarrow\ (\rho + 1/\rho - 2)/4 \leq (\varsigma_k + 1/\varsigma_k - 2)/4$

[(L7), (L8); $t \mapsto t + 1/t$ nondecreasing on $[1, \infty)$ (Fact A.41, item 5)]

(L10) $(\varsigma_k + 1/\varsigma_k - 2)/4 = (\varsigma_k - 1)^2/(4\varsigma_k)$

[(L6) at $\rho := \varsigma_k$]

(L11) $\Rightarrow\ \kappa_k \leq (\varsigma_k - 1)^2/(4\varsigma_k)$

[(L4), (L5), (L6), (L9), (L10), $\forall \nu,\ \mathrm{depth}(\nu) = k\ \forall \psi$; the roots of ν's ring: the ψ^2 (Fact A.43, item 5); κ_k (the statement)]

(L12) $\Rightarrow$ the statement

[(L11)]

□

Lemma G.39 (The perturbed Gram's determinant [to table])**.** *Perturbing a Gram's three entries by absolute amounts at most E_{00}, E_{11}, E_{01} moves its determinant by at most a bilinear combination of the perturbations and the entries' ceilings. Let:*

- $q \in \mathbb{R}$;
- $g_{00}, g_{11} \in \mathbb{R}$;
- $g_{01} \in \mathbb{C}$;
- $E_{00}, E_{11}, E_{01} \in \mathbb{R}$;
- $M_0, \bar{g}_{11}, \bar{g}_{01} \in \mathbb{R}$;
- $a_{00}, a_{11} \in \mathbb{R}$;
- $a \in \mathbb{C}$.

Define:

- $\widetilde{g}_{00} := g_{00} + a_{00}$;
- $\widetilde{g}_{11} := g_{11} + a_{11}$;
- $\widetilde{g}_{01} := g_{01} + a$;
- $\widetilde{\det} := \widetilde{g}_{00}\widetilde{g}_{11} - |\widetilde{g}_{01}|^2$.

Assume:

(A1) $g_{00} \geq 0$;
(A2) $g_{11} \geq 0$;
(A3) $g_{00} \leq M_0$;
(A4) $g_{11} \leq \bar{g}_{11}$;
(A5) $|g_{01}| \leq \bar{g}_{01}$;
(A6) $g_{00}g_{11} - |g_{01}|^2 = q^2$;
(A7) $|a_{00}| \leq E_{00}$;
(A8) $|a_{11}| \leq E_{11}$;
(A9) $|a| \leq E_{01}$.

Then

$$|\widetilde{\det} - q^2| \leq E_{00}\bar{g}_{11} + E_{11}M_0 + E_{00}E_{11} + 2\bar{g}_{01}E_{01} + E_{01}^2.$$

Proof. (L1) $\widetilde{\det} - q^2 = a_{00}g_{11} + a_{11}g_{00} + a_{00}a_{11} - 2\operatorname{Re}(\operatorname{conj} g_{01}a) - |a|^2$ [$\widetilde{\det}$, $\widetilde{g}_{00}$, $\widetilde{g}_{11}$, $\widetilde{g}_{01}$ (the statement); $q^2 = g_{00}g_{11} - |g_{01}|^2$ (assumption A6); Fact A.41, item 1: $x \operatorname{conj} x = |x|^2$; expand]

(L2) $\Rightarrow$ $|\widetilde{\det} - q^2| \leq E_{00}\bar{g}_{11} + E_{11}M_0 + E_{00}E_{11} + 2\bar{g}_{01}E_{01} + E_{01}^2$ [(L1); $g_{00} \in [0, M_0]$, $g_{11} \in [0, \bar{g}_{11}]$, $|g_{01}| \leq \bar{g}_{01}$, $|a_{00}| \leq E_{00}$, $|a_{11}| \leq E_{11}$, $|a| \leq E_{01}$ (assumptions A1, A2, A3, A4, A5, A7, A8, A9); Fact A.41, item 1: $|x + y| \leq |x| + |y|$, $|\operatorname{Re} x| \leq |x|$, $|xy| = |x||y|$]

(L3) $\Rightarrow$ the statement

[(L2)]

□

Lemma G.40 (The computed diagonals at the root node [to table])**.** *Perturbing the key's Gram matrix entries by absolute amounts at most E_{00}, E_{11}, E_{01} moves the root node's computed diagonals by relative amounts at most e_{00} and the second bound. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $g_{00}, g_{11} \in \mathbb{R}$;
- $g_{01} \in \mathbb{C}$;
- $E_{00}, E_{11}, E_{01} \in \mathbb{R}$;
- $m_0 > 0$;
- $M_0, \bar{g}_{11}, \bar{g}_{01}, \bar{g}_0, \bar{g}_2 \in \mathbb{R}$;
- $a_{00}, a_{11} \in \mathbb{R}$;
- $a \in \mathbb{C}$.

Define:

- *The Gram matrix entries*
  - $\widetilde{g}_{00} := g_{00} + a_{00}$;
  - $\widetilde{g}_{11} := g_{11} + a_{11}$;
  - $\widetilde{g}_{01} := g_{01} + a$;
- *The diagonals*
  - $d_{00} := g_{00}$;
  - $d_{11} := g_{11} - |g_{01}|^2/g_{00}$ (LDL† *(Algorithm 5), line 19);*
  - $\widetilde{d}_{00} := \widetilde{g}_{00}$;
  - $\widetilde{d}_{11}$, *the output of* LDL† *(Algorithm 5) in* $\mathcal{F}$ *at* $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$, *line 18;*
- *The terms*
  - $e_{00} := E_{00}/m_0$;
  - $N_E := \left(E_{00}\bar{g}_{11} + E_{11}M_0 + E_{00}E_{11} + 2\bar{g}_{01}E_{01} + E_{01}^2 + (\bar{g}_{01} + E_{01})^2((1+u)^4 - 1)\right)/q^2$;
  - $Z_E := \left(\sqrt{2}(\bar{g}_2 + 2E_{01}\bar{g}_{01}\bar{g}_0 + E_{01}^2\bar{g}_0)(1+u)^4 + \sqrt{2}(\bar{g}_{01} + E_{01})\bar{g}_0(1+u)^3 + ((2(1+u)+1)(1+u)+1)\bar{g}_0\right)\zeta/q^2$.

Assume:

(A1) $u \le 1$;
(A2) $g_{00}g_{11} - |g_{01}|^2 = q^2$;
(A3) $g_{00} \ge m_0$;
(A4) $g_{00} \le M_0$;
(A5) $g_{00} \le \bar{g}_0$;
(A6) $g_{11} \le \bar{g}_{11}$;
(A7) $|g_{01}| \le \bar{g}_{01}$;
(A8) $|g_{01}|^2 g_{00} \le \bar{g}_2$;
(A9) $|a_{00}| \le E_{00}$;
(A10) $|a_{11}| \le E_{11}$;
(A11) $|a| \le E_{01}$;
(A12) $\widetilde{g}_{00}, \widetilde{g}_{11} \in \mathcal{F}$;
(A13) $\widetilde{g}_{01} \in C_{\mathcal{F}}$;
(A14) $e_{00} < 1$.

Then the root node's two computed diagonals satisfy:

1. $\tilde{d}_{00}\ \mathcal{I}\left(e_{00}^{\pm}, 0\right) d_{00}$;
2. $\tilde{d}_{11}\ \mathcal{I}\left(\left((1+N_E)\frac{1+u}{1-e_{00}} - 1 + Z_E\right)^{\pm}, 0\right) d_{11}$.

Proof.

COMPUTES $\widetilde{zo}$, the value LDL† (Algorithm 5) computes in $\mathcal{F}$ at $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$, line 14
DEFINES $\widetilde{\det} = \widetilde{g}_{00}\widetilde{g}_{11} - |\widetilde{g}_{01}|^2$ (Lemma G.39)
DEFINES $k_{zo}(x) := \sqrt{2}\,x^2(1+u)^3 + \sqrt{2}\,x(1+u)^2 + 2(1+u) + 1$, $x \ge 0$: the k_{zo} of Lemma G.24 at $|g_{01}| := x$

Proof of item 1.

(L1) $|\widetilde{d}_{00}/d_{00} - 1| = |a_{00}|/g_{00}$
[$\widetilde{d}_{00}$, $\widetilde{g}_{00}$, d_{00} (the statement)]

(L2) $\Rightarrow$ $|\widetilde{d}_{00}/d_{00} - 1| \le E_{00}/m_0$
[(L1); $|a_{00}| \le E_{00}$, $g_{00} \ge m_0$, $m_0 > 0$ (assumptions A9, A3); Fact A.41, item 5]

(L3) $E_{00}/m_0 = e_{00}$
[e_{00} (the statement)]

(L4) $\Rightarrow$ $\tilde{d}_{00}\ \mathcal{I}\left(e_{00}^{\pm}, 0\right) d_{00}$
[(L2), (L3); Definition A.10]

(L5) $\Rightarrow$ item 1
[(L4)]

8435 □ (item 1)

8436 *Proof of item 2.*

8437 (L6) $\widetilde{g}_{00} \geq (1 - e_{00})g_{00}$

8438 [(L2), (L3)]

8439 (L7) $(1 - e_{00})g_{00} > 0$

8440 [$e_{00} < 1$, $g_{00} \geq m_0$, $m_0 > 0$ (assumptions A14, A3)]

Lemma G.24, item 3	This proof
Shared: $\mathcal{F}$, $\widetilde{zo}$	
g_{00}, g_{01}	$\widetilde{g}_{00}, \widetilde{g}_{01}$ (the statement)
zo	$\frac{\lvert\widetilde{g}_{01}\rvert^2}{\widetilde{g}_{00}}$ (LDL† (Algorithm 5), line 15)
k_{zo}	$k_{zo}(\lvert\widetilde{g}_{01}\rvert)$ (the proof's block)
$\mathcal{F}$ realization at (u, ζ)	The statement
$g_{00} \in \mathcal{F}$	Assumption A12
$g_{01} \in C_{\mathcal{F}}$	Assumption A13
Assumption A1	Assumption A1
Assumption A2	(L6), (L7)
Its conclusion: $\exists\, \delta_{zo}, E_{zo} \in \mathbb{R},\ \lvert\delta_{zo}\rvert \leq (1+u)^4 - 1,\ \lvert E_{zo}\rvert \leq k_{zo}\,\zeta :\ \widetilde{zo} = zo(1+\delta_{zo}) + E_{zo}$	

8441 (I1)

8442 (L8) $\exists\, \delta_{zo}, E_{zo} \in \mathbb{R},\ \lvert\delta_{zo}\rvert \leq (1+u)^4 - 1,\ \lvert E_{zo}\rvert \leq k_{zo}(\lvert\widetilde{g}_{01}\rvert)\zeta :\ \widetilde{zo} = \frac{\lvert\widetilde{g}_{01}\rvert^2}{\widetilde{g}_{00}}(1+\delta_{zo}) + E_{zo}$

8443 [(I1)]

8444 (L9) $\exists\, u_\circ, \zeta_\circ \in \mathbb{R},\ \lvert u_\circ\rvert \leq u,\ \lvert\zeta_\circ\rvert \leq \zeta :\ \widetilde{d}_{11} = (\widetilde{g}_{11} - \widetilde{zo})(1+u_\circ) + \zeta_\circ$

8445 [Definition A.4, item 1, for $-$ (line 18)]

8446 (L10) $\Rightarrow\ \widetilde{d}_{11} = \frac{\widetilde{\det} - \lvert\widetilde{g}_{01}\rvert^2\delta_{zo}}{\widetilde{g}_{00}}(1+u_\circ) - E_{zo}(1+u_\circ) + \zeta_\circ$

8447 [(L8), (L9); $\widetilde{\det}$ (the proof's block); expand]

8448 (L11) $g_{11} \geq 0$

8449 [$g_{00}g_{11} = q^2 + \lvert g_{01}\rvert^2$, $g_{00} \geq m_0$, $m_0 > 0$ (assumptions A2, A3)]

8450 (L12) $\lvert\widetilde{g}_{01}\rvert \leq \bar{g}_{01} + E_{01}$

8451 [$\widetilde{g}_{01}$ (the statement); assumptions A7, A11; Fact A.41, item 1]

Lemma G.39	This proof
Shared: $q,\ g_{00}, g_{11}, g_{01},\ E_{00}, E_{11}, E_{01},\ M_0, \bar{g}_{11}, \bar{g}_{01},\ a_{00}, a_{11}, a,\ \widetilde{g}_{00}, \widetilde{g}_{11}, \widetilde{g}_{01},\ \widetilde{\det}$ Shared: $g_{00}, g_{11} \in \mathbb{R},\ g_{01} \in \mathbb{C},\ E_{00}, E_{11}, E_{01} \in \mathbb{R},\ M_0, \bar{g}_{11}, \bar{g}_{01} \in \mathbb{R},\ a_{00}, a_{11} \in \mathbb{R},\ a \in \mathbb{C}$	
$q \in \mathbb{R}$	$q = 12289$ (the statement)
Assumption A1	$g_{00} \geq m_0$, $m_0 > 0$ (assumption A3)
Assumption A2	(L11)
Assumption A3	Assumption A4
Assumption A4	Assumption A6
Assumption A5	Assumption A7
Assumption A6	Assumption A2
Assumption A7	Assumption A9
Assumption A8	Assumption A10
Assumption A9	Assumption A11
Its conclusion: $\lvert\widetilde{\det} - q^2\rvert \leq E_{00}\bar{g}_{11} + E_{11}M_0 + E_{00}E_{11} + 2\bar{g}_{01}E_{01} + E_{01}^2$	

8452 (I2)

8453 (L13) $\lvert\widetilde{\det} - q^2\rvert \leq E_{00}\bar{g}_{11} + E_{11}M_0 + E_{00}E_{11} + 2\bar{g}_{01}E_{01} + E_{01}^2$

8454 [(I2)]

8455 (L14) $\Rightarrow\ \left\lvert\frac{\widetilde{\det} - \lvert\widetilde{g}_{01}\rvert^2\delta_{zo}}{q^2} - 1\right\rvert \leq N_E$

8456 [(L13), (L12), (L8); Fact A.41, item 1; N_E (the statement)]

	Lemma G.4	This proof
	k	2
	δ_1	$\frac{\widetilde{\det}-\lvert\widetilde{g}_{01}\rvert^2\delta_{zo}}{q^2}-1$ (L14)
	δ_2	$u_\circ$ (L9)
	c_1, c_2	N_E, u (the statement)
(I3)	$k\in\mathbb{Z}_{\geq 0}$	$2\in\mathbb{Z}_{\geq 0}$
	$\delta_1,\delta_2\in\mathbb{C}$	(L14), (L9)
	$c_1, c_2\geq 0$	N_E (the statement); $u\geq 0$ (Definition A.4)
	Assumption A1	(L14), (L9)

Its conclusion: $\lvert\prod_{j=1}^k(1+\delta_j)-1\rvert\leq\prod_{j=1}^k(1+c_j)-1$

(L15) $\left\lvert\frac{(\widetilde{\det}-\lvert\widetilde{g}_{01}\rvert^2\delta_{zo})(1+u_\circ)}{q^2}-1\right\rvert\leq(1+N_E)(1+u)-1$

[(I3)]

(L16) $d_{11}=q^2/g_{00}$

[d_{11} (the statement); $g_{00}g_{11}-\lvert g_{01}\rvert^2=q^2$ (assumption A2)]

	Fact A.41, item 10	This proof
	x	$(\widetilde{\det}-\lvert\widetilde{g}_{01}\rvert^2\delta_{zo})(1+u_\circ)/q^2$ (L15)
	y	$\widetilde{g}_{00}/g_{00}$ (the statement)
	A	$(1+N_E)(1+u)-1$ (L15)
	b	e_{00} (the statement)
(I4)	$x,y,A,b\in\mathbb{R}$	(L15); $\widetilde{g}_{00}$, g_{00}, e_{00} (the statement)
	$\lvert x-1\rvert\leq A$	(L15)
	$\lvert y-1\rvert\leq b$	(L2), (L3); $\widetilde{d}_{00}$, d_{00} (the statement)
	$b<1$	Assumption A14

Its conclusion: $\lvert x/y-1\rvert\leq(1+A)/(1-b)-1$

(L17) $\left\lvert\frac{(\widetilde{\det}-\lvert\widetilde{g}_{01}\rvert^2\delta_{zo})(1+u_\circ)/q^2}{\widetilde{g}_{00}/g_{00}}-1\right\rvert\leq\frac{1+(1+N_E)(1+u)-1}{1-e_{00}}-1$

[(I4)]

(L18) $\left\lvert\frac{\widetilde{\det}-\lvert\widetilde{g}_{01}\rvert^2\delta_{zo}}{\widetilde{g}_{00}\,d_{11}}(1+u_\circ)-1\right\rvert\leq(1+N_E)\frac{1+u}{1-e_{00}}-1$

[(L17), (L16); expand]

(L19) $\lvert\widetilde{g}_{01}\rvert\leq\lvert g_{01}\rvert+E_{01}$

[$\widetilde{g}_{01}$ (the statement); $\lvert a\rvert\leq E_{01}$ (assumption A11); Fact A.41, item 1]

(L20) $k_{zo}(\lvert\widetilde{g}_{01}\rvert)\leq k_{zo}(\lvert g_{01}\rvert+E_{01})$

[(L19); $k_{zo}(\cdot)$ (the proof's block), nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L21) $\frac{\lvert E_{zo}\rvert(1+u)+\lvert\zeta_\circ\rvert}{d_{11}}\leq(k_{zo}(\lvert g_{01}\rvert+E_{01})(1+u)+1)\frac{g_{00}\,\zeta}{q^2}$

[(L8), (L9), (L16), (L20)]

(L22) $(k_{zo}(\lvert g_{01}\rvert+E_{01})(1+u)+1)\frac{g_{00}\,\zeta}{q^2}\leq Z_E$

[$k_{zo}(\cdot)$ (the proof's block); $\lvert g_{01}\rvert^2 g_{00}\leq\bar{g}_2$, $\lvert g_{01}\rvert\leq\bar{g}_{01}$, $g_{00}\leq\bar{g}_0$ (assumptions A5, A7, A8); Fact A.41, item 8; Z_E (the statement)]

(L23) $\Rightarrow$ item 2

[(L10), (L18), (L21), (L22); Fact A.41, item 1: $\lvert x+y\rvert\leq\lvert x\rvert+\lvert y\rvert$; Definition A.10]

□ (item 2)

G.4.3 The perturbation of the leaf standard deviation and of l_{10}

Structure. Corollary G.41 states the computed leaf standard deviation; Lemma G.42 the computed factor $\widetilde{l}_{10}$.

Corollary G.41 (The computed leaf standard deviation [to table])**.** *A leaf diagonal within χ_{leaf} of the one over $\mathbb{R}$ bounds the computed standard deviation within $\chi_\sigma^\zeta/(1-\chi_\sigma^\zeta)$ of the one over $\mathbb{R}$. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $c_n \in \mathbb{R}$*;*
- $d_{11} > 0$*;*
- $\delta_d \in \mathbb{R}$*;*
- $\chi_{\text{leaf}} \in [0, 1)$*;*
- $s_{\min} > 0$.

Define:

- $\widetilde{d_{11}} := d_{11}(1 + \delta_d)$*;*
- $\texttt{isigma} := \sqrt{d_{11}}\, c_n$*;*
- $\widetilde{\texttt{isigma}} := \text{fl}(\text{fl}(\sqrt{\widetilde{d_{11}}}) \cdot \texttt{INV_SIGMA}[\log_2 n])$*;*
- $k_J := (|c_n| + \sqrt{\widetilde{d_{11}}})(1 + u)^2 + (1 + u)\zeta + 1$ *(Lemma G.21);*
- $\sigma := 1/\texttt{isigma}$*;*
- $\widetilde{\sigma} := 1/\widetilde{\texttt{isigma}}$*;*
- $\chi_\sigma := \max\left((1 + \chi_{\text{leaf}})^{1/2}(1 + u)^3 - 1,\ 1 - (1 - \chi_{\text{leaf}})^{1/2}(1 - u)^3\right)$*;*
- $\chi_\sigma^\zeta := \chi_\sigma + k_J\zeta/s_{\min}$.

Assume:

(A1) $u \le 1$*;*
(A2) $\texttt{INV_SIGMA}[\log_2 n]\ \mathcal{I}\,(u^\pm, \zeta^\pm)\ c_n$*;*
(A3) $|\delta_d| \le \chi_{\text{leaf}}$*;*
(A4) $\texttt{isigma} \ge s_{\min}$*;*
(A5) $\chi_\sigma^\zeta < 1$.

Then

$$\widetilde{\sigma}\ \mathcal{I}\left(\left(\chi_\sigma^\zeta/(1 - \chi_\sigma^\zeta)\right)^\pm, 0\right)\ \sigma.$$

Proof.

DEFINES $\delta' := \delta + E/\texttt{isigma}$, δ, E those of (L2)

(L1) $|\delta_d| \le 1$

[$|\delta_d| \le \chi_{\text{leaf}}$ (assumption A3); $\chi_{\text{leaf}} < 1$ (the statement)]

(I1)

Lemma G.21 at $(\mathcal{F}, n, d_{11}, \delta_d, c_n)$	This proof
Shared: $\mathcal{F}, (u, \zeta),\ n, d_{11}, \delta_d, c_n,\ \texttt{isigma},\ \widetilde{d_{11}},\ \widetilde{\texttt{isigma}},\ k_J$ Shared: assumptions A1, A2	
Assumption A3	(L1)
Its conclusion: $\widetilde{\texttt{isigma}}\ \mathcal{I}\left(\sqrt{1 \pm \lvert\delta_d\rvert}\,(1 \pm u)^3 - 1, k_J\zeta^\pm\right)\ \texttt{isigma}$	

(L2) $\exists\, \delta, E \in \mathbb{R},\ \delta \in [(1 - |\delta_d|)^{1/2}(1 - u)^3 - 1,\ (1 + |\delta_d|)^{1/2}(1 + u)^3 - 1],\ |E| \le k_J\zeta :\ \widetilde{\texttt{isigma}} = \texttt{isigma}\,(1 + \delta) + E$

[(I1)]

(L3) $(1 + |\delta_d|)^{1/2} \le (1 + \chi_{\text{leaf}})^{1/2}$

[$|\delta_d| \le \chi_{\text{leaf}}$ (assumption A3); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L4) $(1 - |\delta_d|)^{1/2} \ge (1 - \chi_{\text{leaf}})^{1/2}$

[$|\delta_d| \le \chi_{\text{leaf}}$, $\chi_{\text{leaf}} < 1$ (assumption A3, the statement); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L5) $\Rightarrow\ |\delta| \le \chi_\sigma$

[(L2), (L3), (L4); $u \le 1$ (assumption A1); Fact A.41, item 8; χ_σ (the statement)]

(L6) $\widetilde{\texttt{isigma}} = \texttt{isigma}\,(1 + \delta')$

[δ' (the proof's block); (L2); $\texttt{isigma} \ge s_{\min}$, $s_{\min} > 0$ (assumption A4)]

(L7) $|\delta'| \le \chi_\sigma + k_J\zeta/s_{\min}$

[(L5), (L6); $|E| \le k_J\zeta$ (L2); $\texttt{isigma} \ge s_{\min}$ (assumption A4); Fact A.41, items 1 and 5]

(L8) $\chi_\sigma + k_J\zeta/s_{\min} = \chi_\sigma^\zeta$

[χ_σ^ζ (the statement)]

(L9) $1 + \delta' \geq 1 - \chi_\sigma^\zeta$

[(L7), (L8)]

(L10) $1 - \chi_\sigma^\zeta > 0$

[$\chi_\sigma^\zeta < 1$ (assumption A5)]

(L11) $\widetilde{\sigma}/\sigma - 1 = 1/(1+\delta') - 1$

[(L6), (L9), (L10); σ, $\widetilde{\sigma}$ (the statement)]

(L12) $1/(1+\delta') - 1 = -\delta'/(1+\delta')$

[expand, at $1 + \delta' > 0$ by (L9), (L10)]

(L13) $\Rightarrow$ $|\widetilde{\sigma}/\sigma - 1| \leq \chi_\sigma^\zeta/(1-\chi_\sigma^\zeta)$

[(L7) to (L12); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5); Definition A.10]

(L14) $\Rightarrow$ the statement

[(L13)]

□

Lemma G.42 (The computed factor $\widetilde{l}_{10}$ [to table])**.** *A quotient computed from a perturbed numerator and a perturbed denominator is within the denominator's and the division's relative perturbations of the one over* $\mathbb{R}$*, plus a term in the numerator's perturbation. Let:*

- $d_0 > 0$*;*
- $\widetilde{d}_0 \in \mathbb{R}$*;*
- $d_1, \widetilde{d}_1 \in \mathbb{C}$*;*
- $e_0 \in \mathbb{R}$*;*
- $\delta, e \in \mathbb{C}$*;*
- $\widetilde{l}_{10} \in \mathbb{C}$*.*

Define:

- $l_{10} := \operatorname{conj}(d_1)/d_0$ *(LDL† (Algorithm 5), line 13).*

Assume:

(A1) $|e_0| < 1$*;*

(A2) $\widetilde{d}_0 = d_0(1+e_0)$*;*

(A3) $\widetilde{l}_{10} = (\operatorname{conj}\widetilde{d}_1/\widetilde{d}_0)(1+\delta) + e$*.*

Then

$$\widetilde{l}_{10}\,\mathcal{N}\left(\frac{|\delta|+|e_0|}{1-|e_0|}, \frac{|\widetilde{d}_1 - d_1|}{d_0}\,\frac{1+|\delta|}{1-|e_0|} + |e|\right) l_{10}.$$

Proof. (L1) $\operatorname{conj}\widetilde{d}_1 = \operatorname{conj} d_1 + \operatorname{conj}\widetilde{d}_1 - d_1$

[Fact A.41, item 13: $\operatorname{conj} x + y = \operatorname{conj} x + \operatorname{conj} y$]

(L2) $\widetilde{l}_{10} = \frac{\operatorname{conj}\widetilde{d}_1}{\widetilde{d}_0}(1+\delta) + e$

[assumption A3]

(L3) $\widetilde{d}_0 = d_0(1+e_0)$

[assumption A2]

(L4) $\operatorname{conj} d_1/d_0 = l_{10}$

[l_{10} (the statement)]

(L5) $\widetilde{l}_{10} - l_{10} = l_{10}\left(\frac{1+\delta}{1+e_0} - 1\right) + \frac{\operatorname{conj}\widetilde{d}_1 - d_1(1+\delta)}{d_0(1+e_0)} + e$

[(L1) to (L4); expand]

(L6) $|1+e_0| \geq 1 - |e_0|$

[Fact A.41, item 1: $||x| - |y|| \leq |x-y|$]

(L7) $1 - |e_0| > 0$

[$|e_0| < 1$ (assumption A1)]

(L8) $\frac{1+\delta}{1+e_0} - 1 = \frac{\delta - e_0}{1+e_0}$

[(L6), (L7); expand]

(L9) $\left|\frac{1+\delta}{1+e_0} - 1\right| \le \frac{|\delta|+|e_0|}{1-|e_0|}$

[(L6), (L7), (L8); Fact A.41, item 1: $|x-y| \le |x| + |y|$]

(L10) $\left|\frac{\operatorname{conj}\widetilde{d}_1 - d_1(1+\delta)}{d_0(1+e_0)}\right| \le \frac{|\widetilde{d}_1 - d_1|}{d_0}\,\frac{1+|\delta|}{1-|e_0|}$

[(L6), (L7); $d_0 > 0$ (the statement); Fact A.41, item 1: $|\operatorname{conj} x| = |x|$, $|x+y| \le |x| + |y|$, $|xy| = |x||y|$]

(L11) $|\widetilde{l}_{10} - l_{10}| \le |l_{10}|\,\frac{|\delta|+|e_0|}{1-|e_0|} + \frac{|\widetilde{d}_1 - d_1|}{d_0}\,\frac{1+|\delta|}{1-|e_0|} + |e|$

[(L5), (L9), (L10); Fact A.41, item 1]

(L12) $\widetilde{l}_{10} \,\mathcal{N}\left(\frac{|\delta|+|e_0|}{1-|e_0|}, \frac{|\widetilde{d}_1 - d_1|}{d_0}\,\frac{1+|\delta|}{1-|e_0|} + |e|\right) l_{10}$

[(L11); Definition A.11]

(L13) $\Rightarrow$ the statement

[(L12)]

□

Corollary G.43 (The computed factors at every node [to table])**.** *At the bounds a child and the root node carry, Lemma G.42's bound is at most an explicit constant. Let:*

- $u \in [0, 1)$;
- $\zeta \in \mathbb{R}$;
- $\chi \in [0, 1)$;
- $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$;
- $\ell \in \mathbb{R}$;
- $m_0 > 0$;
- $e_{00} \in [0, 1)$;
- $E_{01} \in \mathbb{R}$;
- $\kappa_{\mathrm{root}} \ge 0$;
- $d_0 > 0$;
- $\widetilde{d}_0 \in \mathbb{R}$;
- $d_1, \widetilde{d}_1 \in \mathbb{C}$;
- $e_0 \in \mathbb{R}$;
- $\delta, e \in \mathbb{C}$;
- $\widetilde{l}_{10} \in \mathbb{C}$.

Define:

- *The node factor*
  - $l_{10} := \operatorname{conj}(d_1)/d_0$ *(LDL† (Algorithm 5), line 13);*
- *The node bounds*
  - $u_0 := (1+u)\,(1 + \zeta/(2d_{\mathrm{lo}}(1-\chi)(1-u))) - 1$;
  - $c_{\mathrm{sa}} := (1+u)^2(1 + u + \sqrt{2}\,\zeta) - 1$;
  - $k_{\mathrm{sa}} := (1+u)(1 + u + \sqrt{2}\,\zeta)/2 + \sqrt{2}$;
  - $M_2 := d_{\mathrm{hi}}(1+\chi)(1+c_{\mathrm{sa}})/2 + k_{\mathrm{sa}}\zeta$;
  - $\bar{\delta}_\mu := (1+u)^2 - 1$;
  - $\bar{e}_0 := (1+\chi)(1+u_0) - 1$;
  - $\bar{a}_1 := c_{\mathrm{sa}} + \chi(1+c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta/d_{\mathrm{lo}}$;
  - $E_l^{\mathrm{child}} := \dfrac{\bar{\delta}_\mu + \bar{e}_0}{1-\bar{e}_0} + \bar{a}_1\,\dfrac{1+\bar{\delta}_\mu}{1-\bar{e}_0} + \sqrt{2}\,(M_2(1+u)+1)\,\zeta$;
  - $E_l^{\mathrm{root}} := \ell\,\dfrac{\bar{\delta}_\mu + e_{00}}{1-e_{00}} + \dfrac{E_{01}}{m_0}\,\dfrac{1+\bar{\delta}_\mu}{1-e_{00}} + \sqrt{2}\,((\sqrt{\kappa_{\mathrm{root}}}\,q + E_{01})(1+u)+1)\,\zeta$.

Assume:

(A1) $|e_0| < 1$;

(A2) $\widetilde{d}_0 = d_0(1+e_0)$;

(A3) $\widetilde{l}_{10} = (\operatorname{conj} \widetilde{d}_1/\widetilde{d}_0)(1+\delta) + e$;
(A4) $|\delta| \le \bar{\delta}_\mu$.
Then the bound is at most E_l^{child} *at a child's bounds and* E_l^{root} *at the root node's:*

1. *Assume:*

   (A5) $\bar{e}_0 < 1$;
   (A6) $|e_0| \le \bar{e}_0$;
   (A7) $|l_{10}| \le 1$;
   (A8) $|\tilde{d}_1 - d_1| \le \bar{a}_1 d_0$;
   (A9) $|e| \le \sqrt{2}\,(M_2(1+u)+1)\,\zeta$.
   Then $|\widetilde{l}_{10} - l_{10}| \le E_l^{\text{child}}$.

2. *Assume:*

   (A10) $|e_0| \le e_{00}$;
   (A11) $|l_{10}| \le \ell$;
   (A12) $d_0 \ge m_0$;
   (A13) $|\tilde{d}_1 - d_1| \le E_{01}$;
   (A14) $|e| \le \sqrt{2}\,((\sqrt{\kappa_{\text{root}}}\,q + E_{01})(1+u)+1)\,\zeta$.
   Then $|\widetilde{l}_{10} - l_{10}| \le E_l^{\text{root}}$.

Proof.

(I1)

Lemma G.42	This proof
Shared: $d_0, \widetilde{d}_0,\ d_1, \widetilde{d}_1,\ e_0, \delta, e,\ \widetilde{l}_{10}, l_{10}$	
Shared: $d_0 > 0,\ \widetilde{d}_0, e_0 \in \mathbb{R},\ d_1, \widetilde{d}_1, \delta, e, \widetilde{l}_{10} \in \mathbb{C}$	
Shared: assumptions A1, A2, A3	
Its conclusion: $\tilde{l}_{10}\,\mathcal{N}\left(\frac{\lvert\delta\rvert+\lvert e_0\rvert}{1-\lvert e_0\rvert}, \frac{\lvert\tilde{d}_1-d_1\rvert}{d_0}\,\frac{1+\lvert\delta\rvert}{1-\lvert e_0\rvert} + \lvert e\rvert\right) l_{10}$	
$\lvert\widetilde{l}_{10} - l_{10}\rvert \le \lvert l_{10}\rvert\,\frac{\lvert\delta\rvert+\lvert e_0\rvert}{1-\lvert e_0\rvert} + \frac{\lvert\tilde{d}_1-d_1\rvert}{d_0}\,\frac{1+\lvert\delta\rvert}{1-\lvert e_0\rvert} + \lvert e\rvert$	
	[(I1); Definition A.11]

(L2) $\forall c \ge 0\ \forall t \in [0,1):\ \frac{c+t}{1-t} = \frac{1+c}{1-t} - 1$
[expand]

(L3) $\forall x, y \in [0,1):\ x \le y \Rightarrow\ \frac{|\delta|+x}{1-x} \le \frac{|\delta|+y}{1-y}$
[(L2) at $c := |\delta|$; $0 < 1-y \le 1-x$; $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L4) $\forall x, y \in [0,1):\ x \le y \Rightarrow\ \frac{1+|\delta|}{1-x} \le \frac{1+|\delta|}{1-y}$
[$0 < 1-y \le 1-x$; $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L5) $|\widetilde{l}_{10} - l_{10}| \le \frac{\bar{\delta}_\mu+\bar{e}_0}{1-\bar{e}_0} + \bar{a}_1\,\frac{1+\bar{\delta}_\mu}{1-\bar{e}_0} + \sqrt{2}\,(M_2(1+u)+1)\,\zeta$
[(L1), (L3), (L4); assumptions A5, A6, A7, A8, A9; $|\delta| \le \bar{\delta}_\mu$ (assumption A4)]

(L6) $\Rightarrow$ item 1
[(L5); E_l^{child} (the statement)]

(L7) $|\widetilde{l}_{10} - l_{10}| \le \ell\,\frac{\bar{\delta}_\mu+e_{00}}{1-e_{00}} + \frac{E_{01}}{m_0}\,\frac{1+\bar{\delta}_\mu}{1-e_{00}} + \sqrt{2}\,((\sqrt{\kappa_{\text{root}}}\,q + E_{01})(1+u)+1)\,\zeta$
[(L1), (L3), (L4); assumptions A10, A11, A12, A13, A14; $|\delta| \le \bar{\delta}_\mu$ (assumption A4)]

(L8) $\Rightarrow$ item 2
[(L7); E_l^{root} (the statement)]

□ (items 1 and 2)

G.5 The centers

Structure. This subsection proves the bound on the shift of the computed leaf centers, Theorem G.59. Section G.5.1 states the center map; Section G.5.2 the entry shifts and the center shift.

The symbols and the constants. $\mathcal{L}_T$ is Definition G.6's, $\mathcal{G}$, d_i, t and z are Section 3.2's, and c_{split}, c_{merge}, k_D, k_E, k_I and k_B are the constants of Section G.3 (Table 20).

G.5.1 The center map

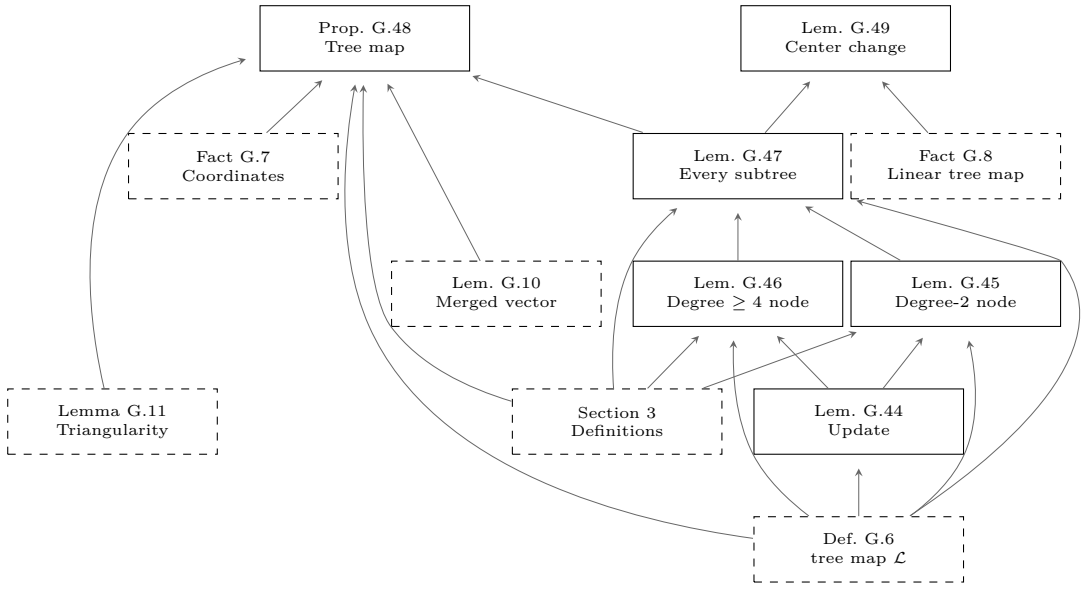


Figure 56: Dependencies, Section G.5.1.

Lemmas G.44 to G.47 state the leaf centers at each node; Proposition G.48 the leaf centers as an affine image of the center. Every norm of this section is the coefficient norm.

Lemma G.44 (The call's update is the node factor [to table])**.** *At every node, the node factor maps the center minus the sample to the updated center minus the sample. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $t \in \mathcal{R}_n \times \mathcal{R}_n$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*, a sample of* ffSampling(t, T) *(Definition G.9).*

Define, at each $\nu \in \mathrm{Sub}(T)$*, the values of* ffSampling *(Definition A.21) at* (t, T) *with the sample* z*:*

- t_ν*, item 6;*
- $\hat{z}_\nu$*, items 12 and 20;*
- $tb_{0,\nu}$*, items 9 and 16;*
- $(t_0, t_1) := t_\nu$*;*
- $(z_0, z_1) := \hat{z}_\nu$*;*
- L_ν*, the node factor (Definition G.6).*

Then

$$\forall \nu = \mathrm{node}(l_{10};\ \cdot, \cdot) \in \mathrm{Sub}(T): \quad (t_\nu - \hat{z}_\nu) L_\nu = (tb_{0,\nu} - z_0,\ t_1 - z_1).$$

Proof.

DEFINES l_{10}, the factor of $\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11})$ (Definition A.18)

(L1) $tb_{0,\nu} = t_0 + (t_1 - z_1)\, l_{10}$
[Definition A.21, item 9 with item 12 at $m = 2$ and item 16 with item 20 at $m \geq 4$: $(z_0, z_1) = \hat{z}_\nu$ (the proof's block) in both]

(L2) $\Rightarrow$ the statement
[(L1); $xL_\nu = (x_0 + x_1 l_{10},\ x_1)$ (Definition G.6, the node factor) at $x := t_\nu - \hat{z}_\nu$]

□

Lemma G.45 (The leaf centers at a node of degree 2 [to table])**.** *At a node whose children are leaves, the leaf centers minus the sample are the node's tree map of its center minus its sample, and the right leaf's center minus its sample is the second part of the node's. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $t \in \mathcal{R}_n \times \mathcal{R}_n$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*, a sample of* ffSampling(t, T) *(Definition G.9).*

Define:

- $c := (c_i)_{i \le N}$*, the leaf centers with the sample* z *(Definition G.9);*
- $t_{T'}$*,* $T' \in \mathrm{Sub}(T)$*, the value of* ffSampling *(Definition A.21) at* (t, T) *with the sample* z*, items 7 to 12;*
- $\hat{z}_{T'}$*,* $T' \in \mathrm{Sub}(T)$*, the value of* ffSampling *(Definition A.21) at* (t, T) *with the sample* z*, items 7 to 12;*
- $I(T')$*,* $T' \in \mathrm{Sub}(T)$*, its positions (Definition A.19);*
- $\mathcal{L}_{T'}$*,* $T' \in \mathrm{Sub}(T)$*, the tree map (Definition G.6);*
- $(x\mathcal{L}_{T'})_i$*, its real coordinates (Definition G.6).*

Then

1. $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T) :\ (c - z)_{I(\nu)} = (t_\nu - \hat{z}_\nu)\mathcal{L}_\nu$*;*
2. $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T),\ (t_0, t_1) := t_\nu,\ (z_0, z_1) := \hat{z}_\nu :\ t_{d_{11}} - \hat{z}_{d_{11}} = t_1 - z_1.$

Proof.

DEFINES $\nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T)$: that of the statement's items
DEFINES $(t_0, t_1) := t_\nu$
DEFINES $(z_0, z_1) := \hat{z}_\nu$
DEFINES $tb_{0,\nu}$: that of ffSampling (Definition A.21) at ν, item 9

(L1) $\forall d \in \{d_{00}, d_{11}\},\ I(d) = \{j, j+1\} :\ (c_j, c_{j+1}) = (\mathrm{Re}\, t_d,\ \mathrm{Im}\, t_d)$
[Definition A.21, item 2]

(L2) $\forall d \in \{d_{00}, d_{11}\},\ I(d) = \{j, j+1\} :\ \hat{z}_d = z_j + i z_{j+1}$
[Definition A.21, item 4]

(L3) $\Rightarrow\ \forall d \in \{d_{00}, d_{11}\},\ I(d) = \{j, j+1\} :\ (c_j - z_j,\ c_{j+1} - z_{j+1}) = (\mathrm{Re}\,(t_d - \hat{z}_d),\ \mathrm{Im}\,(t_d - \hat{z}_d))$
[(L1), (L2)]

(L4) $\forall d \in \{d_{00}, d_{11}\},\ I(d) = \{j, j+1\} :\ (\mathrm{Re}\,(t_d - \hat{z}_d),\ \mathrm{Im}\,(t_d - \hat{z}_d)) = ((t_d - \hat{z}_d)\mathcal{L}_d)_{I(d)}$
[$x\mathcal{L}_d = x$ and $(x\mathcal{L}_T)_{2\ell-1} = \mathrm{Re}\,(x\mathcal{L}_T)_\ell$, $(x\mathcal{L}_T)_{2\ell} = \mathrm{Im}\,(x\mathcal{L}_T)_\ell$ (Definition G.6)]

(L5) $t_{d_{11}} = t_1$
[Definition A.21, item 7]

(L6) $\hat{z}_{d_{11}} = z_1$
[Definition A.21, items 8, 12: $(z_0, z_1) = \hat{z}_\nu$, $\hat{z}_\nu = (\hat{z}_{d_{00}}, \hat{z}_{d_{11}})$]

(L7) $t_{d_{00}} = tb_{0,\nu}$
[Definition A.21, item 10]

(L8) $\hat{z}_{d_{00}} = z_0$
[Definition A.21, items 11, 12: $(z_0, z_1) = \hat{z}_\nu$, $\hat{z}_\nu = (\hat{z}_{d_{00}}, \hat{z}_{d_{11}})$]

(L9) $(t_\nu - \hat{z}_\nu)\mathcal{L}_\nu = (t_1 - z_1,\ tb_{0,\nu} - z_0)$
[$x\mathcal{L}_\nu = (x_1,\ x_0 + x_1 l_{10})$ (Definition G.6); Lemma G.44]

(L10) $I(\nu) = I(d_{11}) \sqcup I(d_{00})$
[Definition A.19]

(L11) $\max I(d_{11}) < \min I(d_{00})$
[Definition A.19]

(L12) $\Rightarrow\ (t_\nu - \hat{z}_\nu)\mathcal{L}_\nu = (t_{d_{11}} - \hat{z}_{d_{11}},\ t_{d_{00}} - \hat{z}_{d_{00}})$
[(L9); (L5) to (L8)]

(L13) $\Rightarrow$ item 1
[(L12); (L3), (L4) at d_{11} and at d_{00}; (L10), (L11)]

(L14) $\Rightarrow$ item 2

[(L5), (L6)]

□ (items 1 and 2)

Lemma G.46 (The leaf centers at a node of degree at least 4 [to table])**.** *At a node of degree at least* 4*, the right child's center minus its sample is the split of the node's, and the relation between the leaf centers and the tree map passes from the two children to the node. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $t \in \mathcal{R}_n \times \mathcal{R}_n$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*, a sample of* ffSampling(t, T) *(Definition G.9);*
- $m \geq 4$*;*
- $\nu = \text{node}(l_{10};\ T_{00}, T_{11}) \in \text{Sub}(T) \cap \mathcal{T}_m$*.*

Define:

- *The node factor*
  - $L_{T'} := \begin{pmatrix} 1 & 0 \\ l_{10} & 1 \end{pmatrix}$*,* l_{10} *the factor of the node* T'*, the node factor (Definition G.6);*
- *The tree map*
  - $\mathcal{L}_{T'}$*,* $T' \in \text{Sub}(T)$*, the tree map (Definition G.6);*
- *The coordinates*
  - $I(T')$*,* $T' \in \text{Sub}(T)$*, its positions (Definition A.19);*
  - $(x\mathcal{L}_{T'})_i$*, its real coordinates (Definition G.6);*
- *The centers and the samples*
  - $c := (c_i)_{i \leq N}$*, the leaf centers with the sample* z *(Definition G.9);*
  - $t_{T'}$*,* $T' \in \text{Sub}(T)$*, the value of* ffSampling *(Definition A.21) at* (t, T) *with the sample* z*, items 13 to 20;*
  - $\hat{z}_{T'}$*,* $T' \in \text{Sub}(T)$*, the value of* ffSampling *(Definition A.21) at* (t, T) *with the sample* z*, items 13 to 20;*
  - $(t_0, t_1) := t_\nu$*;*
  - $(z_0, z_1) := \hat{z}_\nu$*;*
  - $tb_{0,\nu}$*, that of* ffSampling *(Definition A.21) at* ν*, item 16.*

Then

1. $t_{T_{11}} - \hat{z}_{T_{11}} = \text{split}(t_1 - z_1)$*;*
2. *Assume:*

   (A1) $\forall T' \in \{T_{00}, T_{11}\} :\ (c - z)_{I(T')} = (t_{T'} - \hat{z}_{T'})\mathcal{L}_{T'}$*.*

   Then $(c - z)_{I(\nu)} = (t_\nu - \hat{z}_\nu)\mathcal{L}_\nu$*.*

Proof. (L1) $t_{T_{11}} = \text{split}(t_1)$

[Definition A.21, item 13]

(L2) $t_{T_{00}} = \text{split}(tb_{0,\nu})$

[Definition A.21, item 17]

(L3) $z_1 = \text{merge}(\hat{z}_{T_{11}})$

[Definition A.21, items 15, 20]

(L4) $z_0 = \text{merge}(\hat{z}_{T_{00}})$

[Definition A.21, items 19, 20]

(L5) $\Rightarrow$ $\hat{z}_{T_{11}} = \text{split}(z_1)$

[(L3); split(merge(y)) = y (Fact A.42, item 5)]

(L6) $\Rightarrow$ $\hat{z}_{T_{00}} = \text{split}(z_0)$

[(L4); split(merge(y)) = y (Fact A.42, item 5)]

(L7) $\Rightarrow$ $t_{T_{11}} - \hat{z}_{T_{11}} = \mathrm{split}(t_1 - z_1)$

[(L1), (L5); Fact A.42, item 4]

(L8) $\Rightarrow$ $t_{T_{00}} - \hat{z}_{T_{00}} = \mathrm{split}(tb_{0,\nu} - z_0)$

[(L2), (L6); Fact A.42, item 4]

(L9) $(t_\nu - \hat{z}_\nu)\mathcal{L}_\nu = (\mathrm{split}(((t_\nu - \hat{z}_\nu)L_\nu)_1)\mathcal{L}_{T_{11}},\ \mathrm{split}(((t_\nu - \hat{z}_\nu)L_\nu)_0)\mathcal{L}_{T_{00}})$

[$x\mathcal{L}_\nu = (\mathrm{split}((xL_\nu)_1)\mathcal{L}_{T_{11}},\ \mathrm{split}((xL_\nu)_0)\mathcal{L}_{T_{00}})$ (Definition G.6) at $x := t_\nu - \hat{z}_\nu$]

(L10) $(t_\nu - \hat{z}_\nu)L_\nu = (tb_{0,\nu} - z_0,\ t_1 - z_1)$

[Lemma G.44]

(L11) $\Rightarrow$ $(t_\nu - \hat{z}_\nu)\mathcal{L}_\nu = ((t_{T_{11}} - \hat{z}_{T_{11}})\mathcal{L}_{T_{11}},\ (t_{T_{00}} - \hat{z}_{T_{00}})\mathcal{L}_{T_{00}})$

[(L9), (L10), (L7), (L8)]

(L12) $I(\nu) = I(T_{11}) \sqcup I(T_{00})$

[Definition A.19]

(L13) $\max I(T_{11}) < \min I(T_{00})$

[Definition A.19]

(L14) $\Rightarrow$ item 2

[(L11); assumption A1 at T_{11} and at T_{00}; (L12), (L13)]

(L15) $\Rightarrow$ item 1

[(L7)]

$\square$ (items 1 and 2)

Lemma G.47 (The leaf centers at every subtree [to table])**.** *At every subtree, the leaf centers minus the sample are the subtree's tree map of its center minus its sample. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $t \in \mathcal{R}_n \times \mathcal{R}_n$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*, a sample of* ffSampling(t, T) *(Definition G.9).*

Define:

- $c := (c_i)_{i \le N}$*, the leaf centers with the sample* z *(Definition G.9);*
- $t_{T'}$, $T' \in \mathrm{Sub}(T)$*, the value of* ffSampling *(Definition A.21) at* (t, T) *with the sample* z*, items 7, 10, 13, 14, 17, 18;*
- $\hat{z}_{T'}$, $T' \in \mathrm{Sub}(T)$*, the value of* ffSampling *(Definition A.21) at* (t, T) *with the sample* z*, items 8, 11;*
- $I(T')$, $T' \in \mathrm{Sub}(T)$*, its positions (Definition A.19);*
- $\mathcal{L}_{T'}$, $T' \in \mathrm{Sub}(T)$*, the tree map (Definition G.6);*
- $(x\mathcal{L}_{T'})_i$*, its real coordinates (Definition G.6).*

Then

$$\forall T' \in \mathrm{Sub}(T): \quad (c - z)_{I(T')} = (t_{T'} - \hat{z}_{T'})\mathcal{L}_{T'}.$$

Proof. (L1) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\}:\ (c - z)_{I(d)} = (c_j - z_j,\ c_{j+1} - z_{j+1})$

[$I(d) = \{j, j+1\}$ (Definition A.19)]

(L2) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\}:\ (c_j - z_j,\ c_{j+1} - z_{j+1}) = ((t_d - \hat{z}_d)\mathcal{L}_d)_{I(d)}$

[Definition A.21, items 2 and 4: $(c_j, c_{j+1}) = (\mathrm{Re}\, t_d, \mathrm{Im}\, t_d)$, $\hat{z}_d = z_j + iz_{j+1}$; $x\mathcal{L}_d = x$ (Definition G.6) and the real coordinates (Definition G.6)]

(L3) $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T):\ (c - z)_{I(\nu)} = (t_\nu - \hat{z}_\nu)\mathcal{L}_\nu$

[Lemma G.45, item 1]

(L4) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \ge 4:$
$[\forall T' \in \{T_{00}, T_{11}\}:\ (c - z)_{I(T')} = (t_{T'} - \hat{z}_{T'})\mathcal{L}_{T'}] \Rightarrow\ (c - z)_{I(\nu)} = (t_\nu - \hat{z}_\nu)\mathcal{L}_\nu$

[Lemma G.46, item 2, at each such ν]

(L5) $\forall T' \in \mathrm{Sub}(T):\ T' \in \mathbb{R} \vee T' = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \vee (T' = \mathrm{node}(l_{10};\ T_{00}, T_{11}),\ T_{00}, T_{11} \in \mathrm{Sub}(T))$

[Definition A.18]

(L6) $\Rightarrow$ the statement

[induction on the depth from the leaves: (L1), (L2), (L3) the base, (L4) the step, (L5) the cases]

□

Proposition G.48 (The leaf centers and the tree map [to table])**.** *The leaf centers minus the sample are the tree map of the center minus the sample, and the map inverts. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $t \in \mathcal{R}_n \times \mathcal{R}_n$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*, a sample of* ffSampling(t, T) *(Definition G.9).*

Define:

- $c := (c_i)_{i \le N}$*, the leaf centers with the sample* z *(Definition G.9);*
- $\mathcal{L}_T$*, the tree map (Definition G.6);*
- $\mathcal{L}_T^{-1}$*, the inverse of* $\mathcal{L}_T$ *(Lemma G.11).*

Then:

1. $c - z = (t - z)\mathcal{L}_T$*;*
2. $t - z = (c - z)\mathcal{L}_T^{-1}$*.*

Proof.

DEFINES $t_{T'}$, $\hat{z}_{T'}$ (ffSampling (Definition A.21) at (t, T), items 5 to 20)

Proof of item 1.

Lemma G.47	This proof
Shared: $T, t, z,\ N, c,\ t_{T'}, \hat{z}_{T'}$ (the proof's block), $I(T'), \mathcal{L}_{T'}$ Shared: $T \in \mathcal{T}_n,\ t \in \mathcal{R}_n \times \mathcal{R}_n,\ z \in \mathbb{Z}^N$	
T' $T' \in \mathrm{Sub}(T)$	T Definition A.18
Its conclusion: $\forall T' \in \mathrm{Sub}(T) :\ (c - z)_{I(T')} = (t_{T'} - \hat{z}_{T'})\mathcal{L}_{T'}$	

(I1)

(L1) $(c - z)_{I(T)} = (t_T - \hat{z}_T)\mathcal{L}_T$

[(I1); $I(T) = \{1, \ldots, N\}$ (Definition A.19)]

(L2) $t_T = t$

[Definition A.21, item 5]

Lemma G.10, item 3	This proof
Shared: $T, t, z,\ N,\ \hat{z}_{T'}$ (the proof's block) Shared: $T \in \mathcal{T}_n,\ z \in \mathbb{Z}^N$	
$t \in \mathcal{R}_n^2$	$t \in \mathcal{R}_n \times \mathcal{R}_n$ (the statement)
Its item 3: $((\hat{z}_T)_i)_{i \le N} = z$	

(I2)

(L3) $((\hat{z}_T)_i)_{i \le N} = z$

[(I2)]

(L4) $\Rightarrow$ item 1

[(L1), (L2), (L3); x_i (Definition G.6, the coordinates) at $x := t - \hat{z}_T$, $\mathbb{R}$-linear in x (Fact G.7, item 4)]

□ (item 1)

Proof of item 2.

(L5) $c - z = (t - z)\mathcal{L}_T$

[item 1]

(L6) $\Rightarrow$ item 2

[(L5); $\mathcal{L}_T$ invertible (Lemma G.11; Fact A.44, item 5)]

□ (item 2)

Lemma G.49 (The leaf centers under a change of a call's center [to table])**.** *The leaf centers are affine in the center a call receives: a change of that center moves the leaf centers of the call's positions by its tree map. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $t \in \mathcal{R}_n \times \mathcal{R}_n$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*, a sample of* ffSampling(t, T) *(Definition G.9).*

Define:

- t_ν*,* $\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m$*,* $m \in \{2, 4, \ldots, n\}$*, the center the call at* ν *receives with the sample* z*;*
- $c(\cdot, z) : \mathcal{R}_m \times \mathcal{R}_m \to \mathbb{R}^N$ *at such a* ν*,* $y \mapsto$ *the leaf centers with the sample* z *when the call at* ν *receives* y *in place of* t_ν*;*
- $\mathcal{L}_\nu$*,* $\nu \in \mathrm{Sub}(T)$*, the tree map (Definition G.6);*
- $I(\nu)$*,* $\nu \in \mathrm{Sub}(T)$*, the positions (Definition A.19).*

Then the leaf centers move by the tree map:

$$\forall m \in \{2, 4, \ldots, n\}\ \forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m\ \forall e \in \mathcal{R}_m \times \mathcal{R}_m :\ (c(t_\nu + e, z) - c(t_\nu, z))_{I(\nu)} = e\mathcal{L}_\nu.$$

Proof.

DEFINES $\hat{z}_\nu$, $\nu \in \mathrm{Sub}(T)$ (ffSampling (Definition A.21) at (t, T), items 15, 19, 20, 12)

(I1)

Lemma G.47 at every m, $\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m$ and $y \in \mathcal{R}_m \times \mathcal{R}_m$, the call at ν receiving y	This proof
n	m
T	ν
t	y
z	$z_{I(\nu)}$
T'	ν
c	$c(y, z)_{I(\nu)}$ (Definition G.9; Definition A.21)
$t_{T'}$	y (Definition A.21, item 5)
$\hat{z}_{T'}$	$\hat{z}_\nu$
$T \in \mathcal{T}_n$	$\nu \in \mathcal{T}_m$
$t \in \mathcal{R}_n \times \mathcal{R}_n$	$y \in \mathcal{R}_m \times \mathcal{R}_m$
$z \in \mathbb{Z}^{2n}$	$I(\nu)$ (Definition A.19)
$T' \in \mathrm{Sub}(T)$	Definition A.18
Its conclusion: $\forall T' \in \mathrm{Sub}(T) :\ (c - z)_{I(T')} = (t_{T'} - \hat{z}_{T'})\mathcal{L}_{T'}$	

(L1) $\forall m\ \forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m\ \forall y \in \mathcal{R}_m \times \mathcal{R}_m :\ (c(y, z) - z)_{I(\nu)} = (y - \hat{z}_\nu)\mathcal{L}_\nu$

[(I1); $\hat{z}_\nu$ set by z alone (Definition A.21, items 15, 19, 20, 12)]

(L2) $\forall \nu \in \mathrm{Sub}(T)\ \forall x, y\ \forall a \in \mathbb{R} :\ (x + ay)\mathcal{L}_\nu = x\mathcal{L}_\nu + a\, y\mathcal{L}_\nu$

[Fact G.8 at $T' := \nu$]

(L3) $\Rightarrow$ the statement

[(L1) at $y := t_\nu + e$ and at $y := t_\nu$; (L2) at ν]

□

G.5.2 The entry shifts and the center shift

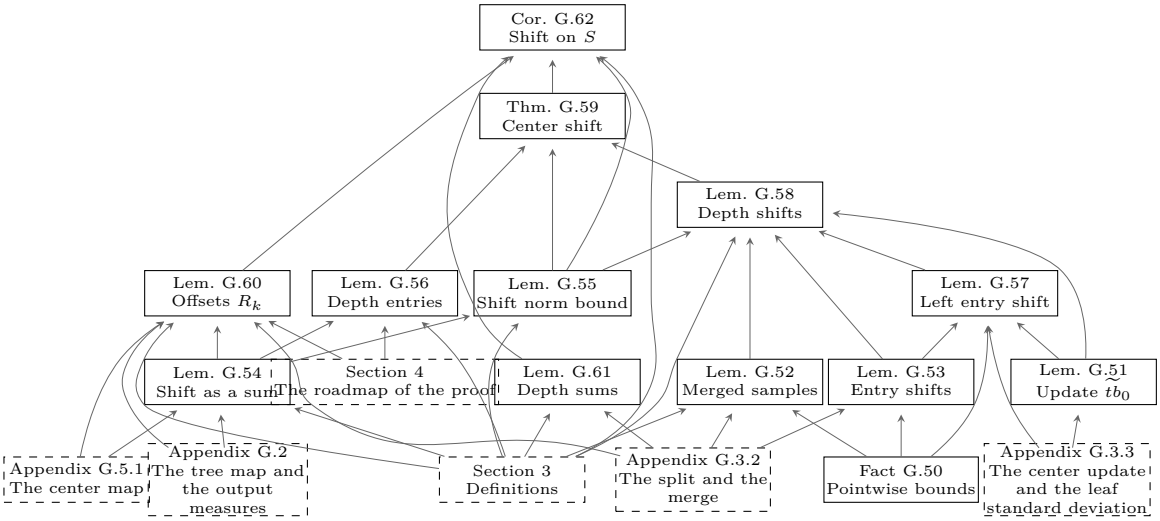


Figure 57: Dependencies, Section G.5.2.

Table 21 lists the constants; Lemmas G.51 to G.58 state the steps; Lemma G.53 the entry shifts at one node; Theorem G.59 the center shift.

k_{split}	$\sqrt{2}/2 + k_D$	Split
e_{mul}	$\sqrt{2}\,u(2+u)$	Complex product
G_X	$u + (1+u)c_{\text{split}}$	Update
G_R	$E_l + (1+c_{\text{split}})(1+u)(u+(1+u)e_{\text{mul}})\widetilde{\ell} + G_X E_l$	Update
G_Z	$(1+G_X)\ell + G_R$	Merged samples
G_γ	$c_{\text{split}} + G_X(1+\ell) + G_R$	Fixed point
K_ζ	$(k_{\text{split}} + (1+c_{\text{split}})k_I(\widetilde{\ell}))\zeta$	Update
M_k	$(1+c_{\text{merge}})^{h-k} - 1$	Merge chain
a_j	$k_E\zeta\,\dfrac{r^j-1}{r-1}$, $r = \sqrt{2}(1+c_{\text{merge}})$	Merge chain
Θ_k	$\sqrt{2^{k-1}}(k_{\text{split}}\zeta + K_\zeta + G_Z a_{h-k})$	Depth k
β_j	$1/\Xi'_{\text{root}}$ at $j=0$, $2\Xi_j$ at $1 \le j \le h-1$	Fixed point

Table 21: The constants of the bounds of Section G.5; c_{split}, k_D, c_{merge}, k_E and k_I are Table 20's, $k_I(\widetilde{\ell})$ at $|l_{10}| := \widetilde{\ell}$, e_{mul} Lemma B.2, item 3's, and ℓ, $\widetilde{\ell}$, E_l Theorem G.59's.

Fact G.50 (Pointwise bounds in the coefficient norm [to table])**.** Pointwise bounds on the entries imply a bound on the vector in the coefficient norm, its absolute part scaled by $(wM)^{1/2}$. Let:

- $w > 0$;
- $M \in \mathbb{Z}_{\ge 0}$ (Definition A.1);
- $x = (x_p)_{p<M}$ with $x_p \in \mathbb{C}$ or $\mathbb{C}^2$;
- $y = (y_p)_{p<M}$ with y_p in the same set as x_p;
- $c, e \ge 0$.

Define:

- $\|x\| := \left(w\sum_{p<M}\|x_p\|^2\right)^{1/2}$, the coefficient norm.

Assume:

(A1) $\forall p < M:\ y_p\,\mathcal{N}(c,e)\,x_p$.

Then

$$y\,\mathcal{N}\left(c,(wM)^{1/2}e\right)\,x.$$

Proof. (L1) $\|y-x\| \le \left(w\sum_{p<M}(c\|x_p\|+e)^2\right)^{1/2}$
[assumption A1 at every p; $\|\cdot\|$ (the statement); $x\mapsto x^2$, $x\mapsto\sqrt{x}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L2) $\left(w\sum_{p<M}e^2\right)^{1/2} = (wM)^{1/2}e$
[expand]

(L3) $\Rightarrow$ the statement
[(L1); $\|x+y\|\le\|x\|+\|y\|$ (Fact A.41, item 3) in $\mathbb{R}^M$ at $X := (c\|x_p\|)_p$, $Y := (e)_p$; (L2)]
□

Lemma G.51 (The computed update $\widetilde{tb}_0$ [to table])**.** *At a node, the computed update is within a term in the factor's perturbation, a term in the sample's perturbation, the update's own roundings and a term in ζ of X_0. Let:*

- $h \ge 1$;
- $\mathcal{F}$ *be a realization at* (u,ζ) *(Definition A.4);*
- $k \ge -1$;
- $T \in \mathcal{T}_n$ *(Definition A.18) at* $n := 2^h$;
- $\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_{2^{k+2}}$;
- $z_1 \in \mathcal{R}_{2^{k+2}}$.

Define:

- *The coefficient norm*
  - x_p, $p<M$, *the values of* x *at the roots with positive imaginary part (Fact G.50);*
  - $w := 2^{-(k+1)}$, *its weight (Fact G.50);*
  - $\|x\| := (w\sum_{p<M}\|x_p\|^2)^{1/2}$ *at* $M := 2^{k+1}$ *(Fact G.50);*
- *The node factor*
  - l_{10}, *the factor of* ν;
  - $\widetilde{l}_{10}$, *its computed value;*
- *The node bounds*
  - $\ell := \max_\psi|l_{10}(\psi)|$;
  - $E_l := \max_\psi|\widetilde{l}_{10}(\psi) - l_{10}(\psi)|$;
  - $\widetilde{\ell} := \max_\psi|\widetilde{l}_{10}(\psi)|$;
- *The center shifts*
  - $e_{\mathrm{mul}} := \sqrt{2}\,u(2+u)$ *(Lemma B.2, item 3);*
  - $k_I(\widetilde{\ell}) := (\sqrt{2}\,\widetilde{\ell}(1+\sqrt{2}\,u(2+u)) + \sqrt{2}(3+2u))(1+u) + \sqrt{2}$ *(Lemma G.20 at* $|l_{10}| := \widetilde{\ell}$*);*
- *The centers and the samples*
  - $\widetilde{t}_1$, $\widetilde{tb}_0$, X, X_0, $\widetilde{z}_1$: *the values* ffsamp *(Algorithm 6) computes at* ν, *lines 1 to 25, at* $k \ge 0$; *at* $k=-1$, *the values* deepest *(Algorithm 7) computes at* ν, *line 9, with* $X := \widetilde{t}_0 + (\widetilde{t}_1 - \widetilde{z}_1)\widetilde{l}_{10}$ *and* $X_0 := \widetilde{t}_0 + (\widetilde{t}_1 - z_1)l_{10}$ *at* ν*'s values and* z_1 *in place of the sample over* $\mathbb{R}$.

Then the update is within the two bounds:

1. $\|\widetilde{tb}_0 - X_0\| \le E_l\|\widetilde{t}_1 - z_1\| + \widetilde{\ell}\|\widetilde{z}_1 - z_1\|$
$\quad + (1+u)(u+(1+u)e_{\mathrm{mul}})\widetilde{\ell}\|\widetilde{t}_1 - \widetilde{z}_1\| + u\|X\| + k_I(\widetilde{\ell})\zeta$;

2. $\|\widetilde{tb}_0 - X_0\| \le E_l\|\widetilde{t}_1 - \widetilde{z}_1\| + \ell\|\widetilde{z}_1 - z_1\|$
$\quad + (1+u)(u+(1+u)e_{\mathrm{mul}})\widetilde{\ell}\|\widetilde{t}_1 - \widetilde{z}_1\| + u\|X\| + k_I(\widetilde{\ell})\zeta$.

Proof.
DEFINES $K := (1+u)(u+(1+u)e_{\mathrm{mul}})\widetilde{\ell}$

Proof of item 1.

(L1) $\forall\psi:\ |\widetilde{l}_{10}(\psi)| \le \widetilde{\ell}$

[$\widetilde{\ell}$ (the statement)]

(L2) $\forall\psi:\ k_I(|\widetilde{l}_{10}(\psi)|) \le k_I(\widetilde{\ell})$

[(L1); k_I (Lemma G.20) nondecreasing in $|l_{10}|$ (Fact A.41, item 5)]

(L3) $(1+u)(1+e_{\mathrm{mul}}) - 1 = u + (1+u)e_{\mathrm{mul}}$

[expand]

(L4) $\forall\psi:\ |(\widetilde{tb}_0 - X)(\psi)| \le u|X(\psi)| + K|(\widetilde{t}_1 - \widetilde{z}_1)(\psi)| + k_I(\widetilde{\ell})\zeta$

[$\widetilde{tb}_0$, X (ffsamp (Algorithm 6), lines 23, 25, at $k \ge 0$; deepest (Algorithm 7), line 9, at $k = -1$); Lemma G.20, $\forall\psi$: its t_1, z_1, l_{10} the values $\widetilde{t}_1(\psi)$, $\widetilde{z}_1(\psi)$, $\widetilde{l}_{10}(\psi)$, its tb_0 the value $X(\psi)$; its e_0 by (L3); (L1), (L2); K (the proof's block)]

(L5) $\|\widetilde{tb}_0 - X\| \le \|(u|X(\psi)| + K|(\widetilde{t}_1 - \widetilde{z}_1)(\psi)| + k_I(\widetilde{\ell})\zeta)_\psi\|$

[(L4); $\|\cdot\|$ (the statement); $t \mapsto t^2$, $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L6) $\forall c \ge 0\ \forall x:\ \|cx\| = c\|x\|$

[$\|\cdot\|$ (the statement): the weighted root of a sum of squared moduli; Fact A.41, item 1: $|xy| = |x||y|$]

(L7) $\forall c \ge 0:\ \|(c)_\psi\| = (wM)^{1/2}c$

[$\|\cdot\|$ (the statement) on M roots (the statement), weight w]

(L8) $\|(u|X(\psi)| + K|(\widetilde{t}_1 - \widetilde{z}_1)(\psi)| + k_I(\widetilde{\ell})\zeta)_\psi\| \le u\|X\| + K\|\widetilde{t}_1 - \widetilde{z}_1\| + (wM)^{1/2}k_I(\widetilde{\ell})\zeta$

[$\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3); (L6), (L7)]

(L9) $wM = 1$

[w, M (the statement)]

(L10) $\Rightarrow\ \|\widetilde{tb}_0 - X\| \le u\|X\| + K\|\widetilde{t}_1 - \widetilde{z}_1\| + k_I(\widetilde{\ell})\zeta$

[(L5), (L8), (L9)]

(L11) $X - X_0 = (\widetilde{t}_1 - z_1)(\widetilde{l}_{10} - l_{10}) - (\widetilde{z}_1 - z_1)\widetilde{l}_{10}$

[X, X_0 (ffsamp (Algorithm 6), lines 23, 24, at $k \ge 0$; deepest (Algorithm 7), line 9, at $k = -1$): $(\widetilde{t}_1 - \widetilde{z}_1)\widetilde{l}_{10} - (\widetilde{t}_1 - z_1)l_{10}$, add and subtract $(\widetilde{t}_1 - z_1)\widetilde{l}_{10}$]

(L12) $\Rightarrow\ \|X - X_0\| \le E_l\|\widetilde{t}_1 - z_1\| + \widetilde{\ell}\|\widetilde{z}_1 - z_1\|$

[(L11); $\forall\psi:\ |\widetilde{l}_{10}(\psi) - l_{10}(\psi)| \le E_l$, $\forall\psi:\ |\widetilde{l}_{10}(\psi)| \le \widetilde{\ell}$ (E_l, $\widetilde{\ell}$, the statement); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3)]

(L13) $\Rightarrow$ item 1

[$\|\widetilde{tb}_0 - X_0\| \le \|\widetilde{tb}_0 - X\| + \|X - X_0\|$ (Fact A.41, item 3); (L10), (L12); K (the proof's block)]

□ (item 1)

Proof of item 2.

(L14) $X - X_0 = (\widetilde{t}_1 - \widetilde{z}_1)(\widetilde{l}_{10} - l_{10}) - (\widetilde{z}_1 - z_1)l_{10}$

[X, X_0 (ffsamp (Algorithm 6), lines 23, 24, at $k \ge 0$; deepest (Algorithm 7), line 9, at $k = -1$): $(\widetilde{t}_1 - \widetilde{z}_1)\widetilde{l}_{10} - (\widetilde{t}_1 - z_1)l_{10}$, add and subtract $(\widetilde{t}_1 - \widetilde{z}_1)l_{10}$]

(L15) $\Rightarrow\ \|X - X_0\| \le E_l\|\widetilde{t}_1 - \widetilde{z}_1\| + \ell\|\widetilde{z}_1 - z_1\|$

[(L14); $\forall\psi:\ |\widetilde{l}_{10}(\psi) - l_{10}(\psi)| \le E_l$, $\forall\psi:\ |l_{10}(\psi)| \le \ell$ (E_l, ℓ, the statement); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3)]

(L16) $\Rightarrow$ item 2

[$\|\widetilde{tb}_0 - X_0\| \le \|\widetilde{tb}_0 - X\| + \|X - X_0\|$ (Fact A.41, item 3); (L10), (L15); K (the proof's block)]

□ (item 2)

Lemma G.52 (The computed merge of a subtree's samples [to table])**.** *At a node, the computed merge of the right subtree's samples is within a relative part growing with the subtree's depth and an absolute part $a_{k'}$ of the merge over $\mathbb{R}$. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $m \geq 2$*;*
- $\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m$.

Define:

- $c_{\mathrm{merge}} := u + (1+u)((1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1)$ *(Lemma G.18);*
- $k_E := 2\sqrt{2}((3+2u)(1+u)+1)$ *(Lemma G.18);*
- $a_0 := 0$*;*
- $a_{j+1} := \sqrt{2}(1+c_{\mathrm{merge}})a_j + k_E\zeta$, $j \geq 0$*;*
- $\forall m' \in \{2,4,\ldots,m\}\ \forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}:\ \mathrm{lev}(T') := \log_2 m' - 1$*;*
- $k' := \mathrm{lev}(\nu)$*;*
- $z_1 := \hat{z}_{\nu,1}$*, the second component of the pair* ffSampling *(Definition A.21) returns at* ν *(items 12, 20);*
- $\widetilde{z}_1$*, the value* ffsamp *(Algorithm 6) computes at* ν*, line 21, on the same integer samples.*

Then

$$\|\widetilde{z}_1 - z_1\| \leq \left((1+c_{\mathrm{merge}})^{k'} - 1\right)\|z_1\| + a_{k'}.$$

Proof.

DEFINES $\forall T' \in \mathrm{Sub}(T):\ \hat{z}_{T'} = (\hat{z}_{T',0}, \hat{z}_{T',1})$, the pair ffSampling (Definition A.21) returns at T' (items 12, 20)
$\forall T' \in \mathrm{Sub}(T):\ \|\hat{z}_{T'}\| := (\|\hat{z}_{T',0}\|^2 + \|\hat{z}_{T',1}\|^2)^{1/2}$
$\forall T' \in \mathrm{Sub}(T):\ \Omega_{T'} := \|\widetilde{\hat{z}}_{T'} - \hat{z}_{T'}\|$
$\forall j \geq 0:\ \hat{a}_j := (1+c_{\mathrm{merge}})a_j + k_E\zeta/\sqrt{2}$

COMPUTES $\forall T' \in \mathrm{Sub}(T):\ \widetilde{\hat{z}}_{T'}$, the pair ffsamp (Algorithm 6) returns in $\mathcal{F}$ (line 20)

(L1) $\forall j:\ a_j \geq 0 \Rightarrow\ a_{j+1} \geq 0$
[$a_{j+1} = \sqrt{2}(1+c_{\mathrm{merge}})a_j + k_E\zeta$ (the statement); $c_{\mathrm{merge}}, k_E \geq 0$ (Lemma G.18), $\zeta \geq 0$ (Definition A.4)]

(L2) $\Rightarrow\ \forall j:\ a_j \geq 0$
[induction on j: $a_0 = 0$ (the statement) the base, (L1) the step]

(L3) $\forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_2:\ \Omega_{T'} = 0$
[$\widetilde{\hat{z}}_{T',i} = \hat{z}_{T',i}$, $\hat{z}_{T',i} = \hat{z}_d$, $\hat{z}_d \in \mathbb{Z} + i\mathbb{Z}$ (Definition A.21, item 4; $\mathrm{fl}(i) = i$: Definition A.4, item 5)]

(L4) $\forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_2:\ ((1+c_{\mathrm{merge}})^{\mathrm{lev}(T')} - 1)\|\hat{z}_{T'}\| + a_{\mathrm{lev}(T')} = 0$
[$\mathrm{lev}(T') = 0$, $a_0 = 0$ (the statement)]

(L5) $\forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'},\ m' \geq 4\ \forall i \in \{0,1\}:\ \|\widetilde{\hat{z}}_{T',i} - \hat{z}_{T',i}\| \leq \|\widetilde{\mathrm{merge}}(\widetilde{\hat{z}}_{T_{ii}}) - \mathrm{merge}(\widetilde{\hat{z}}_{T_{ii}})\| + \|\mathrm{merge}(\widetilde{\hat{z}}_{T_{ii}}) - \mathrm{merge}(\hat{z}_{T_{ii}})\|$
[$\hat{z}_{T',i} = \mathrm{merge}(\hat{z}_{T_{ii}})$, $\widetilde{\hat{z}}_{T',i} = \widetilde{\mathrm{merge}}(\widetilde{\hat{z}}_{T_{ii}})$ (Definition A.21, items 19, 15; ffsamp (Algorithm 6), line 21); T_{ii} the child (Definition A.18, the node); $\|x - z\| \leq \|x - y\| + \|y - z\|$ (Fact A.41, item 3)]

(L6) $\|\widetilde{\mathrm{merge}}(\widetilde{\hat{z}}_{T_{ii}}) - \mathrm{merge}(\widetilde{\hat{z}}_{T_{ii}})\| \leq c_{\mathrm{merge}}\|\mathrm{merge}(\widetilde{\hat{z}}_{T_{ii}})\| + k_E\zeta/\sqrt{2}$
[Lemma G.18 at each of the $2^{\mathrm{lev}(T_{ii})}$ butterflies of merge (Algorithm 4); Fact G.50 over the pairs of $\mathrm{merge}(\widetilde{\hat{z}}_{T_{ii}})$ at $w := 2^{-\mathrm{lev}(T')}$, $M := 2^{\mathrm{lev}(T_{ii})} = 2^{\mathrm{lev}(T')-1}$, $c := c_{\mathrm{merge}}$, $e := k_E\zeta$: $(wM)^{1/2} = 1/\sqrt{2}$]

(L7) $y \mapsto \mathrm{merge}(y)$ is $\mathbb{R}$-linear
[$\mathrm{merge}(y) = \mathrm{merge}(y)$ (merge (Algorithm 4), Postcondition; Definition A.15); Fact A.42, item 4: $\mathrm{merge}(\mathrm{split}(f)) = f$, split linear]

	Proposition G.19, item 2 at every $T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}$, $m' \geq 4$, and $i \in \{0,1\}$	This proof
	m	m'
	(g_0, g_1)	$\widetilde{\hat{z}}_{T_{ii}} - \hat{z}_{T_{ii}}$
(I1)	merge	merge (merge (Algorithm 4), Postcondition; Definition A.15)
	$m \geq 4$	(L5)
	$g_0, g_1 \in \mathcal{R}_{m/2}$	$\hat{z}_{T_{ii}}$, $\widetilde{\hat{z}}_{T_{ii}}$ (the proof's block); T_{ii} (Definition A.20, item 7)
	Its item 2: $\|\mathrm{merge}(g_0, g_1)\| = \|(g_0, g_1)\|$	

(L8) $\|\mathrm{merge}(\widetilde{\hat{z}}_{T_{ii}}) - \mathrm{merge}(\hat{z}_{T_{ii}})\| = \Omega_{T_{ii}}$

[(L7); (I1); $\Omega_{T_{ii}}$ (the proof's block)]

(L9) $\|\mathrm{merge}(\widetilde{\hat{z}}_{T_{ii}})\| \leq \|\hat{z}_{T',i}\| + \Omega_{T_{ii}}$

[(L8); $\hat{z}_{T',i} = \mathrm{merge}(\hat{z}_{T_{ii}})$ (L5); $\|X + Y\| \leq \|X\| + \|Y\|$ (Fact A.41, item 3)]

(L10) $\Rightarrow \ \|\widetilde{\hat{z}}_{T',i} - \hat{z}_{T',i}\| \leq c_{\mathrm{merge}}\|\hat{z}_{T',i}\| + (1 + c_{\mathrm{merge}})\Omega_{T_{ii}} + k_E\zeta/\sqrt{2}$

[(L5), (L6), (L8), (L9); $c_{\mathrm{merge}} \geq 0$ (Lemma G.18)]

(L11) $\Omega_{T_{ii}} \leq ((1 + c_{\mathrm{merge}})^{\mathrm{lev}(T_{ii})} - 1)\|\hat{z}_{T_{ii}}\| + a_{\mathrm{lev}(T_{ii})} \Rightarrow \ \|\widetilde{\hat{z}}_{T',i} - \hat{z}_{T',i}\| \leq c_{\mathrm{merge}}\|\hat{z}_{T',i}\| + (1 + c_{\mathrm{merge}})((1 + c_{\mathrm{merge}})^{\mathrm{lev}(T_{ii})} - 1)\|\hat{z}_{T_{ii}}\| + \hat{a}_{\mathrm{lev}(T_{ii})}$

[(L10); $1 + c_{\mathrm{merge}} \geq 0$ (Lemma G.18); $\hat{a}_j$ (the proof's block)]

	Proposition G.19, item 2 at every $T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}$, $m' \geq 4$, and $i \in \{0,1\}$	This proof
	m	m'
	(g_0, g_1)	$\hat{z}_{T_{ii}}$
(I2)	merge	merge (merge (Algorithm 4), Postcondition; Definition A.15)
	$m \geq 4$	(L5)
	$g_0, g_1 \in \mathcal{R}_{m/2}$	$\hat{z}_{T_{ii}}$ (the proof's block); T_{ii} (Definition A.20, item 7)
	Its item 2: $\|\mathrm{merge}(g_0, g_1)\| = \|(g_0, g_1)\|$	

(L12) $\|\hat{z}_{T_{ii}}\| = \|\hat{z}_{T',i}\|$

[(I2); $\hat{z}_{T',i} = \mathrm{merge}(\hat{z}_{T_{ii}})$ (L5)]

(L13) $\forall c \geq 0 \ \forall j \geq 0 : \ c + (1 + c)((1 + c)^j - 1) = (1 + c)^{j+1} - 1$

[expand]

(L14) $\Rightarrow \ \|\widetilde{\hat{z}}_{T',i} - \hat{z}_{T',i}\| \leq ((1 + c_{\mathrm{merge}})^{\mathrm{lev}(T_{ii})+1} - 1)\|\hat{z}_{T',i}\| + \hat{a}_{\mathrm{lev}(T_{ii})}$

[(L11), (L12); (L13) at $c := c_{\mathrm{merge}}$]

(L15) $\mathrm{lev}(T_{00}) = \mathrm{lev}(T') - 1$

[$\mathrm{lev}(T')$ (the statement); $T_{00} \in \mathcal{T}_{m'/2}$ (Definition A.18, the node)]

(L16) $\mathrm{lev}(T_{11}) = \mathrm{lev}(T') - 1$

[$\mathrm{lev}(T')$ (the statement); $T_{11} \in \mathcal{T}_{m'/2}$ (Definition A.18, the node)]

(L17) $\forall A \geq 0 : \ \|(A, A)\| = \sqrt{2}\, A$

[$\|\hat{z}_{T'}\|$ (the proof's block) at $\|\hat{z}_{T',0}\| = \|\hat{z}_{T',1}\|$, $\|\hat{z}_{T',1}\| = A$]

(L18) $\Rightarrow \ \Omega_{T'} \leq ((1 + c_{\mathrm{merge}})^{\mathrm{lev}(T')} - 1)\|\hat{z}_{T'}\| + \sqrt{2}\, \hat{a}_{\mathrm{lev}(T')-1}$

[(L14) at $i = 0, 1$, (L15), (L16); $\|(x_0, x_1) + (y_0, y_1)\| \leq \|(x_0, x_1)\| + \|(y_0, y_1)\|$ (Fact A.41, item 3) at $y_0 = y_1$, $y_1 = \hat{a}_{\mathrm{lev}(T')-1}$; (L17); $\Omega_{T'}$, $\|\hat{z}_{T'}\|$ (the proof's block)]

(L19) $\forall j \geq 1 : \ a_j = \sqrt{2}((1 + c_{\mathrm{merge}})a_{j-1} + k_E\zeta/\sqrt{2})$

[a_j (the statement); expand]

(L20) $\forall j \geq 1 : \ \sqrt{2}\, \hat{a}_{j-1} = a_j$

[$\hat{a}_{j-1}$ (the proof's block); (L19)]

(L21) $\Rightarrow \ \forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}, \ m' \geq 4 : \ (\forall i : \ \Omega_{T_{ii}} \leq ((1 + c_{\mathrm{merge}})^{\mathrm{lev}(T')-1} - 1)\|\hat{z}_{T_{ii}}\| + a_{\mathrm{lev}(T')-1}) \Rightarrow$

$\Omega_{T'} \le ((1+c_{\text{merge}})^{\text{lev}(T')}-1)\|\hat{z}_{T'}\| + a_{\text{lev}(T')}$

[(L11) to (L20): the step from $\text{lev}(T')-1$ to $\text{lev}(T')$]

(L22) $\Rightarrow$ $\forall m' \in \{2,4,\dots,m\}\ \forall T' \in \text{Sub}(T)\cap\mathcal{T}_{m'}:\ \Omega_{T'} \le ((1+c_{\text{merge}})^{\text{lev}(T')}-1)\|\hat{z}_{T'}\| + a_{\text{lev}(T')}$

[induction on $\text{lev}(T')$: (L3), (L4) the base at $\text{lev}(T')=0$, (L21) the step]

(L23) $k' \ge 1 \Rightarrow \|\widetilde{z}_1 - z_1\| \le ((1+c_{\text{merge}})^{k'}-1)\|z_1\| + \hat{a}_{k'-1}$

[(L11) at $T' := \nu$, $i=1$, its antecedent by (L22) at $T' := T_{11}$; (L14) at $T' := \nu$, $i=1$: $z_1 = \hat{z}_{\nu,1}$, $\widetilde{z}_1 = \widetilde{\hat{z}}_{\nu,1}$ (the statement); $k' = \text{lev}(\nu)$, $\text{lev}(\nu) = \text{lev}(T_{11})+1$ (the statement; (L16))]

(L24) $\forall k' \ge 1:\ \hat{a}_{k'-1} = a_{k'}/\sqrt{2}$

[(L20)]

(L25) $\forall k' \ge 1:\ a_{k'}/\sqrt{2} \le a_{k'}$

[(L2); $\sqrt{2} \ge 1$]

(L26) $k' = 0 \Rightarrow \|\widetilde{z}_1 - z_1\| = 0$

[$k'=0$: $\nu \in \mathcal{T}_2$, $T_{11} = d_{11}$ (the statement; Definition A.18): $\widetilde{z}_1 = z_1$, $z_1 = \hat{z}_{d_{11}}$, $\hat{z}_{d_{11}} \in \mathbb{Z}+i\mathbb{Z}$ (Definition A.21, item 4; $\text{fl}(i) = i$: Definition A.4, item 5)]

(L27) $((1+c_{\text{merge}})^0 - 1)\|z_1\| + a_0 = 0$

[$a_0 = 0$ (the statement)]

(L28) $\Rightarrow$ the statement

[(L23), (L24), (L25) at $k' \ge 1$; (L26), (L27) at $k' = 0$]

□

Lemma G.53 (A node's entry shifts [to table])**.** *At a node, the two entry shifts are the split's own perturbations, the left one plus the update's. Let:*

- $h \ge 1$;
- $\mathcal{F}$ *be a realization at* (u,ζ) *(Definition A.4);*
- $k \ge -1$;
- $T \in \mathcal{T}_n$ *(Definition A.18) at* $n := 2^h$;
- $\nu \in \text{Sub}(T) \cap \mathcal{T}_{2^{k+2}}$;
- $z_1 \in \mathcal{R}_{2^{k+2}}$.

Define:

- $\widetilde{t}_\nu := (\widetilde{t}_0, \widetilde{t}_1)$*, the computed input at* ν *(*ffsamp *(Algorithm 6), line 1, at* $k \ge 0$*; the input of* deepest *(Algorithm 7) at* $k = -1$*);*
- $\widetilde{\psi} \in C_{\mathcal{F}}$*, the stored value of the root* ψ *of each pair* $(\psi, -\psi)$ *of* ν*'s ring, with* $\exists\, u_\circ \in \mathbb{C},\ |u_\circ| \le u + \sqrt{2}\,\zeta:\ \widetilde{\psi} = \psi(1+u_\circ)$ *(Definition A.8, item 1);*
- $c_{\text{split}} := (1+u)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1$ *(Lemma G.16);*
- $k_B := \sqrt{2}(3+2u)$ *(Lemma G.16);*
- $k_D := (\sqrt{2}/2)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) + k_B$ *(Lemma G.16);*
- $k_{\text{split}} := \sqrt{2}/2 + k_D$.

Define, at $k \ge 0$*, as the values* ffsamp *(Algorithm 6) computes at* ν*, lines 1 to 32, with* z_1 *in place of the sample over* $\mathbb{R}$*:*

- f_ν^R;
- $f_\nu^{\mathcal{L}}$;
- $\widetilde{tb}_0$;
- X_0.

Define, at $k = -1$ *(a leaf node):*

- $f_\nu^R := 0$ *at* $k = -1$;
- $\widetilde{tb}_0$*, the value* deepest *(Algorithm 7) computes at* ν*, line 9;*
- $X_0 := \widetilde{t}_0 + (\widetilde{t}_1 - z_1)l_{10}$ *at* ν*'s values;*
- $f_\nu^{\mathcal{L}} := \widetilde{tb}_0 - X_0$ *at* $k = -1$.

Then the right entry shift is the split's perturbation of $\widetilde{t}_1$*, and the left one adds the update's:*

1. $\|f_\nu^R\| \le c_{\text{split}}\|\widetilde{t}_1\| + k_{\text{split}}\zeta$;

2. $\|f_\nu^{\mathcal{L}}\| \le c_{\text{split}}\|\widetilde{tb}_0\| + k_{\text{split}}\zeta + \|\widetilde{tb}_0 - X_0\|$.

Proof. *Proof of item 1.*

(L1) $\forall \widetilde{x}, x: \ \|\text{split}(\widetilde{x}) - \text{split}(x)\| = \|\text{split}(\widetilde{x} - x)\|$
[split(f) = split(f) (split (Algorithm 2), Postcondition; Fact A.42, item 5); Fact A.42, item 4, at $c := -1$]

(L2) $\forall \widetilde{x}, x: \ \|\text{split}(\widetilde{x} - x)\| = \|\widetilde{x} - x\|$
[Proposition G.19, item 1]

(L3) $\forall \widetilde{x}, x: \ \|\widetilde{\text{split}}(\widetilde{x}) - \text{split}(x)\| \le \|\widetilde{\text{split}}(\widetilde{x}) - \text{split}(\widetilde{x})\| + \|\widetilde{x} - x\|$
[$\|a+b\| \le \|a\| + \|b\|$ (Fact A.41, item 3); (L1), (L2)]

(L4) $k \ge 0 \Rightarrow \ \|f_\nu^R\| = \|\widetilde{\text{split}}(\widetilde{t}_1) - \text{split}(\widetilde{t}_1)\|$
[f_ν^R (ffsamp (Algorithm 6), line 18)]

Lemma G.17 at $k \ge 0$, each $\widetilde{x} \in \{\widetilde{t}_1, \widetilde{tb}_0\}$ and each of the 2^k pairs $(\psi, -\psi)$ of ν's ring, $\widetilde{\psi}$ its stored root	This proof
Shared: $\mathcal{F}, (u, \zeta), \ \psi, \widetilde{\psi}, \ c_{\text{split}}, k_B, k_D$	
(a, b)	$(\widetilde{x}(\psi), \widetilde{x}(-\psi))$
(I1) $a, b \in C_{\mathcal{F}}$	$\widetilde{t}_\nu$, $\widetilde{tb}_0$ (the statement)
$\psi \in \mathbb{C}$	$\psi^{2^{k+2}} = -1$ (Fact A.43, item 1)
$\widetilde{\psi} \in C_{\mathcal{F}}$	$\widetilde{\psi}$ (the statement)
Assumption A1	Fact A.42, item 1
Assumption A2	$\widetilde{\psi}$ (the statement); Definition A.10
Its conclusion: $(\tilde{f}_0, \tilde{f}_1) \ \mathcal{N}\left(c_{\text{split}}, (\sqrt{2}/2 + k_D)\zeta\right) \ (f_0, f_1)$	

(L5) $k \ge 0 \Rightarrow \ \forall \widetilde{x} \in \{\widetilde{t}_1, \widetilde{tb}_0\}: \ \|\widetilde{\text{split}}(\widetilde{x}) - \text{split}(\widetilde{x})\| \le c_{\text{split}}\|\text{split}(\widetilde{x})\| + k_{\text{split}}\zeta$
[(I1); Fact G.50 at $w := 2^{-k}$, $M := 2^k$, $c := c_{\text{split}}$, $e := k_{\text{split}}\zeta$]

(L6) $k = -1 \Rightarrow \ \|f_\nu^R\| = 0$
[$f_\nu^R := 0$ (the statement)]

(L7) $0 \le c_{\text{split}}\|\widetilde{t}_1\| + k_{\text{split}}\zeta$
[$c_{\text{split}} \ge 0$ at $u, \zeta \ge 0$ (c_{split}, Lemma G.16, and u, ζ, Definition A.4); $k_{\text{split}} > 0$ (k_{split}, the statement, with k_D, Lemma G.16, at $u, \zeta \ge 0$); $\|\cdot\| \ge 0$ (Fact A.41, item 3)]

Proposition G.19, item 1 at $k \ge 0$	This proof
m	2^{k+2}
f	$\widetilde{t}_1$
(I2) split	split (split (Algorithm 2), Postcondition; Fact A.42, item 5)
$m \ge 4$	$k \ge 0$ (the scope)
$f \in \mathcal{R}_m$	$\widetilde{t}_\nu$ (the statement)
Its item 1: $\|\text{split}(f)\| = \|f\|$	

(L8) $\Rightarrow$ item 1
[(L4); (L5) at $\widetilde{x} := \widetilde{t}_1$; (I2), at $k \ge 0$; (L6), (L7) at $k = -1$]

□ (item 1)

Proof of item 2.

(L9) $k \ge 0 \Rightarrow \ \|\widetilde{\text{split}}(\widetilde{tb}_0) - \text{split}(\widetilde{tb}_0)\| \le c_{\text{split}}\|\widetilde{tb}_0\| + k_{\text{split}}\zeta$
[(L5) at $\widetilde{x} := \widetilde{tb}_0$; $\|\text{split}(\widetilde{tb}_0)\| = \|\widetilde{tb}_0\|$ (Proposition G.19, item 1)]

(L10) $k = -1 \Rightarrow \ \|f_\nu^{\mathcal{L}}\| = \|\widetilde{tb}_0 - X_0\|$
[$f_\nu^{\mathcal{L}} := \widetilde{tb}_0 - X_0$ (the statement)]

(L11) $\|\widetilde{tb}_0 - X_0\| \le c_{\text{split}}\|\widetilde{tb}_0\| + k_{\text{split}}\zeta + \|\widetilde{tb}_0 - X_0\|$
[$c_{\text{split}} \ge 0$ at $u, \zeta \ge 0$ (c_{split}, Lemma G.16, and u, ζ, Definition A.4); $k_{\text{split}} > 0$ (k_{split}, the statement, with k_D, Lemma G.16, at $u, \zeta \ge 0$); $\|\cdot\| \ge 0$ (Fact A.41, item 3)]

(L12) $\Rightarrow$ item 2

[$f^{\mathcal{L}}_{\nu}$ (ffsamp (Algorithm 6), line 32); (L3) at $\widetilde{x} := \widetilde{tb}_0$, $x := X_0$; (L9), at $k \geq 0$; (L10), (L11) at $k = -1$]

□ (item 2)

Lemma G.54 (The shift is the sum of the entry shifts [to table])**.** *The shift of the leaf centers is the root's entry shift through the tree map plus every node's entry shifts through its children's tree maps. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $t \in \mathcal{R}_n \times \mathcal{R}_n$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*.*

Define, at each $T' \in \mathrm{Sub}(T)$ *and each* $\nu \in \mathrm{Sub}(T) \setminus \mathbb{R}$*:*

- *The tree*
  - $\mathrm{Sub}(T')$*, the subtrees of* T' *(Definition A.18);*
  - $\mathcal{N}(T') := \mathrm{Sub}(T') \setminus \mathbb{R}$*;*
- *The tree map*
  - $\mathcal{L}_{T'}$*, the tree map (Definition G.6) at* T'*;*
  - $\mathcal{L}_{R(\nu)}$ *and* $\mathcal{L}_{L(\nu)}$*, the tree maps (Definition G.6) at* $R(\nu)$ *and at* $L(\nu)$ *(Definition A.18);*
- *The centers and the samples*
  - $t_{T'}$*, the entry of the call at* T' *over* $\mathbb{R}$ *(Definition A.21, items 5, 13, 17 at a node, items 7, 10 at a leaf diagonal);*
  - $\widetilde{t}_{T'}$*, the computed entry of the call at* T' *(ffsamp (Algorithm 6), line 1, at a node; at a leaf diagonal, the center* deepest *(Algorithm 7) passes to the base sampler at* T'*, lines 1 to 18);*
  - $\widetilde{tb}_{0,\nu}$*, at a leaf node* $\nu \in \mathcal{T}_2$*, the value* deepest *(Algorithm 7) computes at* ν*, line 9;*
  - $X_{0,\nu} := \widetilde{t}_0 + (\widetilde{t}_1 - z_1)l_{10}$ *at a leaf node* $\nu \in \mathcal{T}_2$*, at* ν*'s values, the expression of line 24 of* ffsamp *(Algorithm 6);*
  - $\Delta := (\widetilde{t}_i - t_i)_{i \leq N}$*:* $\widetilde{t}_i$ *the center* $\mathrm{ffSampling}^{\mathcal{F}}$ *passes to the base sampler at position* i *(*deepest *(Algorithm 7), lines 1 to 18),* t_i *the center* $\mathrm{ffSampling}(t, T)$ *sets there over* $\mathbb{R}$ *(Definition A.21, item 2);*
  - $e_{\mathrm{root}} := \widetilde{t}_T - t$*, with* $\widetilde{t}_T$ *the root node's call's input (*ffsamp *(Algorithm 6), line 1 at* $\nu = T$*);*
- *The entry shifts*
  - f^R_{ν}*, at a node* ν *of degree* $m \geq 4$*, the value* ffsamp *(Algorithm 6) computes at* ν*, line 18;*
  - $f^{\mathcal{L}}_{\nu}$*, at a node* ν *of degree* $m \geq 4$*, the value* ffsamp *(Algorithm 6) computes at* ν*, line 32;*
  - $f^R_{\nu} := 0$ *at a leaf node* $\nu \in \mathcal{T}_2$*;*
  - $f^{\mathcal{L}}_{\nu} := \widetilde{tb}_{0,\nu} - X_{0,\nu}$ *at a leaf node* $\nu \in \mathcal{T}_2$*.*

Then the shift at every subtree is its entry's shift through its tree map plus its nodes' entry shifts, and at the root:

1. $\forall T' \in \mathrm{Sub}(T) : \ (\widetilde{t}_i - t_i)_{i \in I(T')} = (\widetilde{t}_{T'} - t_{T'})\mathcal{L}_{T'} + \sum_{\nu' \in \mathcal{N}(T')} (f^R_{\nu'}\mathcal{L}_{R(\nu')} + f^{\mathcal{L}}_{\nu'}\mathcal{L}_{L(\nu')})$;
2. $\Delta = e_{\mathrm{root}}\mathcal{L}_T + \sum_{\nu \in \mathcal{N}(T)} \left(f^R_{\nu}\mathcal{L}_{R(\nu)} + f^{\mathcal{L}}_{\nu}\mathcal{L}_{L(\nu)} \right)$.

Proof. Proof of item 1.

COMPUTES $X_{0,\nu}$, $\nu \in \mathcal{N}(T) \cap \mathcal{T}_m$, $m \geq 4$ (ffsamp (Algorithm 6), line 24)

(L1) $\forall \nu \in \mathrm{Sub}(T) \ \forall e : \ (c(t_\nu + e, z) - c(t_\nu, z))_{I(\nu)} = e\mathcal{L}_\nu$

[Lemma G.49]

(L2) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_m, \ m \geq 4 : \ \widetilde{t}_{R(\nu)} = \mathrm{split}(\widetilde{t}_1) + f^R_{\nu}$

[ffsamp (Algorithm 6), line 18: $\widetilde{\mathrm{split}}(x) = \mathrm{split}(x) + f$ at the right entry]

(L3) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_m,\ m \geq 4 :\ \widetilde{t}_{L(\nu)} = \mathrm{split}(X_{0,\nu}) + f^{\mathcal{L}}_{\nu}$

[ffsamp (Algorithm 6), line 32: $\widetilde{\mathrm{split}}(x) = \mathrm{split}(x) + f$ at the left entry]

(L4) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_m,\ m \geq 4 :\ t_{R(\nu)} = \mathrm{split}(t_1)$

[Definition A.21, item 13]

(L5) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_m,\ m \geq 4 :\ t_{L(\nu)} = \mathrm{split}(tb_{0,\nu})$

[Definition A.21, item 17]

(L6) $X_{0,\nu} - tb_{0,\nu} = ((\widetilde{t}_\nu - t_\nu)L_\nu)_0$

[Definition A.21, item 16, and ffsamp (Algorithm 6), line 24, at $m \geq 4$; Definition A.21, item 9, and $X_{0,\nu}$ (the statement) at $m = 2$; Definition G.6, the node factor]

(L7) $\Rightarrow\ \forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_m,\ m \geq 4 :\ \mathrm{split}(\widetilde{t}_1) - t_{R(\nu)} = \mathrm{split}(((\widetilde{t}_\nu - t_\nu)L_\nu)_1)$

[(L4); Fact A.42, item 4; $((\widetilde{t}_\nu - t_\nu)L_\nu)_1 = \widetilde{t}_1 - t_1$ (Definition G.6, the node factor)]

(L8) $\Rightarrow\ \forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_m,\ m \geq 4 :\ \mathrm{split}(X_{0,\nu}) - t_{L(\nu)} = \mathrm{split}(((\widetilde{t}_\nu - t_\nu)L_\nu)_0)$

[(L5), (L6); Fact A.42, item 4]

(L9) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_2 :\ \widetilde{t}_{R(\nu)} = \widetilde{t}_1$

[deepest (Algorithm 7), the right leaf's center, lines 1 to 18]

(L10) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_2 :\ t_{R(\nu)} = t_1$

[Definition A.21, item 7]

(L11) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_2 :\ \widetilde{t}_{L(\nu)} = \widetilde{tb}_{0,\nu}$

[deepest (Algorithm 7), the left leaf's center, line 9; $\widetilde{tb}_{0,\nu}$ (the statement)]

(L12) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_2 :\ t_{L(\nu)} = tb_{0,\nu}$

[Definition A.21, items 9, 10]

(L13) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_2 :\ \widetilde{t}_{R(\nu)} - t_{R(\nu)} = ((\widetilde{t}_\nu - t_\nu)L_\nu)_1 + f^R_\nu$

[(L9), (L10); $f^R_\nu := 0$ (the statement); $xL_\nu = (x_0 + x_1 l_{10},\ x_1)$ (Definition G.6, the node factor) at $x := \widetilde{t}_\nu - t_\nu$]

(L14) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_2 :\ \widetilde{t}_{L(\nu)} - t_{L(\nu)} = ((\widetilde{t}_\nu - t_\nu)L_\nu)_0 + f^{\mathcal{L}}_\nu$

[(L11), (L12), (L6); $f^{\mathcal{L}}_\nu := \widetilde{tb}_{0,\nu} - X_{0,\nu}$ (the statement)]

(L15) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_m,\ m \geq 4 :\ \widetilde{t}_{R(\nu)} - t_{R(\nu)} = \mathrm{split}(((\widetilde{t}_\nu - t_\nu)L_\nu)_1) + f^R_\nu$

[(L2), (L7)]

(L16) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_m,\ m \geq 4 :\ \widetilde{t}_{L(\nu)} - t_{L(\nu)} = \mathrm{split}(((\widetilde{t}_\nu - t_\nu)L_\nu)_0) + f^{\mathcal{L}}_\nu$

[(L3), (L8)]

(L17) $\forall m \geq 4\ \forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_m :\ x\mathcal{L}_\nu = (\mathrm{split}((xL_\nu)_1)\mathcal{L}_{R(\nu)},\ \mathrm{split}((xL_\nu)_0)\mathcal{L}_{L(\nu)})$

[Definition G.6]

(L18) $\forall \nu \in \mathcal{N}(T) \cap \mathcal{T}_2 :\ x\mathcal{L}_\nu = ((xL_\nu)_1,\ (xL_\nu)_0)$

[Definition G.6]

(L19) $\forall \nu \in \mathcal{N}(T) :$

$$\Big[\forall T' \in \{L(\nu), R(\nu)\} :\ (\widetilde{t}_i - t_i)_{i \in I(T')} = (\widetilde{t}_{T'} - t_{T'})\mathcal{L}_{T'} + \sum_{\nu' \in \mathcal{N}(T')} (f^R_{\nu'}\mathcal{L}_{R(\nu')} + f^{\mathcal{L}}_{\nu'}\mathcal{L}_{L(\nu')})\Big] \Rightarrow$$

$$(\widetilde{t}_i - t_i)_{i \in I(\nu)} = (\widetilde{t}_\nu - t_\nu)\mathcal{L}_\nu + \sum_{\nu' \in \mathcal{N}(\nu)} (f^R_{\nu'}\mathcal{L}_{R(\nu')} + f^{\mathcal{L}}_{\nu'}\mathcal{L}_{L(\nu')})$$

[(L13) to (L18); (L1) at $R(\nu)$ with $e := f^R_\nu$ and at $L(\nu)$ with $e := f^{\mathcal{L}}_\nu$; the bracket at $T' := R(\nu)$ and at $T' := L(\nu)$; $I(\nu) = I(R(\nu)) \sqcup I(L(\nu))$ (Definition A.19)]

(L20) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R} :$

$$(\widetilde{t}_i - t_i)_{i \in I(d)} = (\widetilde{t}_d - t_d)\mathcal{L}_d + \sum_{\nu' \in \mathcal{N}(d)} (f^R_{\nu'}\mathcal{L}_{R(\nu')} + f^{\mathcal{L}}_{\nu'}\mathcal{L}_{L(\nu')})$$

[$\mathcal{N}(d) = \mathrm{Sub}(d) \setminus \mathbb{R}$, $\mathrm{Sub}(d) \setminus \mathbb{R} = \emptyset$ (the statement; Definition A.18); $x\mathcal{L}_d = x$ (Definition G.6) and the real coordinates (Definition G.6)]

(L21) $\Rightarrow$ $\forall T' \in \mathrm{Sub}(T)$:

$$(\widetilde{t}_i - t_i)_{i \in I(T')} = (\widetilde{t}_{T'} - t_{T'})\mathcal{L}_{T'} + \sum_{\nu' \in \mathcal{N}(T')} (f^R_{\nu'}\mathcal{L}_{R(\nu')} + f^{\mathcal{L}}_{\nu'}\mathcal{L}_{L(\nu')})$$

[induction on the depth from the leaves: (L20) the base at a leaf diagonal, (L19) the step at a node]

(L22) $\Rightarrow$ item 1

[(L21)]

□ (item 1)

Proof of item 2.

(L23) $\Delta = e_{\mathrm{root}}\mathcal{L}_T + \sum_{\nu \in \mathcal{N}(T)} \left(f^R_\nu \mathcal{L}_{R(\nu)} + f^{\mathcal{L}}_\nu \mathcal{L}_{L(\nu)} \right)$

[(L21) at $T' = T$; $\widetilde{t}_T - t_T = e_{\mathrm{root}}$ (the statement; $t_T = t$); $\Delta = (\widetilde{t}_i - t_i)_{i \le N}$ (the statement)]

(L24) $\Rightarrow$ item 2

[(L23)]

□ (item 2)

Lemma G.55 (The shift's norm bound [to table])**.** *The shift is at most the root's perturbation through the tree map plus each depth's entry shifts through its operator norm. Let:*

- $h \ge 1$;
- $T \in \mathcal{T}_n$ *(Definition A.18) at* $n := 2^h$;
- $t \in \mathcal{R}_n \times \mathcal{R}_n$;
- $z \in \mathbb{Z}^N$ *at* $N := 2n$.

Define:

- *The tree map*
  - $\mathcal{L}_\nu$, *the tree map at* ν *(Definition G.6);*
- *The key constants*
  - $\Xi'_k := \max_{\mathrm{depth}(\nu)=k} \|\mathcal{L}_\nu\|$ *(Definition 4.6, item 8, at* T*);*
  - $\Xi'_{\mathrm{root}} := \|\mathcal{L}_T\|$ *(Definition 4.6, item 10, at* T*);*
- *The centers and the samples*
  - $\Delta := (\widetilde{t}_i - t_i)_{i \le N}$: $\widetilde{t}_i$ *the center* $\mathrm{ffSampling}^{\mathcal{F}}$ *passes to the base sampler at position* i *(*deepest *(Algorithm 7), lines 1 to 18),* t_i *the center* $\mathrm{ffSampling}(t, T)$ *sets there over* $\mathbb{R}$ *(Definition A.21, item 2);*
  - $\widetilde{t}_\nu$, $\nu \in \mathrm{Sub}(T)$, *the computed entry at* ν *(*ffsamp *(Algorithm 6), line 1);*
  - $e_{\mathrm{root}} := \widetilde{t}_T - t$;
  - $X_{0,\nu} := \widetilde{t}_0 + (\widetilde{t}_1 - z_1)l_{10}$ *at the leaf node's values (Lemma G.54);*
  - $\widetilde{tb}_{0,\nu}$, *the value* deepest *(Algorithm 7) computes at* ν*, line 9 (Lemma G.54);*
- *The entry shifts*
  - f^R_ν *for* $m \ge 4$, ffsamp *(Algorithm 6), line 18, at the node* ν *(Lemma G.54);*
  - $f^R_\nu := 0$ *for* $m := 2$*, at a leaf node* $\nu \in \mathcal{T}_2$ *(Lemma G.54);*
  - $f_{R(\nu)} := f^R_\nu$, $\nu \in \mathrm{Sub}(T) \setminus \mathbb{R}$ *(Lemma G.54);*
  - $f^{\mathcal{L}}_\nu$ *for* $m \ge 4$, ffsamp *(Algorithm 6), line 32, at the node* ν *(Lemma G.54);*
  - $f^{\mathcal{L}}_\nu := \widetilde{tb}_{0,\nu} - X_{0,\nu}$ *for* $m := 2$*, at a leaf node* $\nu \in \mathcal{T}_2$ *(Lemma G.54);*
  - $f_{L(\nu)} := f^{\mathcal{L}}_\nu$, $\nu \in \mathrm{Sub}(T) \setminus \mathbb{R}$ *(Lemma G.54);*
  - $\mathfrak{f}_k := \left(\sum_{\mathrm{depth}(\nu)=k} \|f_\nu\|^2 \right)^{1/2}$, $k \ge 1$.

Then

$$\|\Delta\| \le \Xi'_{\mathrm{root}} \|e_{\mathrm{root}}\| + \sum_{k=1}^{h} \Xi'_k \mathfrak{f}_k.$$

Proof. (L1) $\forall k\ \forall \nu \ne \nu',\ \mathrm{depth}(\nu) = \mathrm{depth}(\nu') = k :\ I(\nu) \cap I(\nu') = \emptyset$

[Definition A.19]

(L2) $\Rightarrow$ $\forall k:\ \left\|\sum_{\mathrm{depth}(\nu)=k} f_\nu \mathcal{L}_\nu\right\|^2 = \sum_{\mathrm{depth}(\nu)=k} \|f_\nu \mathcal{L}_\nu\|^2$

[(L1); $(f_\nu \mathcal{L}_\nu)_i = 0$ at $i \notin I(\nu)$ (Definition G.6); $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead)]

(L3) $\forall \nu:\ \|f_\nu \mathcal{L}_\nu\| \le \|\mathcal{L}_\nu\| \|f_\nu\|$

[the operator norm (Definition 4.6, item 7, at T)]

(L4) $\forall \nu,\ \mathrm{depth}(\nu) = k:\ \|\mathcal{L}_\nu\| \|f_\nu\| \le \Xi'_k \|f_\nu\|$

[Ξ'_k (the statement)]

(L5) $\Rightarrow$ $\forall k:\ \left\|\sum_{\mathrm{depth}(\nu)=k} f_\nu \mathcal{L}_\nu\right\|^2 \le \Xi'^2_k \mathfrak{f}^2_k$

[(L2), (L3), (L4); $\mathfrak{f}_k$ (the statement)]

(L6) $\Rightarrow$ the statement

[Lemma G.54, item 2; (L5); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3) over the depths]

□

Lemma G.56 (The computed entries at a depth [to table])**.** *Each depth's computed entries are within Ξ_k times the shift and the deeper depths' entry shifts of the ones over $\mathbb{R}$. Let:*

- $h \ge 1$;
- $T \in \mathcal{T}_n$ *(Definition A.18) at* $n := 2^h$;
- $t \in \mathcal{R}_n \times \mathcal{R}_n$;
- $z \in \mathbb{Z}^N$ *at* $N := 2n$;
- $k \in \{1, \dots, h-1\}$.

Define:

- *The tree map*
  - $\mathcal{L}_\nu$, *the tree map at* ν *(Definition G.6);*
- *The key constants*
  - $\Xi'_j := \max_{\mathrm{depth}(\nu)=j} \|\mathcal{L}_\nu\|$ *(Definition 4.6, item 8, at* T*);*
  - Ξ_k, *that of Definition 4.6, item 9, at* T*;*
- *The centers and the samples*
  - $\Delta := (\widetilde{t}_i - t_i)_{i \le N}$: $\widetilde{t}_i$ *the center* $\mathrm{ffSampling}^{\mathcal{F}}$ *passes to the base sampler at position* i *(*deepest *(Algorithm 7), lines 1 to 18),* t_i *the center* $\mathrm{ffSampling}(t, T)$ *sets there over* $\mathbb{R}$ *(Definition A.21, item 2);*
  - $\widetilde{t}_\nu$, $\nu \in \mathrm{Sub}(T)$, *the computed entry at* ν *(*ffsamp *(Algorithm 6), line 1);*
  - $X_{0,\nu} := \widetilde{t}_0 + (\widetilde{t}_1 - z_1) l_{10}$ *at the leaf node's values (Lemma G.54);*
  - $\widetilde{tb}_{0,\nu}$, *the value* deepest *(Algorithm 7) computes at* ν, *line 9 (Lemma G.54);*
- *The entry shifts*
  - f^R_ν *for* $m \ge 4$, ffsamp *(Algorithm 6), line 18, at the node* ν *(Lemma G.54);*
  - $f^R_\nu := 0$ *for* $m := 2$, *at a leaf node* $\nu \in \mathcal{T}_2$ *(Lemma G.54);*
  - $f_{R(\nu)} := f^R_\nu$, $\nu \in \mathrm{Sub}(T) \setminus \mathbb{R}$ *(Lemma G.54);*
  - $f^{\mathcal{L}}_\nu$ *for* $m \ge 4$, ffsamp *(Algorithm 6), line 32, at the node* ν *(Lemma G.54);*
  - $f^{\mathcal{L}}_\nu := \widetilde{tb}_{0,\nu} - X_{0,\nu}$ *for* $m := 2$, *at a leaf node* $\nu \in \mathcal{T}_2$ *(Lemma G.54);*
  - $f_{L(\nu)} := f^{\mathcal{L}}_\nu$, $\nu \in \mathrm{Sub}(T) \setminus \mathbb{R}$ *(Lemma G.54);*
  - $\mathfrak{f}_k := \left(\sum_{\mathrm{depth}(\nu)=k} \|f_\nu\|^2\right)^{1/2}$, $k \ge 1$.

Then

$$\|(\widetilde{t}_\nu - t_\nu)_{\mathrm{depth}(\nu)=k}\| \le \Xi_k \left(\|\Delta\| + \sum_{j=1}^{h} \Xi'_j \mathfrak{f}_j \right).$$

Proof.

DEFINES $I(\nu)$, the positions of ν (Definition A.19)

DEFINES $\mathcal{N}(\nu) = \mathrm{Sub}(\nu) \setminus \mathbb{R}$

Lemma G.54, item 1 at every ν with $\mathrm{depth}(\nu)=k$	This proof
Shared: $T, t, z,\ N,\ \widetilde{t}_i, t_i,\ f^R_{\nu'}, f^{\mathcal{L}}_{\nu'}$	
(I1) Shared: $T \in \mathcal{T}_n,\ t \in \mathcal{R}_n \times \mathcal{R}_n,\ z \in \mathbb{Z}^N$	
T'	ν
$T' \in \mathrm{Sub}(T)$	ν (the scope); Definition A.18
Its item 1: $\forall T' \in \mathrm{Sub}(T):\ (\widetilde{t}_i - t_i)_{i\in I(T')} = (\widetilde{t}_{T'} - t_{T'})\mathcal{L}_{T'} + \sum_{\nu'\in\mathcal{N}(T')}(f^R_{\nu'}\mathcal{L}_{R(\nu')} + f^{\mathcal{L}}_{\nu'}\mathcal{L}_{L(\nu')})$	

(L1) $\forall \nu,\ \mathrm{depth}(\nu)=k:\ (\widetilde{t}_\nu - t_\nu)\mathcal{L}_\nu = (\widetilde{t}_i - t_i)_{i\in I(\nu)} - \sum_{\nu'\in\mathcal{N}(\nu)}(f^R_{\nu'}\mathcal{L}_{R(\nu')} + f^{\mathcal{L}}_{\nu'}\mathcal{L}_{L(\nu')})$

[(I1)]

(L2) $\forall \nu:\ \mathrm{Sub}(\nu)\setminus\{\nu\} = \{R(\nu'),\ L(\nu') : \nu' \in \mathcal{N}(\nu)\}$

[Definition A.18, the subtrees]

(L3) $\forall \nu,\ \mathrm{depth}(\nu)=k\ \forall \nu'' \in \mathrm{Sub}(\nu)\setminus\{\nu\}:\ \mathrm{depth}(\nu'') > k$

[Definition A.18, the depth]

(L4) $\forall \nu,\ \mathrm{depth}(\nu)=k:\ \sum_{\nu'\in\mathcal{N}(\nu)}(f^R_{\nu'}\mathcal{L}_{R(\nu')} + f^{\mathcal{L}}_{\nu'}\mathcal{L}_{L(\nu')}) = \sum_{j=k+1}^{h} \sum_{\substack{\nu''\in\mathrm{Sub}(\nu)\\ \mathrm{depth}(\nu'')=j}} f_{\nu''}\mathcal{L}_{\nu''}$

[$f_{R(\nu')} := f^R_{\nu'}$, $f_{L(\nu')} := f^{\mathcal{L}}_{\nu'}$ (the statement); (L2), (L3)]

(L5) $\forall \nu,\ \mathrm{depth}(\nu)=k:\ \|(\widetilde{t}_\nu - t_\nu)\mathcal{L}_\nu\| \le \|(\widetilde{t}_i - t_i)_{i\in I(\nu)}\| + \sum_{j=k+1}^{h} \left\| \sum_{\substack{\nu''\in\mathrm{Sub}(\nu)\\ \mathrm{depth}(\nu'')=j}} f_{\nu''}\mathcal{L}_{\nu''} \right\|$

[(L1), (L4); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3) over the $h-k$ terms]

(L6) $\{I(\nu) : \mathrm{depth}(\nu)=k\}$ partitions $\{1,\dots,N\}$

[Definition A.19]

(L7) $\left(\sum_{\mathrm{depth}(\nu)=k}\|(\widetilde{t}_i - t_i)_{i\in I(\nu)}\|^2\right)^{1/2} = \|\Delta\|$

[(L6); $\Delta = (\widetilde{t}_i - t_i)_{i\le N}$ (the statement); $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead)]

(L8) $\forall j > k\ \forall \nu'' \ne \nu''',\ \mathrm{depth}(\nu'') = \mathrm{depth}(\nu''') = j:\ I(\nu'') \cap I(\nu''') = \emptyset$

[Definition A.19]

(L9) $\forall j > k\ \forall \nu,\ \mathrm{depth}(\nu)=k:\ \left\| \sum_{\substack{\nu''\in\mathrm{Sub}(\nu)\\ \mathrm{depth}(\nu'')=j}} f_{\nu''}\mathcal{L}_{\nu''} \right\|^2 = \sum_{\substack{\nu''\in\mathrm{Sub}(\nu)\\ \mathrm{depth}(\nu'')=j}} \|f_{\nu''}\mathcal{L}_{\nu''}\|^2$

[(L8); $(f_{\nu''}\mathcal{L}_{\nu''})_i = 0$ at $i \notin I(\nu'')$ (Definition G.6); $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead)]

(L10) $\forall j > k\ \forall \nu'',\ \mathrm{depth}(\nu'') = j\ \exists!\, \nu,\ \mathrm{depth}(\nu) = k:\ \nu'' \in \mathrm{Sub}(\nu)$

[Definition A.18, the subtrees and the depth]

(L11) $\Rightarrow\ \forall j > k:\ \sum_{\mathrm{depth}(\nu)=k} \sum_{\substack{\nu''\in\mathrm{Sub}(\nu)\\ \mathrm{depth}(\nu'')=j}} \|f_{\nu''}\mathcal{L}_{\nu''}\|^2 = \sum_{\mathrm{depth}(\nu'')=j} \|f_{\nu''}\mathcal{L}_{\nu''}\|^2$

[(L10)]

(L12) $\forall \nu'',\ \mathrm{depth}(\nu'') = j:\ \|f_{\nu''}\mathcal{L}_{\nu''}\| \le \Xi'_j \|f_{\nu''}\|$

[the operator norm (Definition 4.6, item 7, at T); Ξ'_j (the statement)]

(L13) $\forall j > k:\ \left(\sum_{\mathrm{depth}(\nu)=k} \left\| \sum_{\substack{\nu''\in\mathrm{Sub}(\nu)\\ \mathrm{depth}(\nu'')=j}} f_{\nu''}\mathcal{L}_{\nu''} \right\|^2 \right)^{1/2} \le \Xi'_j \mathfrak{f}_j$

[(L9), (L11), (L12); $\mathfrak{f}_j$ (the statement)]

(L14) $\left(\sum_{\mathrm{depth}(\nu)=k}\|(\widetilde{t}_\nu - t_\nu)\mathcal{L}_\nu\|^2\right)^{1/2} \le \|\Delta\| + \sum_{j=k+1}^{h} \Xi'_j \mathfrak{f}_j$

[(L5), the root sum of squares over the ν at depth k; $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3) over the $h-k+1$ terms; (L7), (L13)]

(L15) $\forall \nu,\ \mathrm{depth}(\nu)=k:\ \widetilde{t}_\nu - t_\nu = ((\widetilde{t}_\nu - t_\nu)\mathcal{L}_\nu)\mathcal{L}_\nu^{-1}$

[$\mathcal{L}_\nu^{-1}$ (Definition 4.6, item 7, at T)]

(L16) $\forall \nu\ \forall y:\ \|y\mathcal{L}_\nu^{-1}\| \le \|\mathcal{L}_\nu^{-1}\|\|y\|$

[the operator norm (Definition 4.6, item 7, at T)]

(L17) $\forall \nu,\ \mathrm{depth}(\nu)=k\ \forall y:\ \|\mathcal{L}_\nu^{-1}\|\|y\| \le \Xi_k\|y\|$

[Ξ_k (Definition 4.6, item 9, at T)]

(L18) $\Rightarrow\ \forall \nu,\ \mathrm{depth}(\nu)=k:\ \|\widetilde{t}_\nu - t_\nu\| \le \Xi_k\|(\widetilde{t}_\nu - t_\nu)\mathcal{L}_\nu\|$

[(L15), (L16), (L17)]

(L19) $\forall (x_\nu)_\nu :\ \|(x_\nu)_\nu\|^2 = \sum_\nu \|x_\nu\|^2$

[$\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead)]

(L20) $\|(\widetilde{t}_\nu - t_\nu)_{\mathrm{depth}(\nu)=k}\| \le \Xi_k \left(\sum_{\mathrm{depth}(\nu)=k} \|(\widetilde{t}_\nu - t_\nu)\mathcal{L}_\nu\|^2\right)^{1/2}$

[(L18) squared and summed over the ν at depth k; (L19)]

(L21) $\forall j \le k :\ \Xi'_j \mathfrak{f}_j \ge 0$

[Ξ'_j, $\mathfrak{f}_j$ (the statement), norms (Fact A.41, item 3); Fact A.41, item 8]

(L22) $\Rightarrow$ the statement

[(L20), (L14); (L21)]

□

Lemma G.57 (The left entry shift at one node [to table])**.** *At one node, the left entry shift its split adds is at most a combination of the exact-factor update and the two center gaps. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $h \ge 1$*;*
- $T \in \mathcal{T}_n$ *(Definition A.18) at* $n := 2^h$*;*
- $t \in \mathcal{R}_n \times \mathcal{R}_n$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*;*
- $\nu \in \mathrm{Sub}(T)$ *of depth at most* $h - 1$.

Define, at (t, T, z)*:*

- *The node factor*
  - l_{10}*, the node's factor over* $\mathbb{R}$ *(*ffsamp *(Algorithm 6), line 4);*
  - $\widetilde{l}_{10}$*, the factor the tree stores at* ν*;*
- *The node bounds*
  - ℓ*,* $\widetilde{\ell}$*,* E_l*,* e_{mul} *and* k_I*, those of Lemma G.51;*
- *The centers and the samples*
  - $(\widetilde{t}_{0,\nu}, \widetilde{t}_{1,\nu})$*, the values* ffsamp *(Algorithm 6) computes at* ν*, line 1 (the input of* deepest *(Algorithm 7) at a leaf node);*
  - $z_{1,\nu}$*, that of Definition A.21 at* ν*, its* z_1 *over* $\mathbb{R}$ *(item 20; item 8 at a leaf node);*
  - $\widetilde{z}_{1,\nu}$*, the value* ffsamp *(Algorithm 6) computes at* ν*, line 21 (the right leaf's sample of* deepest *(Algorithm 7), lines 1 to 3, at a leaf node);*
  - $X'_\nu := \widetilde{t}_{0,\nu} + (\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}) l_{10}$*;*
- *The center shifts*
  - c_{split} *and* k_{split}*, those of Lemma G.53;*
  - $G_X := u + (1 + u)c_{\mathrm{split}}$*;*
  - $K_0 := E_l + (1 + c_{\mathrm{split}})(1 + u)\,(u + (1 + u)e_{\mathrm{mul}})\,\widetilde{\ell}$*;*
  - $G_R := K_0 + G_X E_l$*;*
  - $K_\zeta := \left(k_{\mathrm{split}} + (1 + c_{\mathrm{split}})k_I(\widetilde{\ell})\right)\zeta$*;*
- *The entry shifts*
  - $f^{\mathcal{L}}_\nu$*, that of Lemma G.54.*

Then

$$\|f^{\mathcal{L}}_\nu\| \le G_X \|X'_\nu\| + G_R \|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\| + \ell \|\widetilde{z}_{1,\nu} - z_{1,\nu}\| + K_\zeta.$$

Proof.

COMPUTES $X_\nu := \widetilde{t}_{0,\nu} + (\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu})\widetilde{l}_{10}$ (ffsamp (Algorithm 6) at ν, line 23; the same expression at a leaf node)

COMPUTES $X_{0,\nu} := \widetilde{t}_{0,\nu} + (\widetilde{t}_{1,\nu} - z_{1,\nu}) l_{10}$ (line 24; the same expression at a leaf node)

COMPUTES $\widetilde{tb}_{0,\nu}$ (line 25; deepest (Algorithm 7), line 9, at a leaf node)

(L1) $X_\nu - X'_\nu = (\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu})\widetilde{l}_{10} - (\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}) l_{10}$

[X_ν (the proof's block); X'_ν (the statement)]

(L2) $\Rightarrow\ X_\nu - X'_\nu = (\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu})(\widetilde{l}_{10} - l_{10})$

[(L1); collect]

(L3) $\Rightarrow\ \|X_\nu - X'_\nu\| \le E_l \|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\|$

[(L2); $\forall\psi:\ |\widetilde{l}_{10}(\psi) - l_{10}(\psi)| \le E_l$ (E_l, Lemma G.51)]

Lemma G.20 $\forall\psi$	This proof
$\mathcal{F}$	$\mathcal{F}$ (the statement)
t_0, t_1	$\widetilde{t}_{0,\nu}(\psi), \widetilde{t}_{1,\nu}(\psi)$ (the statement)
z_1	$\widetilde{z}_{1,\nu}(\psi)$ (the statement)
l_{10}	$\widetilde{l}_{10}(\psi)$ (the statement)
tb_0	$X_\nu(\psi)$ (the proof's block)
(I1) $\tilde{tb}_0$	$\widetilde{tb}_{0,\nu}(\psi)$ (the proof's block)
k_B, e_0	k_B, e_0 (Lemma G.20)
k_I	$k_I(\lvert\widetilde{l}_{10}(\psi)\rvert)$ (the statement; Lemma G.51)
$\mathcal{F}$ realization at (u, ζ)	The statement
$t_0, t_1, z_1, l_{10} \in C_\mathcal{F}$	Values ffsamp (Algorithm 6) computes in $\mathcal{F}$ (the statement)
Its conclusion: $\tilde{tb}_0\ \mathcal{N}\,(u, (1+u)\lvert t_1 - z_1\rvert\lvert l_{10}\rvert e_0 + k_I\zeta)\ tb_0$	

(L4) $\forall\psi:\ \widetilde{tb}_{0,\nu}(\psi)\ \mathcal{N}\left(u, (1+u)|\widetilde{t}_{1,\nu}(\psi) - \widetilde{z}_{1,\nu}(\psi)||\widetilde{l}_{10}(\psi)|e_0 + k_I(|\widetilde{l}_{10}(\psi)|)\zeta\right)\ X_\nu(\psi)$

[(I1)]

(L5) $e_0 = u + (1+u)e_{\mathrm{mul}}$

[e_0 (Lemma G.20); e_{mul} (the statement); Lemma G.51, (L3)]

(L6) $\forall\psi:\ k_I(|\widetilde{l}_{10}(\psi)|) \le k_I(\widetilde{\ell})$

[Lemma G.51, (L2)]

(L7) $\|\widetilde{tb}_{0,\nu} - X_\nu\| \le u\|X_\nu\| + (1+u)(u + (1+u)e_{\mathrm{mul}})\widetilde{\ell}\|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\| + k_I(\widetilde{\ell})\zeta$

[(L4), (L5), (L6); $\forall\psi:\ |\widetilde{l}_{10}(\psi)| \le \widetilde{\ell}$ ($\widetilde{\ell}$, Lemma G.51); Definition A.11; Fact G.50 at $c := 0$, $e := k_I(\widetilde{\ell})\zeta$, $(wM)^{1/2} = 1$; $\|X+Y\| \le \|X\| + \|Y\|$ (Fact A.41, item 3)]

(L8) $\|\widetilde{tb}_{0,\nu}\| \le (1+u)\|X_\nu\| + (1+u)(u + (1+u)e_{\mathrm{mul}})\widetilde{\ell}\|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\| + k_I(\widetilde{\ell})\zeta$

[(L7); $\|\widetilde{tb}_{0,\nu}\| \le \|X_\nu\| + \|\widetilde{tb}_{0,\nu} - X_\nu\|$ (Fact A.41, item 3)]

(L9) $\mathrm{depth}(\nu) \le h - 1$

[ν (the statement)]

Lemma G.53, item 2 at ν	This proof
Shared: $\mathcal{F},\ T, \nu,\ c_{\mathrm{split}}, k_{\mathrm{split}}$	
Shared: $h \ge 1,\ n := 2^h,\ T \in \mathcal{T}_n$	
z_1	$z_{1,\nu}$ (the statement)
$\widetilde{t}_0, \widetilde{t}_1$	$\widetilde{t}_{0,\nu}, \widetilde{t}_{1,\nu}$ (the statement)
$f_\nu^{\mathcal{L}}$	$f_\nu^{\mathcal{L}}$ (the statement)
(I2) $\widetilde{tb}_0, X_0$	$\widetilde{tb}_{0,\nu}, X_{0,\nu}$ (the proof's block)
$\mathcal{F}$ realization at (u, ζ)	The statement
$k \ge -1$	$k := h - \mathrm{depth}(\nu) - 2$; (L9)
$\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_{2^{k+2}}$	ν (the statement), of depth $\log_2(n/2^{k+2})$ (Definition A.18)
$z_1 \in \mathcal{R}_{2^{k+2}}$	$z_{1,\nu}$ (the statement)
Its conclusion: $\|f_\nu^{\mathcal{L}}\| \le c_{\mathrm{split}}\|\widetilde{tb}_0\| + k_{\mathrm{split}}\zeta + \|\widetilde{tb}_0 - X_0\|$	

(L10) $\|f_\nu^{\mathcal{L}}\| \le c_{\mathrm{split}}\|\widetilde{tb}_{0,\nu}\| + k_{\mathrm{split}}\zeta + \|\widetilde{tb}_{0,\nu} - X_{0,\nu}\|$

[(I2)]

	Lemma G.51, item 2 at ν	This proof
	Shared: $\mathcal{F},\ T, \nu,\ l_{10}, \widetilde{l}_{10},\ \ell, \widetilde{\ell}, E_l, e_{\mathrm{mul}}, k_I(\widetilde{\ell})$ Shared: $h \geq 1,\ n := 2^h,\ T \in \mathcal{T}_n$	
	z_1	$z_{1,\nu}$ (the statement)
	$\widetilde{t}_1, \widetilde{tb}_0, X, X_0, \widetilde{z}_1$	$\widetilde{t}_{1,\nu}, \widetilde{tb}_{0,\nu}, X_\nu, X_{0,\nu}, \widetilde{z}_{1,\nu}$ (the statement; the proof's block)
(I3)	$\mathcal{F}$ realization at (u, ζ)	The statement
	$k \geq -1$	$k := h - \mathrm{depth}(\nu) - 2$; (L9)
	$\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_{2^{k+2}}$	ν (the statement), of depth $\log_2(n/2^{k+2})$ (Definition A.18)
	$z_1 \in \mathcal{R}_{2^{k+2}}$	$z_{1,\nu}$ (the statement)
	Its conclusion: $\|\widetilde{tb}_0 - X_0\| \leq E_l\|\widetilde{t}_1 - \widetilde{z}_1\| + \ell\|\widetilde{z}_1 - z_1\| + (1+u)(u + (1+u)e_{\mathrm{mul}})\widetilde{\ell}\|\widetilde{t}_1 - \widetilde{z}_1\| + u\|X\| + k_I(\widetilde{\ell})\zeta$	

(L11) $\|\widetilde{tb}_{0,\nu} - X_{0,\nu}\| \leq E_l\|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\| + \ell\|\widetilde{z}_{1,\nu} - z_{1,\nu}\| + (1+u)(u + (1+u)e_{\mathrm{mul}})\widetilde{\ell}\|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\| + u\|X_\nu\| + k_I(\widetilde{\ell})\zeta$

[(I3)]

(L12) $\|f^{\mathcal{L}}_\nu\| \leq G_X\|X_\nu\| + K_0\|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\| + \ell\|\widetilde{z}_{1,\nu} - z_{1,\nu}\| + K_\zeta$

[(L10), (L8), (L11); G_X, K_0, K_ζ (the statement) collect the coefficients]

(L13) $\|f^{\mathcal{L}}_\nu\| \leq G_X\|X'_\nu\| + G_R\|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\| + \ell\|\widetilde{z}_{1,\nu} - z_{1,\nu}\| + K_\zeta$

[(L12); $\|X_\nu\| \leq \|X'_\nu\| + \|X_\nu - X'_\nu\|$ (Fact A.41, item 3); (L3); $G_R = K_0 + G_X E_l$ (the statement)]

(L14) $\Rightarrow$ the statement

[(L13)]

□

Lemma G.58 (The entry shifts of a depth [to table])**.** *At each depth, the entry shifts the nodes of the previous depth add are at most a term over $\mathbb{R}$ plus a multiple of the previous depth's entry deviation. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *$h \geq 1$;*
- *$T \in \mathcal{T}_n$ (Definition A.18) at $n := 2^h$;*
- *$t \in \mathcal{R}_n \times \mathcal{R}_n$;*
- *$z \in \mathbb{Z}^N$ at $N := 2n$;*
- *$k \in \{1, \ldots, h\}$;*
- *$B \geq 0$.*

Define, at each $\nu \in \mathrm{Sub}(T)$, at (t, T, z):

- *The node bounds*
  - *ℓ, that of Lemma G.51;*
- *The centers and the samples*
  - *t_ν, the center over $\mathbb{R}$ (Definition A.21, item 6);*
  - *$\widetilde{t}_\nu$, the value ffsamp (Algorithm 6) computes at line 1 (the input of deepest (Algorithm 7) at a leaf node);*
  - *$tb_{0,\nu}$, over $\mathbb{R}$ (Definition A.21, item 16; item 9 at a leaf node);*
  - *$t_{1,\nu}$, that of Definition A.21 at ν, its t_1 over $\mathbb{R}$ (item 6);*
  - *$z_{1,\nu}$, that of Definition A.21 at ν, its z_1 over $\mathbb{R}$ (item 20; item 8 at a leaf node);*
- *The center shifts*
  - *c_{split} and k_{split}, those of Lemma G.53;*
  - *c_{merge} and a_j, those of Lemma G.52;*
  - *G_X, G_R and K_ζ, those of Lemma G.57;*
  - *$G_\gamma := c_{\mathrm{split}} + G_X(1+\ell) + G_R$;*
- *The entry shifts*

- $f_{R(\nu)} := f^R_\nu$, *that of Lemma G.54;*
- $f_{L(\nu)} := f^{\mathcal{L}}_\nu$, *that of Lemma G.54;*
- $\mathfrak{f}_k := \left(\sum_{\mathrm{depth}(\nu)=k} \|f_\nu\|^2\right)^{1/2}$;

• *The terms*

- $\mathfrak{T}_k := \left(\sum_{\mathrm{depth}(\nu)=k-1} \|t_\nu\|^2\right)^{1/2}$;
- $\mathfrak{T}'_k := \left(\sum_{\mathrm{depth}(\nu)=k-1} \|tb_{0,\nu}\|^2\right)^{1/2}$;
- $R_k := \left(\sum_{\mathrm{depth}(\nu)=k-1} \|t_{1,\nu} - z_{1,\nu}\|^2\right)^{1/2}$;
- $M_k := (1 + c_{\mathrm{merge}})^{h-k} - 1$;
- $Z := \|z\|$;
- $G_Z := G_X \ell + G_R + \ell$;
- $\Theta_k := \sqrt{2^{k-1}}\,(k_{\mathrm{split}}\zeta + K_\zeta + G_Z\, a_{h-k})$;
- $\Delta^*_k := c_{\mathrm{split}}\mathfrak{T}_k + G_X\mathfrak{T}'_k + G_R R_k + G_Z M_k Z + \Theta_k$.

Assume:

(A1) $\|(\widetilde{t}_\nu - t_\nu)_{\mathrm{depth}(\nu)=k-1}\| \le B$.

Then

$$\mathfrak{f}_k \le \Delta^*_k + G_\gamma B.$$

Proof.

DEFINES $X'_\nu := \widetilde{t}_{0,\nu} + (\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}) l_{10}$

(L1) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \|\widetilde{t}_{1,\nu}\| \le \|t_\nu\| + \|\widetilde{t}_\nu - t_\nu\|$

[$\widetilde{t}_{1,\nu}$, a component of $\widetilde{t}_\nu$; $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3)]

(L2) $\|(\widetilde{t}_{1,\nu})_{\mathrm{depth}(\nu)=k-1}\| \le \mathfrak{T}_k + B$

[(L1); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3) over the nodes of depth $k-1$; assumption A1; $\mathfrak{T}_k$ (the statement)]

Lemma G.52 at every ν with $\mathrm{depth}(\nu) = k-1$	This proof
Shared: $\mathcal{F}, (u,\zeta),\ T, \nu,\ c_{\mathrm{merge}}, a_j$	
Shared: $T \in \mathcal{T}_n$	
(I1)	
m	2^{h-k+1}
k'	$h-k$ (Definition A.18)
$(z_1, \widetilde{z}_1)$	$(z_{1,\nu}, \widetilde{z}_{1,\nu})$
$m \ge 2$	$k \in \{1, \dots, h\}$ (the statement)
$\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m$	ν (the scope); Definition A.18
Its conclusion: $\|\widetilde{z}_1 - z_1\| \le ((1 + c_{\mathrm{merge}})^{k'} - 1)\|z_1\| + a_{k'}$	

(L3) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \|\widetilde{z}_{1,\nu} - z_{1,\nu}\| \le M_k \|z_\nu\| + a_{h-k}$

[(I1)]

(L4) $\|(\widetilde{z}_{1,\nu} - z_{1,\nu})_{\mathrm{depth}(\nu)=k-1}\| \le M_k Z + \sqrt{2^{k-1}}\, a_{h-k}$

[(L3); $I(\nu) \cap I(\nu') = \emptyset$ at $\nu \ne \nu'$ of one depth (Definition A.19); $\left(\sum_\nu \|z_\nu\|^2\right)^{1/2} = Z$ (Z, the statement); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3) over the 2^{k-1} nodes]

(L5) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu} = (t_{1,\nu} - z_{1,\nu}) + (\widetilde{t}_{1,\nu} - t_{1,\nu}) - (\widetilde{z}_{1,\nu} - z_{1,\nu})$

[expand]

(L6) $\|(\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu})_{\mathrm{depth}(\nu)=k-1}\| \le R_k + B + M_k Z + \sqrt{2^{k-1}}\, a_{h-k}$

[(L5); assumption A1; (L4); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3); R_k (the statement)]

(L7) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ X'_\nu - tb_{0,\nu} = (\widetilde{t}_{0,\nu} - t_{0,\nu}) + (\widetilde{t}_{1,\nu} - t_{1,\nu})\, l_{10} - (\widetilde{z}_{1,\nu} - z_{1,\nu})\, l_{10}$

[X'_ν (the proof's block); $tb_{0,\nu}$ (Definition A.21, item 16); expand]

(L8) $\forall \psi:\ |l_{10}(\psi)| \le \ell$

[$\ell := \max_\psi |l_{10}|$ (Lemma G.51)]

(L9) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \|X'_\nu\| \le \|tb_{0,\nu}\| + (1+\ell)\|\widetilde{t}_\nu - t_\nu\| + \ell\|\widetilde{z}_{1,\nu} - z_{1,\nu}\|$

[(L7), (L8); $\widetilde{t}_{0,\nu} - t_{0,\nu}$ and $\widetilde{t}_{1,\nu} - t_{1,\nu}$, the components of $\widetilde{t}_\nu - t_\nu$; $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3)]

(L10) $\|(X'_\nu)_{\mathrm{depth}(\nu)=k-1}\| \le \mathfrak{T}'_k + (1+\ell)B + \ell(M_k Z + \sqrt{2^{k-1}}\, a_{h-k})$

[(L9); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3) over the nodes; assumption A1; (L4); $\mathfrak{T}'_k$ (the statement)]

Lemma G.53, item 1 at every ν with $\mathrm{depth}(\nu) = k-1$	This proof
Shared: $\mathcal{F},\ h, T, \nu,\ f^R_\nu,\ c_{\mathrm{split}}, k_{\mathrm{split}}$	
Shared: $h \ge 1,\ n := 2^h,\ T \in \mathcal{T}_n$	
k	$h-k-1$
(I2) z_1	$z_{1,\nu}$
$\widetilde{t}_1$	$\widetilde{t}_{1,\nu}$
$k \ge -1$	$k \in \{1,\dots,h\}$ (the statement)
$\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_{2^{k+2}}$	ν (the scope); Definition A.18
$z_1 \in \mathcal{R}_{2^{k+2}}$	$z_{1,\nu}$ (the statement)
Its item 1: $\|f^R_\nu\| \le c_{\mathrm{split}}\|\widetilde{t}_1\| + k_{\mathrm{split}}\zeta$	

(L11) $\forall \nu,\ \mathrm{depth}(\nu) = k-1 :\ \|f^R_\nu\| \le c_{\mathrm{split}}\|\widetilde{t}_{1,\nu}\| + k_{\mathrm{split}}\zeta$

[(I2)]

Lemma G.57 at every ν with $\mathrm{depth}(\nu) = k-1$	This proof
Shared: $\mathcal{F}, (u,\zeta),\ h, T, t, z,\ \nu,\ \widetilde{t}_{0,\nu}, \widetilde{t}_{1,\nu}, z_{1,\nu}, \widetilde{z}_{1,\nu},\ l_{10},\ X'_\nu$ (the proof's block), $f^{\mathcal{L}}_\nu,\ \ell, G_X, G_R, K_\zeta$	
(I3) Shared: $h \ge 1,\ T \in \mathcal{T}_n,\ t \in \mathcal{R}_n \times \mathcal{R}_n,\ z \in \mathbb{Z}^N$	
$\mathrm{depth}(\nu) \le h-1$	$\mathrm{depth}(\nu) = k-1,\ k \in \{1,\dots,h\}$ (the statement)
Its conclusion: $\|f^{\mathcal{L}}_\nu\| \le G_X\|X'_\nu\| + G_R\|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\| + \ell\|\widetilde{z}_{1,\nu} - z_{1,\nu}\| + K_\zeta$	

(L12) $\forall \nu,\ \mathrm{depth}(\nu) = k-1 :\ \|f^{\mathcal{L}}_\nu\| \le G_X\|X'_\nu\| + G_R\|\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu}\| + \ell\|\widetilde{z}_{1,\nu} - z_{1,\nu}\| + K_\zeta$

[(I3)]

(L13) $\mathfrak{f}_k^2 = \sum_{\mathrm{depth}(\nu)=k-1}(\|f^R_\nu\|^2 + \|f^{\mathcal{L}}_\nu\|^2)$

[$\mathfrak{f}_k$, f_ν (Lemma G.55) at the 2^{k-1} nodes ν of depth $k-1$]

(L14) $\forall c \ge 0 :\ \left(\sum_{\mathrm{depth}(\nu)=k-1} c^2\right)^{1/2} = \sqrt{2^{k-1}}\, c$

[the 2^{k-1} nodes of depth $k-1$ (Definition A.18)]

(L15) $\mathfrak{f}_k \le c_{\mathrm{split}}\|(\widetilde{t}_{1,\nu})_{\mathrm{depth}(\nu)=k-1}\| + G_X\|(X'_\nu)_{\mathrm{depth}(\nu)=k-1}\| + G_R\|(\widetilde{t}_{1,\nu} - \widetilde{z}_{1,\nu})_{\mathrm{depth}(\nu)=k-1}\|$
$+ \ell\|(\widetilde{z}_{1,\nu} - z_{1,\nu})_{\mathrm{depth}(\nu)=k-1}\| + \sqrt{2^{k-1}}(k_{\mathrm{split}}\zeta + K_\zeta)$

[(L11), (L12), (L13); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3) over the terms of the two bounds; (L14)]

(L16) $\mathfrak{f}_k \le c_{\mathrm{split}}(\mathfrak{T}_k + B) + G_X(\mathfrak{T}'_k + (1+\ell)B + \ell(M_k Z + \sqrt{2^{k-1}}a_{h-k}))$
$+ G_R(R_k + B + M_k Z + \sqrt{2^{k-1}}a_{h-k}) + \ell(M_k Z + \sqrt{2^{k-1}}a_{h-k})$
$+ \sqrt{2^{k-1}}(k_{\mathrm{split}}\zeta + K_\zeta)$

[(L15); (L2), (L10), (L6), (L4) for the four norms]

(L17) $\Rightarrow$ the statement

[(L16); G_γ, G_R, G_Z, G_Z the coefficients of B, R_k, $M_k Z$, $\sqrt{2^{k-1}}a_{h-k}$ (the statement); Δ^*_k the rest (the statement)]

□

Theorem G.59 (The center shift [to table])**.** *The shift of the computed leaf centers, times $1-\gamma$, is at most Δ^*, Δ^* collecting the root's perturbation and each depth's entry shifts. Let:*

- *$\mathcal{F}$ be a realization at (u,ζ) (Definition A.4);*
- *$h \ge 1$;*
- *$T \in \mathcal{T}_n$ at $n := 2^h$;*
- *$t \in \mathcal{R}_n \times \mathcal{R}_n$;*
- *$z \in \mathbb{Z}^N$ at $N := 2n$.*

Define:

- *The key constants*
  - Ξ'_{root}, Ξ'_k *and* Ξ_k, *those of Definition 4.6, items 10, 8 and 9, at* T;
  - $\ell := \max_\psi |l_{10}(\psi)|$, *taken over the nodes (Lemma G.51 at each node);*
- *The node bounds*
  - $\widetilde{\ell} := \max_\psi |\widetilde{l}_{10}|$, *taken over the nodes;*
  - $E_l := \max_\psi |\widetilde{l}_{10} - l_{10}|$, *taken over the nodes;*
- *The centers and the samples*
  - $\widetilde{t}_T$, *the root node's computed input (*ffsamp *(Algorithm 6), line 1 at* $\nu = T$*);*
  - $e_{\text{root}} := \widetilde{t}_T - t$;
  - $\Delta := (\widetilde{t}_i - t_i)_{i \le N}$: $\widetilde{t}_i$ *the center* $\text{ffSampling}^{\mathcal{F}}$ *passes to the base sampler at position* i *(deepest (Algorithm 7), lines 1 to 18),* t_i *the center* $\text{ffSampling}(t, T)$ *sets there over* $\mathbb{R}$ *(Definition A.21, item 2);*
  - t_ν, *the value of* $\text{ffSampling}(t, T)$ *at* ν *(Definition A.21, item 6);*
  - $tb_{0,\nu}$, *that of item 16, item 9 at a leaf node;*
  - $t_{1,\nu}$, *that of item 6;*
  - $z_{1,\nu}$, *that of item 15, item 8 at a leaf node;*
  - $Z := \|z\|$;
- *The center shifts*
  - $c_{\text{split}} := (1+u)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1$ *(Lemma G.53);*
  - $k_{\text{split}} := \sqrt{2}/2 + (\sqrt{2}/2)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) + \sqrt{2}(3+2u)$ *(Lemma G.53);*
  - $e_{\text{mul}} := \sqrt{2}\,u(2+u)$ *(Lemma G.51);*
  - $k_I(\widetilde{\ell}) := (\sqrt{2}\,\widetilde{\ell}(1+\sqrt{2}\,u(2+u)) + \sqrt{2}(3+2u))(1+u) + \sqrt{2}$ *(Lemma G.51);*
  - $c_{\text{merge}} := u + (1+u)((1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1)$ *(Lemma G.52);*
  - a_j, *by* $a_0 := 0$ *and* $a_{j+1} := \sqrt{2}(1+c_{\text{merge}})a_j + 2\sqrt{2}((3+2u)(1+u)+1)\zeta$ *(Lemma G.52);*
- *The terms*
  - $\mathfrak{T}_k := \left(\sum_{\text{depth}(\nu)=k-1} \|t_\nu\|^2\right)^{1/2}$;
  - $\mathfrak{T}'_k := \left(\sum_{\text{depth}(\nu)=k-1} \|tb_{0,\nu}\|^2\right)^{1/2}$;
  - $R_k := \left(\sum_{\text{depth}(\nu)=k-1} \|t_{1,\nu} - z_{1,\nu}\|^2\right)^{1/2}$;
  - $G_X := u + (1+u)c_{\text{split}}$;
  - $K_0 := E_l + (1+c_{\text{split}})(1+u)\,(u + (1+u)e_{\text{mul}})\,\widetilde{\ell}$;
  - $G_R := K_0 + G_X E_l$;
  - $G_Z := G_X \ell + G_R + \ell$;
  - $G_\gamma := c_{\text{split}} + G_X(1+\ell) + G_R$;
  - $K_\zeta := \left(k_{\text{split}} + (1+c_{\text{split}})k_I(\widetilde{\ell})\right)\zeta$;
  - $M_k := (1+c_{\text{merge}})^{h-k} - 1$;
  - $\Theta_k := \sqrt{2^{k-1}}\,(k_{\text{split}}\zeta + K_\zeta + G_Z\, a_{h-k})$;
  - $\beta_0 := 1/\Xi'_{\text{root}}$;
  - $\forall j \in \{1, \ldots, h-1\} :\ \beta_j := 2\Xi_j$;
  - $\Delta^*_k := c_{\text{split}}\mathfrak{T}_k + G_X\mathfrak{T}'_k + G_R R_k + G_Z M_k Z + \Theta_k$;
  - $\gamma := G_\gamma \sum_{k=1}^h \Xi'_k \beta_{k-1}$;
  - $\Delta^* := \Xi'_{\text{root}}\|e_{\text{root}}\| + \sum_{k=1}^h \Xi'_k \Delta^*_k$.

Then

$$(1-\gamma)\|\Delta\| \le \Delta^*.$$

Proof.

DEFINES $\mathfrak{f}_k = (\sum_{\text{depth}(\nu)=k} \|f_\nu\|^2)^{1/2}$, $k \ge 1$ (Lemma G.55)

DEFINES f_ν, those of Lemma G.55

DEFINES $B := \Xi'_{\text{root}}\|e_{\text{root}}\| + \sum_{k=1}^h \Xi'_k \mathfrak{f}_k$

(L1) $\|\Delta\| \le B$

[Lemma G.55; B (the proof's block)]

(L2) $\Xi'_{\text{root}}\|e_{\text{root}}\| \ge 0$

[Ξ'_{root}, an operator norm (Definition 4.6, item 10, at T); $\|e_{\text{root}}\| \ge 0$ (Fact A.41, item 3)]

(L3) $\sum_{k=1}^{h} \Xi'_k \mathfrak{f}_k \ge 0$

[Ξ'_k, operator norms (Definition 4.6, item 8, at T); $\mathfrak{f}_k \ge 0$ (Lemma G.55)]

(L4) $\Rightarrow\ \Xi'_{\text{root}}\|e_{\text{root}}\| \le B$

[(L3); B (the proof's block)]

(L5) $\Rightarrow\ \sum_{k=1}^{h} \Xi'_k \mathfrak{f}_k \le B$

[(L2); B (the proof's block)]

Lemma G.11	This proof
Shared: $T,\ \mathcal{L}_T$	
Shared: $T \in \mathcal{T}_n$	
(I1) $(x_j)_{j\le N}$	$(1,0,\dots,0)$
i	1
$i \le N$	$N = 2n$ (the statement)
Its conclusion: $\forall x \in \mathcal{R}_n \times \mathcal{R}_n\ \forall i \le N:\ (x\mathcal{L}_T)_i = x_i + \sum_{j<i} x_j (\mathcal{L}_T)_{ji}$	

(L6) $\Xi'_{\text{root}} \ge 1$

[(I1); Definition 4.6, item 10, at T]

(L7) $\Rightarrow\ \|e_{\text{root}}\| \le \beta_0 B$

[(L4), (L6); $\beta_0 = 1/\Xi'_{\text{root}}$ (Table 21)]

(L8) $\forall j \in \{1,\dots,h-1\}:\ \|(\widetilde{t}_\nu - t_\nu)_{\text{depth}(\nu)=j}\| \le \beta_j B$

[Lemma G.56; (L1), (L5); $\beta_j = 2\Xi_j$ (Table 21)]

Lemma G.58 at every $k \in \{1,\dots,h\}$	This proof
Shared: $\mathcal{F}, h, T, t, z, k,\ \widetilde{t}_\nu, t_\nu, \mathfrak{f}_k, \Delta^*_k, G_\gamma$	
B	$\beta_{k-1}B$ (the scope)
(I2) $B \ge 0$	$\beta_{k-1}B \ge 0$: $B \ge 0$ by (L2), (L3); $\beta_{k-1} \ge 0$ by (L6) and Table 21
Assumption A1	(L7) at $k=1$, (L8) at $k \ge 2$
Its conclusion: $\mathfrak{f}_k \le \Delta^*_k + G_\gamma B$	

(L9) $\forall k \in \{1,\dots,h\}:\ \mathfrak{f}_k \le \Delta^*_k + G_\gamma \beta_{k-1} B$

[(I2)]

(L10) $\sum_{k=1}^{h} \Xi'_k(\Delta^*_k + G_\gamma\beta_{k-1}B) = \sum_{k=1}^{h} \Xi'_k \Delta^*_k + \gamma B$

[γ (the statement)]

(L11) $\Rightarrow\ B \le \Delta^* + \gamma B$

[B (the proof's block); (L9), (L10); Δ^* (the statement)]

(L12) $\Rightarrow\ (1-\gamma)B \le \Delta^*$

[(L11)]

(L13) $\gamma \le 1 \Rightarrow\ (1-\gamma)\|\Delta\| \le (1-\gamma)B$

[(L1)]

(L14) $\Delta^* \ge 0$

[$\Xi'_{\text{root}}, \Xi'_k \ge 0$ (Definition 4.6, items 10 and 8, at T); $\|e_{\text{root}}\| \ge 0$ (Fact A.41, item 3); $\Delta^*_k \ge 0$ (Δ^*_k, the statement)]

(L15) $\gamma > 1 \Rightarrow\ (1-\gamma)\|\Delta\| \le 0$

[$\|\Delta\| \ge 0$ (Fact A.41, item 3)]

(L16) $\Rightarrow$ the statement

[(L12), (L13), (L14), (L15)]

□

Lemma G.60 (The offsets R_k on the tail-cut event [to table])**.** *On the tail-cut event, the sample's offset from the centers at each depth is at most the tree-wide inverse norm times the leaves' reach.*
Let:
- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- $h \geq 1$*;*
- $T \in \mathcal{T}_n$ *at* $n := 2^h$*;*
- $z \in \mathbb{Z}^N$ *at* $N := 2n$*;*
- $k \in \{1, \dots, h\}$*;*
- $\bar{\delta} \in \mathbb{R}$.

Define:
- *The key constants*
  - Ξ*, that of Definition 4.6, item 13, at* T*;*
- *The tail-cut event*
  - τ*, the radius of the tail-cut event (Definition A.26);*
  - $S := \{ z \in \mathbb{Z}^N : \forall i \leq N \ |z_i - \widetilde{t}_i(z_{<i})| \leq \tau\, \widetilde{\sigma}_i(z_{<i}) \}$ *(Definition A.26);*
- *The leaf standard deviations*
  - $\sigma_{\max} := \max_i \sigma_i$*;*
- *The centers and the samples*
  - t*, the root node's center;*
  - $t_{1,\nu}$ *and* $z_{1,\nu}$*, those of Theorem G.59;*
  - $\Delta := (\widetilde{t}_i - t_i)_{i \leq N}$*:* $\widetilde{t}_i$ *the center* ffSampling$^{\mathcal{F}}$ *passes to the base sampler at position* i *(deepest (Algorithm 7), lines 1 to 18),* t_i *the center* ffSampling(t, T) *sets there over* $\mathbb{R}$ *(Definition A.21, item 2);*
- *The terms*
  - $R_k := (\sum_{\mathrm{depth}(\nu)=k-1} \|t_{1,\nu} - z_{1,\nu}\|^2)^{1/2}$ *(Theorem G.59).*

Assume:
(A1) $z \in S$*;*
(A2) $\forall i \leq N \ \exists \delta_i \in \mathbb{R},\ |\delta_i| \leq \bar{\delta} :\ \widetilde{\sigma}_i = \sigma_i(1 + \delta_i)$.
Then

$$R_k \leq \Xi(\sqrt{2}\,\tau\sigma_{\max}(1 + \bar{\delta}) + \|\Delta\|)(n/2)^{1/2}. \qquad \textit{[derived]}$$

Proof.

DEFINES $\Delta_i(z_{<i}) := \widetilde{t}_i(z_{<i}) - t_i(z_{<i})$ for $i \leq N$ and every $z_{<i}$ (Definition A.27)
DEFINES $c = (c_i)_{i \leq N}$, the leaf centers with the sample z (Definition G.9)
DEFINES $d_v := d_{2v-1}$ for $v \leq n$, equal to d_{2v} (Definition A.19)
DEFINES $\forall x \in \mathbb{R}^N \ \forall v \leq n :\ x_{(v)} := x_{2v-1} + i x_{2v} \in \mathbb{C}$

(L1) $\forall z \in S \ \forall i \leq N :\ |z_i - \widetilde{t}_i| \leq \tau\widetilde{\sigma}_i$
[S (Definition A.26)]

(L2) $\Rightarrow\ \forall z \in S \ \forall v \leq n :\ |(z - \widetilde{t})_{(v)}| \leq \sqrt{2}\,\tau\widetilde{\sigma}_{2v}$
[(L1) at $i = 2v - 1$ and $i = 2v$; $\widetilde{\sigma}_{2v-1} = \widetilde{\sigma}_{2v}$ (line 3 of deepest (Algorithm 7), one $\widetilde{\texttt{isigma}}$ per leaf diagonal); $d_{2v-1} = d_{2v}$ (Definition A.19); $|x + iy|^2 = x^2 + y^2$ (Fact A.41, item 1)]

(L3) $\Rightarrow\ \forall z \in S \ \forall v \leq n :\ |(c - z)_{(v)}| \leq \sqrt{2}\,\tau\widetilde{\sigma}_{2v} + |\Delta_{(v)}|$
[(L2); $c_i = t_i(z_{<i})$ (the leaf center over $\mathbb{R}$, Proposition G.48; Definition A.25); $\Delta_i = \widetilde{t}_i - t_i$ (Definition A.27); $|x + y| \leq |x| + |y|$ (Fact A.41, item 1)]

(L4) $\forall v \leq n :\ \widetilde{\sigma}_{2v} \leq \sigma_{\max}(1 + \bar{\delta})$
[$\widetilde{\sigma}_i = \sigma_i(1 + \delta_i)$, $|\delta_i| \leq \bar{\delta}$ (assumption A2); $\sigma_{\max}$ (the statement)]

(L5) $\forall v \leq n :\ |\Delta_{(v)}| \leq \|\Delta\|$
[$\Delta = (\Delta_i)_{i \leq N}$ (Lemma G.54); $|\Delta_{(v)}|^2 = \Delta_{2v-1}^2 + \Delta_{2v}^2$, $\Delta_{2v-1}^2 + \Delta_{2v}^2 \leq \sum_i \Delta_i^2$ (Fact A.41, items 1, 3)]

(L6) $\forall \nu,\ \mathrm{depth}(\nu) = k - 1 :\ |I(T_{11}(\nu))| = 2n/2^k$
[$T_{11}(\nu)$ of degree $n/2^k$; $|I(T')| = 2m'$ (Definition A.19) at T' of degree m']

(L7) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \|(c-z)_{I(T_{11}(\nu))}\|^2 = \sum_{v:\ d_v \in \mathrm{Sub}(T_{11}(\nu)) \cap \mathbb{R}} |(c-z)_{(v)}|^2$
[the leaf diagonals of $T_{11}(\nu)$ cover $I(T_{11}(\nu))$, two positions each (Definition A.19); $|x+iy|^2 = x^2+y^2$ (Fact A.41, item 1)]

(L8) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \sum_{v:\ d_v \in \mathrm{Sub}(T_{11}(\nu)) \cap \mathbb{R}} |(c-z)_{(v)}|^2 \le \frac{n}{2^k} (\sqrt{2}\,\tau\sigma_{\max}(1+\bar{\delta}) + \|\Delta\|)^2$
[(L3), (L4), (L5), (L6); $z \in S$ (assumption A1)]

Lemma G.47 at every ν with $\mathrm{depth}(\nu) = k-1$	This proof
Shared: $T, t, z,\ N,\ c$ (the proof's block)	
Shared: $T \in \mathcal{T}_n,\ z \in \mathbb{Z}^N$	
T'	$T_{11}(\nu)$
$t \in \mathcal{R}_n \times \mathcal{R}_n$	t (the statement)
$T' \in \mathrm{Sub}(T)$	ν, k (the statement); Definition A.18
Its conclusion: $\forall T' \in \mathrm{Sub}(T):\ (c-z)_{I(T')} = (t_{T'} - \hat{z}_{T'})\mathcal{L}_{T'}$	

(I1)

(L9) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ (c-z)_{I(T_{11}(\nu))} = (t_{T_{11}(\nu)} - \hat{z}_{T_{11}(\nu)})\mathcal{L}_{T_{11}(\nu)}$
[(I1)]

Lemma G.46, item 1 at every ν with $\mathrm{depth}(\nu) = k-1$ in $\mathcal{T}_m$	This proof
Shared: $T, t, z,\ m, \nu,\ t_{T'}, \hat{z}_{T'}$	
Shared: $T \in \mathcal{T}_n,\ z \in \mathbb{Z}^N$	
(t_1, z_1)	$(t_{1,\nu}, z_{1,\nu})$
$t \in \mathcal{R}_n \times \mathcal{R}_n$	t (the statement)
$m \ge 4$	The scope
Its item 1: $t_{T_{11}} - \hat{z}_{T_{11}} = \mathrm{split}(t_1 - z_1)$	

(I2)

Proposition G.19, item 1 at every ν with $\mathrm{depth}(\nu) = k-1$ in $\mathcal{T}_m$	This proof
Shared: m	
f	$t_{1,\nu} - z_{1,\nu}$
$m \ge 4$	The scope
$f \in \mathcal{R}_m$	(I2)
Its item 1: $\|\mathrm{split}(f)\| = \|f\|$	

(I3)

(L10) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \|t_{T_{11}(\nu)} - \hat{z}_{T_{11}(\nu)}\| = \|t_{1,\nu} - z_{1,\nu}\|$
[at a node in $\mathcal{T}_m$ with $m \ge 4$, (I2), (I3); at a node in $\mathcal{T}_2$, Lemma G.45, item 2]

(L11) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \|t_{1,\nu} - z_{1,\nu}\| \le \|\mathcal{L}^{-1}_{T_{11}(\nu)}\|\ \|(c-z)_{I(T_{11}(\nu))}\|$
[(L9), (L10); the operator norm (Definition 4.6, item 7, at T)]

(L12) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \|\mathcal{L}^{-1}_{T_{11}(\nu)}\| \le \Xi$
[$\mathrm{depth}(T_{11}(\nu)) = k$ (Definition A.18): $\Xi_k \le \Xi$ at $k \le h-1$ (Ξ, Definition 4.6, item 13, at T; Fact A.41, item 20); at $k = h$, the tree map of a leaf diagonal the identity (Definition G.6), of norm 1; $1 \le \Xi$ (Ξ, Definition 4.6, item 13, at T; Fact A.41, item 20)]

(L13) $\forall \nu,\ \mathrm{depth}(\nu) = k-1:\ \|\mathcal{L}^{-1}_{T_{11}(\nu)}\|\ \|(c-z)_{I(T_{11}(\nu))}\| \le \Xi(\sqrt{2}\,\tau\sigma_{\max}(1+\bar{\delta}) + \|\Delta\|) \left(\frac{n}{2^k}\right)^{1/2}$
[(L7), (L8), (L12)]

(L14) $R_k^2 = \sum_{\mathrm{depth}(\nu)=k-1} \|t_{1,\nu} - z_{1,\nu}\|^2$
[R_k (the statement)]

(L15) $\sum_{\mathrm{depth}(\nu)=k-1} \|t_{1,\nu} - z_{1,\nu}\|^2 \le 2^{k-1}\,\Xi^2(\sqrt{2}\,\tau\sigma_{\max}(1+\bar{\delta}) + \|\Delta\|)^2\ \frac{n}{2^k}$
[(L11), (L13); 2^{k-1} nodes at depth $k-1$ (Fact A.31, item 1)]

(L16) $2^{k-1}\,\Xi^2(\sqrt{2}\,\tau\sigma_{\max}(1+\bar{\delta}) + \|\Delta\|)^2\ \frac{n}{2^k} = \Xi^2(\sqrt{2}\,\tau\sigma_{\max}(1+\bar{\delta}) + \|\Delta\|)^2\ \frac{n}{2}$
[expand]

(L17) $\Rightarrow\ R_k \le \Xi(\sqrt{2}\,\tau\sigma_{\max}(1+\bar{\delta}) + \|\Delta\|)(n/2)^{1/2}$
[(L14), (L15), (L16); $t \mapsto \sqrt{t}$ nondecreasing (Fact A.41, item 5)]

(L18) $\Rightarrow$ the statement

[(L17)]

□

Lemma G.61 (The depth sums of the centers over $\mathbb{R}$ [to table])**.** *Over $\mathbb{R}$, the depth sums of the centers and of the updated centers grow by at most ℓR_k per depth. Let:*

- $h \geq 1$;
- $T \in \mathcal{T}_n$ *at* $n := 2^h$;
- $z \in \mathbb{Z}^N$ *at* $N := 2n$;
- $k \in \{1, \ldots, h\}$.

Define:

- t, *the root node's center;*
- $\mathfrak{T}_k := (\sum_{\mathrm{depth}(\nu)=k-1} \|t_\nu\|^2)^{1/2}$ *(Theorem G.59);*
- $\mathfrak{T}'_k := (\sum_{\mathrm{depth}(\nu)=k-1} \|tb_{0,\nu}\|^2)^{1/2}$ *(Theorem G.59);*
- $R_k := (\sum_{\mathrm{depth}(\nu)=k-1} \|t_{1,\nu} - z_{1,\nu}\|^2)^{1/2}$ *(Theorem G.59);*
- t_ν, $tb_{0,\nu}$, $t_{1,\nu}$ *and* $z_{1,\nu}$, *those of Theorem G.59;*
- $\ell := \max_\psi |l_{10}(\psi)|$ *(Theorem G.59).*

Then the depth sums grow by at most ℓR_k:

1. $\mathfrak{T}'_k \leq \mathfrak{T}_k + \ell R_k$ *[derived];*
2. $\mathfrak{T}_{k+1} \leq \mathfrak{T}_k + \ell R_k$ *[derived].*

Proof. Proof of item 1.

(L1) $tb_{0,\nu} = t_{0,\nu} + (t_{1,\nu} - z_{1,\nu})\, l_{10,\nu}$

[Definition A.21, item 16 over $\mathbb{R}$]

(L2) $\Rightarrow$ $\|tb_{0,\nu}\| \leq \|t_{0,\nu}\| + \ell \|t_{1,\nu} - z_{1,\nu}\|$

[(L1); $\|x+y\| \leq \|x\| + \|y\|$ (Fact A.41, item 3); $|l_{10,\nu}| \leq \ell$ (the statement)]

(L3) $\sum_\nu \|t_{0,\nu}\|^2 \leq \sum_\nu \|t_\nu\|^2$

[$\|t_\nu\|^2 = \|t_{0,\nu}\|^2 + \|t_{1,\nu}\|^2$ (Fact A.41, its lead: $\|(X,Y)\|^2 := \|X\|^2 + \|Y\|^2$)]

(L4) $\sum_{\mathrm{depth}(\nu)=k-1} \|t_\nu\|^2 = \mathfrak{T}_k^2$

[$\mathfrak{T}_k$ (the statement)]

(L5) $\Rightarrow$ $\mathfrak{T}'_k \leq \mathfrak{T}_k + \ell R_k$

[(L2) square-summed over the 2^{k-1} nodes at depth $k-1$; $\|x+y\| \leq \|x\| + \|y\|$ (Fact A.41, item 3) in $\mathbb{R}^{2^{k-1}}$; (L3), (L4)]

(L6) $\Rightarrow$ item 1

[(L5)]

□ (item 1)

Proof of item 2.

(L7) $\forall \nu,\ \mathrm{depth}(\nu) = k-1 :\ \|t_{R(\nu)}\| = \|t_{1,\nu}\|$

[$t_{T_{11}}$ (Definition A.21, item 13) at $T_{11} := R(\nu)$; Proposition G.19, item 1]

(L8) $\forall \nu,\ \mathrm{depth}(\nu) = k-1 :\ \|t_{L(\nu)}\| = \|tb_{0,\nu}\|$

[$t_{T_{00}}$ (Definition A.21, item 17) at $T_{00} := L(\nu)$; Proposition G.19, item 1]

(L9) $\mathfrak{T}_{k+1}^2 = \sum_{\mathrm{depth}(\nu)=k-1} (\|t_{1,\nu}\|^2 + \|tb_{0,\nu}\|^2)$

[$\mathfrak{T}_{k+1}$ over the nodes of depth k (Definition A.18, the subtrees and the depth); (L7), (L8)]

(L10) $\sum_{\mathrm{depth}(\nu)=k-1} (\|t_{1,\nu}\|^2 + \|tb_{0,\nu}\|^2) \leq \sum_{\mathrm{depth}(\nu)=k-1} (\|t_{1,\nu}\|^2 + (\|t_{0,\nu}\| + \ell \|t_{1,\nu} - z_{1,\nu}\|)^2)$

[(L2); Fact A.41, item 5: $t \mapsto t^2$ nondecreasing on $[0, \infty)$]

(L11) $\forall \nu :\ \|t_{1,\nu}\|^2 + \|t_{0,\nu}\|^2 = \|t_\nu\|^2$

[Fact A.41, its lead: $\|(X,Y)\|^2 := \|X\|^2 + \|Y\|^2$]

(L12) $\Rightarrow$ $\mathfrak{T}_{k+1} \le \mathfrak{T}_k + \ell R_k$
[(L9), (L10), (L11); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3) at $x := (\|t_{1,\nu}\|, \|t_{0,\nu}\|)_\nu$, $y := (0, \ell\|t_{1,\nu} - z_{1,\nu}\|)_\nu$]
(L13) $\Rightarrow$ item 2
[(L12)]
□ (item 2)

Corollary G.62 (The center shift on the tail-cut event [to table]). *On the tail-cut event, the center shift, times $1-\gamma-\gamma_S$, is at most D°. Let:*

- *$\mathcal{F}$ be a realization at (u,ζ) (Definition A.4);*
- *$h \ge 1$;*
- *$T \in \mathcal{T}_n$ at $n := 2^h$;*
- *$t \in \mathcal{R}_n \times \mathcal{R}_n$;*
- *$z \in \mathbb{Z}^N$ at $N := 2n$;*
- *$Z \ge 0$;*
- *$\bar{T} \in \mathbb{R}$;*
- *$e_{\text{root}} \in \mathcal{R}_n \times \mathcal{R}_n$;*
- *$\bar{\delta} \in \mathbb{R}$.*

Define:

- *The key constants*
  - *Ξ, Ξ'_{root} and Ξ'_k, those of Definition 4.6, items 13, 10 and 8, at T;*
  - *$\ell := \max_\psi |l_{10}(\psi)|$ (Theorem G.59);*
- *The tail-cut event*
  - *S, that of Theorem 4.3;*
  - *τ, the radius of S (Definition A.26);*
- *The leaf standard deviations*
  - *$\sigma_{\max} := \max_i \sigma_i$;*
- *The centers and the samples*
  - *$\widetilde{t}_T$, the root node's computed input (ffsamp (Algorithm 6), line 1 at $\nu = T$);*
  - *t_ν, $tb_{0,\nu}$, $t_{1,\nu}$, $z_{1,\nu}$, K_0, E_l and c_{merge}, those of Theorem G.59 at $(\mathcal{F}, h, T, t, z)$;*
  - *$\Delta := (\widetilde{t}_i - t_i)_{i \le N}$: $\widetilde{t}_i$ the center $\text{ffSampling}^{\mathcal{F}}$ passes to the base sampler at position i (deepest (Algorithm 7), lines 1 to 18), t_i the center $\text{ffSampling}(t,T)$ sets there over $\mathbb{R}$ (Definition A.21, item 2);*
- *The center shifts*
  - *$c_{\text{split}} := (1+u)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1$ (Lemma G.16);*
  - *k_{split}, K_ζ, G_γ and β_j, those of Theorem G.59 at $(\mathcal{F}, h, T, t, z)$;*
  - *a_j, that of Lemma G.52 at $\mathcal{F}$;*
  - *$R_k := (\sum_{\text{depth}(\nu)=k-1} \|t_{1,\nu} - z_{1,\nu}\|^2)^{1/2}$ and $G_X := u + (1+u)c_{\text{split}}$ (Theorem G.59);*
  - *$G_R := K_0 + G_X E_l$, $G_Z := G_X \ell + G_R + \ell$ and $M_k := (1+c_{\text{merge}})^{h-k} - 1$ (Theorem G.59);*
  - *$\Theta_k := \sqrt{2^{k-1}}(k_{\text{split}}\zeta + K_\zeta + G_Z\, a_{h-k})$ and $\gamma = G_\gamma \sum_{k=1}^h \Xi'_k \beta_{k-1}$ (Theorem G.59);*
  - *Υ_k, R° and c_S under "where";*
  - *$\gamma_S := c_S \sum_{k=1}^h \Xi'_k \Upsilon_k$;*
- *The terms*
  - *$\mathfrak{T}_k := (\sum_{\text{depth}(\nu)=k-1} \|t_\nu\|^2)^{1/2}$ and $\mathfrak{T}'_k = (\sum_{\text{depth}(\nu)=k-1} \|tb_{0,\nu}\|^2)^{1/2}$ (Theorem G.59);*
  - *$D^\circ := \Xi'_{\text{root}} \|e_{\text{root}}\| + \sum_{k=1}^h \Xi'_k [(c_{\text{split}} + G_X)\bar{T} + \Upsilon_k R^\circ + G_Z M_k Z + \Theta_k]$.*

Assume:

(A1) $z \in S$;
(A2) $\|z\| \le Z$;
(A3) $\|t\| \le \bar{T}$;
(A4) $\|\widetilde{t}_T - t\| \le \|e_{\text{root}}\|$;

(A5) $\forall i \le N\ \exists \delta_i \in \mathbb{R},\ |\delta_i| \le \bar{\delta} :\ \widetilde{\sigma}_i = \sigma_i(1+\delta_i)$.
Then the shift is bounded:

$$(1-\gamma-\gamma_S)\|\Delta\| \le D^\circ \qquad \textit{[derived]}$$

where

$$\Upsilon_k = (c_{\text{split}} + G_X)(k-1)\ell + G_X\ell + G_R,$$
$$R^\circ = \sqrt{2}\,\Xi\tau\sigma_{\max}(1+\bar{\delta})(n/2)^{1/2}, \qquad c_S = \Xi(n/2)^{1/2}.$$

Proof. (I1)

Theorem G.59	This proof
Shared: $\mathcal{F}, (u,\zeta),\ h, T, t, z,\ \widetilde{t}_T,\ \Delta,\ \Xi'_{\text{root}}, \Xi'_k,\ \mathfrak{T}_k, \mathfrak{T}'_k, R_k,\ c_{\text{split}}, G_X, G_R, G_Z, M_k, \Theta_k, \gamma$ Shared: $h \ge 1,\ T \in \mathcal{T}_n,\ t \in \mathcal{R}_n \times \mathcal{R}_n,\ z \in \mathbb{Z}^N$	
Z	$\|z\|$
e_{root}	$\widetilde{t}_T - t$
Its conclusion: $(1-\gamma)\|\Delta\| \le \Xi'_{\text{root}}\|e_{\text{root}}\| + \sum_{k=1}^h \Xi'_k\Delta^*_k,\ \Delta^*_k = c_{\text{split}}\mathfrak{T}_k + G_X\mathfrak{T}'_k + G_R R_k + G_Z M_k Z + \Theta_k$	
$(1-\gamma)\|\Delta\| \le \Xi'_{\text{root}}\|e_{\text{root}}\| + \sum_{k=1}^h \Xi'_k[c_{\text{split}}\mathfrak{T}_k + G_X\mathfrak{T}'_k + G_R R_k + G_Z M_k\|z\| + \Theta_k]$	[(I1); $\|\widetilde{t}_T - t\| \le \|e_{\text{root}}\|$ (assumption A4)]

Lemma G.60 at every $k \in \{1,\dots,h\}$	This proof
(I2) Shared: $\mathcal{F}, h, T, z,\ S, \tau, \bar{\delta},\ t,\ \Xi,\ \sigma_{\max},\ \Delta,\ R_k$ Shared: assumptions A1, A5	
Its conclusion: $R_k \le \Xi(\sqrt{2}\,\tau\sigma_{\max}(1+\bar{\delta}) + \|\Delta\|)(n/2)^{1/2}$	

(L2) $\forall k \in \{1,\dots,h\} :\ R_k \le R^\circ + c_S\|\Delta\|$
[(I2); R°, c_S (the statement)]

(L3) $\forall k \in \{1,\dots,h\} :\ \mathfrak{T}'_k \le \mathfrak{T}_k + \ell R_k$
[Lemma G.61, item 1]

(L4) $\forall k \in \{1,\dots,h\} :\ \mathfrak{T}_{k+1} \le \mathfrak{T}_k + \ell R_k$
[Lemma G.61, item 2]

(L5) $\mathfrak{T}_1 = \|t\|$
[$\mathfrak{T}_1$ over the root node (Theorem G.59)]

(L6) $\|t\| \le \bar{T}$
[assumption A3]

(L7) $\forall k \in \{1,\dots,h-1\} :\ \mathfrak{T}_{k+1} \le \mathfrak{T}_k + \ell(R^\circ + c_S\|\Delta\|)$
[(L2), (L4)]

(L8) $\Rightarrow\ \forall k \in \{1,\dots,h\} :\ \mathfrak{T}_k \le \bar{T} + (k-1)\ell(R^\circ + c_S\|\Delta\|)$
[induction on k: (L5), (L6) the base, (L7) the step]

(L9) $\forall k \in \{1,\dots,h\} :\ c_{\text{split}}\mathfrak{T}_k + G_X\mathfrak{T}'_k + G_R R_k \le (c_{\text{split}} + G_X)\bar{T} + \Upsilon_k(R^\circ + c_S\|\Delta\|)$
[(L2), (L3), (L8); $c_{\text{split}}, G_X, G_R \ge 0$ (the statement); Υ_k (the statement): $(c_{\text{split}} + G_X)(k-1)\ell + G_X\ell + G_R$]

(L10) $\forall k \in \{1,\dots,h\} :\ M_k \ge 0$
[M_k (Theorem G.59) at the c_{merge} of Lemma G.18; $u \ge 0$, $\zeta \ge 0$ (Definition A.4); Fact A.41, items 5 and 8]

(L11) $G_Z \ge 0$
[G_Z, G_X, G_R, K_0, E_l, $\widetilde{\ell}$ and ℓ (Theorem G.59) at the c_{split} of Lemma G.16 and the e_{mul} of Lemma G.51; $u \ge 0$, $\zeta \ge 0$ (Definition A.4); $|x| \ge 0$ (Fact A.41, item 1); Fact A.41, items 5 and 8]

(L12) $\forall k \in \{1,\dots,h\} :\ G_Z M_k\|z\| \le G_Z M_k Z$
[assumption A2; (L10), (L11); Fact A.41, item 8]

(L13) $\Rightarrow\ (1-\gamma)\|\Delta\| \le D^\circ + \gamma_S\|\Delta\|$
[(L1), (L9), (L12); $\Xi'_k \ge 0$ (Lemma G.55); D°, γ_S (the statement)]

(L14) $\Rightarrow$ the statement

[(L13); collect]

□

G.6 The base sampler under $\mathcal{F}$

Structure. This subsection proves the bounds on $\bar{\rho}_B$. Lemma G.63 states the base sampler's acceptance over $\mathbb{R}$; Lemma G.64 its output measure over $\mathbb{R}$; Lemma G.65 the second-moment form of the Rényi divergence; Fact G.66 the exact acceptance; Lemma G.68 a leaf's weighted second moment; Section G.6.1 the moment at a leaf, by rows; Corollary G.75 the bounds on $\bar{\rho}_B$.

Lemma G.63 (The base sampler's acceptance over $\mathbb{R}$ [to table])**.** *Over $\mathbb{R}$, the base sampler's acceptance probability is at most 1 when its standard deviation lies in $[\sigma_{\min}, \sigma_0]$. Let:*

- $\sigma > 0$;
- $\sigma_{\min} \in \mathbb{R}$;
- $t \in \mathbb{R}$.

Define, for SamplerZ$(t, 1/\sigma)$ *(Algorithm 8) run over $\mathbb{R}$:*

- *The leaf parameters*
  - $s := \lfloor t \rceil$ *(line 1)*;
  - $r := t - s$ *(line 3)*;
- *The candidates*
  - $z_0 \leftarrow m$, *the table's probability measure* $m(z_0) = \Pr[\texttt{GAUSS0} = z_0]$ *on* $\{0, \ldots, 18\}$ *(line 9)*;
  - $b \leftarrow \{0, 1\}$ *uniform (line 8)*;
  - $z := b + (2b - 1)z_0$ *(line 10)*;
  - $\bar{z}_0(z) := |z - [z > 0]|$;
- *The exponent*
  - $\sigma_0 := 1.8205$;
  - $x(z) := (z - r)^2/(2\sigma^2) - \bar{z}_0(z)^2/(2\sigma_0^2)$ *(line 16)*;
- *The acceptance*
  - $ccs := \sigma_{\min}/\sigma$ *(line 7)*;
  - $acc(z) := ccs\, e^{-x(z)}$ *(line 18)*.

Assume:
(A1) $\sigma \geq \sigma_{\min}$;
(A2) $\sigma \leq \sigma_0$.
Then the acceptance is a probability:

$$\forall z : \ acc(z) \leq 1.$$

Proof. (L1) $r \in [0, 1)$

[$r = t - \lfloor t \rceil$ (the statement)]

(L2) $b = 0 \Rightarrow z = -z_0$

[z (the statement)]

(L3) $b = 0 \Rightarrow (z - r)^2 = (z_0 + r)^2$

[(L2)]

(L4) $(z_0 + r)^2 \geq z_0^2$

[(L1); $z_0 \geq 0$ (the statement)]

(L5) $b = 1 \Rightarrow z = z_0 + 1$

[z (the statement)]

(L6) $b = 1 \Rightarrow (z - r)^2 = (z_0 + 1 - r)^2$

[(L5)]

(L7) $(z_0 + 1 - r)^2 \geq z_0^2$

[(L1); $z_0 \geq 0$ (the statement)]

(L8) $\Rightarrow$ $\forall z:\ (z-r)^2 \geq \bar{z}_0(z)^2$

[(L2) to (L7); $\bar{z}_0(z)$ (the statement)]

(L9) $\Rightarrow$ $x(z) \geq \bar{z}_0(z)^2(1/(2\sigma^2) - 1/(2\sigma_0^2))$

[$x(z)$ (the statement); (L8)]

(L10) $\bar{z}_0(z)^2(1/(2\sigma^2) - 1/(2\sigma_0^2)) \geq 0$

[$\sigma \leq \sigma_0$ (assumption A2)]

(L11) $ccs = \sigma_{\min}/\sigma$

[ccs (the statement)]

(L12) $\sigma_{\min}/\sigma \leq 1$

[$\sigma \geq \sigma_{\min}$ (assumption A1)]

(L13) $\Rightarrow$ the statement

[(L9) to (L12); $acc = ccs\, e^{-x}$ (the statement); $e^{-x} \leq e^0$, $e^0 = 1$ (exp increasing, Fact A.41, item 5)]

□

Lemma G.64 (The base sampler's output measure over $\mathbb{R}$ [to table])**.** *Over $\mathbb{R}$, the base sampler's output follows the Gaussian at the center weighted by the table's weight. Let:*

- $\sigma > 0$;
- $\sigma_{\min} > 0$;
- $t \in \mathbb{R}$.

Define, for SamplerZ$(t, 1/\sigma)$ *(Algorithm 8) run over $\mathbb{R}$:*

- *The leaf parameters*
  - $s := \lfloor t \rfloor$ *(line 1)*;
  - $r := t - s$ *(line 3)*;
- *The candidates*
  - $z_0 \leftarrow m$, *the table's probability measure* $m(z_0) = \Pr[\texttt{GAUSS0} = z_0]$ *on* $\{0, \ldots, 18\}$ *(line 9)*;
  - $b \leftarrow \{0,1\}$ *uniform (line 8)*;
  - $z := b + (2b-1)z_0$ *(line 10)*;
  - $\bar{z}_0(z) := |z - [z > 0]|$;
- *The exponent*
  - $\sigma_0 := 1.8205$;
  - $x(z) := (z-r)^2/(2\sigma^2) - \bar{z}_0(z)^2/(2\sigma_0^2)$ *(line 16)*;
- *The acceptance*
  - $ccs := \sigma_{\min}/\sigma$ *(line 7)*;
  - $acc(z) := ccs\, e^{-x(z)}$ *(line 18)*;
- *The table*
  - ρ_σ, *that of Definition A.2*;
  - $w(z_0) := m(z_0)\, \rho_{\sigma_0}(\mathbb{Z}_{\geq 0})/\rho_{\sigma_0}(z_0)$;
- *The probability measures*
  - $\forall A \subseteq \mathbb{Z}:\ P_0(A) := \Pr[s + z \in A]$.

Assume:

(A1) $\sigma \geq \sigma_{\min}$;

(A2) $\sigma \leq \sigma_0$.

Then the exponent and the output's probability measure satisfy:

1. $\bar{z}_0(z) = z_0$ *and* $x(z) = (z-r)^2/(2\sigma^2) - z_0^2/(2\sigma_0^2)$;
2. $P_0(s+z) = \dfrac{\rho_\sigma(z-r)\, w(\bar{z}_0(z))}{\sum_{z'} \rho_\sigma(z'-r)\, w(\bar{z}_0(z'))}$.

Proof.

DEFINES $q(z) := m(\bar{z}_0(z))/2$

Proof of item 1.

(L1) $b = 1 \Rightarrow\ z = z_0 + 1 > 0$

[$z = b + (2b-1)z_0$, $z_0 \geq 0$ (the statement)]

(L2) $b = 1 \Rightarrow\ \bar{z}_0(z) = z_0$

[(L1); $\bar{z}_0(z) = |z - [z > 0]|$ (the statement)]

(L3) $b = 0 \Rightarrow\ \bar{z}_0(z) = z_0$

[$z = -z_0$, $-z_0 \leq 0$ at $b = 0$ ($z = b + (2b-1)z_0$, $z_0 \geq 0$, line 10); $\bar{z}_0(z) = |z - [z > 0]|$ (the statement)]

(L4) $\Rightarrow\ \bar{z}_0(z) = z_0$

[(L2), (L3); $b \in \{0, 1\}$ (the statement)]

(L5) $x(z) = (z - r)^2/(2\sigma^2) - z_0^2/(2\sigma_0^2)$

[$x(z)$ (the statement); (L4)]

(L6) $\Rightarrow$ item 1

[(L4), (L5)]

□ (item 1)

Proof of item 2.

(L7) $\forall z:\ acc(z) > 0$

[$ccs = \sigma_{\min}/\sigma$, $\sigma_{\min}/\sigma > 0$ at $\sigma_{\min}, \sigma > 0$ (the statement); $e^{-x(z)} > 0$ (Fact A.41, item 12); acc (the statement)]

Lemma G.63	This proof
(I1)	Shared: $\sigma, \sigma_{\min}, t,\ s, r, z_0, b, z,\ \bar{z}_0, \sigma_0, x, ccs, acc$ Shared: assumptions A1, A2
	Its conclusion: $\forall z:\ acc(z) \leq 1$

(L8) $\forall z:\ acc(z) \leq 1$

[(I1)]

(L9) $\sum_{z'} q(z')\, acc(z') > 0$

[(L7); $q(z') = m(\bar{z}_0(z'))/2$ (the proof's block); $q \geq 0$, and $q(z') > 0$ at some z' (m a probability measure, the statement)]

(L10) $P_0(s + z) = q(z)\, acc(z) \Big/ \sum_{z'} q(z')\, acc(z')$

[Fact A.45, item 4, its acc with values in $[0, 1]$ by (L7), (L8) and its $\sum_{z'} q(z')\, acc(z') > 0$ by (L9); q (the proof's block); acc (the statement)]

(L11) $e^{-x(z)} = e^{-(z-r)^2/(2\sigma^2)} e^{z_0^2/(2\sigma_0^2)}$

[(L5); Fact A.41, item 12: $e^x e^y = e^{x+y}$]

(L12) $\Rightarrow\ q(z)\, acc(z) = \frac{ccs}{2}\, m(z_0)\, e^{z_0^2/(2\sigma_0^2)}\, \rho_\sigma(z - r)$

[(L11); q (the proof's block), its $m(\bar{z}_0(z)) = m(z_0)$ by (L4); acc (the statement); Definition A.2, item 1, at $(s, c) := (\sigma, 0)$]

(L13) $m(z_0)\, e^{z_0^2/(2\sigma_0^2)} = w(z_0)/\rho_{\sigma_0}(\mathbb{Z}_{\geq 0})$

[$w(z_0) = m(z_0)\rho_{\sigma_0}(\mathbb{Z}_{\geq 0})/\rho_{\sigma_0}(z_0)$ (the statement); Definition A.2, item 1, at $(s, c) := (\sigma_0, 0)$]

(L14) $z_0 \leq 18$

[m on $\{0, \ldots, 18\}$ (the statement)]

(L15) $z \in [-18, 19]$

[$z = b + (2b-1)z_0$, $b \in \{0, 1\}$ (the statement); (L14)]

(L16) $\Rightarrow$ item 2

[(L10), (L12), (L13), (L15); collect]

□ (item 2)

The base sampler's table. The table is read as integers from the three 31-, 24- and 24-bit chunks of each row [L0: `sign_sampler.c:87-107`] [L0: `fxp/sign_fxsampler.c:33-68`]. The exact mass beyond $z_0 = 18$ is $2^{-80.04}$ (the support truncation); the worst $|w - 1|$ over $z_0 \leq 15$ is 7.468e-11.

`verify/reports/sampler/table.py` The table's relative deviation is the rounding of a 79-bit cumulative table: a row's mass is a difference of two rounded values, so its absolute perturbation is below 2^{-78} and its relative perturbation grows as the mass shrinks. [derived]

Lemma G.65 (The weighted sum of the ratio's power [to table])**.** *On a set $\mathcal{Y}$, the weighted sum of the ratio's power is at most* 1 *plus a term on $\mathcal{Y}$'s complement and a term in the weighted second moment on $\mathcal{Y}$. Let:*

- $\alpha \geq 2$;
- B *and* D, *probability measures on* $\mathbb{Z}$;
- $\mathcal{Y} \subseteq \mathbb{Z}$.

Define:

- $U(z) := \begin{cases} B(z)/D(z) & z \in \mathrm{Supp}(B) \\ 0 & z \notin \mathrm{Supp}(B) \end{cases}$;
- $\epsilon := U - 1$;
- $\epsilon_+ := \max(\epsilon, 0)$;
- $\epsilon_{\mathcal{Y}} := \sup_{z \in \mathcal{Y}^c} \max(1 - U(z), 0)$;
- $M_{\alpha,\mathcal{Y}} := \sum_{z \in \mathcal{Y}} D(z)(1 + \epsilon_+(z))^{\alpha-2}\epsilon(z)^2$.

Assume:

(A1) $\mathrm{Supp}(B) \subseteq \mathrm{Supp}(D)$;

(A2) $M_{\alpha,\mathcal{Y}} < \infty$.

Then

$$\sum_{z \in \mathcal{Y}} D(z)\, U(z)^\alpha \leq 1 + \alpha\, D(\mathcal{Y}^c)\, \epsilon_{\mathcal{Y}} + \tfrac{\alpha(\alpha-1)}{2}\, M_{\alpha,\mathcal{Y}}.$$

Proof.

(L1) $\forall \epsilon \geq -1 :\ (1+\epsilon)^\alpha \leq 1 + \alpha\epsilon + \frac{\alpha(\alpha-1)}{2}(1+\epsilon_+)^{\alpha-2}\epsilon^2$
[Fact A.41, item 6; $\epsilon_+ = \max(\epsilon, 0)$ (the statement)]

(L2) $\Rightarrow\ \sum_{z \in \mathcal{Y}} D\, U^\alpha \leq D(\mathcal{Y}) + \alpha \sum_{z \in \mathcal{Y}} D\, \epsilon + \frac{\alpha(\alpha-1)}{2} M_{\alpha,\mathcal{Y}}$
[(L1) at $U = 1 + \epsilon$, multiplied by $D(z) \geq 0$ and summed over $z \in \mathcal{Y}$; $M_{\alpha,\mathcal{Y}}$ (the statement); the sum finite by assumption A2]

(L3) $\forall z :\ D(z)\, \epsilon(z) = B(z) - D(z)$
[U, ϵ (the statement); $\mathrm{Supp}(B) \subseteq \mathrm{Supp}(D)$ (assumption A1)]

(L4) $\sum_z B(z) = 1$
[B a probability measure (the statement)]

(L5) $\sum_z D(z) = 1$
[D a probability measure (the statement)]

(L6) $\Rightarrow\ \sum_{z \in \mathcal{Y}} D\, \epsilon = B(\mathcal{Y}) - D(\mathcal{Y})$
[(L3)]

(L7) $B(\mathcal{Y}) - D(\mathcal{Y}) = D(\mathcal{Y}^c) - B(\mathcal{Y}^c)$
[(L4), (L5)]

(L8) $D(\mathcal{Y}^c) - B(\mathcal{Y}^c) = \sum_{z \in \mathcal{Y}^c} D\,(1 - U)$
[(L3); $\epsilon = U - 1$ (the statement)]

(L9) $\forall z \in \mathcal{Y}^c :\ D(z)(1 - U(z)) \leq D(z) \max(1 - U(z), 0)$
[$D \geq 0$ (the statement)]

(L10) $\forall z \in \mathcal{Y}^c :\ D(z) \max(1 - U(z), 0) \leq D(z)\, \epsilon_{\mathcal{Y}}$
[$D \geq 0$ (the statement); $\epsilon_{\mathcal{Y}}$ (the statement)]

(L11) $\Rightarrow\ \sum_{z \in \mathcal{Y}^c} D\,(1 - U) \leq D(\mathcal{Y}^c)\, \epsilon_{\mathcal{Y}}$
[(L9), (L10), summed over $z \in \mathcal{Y}^c$]

(L12) $D(\mathcal{Y}) \leq 1$
[(L5); $D \geq 0$ (the statement)]

(L13) $\Rightarrow$ the statement
[(L2), (L6), (L7), (L8), (L11), (L12)]

□

The Rényi divergence of the table, measured. At $B = P_0$, $D = D_{\mathbb{Z},\sigma,\mu}$ and $\mathcal{Y} = \mathbb{Z}$, `verify/reports/sampler/renyi.py` cross-checks Lemma G.65 by brute force at sampled parameters, with $\ln R_\alpha = \ln \sum_z D(z)U(z)^\alpha/(\alpha-1)$ computed in the log domain at 60 digits: the Rényi divergence is far below the pointwise $\max_z U(z) - 1$, set by row 18 of the table.

Fact G.66 (The exact acceptance [to table])**.** The acceptance of BerExp is its acceptance word over 2^{64}. Let:

- $si \in \mathbb{Z}$;
- $r' \in \mathbb{R}$;
- ccs be the scale BerExp (Algorithm 9) takes (line 6 of SamplerZ (Algorithm 8)).

Define:

- $s_x := \min(si, 63)$;
- $z_{\mathrm{acc}} := ((\texttt{expm_p63}(r', ccs) \ll 1) - 1) \gg s_x$, the 64-bit word of line 13;
- $\widetilde{acc}(si, r', ccs) := \Pr_w[w < z_{\mathrm{acc}}]$, w uniform on $\{0, \ldots, 2^{64} - 1\}$, the acceptance of line 18.

Assume:

(A1) $si \geq 0$.

Then

$$\widetilde{acc}(si, r', ccs) = z_{\mathrm{acc}}/2^{64}.$$

Lemma G.67 (The sampler's relative perturbation and its weight [to table])**.** *At a leaf, the sampler's relative perturbation factors through the table's and the acceptance's, and so does its weight. Let:*

- $\alpha \geq 2$;
- $\sigma_{\min} > 0$;
- $\widetilde{\sigma} > 0$, *a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$, *its computed center.*

Define:

- *The signer's words and parameters*
  - $\sigma_0 := 1.8205$ *(Lemma G.64);*
- *The probability measures*
  - $\widetilde{B}(A) := \Pr[z \in A]$ *for* $z \leftarrow \mathrm{SamplerZ}(\widetilde{t}, 1/\widetilde{\sigma})$ *in* $\mathcal{F}$ *(Algorithm 8);*
  - $\widetilde{D} := D_{\mathbb{Z},\widetilde{\sigma},\widetilde{t}}$;
  - P_0, *the probability measure of Lemma G.64 at* $(\sigma, t) := (\widetilde{\sigma}, \widetilde{t})$;
- *The relative perturbations*
  - $\epsilon := \widetilde{B}/\widetilde{D} - 1$;
  - $\epsilon_{\mathrm{tab}} := P_0/\widetilde{D} - 1$;
  - $\epsilon_{\mathrm{ar}}(y) := \begin{cases} \widetilde{B}(y)/P_0(y) - 1 & y \in \mathrm{Supp}(P_0) \\ 0 & y \notin \mathrm{Supp}(P_0) \end{cases}$;
  - $x_+ := \max(x, 0)$ *at* $x \in \{\epsilon, \epsilon_{\mathrm{tab}}, \epsilon_{\mathrm{ar}}\}$;
- *The weights*
  - $w_{\mathrm{tab}} := (1 + \epsilon_{\mathrm{tab},+})^{\alpha-2}$;
  - $w_{\mathrm{ar}} := (1 + \epsilon_{\mathrm{ar},+})^{\alpha-2}$.

Assume:

(A1) $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$.

Then the perturbation factors and its weight is bounded:

1. $\forall y: \ \epsilon = \epsilon_{\mathrm{tab}} + \epsilon_{\mathrm{ar}}(1 + \epsilon_{\mathrm{tab}})$;
2. $(1 + \epsilon_+)^{\alpha-2} \leq w_{\mathrm{tab}} w_{\mathrm{ar}}$.

Proof. (L1) $1 + \epsilon = \widetilde{B}/\widetilde{D}$ [ϵ (the statement)]

	Lemma G.64 at $(\sigma, t) := (\widetilde{\sigma}, \widetilde{t})$	This proof
	Shared: $\sigma_{\min},\ \sigma_0, P_0$	
	Shared: $\sigma_{\min} > 0,\ t \in \mathbb{R}$	
	σ	$\widetilde{\sigma}$ (the statement)
	t	$\widetilde{t}$ (the statement)
(I1)	$\sigma > 0$	$\widetilde{\sigma} > 0$ (the statement)
	Assumption A1	Assumption A1
	Assumption A2	Assumption A1
	Its item 1: $\bar{z}_0(z) = z_0$ and $x(z) = (z-r)^2/(2\sigma^2) - z_0^2/(2\sigma_0^2)$	
	Its item 2: $P_0(s+z) = \frac{\rho_\sigma(z-r)\, w(\bar{z}_0(z))}{\sum_{z'} \rho_\sigma(z'-r)\, w(\bar{z}_0(z'))}$	

(L2) $\bar{z}_0(z) = z_0$

[item 1 of (I1)]

(L3) $\forall z \in \mathbb{Z}:\ P_0(s+z) = \frac{\rho_{\widetilde{\sigma}}(z-r)\, w(\bar{z}_0(z))}{\sum_{z'} \rho_{\widetilde{\sigma}}(z'-r)\, w(\bar{z}_0(z'))}$

[item 2 of (I1)]

(L4) $\forall z \in \mathbb{Z}:\ P_0(s+z) > 0 \iff m(\bar{z}_0(z)) > 0$

[(L3); $\rho_{\widetilde{\sigma}} > 0$ (Fact A.41, item 12); $w(z_0) > 0 \iff m(z_0) > 0$ (w, Lemma G.64)]

(L5) $\forall z \in \mathbb{Z}:\ \widetilde{B}(s+z) > 0 \Rightarrow\ m(\bar{z}_0(z)) > 0$

[$z = b + (2b-1)z_0$, $z_0 \leftarrow m$ (SamplerZ (Algorithm 8), lines 9 and 10), in $\mathcal{F}$ as over $\mathbb{R}$; (L2)]

(L6) $\Rightarrow\ \forall y \notin \mathrm{Supp}(P_0):\ \widetilde{B}(y) = 0$

[(L4), (L5); $\widetilde{B} \geq 0$ (the statement)]

(L7) $\forall y \in \mathrm{Supp}(P_0):\ \widetilde{B}/\widetilde{D} = (\widetilde{B}/P_0)(P_0/\widetilde{D})$

[expand]

(L8) $\forall y \in \mathrm{Supp}(P_0):\ (\widetilde{B}/P_0)(P_0/\widetilde{D}) = (1+\epsilon_{\mathrm{ar}})(1+\epsilon_{\mathrm{tab}})$

[ϵ_{tab}, ϵ_{ar} (the statement)]

(L9) $\forall y \notin \mathrm{Supp}(P_0):\ \epsilon(y) = -1$

[(L1), (L6)]

(L10) $\forall y \notin \mathrm{Supp}(P_0):\ \epsilon_{\mathrm{tab}}(y) = -1$

[ϵ_{tab} (the statement) at $P_0(y) = 0$]

(L11) $\forall y \notin \mathrm{Supp}(P_0):\ \epsilon_{\mathrm{ar}}(y) = 0$

[ϵ_{ar} (the statement)]

(L12) $\Rightarrow\ \forall y:\ \epsilon = \epsilon_{\mathrm{tab}} + \epsilon_{\mathrm{ar}}(1+\epsilon_{\mathrm{tab}})$

[(L1), (L7), (L8) on $\mathrm{Supp}(P_0)$; (L9), (L10), (L11) off it; expand]

(L13) $\Rightarrow$ item 1

[(L12)]

(L14) $P_0 \geq 0$

[P_0 a probability measure (Lemma G.64)]

(L15) $\widetilde{B} \geq 0$

[$\widetilde{B}$ a probability measure (the statement)]

(L16) $\widetilde{D} > 0$

[$\widetilde{D}$ (the statement), $D_{\mathbb{Z},s,c}$ (Definition A.2, items 2 and 1) at $(s,c) := (\widetilde{\sigma}, \widetilde{t})$: $\rho_{\widetilde{\sigma}} > 0$ (Fact A.41, item 12: $e^t > 0$)]

(L17) $\epsilon_{\mathrm{tab}} \geq -1$

[ϵ_{tab} (the statement); (L14), (L16)]

(L18) $\epsilon_{\mathrm{ar}} \geq -1$

[ϵ_{ar} (the statement), 0 off $\mathrm{Supp}(P_0)$; (L14), (L15)]

(L19) $\forall x \in \{\epsilon, \epsilon_{\mathrm{tab}}, \epsilon_{\mathrm{ar}}\}:\ 1 + x \leq 1 + x_+$

[x_+ (the statement)]

(L20) $1 + \epsilon_+ \leq (1+\epsilon_{\mathrm{tab},+})(1+\epsilon_{\mathrm{ar},+})$

[(L12), (L17), (L18), (L19); Fact A.41, item 8]

(L21) $\Rightarrow$ $(1+\epsilon_+)^{\alpha-2} \le w_{\text{tab}} w_{\text{ar}}$

[(L20); $t \mapsto t^{\alpha-2}$ nondecreasing on $[0,\infty)$ at $\alpha \ge 2$ (Fact A.41, item 5); w_{tab}, w_{ar} (the statement)]

(L22) $\Rightarrow$ item 2

[(L21)]

□

Lemma G.68 (A leaf's weighted second moment on a set [to table])**.** *At a leaf, the weighted second moment of the sampler's relative perturbation on a set is at most the square of the sum of the square roots of the table's and the acceptance's moments. Let:*

- $\alpha \ge 2$;
- $\sigma_{\min} > 0$;
- $\widetilde{\sigma} > 0$, *a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$, *its computed center;*
- $\mathcal{Y} \subseteq \mathbb{Z}$.

Define:

- *The signer's words and parameters*
  - $\sigma_0 := 1.8205$ *(Lemma G.64);*
- *The probability measures*
  - $\widetilde{B}(A) := \Pr[z \in A]$ *for* $z \leftarrow \text{SamplerZ}(\widetilde{t}, 1/\widetilde{\sigma})$ *in* $\mathcal{F}$ *(Lemma G.67);*
  - $\widetilde{D} := D_{\mathbb{Z},\widetilde{\sigma},\widetilde{t}}$ *(Lemma G.67);*
  - P_0, *the probability measure of Lemma G.64 at* $(\sigma, t) := (\widetilde{\sigma}, \widetilde{t})$;
- *The relative perturbations*
  - $\epsilon := \widetilde{B}/\widetilde{D} - 1$ *(Lemma G.67);*
  - $\epsilon_{\text{tab}} := P_0/\widetilde{D} - 1$ *(Lemma G.67);*
  - $\epsilon_{\text{ar}}(y) := \begin{cases} \widetilde{B}(y)/P_0(y) - 1 & y \in \text{Supp}(P_0) \\ 0 & y \notin \text{Supp}(P_0) \end{cases}$ *(Lemma G.67);*
  - $x_+ := \max(x, 0)$ *at* $x \in \{\epsilon, \epsilon_{\text{tab}}, \epsilon_{\text{ar}}\}$ *(Lemma G.67);*
- *The weights*
  - $w_{\text{tab}} := (1+\epsilon_{\text{tab},+})^{\alpha-2}$ *(Lemma G.67);*
  - $w_{\text{ar}} := (1+\epsilon_{\text{ar},+})^{\alpha-2}$ *(Lemma G.67);*
- *The moments*
  - $M_{\alpha,\mathcal{Y}} := \sum_{z\in\mathcal{Y}} \widetilde{D}(z)(1+\epsilon_+)^{\alpha-2}\epsilon^2$, *that of Lemma G.65 at* $B := \widetilde{B}$, $D := \widetilde{D}$;
  - $M_{\text{tab},\mathcal{Y}} := \sum_{z\in\mathcal{Y}} \widetilde{D}\, w_{\text{tab}} w_{\text{ar}} \epsilon_{\text{tab}}^2$;
  - $M_{\text{ar},\mathcal{Y}} := \sum_{z\in\mathcal{Y}} \widetilde{D}\, w_{\text{tab}} w_{\text{ar}} \epsilon_{\text{ar}}^2 (1+\epsilon_{\text{tab}})^2$.

Assume:

(A1) $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$;
(A2) $M_{\alpha,\mathcal{Y}} < \infty$;
(A3) $M_{\text{tab},\mathcal{Y}} < \infty$;
(A4) $M_{\text{ar},\mathcal{Y}} < \infty$.

Then

$$M_{\alpha,\mathcal{Y}} \le \left(\sqrt{M_{\text{tab},\mathcal{Y}}} + \sqrt{M_{\text{ar},\mathcal{Y}}}\right)^2.$$

Proof. (L1) $M_{\alpha,\mathcal{Y}} = \sum_{z\in\mathcal{Y}} \widetilde{D}(1+\epsilon_+)^{\alpha-2}\epsilon^2$

[$M_{\alpha,\mathcal{Y}}$ (the statement)]

Lemma G.67	This proof
Shared: $\alpha, \sigma_{\min}, \widetilde{\sigma}, \widetilde{t},\ \sigma_0,\ \widetilde{B}, \widetilde{D}, P_0,\ \epsilon, \epsilon_{\text{tab}}, \epsilon_{\text{ar}}, x_+, w_{\text{tab}}, w_{\text{ar}}$	
(I1) Shared: assumption A1	
Its item 1: $\forall y:\ \epsilon = \epsilon_{\text{tab}} + \epsilon_{\text{ar}}(1+\epsilon_{\text{tab}})$	
Its item 2: $(1+\epsilon_+)^{\alpha-2} \le w_{\text{tab}} w_{\text{ar}}$	
(L2) $\sum_{z\in\mathcal{Y}} \widetilde{D}(1+\epsilon_+)^{\alpha-2}\epsilon^2 \le \sum_{z\in\mathcal{Y}} \widetilde{D}\, w_{\text{tab}} w_{\text{ar}} (\epsilon_{\text{tab}} + \epsilon_{\text{ar}}(1+\epsilon_{\text{tab}}))^2$	[items 1 and 2 of (I1)]
(L3) $\Rightarrow$ the statement	[(L1), (L2); $\|X+Y\| \le \|X\| + \|Y\|$ (Fact A.41, item 3, in $L^2(w_{\text{tab}} w_{\text{ar}}\, \widetilde{D})$ over $z \in \mathcal{Y}$) at $X := \epsilon_{\text{tab}}$, $Y := \epsilon_{\text{ar}}(1+\epsilon_{\text{tab}})$; $M_{\text{tab},\mathcal{Y}}$, $M_{\text{ar},\mathcal{Y}}$ (the statement); the sums finite by assumptions A2, A3, A4]
	□

G.6.1 The moment at a leaf, by rows

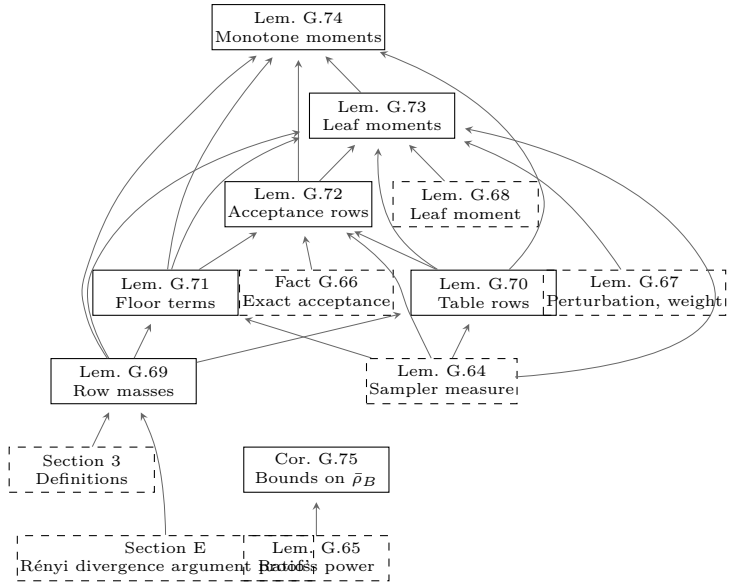


Figure 58: Dependencies, Section G.6.1.

Lemma G.69 (A leaf's normalizer and row masses [to table])**.** *At a leaf, the normalizer has a floor, each row of two integers has a mass ceiling, and the tail cut reaches only the first rows. Let:*

- $\sigma_{\min} > 0$*;*
- $\sigma_{\max} \in [\sigma_{\min}, 2]$*;*
- $\widetilde{\sigma} > 0$*, a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$*, its computed center.*

Define:

- *The rows*
  - $\bar{z}_0(z) := |z - [z > 0]|$ *(Lemma G.64);*
  - $s := \lfloor \widetilde{t} \rceil$*;*
  - $r := \widetilde{t} - s$*;*
  - $\widetilde{D} := D_{\mathbb{Z},\widetilde{\sigma},\widetilde{t}}$*;*
  - $k(y) := \bar{z}_0(y - s)$*, the row of* $y \in \mathbb{Z}$*;*
  - $V_k = \{\, y : k(y) = k \,\} = \{s - k,\ s + k + 1\}$*,* $k \ge 0$*;*
- *The normalizer*
  - $\bar{\varepsilon}_0 := 2e^{-2\pi^2\sigma_{\min}^2}/(1 - e^{-2\pi^2\sigma_{\min}^2})$*;*

- *The row masses*
  - $\forall k \geq 0 :\ \bar{D}_k := \begin{cases} 2/(\sqrt{2\pi}\,\sigma_{\min}(1-\bar{\varepsilon}_0)) & k \leq 1 \\ (\rho_{\sigma_{\max}}(k) + \rho_{\sigma_{\max}}(k+1))/(\sqrt{2\pi}\,\sigma_{\max}(1-\bar{\varepsilon}_0)) & k \geq 2 \end{cases}$;
- *The tail cut*
  - $\mathcal{Z} := \{\, y \in \mathbb{Z} : |y - \widetilde{t}| \leq \tau\widetilde{\sigma} \,\}$;
  - $k_\tau := \lfloor \tau\sigma_{\max} \rfloor$.

Assume:

(A1) $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_{\max}]$.

Then the normalizer, the rows and the tail cut satisfy:

1. $\rho_{\widetilde{\sigma},\widetilde{t}}(\mathbb{Z}) \geq \sqrt{2\pi}\,\widetilde{\sigma}(1-\bar{\varepsilon}_0)$;
2. $\forall k \geq 0 :\ \widetilde{D}(V_k) \leq \bar{D}_k$;
3. $\forall k \geq 0\ \forall y \in V_k :\ |y - \widetilde{t}| \in [k, k+1]$;
4. $\forall k \geq 0\ \forall y \in \mathcal{Z} \cap V_k :\ k \leq k_\tau$.

Proof. (L1) $\varepsilon_0(\sigma_{\min}) = 2\sum_{k\geq 1} e^{-2\pi^2\sigma_{\min}^2 k^2}$

[ε_0 (Definition A.38)]

(L2) $\forall k \geq 1 :\ k^2 \geq k$

[$k \geq 1$]

(L3) $2\sum_{k\geq 1} e^{-2\pi^2\sigma_{\min}^2 k^2} \leq 2\sum_{k\geq 1} e^{-2\pi^2\sigma_{\min}^2 k}$

[(L2); exp increasing (Fact A.41, item 5)]

(L4) $2\sum_{k\geq 1} e^{-2\pi^2\sigma_{\min}^2 k} = \bar{\varepsilon}_0$

[Fact A.41, item 7, at $\omega := e^{-2\pi^2\sigma_{\min}^2}$, $N \to \infty$; $\bar{\varepsilon}_0$ (the statement)]

(I1)

Lemma E.2, item 2	This proof
Shared: ε_0	
s	$\widetilde{\sigma}$
c	$\widetilde{t}$
$s > 0$	$\widetilde{\sigma} > 0$ (the statement)
$c \in \mathbb{R}$	$\widetilde{t} \in \mathbb{R}$ (the statement)
Its item 2: $\forall s > 0\ \forall c \in \mathbb{R} :\ \lvert d(s,c)\rvert \leq \varepsilon_0(s)$	

(L5) $\rho_{\widetilde{\sigma},\widetilde{t}}(\mathbb{Z}) \geq \sqrt{2\pi}\,\widetilde{\sigma}(1-\bar{\varepsilon}_0)$

[(I1); Fact E.4 at $\sigma_{\min} \leq \widetilde{\sigma}$ (assumption A1); (L1), (L3), (L4)]

(L6) $\Rightarrow$ item 1

[(L5)]

(L7) $\forall k \leq 1 :\ \widetilde{D}(V_k) \leq \bar{D}_k$

[(L5); Definition A.2, item 1, at $(s,c) := (\widetilde{\sigma}, 0)$, at both points of V_k, $e^{-y^2/(2\widetilde{\sigma}^2)} \leq 1$ (exp increasing, Fact A.41, item 5); $\widetilde{\sigma} \geq \sigma_{\min}$ (assumption A1); $\bar{D}_k$ (the statement)]

(L8) $\forall y :\ \rho''_{\widetilde{\sigma}}(y) = (y^2 - \widetilde{\sigma}^2)\rho_{\widetilde{\sigma}}(y)/\widetilde{\sigma}^4$

[Definition A.2, item 1, at $(s,c) := (\widetilde{\sigma}, 0)$; differentiate twice]

(L9) $\forall y \geq \widetilde{\sigma} :\ (y^2 - \widetilde{\sigma}^2)\rho_{\widetilde{\sigma}}(y)/\widetilde{\sigma}^4 \geq 0$

[$y^2 \geq \widetilde{\sigma}^2$ ($y \geq \widetilde{\sigma}$, the line's quantifier; Fact A.41, item 5); $\rho_{\widetilde{\sigma}} > 0$ (Fact A.41, item 12)]

(L10) $\Rightarrow$ $\rho_{\widetilde{\sigma}}$ convex on $[\widetilde{\sigma}, \infty)$

[(L8), (L9)]

(L11) $\forall k \geq 2 :\ \rho_{\widetilde{\sigma}}(k+r) + \rho_{\widetilde{\sigma}}(k+1-r) \leq \rho_{\widetilde{\sigma}}(k) + \rho_{\widetilde{\sigma}}(k+1)$

[(L10); $\widetilde{\sigma} \leq \sigma_{\max}$, $\sigma_{\max} \leq 2$, $2 \leq k$ (the statement); $r \in [0,1)$ (r, the statement)]

(L12) $\forall y\ \forall s > 0 :\ \partial_s(\rho_s(y)/s) = (y^2 - s^2)\rho_s(y)/s^4$

[Definition A.2, item 1, at $c := 0$; differentiate in s]

(L13) $\forall y \geq s > 0 :\ (y^2 - s^2)\rho_s(y)/s^4 \geq 0$

[$y^2 \geq s^2$ ($y \geq s$, $s > 0$, the line's quantifier; Fact A.41, item 5); $\rho_s > 0$ (Fact A.41, item 12)]

(L14) $\Rightarrow$ $\forall y \geq s' \geq s > 0:\ \rho_s(y)/s \leq \rho_{s'}(y)/s'$
[$s \mapsto \rho_s(y)/s$ nondecreasing on $(0, y]$ ((L12), (L13); Fact A.41, item 5)]

(L15) $\Rightarrow$ $\forall k \geq 2:\ \widetilde{D}(V_k) \leq \bar{D}_k$
[(L5), (L11), (L14) at $(s, s') := (\widetilde{\sigma}, \sigma_{\max})$, $\widetilde{\sigma} \leq \sigma_{\max}$, $\sigma_{\max} \leq k$; $\widetilde{D}$ (the statement); $\bar{D}_k$ (the statement)]

(L16) $\forall k \geq 0:\ \widetilde{D}(V_k) \leq \bar{D}_k$
[(L7), (L15)]

(L17) $\Rightarrow$ item 2
[(L16)]

(L18) $\forall k\ \forall y \in V_k:\ |y - \widetilde{t}| \in \{k + r,\ k + 1 - r\}$
[V_k, r (the statement)]

(L19) $\{k + r,\ k + 1 - r\} \subseteq [k, k + 1]$
[$r \in [0, 1)$ (r, the statement)]

(L20) $\Rightarrow$ $\forall k \geq 0\ \forall y \in V_k:\ |y - \widetilde{t}| \in [k, k + 1]$
[(L18), (L19)]

(L21) $\Rightarrow$ item 3
[(L20)]

(L22) $\forall y \in \mathcal{Z}:\ |y - \widetilde{t}| \leq \tau\sigma_{\max}$
[$\mathcal{Z}$ (the statement); $\widetilde{\sigma} \leq \sigma_{\max}$ (assumption A1)]

(L23) $\Rightarrow$ $\forall k\ \forall y \in \mathcal{Z} \cap V_k:\ k \leq k_\tau$
[(L18), (L19), (L22); $k \in \mathbb{Z}$; k_τ (the statement)]

(L24) $\Rightarrow$ item 4
[(L23)]

□ (items 1 to 4)

Lemma G.70 (The table's perturbation per row [to table])**.** *At a leaf, the table's relative perturbation is bounded per row, so is its mass, and it vanishes past the table's last row. Define:*

- $\sigma_0 := 1.8205$ *(Lemma G.64).*

Let:

- $\sigma_{\min} > 0$*;*
- $\sigma_{\max} \in [\sigma_{\min}, \sigma_0]$*;*
- $\widetilde{\sigma} > 0$*, a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$*, its computed center.*

Define:

- *The table*
  - $m(z_0) := \Pr[\texttt{GAUSSO} = z_0]$ *(Lemma G.64);*
  - $w(z_0) := m(z_0)\,\rho_{\sigma_0}(\mathbb{Z}_{\geq 0})/\rho_{\sigma_0}(z_0)$ *(Lemma G.64);*
  - $\forall k \geq 0:\ w_k := \begin{cases} w(k) & k \leq 18 \\ 0 & k \geq 19 \end{cases}$*;*
- *The rows*
  - $\widetilde{D} := D_{\mathbb{Z},\widetilde{\sigma},\widetilde{t}}$ *(Lemma G.69);*
  - $s := \lfloor \widetilde{t} \rceil$ *(Lemma G.69);*
  - $\bar{z}_0(z) := |z - [z > 0]|$ *(Lemma G.64);*
  - $\forall y \in \mathbb{Z}:\ k(y) := \bar{z}_0(y - s)$ *(Lemma G.69);*
  - $\forall k \geq 0:\ V_k := \{\, y : k(y) = k \,\} = \{s - k,\ s + k + 1\}$ *(Lemma G.69);*
- *The normalizer*
  - $\bar{\varepsilon}_0 := 2e^{-2\pi^2\sigma_{\min}^2}/(1 - e^{-2\pi^2\sigma_{\min}^2})$ *(Lemma G.69);*
- *The row masses*
  - $\forall k \leq 1:\ \bar{D}_k := 2/(\sqrt{2\pi}\,\sigma_{\min}(1 - \bar{\varepsilon}_0))$ *(Lemma G.69);*
  - $\forall k \geq 2:\ \bar{D}_k := (\rho_{\sigma_{\max}}(k) + \rho_{\sigma_{\max}}(k + 1))/(\sqrt{2\pi}\,\sigma_{\max}(1 - \bar{\varepsilon}_0))$ *(Lemma G.69);*
- *The table's perturbation*

– P_0, *that of Lemma G.64 at* $(\sigma, t) := (\widetilde{\sigma}, \widetilde{t})$;
– $\epsilon_{\text{tab}} := P_0/\widetilde{D} - 1$;
– $\varpi := \sum_{k\geq 0} \bar{D}_k |w_k - 1|$;
– $\epsilon_k^- := w_k/(1+\varpi) - 1$;
– $\epsilon_k^+ := w_k/(1-\varpi) - 1$.

Assume:

(A1) $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_{\max}]$;

(A2) $\varpi < 1$.

Then the table's perturbation and mass satisfy:

1. $\forall k \geq 0\ \forall y \in V_k :\ \epsilon_{\text{tab}}(y) \in [\epsilon_k^-, \epsilon_k^+]$;
2. $\forall k \geq 0\ \forall y \in V_k :\ P_0(y) \leq \widetilde{D}(y)(1+\epsilon_k^+)$;
3. $\forall k \geq 0 :\ P_0(V_k) \leq \bar{D}_k(1+\epsilon_k^+)$;
4. $\forall y,\ k(y) \geq 19 :\ P_0(y) = 0$.

Proof.

DEFINES $\langle w \rangle := \sum_y \widetilde{D}(y)\, w_{k(y)}$

Lemma G.64, item 2 over $\mathbb{R}$, at $(\sigma, t) := (\widetilde{\sigma}, \widetilde{t})$	This proof
Shared: $\sigma_{\min},\ \sigma_0, w, P_0$	
σ	$\widetilde{\sigma}$ (the statement)
t	$\widetilde{t}$ (the statement)
(I1) $\sigma > 0$	$\widetilde{\sigma} > 0$ (the statement)
$t \in \mathbb{R}$	$\widetilde{t}$ (the statement)
Assumption A1	Assumption A1
Assumption A2	Assumption A1; $\sigma_{\max} \leq \sigma_0$ (the statement)
Its conclusion: $P_0(s+z) = \frac{\rho_\sigma(z-r)\, w(\bar{z}_0(z))}{\sum_{z'} \rho_\sigma(z'-r)\, w(\bar{z}_0(z'))}$	

(L1) $\forall y :\ P_0(y) = \widetilde{D}(y)\, w_{k(y)}/\langle w \rangle$
[(I1); $\widetilde{D}$ (the statement); w_k (the statement); $\langle w \rangle$ (the proof's block)]

(L2) $|\langle w \rangle - 1| \leq \sum_k \widetilde{D}(V_k)|w_k - 1|$
[$\langle w \rangle$ (the proof's block); $\widetilde{D}$ a probability measure (the statement)]

Lemma G.69, item 2	This proof
Shared: $\sigma_{\min}, \sigma_{\max},\ \widetilde{\sigma}, \widetilde{t},\ \widetilde{D}, V_k, \bar{D}_k$	
Shared: $\sigma_{\min} > 0,\ \widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R}$	
(I2) Shared: assumption A1	
$\sigma_{\max} \in [\sigma_{\min}, 2]$	$\sigma_{\max} \in [\sigma_{\min}, \sigma_0]$ (the statement); $\sigma_0 = 1.8205$ (Lemma G.64)
Its conclusion: $\forall k \geq 0 :\ \widetilde{D}(V_k) \leq \bar{D}_k$	

(L3) $\sum_k \widetilde{D}(V_k)|w_k - 1| \leq \varpi$
[(I2); ϖ (the statement)]

(L4) $\forall k\ \forall y \in V_k :\ \epsilon_{\text{tab}}(y) = w_k/\langle w \rangle - 1$
[(L1); ϵ_{tab} (the statement)]

(L5) $\forall k :\ w_k/\langle w \rangle - 1 \in [\epsilon_k^-, \epsilon_k^+]$
[(L2), (L3); $\varpi < 1$ (assumption A2); $w_k \geq 0$ (the statement); $\epsilon_k^\pm$ (the statement)]

(L6) $\Rightarrow\ \forall k \geq 0\ \forall y \in V_k :\ \epsilon_{\text{tab}}(y) \in [\epsilon_k^-, \epsilon_k^+]$
[(L4), (L5)]

(L7) $\Rightarrow$ item 1

[(L6)]

(L8) $\forall k\ \forall y \in V_k :\ P_0(y) \le \widetilde{D}(y)(1+\epsilon_k^+)$

[(L4), (L5); ϵ_{tab} (the statement)]

(L9) $\Rightarrow$ item 2

[(L8)]

(L10) $\forall y,\ k(y) \ge 19 :\ P_0(y) = 0$

[(L1); $w_k = 0$ at $k \ge 19$ (the statement)]

(L11) $\Rightarrow$ item 4

[(L10)]

(L12) $\forall k :\ P_0(V_k) \le \bar{D}_k(1+\epsilon_k^+)$

[(I2); (L8)]

(L13) $\Rightarrow$ item 3

[(L12)]

□ (items 1 to 4)

Lemma G.71 (The floor terms per row [to table])**.** *At a leaf, the relative perturbation the acceptance's floor adds, and its square, weigh at most per-row constants. Let:*

- $\sigma_{\min} > 0$;
- $\sigma_{\max} \in [\sigma_{\min}, 2]$;
- $\widetilde{\sigma} > 0$, *a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$, *its computed center;*
- $e_{\text{ccs}} \in [0, 1)$.

Define:

- *The exponent*
  - $\sigma_0 := 1.8205$ *(Lemma G.64);*
  - x, *that of Lemma G.64;*
- *The rows*
  - $\widetilde{D} := D_{\mathbb{Z},\widetilde{\sigma},\widetilde{t}}$ *(Lemma G.69);*
  - $s := \lfloor \widetilde{t} \rceil$ *(Lemma G.69);*
  - $\bar{z}_0(z) := |z - [z > 0]|$ *(Lemma G.64);*
  - $\forall y \in \mathbb{Z} :\ k(y) := \bar{z}_0(y - s)$ *(Lemma G.69);*
  - $\forall k \ge 0 :\ V_k := \{\, y : k(y) = k \,\} = \{s - k,\ s + k + 1\}$ *(Lemma G.69);*
- *The normalizer*
  - $\bar{\varepsilon}_0 := 2e^{-2\pi^2\sigma_{\min}^2}/(1 - e^{-2\pi^2\sigma_{\min}^2})$ *(Lemma G.69);*
- *The acceptance*
  - $\widetilde{ccs}$, *the code's value of line 6 of* SamplerZ *(Algorithm 8);*
  - $acc(y) := \widetilde{ccs}\, e^{-x(y-s)}$;
- *The floor terms*
  - $e_{\text{fl}}(y) := 2^{-63}/acc(y)$;
  - $\bar{e}_{\text{fl},k} := 2^{-62} e^{-k^2/(2\sigma_0^2)}/(\sqrt{2\pi}\,\sigma_{\min}(1-\bar{\varepsilon}_0)(1-e_{\text{ccs}}))$;
  - $\bar{e}^{(2)}_{\text{fl},k} := 2^{-125} e^{(k+1)^2/(2\sigma_{\min}^2) - k^2/\sigma_0^2}\,\sigma_{\max}/(\sqrt{2\pi}\,\sigma_{\min}^2(1-\bar{\varepsilon}_0)(1-e_{\text{ccs}})^2)$.

Assume:

(A1) $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_{\max}]$;

(A2) $\widetilde{ccs} \ge (1 - e_{\text{ccs}})\,\sigma_{\min}/\widetilde{\sigma}$.

Then the floor terms satisfy:

1. $\forall k \ge 0 :\ \sum_{y \in V_k} \widetilde{D}(y)\, e_{\text{fl}}(y) \le \bar{e}_{\text{fl},k}$;
2. $\forall k \ge 0 :\ \sum_{y \in V_k} \widetilde{D}(y)\, e_{\text{fl}}(y)^2 \le \bar{e}^{(2)}_{\text{fl},k}$.

Proof. (L1) $\forall k\ \forall y \in V_k:\ \widetilde{D}(y)\, e_{\mathrm{fl}}(y) \le \frac{2^{-63} e^{-k^2/(2\sigma_0^2)} \widetilde{\sigma}}{\sigma_{\min}(1-e_{\mathrm{ccs}})\, \rho_{\widetilde{\sigma},\widetilde{t}}(\mathbb{Z})}$

[e_{fl}, *acc* (the statement); $\widetilde{ccs} \ge (1-e_{\mathrm{ccs}})\sigma_{\min}/\widetilde{\sigma}$ (assumption A2); $x(y-s) = (y-\widetilde{t})^2/(2\widetilde{\sigma}^2) - k^2/(2\sigma_0^2)$ (Lemma G.64); $\widetilde{D}$ (the statement)]

Lemma G.69	This proof
Shared: $\sigma_{\min}, \sigma_{\max},\ \widetilde{\sigma}, \widetilde{t},\ \bar{z}_0, s, \widetilde{D}, k(y), V_k, \bar{\varepsilon}_0$ Shared: $\tau > 1,\ \sigma_{\min} > 0,\ \sigma_{\max} \in [\sigma_{\min}, 2],\ \widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R}$	
(I1) Assumption A1	Assumption A1
Its item 1: $\rho_{\widetilde{\sigma},\widetilde{t}}(\mathbb{Z}) \ge \sqrt{2\pi}\,\widetilde{\sigma}(1-\bar{\varepsilon}_0)$	
Its item 3: $\forall k \ge 0\ \forall y \in V_k:\ \lvert y - \widetilde{t}\rvert \in [k, k+1]$	

(L2) $\rho_{\widetilde{\sigma},\widetilde{t}}(\mathbb{Z}) \ge \sqrt{2\pi}\,\widetilde{\sigma}(1-\bar{\varepsilon}_0)$

[item 1 of (I1)]

(L3) $\forall k \ge 0\ \forall y \in V_k:\ \lvert y - \widetilde{t}\rvert \in [k, k+1]$

[item 3 of (I1)]

(L4) $\Rightarrow\ \forall k:\ \sum_{y\in V_k} \widetilde{D}(y)\, e_{\mathrm{fl}}(y) \le \bar{e}_{\mathrm{fl},k}$

[(L1) at the two points of V_k; (L2); $\bar{e}_{\mathrm{fl},k}$ (the statement)]

(L5) $\Rightarrow$ item 1

[(L4)]

(L6) $\forall k\ \forall y \in V_k:\ \widetilde{D}(y)\, e_{\mathrm{fl}}(y)^2 \le \frac{2^{-126} e^{(y-\widetilde{t})^2/(2\widetilde{\sigma}^2) - k^2/\sigma_0^2} \widetilde{\sigma}^2}{\sigma_{\min}^2 (1-e_{\mathrm{ccs}})^2 \rho_{\widetilde{\sigma},\widetilde{t}}(\mathbb{Z})}$

[e_{fl}, *acc* (the statement); $\widetilde{ccs} \ge (1-e_{\mathrm{ccs}})\sigma_{\min}/\widetilde{\sigma}$ (assumption A2); x (Lemma G.64); $\widetilde{D}$ (the statement)]

(L7) $\Rightarrow\ \forall k:\ \sum_{y\in V_k} \widetilde{D}(y)\, e_{\mathrm{fl}}(y)^2 \le \bar{e}^{(2)}_{\mathrm{fl},k}$

[(L6) at the two points of V_k; (L3); $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_{\max}]$ (assumption A1); (L2); $\bar{e}^{(2)}_{\mathrm{fl},k}$ (the statement)]

(L8) $\Rightarrow$ item 2

[(L7)]

□ (items 1 and 2)

Lemma G.72 (The acceptance's perturbation per row [to table])**.** *At a leaf, the acceptance's relative perturbation is a ratio of two perturbed acceptances, its normalizer's perturbation is at most a constant of the rows, and its positive part and modulus are bounded per row. Define:*

- $\sigma_0 := 1.8205$ *(Lemma G.64).*

Let:

- $\sigma_{\min} > 0$*;*
- $\sigma_{\max} \in [\sigma_{\min}, \sigma_0]$*;*
- $\widetilde{\sigma} > 0$*, a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$*, its computed center;*
- $e_{+,k} \ge 0$ *for* $k \le 18$*;*
- $e_{\mathrm{ccs}} \in [0, 1)$*;*
- $\mathcal{Y} \subseteq \mathbb{Z}$*.*

Define:

- *The table*
  - $m(z_0) := \Pr[\texttt{GAUSSO} = z_0]$ *(Lemma G.64);*
  - $w(z_0) := m(z_0)\, \rho_{\sigma_0}(\mathbb{Z}_{\ge 0})/\rho_{\sigma_0}(z_0)$ *(Lemma G.64);*
  - $\forall k \ge 0:\ w_k := \begin{cases} w(k) & k \le 18 \\ 0 & k \ge 19 \end{cases}$ *(Lemma G.70);*
- *The rows*
  - $s := \lfloor \widetilde{t} \rceil$ *(Lemma G.69);*
  - $\bar{z}_0(z) := \lvert z - [z > 0]\rvert$ *(Lemma G.64);*
  - $\forall y \in \mathbb{Z}:\ k(y) := \bar{z}_0(y - s)$ *(Lemma G.69);*

- *The normalizer*
  - $\bar{\varepsilon}_0 := 2e^{-2\pi^2\sigma_{\min}^2}/(1-e^{-2\pi^2\sigma_{\min}^2})$ *(Lemma G.69);*
- *The row masses*
  - $\forall k \le 1:\ \bar{D}_k := 2/(\sqrt{2\pi}\,\sigma_{\min}(1-\bar{\varepsilon}_0))$ *(Lemma G.69);*
  - $\forall k \ge 2:\ \bar{D}_k := (\rho_{\sigma_{\max}}(k)+\rho_{\sigma_{\max}}(k+1))/(\sqrt{2\pi}\,\sigma_{\max}(1-\bar{\varepsilon}_0))$ *(Lemma G.69);*
- *The probability measures*
  - $\widetilde{B}(A) := \Pr[z \in A]$ *for* $z \leftarrow \mathrm{SamplerZ}(\widetilde{t}, 1/\widetilde{\sigma})$ *in* $\mathcal{F}$ *(Lemma G.67);*
  - $\widetilde{D} := D_{\mathbb{Z},\widetilde{\sigma},\widetilde{t}}$ *(Lemma G.67);*
  - P_0*, that of Lemma G.64 at* $(\sigma,t) := (\widetilde{\sigma},\widetilde{t})$*;*
- *The table's perturbation*
  - $\varpi := \sum_{k\ge 0}\bar{D}_k|w_k - 1|$ *(Lemma G.70);*
  - $\epsilon_k^+ := w_k/(1-\varpi) - 1$ *(Lemma G.70);*
- *The acceptance*
  - *ccs, that of Lemma G.64;*
  - $\widetilde{ccs}$*, the code's value of line 6 of* SamplerZ *(Algorithm 8);*
  - x*, that of Lemma G.64;*
  - $acc(y) := \widetilde{ccs}\,e^{-x(y-s)}$*;*
  - $e_{\mathrm{fl}}(y) := 2^{-63}/acc(y)$*;*
  - $\widetilde{acc}(y) := \widetilde{acc}(si, r', \widetilde{ccs})$ *of Fact G.66 at the si and* r' BerExp *(Algorithm 9) computes in* $\mathcal{F}$ *at* $y-s$*;*
  - $e_{acc}(y) := \widetilde{acc}(y)/acc(y) - 1$*;*
- *The floor terms*
  - $\bar{e}_{\mathrm{fl},k} := 2^{-62}e^{-k^2/(2\sigma_0^2)}/(\sqrt{2\pi}\,\sigma_{\min}(1-\bar{\varepsilon}_0)(1-e_{\mathrm{ccs}}))$ *(Lemma G.71);*
- *The normalizer's perturbation*
  - $\bar{e} := \sum_y P_0(y)\,e_{acc}(y)$*;*
  - $\bar{e}_{\mathrm{norm}} := \min_{v\in\{0,e_{+,0},\ldots,e_{+,18}\}}(v+\sum_{k\le 18}\bar{D}_k(1+\epsilon_k^+)\max(e_{+,k}-v,0))+\sum_{k\le 18}(1+\epsilon_k^+)\,\bar{e}_{\mathrm{fl},k}$*;*
- *The relative perturbations*
  - $\epsilon := \widetilde{B}/\widetilde{D} - 1$ *(Lemma G.67);*
  - $\epsilon_{\mathrm{tab}} := P_0/\widetilde{D} - 1$ *(Lemma G.67);*
  - $\epsilon_{\mathrm{ar}}(y) := \begin{cases}\widetilde{B}(y)/P_0(y)-1 & y\in\mathrm{Supp}(P_0)\\ 0 & y\notin\mathrm{Supp}(P_0)\end{cases}$ *(Lemma G.67);*
  - $\forall x \in \{\epsilon,\epsilon_{\mathrm{tab}},\epsilon_{\mathrm{ar}}\}:\ x_+ := \max(x,0)$ *(Lemma G.67).*

Assume:

(A1) $\widetilde{\sigma} \in [\sigma_{\min},\sigma_{\max}]$*;*

(A2) $\widetilde{ccs} \ge (1-e_{\mathrm{ccs}})\,\sigma_{\min}/\widetilde{\sigma}$*;*

(A3) $\varpi < 1$*;*

(A4) $\bar{e}_{\mathrm{norm}} < 1$*;*

(A5) $\forall y \in \mathrm{Supp}(P_0):\ |e_{acc}(y)| \le e_{+,k(y)} + e_{\mathrm{fl}}(y)$*;*

(A6) $\forall y \in \mathcal{Y}\cap\mathrm{Supp}(P_0):\ e_{acc}(y) \le e_{+,k(y)}$*.*

Then the acceptance's perturbation satisfies:

1. $1+\epsilon_{\mathrm{ar}} = (1+e_{acc})/(1+\bar{e})$ *on* $\mathrm{Supp}(P_0)$*;*
2. $|\bar{e}| \le \bar{e}_{\mathrm{norm}}$*;*
3. $\forall y \in \mathcal{Y}\cap\mathrm{Supp}(P_0):\ \epsilon_{\mathrm{ar},+}(y) \le (e_{+,k(y)}+\bar{e}_{\mathrm{norm}})/(1-\bar{e}_{\mathrm{norm}})$*;*
4. $\forall y \in \mathcal{Y}\cap\mathrm{Supp}(P_0):\ |\epsilon_{\mathrm{ar}}(y)| \le (e_{+,k(y)}+\min(e_{\mathrm{fl}}(y),1)+\bar{e}_{\mathrm{norm}})/(1-\bar{e}_{\mathrm{norm}})$*.*

Proof.

DEFINES $q(y) := m(k(y))/2$, $N_{\mathrm{acc}} := \sum_y q\,acc$, $\widetilde{N}_{\mathrm{acc}} := \sum_y q\,\widetilde{acc}$

(L1) $\widetilde{ccs}/ccs$ is the same at every y

[$\widetilde{ccs}$ (line 6 of SamplerZ (Algorithm 8)), ccs (Lemma G.64): neither depends on y]

Lemma G.64, item 2 over $\mathbb{R}$, at $(\sigma, t) := (\widetilde{\sigma}, \widetilde{t})$	This proof
Shared: $\sigma_{\min},\ \sigma_0, ccs, P_0,\ s,\ m$	
Shared: $\sigma_{\min} > 0,\ t \in \mathbb{R}$	
σ	$\widetilde{\sigma}$ (the statement)
t	$\widetilde{t}$ (the statement)
$\sigma > 0$	$\widetilde{\sigma} > 0$ (the statement)
Assumption A1	Assumption A1
Assumption A2	Assumption A1; $\sigma_{\max} \le \sigma_0$ (the statement)
Its conclusion: $P_0(s+z) = \frac{\rho_\sigma(z-r)\, w(\bar{z}_0(z))}{\sum_{z'} \rho_\sigma(z'-r)\, w(\bar{z}_0(z'))}$	

(I1)

(L2) $\forall z \in \mathbb{Z}:\ P_0(s+z) = \frac{\rho_{\widetilde{\sigma}}(z-r)\, w(\bar{z}_0(z))}{\sum_{z'} \rho_{\widetilde{\sigma}}(z'-r)\, w(\bar{z}_0(z'))}$

[(I1)]

(L3) $P_0 = q\, acc/N_{\text{acc}}$

[(L2), (L1); w, x (Lemma G.64); acc (the statement); q, N_{acc} (the proof's block)]

Lemma G.64, item 2 in $\mathcal{F}$ with the acceptance $\widetilde{acc}$ (Fact G.66), at $(\sigma, t) := (\widetilde{\sigma}, \widetilde{t})$	This proof
Shared: $\sigma_{\min},\ \sigma_0, ccs,\ s,\ m$	
Shared: $\sigma_{\min} > 0,\ t \in \mathbb{R}$	
σ	$\widetilde{\sigma}$ (the statement)
t	$\widetilde{t}$ (the statement)
acc	$\widetilde{acc}$ (Fact G.66)
P_0	$\widetilde{B}$ (the statement)
$\sigma > 0$	$\widetilde{\sigma} > 0$ (the statement)
Assumption A1	Assumption A1
Assumption A2	Assumption A1; $\sigma_{\max} \le \sigma_0$ (the statement)
Its conclusion: $P_0(s+z) = \frac{\rho_\sigma(z-r)\, w(\bar{z}_0(z))}{\sum_{z'} \rho_\sigma(z'-r)\, w(\bar{z}_0(z'))}$	

(I2)

(L4) $\widetilde{B} = q\, \widetilde{acc}/\widetilde{N}_{\text{acc}}$

[(I2); $\widetilde{N}_{\text{acc}}$ (the proof's block); $si \ge 0$ (line 2 at $x \ge 0$, the precondition of BerExp (Algorithm 9)), assumption A1 of Fact G.66 at the si and r' of $\widetilde{acc}(y)$]

(L5) $\widetilde{N}_{\text{acc}}/N_{\text{acc}} = \sum_y P_0(y)(1 + e_{acc}(y))$

[(L3); N_{acc}, $\widetilde{N}_{\text{acc}}$ (the proof's block); e_{acc} (the statement)]

(L6) $\sum_y P_0(y)(1 + e_{acc}(y)) = 1 + \bar{e}$

[P_0 a probability measure (Lemma G.64); $\bar{e}$ (the statement)]

(L7) $\Rightarrow\ 1 + \epsilon_{\text{ar}} = (1 + e_{acc})/(1 + \bar{e})$ on $\text{Supp}(P_0)$

[(L3) to (L6); ϵ_{ar} (the statement)]

(L8) $\Rightarrow$ item 1

[(L7)]

(L9) $\sigma_{\max} \le 2$

[$\sigma_{\max} \le \sigma_0$ (the statement); $\sigma_0 = 1.8205$ (Lemma G.64)]

	Lemma G.71, item 1	This proof
	Shared: $\sigma_{\min}, \sigma_{\max},\ \widetilde{\sigma}, \widetilde{t},\ e_{\text{ccs}},\ \sigma_0, s, k(y),\ \widetilde{ccs}, acc, e_{\text{fl}}, \bar{e}_{\text{fl},k}$	
	Shared: $\sigma_{\min} > 0,\ \widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R},\ e_{\text{ccs}} \in [0, 1)$	
(I3)	Shared: assumptions A1, A2	
	$\sigma_{\max} \in [\sigma_{\min}, 2]$	$\sigma_{\max} \geq \sigma_{\min}$ (the statement); (L9)
	Its conclusion: $\forall k \geq 0 :\ \sum_{y \in V_k} \widetilde{D}(y)\, e_{\text{fl}}(y) \leq \bar{e}_{\text{fl},k}$	
(L10)	$\forall k \geq 0 :\ \sum_{y \in V_k} \widetilde{D}(y)\, e_{\text{fl}}(y) \leq \bar{e}_{\text{fl},k}$	
		[(I3)]

	Lemma G.70	This proof
	Shared: $\sigma_{\min}, \sigma_{\max},\ \widetilde{\sigma}, \widetilde{t},\ \sigma_0, k(y), \bar{D}_k, P_0,\ \varpi, \epsilon_k^+$	
	Shared: $\sigma_{\min} > 0,\ \sigma_{\max} \in [\sigma_{\min}, \sigma_0],\ \widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R}$	
(I4)	Assumption A1 Assumption A2	Assumption A1 Assumption A3
	Its item 2: $\forall k \geq 0\ \forall y \in V_k :\ P_0(y) \leq \widetilde{D}(y)(1 + \epsilon_k^+)$	
	Its item 3: $\forall k \geq 0 :\ P_0(V_k) \leq \bar{D}_k(1 + \epsilon_k^+)$	
	Its item 4: $\forall y,\ k(y) \geq 19 :\ P_0(y) = 0$	
(L11)	$\forall k \geq 0\ \forall y \in V_k :\ P_0(y) \leq \widetilde{D}(y)(1 + \epsilon_k^+)$	
		[item 2 of (I4)]
(L12)	$\forall k \geq 0 :\ P_0(V_k) \leq \bar{D}_k(1 + \epsilon_k^+)$	
		[item 3 of (I4)]
(L13)	$\forall y,\ k(y) \geq 19 :\ P_0(y) = 0$	
		[item 4 of (I4)]
(L14)	$\lvert\bar{e}\rvert \leq \sum_k P_0(V_k)\, e_{+,k} + \sum_k (1 + \epsilon_k^+)\, \bar{e}_{\text{fl},k}$	
	[$\bar{e}$ (the statement); $\lvert e_{acc}\rvert \leq e_{+,k} + e_{\text{fl}}$ on $\text{Supp}(P_0)$ (assumption A5); (L10), (L11), (L13)]	
(L15)	$\forall x, v \in \mathbb{R} :\ x \leq v + \max(x - v, 0)$	
		[$\max(x - v, 0) \geq x - v$ (Fact A.41, item 20)]
(L16)	$\forall v \geq 0 :\ \sum_k P_0(V_k)\, e_{+,k} \leq v + \sum_k \bar{D}_k(1 + \epsilon_k^+) \max(e_{+,k} - v, 0)$	
		[(L12); (L15) at $x := e_{+,k}$; P_0 a probability measure (Lemma G.64)]
(L17)	$\Rightarrow\ \lvert\bar{e}\rvert \leq \bar{e}_{\text{norm}}$	
		[(L14), (L16) at the $v \in \{0, e_{+,0}, \ldots, e_{+,18}\}$ of the minimum; $\bar{e}_{\text{norm}}$ (the statement)]
(L18)	$\Rightarrow$ item 2	
		[(L17)]
(L19)	$\forall y :\ e_{acc}(y) \geq -1$	
	[e_{acc} (the statement); $\widetilde{acc} \geq 0$ (Fact G.66); $si \geq 0$ (line 2 at $x \geq 0$, the precondition of BerExp (Algorithm 9)), assumption A1 of Fact G.66 at the si and r' of $\widetilde{acc}(y)$]	
(L20)	$\forall y \in \mathcal{Y} \cap \text{Supp}(P_0) :\ \epsilon_{\text{ar},+}(y) \leq \frac{e_{+,k(y)} + \bar{e}_{\text{norm}}}{1 - \bar{e}_{\text{norm}}}$	
	[(L7), (L17), (L19); $e_{acc} \leq e_{+,k}$ on $\mathcal{Y} \cap \text{Supp}(P_0)$ (assumption A6); $\bar{e}_{\text{norm}} < 1$ (assumption A4)]	
(L21)	$\Rightarrow$ item 3	
		[(L20)]
(L22)	$\forall y \in \mathcal{Y} \cap \text{Supp}(P_0) :\ \lvert\epsilon_{\text{ar}}(y)\rvert \leq \frac{e_{+,k(y)} + \min(e_{\text{fl}}(y), 1) + \bar{e}_{\text{norm}}}{1 - \bar{e}_{\text{norm}}}$	
	[(L7), (L17), (L19); $\lvert e_{acc}\rvert \leq e_{+,k} + e_{\text{fl}}$ on $\text{Supp}(P_0)$ (assumption A5); $e_{acc} \leq e_{+,k}$ on $\mathcal{Y} \cap \text{Supp}(P_0)$ (assumption A6); $\bar{e}_{\text{norm}} < 1$ (assumption A4)]	
(L23)	$\Rightarrow$ item 4	
		[(L22)]
		□ (items 1 to 4)

Lemma G.73 (The moments at every leaf [to table])**.** *At every leaf, the table's and the acceptance's moments are at most constants of the leaves' range, and so is the moment they bound. Define:*

- $\sigma_0 := 1.8205$ *(Lemma G.64).*

Let:

- $\alpha \geq 2$*;*
- $\sigma_{\min} > 0$*;*
- $\sigma_{\max} \in [\sigma_{\min}, \sigma_0]$*;*
- $e_{+,k} \geq 0$ *for* $k \leq 18$*;*
- $e_{\text{ccs}} \in [0, 1)$*;*
- $\widetilde{\sigma} > 0$*, a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$*, its computed center;*
- $\mathcal{Y} \subseteq \mathbb{Z}$*.*

Define:

- *The table*
  - $m(z_0) := \Pr[\texttt{GAUSSO} = z_0]$ *(Lemma G.64);*
  - $w(z_0) := m(z_0)\, \rho_{\sigma_0}(\mathbb{Z}_{\geq 0})/\rho_{\sigma_0}(z_0)$ *(Lemma G.64);*
  - $\forall k \geq 0 :\ w_k := \begin{cases} w(k) & k \leq 18 \\ 0 & k \geq 19 \end{cases}$ *(Lemma G.70);*
- *The rows*
  - $s := \lfloor \widetilde{t} \rceil$ *(Lemma G.69);*
  - $\mathcal{Z} := \{\, y \in \mathbb{Z} : |y - \widetilde{t}| \leq \tau\widetilde{\sigma} \,\}$ *(Lemma G.69);*
  - $\bar{z}_0(z) := |z - [z > 0]|$ *(Lemma G.64);*
  - $\forall y \in \mathbb{Z} :\ k(y) := \bar{z}_0(y - s)$ *(Lemma G.69);*
  - $V_k = \{\, y : k(y) = k \,\} = \{s - k,\ s + k + 1\}$*,* $k \geq 0$ *(Lemma G.69);*
  - $k_\tau := \lfloor \tau\sigma_{\max} \rfloor$ *(Lemma G.69);*
  - $k'_\tau := \min(k_\tau, 18)$*;*
- *The normalizer*
  - $\bar{\varepsilon}_0 := 2e^{-2\pi^2\sigma_{\min}^2}/(1 - e^{-2\pi^2\sigma_{\min}^2})$ *(Lemma G.69);*
- *The row masses*
  - $\bar{D}_k := 2/(\sqrt{2\pi}\,\sigma_{\min}(1 - \bar{\varepsilon}_0))$ *for* $k \leq 1$ *(Lemma G.69);*
  - $\bar{D}_k := (\rho_{\sigma_{\max}}(k) + \rho_{\sigma_{\max}}(k+1))/(\sqrt{2\pi}\,\sigma_{\max}(1 - \bar{\varepsilon}_0))$ *for* $k \geq 2$ *(Lemma G.69);*
- *The probability measures*
  - $\widetilde{B}(A) := \Pr[z \in A]$ *for* $z \leftarrow \text{SamplerZ}(\widetilde{t}, 1/\widetilde{\sigma})$ *in* $\mathcal{F}$ *(Lemma G.67);*
  - $\widetilde{D} := D_{\mathbb{Z},\widetilde{\sigma},\widetilde{t}}$ *(Lemma G.67);*
  - P_0*, the probability measure of Lemma G.64 at* $(\sigma, t) := (\widetilde{\sigma}, \widetilde{t})$*;*
- *The table's perturbation*
  - $\varpi := \sum_{k \geq 0} \bar{D}_k |w_k - 1|$ *(Lemma G.70);*
  - $\epsilon_k^{\pm} := w_k/(1 \pm \varpi) - 1$ *(Lemma G.70);*
- *The acceptance*
  - $\widetilde{ccs}$*, the code's value of line 6 of* SamplerZ *(Algorithm 8);*
  - x*, that of Lemma G.64;*
  - $acc(y) := \widetilde{ccs}\, e^{-x(y-s)}$*;*
  - $e_{\text{fl}}(y) := 2^{-63}/acc(y)$*;*
  - $\widetilde{acc}(y) := \widetilde{acc}(si, r', \widetilde{ccs})$ *of Fact G.66 at the si and* r' BerExp *(Algorithm 9) computes in* $\mathcal{F}$ *at* $y - s$*;*
  - $e_{acc}(y) := \widetilde{acc}(y)/acc(y) - 1$ *(Lemma G.72);*
- *The floor terms*
  - $\bar{e}_{\text{fl},k} := 2^{-62} e^{-k^2/(2\sigma_0^2)}/(\sqrt{2\pi}\,\sigma_{\min}(1 - \bar{\varepsilon}_0)(1 - e_{\text{ccs}}))$ *(Lemma G.71);*
  - $\bar{e}^{(2)}_{\text{fl},k} := 2^{-125} e^{(k+1)^2/(2\sigma_{\min}^2) - k^2/\sigma_0^2}\, \sigma_{\max}/(\sqrt{2\pi}\,\sigma_{\min}^2(1 - \bar{\varepsilon}_0)(1 - e_{\text{ccs}})^2)$ *(Lemma G.71);*
- *The normalizer's perturbation*
  - $\bar{e}_{\text{norm}}$*, that of Lemma G.72 at* $(e_{+,k})_k$*;*

- *The relative perturbations*
  - $\epsilon := \widetilde{B}/\widetilde{D} - 1$ *(Lemma G.67);*
  - $\epsilon_{\text{tab}} := P_0/\widetilde{D} - 1$ *(Lemma G.67);*
  - $\epsilon_{\text{ar}}(y) := \begin{cases} \widetilde{B}(y)/P_0(y) - 1 & y \in \text{Supp}(P_0) \\ 0 & y \notin \text{Supp}(P_0) \end{cases}$ *(Lemma G.67);*
  - $x_+ := \max(x, 0)$ *at* $x \in \{\epsilon, \epsilon_{\text{tab}}, \epsilon_{\text{ar}}\}$ *(Lemma G.67);*
- *The weights*
  - $w_{\text{tab}} := (1 + \epsilon_{\text{tab},+})^{\alpha-2}$ *(Lemma G.67);*
  - $w_{\text{ar}} := (1 + \epsilon_{\text{ar},+})^{\alpha-2}$ *(Lemma G.67);*
  - $\bar{w}_{\text{ar}} := \left(1 + (\max_{k \le k'_\tau} e_{+,k} + \bar{e}_{\text{norm}})/(1 - \bar{e}_{\text{norm}})\right)^{\alpha-2}$;
  - $\bar{w}_k := (1 + \max(\epsilon_k^+, 0))^{\alpha-2}\, \bar{w}_{\text{ar}}$;
  - $\bar{w}'_k := \bar{w}_k (1 + \epsilon_k^+)^2/(1 - \bar{e}_{\text{norm}})^2$;
- *The moments*
  - $\bar{M}_{\text{tab}} := \sum_{k \le k_\tau} \bar{D}_k\, \bar{w}_k \max((\epsilon_k^-)^2, (\epsilon_k^+)^2)$;
  - $\bar{v}_k := \bar{w}'_k (e_{+,k} + \bar{e}_{\text{norm}})^2$;
  - $\bar{M}^{\text{fl}}_{\text{ar}} := \sum_{k \le k'_\tau} \bar{w}'_k (2(e_{+,k} + \bar{e}_{\text{norm}}) \min(\bar{D}_k, \bar{e}_{\text{fl},k}) + \min(\bar{D}_k, \bar{e}_{\text{fl},k}, \bar{e}^{(2)}_{\text{fl},k}))$;
  - $\bar{M}_{\text{ar}} := \min_{v \in \{0, \bar{v}_0, \ldots, \bar{v}_{k'_\tau}\}} (v + \sum_{k \le k'_\tau} \bar{D}_k \max(\bar{v}_k - v, 0)) + \bar{M}^{\text{fl}}_{\text{ar}}$.

Assume:

(A1) $\mathcal{Y} \subseteq \mathcal{Z}$;

(A2) $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_{\max}]$;

(A3) $\widetilde{ccs} \ge (1 - e_{\text{ccs}})\, \sigma_{\min}/\widetilde{\sigma}$;

(A4) $\varpi < 1$;

(A5) $\bar{e}_{\text{norm}} < 1$;

(A6) $\forall y \in \text{Supp}(P_0) :\ |e_{acc}(y)| \le e_{+,k(y)} + e_{\text{fl}}(y)$;

(A7) $\forall y \in \mathcal{Y} \cap \text{Supp}(P_0) :\ e_{acc}(y) \le e_{+,k(y)}$.

Then the moments and the fringe mass are bounded:

1. $\sum_{y \in \mathcal{Y}} \widetilde{D}\, w_{\text{tab}} w_{\text{ar}} \epsilon_{\text{tab}}^2 \le \bar{M}_{\text{tab}}$;
2. $\sum_{y \in \mathcal{Y}} \widetilde{D}\, w_{\text{tab}} w_{\text{ar}} \epsilon_{\text{ar}}^2 (1 + \epsilon_{\text{tab}})^2 \le \bar{M}_{\text{ar}}$;
3. $\sum_{y \in \mathcal{Y}} \widetilde{D} (1 + \epsilon_+)^{\alpha-2} \epsilon^2 \le \left(\sqrt{\bar{M}_{\text{tab}}} + \sqrt{\bar{M}_{\text{ar}}}\right)^2$;
4. $\forall C \subseteq \mathbb{Z},\ e_{\text{fl}} \ge 1$ *on* $C :\ \widetilde{D}(C) \le \sum_{k \in k(C)} \bar{e}_{\text{fl},k}$.

Proof.

DEFINES $M_{\alpha,\mathcal{Y}} = \sum_{z \in \mathcal{Y}} \widetilde{D}(z)(1 + \epsilon_+)^{\alpha-2} \epsilon^2$ (Lemma G.68)

DEFINES $M_{\text{tab},\mathcal{Y}} = \sum_{z \in \mathcal{Y}} \widetilde{D}\, w_{\text{tab}} w_{\text{ar}} \epsilon_{\text{tab}}^2$ (Lemma G.68)

DEFINES $M_{\text{ar},\mathcal{Y}} = \sum_{z \in \mathcal{Y}} \widetilde{D}\, w_{\text{tab}} w_{\text{ar}} \epsilon_{\text{ar}}^2 (1 + \epsilon_{\text{tab}})^2$ (Lemma G.68)

(L1) $\forall x, v \in \mathbb{R} :\ x \le v + \max(x - v, 0)$

[$\max(x - v, 0) \ge x - v$ (Fact A.41, item 20)]

(L2) $\sigma_{\max} \le 2$

[$\sigma_{\max} \le \sigma_0$ (the statement); $\sigma_0 = 1.8205$ (Lemma G.64)]

Lemma G.69	This proof
Shared: $\sigma_{\min}, \sigma_{\max},\ \widetilde{\sigma}, \widetilde{t},\ s, \mathcal{Z}, k(y), V_k, \bar{\varepsilon}_0, \bar{D}_k, k_\tau,\ \widetilde{D}$ Shared: $\tau > 1,\ \sigma_{\min} > 0,\ \widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R}$	
(I1) $\sigma_{\max} \in [\sigma_{\min}, 2]$	$\sigma_{\max} \ge \sigma_{\min}$ (the statement); (L2)
Assumption A1	Assumption A2
Its item 2: $\forall k \ge 0 :\ \widetilde{D}(V_k) \le \bar{D}_k$	
Its item 4: $\forall k \ge 0\ \forall y \in \mathcal{Z} \cap V_k :\ k \le k_\tau$	

(L3) $\forall k \geq 0 :\ \widetilde{D}(V_k) \leq \bar{D}_k$

[item 2 of (I1)]

(L4) $\forall k \geq 0\ \forall y \in \mathcal{Z} \cap V_k :\ k \leq k_\tau$

[item 4 of (I1)]

Lemma G.70	This proof
Shared: $\sigma_{\min}, \sigma_{\max},\ \widetilde{\sigma}, \widetilde{t},\ \sigma_0, w_k, \varpi, \epsilon_k^-, \epsilon_k^+,\ \widetilde{D}, k(y), V_k, \bar{D}_k, P_0, \epsilon_{\text{tab}}$	
Shared: $\sigma_{\min} > 0,\ \sigma_{\max} \in [\sigma_{\min}, \sigma_0],\ \widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R}$	
(I2) Assumption A1	Assumption A2
Assumption A2	Assumption A4
Its item 1: $\forall k \geq 0\ \forall y \in V_k :\ \epsilon_{\text{tab}}(y) \in [\epsilon_k^-, \epsilon_k^+]$	
Its item 4: $\forall y,\ k(y) \geq 19 :\ P_0(y) = 0$	

(L5) $\forall k \geq 0\ \forall y \in V_k :\ \epsilon_{\text{tab}}(y) \in [\epsilon_k^-, \epsilon_k^+]$

[item 1 of (I2)]

(L6) $\forall y,\ k(y) \geq 19 :\ P_0(y) = 0$

[item 4 of (I2)]

Lemma G.72	This proof
Shared: $\sigma_{\min}, \sigma_{\max},\ \widetilde{\sigma}, \widetilde{t},\ e_{+,k}, e_{\text{ccs}}, \mathcal{Y},\ \sigma_0, \widetilde{B}, P_0, \epsilon_{\text{ar}},\ s, k(y), \bar{D}_k, \varpi, \epsilon_k^+,\ \widetilde{ccs}, acc, e_{\text{fl}}, \bar{e}_{\text{fl},k}, \widetilde{acc}, e_{acc}, \bar{e}_{\text{norm}}$	
Shared: $\sigma_{\min} > 0,\ \sigma_{\max} \in [\sigma_{\min}, \sigma_0],\ \widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R},\ e_{+,k} \geq 0,\ e_{\text{ccs}} \in [0, 1),\ \mathcal{Y} \subseteq \mathbb{Z}$	
$\epsilon_{\text{ar}} = 0$ off $\text{Supp}(P_0)$	ϵ_{ar} (the statement)
(I3) Assumption A1	Assumption A2
Assumption A2	Assumption A3
Assumption A3	Assumption A4
Assumption A4	Assumption A5
Assumption A5	Assumption A6
Assumption A6	Assumption A7
Its item 3: $\forall y \in \mathcal{Y} \cap \text{Supp}(P_0) :\ \epsilon_{\text{ar},+}(y) \leq (e_{+,k(y)} + \bar{e}_{\text{norm}})/(1 - \bar{e}_{\text{norm}})$	
Its item 4: $\forall y \in \mathcal{Y} \cap \text{Supp}(P_0) :\ \lvert\epsilon_{\text{ar}}(y)\rvert \leq (e_{+,k(y)} + \min(e_{\text{fl}}(y), 1) + \bar{e}_{\text{norm}})/(1 - \bar{e}_{\text{norm}})$	

(L7) $\forall y \in \mathcal{Y} \cap \text{Supp}(P_0) :\ \epsilon_{\text{ar},+}(y) \leq (e_{+,k(y)} + \bar{e}_{\text{norm}})/(1 - \bar{e}_{\text{norm}})$

[item 3 of (I3)]

(L8) $\forall y \in \mathcal{Y} \cap \text{Supp}(P_0) :\ \lvert\epsilon_{\text{ar}}(y)\rvert \leq (e_{+,k(y)} + \min(e_{\text{fl}}(y), 1) + \bar{e}_{\text{norm}})/(1 - \bar{e}_{\text{norm}})$

[item 4 of (I3)]

Lemma G.71	This proof
Shared: $\sigma_{\min}, \sigma_{\max},\ \widetilde{\sigma}, \widetilde{t},\ e_{\text{ccs}},\ \sigma_0, \widetilde{D}, s, k(y), V_k, \bar{\varepsilon}_0,\ \widetilde{ccs}, acc, e_{\text{fl}}, \bar{e}_{\text{fl},k}, \bar{e}^{(2)}_{\text{fl},k}$	
Shared: $\sigma_{\min} > 0,\ \widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R},\ e_{\text{ccs}} \in [0, 1)$	
$\sigma_{\max} \in [\sigma_{\min}, 2]$	$\sigma_{\max} \geq \sigma_{\min}$ (the statement); (L2)
(I4) Assumption A1	Assumption A2
Assumption A2	Assumption A3
Its item 1: $\forall k \geq 0 :\ \sum_{y \in V_k} \widetilde{D}(y)\, e_{\text{fl}}(y) \leq \bar{e}_{\text{fl},k}$	
Its item 2: $\forall k \geq 0 :\ \sum_{y \in V_k} \widetilde{D}(y)\, e_{\text{fl}}(y)^2 \leq \bar{e}^{(2)}_{\text{fl},k}$	

(L9) $\forall k \geq 0 :\ \sum_{y \in V_k} \widetilde{D}(y)\, e_{\text{fl}}(y) \leq \bar{e}_{\text{fl},k}$

[item 1 of (I4)]

(L10) $\forall k \geq 0 :\ \sum_{y \in V_k} \widetilde{D}(y)\, e_{\text{fl}}(y)^2 \leq \bar{e}^{(2)}_{\text{fl},k}$

[item 2 of (I4)]

(L11) $\forall y \in \mathcal{Y} :\ w_{\text{tab}} w_{\text{ar}} \leq \bar{w}_{k(y)}$

[(L4), (L5), (L6), (L7); $\mathcal{Y} \subseteq \mathcal{Z}$ (assumption A1); $\epsilon_{\text{ar}} = 0$ on the complement of $\text{Supp}(P_0)$ (the statement);

$\alpha \geq 2$ (the statement)]

(L12) $\forall y \in \mathcal{Y}:\ (1+\epsilon_{\text{tab}})^2 \leq (1+\epsilon^+_{k(y)})^2$

[(L5)]

(L13) $\forall k\ \forall y \in \mathcal{Y} \cap V_k:\ \widetilde{D}\, w_{\text{tab}} w_{\text{ar}} \epsilon^2_{\text{tab}} \leq \widetilde{D}(y)\, \bar{w}_k \max((\epsilon^-_k)^2, (\epsilon^+_k)^2)$

[(L5); (L11)]

(L14) $\Rightarrow$ item 1

[(L13) summed over the rows $k \leq k_\tau$: (L4), (L3); $\bar{M}_{\text{tab}}$ (the statement)]

(L15) $\forall k\ \forall y \in \mathcal{Y} \cap V_k:\ \widetilde{D}\, w_{\text{tab}} w_{\text{ar}} \epsilon^2_{\text{ar}} (1+\epsilon_{\text{tab}})^2 \leq \widetilde{D}(y)\, \bar{w}'_k (e_{+,k} + \bar{e}_{\text{norm}} + \min(e_{\text{fl}}(y), 1))^2$

[(L8); (L11), (L12); $\bar{w}'_k$ (the statement); $\epsilon_{\text{ar}} = 0$ on the complement of $\text{Supp}(P_0)$ (the statement)]

(L16) $\forall s \in [0,1]:\ s^2 \leq s$

[$s \leq 1$, $s \geq 0$]

(L17) $\forall x \geq 0\ \forall s \in [0,1]:\ (x+s)^2 \leq x^2 + 2xs + s$

[expand; (L16)]

(L18) $\forall y \in \mathcal{Y} \cap \text{Supp}(P_0):\ k(y) \leq k'_\tau$

[(L4); (L6); $\mathcal{Y} \subseteq \mathcal{Z}$ (assumption A1); k'_τ (the statement)]

(L19) $\forall v \geq 0:\ \sum_{k \leq k'_\tau} \bar{w}'_k (e_{+,k} + \bar{e}_{\text{norm}})^2\, \widetilde{D}(V_k \cap \mathcal{Y}) \leq v + \sum_{k \leq k'_\tau} \bar{D}_k \max(\bar{v}_k - v, 0)$

[$\bar{v}_k$ (the statement); (L1) at $x := \bar{v}_k$; $\widetilde{D}$ a probability measure (Lemma G.67); (L3); (L18)]

(L20) $\forall e \geq 0:\ \min(e,1) \leq 1$

[min]

(L21) $\forall e \geq 0:\ \min(e,1) \leq e$

[min]

(L22) $\forall e \geq 0:\ \min(e,1)^2 \leq \min(e,1)$

[(L16) at $s := \min(e,1) \in [0,1]$]

(L23) $\forall e \geq 0:\ \min(e,1)^2 \leq e^2$

[(L21); $t \mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L24) $\sum_{k \leq k'_\tau} \bar{w}'_k \sum_{y \in V_k} \widetilde{D}(y) \big(2(e_{+,k} + \bar{e}_{\text{norm}}) \min(e_{\text{fl}}(y), 1) + \min(e_{\text{fl}}(y), 1)^2\big) \leq \bar{M}^{\text{fl}}_{\text{ar}}$

[(L20) to (L23) at $e := e_{\text{fl}}(y)$; (L3); (L9), (L10); $\bar{M}^{\text{fl}}_{\text{ar}}$ (the statement)]

(L25) $\Rightarrow$ item 2

[(L15), (L17) at $x := e_{+,k} + \bar{e}_{\text{norm}}$, $s := \min(e_{\text{fl}}, 1)$; (L19) at the $v \in \{0, \bar{v}_0, \ldots, \bar{v}_{k'_\tau}\}$ of the minimum; (L24); $\bar{M}_{\text{ar}}$ (the statement)]

Lemma G.68 at $\mathcal{Y}$	This proof
Shared: α, $\sigma_{\min}$, $\widetilde{\sigma}, \widetilde{t}$, $\mathcal{Y}$, $\widetilde{B}, \widetilde{D}, P_0, \epsilon, \epsilon_{\text{tab}}, \epsilon_{\text{ar}}, w_{\text{tab}}, w_{\text{ar}}, \sigma_0$, $M_{\alpha,\mathcal{Y}}, M_{\text{tab},\mathcal{Y}}, M_{\text{ar},\mathcal{Y}}$	
Shared: $\alpha \geq 2$, $\sigma_{\min} > 0$, $\widetilde{\sigma} > 0$, $\widetilde{t} \in \mathbb{R}$, $\mathcal{Y} \subseteq \mathbb{Z}$	
(I5) Assumption A1	Assumption A2; $\sigma_{\max} \leq \sigma_0$ (the statement)
Assumption A2	$\mathcal{Y} \subseteq \mathcal{Z}$ (assumption A1); $\mathcal{Z}$ finite (Lemma G.69)
Assumption A3	Item 1; $M_{\text{tab},\mathcal{Y}}$ (the proof's block)
Assumption A4	Item 2; $M_{\text{ar},\mathcal{Y}}$ (the proof's block)
Its conclusion: $M_{\alpha,\mathcal{Y}} \leq \big(\sqrt{M_{\text{tab},\mathcal{Y}}} + \sqrt{M_{\text{ar},\mathcal{Y}}}\big)^2$	

(L26) $M_{\alpha,\mathcal{Y}} \leq \big(\sqrt{M_{\text{tab},\mathcal{Y}}} + \sqrt{M_{\text{ar},\mathcal{Y}}}\big)^2$

[(I5)]

(L27) $\sum_{y \in \mathcal{Y}} \widetilde{D}(1+\epsilon_+)^{\alpha-2} \epsilon^2 \leq \big(\sqrt{\bar{M}_{\text{tab}}} + \sqrt{\bar{M}_{\text{ar}}}\big)^2$

[(L26); $M_{\alpha,\mathcal{Y}}$, $M_{\text{tab},\mathcal{Y}}$, $M_{\text{ar},\mathcal{Y}}$ (the proof's block); items 1 and 2; $t \mapsto \sqrt{t}$, $t \mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L28) $\Rightarrow$ item 3

[(L27)]

(L29) $\forall C \subseteq \mathbb{Z},\ e_{\text{fl}} \geq 1 \text{ on } C\ \forall y \in C:\ \widetilde{D}(y) \leq \widetilde{D}(y)\, e_{\text{fl}}(y)$

[$e_{\text{fl}} \geq 1$ on C (the item's quantifier); $\widetilde{D} \geq 0$ (the statement)]

(L30) $\Rightarrow$ item 4

[(L29); (L9) on each row $k \in k(C)$]

□ (items 1 to 4)

Lemma G.74 (Monotonicity of the moment bounds [to table])**.** *Raising the ceiling $\sigma_{\max}$ of the leaves' standard deviations raises the bounds of Lemma G.73 or keeps them. Define:*

- $\sigma_0 := 1.8205$ *(Lemma G.64).*

Let:

- $\alpha \geq 2$*;*
- $\tau > 1$*, a radius;*
- $\sigma_{\min} > 0$*;*
- $e_{+,k} \geq 0$ *for* $k \leq 18$*;*
- $e_{\text{ccs}} \in [0, 1)$*;*
- $s, s' \in [\sigma_{\min}, \sigma_0]$.

Define:

- $\varpi(x)$*,* $\bar{e}_{\text{norm}}(x)$*,* $\bar{M}_{\text{tab}}(x)$ *and* $\bar{M}_{\text{ar}}(x)$*,* $x \in \{s, s'\}$*, the* ϖ*,* $\bar{e}_{\text{norm}}$*,* $\bar{M}_{\text{tab}}$ *and* $\bar{M}_{\text{ar}}$ *of Lemma G.73 at order* α*,* τ*,* $\sigma_{\min}$*,* $\sigma_{\max} := x$*,* $e_{+,k}$ *and* e_{ccs}*;*
- $\bar{\varepsilon}_0 := 2e^{-2\pi^2\sigma_{\min}^2}/(1 - e^{-2\pi^2\sigma_{\min}^2})$ *(Lemma G.69 at* $\sigma_{\min}$*).*

Assume:

(A1) $s \leq s'$*;*
(A2) $\bar{\varepsilon}_0 < 1$*;*
(A3) $\varpi(s') < 1$*;*
(A4) $\bar{e}_{\text{norm}}(s') < 1$.

Then the bounds at s *are at most those at* s'*:*

1. $\varpi(s) \leq \varpi(s')$*;*
2. $\bar{e}_{\text{norm}}(s) \leq \bar{e}_{\text{norm}}(s')$*;*
3. $\left(\sqrt{\bar{M}_{\text{tab}}(s)} + \sqrt{\bar{M}_{\text{ar}}(s)}\right)^2 \leq \left(\sqrt{\bar{M}_{\text{tab}}(s')} + \sqrt{\bar{M}_{\text{ar}}(s')}\right)^2$.

Proof.

DEFINES $\bar{D}_k(x)$, $\epsilon_k^{\pm}(x)$, $k_\tau(x)$, $k'_\tau(x)$, $\bar{w}_{\text{ar}}(x)$, $\bar{w}_k(x)$, $\bar{w}'_k(x)$, $\bar{v}_k(x)$, $\bar{e}^{(2)}_{\text{fl},k}(x)$ and $\bar{M}^{\text{fl}}_{\text{ar}}(x)$, $x \in \{s, s'\}$, those of Lemma G.73 at $\sigma_{\max} := x$
$w_k := w(k)$ for $k \leq 18$, and $w_k := 0$ for $k \geq 19$ (Lemma G.70)
$\bar{e}_{\text{fl},k}$, that of Lemma G.71
$h_x(v) := v + \sum_{k \leq 18} \bar{D}_k(x)(1 + \epsilon_k^+(x)) \max(e_{+,k} - v, 0)$, $v \in [0, \infty)$, $x \in \{s, s'\}$
$f_x(v) := v + \sum_{k \leq k'_\tau(x)} \bar{D}_k(x) \max(\bar{v}_k(x) - v, 0)$, $v \in [0, \infty)$, $x \in \{s, s'\}$
$V(x) := \{0, \bar{v}_0(x), \ldots, \bar{v}_{k'_\tau(x)}(x)\}$, $x \in \{s, s'\}$

(L1) $\forall y \geq x' \geq x > 0 :\ \rho_x(y)/x \leq \rho_{x'}(y)/x'$
[Lemma G.69, (L14)]

(L2) $s' < 2$
[$s' \leq \sigma_0$ (the statement); $\sigma_0 = 1.8205$ (Lemma G.64)]

(L3) $1 - \bar{\varepsilon}_0 > 0$
[assumption A2]

(L4) $\forall k \geq 2 :\ \rho_s(k)/s + \rho_s(k+1)/s \leq \rho_{s'}(k)/s' + \rho_{s'}(k+1)/s'$
[(L1) at $y := k$ and at $y := k+1$ and $(x, x') := (s, s')$, by (L2) and $k \geq 2$ (the line's quantifier); $s \leq s'$ (assumption A1); $s, s' \in [\sigma_{\min}, \sigma_0]$ and $\sigma_{\min} > 0$ (the statement)]

(L5) $\Rightarrow\ \forall k \geq 2 :\ \bar{D}_k(s) \leq \bar{D}_k(s')$
[(L3), (L4); $\bar{D}_k$ (Lemma G.69); Fact A.41, item 8]

(L6) $\forall k \leq 1 :\ \bar{D}_k(s) = \bar{D}_k(s')$
[$\bar{D}_k := 2/(\sqrt{2\pi}\,\sigma_{\min}(1 - \bar{\varepsilon}_0))$ for $k \leq 1$ (Lemma G.69)]

(L7) $\forall k \geq 0\ \forall x \in \{s, s'\} :\ \bar{D}_k(x) \geq 0$
[(L3); $\bar{D}_k$ (Lemma G.69); Definition A.2, item 1, at $(s, c) := (x, 0)$; $e^t > 0$ (Fact A.41, item 12)]

(L8) $\Rightarrow$ $\forall k \geq 0:\ \bar{D}_k(s) \leq \bar{D}_k(s')$

[(L5), (L6)]

(L9) $\forall k \geq 0:\ \bar{D}_k(s)|w_k - 1| \in [0, \bar{D}_k(s')|w_k - 1|]$

[(L7), (L8); $|w_k - 1| \geq 0$ (Fact A.41, item 1); Fact A.41, item 8]

(L10) $\Rightarrow$ $\varpi(s) \leq \varpi(s')$

[(L9); assumption A3; $\varpi := \sum_{k\geq 0} \bar{D}_k|w_k - 1|$ (Lemma G.70); Fact A.45, item 9]

(L11) $\Rightarrow$ item 1

[(L10)]

(L12) $\forall x \in \{s, s'\}:\ \varpi(x) \in [0, 1)$

[(L9), (L10); assumption A3; Fact A.45, item 9]

(L13) $\forall k \geq 0:\ w_k \geq 0$

[$w(z_0) = m(z_0)\,\rho_{\sigma_0}(\mathbb{Z}_{\geq 0})/\rho_{\sigma_0}(z_0)$ (Lemma G.64); m, a probability measure (Lemma G.64); $w_k = 0$ for $k \geq 19$ (Lemma G.70); $e^t > 0$ (Fact A.41, item 12)]

(L14) $1/(1 - \varpi(s)) \leq 1/(1 - \varpi(s'))$

[(L10), (L12); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L15) $\Rightarrow$ $\forall k \geq 0:\ \epsilon_k^+(s) \leq \epsilon_k^+(s')$

[(L13), (L14); $\epsilon_k^+ := w_k/(1 - \varpi) - 1$ (Lemma G.70); Fact A.41, item 8]

(L16) $\forall k \geq 0\ \forall x \in \{s, s'\}:\ 1 + \epsilon_k^+(x) \geq 0$

[(L12), (L13); $\epsilon_k^+ := w_k/(1 - \varpi) - 1$ (Lemma G.70); Fact A.41, item 8]

(L17) $1/(1 + \varpi(s)) \leq 1/(1 - \varpi(s))$

[(L12); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L18) $\Rightarrow$ $\forall k \geq 0:\ \epsilon_k^-(s) \leq \epsilon_k^+(s)$

[(L13), (L17); $\epsilon_k^- := w_k/(1 + \varpi) - 1$, $\epsilon_k^+ := w_k/(1 - \varpi) - 1$ (Lemma G.70); Fact A.41, item 8]

(L19) $1/(1 + \varpi(s')) \leq 1/(1 + \varpi(s))$

[(L10), (L12); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L20) $\Rightarrow$ $\forall k \geq 0:\ \epsilon_k^-(s') \leq \epsilon_k^-(s)$

[(L13), (L19); $\epsilon_k^- := w_k/(1 + \varpi) - 1$ (Lemma G.70); Fact A.41, item 8]

(L21) $\forall a, b \in \mathbb{R}\ \forall t \in [a, b]:\ t^2 \leq \max(a^2, b^2)$

[$|t| \leq \max(|a|, |b|)$ at $t \in [a, b]$ (Fact A.41, items 1 and 20); $t \mapsto t^2$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L22) $\Rightarrow$ $\forall k \geq 0:\ \max(\epsilon_k^-(s)^2, \epsilon_k^+(s)^2) \leq \max(\epsilon_k^-(s')^2, \epsilon_k^+(s')^2)$

[(L21) at $t := \epsilon_k^{\pm}(s) \in [\epsilon_k^-(s'), \epsilon_k^+(s')]$ by (L15), (L18), (L20); Fact A.41, item 20]

(L23) $\forall k \leq 18:\ \bar{D}_k(s)(1 + \epsilon_k^+(s)) \in [0, \bar{D}_k(s')(1 + \epsilon_k^+(s'))]$

[(L7), (L8), (L15), (L16); Fact A.41, item 8]

(L24) $\Rightarrow$ $\forall v \in [0, \infty):\ h_s(v) \leq h_{s'}(v)$

[(L23); h_x (the proof's block); $\max(e_{+,k} - v, 0) \geq 0$ (Fact A.41, item 20); Fact A.41, item 8]

(L25) $\Rightarrow$ $\min_{v \in \{0, e_{+,0}, \ldots, e_{+,18}\}} h_s(v) \leq \min_{v \in \{0, e_{+,0}, \ldots, e_{+,18}\}} h_{s'}(v)$

[(L24); Fact A.41, item 20]

(L26) $\sum_{k\leq 18}(1 + \epsilon_k^+(s))\,\bar{e}_{\mathrm{fl},k} \leq \sum_{k\leq 18}(1 + \epsilon_k^+(s'))\,\bar{e}_{\mathrm{fl},k}$

[(L15), (L16); $\bar{e}_{\mathrm{fl},k}$ nonnegative ($\bar{e}_{\mathrm{fl},k}$, Lemma G.71); Fact A.41, item 8]

(L27) $\Rightarrow$ $\bar{e}_{\mathrm{norm}}(s) \leq \bar{e}_{\mathrm{norm}}(s')$

[(L25), (L26); $\bar{e}_{\mathrm{norm}}$ of Lemma G.72, at $\sigma_{\max} := s$ and at $\sigma_{\max} := s'$, the minimum of h_x over $\{0, e_{+,0}, \ldots, e_{+,18}\}$ plus $\sum_{k\leq 18}(1 + \epsilon_k^+(x))\,\bar{e}_{\mathrm{fl},k}$]

(L28) $\Rightarrow$ item 2

[(L27)]

(L29) $\forall x \in \{s, s'\}:\ \bar{e}_{\mathrm{norm}}(x) \in [0, 1)$

[(L7), (L16), (L27); assumption A4; $\bar{e}_{\mathrm{norm}}$ (Lemma G.72); Fact A.41, items 8 and 20]

(L30) $k_\tau(s) \leq k_\tau(s')$

[$k_\tau := \lfloor \tau\sigma_{\max} \rfloor$ (Lemma G.69); $s \leq s'$ (assumption A1); $\tau > 1$ (the statement); Fact A.41, item 22]

(L31) $k'_\tau(s) \leq k'_\tau(s')$

[(L30); $k'_\tau := \min(k_\tau, 18)$ (Lemma G.73); Fact A.41, item 20]

(L32) $\max_{k\le k'_\tau(s)} e_{+,k} \le \max_{k\le k'_\tau(s')} e_{+,k}$

[(L31); Fact A.41, item 20]

(L33) $1/(1-\bar e_{\mathrm{norm}}(s)) \le 1/(1-\bar e_{\mathrm{norm}}(s'))$

[(L27), (L29); $t\mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L34) $(\max_{k\le k'_\tau(s)} e_{+,k} + \bar e_{\mathrm{norm}}(s))/(1-\bar e_{\mathrm{norm}}(s)) \in [0, (\max_{k\le k'_\tau(s')} e_{+,k} + \bar e_{\mathrm{norm}}(s'))/(1-\bar e_{\mathrm{norm}}(s'))]$

[(L27), (L29), (L32), (L33); $e_{+,k}\ge 0$ (the statement); Fact A.41, item 8]

(L35) $\Rightarrow\ \bar w_{\mathrm{ar}}(s) \in [0, \bar w_{\mathrm{ar}}(s')]$

[(L34); $\bar w_{\mathrm{ar}}$ (Lemma G.73); $\alpha\ge 2$ (the statement); $t\mapsto t^p$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L36) $\forall k\ge 0:\ \max(\epsilon_k^+(s),0) \le \max(\epsilon_k^+(s'),0)$

[(L15); Fact A.41, item 24]

(L37) $\Rightarrow\ \forall k\ge 0:\ (1+\max(\epsilon_k^+(s),0))^{\alpha-2} \in [0, (1+\max(\epsilon_k^+(s'),0))^{\alpha-2}]$

[(L36); $1+\max(\epsilon_k^+(s),0)\ge 1$ (Fact A.41, item 20); $\alpha\ge 2$ (the statement); $t\mapsto t^p$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L38) $\Rightarrow\ \forall k\ge 0:\ \bar w_k(s) \in [0, \bar w_k(s')]$

[(L35), (L37); $\bar w_k$ (Lemma G.73); Fact A.41, item 8]

(L39) $\forall k\ge 0:\ (1+\epsilon_k^+(s))^2 \le (1+\epsilon_k^+(s'))^2$

[(L15), (L16); $t\mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L40) $(1/(1-\bar e_{\mathrm{norm}}(s)))^2 \le (1/(1-\bar e_{\mathrm{norm}}(s')))^2$

[(L29), (L33); $t\mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L41) $\Rightarrow\ \forall k\ge 0:\ \bar w'_k(s) \in [0, \bar w'_k(s')]$

[(L29), (L38), (L39), (L40); $\bar w'_k$ (Lemma G.73); Fact A.41, item 8]

(L42) $\forall k\ge 0:\ \bar D_k(s)\bar w_k(s)\max(\epsilon_k^-(s)^2, \epsilon_k^+(s)^2) \in [0, \bar D_k(s')\bar w_k(s')\max(\epsilon_k^-(s')^2, \epsilon_k^+(s')^2)]$

[(L7), (L8), (L22), (L38); $t^2\ge 0$ (Fact A.41, item 13); Fact A.41, item 8]

(L43) $\Rightarrow\ \bar M_{\mathrm{tab}}(s) \in [0, \bar M_{\mathrm{tab}}(s')]$

[(L30), (L42); $\bar M_{\mathrm{tab}}$ (Lemma G.73); Fact A.45, item 9]

(L44) $\forall k\ge 0:\ (e_{+,k}+\bar e_{\mathrm{norm}}(s))^2 \le (e_{+,k}+\bar e_{\mathrm{norm}}(s'))^2$

[(L27), (L29); $e_{+,k}\ge 0$ (the statement); $t\mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L45) $\Rightarrow\ \forall k\ge 0:\ \bar v_k(s) \in [0, \bar v_k(s')]$

[(L41), (L44); $\bar v_k$ (Lemma G.73); Fact A.41, item 8]

(L46) $\forall k\ge 0:\ \bar e^{(2)}_{\mathrm{fl},k}(s) \le \bar e^{(2)}_{\mathrm{fl},k}(s')$

[(L3); $s\le s'$ (assumption A1); $\bar e^{(2)}_{\mathrm{fl},k}$ of Lemma G.71, at $\sigma_{\max} := s$ and at $\sigma_{\max} := s'$; $\sigma_{\min}>0$ and $e_{\mathrm{ccs}}\in[0,1)$ (the statement); $e^t>0$ (Fact A.41, item 12); Fact A.41, item 8]

(L47) $\forall k\ge 0:\ \min(\bar D_k(s), \bar e_{\mathrm{fl},k}) \le \min(\bar D_k(s'), \bar e_{\mathrm{fl},k})$

[(L8); Fact A.41, item 25]

(L48) $\forall k\ge 0:\ \min(\bar D_k(s), \bar e_{\mathrm{fl},k}, \bar e^{(2)}_{\mathrm{fl},k}(s)) \le \min(\bar D_k(s'), \bar e_{\mathrm{fl},k}, \bar e^{(2)}_{\mathrm{fl},k}(s'))$

[(L8), (L46); Fact A.41, item 25]

(L49) $\forall k\ge 0:\ 2(e_{+,k}+\bar e_{\mathrm{norm}}(s))\min(\bar D_k(s), \bar e_{\mathrm{fl},k}) + \min(\bar D_k(s), \bar e_{\mathrm{fl},k}, \bar e^{(2)}_{\mathrm{fl},k}(s)) \in [0, 2(e_{+,k}+\bar e_{\mathrm{norm}}(s'))\min(\bar D_k(s'), \bar e_{\mathrm{fl},k}) + \min(\bar D_k(s'), \bar e_{\mathrm{fl},k}, \bar e^{(2)}_{\mathrm{fl},k}(s'))]$

[(L7), (L27), (L29), (L47), (L48); $e_{+,k}\ge 0$ (the statement); (L3); $\bar e_{\mathrm{fl},k}$ and $\bar e^{(2)}_{\mathrm{fl},k}$ of Lemma G.71; $\sigma_{\min}>0$ and $e_{\mathrm{ccs}}\in[0,1)$ (the statement); $e^t>0$ (Fact A.41, item 12); Fact A.41, item 8]

(L50) $\Rightarrow\ \forall k\ge 0:\ \bar w'_k(s)(2(e_{+,k}+\bar e_{\mathrm{norm}}(s))\min(\bar D_k(s), \bar e_{\mathrm{fl},k}) + \min(\bar D_k(s), \bar e_{\mathrm{fl},k}, \bar e^{(2)}_{\mathrm{fl},k}(s))) \in [0, \bar w'_k(s')(2(e_{+,k}+\bar e_{\mathrm{norm}}(s'))\min(\bar D_k(s'), \bar e_{\mathrm{fl},k}) + \min(\bar D_k(s'), \bar e_{\mathrm{fl},k}, \bar e^{(2)}_{\mathrm{fl},k}(s')))]$

[(L41), (L49); Fact A.41, item 8]

(L51) $\Rightarrow\ \bar M^{\mathrm{fl}}_{\mathrm{ar}}(s) \in [0, \bar M^{\mathrm{fl}}_{\mathrm{ar}}(s')]$

[(L31), (L50); $\bar M^{\mathrm{fl}}_{\mathrm{ar}}$ (Lemma G.73); Fact A.45, item 9]

(L52) $\forall k\ge 0\ \forall v\in[0,\infty):\ \max(\bar v_k(s)-v, 0) \le \max(\bar v_k(s')-v, 0)$

[(L45); Fact A.41, item 24]

(L53) $\forall k \geq 0\ \forall v \in [0,\infty):\ \bar{D}_k(s)\max(\bar{v}_k(s)-v,0) \in [0, \bar{D}_k(s')\max(\bar{v}_k(s')-v,0)]$
[(L7), (L8), (L52); $\max(\bar{v}_k(s)-v,0) \geq 0$ (Fact A.41, item 20); Fact A.41, item 8]

(L54) $\Rightarrow\ \forall v \in [0,\infty):\ f_s(v) \leq f_{s'}(v)$
[(L31), (L53); f_x (the proof's block); Fact A.45, item 9]

(L55) $\forall x \in \{s,s'\}\ \forall v \geq \max V(x):\ f_x(v) = v$
[f_x and $V(x)$ (the proof's block); $\max(\bar{v}_k(x)-v,0) = 0$ at $\bar{v}_k(x) \leq v$ (Fact A.41, item 20)]

(L56) $\forall x \in \{s,s'\}\ \forall v \geq \max V(x):\ f_x(\max V(x)) \leq f_x(v)$
[(L55) at v and at $\max V(x)$]

(L57) $\forall x \in \{s,s'\}\ \forall a,b \in V(x),\ a<b,\ (a,b)\cap V(x) = \emptyset\ \forall v \in [a,b]:\ f_x(v) \geq \min(f_x(a), f_x(b))$
[f_x affine on $[a,b]$ (f_x and $V(x)$, the proof's block); Fact A.41, item 16 at $-f_x$]

(L58) $\Rightarrow\ \forall x \in \{s,s'\}\ \forall v \in [0,\infty)\ \exists w \in V(x):\ f_x(w) \leq f_x(v)$
[(L56), (L57); $0 \in V(x)$ ($V(x)$, the proof's block); $V(x)$ finite ($V(x)$, the proof's block)]

(L59) $\min_{w\in V(s)} f_s(w) \leq \min_{w\in V(s')} f_{s'}(w)$
[(L58) at $x := s$ and at v a minimizer of $f_{s'}$ on $V(s')$, $V(s') \subseteq [0,\infty)$ by (L45); (L54)]

(L60) $\Rightarrow\ \bar{M}_{\mathrm{ar}}(s) \leq \bar{M}_{\mathrm{ar}}(s')$
[(L51), (L59); $\bar{M}_{\mathrm{ar}}$ of Lemma G.73, at $\sigma_{\max} := s$ and at $\sigma_{\max} := s'$, the minimum of f_x over $V(x)$ plus $\bar{M}^{\mathrm{fl}}_{\mathrm{ar}}(x)$]

(L61) $\forall v \in [0,\infty):\ f_s(v) \geq v$
[(L53); f_s (the proof's block); collect]

(L62) $\bar{M}_{\mathrm{ar}}(s) \geq 0$
[(L45), (L51), (L61); $V(s)$ (the proof's block); $\bar{M}_{\mathrm{ar}}$ of Lemma G.73, at $\sigma_{\max} := s$, the minimum of f_s over $V(s)$ plus $\bar{M}^{\mathrm{fl}}_{\mathrm{ar}}(s)$]

(L63) $\bar{M}_{\mathrm{tab}}(s)^{1/2} \leq \bar{M}_{\mathrm{tab}}(s')^{1/2}$
[(L43); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L64) $\bar{M}_{\mathrm{ar}}(s)^{1/2} \leq \bar{M}_{\mathrm{ar}}(s')^{1/2}$
[(L60), (L62); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L65) $\Rightarrow$ item 3
[(L63), (L64); $t \mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

□ (items 1 to 3)

Corollary G.75 (The bounds on $\bar{\rho}_B$ [to table])**.** *Bounds on the leaves' moments and tails on the sets $\mathcal{Z}_i$ bound the leaves' divergence $\bar{\rho}_B$ from above and below, and the fringe classes' factor κ_C from above. Let:*

- $\alpha > 1$, *an order;*
- $M_{2\alpha}$, p_τ, $p'_\tau \in \mathbb{R}$.

Define:

- $\epsilon_i := \widetilde{B}_i/\widetilde{D}_i - 1$;
- $\epsilon_{i,+} := \max(\epsilon_i, 0)$;
- $\epsilon_{\mathcal{Z}_i\setminus C_i} := \sup_{z_i \notin \mathcal{Z}_i\setminus C_i} \max(-\epsilon_i, 0)$, *that of Lemma G.65 at* $B := \widetilde{B}_i$, $D := \widetilde{D}_i$, $\mathcal{Y} := \mathcal{Z}_i \setminus C_i$.

Assume:

(A1) $\forall i \leq N\ \forall z_{<i} \in S_{<i}:\ \sum_{z_i \in \mathcal{Z}_i\setminus C_i} \widetilde{D}_i(1+\epsilon_{i,+})^{2\alpha-2}\epsilon_i^2 \leq M_{2\alpha}$;
(A2) $p_\tau \geq 0$;
(A3) $\forall i \leq N\ \forall z_{<i} \in S_{<i}:\ \widetilde{D}_i((\mathcal{Z}_i \setminus C_i)^c)\,\epsilon_{\mathcal{Z}_i\setminus C_i} \leq p_\tau$;
(A4) $\forall i \leq N\ \forall z_{<i} \in S_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i^c) \leq p'_\tau$;
(A5) $p'_\tau + \bar{p}_C < 1$.

Then $\ln \bar{\rho}_B$ is bounded above, $\bar{\rho}_B$ below, and κ_C above:

1. $\ln \bar{\rho}_B \leq \alpha\, M_{2\alpha} + 2\, p_\tau$;
2. $\bar{\rho}_B \geq (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$;

3. $\kappa_C \le \bar{U}^\alpha\,(1-p'_\tau-\bar{p}_C)^{-\alpha}$. *[derived]*

Proof. *Proof of item 1.*

Lemma G.65 at every $i \le N$ and $z_{<i} \in S_{<i}$	This proof
α	2α
(B, D)	$(\widetilde{B}_i, \widetilde{D}_i)$
$\mathcal{Y}$	$\mathcal{Z}_i \setminus C_i$
(ϵ, ϵ_+)	$(\epsilon_i, \epsilon_{i,+})$
$\epsilon_{\mathcal{Y}}$	$\epsilon_{\mathcal{Z}_i \setminus C_i}$
(I1) $M_{\alpha,\mathcal{Y}}$	$\sum_{z_i \in \mathcal{Z}_i \setminus C_i} \widetilde{D}_i (1+\epsilon_{i,+})^{2\alpha-2} \epsilon_i^2$
$\alpha \ge 2$	$\alpha > 1$ (the statement)
$B, D : \mathbb{Z} \to [0,1]$, $\sum_{x\in\mathbb{Z}} B(x) = 1$, $\sum_{x\in\mathbb{Z}} D(x) = 1$	$\widetilde{B}_i$, $\widetilde{D}_i$ (Definition A.28)
$\mathcal{Y} \subseteq \mathbb{Z}$	$\mathcal{Z}_i$ (Definition A.28)
Assumption A1	$\widetilde{D}_i$ (Definition A.28)
Assumption A2	Assumption A1; $M_{2\alpha}$ (the statement)
Its conclusion: $\sum_{z\in\mathcal{Y}} D(z)\,U(z)^\alpha \le 1 + \alpha\, D(\mathcal{Y}^c)\,\epsilon_{\mathcal{Y}} + \frac{\alpha(\alpha-1)}{2}\, M_{\alpha,\mathcal{Y}}$	

(L1) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i\setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha \widetilde{D}_i((\mathcal{Z}_i\setminus C_i)^c)\epsilon_{\mathcal{Z}_i\setminus C_i} + \alpha\,\alpha_L \sum_{z_i\in\mathcal{Z}_i\setminus C_i} \widetilde{D}_i(1+\epsilon_{i,+})^{2\alpha-2}\epsilon_i^2$

[(I1); $R_{2\alpha}^{\mathcal{Z}_i\setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} = \sum_{z_i\in\mathcal{Z}_i\setminus C_i} \widetilde{B}_i^{2\alpha}\widetilde{D}_i^{1-2\alpha}$ (Definition A.28)]

(L2) $\Rightarrow\ \forall i \le N\ \forall z_{<i} \in S_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i\setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\,\alpha_L M_{2\alpha}$

[(L1); assumptions A1, A2, A3]

(L3) $\Rightarrow\ \forall i \le N\ \forall z_{<i} \in S_{<i}:\ \alpha_L \ln R_{2\alpha}^{\mathcal{Z}_i\setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i) \le 2\alpha\, p_\tau + \alpha\,\alpha_L M_{2\alpha}$

[(L2); ln nondecreasing on $(0,\infty)$ and $\ln(1+x) \le x$ (Fact A.41, item 5); $\ln(y^{\alpha_L}) = \alpha_L \ln y$ (Fact A.41, item 12)]

(L4) $2\alpha/\alpha_L \le 2$

[$\alpha > 1$ (the statement)]

(L5) $\Rightarrow\ \forall i \le N\ \forall z_{<i} \in S_{<i}:\ \ln R_{2\alpha}^{\mathcal{Z}_i\setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i) \le \alpha\, M_{2\alpha} + 2\, p_\tau$

[(L3) divided by $\alpha_L > 0$; (L4); $p_\tau \ge 0$ (assumption A2)]

(L6) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i \setminus C_i) \ge (1 - p'_\tau - \bar{p}_C)$

[$\widetilde{B}_i(\mathbb{Z}) = 1$ (Fact A.45, item 5); $\widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$ (assumption A4) and $\widetilde{B}_i(C_i) \le \bar{p}_C$ at $z_{<i} \in S_{<i}$ ($\bar{p}_C$, Definition A.28); $(\mathcal{Z}_i \setminus C_i)^c = \mathcal{Z}_i^c \cup C_i$ (Fact A.41, item 17, at $(A,B) := (\mathcal{Z}_i, C_i)$); Fact A.45, item 5]

(L7) $(1 - p'_\tau - \bar{p}_C) > 0$

[$p'_\tau + \bar{p}_C < 1$ (assumption A5)]

(L8) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i\setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i) > 0$

[(L6), (L7); $R_{2\alpha}^{\mathcal{Z}_i\setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} = \sum_{z_i\in\mathcal{Z}_i\setminus C_i} \widetilde{B}_i^{2\alpha}\widetilde{D}_i^{1-2\alpha}$ (Definition A.28)]

(L9) $\bar{\rho}_B > 0$

[(L8); $\bar{\rho}_B = \max_{i\le N} \sup_{z_{<i}\in S_{<i}} R_{2\alpha}^{\mathcal{Z}_i\setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)$ (Definition A.28)]

(L10) $\bar{\rho}_B \le e^{\alpha M_{2\alpha} + 2p_\tau}$

[(L5) at every i, $z_{<i}$; $\bar{\rho}_B$ (Definition A.28); exp increasing (Fact A.41, item 5)]

(L11) $\Rightarrow$ item 1

[(L9), (L10); ln nondecreasing on $(0,\infty)$ (Fact A.41, item 5)]

□ (item 1)

Proof of item 2.

(L12) $\forall i \le N\ \forall z_{<i}:\ \sum_{z_i\in\mathcal{Z}_i\setminus C_i} \widetilde{B}_i^{2\alpha}\widetilde{D}_i^{1-2\alpha} \ge \widetilde{B}_i(\mathcal{Z}_i \setminus C_i)^{2\alpha}\, \widetilde{D}_i(\mathcal{Z}_i \setminus C_i)^{1-2\alpha}$

[Fact A.45, item 7 at $\mu := \widetilde{B}_i$, $\nu := \widetilde{D}_i$, $B := \mathcal{Z}_i \setminus C_i$ and the order $2\alpha > 1$ ($\mathrm{Supp}(\widetilde{D}_i) = \mathbb{Z}$, Definition A.28), raised to the power 2α and divided by $\widetilde{D}_i(B)^{\alpha_L} > 0$]

(L13) $\forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i \setminus C_i)^{2\alpha}\, \widetilde{D}_i(\mathcal{Z}_i \setminus C_i)^{1-2\alpha} \ge \widetilde{B}_i(\mathcal{Z}_i \setminus C_i)^{2\alpha}$
[$\widetilde{D}_i(\mathcal{Z}_i \setminus C_i) \le 1$ ($\widetilde{D}_i$ a probability measure, Definition A.28); $1-2\alpha < 0$ ($\alpha > 1$, the statement)]

(L14) $\Rightarrow\ \forall i \le N\ \forall z_{<i} \in S_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i) \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$
[(L6), (L7), (L12), (L13); $R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i) = (\sum_{z_i \in \mathcal{Z}_i \setminus C_i} \widetilde{B}_i^{2\alpha} \widetilde{D}_i^{1-2\alpha})^{1/\alpha_L}$ (Definition A.28); $t \mapsto t^{1/\alpha_L}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L15) $\Rightarrow\ \bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$
[(L14) at every i, $z_{<i}$; $\bar{\rho}_B = \max_{i \le N} \sup_{z_{<i} \in S_{<i}} R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)$ (Definition A.28)]

(L16) $\Rightarrow$ item 2
[(L15)]

□ (item 2)

Proof of item 3.

(L17) $((1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L})^{-\alpha_L/2} = (1 - p'_\tau - \bar{p}_C)^{-\alpha}$
[multiply the exponents]

(L18) $\kappa_C \le \bar{U}^\alpha\, (1 - p'_\tau - \bar{p}_C)^{-\alpha}$
[(L15); $\kappa_C = \bar{U}^\alpha \bar{\rho}_B^{-\alpha_L/2}$ and $\bar{U} \ge 0$ (Definition A.28); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ and $t \mapsto t^{\alpha_L/2}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5); (L17)]

(L19) $\Rightarrow$ item 3
[(L18)]

□ (item 3)

G.7 The terms of $\ln R$

G.7.1 The root node's diagonals

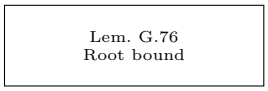


Figure 59: Dependencies, Section G.7.1.

Lemma G.76 (The root diagonals' bound [to table])**.** *At the root node, the computed diagonals of a Falcon-type signer are within χ_{root} of the ones over $\mathbb{R}$. Let:*

- *The signer be a Falcon-type signer at (u, ζ) (Definition 4.5);*
- $\chi_{00}, \chi_{11} \ge 0$.

Define:

- $\chi_{\text{root}} := \max(\chi_{00},\ \chi_{11})$.

Assume:

(A1) $\forall \psi:\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi_{00}^{\pm}, 0\right)\ d_{00}(\psi)$ *at the root node;*

(A2) $\forall \psi:\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi_{11}^{\pm}, 0\right)\ d_{11}(\psi)$ *at the root node.*

Then at the root node:

1. $\forall \psi:\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi_{\text{root}}^{\pm}, 0\right)\ d_{00}(\psi)$;
2. $\forall \psi:\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi_{\text{root}}^{\pm}, 0\right)\ d_{11}(\psi)$.

Proof. (L1) $\forall \psi:\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi_{\text{root}}^{\pm}, 0\right)\ d_{00}(\psi)$
[at the root node, χ_{00} for $\widetilde{d}_{00}$ (assumption A1); $\chi_{\text{root}} = \max(\chi_{00}, \chi_{11})$ (the statement)]

(L2) $\Rightarrow$ item 1
[(L1)]

(L3) $\forall \psi:\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{\mathrm{root}}, 0\right)\ d_{11}(\psi)$

[at the root node, χ_{11} for $\widetilde{d}_{11}$ (assumption A2); $\chi_{\mathrm{root}} = \max(\chi_{00}, \chi_{11})$ (the statement)]

(L4) $\Rightarrow$ item 2

[(L3)]

□

G.7.2 The leaf diagonals

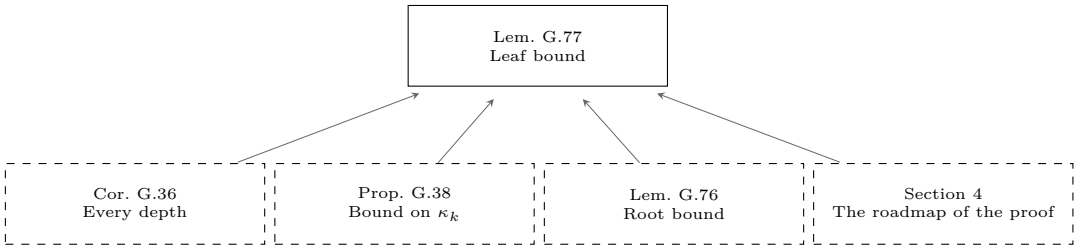


Figure 60: Dependencies, Section G.7.2.

Lemma G.77 (The leaf diagonals' bound [to table])**.** *The diagonals at the depth of the leaves are within χ_{leaf} of the ones over $\mathbb{R}$, those at each depth within that depth's iterate, and no iterate exceeds χ_{leaf}. Let:*

- *The signer be a Falcon-type signer at (u, ζ) (Definition 4.5);*
- $\chi_{00}, \chi_{11} \geq 0$.

Define:

- *The key constants*
  - *$\hat{K}$, the signer's key constants (Definition 4.6);*
  - *d_{lo} and d_{hi}, the floor and the ceiling of the diagonals below the root node (Definition 4.6);*
- *The tree*
  - *$T :=$ ffLDL$^{\dagger}(\mathcal{G})$ (Definition A.20), $\mathcal{G}$ the key's Gram matrix (Definition 4.6);*
  - *$\forall \nu \in \mathrm{Sub}(T):\ \mathcal{G}_\nu$, that of Definition A.32;*
  - *$\forall \nu \in \mathrm{Sub}(T)\ \forall \psi:\ (g_{00}, g_{01}, g_{11})$, the entries of $\mathcal{G}_\nu(\psi)$ (Definition A.14);*
- *The diagonals*
  - *$\forall \nu \in \mathrm{Sub}(T)\ \forall \psi:\ d^{\nu}_{00}(\psi) := g_{00}$ and $d^{\nu}_{11}(\psi) := g_{11} - |g_{01}|^2/g_{00}$ (Corollary G.36);*
  - *$\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}:\ \widetilde{d}^{\nu}_{j}$, the diagonal ffLDL† computes in $\mathcal{F}$ at ν in place of d^{ν}_{j} (Corollary G.36);*
- *The error chain*
  - *$\chi_{\mathrm{root}} := \max(\chi_{00},\ \chi_{11})$;*
  - *$\forall k \in \{1, \ldots, h-1\}:\ \vartheta_{k-1} := (1 + \chi^{\zeta}_{k-1})/(1 - \chi^{\zeta}_{k-1})$ (Corollary G.36);*
  - *$\forall k \in \{1, \ldots, h-1\}:\ \hat{\kappa}_k := \vartheta_{k-1}\kappa_k + (\vartheta_{k-1} - 1)/2$ (Corollary G.36);*
  - *$\chi^{\zeta}_{k} := \mathcal{U}^{\zeta}_{\hat{\kappa}_k}(\chi^{\zeta}_{k-1})$ from $\chi^{\zeta}_{0} := \chi_{\mathrm{root}}$, $\mathcal{U}^{\zeta}_{\kappa}$ that of Corollary G.36 at (u, ζ), d_{lo}, d_{hi} and κ_k of $\hat{K}$;*
  - *$\chi_{\mathrm{leaf}} := \chi^{\zeta}_{h-1}$.*

Assume:

(A1) $\forall \psi:\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{00}, 0\right)\ d_{00}(\psi)$ *at the root node;*

(A2) $\forall \psi:\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{11}, 0\right)\ d_{11}(\psi)$ *at the root node;*

(A3) $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi:\ d^{\nu}_{j}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$ *(Proposition D.9);*

(A4) $\forall k \in \{0, \ldots, h-1\}:\ \chi^{\zeta}_{k} \in \mathcal{A}$, *the admissible set of Corollary G.36.*

Then the diagonals and the iterates satisfy:

1. $\max_{\nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1}\ \max_{\psi} |\widetilde{d}_{\nu}/d_{\nu} - 1| \leq \chi_{\mathrm{leaf}}$;

2. $\forall k \in \{0,\dots,h-1\}\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = k\ \forall j \in \{00,11\}\ \forall \psi :\ \widetilde{d}^{\nu}_{j}(\psi)\ \mathcal{I}\left((\chi^{\zeta}_{k})^{\pm}, 0\right) d^{\nu}_{j}(\psi)$;

3. $\forall k \in \{0,\dots,h-1\} :\ \chi^{\zeta}_{k} \le \chi_{\mathrm{leaf}}$.

Proof. (L1) $\forall k \in \{1,\dots,h-1\}\ \forall \nu,\ \mathrm{depth}(\nu) = k\ \forall \psi :\ \kappa_{\nu}(\psi) \le \kappa_{k}$
[κ_k of $\hat{K}$ (Definition 4.6; Proposition G.38)]

(L2) $\forall k \in \{0,\dots,h-1\} :\ \chi^{\zeta}_{k} \ge 0$
[assumption A4; $\mathcal{A}$ (Corollary G.36)]

(L3) $\forall k \in \{0,\dots,h-1\} :\ \chi^{\zeta}_{k} < 1$
[assumption A4; $\mathcal{A}$ (Corollary G.36)]

(L4) $\forall k \in \{0,\dots,h-1\} :\ u_0(\chi^{\zeta}_{k}) < 1$
[assumption A4; $\mathcal{A}$ (Corollary G.36)]

(I1)

Lemma G.76 at the root node	This proof
Shared: the signer, u, ζ, χ_{00}, χ_{11}, χ_{root} Shared: $\chi_{00}, \chi_{11} \ge 0$ Shared: assumptions A1, A2	
the signer a Falcon-type signer at (u,ζ)	The statement
Its item 1: $\forall \psi :\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{\mathrm{root}}, 0\right) d_{00}(\psi)$	
Its item 2: $\forall \psi :\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{\mathrm{root}}, 0\right) d_{11}(\psi)$	

(L5) $\forall \psi :\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{\mathrm{root}}, 0\right) d_{00}(\psi)$
[item 1 of (I1)]

(L6) $\forall \psi :\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{\mathrm{root}}, 0\right) d_{11}(\psi)$
[item 2 of (I1)]

(I2)

Corollary G.36 at $(\mathcal{F}, \chi_0, \kappa_k) := (\mathcal{F}, \chi_{\mathrm{root}}, \kappa_k)$	This proof
Shared: $\mathcal{G}, T$ (Definition 4.6), $d_{\mathrm{lo}}, d_{\mathrm{hi}}$, κ_k, $\hat{\kappa}_k, \chi^{\zeta}_{k}$	
$\mathcal{F}, h$	$\mathcal{F}, h$ (the statement; Definition 4.5)
χ_0	χ_{root} (the statement)
$\mathcal{F}$ realization at (u,ζ)	The signer at (u,ζ) (the statement; Definition 4.5)
$h \ge 1$	Definition 4.5
$\mathcal{G} \in \mathrm{Gram}_n$	$\mathcal{G}$ (Definition 4.6)
$n := 2^h$	n (Definition 4.5)
$d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$	$d_{\mathrm{lo}} > 0$, $d_{\mathrm{hi}} \ge d_{\mathrm{lo}}$ (Definition 4.6)
$\forall k \in \{1,\dots,h-1\} :\ \kappa_k \in \mathbb{R}$	κ_k of $\hat{K}$ (Definition 4.6)
$\chi_0 \in [0,1)$	(L2), (L3) at $k=0$; $\chi^{\zeta}_{0} = \chi_{\mathrm{root}}$ (the statement)
Assumption A1	$u \in [0,1)$ (the statement; Definition 4.5)
Assumption A2	Assumption A3
Assumption A3	(L1)
Assumption A4	(L5), (L6)
Assumption A5	Definition A.8, item 1; $\lvert\psi\rvert = 1$ (Fact A.42, item 1)
Assumption A6	Assumption A4; (L2), (L3), (L4)
Its item 1: $\forall k \in \{0,\dots,h-1\}\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = k\ \forall j \in \{00,11\}\ \forall \psi :\ \widetilde{d}^{\nu}_{j}(\psi)\ \mathcal{I}\left((\chi^{\zeta}_{k})^{\pm}, 0\right) d^{\nu}_{j}(\psi)$	
Its item 3: $\forall k \in \{0,\dots,h-1\} :\ \chi^{\zeta}_{k} \le \chi^{\zeta}_{h-1}$	

(L7) $\forall k \in \{0,\dots,h-1\}\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = k\ \forall j \in \{00,11\}\ \forall \psi :\ \widetilde{d}^{\nu}_{j}(\psi)\ \mathcal{I}\left((\chi^{\zeta}_{k})^{\pm}, 0\right) d^{\nu}_{j}(\psi)$
[item 1 of (I2)]

(L8) $\max_{\nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu)=h-1}\ \max_{\psi} |\widetilde{d}_{\nu}/d_{\nu} - 1| \le \chi^{\zeta}_{h-1}$

[(L7) at $k := h-1$; Definition A.10]

(L9) $\chi^{\zeta}_{h-1} = \chi_{\text{leaf}}$

[χ_{leaf} (the statement)]

(L10) $\Rightarrow$ $\max_{\nu \in \text{Sub}(T),\ \text{depth}(\nu)=h-1}\ \max_{\psi} |\widetilde{d}_{\nu}/d_{\nu} - 1| \le \chi_{\text{leaf}}$

[(L8), (L9)]

(L11) $\Rightarrow$ item 1

[(L10)]

(L12) $\Rightarrow$ item 2

[(L7)]

(L13) $\forall k \in \{0, \ldots, h-1\}:\ \chi^{\zeta}_{k} \le \chi^{\zeta}_{h-1}$

[item 3 of (I2)]

(L14) $\Rightarrow$ $\forall k \in \{0, \ldots, h-1\}:\ \chi^{\zeta}_{k} \le \chi_{\text{leaf}}$

[(L13), (L9)]

(L15) $\Rightarrow$ item 3

[(L14)]

□ (items 1 to 3)

G.7.3 The leaf standard deviations

Lemma 4.7 (*Leaf standard deviations of a Falcon-type signer [to table]*) [to statement].
At every leaf the computed standard deviation is within $\bar{\delta}$ of the one over $\mathbb{R}$. Let:

- *The signer be a Falcon-type signer at (u, ζ) (Definition 4.5);*
- *$E_{00}, E_{11}, E_{01} \ge 0$;*
- *$\chi_{00}, \chi_{11} \ge 0$.*

Define:

- *$\hat{K}$, the signer's key constants, and m_0, M_0, d_{lo} and d_{hi}, the key's diagonal floors and ceilings (Definition 4.6);*
- *$T := \text{ffLDL}^{\dagger}(\mathcal{G})$ and $\mathcal{G}$, those of Definition 4.6;*
- *$\forall \nu \in \text{Sub}(T)\ \forall j \in \{00, 11\}:\ d^{\nu}_{j}$, that of Corollary G.36 at $\mathcal{G}$;*
- *$e_{00} := E_{00}/m_0$;*
- *$\texttt{INV_SIGMA}[\log_2 n]$, the stored inverse standard deviation of ffsamp (Algorithm 6) at the signer's degree n.*

Define:

Precondition 1. $\chi_{\text{root}} := \max(\chi_{00},\ \chi_{11})$: *$\chi_{00}$ the bound e_{00} of Lemma G.40, item 1, or the signer's own bound; χ_{11} the bound of Lemma G.40, item 2 at (u, ζ), E_{00}, E_{11}, E_{01} when $\widetilde{d}_{11}$ is the $LDL^{\dagger}$ step's, or the signer's own bound, from the NTRU identity (Fact A.33, item 2) or from its own corollary;*

Precondition 2. $\chi_{\text{leaf}} := \chi^{\zeta}_{h-1}$, *the iterate $\chi^{\zeta}_{k} = \mathcal{U}^{\zeta}_{\kappa_k}(\chi^{\zeta}_{k-1})$ from $\chi^{\zeta}_{0} = \chi_{\text{root}}$ of Corollary G.36 at (u, ζ), d_{lo}, d_{hi} and κ_k of $\hat{K}$, every iterate in its admissible set $\mathcal{A}$;*

Precondition 3. $k_J := (|c_n| + \sqrt{d_{\text{hi}}(1+\chi_{\text{leaf}})})(1+u)^2 + (1+u)\zeta + 1$ *and* $\chi^{\zeta}_{\sigma} := \chi_{\sigma} + k_J \zeta / s_{\min}$, *with χ_{σ} of Corollary G.41 at χ_{leaf}, $s_{\min} := \sqrt{d_{\text{lo}}}\, c_n$, $c_n := 1/s$ with s of Definition A.25;*

Precondition 4. $\bar{\delta} := \chi^{\zeta}_{\sigma}/(1 - \chi^{\zeta}_{\sigma})$ *(Definition A.27);*

Assume:

(A1) $\forall \psi:\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{00}, 0\right)\ d_{00}(\psi)$ *at the root node;*

(A2) $\forall \psi:\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi^{\pm}_{11}, 0\right)\ d_{11}(\psi)$ *at the root node;*

(A3) $\forall \nu \in \text{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi:\ d^{\nu}_{j}(\psi) \in [d_{\text{lo}}, d_{\text{hi}}]$ *(Proposition D.9);*

(A4) $\forall k \in \{0, \ldots, h-1\}:\ \chi^{\zeta}_{k} \in \mathcal{A}$, *the admissible set of Corollary G.36;*

(A5) $\chi_\sigma^\zeta < 1$;
(A6) $\texttt{INV_SIGMA}[\log_2 n]\ \mathcal{I}\,(u^\pm, \zeta^\pm)\ c_n$.
Then the leaf standard deviations are within $\bar\delta$ *at every prefix and on the tail-cut event:*

1. $\forall i \le N\ \forall z_{<i} :\ |\delta_i| \le \bar\delta$;
2. $\forall z \in S\ \forall i \le N :\ |\delta_i| \le \bar\delta$.

Proof.

DEFINES $k_J(t) := (|c_n| + \sqrt{t})(1+u)^2 + (1+u)\zeta + 1$, $t \ge 0$ (Corollary G.41 at $\widetilde{d}_{11} := t$)
DEFINES $\chi_\sigma^\zeta(t) := \chi_\sigma + k_J(t)\zeta/s_{\min}$, $t \ge 0$ (Corollary G.41 at $\widetilde{d}_{11} := t$)

(L1) $\texttt{isigma} = \sqrt{d_{11}}\, c_n$
[at a leaf diagonal (Lemma G.21)]

(L2) $\sqrt{d_{11}}\, c_n \ge \sqrt{d_{\mathrm{lo}}}\, c_n$
[$d_{11} \ge d_{\mathrm{lo}}$ (assumption A3); $c_n > 0$ ($c_n = 1/s$, the statement; $s > 0$, Definition A.25); $x \mapsto \sqrt{x}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L3) $\sqrt{d_{\mathrm{lo}}}\, c_n = s_{\min}$
[$s_{\min}$ (the statement)]

Lemma G.77	This proof
Shared: the signer, u, ζ, χ_{00}, χ_{11}, $\hat K, d_{\mathrm{lo}}, d_{\mathrm{hi}}$, χ_{root}, $\hat\kappa_k, \chi_k^\zeta, \chi_{\mathrm{leaf}}$ Shared: $\chi_{00}, \chi_{11} \ge 0$ Shared: assumptions A1, A2, A3, A4	(I1)
the signer a Falcon-type signer at (u,ζ)	The statement
Its item 1: $\max_{\nu\in\mathrm{Sub}(T),\ \mathrm{depth}(\nu)=h-1}\ \max_\psi \lvert\widetilde{d}_\nu/d_\nu - 1\rvert \le \chi_{\mathrm{leaf}}$	

(L4) $\max_{\nu\in\mathrm{Sub}(T),\ \mathrm{depth}(\nu)=h-1}\ \max_\psi \lvert\widetilde{d}_\nu/d_\nu - 1\rvert \le \chi_{\mathrm{leaf}}$
[item 1 of (I1)]

(L5) $\chi_{\mathrm{leaf}} \in [0,1)$
[$\chi_{\mathrm{leaf}} = \chi_{h-1}^\zeta$ (precondition 2); assumption A4]

(L6) $s_{\min} > 0$
[$s_{\min} = \sqrt{d_{\mathrm{lo}}}\, c_n$ (precondition 3); $d_{\mathrm{lo}} > 0$ (Definition 4.6); $c_n > 0$ ($c_n = 1/s$, precondition 3; $s > 0$, Definition A.25)]

(L7) $0 \le \chi_\sigma^\zeta$
[χ_σ^ζ and k_J (precondition 3); χ_σ (Corollary G.41); (L5), (L6); u and ζ (Definition A.4); Fact A.41, items 5 and 8]

(L8) $\forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1\ \forall \psi :\ \widetilde{d}_\nu \in (0, d_\nu(1+\chi_{\mathrm{leaf}})]$
[(L4), (L5); $d_j^\nu(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$ (assumption A3); $d_{\mathrm{lo}} > 0$ (Definition 4.6); Fact A.41, items 1 and 26]

(L9) $\forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1\ \forall \psi :\ d_\nu(1+\chi_{\mathrm{leaf}}) \le d_{\mathrm{hi}}(1+\chi_{\mathrm{leaf}})$
[$d_j^\nu(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$ (assumption A3); (L5); Fact A.41, item 26, at $c := 1+\chi_{\mathrm{leaf}}$]

(L10) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1\ \forall \psi :\ \sqrt{\widetilde{d}_\nu} \le \sqrt{d_{\mathrm{hi}}(1+\chi_{\mathrm{leaf}})}$
[(L8), (L9); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L11) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1\ \forall \psi :\ k_J(\widetilde{d}_\nu) \le k_J$
[(L10); $(1+u)^2 \ge 0$ (Fact A.41, item 13); Fact A.41, item 26, at $c := (1+u)^2$; $k_J(t)$ (the proof's block); k_J (precondition 3)]

(L12) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1\ \forall \psi :\ \chi_\sigma^\zeta(\widetilde{d}_\nu) \le \chi_\sigma^\zeta$
[(L11); $\zeta \ge 0$ (Definition A.4); (L6); Fact A.41, item 26, at $c := \zeta/s_{\min}$; $\chi_\sigma^\zeta(t)$ (the proof's block); χ_σ^ζ (precondition 3)]

(L13) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1\ \forall \psi :\ \chi_\sigma^\zeta(\widetilde{d}_\nu) < 1$
[(L12); $\chi_\sigma^\zeta < 1$ (assumption A5)]

(L14) $\forall t < 1 :\ t/(1-t) = 1/(1-t) - 1$
[expand]

(L15) $\Rightarrow$ $\forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1\ \forall \psi :\ \chi_\sigma^\zeta(\widetilde{d}_\nu)/(1-\chi_\sigma^\zeta(\widetilde{d}_\nu)) \le \chi_\sigma^\zeta/(1-\chi_\sigma^\zeta)$
[(L12), (L13), (L14); $\chi_\sigma^\zeta < 1$ (assumption A5); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

Corollary G.41 at every $i \le N$ and $z_{<i}$, at the leaf diagonal d_ν of σ_i	This proof

Shared: $\mathcal{F}$, $c_n, \chi_{\mathrm{leaf}}, s_{\min}$, `isigma` (L1), χ_σ
Shared: $n \in \{512, 1024\}$, $c_n \in \mathbb{R}$

(I2)

$d_{11}, \widetilde{d}_{11}$	$d_\nu, \widetilde{d}_\nu$ (L4)
δ_d	$\widetilde{d}_\nu/d_\nu - 1$ (L4)
k_J, χ_σ^ζ	$k_J(\widetilde{d}_\nu), \chi_\sigma^\zeta(\widetilde{d}_\nu)$ (the proof's block)
$\sigma, \widetilde{\sigma}$	$\sigma_i, \widetilde{\sigma}_i$ (Definition A.25; Definition A.27)
$\mathcal{F}$ realization at (u,ζ)	The signer at (u,ζ) (the statement; Definition 4.5)
$d_{11} > 0$	$d_j^\nu(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$ (assumption A3); $d_{\mathrm{lo}} > 0$ (Definition 4.6)
$\delta_d \in \mathbb{R}$	(L4)
$\chi_{\mathrm{leaf}} \in [0,1)$	(L5)
$s_{\min} > 0$	(L6)

Assumption A1	$u \in [0,1)$ (the statement; Definition 4.5)
Assumption A2	Assumption A6
Assumption A3	(L4)
Assumption A4	(L1), (L2), (L3)
Assumption A5	(L13)

Its conclusion: $\tilde{\sigma}\ \mathcal{I}\left(\left(\chi_\sigma^\zeta/(1-\chi_\sigma^\zeta)\right)^{\pm}, 0\right)\ \sigma$

(L16) $\forall i \le N\ \forall z_{<i} :\ \widetilde{\sigma}_i\ \mathcal{I}\left(\bar{\delta}^{\pm}, 0\right)\ \sigma_i$
[(I2); (L15); $\bar{\delta}$ (precondition 4); Definition A.10]

(L17) $\forall i \le N\ \forall z_{<i} :\ |\delta_i| \le \bar{\delta}$
[(L16); $\widetilde{\sigma}_i =: \sigma_i(1+\delta_i)$ (Definition A.27); Definition A.10]

(L18) $\Rightarrow$ item 1
[(L17)]

(L19) $\forall z \in S\ \forall i \le N :\ |\delta_i| \le \bar{\delta}$
[(L17) at $z_{<i}$ of $z \in S$]

(L20) $\Rightarrow$ item 2
[(L19)]

□ (items 1 and 2)

G.7.4 The node factors

Lemma 4.8 (*Node factors of a Falcon-type signer [to table]*) [to statement].
At every node the computed factor l_{10} is within E_l of the one over $\mathbb{R}$. Let:
- *The signer be a Falcon-type signer at (u,ζ) (Definition 4.5);*
- *$E_{00}, E_{11}, E_{01} \ge 0$;*
- *$\chi_{00}, \chi_{11} \ge 0$.*

Define:
- *The signer's words and parameters*
  - *$n := 2^h$, the signer's degree (Definition 4.5);*
  - *$\Psi_n := \{\psi_k : k < n/2\}$, that of Fact A.43 at $m := n$;*
- *The key constants*
  - *$\hat{K}$, the signer's key constants, and m_0, M_0, d_{lo} and d_{hi}, the key's diagonal floors and ceilings (Definition 4.6);*
  - *ℓ and κ_{root}, those of $\hat{K}$ (Definition 4.6);*
- *The tree*

– $T := \mathrm{ffLDL}^{\dagger}(\mathcal{G})$ *and* $\mathcal{G}$*, those of Definition 4.6;*
– $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\} :\ d_j^{\nu}$*, that of Corollary G.36 at* $\mathcal{G}$*;*

- *The error chain*
  – $e_{00} := E_{00}/m_0$*;*
  – $\chi_{\mathrm{root}} := \max(\chi_{00},\ \chi_{11})$*;*
  – $\forall k \in \{1, \ldots, h-1\} :\ \vartheta_{k-1} := (1 + \chi_{k-1}^{\zeta})/(1 - \chi_{k-1}^{\zeta})$ *(Corollary G.36);*
  – $\forall k \in \{1, \ldots, h-1\} :\ \hat{\kappa}_k := \vartheta_{k-1}\kappa_k + (\vartheta_{k-1} - 1)/2$ *(Corollary G.36);*
  – $\chi_k^{\zeta} := \mathcal{U}_{\hat{\kappa}_k}^{\zeta}(\chi_{k-1}^{\zeta})$ *from* $\chi_0^{\zeta} := \chi_{\mathrm{root}}$*,* $\mathcal{U}_{\kappa}^{\zeta}$ *that of Corollary G.36 at* (u, ζ)*,* d_{lo}*,* d_{hi} *and* κ_k *of* $\hat{K}$*;*
  – $\chi_{\mathrm{leaf}} := \chi_{h-1}^{\zeta}$*;*
- *The node bounds*
  – $u_0 := (1+u)(1+\zeta/(2d_{\mathrm{lo}}(1-\chi_{\mathrm{leaf}})(1-u))) - 1$ *and* $\bar{\delta}_{\mu} := (1+u)^2 - 1$ *(Corollary G.43 at* $\chi := \chi_{\mathrm{leaf}}$*);*
  – $c_{\mathrm{sa}} := (1+u)^2(1+u+\sqrt{2}\,\zeta) - 1$ *and* $k_{\mathrm{sa}} := (1+u)(1+u+\sqrt{2}\,\zeta)/2 + \sqrt{2}$ *(Corollary G.43);*
  – $M_2 := d_{\mathrm{hi}}(1+\chi_{\mathrm{leaf}})(1+c_{\mathrm{sa}})/2 + k_{\mathrm{sa}}\zeta$ *and* $\bar{e}_0 := (1+\chi_{\mathrm{leaf}})(1+u_0) - 1$ *(Corollary G.43 at* $\chi := \chi_{\mathrm{leaf}}$*);*
  – $\bar{a}_1 := c_{\mathrm{sa}} + \chi_{\mathrm{leaf}}(1+c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta/d_{\mathrm{lo}}$ *(Corollary G.43);*
  – $E_l^{\mathrm{child}} := \dfrac{\bar{\delta}_{\mu} + \bar{e}_0}{1 - \bar{e}_0} + \bar{a}_1 \dfrac{1 + \bar{\delta}_{\mu}}{1 - \bar{e}_0} + \sqrt{2}\,(M_2(1+u) + 1)\,\zeta$ *(Corollary G.43);*
  – $E_l^{\mathrm{root}} := \ell \dfrac{\bar{\delta}_{\mu} + e_{00}}{1 - e_{00}} + \dfrac{E_{01}}{m_0} \dfrac{1 + \bar{\delta}_{\mu}}{1 - e_{00}} + \sqrt{2}\,((\sqrt{\kappa_{\mathrm{root}}}\,q + E_{01})(1+u) + 1)\,\zeta$ *(Corollary G.43).*

Define:

Precondition 1. $E_l := \max(E_l^{\mathrm{child}}, E_l^{\mathrm{root}})$ *of Corollary G.43 at* (u, ζ)*,* $\chi := \chi_{\mathrm{leaf}}$*,* d_{lo}*,* d_{hi}*,* ℓ*,* m_0*,* e_{00}*,* E_{01} *and* κ_{root} *of* $\hat{K}$*, and* $\widetilde{\ell} := \ell + E_l$*;*

Assume:
(A1) $\forall \psi :\ |\widetilde{g}_{00}(\psi) - g_{00}(\psi)| \le E_{00}$*, for the computed Gram matrix entries against the Gram matrix over* $\mathbb{R}$ *of the images;*
(A2) $\forall \psi :\ |\widetilde{g}_{11}(\psi) - g_{11}(\psi)| \le E_{11}$*;*
(A3) $\forall \psi :\ |\widetilde{g}_{01}(\psi) - g_{01}(\psi)| \le E_{01}$*;*
(A4) $e_{00} < 1$*;*
(A5) $\forall \psi \in \Psi_n :\ g_{00}(\psi) \ge m_0$*;*
(A6) $\forall \psi \in \Psi_n :\ g_{00}(\psi) \le M_0$*;*
(A7) $\forall \psi :\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi_{00}^{\pm}, 0\right) d_{00}(\psi)$ *at the root node;*
(A8) $\forall \psi :\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi_{11}^{\pm}, 0\right) d_{11}(\psi)$ *at the root node;*
(A9) $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi :\ d_j^{\nu}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$ *(Proposition D.9);*
(A10) $\forall k \in \{0, \ldots, h-1\} :\ \chi_k^{\zeta} \in \mathcal{A}$*, the admissible set of Corollary G.36;*
(A11) $\bar{e}_0 < 1$*, with* $\bar{e}_0$ *that of Corollary G.43 at* (u, ζ)*,* $\chi := \chi_{\mathrm{leaf}}$ *and* d_{lo}*.*
Then the computed factors satisfy:

1. $\max_{\psi} |\widetilde{l}_{10} - l_{10}| \le E_l$*;*
2. $\max_{\psi} |\widetilde{l}_{10}| \le \widetilde{\ell}$*.*

Proof.

DEFINES $\widetilde{d}_j^{\nu}$, the diagonal ffLDL† computes in $\mathcal{F}$ at ν (Corollary G.36)
DEFINES $k \in \{1, \ldots, h-1\}$
DEFINES $\nu \in \mathrm{Sub}(T)$ at depth k, the child T_{jj} of its parent π, $j \in \{00, 11\}$ (Definition A.32)
DEFINES ψ, a root of π's ring
DEFINES $\widetilde{\psi} \in C_{\mathcal{F}}$, the stored root of ψ (Definition A.8, item 1)
DEFINES $a := d_j^{\pi}(\psi)$
DEFINES $b := d_j^{\pi}(-\psi)$
DEFINES $\widetilde{a} := \widetilde{d}_j^{\pi}(\psi)$
DEFINES $\widetilde{b} := \widetilde{d}_j^{\pi}(-\psi)$
DEFINES $\omega_a := \widetilde{a}/a - 1$
DEFINES $\omega_b := \widetilde{b}/b - 1$
DEFINES (d_0, d_1): the values of $\mathrm{split}_{\mathrm{sa}}$ (Algorithm 3) at d_j^{π} and ψ, at lines 5 and 7
COMPUTES $(\widetilde{d}_0, \widetilde{d}_1)$: the values $\mathrm{split}_{\mathrm{sa}}$ computes in $\mathcal{F}$ from $(f(\psi), f(-\psi)) := (\widetilde{a}, \widetilde{b})$ at lines 4 and 6, with $\widetilde{s} := \widetilde{\psi}$

Proof of item 1.

Lemma G.77	This proof
Shared: the signer, u, ζ, χ_{00}, χ_{11}, $\hat{K}, d_{\mathrm{lo}}, d_{\mathrm{hi}}$, χ_{root}, $\hat{\kappa}_k, \chi_k^{\zeta}, \chi_{\mathrm{leaf}}$ Shared: $\chi_{00}, \chi_{11} \geq 0$ Shared: assumptions A7, A8, A9, A10	
(I1) the signer a Falcon-type signer at (u, ζ)	The statement
Its item 2: $\forall k \in \{0, \ldots, h-1\}\ \forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = k\ \forall j \in \{00, 11\}\ \forall \psi :\ \widetilde{d}_j^{\nu}(\psi)\ \mathcal{I}\left((\chi_k^{\zeta})^{\pm}, 0\right)\ d_j^{\nu}(\psi)$	
Its item 3: $\forall k \in \{0, \ldots, h-1\} :\ \chi_k^{\zeta} \leq \chi_{\mathrm{leaf}}$	

(L1) at a child: $|\omega_a|, |\omega_b| \leq \chi_{k-1}^{\zeta}$
[item 2 of (I1) at π, depth $k-1$, j and $\pm\psi$; ω_a, ω_b (the proof's block); Definition A.10]

(L2) $\chi_{k-1}^{\zeta} \leq \chi_{\mathrm{leaf}}$
[item 3 of (I1) at $k-1$]

(L3) $\Rightarrow$ at a child: $|\omega_a|, |\omega_b| \leq \chi_{\mathrm{leaf}}$
[(L1), (L2)]

(L4) $u < 1$
[$u \in [0, 1)$ (the statement; Definition 4.5)]

(L5) $\chi_{\mathrm{leaf}} \in [0, 1)$
[$\chi_{\mathrm{leaf}} = \chi_{h-1}^{\zeta}$ (the statement); assumption A10; $\mathcal{A}$ (Corollary G.36)]

(L6) $u_0(\chi_{\mathrm{leaf}}) < 1$
[$\chi_{\mathrm{leaf}} = \chi_{h-1}^{\zeta}$ (the statement); assumption A10; $\mathcal{A}$ (Corollary G.36)]

	Fact D.1 at a child	This proof
	Shared: $\psi,\ a, b,\ \mathrm{AM}(a,b)$ (Definition A.46), d_0, d_1	
	m	2^{h-k+1} (π at depth $k-1$, the proof's block; Definition A.32)
	d	d_j^π (the proof's block)
	$m \geq 2$	π at depth $k-1 \leq h-2$ (the proof's block)
	$m \in \{2^j : j \in \mathbb{Z}_{\geq 0}\}$	$m := 2^{h-k+1}$ (the rows above)
	$d \in \mathcal{R}_m$	d_j^π (the proof's block)
(I2)	$\psi \in \mathbb{C}$	ψ, a root of π's ring (the proof's block)
	$\psi^m = -1$	ψ, a root of π's ring (the proof's block)
	Assumption A1	Assumption A9 at a (the proof's block); $d_{\mathrm{lo}} > 0$ (Definition 4.6)
	Assumption A2	Assumption A9 at b (the proof's block); $d_{\mathrm{lo}} > 0$ (Definition 4.6)
	Its item 1: $d_0 = \mathrm{AM}(a,b)$	
	Its item 2: $d_1 = ((a-b)/2)\ \mathrm{conj}\,\psi$	
	Its item 3: $\lvert d_1\rvert = \lvert a-b\rvert/2$	

(L7) at a child: $d_0 = \mathrm{AM}(a,b)$ [item 1 of (I2)]

(L8) at a child: $d_1 = ((a-b)/2)\ \mathrm{conj}\,\psi$ [item 2 of (I2)]

(L9) at a child: $\lvert d_1\rvert = \lvert a-b\rvert/2$ [item 3 of (I2)]

	Lemma G.32, item 1 at a child, at $\chi := \chi_{\mathrm{leaf}}$	This proof
	Shared: $\mathcal{F},\ d_{\mathrm{lo}}, d_{\mathrm{hi}},\ a, b,\ \psi, \widetilde{\psi},\ \omega_a, \omega_b$	
	χ	χ_{leaf} (the statement)
	u_0	$u_0(\chi_{\mathrm{leaf}})$ (Lemma G.32)
	$\mathcal{F}$ realization at (u,ζ)	The signer at (u,ζ) (the statement; Definition 4.5)
	$d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$	$d_{\mathrm{lo}} > 0$, $d_{\mathrm{hi}} \geq d_{\mathrm{lo}}$ (Definition 4.6)
	$a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$	Assumption A9
	$\psi \in \mathbb{C}$	ψ, a root of π's ring (the proof's block)
	$\widetilde{\psi} \in C_{\mathcal{F}}$	$\widetilde{\psi}$ (the proof's block)
(I3)	$\chi \in [0,1)$	(L5)
	$\omega_a, \omega_b \in \mathbb{R}$	ω_a, ω_b (the proof's block)
	Assumption A1	$\widetilde{a}$, $\widetilde{b}$, $\widetilde{d}_j^\nu$, computed in $\mathcal{F}$ (the proof's block)
	Assumption A2	(L4)
	Assumption A3	(L3)
	Assumption A4	(L3)
	Assumption A5	ψ, a root of π's ring (the proof's block); Fact A.42, item 1
	Assumption A6	Definition A.8, item 1; $\lvert\psi\rvert = 1$ (Fact A.42, item 1)
	Assumption A7	(L6)
	Its item 1: $\tilde{d}_0\ \mathcal{I}\left(((1+\chi)(1+u_0)-1)^{\pm}, 0\right)\ \mathrm{AM}(a,b)$	

(L10) at a child: $\widetilde{d}_0\ \mathcal{I}\left(((1+\chi_{\mathrm{leaf}})(1+u_0(\chi_{\mathrm{leaf}}))-1)^{\pm}, 0\right)\ \mathrm{AM}(a,b)$ [item 1 of (I3)]

(L11) at a child: $\exists\, e_0 \in \mathbb{R},\ \lvert e_0\rvert \leq \bar{e}_0 :\ \widetilde{d}_0 = d_0(1+e_0)$ [(L10), (L7); $\bar{e}_0$ (the statement); u_0 (Corollary G.43; Lemma G.32); Definition A.10]

(L12) at a child: $\lvert e_0\rvert < 1$ [(L11); $\bar{e}_0 < 1$ (assumption A11)]

(L13) at a child: $d_0 \geq d_{\mathrm{lo}}$

[(L7); $a, b \geq d_{\mathrm{lo}}$ (assumption A9); $\min(a,b) \leq \mathrm{AM}(a,b)$ (Fact A.41, item 9)]

(L14) at a child: $|d_1| \leq d_0$

[(L7), (L9); $a, b > 0$ (assumption A9; $d_{\mathrm{lo}} > 0$, Definition 4.6); $|x+y| \leq |x| + |y|$ (Fact A.41, item 1) at $(x, y) := (a, -b)$]

(L15) at a child: $|l_{10}| \leq 1$

[(L14); $l_{10} = \mathrm{conj}(d_1)/d_0$ (Corollary G.43); $|\mathrm{conj}\, x| = |x|$ (Fact A.41, item 1)]

Lemma G.37 at a child, at $\chi := \chi_{\mathrm{leaf}}$	This proof
Shared: $\mathcal{F}$, a, b, $\psi, \widetilde{\psi}$, ω_a, ω_b	
χ	χ_{leaf} (the statement)
$\mathcal{F}$ realization at (u, ζ)	The signer at (u, ζ) (the statement; Definition 4.5)
$a, b > 0$	Assumption A9; $d_{\mathrm{lo}} > 0$ (Definition 4.6)
$\psi \in \mathbb{C}$	ψ, a root of π's ring (the proof's block)
$\widetilde{\psi} \in C_{\mathcal{F}}$	$\widetilde{\psi}$ (the proof's block)
$\chi \in \mathbb{R}$	(L5)
(I4) $\omega_a, \omega_b \in \mathbb{R}$	ω_a, ω_b (the proof's block)
Assumption A1	(L3)
Assumption A2	(L3)
Assumption A3	$\widetilde{a}$, $\widetilde{b}$ (the proof's block)
Assumption A4	ψ, a root of π's ring (the proof's block); Fact A.42, item 1
Assumption A5	Definition A.8, item 1; $\lvert\psi\rvert = 1$ (Fact A.42, item 1)
Its conclusion: $\lvert\widetilde{d}_1 - d_1\rvert \leq c_{\mathrm{sa}}\lvert d_1\rvert + \chi\, d_0(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta$	

(L16) at a child: $|\widetilde{d}_1 - d_1| \leq c_{\mathrm{sa}}|d_1| + \chi_{\mathrm{leaf}} d_0(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta$

[(I4); $d_0 = (a+b)/2$ (L7); $d_1 = ((a-b)/2)\ \mathrm{conj}\,\psi$ (L8)]

(L17) $\Rightarrow$ at a child: $|\widetilde{d}_1 - d_1| \leq \bar{a}_1 d_0$

[(L16), (L13), (L14); c_{sa}, k_{sa} (Corollary G.43); u, ζ (Definition A.4); $\bar{a}_1$ (the statement)]

Lemma G.26 at a child	This proof
Shared: $\mathcal{F}$, $\psi, \widetilde{\psi}$, $\widetilde{a}, \widetilde{b}$	
$\mathcal{F}$ realization at (u, ζ)	The signer at (u, ζ) (the statement; Definition 4.5)
$\psi \in \mathbb{C}$	ψ, a root of π's ring (the proof's block)
$\widetilde{\psi} \in C_{\mathcal{F}}$	$\widetilde{\psi}$ (the proof's block)
(I5) $\widetilde{a}, \widetilde{b} \in \mathcal{F}$	$\widetilde{a}$, $\widetilde{b}$ (the proof's block)
Assumption A1	ψ, a root of π's ring (the proof's block); Fact A.42, item 1
Assumption A2	Definition A.8, item 1; $\lvert\psi\rvert = 1$ (Fact A.42, item 1)
Its conclusion: $\exists\, \delta_{\mathrm{sa}}, e_{\mathrm{sa}} \in \mathbb{C},\ \lvert\delta_{\mathrm{sa}}\rvert \leq c_{\mathrm{sa}},\ \lvert e_{\mathrm{sa}}\rvert \leq k_{\mathrm{sa}}\zeta :\ \widetilde{d}_1 = \frac{\widetilde{a}-\widetilde{b}}{2}\,\mathrm{conj}(\psi)(1+\delta_{\mathrm{sa}}) + e_{\mathrm{sa}}$	

(L18) at a child: $\exists\, \delta_{\mathrm{sa}}, e_{\mathrm{sa}} \in \mathbb{C},\ |\delta_{\mathrm{sa}}| \leq c_{\mathrm{sa}},\ |e_{\mathrm{sa}}| \leq k_{\mathrm{sa}}\zeta :\ \widetilde{d}_1 = \frac{\widetilde{a}-\widetilde{b}}{2}\,\mathrm{conj}(\psi)(1+\delta_{\mathrm{sa}}) + e_{\mathrm{sa}}$

[(I5)]

(L19) at a child: $\widetilde{a}, \widetilde{b} \in (0, d_{\mathrm{hi}}(1 + \chi_{\mathrm{leaf}})]$

[$\widetilde{a}$, $\widetilde{b}$, ω_a, ω_b (the proof's block); assumption A9; d_{lo} (Definition 4.6); (L3), (L5)]

(L20) $\Rightarrow$ at a child: $|\widetilde{a} - \widetilde{b}| \leq d_{\mathrm{hi}}(1 + \chi_{\mathrm{leaf}})$

[(L19); $\widetilde{a} - \widetilde{b} < \widetilde{a}$ and $\widetilde{b} - \widetilde{a} < \widetilde{b}$ ($\widetilde{a}, \widetilde{b} > 0$, (L19))]

(L21) $\Rightarrow$ at a child: $|\widetilde{d}_1| \leq M_2$

[(L18), (L20); $|\mathrm{conj}\,\psi| = 1$ (Fact A.42, item 1); $|x+y| \leq |x| + |y|$, $|xy| = |x||y|$ (Fact A.41, item 1); M_2 (the statement)]

(L22) at a child: $\widetilde{d}_0 > 0$

[(L11), (L12), (L13); $d_{\mathrm{lo}} > 0$ (Definition 4.6)]

	Lemma G.24, item 2 at a child	This proof
	Shared: $\mathcal{F}$	
	g_{00}, g_{01}	$\widetilde{d}_0, \widetilde{d}_1$ (the proof's block)
	$\mathcal{F}$ realization at (u, ζ)	The signer at (u, ζ) (the statement; Definition 4.5)
(I6)	$g_{00} \in \mathcal{F}$	$\widetilde{d}_0$, computed in $\mathcal{F}$ (the proof's block)
	$g_{01} \in C_{\mathcal{F}}$	$\widetilde{d}_1$, computed in $\mathcal{F}$ (the proof's block)
	Assumption A1	(L4)
	Assumption A2	(L22)
	Its item 2: $\exists\, \delta', e' \in \mathbb{C},\ \lvert\delta'\rvert \le (1+u)^2 - 1,\ \lvert e'\rvert \le k_\mu\, \zeta :\ \widetilde{l}_{10} = l_{10}(1+\delta') + e'$	
(L23)	at a child: $\exists\, \delta, e \in \mathbb{C},\ \lvert\delta\rvert \le \bar{\delta}_\mu,\ \lvert e\rvert \le \sqrt{2}\,(M_2(1+u)+1)\,\zeta :\ \widetilde{l}_{10} = (\operatorname{conj}\widetilde{d}_1/\widetilde{d}_0)(1+\delta) + e$ [item 2 of (I6); $l_{10} = \operatorname{conj}(\widetilde{d}_1)/\widetilde{d}_0$ at $(\widetilde{d}_0, \widetilde{d}_1, \widetilde{d}_0)$ (LDL† (Algorithm 5), line 13); k_μ (Lemma G.24) at $\lvert g_{01}\rvert := \lvert\widetilde{d}_1\rvert$, (L21); $\bar{\delta}_\mu$ (the statement)]	

	Corollary G.43, item 1 at a child, at (u, ζ) and $\chi := \chi_{\text{leaf}}$	This proof
	Shared: $u, \zeta,\ d_{\text{lo}}, d_{\text{hi}}, \ell, m_0, e_{00}, E_{01}, \kappa_{\text{root}},\ e_0$ (L11), δ, e (L23), $M_2, \bar{\delta}_\mu, \bar{e}_0, \bar{a}_1, E_l^{\text{child}}$	
	χ	χ_{leaf} (the statement)
	$d_0, \widetilde{d}_0, d_1, \widetilde{d}_1, \widetilde{l}_{10}$	$d_0, \widetilde{d}_0, d_1, \widetilde{d}_1, \widetilde{l}_{10}$ (L7) to (L23), at a child
	$q := 12289$	The statement
	$u \in [0, 1)$	$u \ge 0$ (Definition A.4); (L4)
	$\zeta \in \mathbb{R}$	ζ (Definition A.4)
	$\chi \in [0, 1)$	$\chi_{\text{leaf}} = \chi_{h-1}^{\zeta}$ (the statement); assumption A10
	$d_{\text{lo}}, d_{\text{hi}} > 0$	$d_{\text{lo}} > 0$, $d_{\text{hi}} \ge d_{\text{lo}}$ (Definition 4.6)
	$\ell \in \mathbb{R}$	ℓ (Definition 4.6)
	$m_0 > 0$	Definition 4.6
	$e_{00} \in [0, 1)$	e_{00} (the statement); assumption A4
	$E_{01} \in \mathbb{R}$	$E_{00}, E_{11}, E_{01} \ge 0$ (the statement)
	$\kappa_{\text{root}} \ge 0$	κ_{root} (Definition 4.6)
(I7)	$d_0 > 0$	(L13); $d_{\text{lo}} > 0$ (Definition 4.6)
	$\widetilde{d}_0 \in \mathbb{R}$	(L11)
	$d_1, \widetilde{d}_1 \in \mathbb{C}$	(L17)
	$e_0 \in \mathbb{R}$	(L11)
	$\delta, e \in \mathbb{C}$	(L23)
	$\widetilde{l}_{10} \in \mathbb{C}$	(L23)
	Assumption A1	(L12)
	Assumption A2	(L11)
	Assumption A3	(L23)
	Assumption A4	(L23)
	Assumption A5	Assumption A11
	Assumption A6	(L11)
	Assumption A7	(L15)
	Assumption A8	(L17)
	Assumption A9	(L23)
	Its conclusion: $\lvert\widetilde{l}_{10} - l_{10}\rvert \le E_l^{\text{child}}$	
(L24)	at a child: $\lvert\widetilde{l}_{10} - l_{10}\rvert \le E_l^{\text{child}}$ [(I7)]	
(L25)	at the root node: $\forall \psi \in \Psi_n :\ g_{00}(\psi) \ge m_0$ [assumption A5]	

Lemma G.40, item 1 at the root node, at every $\psi \in \Psi_n$	This proof
Shared: $u, \zeta,\ g_{00}, g_{11}, g_{01},\ \widetilde{g}_{00}, \widetilde{g}_{11}, \widetilde{g}_{01},\ E_{00}, E_{11}, E_{01},\ m_0, M_0, e_{00},\ \widetilde{d}_{00}$	
(a_{00}, a_{11}, a)	$(\widetilde{g}_{00} - g_{00}, \widetilde{g}_{11} - g_{11}, \widetilde{g}_{01} - g_{01})$
$(\bar{g}_0, \bar{g}_{11}, \bar{g}_{01}, \bar{g}_2)$	$(M_0, g_{11}, \lvert g_{01}\rvert, \lvert g_{01}\rvert^2 g_{00})$
d_{00}	g_{00} (the proof's block, at the root node)
$\mathcal{F}$ realization at (u, ζ)	The signer at (u, ζ) (the statement; Definition 4.5)
$q = 12289$	Fact A.33
$g_{00}, g_{11} \in \mathbb{R},\ g_{01} \in \mathbb{C}$	g_{00}, g_{11}, g_{01} (assumption A1; Definition 4.6)
$E_{00}, E_{11}, E_{01} \in \mathbb{R}$	$E_{00}, E_{11}, E_{01} \geq 0$ (the statement)
$m_0 > 0$	Definition 4.6
Assumption A1	(L4)
(I8) Assumption A2	Fact A.33, item 2
Assumption A3	(L25)
Assumption A4	Assumption A6
Assumption A5	Assumption A6
Assumption A6	$\bar{g}_{11} := g_{11}$ (the rows above)
Assumption A7	$\bar{g}_{01} := \lvert g_{01}\rvert$ (the rows above)
Assumption A8	$\bar{g}_2 := \lvert g_{01}\rvert^2 g_{00}$ (the rows above)
Assumption A9	Assumption A1
Assumption A10	Assumption A2
Assumption A11	Assumption A3
Assumption A12	$\widetilde{g}_{00}$, $\widetilde{g}_{11}$, computed in $\mathcal{F}$ (assumption A1)
Assumption A13	$\widetilde{g}_{01}$, computed in $\mathcal{F}$ (assumption A3)
Assumption A14	Assumption A4
Its item 1: $\tilde{d}_{00}\ \mathcal{I}\left(e_{00}^{\pm}, 0\right)\ d_{00}$	

(L26) at the root node: $\exists\, e_0 \in \mathbb{R},\ |e_0| \leq e_{00} :\ \widetilde{d}_{00} = g_{00}(1 + e_0)$

[(I8); $e_{00} < 1$ (assumption A4); e_{00} (the statement)]

(L27) at the root node: $|e_0| < 1$

[(L26); $e_{00} < 1$ (assumption A4)]

(L28) at the root node: $|\widetilde{g}_{01} - g_{01}| \leq E_{01}$

[assumption A3]

(L29) at the root node: $|l_{10}| \leq \ell$

[ℓ (Definition 4.6)]

(L30) at the root node: $|\widetilde{g}_{01}| \leq \sqrt{\kappa_{\text{root}}}\, q + E_{01}$

[(L28); $|g_{01}| \leq \sqrt{\kappa_{\text{root}}}\, q$ (Fact A.33, item 6); $|x + y| \leq |x| + |y|$ (Fact A.41, item 1)]

Lemma G.24, item 1 at the root node	This proof
Shared: $\mathcal{F}$	
g_{00}, g_{01}	$\widetilde{g}_{00}, \widetilde{g}_{01}$
$\mathcal{F}$ realization at (u, ζ)	The signer at (u, ζ) (the statement; Definition 4.5)
(I9) $g_{00} \in \mathcal{F}$	$\widetilde{g}_{00}$, computed in $\mathcal{F}$ (assumption A1)
$g_{01} \in C_{\mathcal{F}}$	$\widetilde{g}_{01}$, computed in $\mathcal{F}$ (assumption A3)
Assumption A1	(L4)
Assumption A2	(L25), (L26), (L27)
Its item 1: $\exists\, \delta, e \in \mathbb{C},\ \lvert\delta\rvert \leq (1+u)^2 - 1,\ \lvert e\rvert \leq k_\mu\, \zeta :\ \widetilde{\mu} = \mu(1+\delta) + e$	

(L31) at the root node: $\exists\, \delta, e \in \mathbb{C},\ |\delta| \leq \bar{\delta}_\mu,\ |e| \leq \sqrt{2}\,((\sqrt{\kappa_{\text{root}}}\, q + E_{01})(1+u) + 1)\,\zeta :\ \widetilde{l}_{10} = (\operatorname{conj} \widetilde{g}_{01}/\widetilde{d}_{00})(1+\delta) + e$

[(I9); (L30); $\widetilde{l}_{10} = \operatorname{conj}(\widetilde{\mu})$ at LDL† (Algorithm 5), line 10; $|\operatorname{conj} x| = |x|$ (Fact A.41, item 1); $\bar{\delta}_\mu$ (the statement)]

	Corollary G.43, item 2 at the root node, at (u, ζ), ℓ, m_0, e_{00}, E_{01} and κ_{root}	This proof
	Shared: $u, \zeta,\ d_{\text{lo}}, d_{\text{hi}}, \ell, m_0, e_{00}, E_{01}, \kappa_{\text{root}},\ e_0$ (L26), δ, e (L31), $\bar{\delta}_\mu, E_l^{\text{root}}$	
	χ	χ_{leaf} (the statement)
	$d_0, \widetilde{d}_0, d_1, \widetilde{d}_1$	$g_{00}, \widetilde{d}_{00}, g_{01}, \widetilde{g}_{01}$ (L25), (L26), (L28), at the root node
	$\widetilde{l}_{10}$	$\widetilde{l}_{10}$ (L31), at the root node
	$q := 12289$	The statement
	$u \in [0, 1)$	$u \geq 0$ (Definition A.4); (L4)
	$\zeta \in \mathbb{R}$	ζ (Definition A.4)
	$\chi \in [0, 1)$	$\chi_{\text{leaf}} = \chi_{h-1}^{\zeta}$ (the statement); assumption A10
	$d_{\text{lo}}, d_{\text{hi}} > 0$	$d_{\text{lo}} > 0$, $d_{\text{hi}} \geq d_{\text{lo}}$ (Definition 4.6)
	$\ell \in \mathbb{R}$	ℓ (Definition 4.6)
	$m_0 > 0$	Definition 4.6
	$e_{00} \in [0, 1)$	e_{00} (the statement); assumption A4
	$E_{01} \in \mathbb{R}$	$E_{00}, E_{11}, E_{01} \geq 0$ (the statement)
(I10)	$\kappa_{\text{root}} \geq 0$	κ_{root} (Definition 4.6)
	$d_0 > 0$	(L25); $m_0 > 0$ (Definition 4.6)
	$\widetilde{d}_0 \in \mathbb{R}$	(L26)
	$d_1, \widetilde{d}_1 \in \mathbb{C}$	(L28)
	$e_0 \in \mathbb{R}$	(L26)
	$\delta, e \in \mathbb{C}$	(L31)
	$\widetilde{l}_{10} \in \mathbb{C}$	(L31)
	Assumption A1	(L27)
	Assumption A2	(L26)
	Assumption A3	(L31)
	Assumption A4	(L31)
	Assumption A10	(L26)
	Assumption A11	(L29)
	Assumption A12	(L25)
	Assumption A13	(L28)
	Assumption A14	(L31)
	Its conclusion: $\lvert\widetilde{l}_{10} - l_{10}\rvert \leq E_l^{\text{root}}$	

(L32) at the root node: $|\widetilde{l}_{10} - l_{10}| \leq E_l^{\text{root}}$

[(I10)]

(L33) $\max_\psi |\widetilde{l}_{10} - l_{10}| \leq E_l$

[(L24), (L32); $E_l = \max(E_l^{\text{child}}, E_l^{\text{root}})$ (the statement)]

(L34) $\Rightarrow$ item 1

[(L33)]

□ (item 1)

Proof of item 2.

(L35) $\max_\psi |\widetilde{l}_{10}| \leq \ell + E_l$

[(L33); $|l_{10}| \leq \ell$ (Definition 4.6); $|x + y| \leq |x| + |y|$ (Fact A.41, item 1)]

(L36) $\ell + E_l = \widetilde{\ell}$

[$\widetilde{\ell}$ (the statement)]

(L37) $\Rightarrow$ $\max_\psi |\widetilde{l}_{10}| \leq \widetilde{\ell}$

[(L35), (L36)]

(L38) $\Rightarrow$ item 2

[(L37)]

□ (item 2)

G.7.5 The center shift

Lemma 4.9 (*Center shift of a Falcon-type signer [to table]*) [to statement].

The shift of the leaf centers is at most D_S, so the sum of the squared relative shifts is at most W° on the tail-cut event. Let:

- *The signer be a Falcon-type signer at (u, ζ) (Definition 4.5);*
- *$t \in \mathcal{R}_n \times \mathcal{R}_n$, a center;*
- *$\widetilde{t}_T$, the value the signer computes for t in $\mathcal{F}$;*
- *$e_{\text{root}} \in \mathcal{R}_n \times \mathcal{R}_n$;*
- *$\bar{T} \geq 0$;*
- *$\bar{Z} \geq 0$;*
- *$\bar{\delta} \in [0, 1)$ with $\forall z \in S\ \forall i \leq N :\ |\delta_i| \leq \bar{\delta}$, δ_i of Definition A.27;*
- *$E_l \in \mathbb{R}$ with $\max_\psi |\widetilde{l}_{10} - l_{10}| \leq E_l$ at every node of the key's tree;*
- *$\widetilde{\ell} \in \mathbb{R}$ with $\max_\psi |\widetilde{l}_{10}| \leq \widetilde{\ell}$ at every node of the key's tree.*

Define:

- *The key constants*
  - *$\hat{K}$, the signer's key constants (Definition 4.6);*
  - *ℓ, that of $\hat{K}$ (Definition 4.6);*
- *The samples*
  - *$z' := (z_0, z_1)$, the sample* ffsamp *(Algorithm 6) returns at t (*ffSampling$^{\mathcal{F}}$ *(Algorithm 10), line 24);*
- *The leaf perturbations*
  - *$\forall i \leq N\ \forall z_{<i} :\ \Delta_i(z_{<i}) := \widetilde{t}_i(z_{<i}) - t_i(z_{<i})$ (Definition A.27);*
  - *$\Delta := (\Delta_i)_{i \leq N}$;*
  - *$W(z) := \sum_{i \leq N} \Delta_i(z_{<i})^2 / \sigma_i(z_{<i})^2$.*

Define:

Precondition 1. *$D_S := D^\circ / (1 - \gamma - \gamma_S)$ with D°, γ, γ_S of Corollary G.62 at (u, ζ) and the key's own constants: at $T :=$ ffLDL$^\dagger(\mathcal{G})$ (Definition 4.6), the key's tree, its Ξ'_{root}, Ξ'_k and Ξ (Definition 4.6), its ℓ of $\hat{K}$, and the maxima $\max_{\nu,\psi} |\widetilde{l}_{10}|$ and $\max_{\nu,\psi} |\widetilde{l}_{10} - l_{10}|$ over T's nodes (Theorem G.59); at $\|e_{\text{root}}\|$, $\bar{T}$, $Z := \bar{Z}$, τ and $\sigma_{\max} := 1.17^2 \sigma_{\min}$;*

Precondition 2. *$W^\circ := D_S^2 / \sigma_{\min}^2$;*

Assume:

(A1) $\|\widetilde{t}_T - t\| \leq \|e_{\text{root}}\|$, in the coefficient norm (Appendix G.5);
(A2) $\|t\| \leq \bar{T}$;
(A3) $\forall z \in S :\ \|z'\| \leq \bar{Z}$;
(A4) $\gamma + \gamma_S < 1$;
(A5) $\sigma_{\min} > 0$;
(A6) $\forall i \leq N\ \forall z_{<i} \in S_{<i} :\ \sigma_i \geq \sigma_{\min}$.

Then the center shift and its relative square satisfy:

1. *$\|\Delta\| \leq D_S$;*
2. *$\forall z \in S :\ W(z) \leq W^\circ$;*
3. *$\bar{W}_S \leq W^\circ$ (Definition A.27).*

Proof. Proof of item 1.

(L1) $\forall z \in S\ \forall i \leq N :\ |\delta_i| \leq \bar{\delta}$ [the statement]

(L2) $\max_\psi |\widetilde{l}_{10} - l_{10}| \leq E_l$ [the statement]

(L3) $\max_\psi |\widetilde{l}_{10}| \le \widetilde{\ell}$

[the statement]

Corollary G.62 at every $z' \in S$	This proof
Shared: $t, \widetilde{t}_T,\ S, \tau, \bar{\delta},\ \ell, \sigma_{\max},\ \Delta,\ \gamma, \gamma_S, D^\circ$ Shared: $\tau > 1,\ \bar{T} \in \mathbb{R},\ e_{\mathrm{root}} \in \mathcal{R}_n \times \mathcal{R}_n,\ \bar{\delta} \in \mathbb{R}$	
$\mathcal{F}, h$	$\mathcal{F}, h$ (the statement; Definition 4.5)
T	ffLDL$^\dagger(\mathcal{G})$ (Definition 4.6)
z	z' (the statement; the scope)
$Z, \bar{T}, e_{\mathrm{root}}$	$\bar{Z}, \bar{T}, e_{\mathrm{root}}$ (the statement)
$E_l, \widetilde{\ell}$	$E_l, \widetilde{\ell}$ ((L2), (L3); the statement)
t_i	t_i (Definition A.25; Fact G.5, its assumption `INV_SIGMA` $= 1/s$ over $\mathbb{R}$)
(I1) $\mathcal{F}$ realization at (u, ζ)	The signer at (u, ζ) (the statement; Definition 4.5)
$h \ge 1$	Definition 4.5
$T \in \mathcal{T}_n,\ n := 2^h$	ffLDL$^\dagger(\mathcal{G})$ (Definition 4.6); n (Definition 4.5)
$t \in \mathcal{R}_n \times \mathcal{R}_n$	t (the statement)
$z \in \mathbb{Z}^N,\ N := 2n$	z', a sample of ffSampling(t, T) (the statement)
$Z \ge 0$	$\bar{Z} \ge 0$ (the statement)
Assumption A1	The scope
Assumption A2	Assumption A3
Assumption A3	Assumption A2
Assumption A4	Assumption A1
Assumption A5	(L1); δ_i (Definition A.27)
Its conclusion: $(1 - \gamma - \gamma_S)\|\Delta\| \le D^\circ$	

(L4) $(1 - \gamma - \gamma_S)\|\Delta\| \le D^\circ$

[(I1)]

(L5) $\Rightarrow\ \|\Delta\| \le D_S$

[(L4); $\gamma + \gamma_S < 1$ (assumption A4); D_S (precondition 1)]

(L6) $\Rightarrow$ item 1

[(L5)]

□ (item 1)

Proof of item 2.

(L7) $\forall z \in S:\ W(z) = \sum_i \Delta_i^2/\sigma_i^2$

[W (the statement)]

(L8) $\forall z \in S:\ \sum_i \Delta_i^2/\sigma_i^2 \le \|\Delta\|^2/\sigma_{\min}^2$

[$\|\Delta\|^2 = \sum_i \Delta_i^2$ (Fact A.41, its lead); $\sigma_i \ge \sigma_{\min}$ (assumption A6); $\sigma_{\min} > 0$ (assumption A5)]

(L9) $\Rightarrow\ \forall z \in S:\ W(z) \le D_S^2/\sigma_{\min}^2$

[(L5), (L7), (L8)]

(L10) $D_S^2/\sigma_{\min}^2 = W^\circ$

[W° (precondition 2)]

(L11) $\Rightarrow\ \forall z \in S:\ W(z) \le W^\circ$

[(L9), (L10)]

(L12) $\Rightarrow$ item 2

[(L11)]

□ (item 2)

Proof of item 3.

(L13) $\bar{W}_S \le W^\circ$

[(L11); $\bar{W}_S$ (Definition A.27)]

(L14) $\Rightarrow$ item 3

[(L13)]

□ (item 3)

G.7.6 The core class and the terms

Lemma G.78 (Positive probability of the core class [to table])**.** *A floor β on every leaf's unsaturated mass bounds the core class's probability below. Let:*

- $\beta > 0$.

Define:

- $\mathcal{K}(z) := \{\, i \le N : z_i \in C_i(z_{<i}) \,\}$ *(Definition A.26 at τ);*
- $S_0 := \{\, z \in S : |\mathcal{K}(z)| = 0 \,\}$ *(Definition A.26 at τ).*

Assume:

(A1) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i \setminus C_i) \ge \beta$;
(A2) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \sigma_i > 0$;
(A3) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i > 0$;
(A4) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \mathcal{Z}_i \ne \emptyset$.

Then the core class S_0 has positive probability under P and under Q:

1. $P(S_0) \ge \beta^N$;
2. $P(S_0) > 0$;
3. $Q(S_0) > 0$.

Proof.

DEFINES $P_{<i}(z_{<i}) := P(\{\, w \in \mathbb{Z}^N : w_{<i} = z_{<i} \,\})$, $i \le N+1$, $z_{<i} \in \mathbb{Z}^{i-1}$ ($z_{<i}$ of Definition A.25)
DEFINES $T_{<i} := \{\, z_{<i} \in \mathbb{Z}^{i-1} : \forall j < i :\ z_j \in \mathcal{Z}_j(z_{<j}) \setminus C_j(z_{<j}) \,\}$, $i \le N+1$
DEFINES $m_i := \sum_{z_{<i} \in T_{<i}} P_{<i}(z_{<i})$, $i \le N+1$
DEFINES $e(z_{<i}) \in \mathbb{Z}^N$, $i \le N$, $z_{<i} \in \mathbb{Z}^{i-1}$: $e(z_{<i})_j := z_j$ at $j < i$, $e(z_{<i})_j \in \mathcal{Z}_j(e(z_{<i})_{<j})$ at $i \le j \le N$ (assumption A4)

Proof of item 1.

(L1) $S_0 = \{\, z \in \mathbb{Z}^N : \forall i \le N :\ z_i \in \mathcal{Z}_i(z_{<i}) \setminus C_i(z_{<i}) \,\}$
[S, $\mathcal{K}$ and S_k at $k := 0$ (Definition A.26); $\mathcal{Z}_i$ (Definition A.28); $\widetilde{\sigma}_i > 0$ (assumption A3)]

(L2) $T_{<N+1} = S_0$
[(L1); $T_{<i}$ at $i := N+1$ (the proof's block)]

(L3) $\forall i \le N\ \forall z_{<i} \in T_{<i} :\ e(z_{<i}) \in S$
[$e(z_{<i})$ (the proof's block); $\mathcal{Z}_j \setminus C_j \subseteq \mathcal{Z}_j$ at $j < i$ ($T_{<i}$, the proof's block; Fact A.41, item 17, at $(A, B) := (\mathcal{Z}_j, C_j^c)$); S (Definition A.26); $\mathcal{Z}_i$ (Definition A.28) at $i := j$; assumption A3 at every $j \le N$]

(L4) $\Rightarrow\ \forall i \le N :\ T_{<i} \subseteq S_{<i}$
[(L3); $e(z_{<i})_{<i} = z_{<i}$ (the proof's block); $S_{<i}$ (Definition A.26)]

(L5) $\forall i \le N\ \forall z_{<i} \in T_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i \setminus C_i) \ge \beta$
[(L4); assumption A1]

(L6) $\forall i \le N :\ T_{<i+1} = \{\, (z_{<i}, z_i) : z_{<i} \in T_{<i},\ z_i \in \mathcal{Z}_i(z_{<i}) \setminus C_i(z_{<i}) \,\}$
[$T_{<i}$ (the proof's block)]

(L7) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1}\ \forall z_i \in \mathbb{Z} :\ P_{<i+1}(z_{<i+1}) = P_{<i}(z_{<i})\, \widetilde{B}_i(\{z_i\})$
[Fact A.45, item 1, on the first i samples; $\widetilde{B}_i$ (Definition A.28); $P_{<i}$ (the proof's block)]

(L8) $\forall i \le N :\ m_{i+1} = \sum_{z_{<i} \in T_{<i}}\ \sum_{z_i \in \mathcal{Z}_i \setminus C_i} P_{<i+1}(z_{<i+1})$
[(L6); m_{i+1} (the proof's block); Fact A.45, item 11]

(L9) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \sum_{z_i \in \mathcal{Z}_i \setminus C_i} P_{<i+1}(z_{<i+1}) = P_{<i}(z_{<i})\, \widetilde{B}_i(\mathcal{Z}_i \setminus C_i)$
[(L7); Fact A.45, item 9; $\widetilde{B}_i$ a probability measure on $\mathbb{Z}$ (Definition A.28)]

(L10) $\Rightarrow\ \forall i \le N :\ m_{i+1} = \sum_{z_{<i} \in T_{<i}} P_{<i}(z_{<i})\, \widetilde{B}_i(\mathcal{Z}_i \setminus C_i)$
[(L8), (L9)]

(L11) $\forall i \le N:\ \sum_{z_{<i}\in T_{<i}} P_{<i}(z_{<i})\,\widetilde{B}_i(\mathcal{Z}_i \setminus C_i) \ge \beta\, m_i$
[(L5); $P_{<i} \ge 0$ (Fact A.45, item 12); Fact A.45, item 9, at $f := \beta P_{<i}$, $g := P_{<i}\widetilde{B}_i(\mathcal{Z}_i \setminus C_i)$ on $T_{<i}$; m_i (the proof's block)]

(L12) $\Rightarrow\ \forall i \le N:\ m_{i+1} \ge \beta\, m_i$
[(L10), (L11)]

(L13) $T_{<1} = \mathbb{Z}^0$
[$T_{<i}$ at $i := 1$ (the proof's block)]

(L14) $m_1 = P(\mathbb{Z}^N)$
[(L13); m_1, $P_{<1}$ (the proof's block)]

(L15) $P(\mathbb{Z}^N) = 1$
[Fact A.45, item 5, at $A := \mathbb{Z}^N$; Fact A.45, item 12]

(L16) $m_1 \ge \beta^0$
[(L14), (L15)]

(L17) $\forall i \le N:\ m_i \ge \beta^{i-1} \Rightarrow\ m_{i+1} \ge \beta^i$
[(L12); $\beta > 0$ (the statement); Fact A.41, item 26, at $c := \beta$]

(L18) $\forall i \le N+1:\ m_i \ge \beta^{i-1}$
[induction on i: base (L16), step (L17)]

(L19) $m_{N+1} = P(S_0)$
[(L2); m_{N+1}, $P_{<N+1}$ (the proof's block); P (Definition A.25), a probability measure on $\mathbb{Z}^N$]

(L20) $\Rightarrow\ P(S_0) \ge \beta^N$
[(L18) at $i := N+1$; (L19)]

(L21) $\Rightarrow$ item 1
[(L20)]

□ (item 1)

Proof of item 2.

(L22) $\beta^N = e^{N \ln \beta}$
[$\beta > 0$ (the statement); Fact A.41, items 28 and 12]

(L23) $e^{N \ln \beta} > 0$
[Fact A.41, item 12]

(L24) $\Rightarrow\ P(S_0) > 0$
[(L20), (L22), (L23)]

(L25) $\Rightarrow$ item 2
[(L24)]

□ (item 2)

Proof of item 3.

(L26) $\exists z^* \in S_0:\ P(z^*) > 0$
[(L24); P (Definition A.25), a probability measure on $\mathbb{Z}^N$; Fact A.45, item 9, at $f := P$ on S_0, $g := 0$]

(L27) $z^* \in S$
[(L26); $S_k \subseteq S$ at $k := 0$ (Definition A.26)]

(L28) $\forall i \le N:\ z^*_{<i} \in S_{<i}$
[(L27); $S_{<i}$ (Definition A.26)]

(L29) $\forall i \le N:\ \sigma_i(z^*_{<i}) > 0$
[(L28); assumption A2]

(L30) $\forall i \le N:\ \rho_{\sigma_i,t_i}(z^*_i) > 0$
[(L29); Definition A.2, item 1, at $(s,c) := (\sigma_i, t_i)(z^*_{<i})$; Fact A.41, item 12]

(L31) $\forall i \le N:\ \rho_{\sigma_i,t_i}(\mathbb{Z}) \in [0,\infty)$
[(L29); Fact A.45, item 6, at $s := \sigma_i(z^*_{<i})$]

(L32) $\forall i \le N:\ \rho_{\sigma_i,t_i}(\mathbb{Z}) \ge \rho_{\sigma_i,t_i}(z^*_i)$
[(L31); $\rho_{\sigma_i,t_i} \ge 0$ (Fact A.41, item 12); Fact A.45, item 9, at $f := \rho_{\sigma_i,t_i}$ on $\{z^*_i\}$, $g := \rho_{\sigma_i,t_i}$]

(L33) $\forall i \le N :\ D_{\mathbb{Z},\sigma_i,t_i}(z_i^*) > 0$

[Definition A.2, item 2, at $(s,c) := (\sigma_i, t_i)(z^*_{<i})$; (L30), (L32)]

(L34) $Q(z^*) = \prod_{i\le N} D_{\mathbb{Z},\sigma_i,t_i}(z_i^*)$

[Definition A.25, item 2; Fact A.45, item 1]

(L35) $\prod_{i\le N} D_{\mathbb{Z},\sigma_i,t_i}(z_i^*) = e^{\sum_{i\le N} \ln D_{\mathbb{Z},\sigma_i,t_i}(z_i^*)}$

[(L33); Fact A.41, items 28 and 12]

(L36) $\Rightarrow\ Q(z^*) > 0$

[(L34), (L35); Fact A.41, item 12]

(L37) $Q(S_0) \ge Q(z^*)$

[(L26); Fact A.45, item 12, at $\{z^*\} \subseteq S_0$]

(L38) $\Rightarrow\ Q(S_0) > 0$

[(L36), (L37)]

(L39) $\Rightarrow$ item 3

[(L38)]

□ (item 3)

Theorem 4.11 (*Divergence of a Falcon-type signer [to table]*) [to statement].

A Falcon-type signer's $\ln R$ *is at most the sum* A *of its terms, and at* $S' = S$ *its divergence conditioned on the core class* S_0 *is at most* R *times the conditioning factor. Let:*

- *The signer be a Falcon-type signer at* (u, ζ) *(Definition 4.5);*
- $\bar\delta_{S'} \in [0, 1)$*;*
- $W^\circ_{S'} \ge 0$*.*

Define:

- *The signer's parameters*
  - $\sigma_{\max} := 1.17^2\sigma_{\min}$ *(Lemma 4.9, precondition 1);*
- *The prefix sets*
  - $\forall i \le N :\ S_{<i} := \{\, z_{<i} : z \in S \,\}$ *and* $\forall i \le N :\ S'_{<i} := \{\, z_{<i} : z \in S' \,\}$ *(Definition A.26);*
- *The leaf measures*
  - $\widetilde B_i$, $\widetilde D_i$ *and* $\bar\rho_B$*, those of Definition A.28 at the signer's base sampler;*
- *The fringe classes*
  - $\mathcal{K}(z) := \{\, i \le N : z_i \in C_i(z_{<i}) \,\}$ *(Definition A.26);*
  - $\forall k \le N :\ S'_k := \{\, z \in S' : |\mathcal{K}(z)| = k \,\}$ *(Definition A.26);*
  - $R_\alpha^{S'_k}(P \,\|\, Q)$*, that of Definition A.28 at* $\mathcal{Y} := S'_k$*;*
  - $S_0 := \{\, z \in S : |\mathcal{K}(z)| = 0 \,\}$ *(Definition A.26);*
- *The conditional probability measures*
  - $P_{S_0}(A) := P(A \cap S_0)/P(S_0)$ *and* $Q_{S_0}(A) := Q(A \cap S_0)/Q(S_0)$ *(Definition A.26 at* $S := S_0$*).*

Let:

- $M_{2\alpha}, p_\tau \in \mathbb{R}$ *with* $p_\tau \ge 0$ *and* $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde B_i \,\|\, \widetilde D_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}$*;*
- $p'_\tau \in \mathbb{R}$ *with* $\forall i \le N\ \forall z_{<i} :\ \widetilde B_i(\mathcal{Z}_i^c) \le p'_\tau$ *and* $\bar\rho_B \ge (1 - p'_\tau - \bar p_C)^{2\alpha/\alpha_L}$*.*

Define:

Precondition 1. $\mathfrak{L}_B$, $\mathfrak{L}_{\bar\delta}$, $\mathfrak{L}_\Delta$, $\mathfrak{L}_\Phi$ *and* $A := \mathfrak{L}_B + \mathfrak{L}_{\bar\delta} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$*, the four terms of* $\ln R$ *and their sum, written under "where" below at* $\bar\delta_{S'}$*,* $W^\circ_{S'}$ *and* $\bar\phi := \bar\phi_{\mathrm{u}}$*: the terms those of Definition A.30 and Corollary G.75,* $\bar\phi_{\mathrm{u}}$ *that of Definition A.40.*

Assume:

(A1) $\sigma_{\min} > 0$*;*

(A2) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \sigma_i \in [\sigma_{\min}, \sigma_{\max}]$*, with* σ_i *and* $\widetilde\sigma_i$ *those of Definition A.25,* $S_{<i}$ *that of Definition A.26 and* $\sigma_{\max}$ *that of Lemma 4.9, precondition 1;*

(A3) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde\sigma_i \ge \sigma_{\min}$*;*

(A4) $(1+\bar\delta_{S'})^2 < \alpha_L/(\alpha_L-1)$;
(A5) $p'_\tau + \bar p_C < 1$;
(A6) $\varepsilon_0^\circ < 1$, *with* ε_0° *that of Definition A.40 at* $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \bar\delta_{S'}, \bar\Delta)$;
(A7) $\forall z \in S'\ \forall i \le N:\ |\delta_i(z_{<i})| \le \bar\delta_{S'}$;
(A8) $\forall z \in S':\ \sum_{i\le N} \Delta_i(z_{<i})^2/\sigma_i^2 \le W^\circ_{S'}$.
Then the divergence is at most its terms, the fringe classes are bounded, and at $S' = S$ *the conditional divergence on* S_0 *is at most* R *times the conditioning factor:*

1. $\ln R \le A$ *(*R *of Definition A.30 at* S'*);*
2. $\forall k \le N:\ R_\alpha^{S'_k}(P\,\|\,Q)^{\alpha-1} \le \binom{N}{k}\,\kappa_C^k\,R^{\alpha-1}$;
3. *Let* $S' := S$. *Then* $R_\alpha(P_{S_0}\,\|\,Q_{S_0}) \le R\,(1-P(S_0^c))^{-\alpha/(\alpha-1)}$, *with* R *of Definition A.30 at* S.

where

$$\mathfrak{L}_B = N\frac{\alpha_L\,(\alpha\,M_{2\alpha}+2\,p_\tau)}{2(\alpha-1)}, \qquad \mathfrak{L}_{\bar\delta} = \frac{N\ln \bar W_{\alpha_L}}{2(\alpha-1)},$$
$$\mathfrak{L}_\Delta = \frac{\alpha_L\,\bar\theta_{\alpha_L}\,W^\circ_{S'}}{2}, \qquad \mathfrak{L}_\Phi = \frac{N\bar\phi}{2(\alpha-1)}, \qquad \bar\Delta = \sigma_{\max}(W^\circ_{S'})^{1/2},$$

with $\bar W_{\alpha_L}$, $\bar\theta_{\alpha_L}$ *of Definition A.30 at* $\bar\delta_{S'}$ *and* $\bar\phi$ *of Definition A.40 at* $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \bar\delta_{S'}, \bar\Delta)$.

Proof.
DEFINES $\Phi_{\alpha_L,i} := (1+d(s''_i, m_i))(1+d(\widetilde\sigma_i, \widetilde t_i))^{-\alpha_L}(1+d(\sigma_i,t_i))^{\alpha_L-1}$ (Definition A.29)
DEFINES $d(s,c) := \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\,s) - 1$ (Definition A.29)
DEFINES $s''_i := \sigma_i(1+\delta_i)\,\theta_{\alpha_L}(\delta_i)^{1/2}$ and $m_i := t_i + \alpha_L\theta_{\alpha_L}(\delta_i)\,\Delta_i$ (Definition A.29)
DEFINES $\theta_{\alpha_L}(\delta) := 1/(\alpha_L + (1-\alpha_L)(1+\delta)^2)$ (Definition A.30)
DEFINES $\beta := 1 - p'_\tau - \bar p_C$ (p'_τ of the statement, $\bar p_C$ of Definition A.28)
DEFINES $\epsilon_i := \widetilde B_i/\widetilde D_i - 1$ and $\epsilon_{i,+} := \max(\epsilon_i, 0)$ (Corollary G.75)

Proof of items 1 and 2.

(L1) $\bar W_{S'} \le W^\circ_{S'}$
[assumption A8; $\bar W_{S'} = \sup_{z\in S'}\sum_i \Delta_i^2/\sigma_i^2$ (Definition A.27)]

(L2) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ \sigma_i \ge \sigma_{\min}$
[assumption A2]

(L3) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ \sigma_i \le \sigma_{\max}$
[assumption A2]

(L4) $\forall i \le N\ \forall z_{<i} \in S'_{<i}:\ |\delta_i| \le \bar\delta_{S'}$
[assumption A7; $S'_{<i}$ (Definition A.26)]

(L5) $\forall i \le N\ \forall z_{<i} \in S'_{<i}:\ |\Delta_i| \le \sigma_i(\bar W_{S'})^{1/2}$
[$\Delta_i^2/\sigma_i^2 \le \bar W_{S'}$ on S' (Definition A.27)]

(L6) $\forall i \le N:\ S'_{<i} \subseteq S_{<i}$
[$S' \subseteq S$ (Definition A.26); $S'_{<i}$, $S_{<i}$ (Definition A.26)]

(L7) $\forall i \le N\ \forall z_{<i} \in S'_{<i}:\ \sigma_i(\bar W_{S'})^{1/2} \le \bar\Delta$
[(L1); (L3) on $S'_{<i}$, by (L6); $\bar\Delta$ (the statement)]

	Corollary E.13 at $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \bar\delta_{S'}, \bar\Delta)$, at every $i \le N$ and $z_{<i} \in S'_{<i}$	This proof
	α	α_L (the statement)
	$s_{\mathrm{lo}}, s_{\mathrm{hi}}$	$\sigma_{\min}, \sigma_{\max}$ (the statement)
	$\bar\delta, \bar\Delta$	$\bar\delta_{S'}, \bar\Delta$ (the statement)
	s, δ, c', Δ	$\sigma_i, \delta_i, t_i, \Delta_i$ (Definitions A.25 and A.27)
	$\Phi(s, \delta, c', \Delta)$	$\Phi_{\alpha_L, i}$ (the proof's block; Definition A.29)
	$\bar\phi_{\mathrm{u}}$	$\bar\phi$ (precondition 1)
	$\alpha > 1$	$\alpha_L > 1$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement)
	$s_{\mathrm{lo}} > 0$	Assumption A1
(I1)	$s_{\mathrm{lo}} \le s_{\mathrm{hi}}$	$\sigma_{\max} = 1.17^2 \sigma_{\min}$ (Lemma 4.9, precondition 1); assumption A1
	$\bar\delta \in [0, 1)$	$\bar\delta_{S'} \in [0, 1)$ (the statement)
	$\bar\Delta \ge 0$	$0 \le \bar\Delta$ ($\bar\Delta = \sigma_{\max}(W^\circ_{S'})^{1/2}$, the statement)
	$s \in [s_{\mathrm{lo}}, s_{\mathrm{hi}}]$	(L2), (L3) on $S'_{<i}$, by (L6)
	$\lvert\delta\rvert \le \bar\delta$	(L4)
	$c' \in \mathbb{R}$	t_i (Definition A.25)
	$\lvert\Delta\rvert \le \bar\Delta$	(L5), (L7)
	Assumption A1	Assumption A4
	Assumption A2	Assumption A6
	Its conclusion: $\forall s \in [s_{\mathrm{lo}}, s_{\mathrm{hi}}]\ \forall \delta \in [-\bar\delta, \bar\delta]\ \forall c' \in \mathbb{R}\ \forall \Delta \in [-\bar\Delta, \bar\Delta] :\ \lvert\ln \Phi(s, \delta, c', \Delta)\rvert \le \bar\phi_{\mathrm{u}}$	
(L8)	$\Rightarrow\ \forall i \le N\ \forall z_{<i} \in S'_{<i} :\ \lvert\ln \Phi_{\alpha_L, i}\rvert \le \bar\phi$	
		[(I1)]
(L9)	$\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde\sigma_i > 0$	
		[assumption A3; $\sigma_{\min} > 0$ (assumption A1)]
	Corollary G.75, (L3) to (L11) at order 2α, at $M_{2\alpha}$, p_τ and p'_τ	This proof
	Shared: α, $\bar p_C$, $\widetilde B_i, \widetilde D_i$, $\bar\rho_B$ (Definition A.28)	
	Shared: $n \in \{512, 1024\}$, $N := 2n$, $\tau > 1$, $\alpha_L := 2\alpha - 1$, $\alpha > 1$	
	$M_{2\alpha}, p_\tau, p'_\tau$	$M_{2\alpha}, p_\tau, p'_\tau$ (the statement)
	$M_{2\alpha}, p_\tau, p'_\tau \in \mathbb{R}$	The statement
(I2)	$\forall i \le N\ \forall z_{<i} \in S_{<i} :$ $R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde B_i \,\|\, \widetilde D_i)^{\alpha_L} \le$ $1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}$	The statement
	Assumption A2	The statement
	Assumption A4	The statement
	Assumption A5	Assumption A5
	Its conclusion: $\ln \bar\rho_B \le \alpha\, M_{2\alpha} + 2\, p_\tau$	
(L10)	$\ln \bar\rho_B \le \alpha\, M_{2\alpha} + 2\, p_\tau$	
		[(I2)]
(L11)	$(1 + \bar\delta_{S'})^2 < \frac{\alpha_L}{\alpha_L - 1}$	
		[assumption A4]
(L12)	$\bar\phi \ge \max_{i \le N}\ \sup_{z_{<i} \in S'_{<i}} \lvert\ln \Phi_{\alpha_L, i}(z_{<i})\rvert$	
		[(L8); $\bar\phi$ admissible in Definition A.29]

	Corollary E.13 at $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \bar{\delta}_{S'}, \bar{\Delta})$	This proof
	α	α_L (the statement)
	$s_{\text{lo}}, s_{\text{hi}}$	$\sigma_{\min}, \sigma_{\max}$ (the statement)
	$\bar{\delta}, \bar{\Delta}$	$\bar{\delta}_{S'}, \bar{\Delta}$ (the statement)
	s, δ, c', Δ	$\sigma_{\min}, 0, 0, 0$
	$\Phi(s, \delta, c', \Delta)$	$\Phi(\sigma_{\min}, 0, 0, 0)$ (Definition A.39)
	$\bar{\phi}_{\text{u}}$	$\bar{\phi}$ (precondition 1)
	$\alpha > 1$	$\alpha_L > 1$ ($\alpha_L = 2\alpha - 1$, $\alpha > 1$, the statement)
	$s_{\text{lo}} > 0$	Assumption A1
	$s_{\text{lo}} \le s_{\text{hi}}$	$\sigma_{\max} = 1.17^2 \sigma_{\min}$ (Lemma 4.9, precondition 1);
(I3)		assumption A1
	$\bar{\delta} \in [0, 1)$	$\bar{\delta}_{S'} \in [0, 1)$ (the statement)
	$\bar{\Delta} \ge 0$	$0 \le \bar{\Delta}$ ($\bar{\Delta} = \sigma_{\max}(W^{\circ}_{S'})^{1/2}$, the statement)
	$s \in [s_{\text{lo}}, s_{\text{hi}}]$	$\sigma_{\max} = 1.17^2 \sigma_{\min}$ (Lemma 4.9, precondition 1);
		assumption A1
	$\lvert\delta\rvert \le \bar{\delta}$	$\bar{\delta}_{S'} \ge 0$ (the statement)
	$c' \in \mathbb{R}$	$c' := 0$ (the rows above)
	$\lvert\Delta\rvert \le \bar{\Delta}$	$0 \le \bar{\Delta}$ ($\bar{\Delta} = \sigma_{\max}(W^{\circ}_{S'})^{1/2}$, the statement)
	Assumption A1	Assumption A4
	Assumption A2	Assumption A6
	Its conclusion: $\forall s \in [s_{\text{lo}}, s_{\text{hi}}]\ \forall \delta \in [-\bar{\delta}, \bar{\delta}]\ \forall c' \in \mathbb{R}\ \forall \Delta \in [-\bar{\Delta}, \bar{\Delta}] :\ \lvert\ln \Phi(s, \delta, c', \Delta)\rvert \le \bar{\phi}_{\text{u}}$	

(L13) $\lvert\ln \Phi(\sigma_{\min}, 0, 0, 0)\rvert \le \bar{\phi}$ at $\alpha := \alpha_L$

[(I3)]

(L14) $\forall i \le N\ \forall z_{<i} :\ P(z_i \in \cdot \mid z_{<i}) = \widetilde{B}_i$

[P of Definition A.25 at the signer's ffSampling$^{\mathcal{F}}$, its item 1; $\widetilde{B}_i$ (Definition A.28)]

(L15) $\forall i \le N\ \forall z_{<i} :\ Q(z_i \in \cdot \mid z_{<i}) = D_{\mathbb{Z}, \sigma_i, t_i}$

[Q of Definition A.25 at the signer's ffSampling$^{\mathbb{R}}$, its item 2]

(L16) $\forall i \le N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$

[the statement]

(L17) $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$

[the statement]

(L18) $\bar{\rho}_B > 0$

[(L17); $p'_\tau + \bar{p}_C < 1$ (assumption A5); $y^a > 0$ at $y > 0$ (Fact A.41, items 12 and 28)]

	Theorem 4.4 at α, τ, S', $\bar{\delta} := \bar{\delta}_{S'}$ and $\bar{\phi}$	This proof
	Shared: $\alpha, \tau, N,\ S', S'_k,\ C_i, \kappa_C, \bar{p}_C,\ \bar{\rho}_B$ (Definition A.28), $\bar{W}_{\alpha_L}, \bar{\theta}_{\alpha_L}$	
	Shared: $n \in \{512, 1024\},\ N := 2n,\ \alpha > 1,\ \tau > 1,\ S' \subseteq S,\ \alpha_L := 2\alpha - 1$	
	$\bar{\delta}$	$\bar{\delta}_{S'}$ (L4)
	$\bar{\phi}$	$\bar{\phi}$ (L12), (L13)
(I4)	R	R (Definition A.30 at $\bar{\rho}_B$, $\bar{\phi}$, $\bar{\delta}_{S'}$ and $\bar{W}_{S'}$; (L1))
	P, Q	P, Q (L14), (L15)
	Assumption A1	(L11)
	Assumption A2	(L9)
	Assumption A3	(L18)
	Its item 2: $\forall k \le N :\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k R^{\alpha-1}$	

(L19) $\Rightarrow\ \forall k \le N :\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k R^{\alpha-1}$

[item 2 of (I4)]

(L20) $\Rightarrow$ item 2

[(L19)]

(L21) $\bar{W}_{\alpha_L} > 0$

[$\bar{W}_{\alpha_L}$ a maximum of values each positive (Definition A.30)]

(L22) $\ln R = \frac{N}{\alpha-1}\left(\frac{\alpha_L}{2}\ln\bar{\rho}_B + \frac{\bar{\phi}+\ln\bar{W}_{\alpha_L}}{2}\right) + \frac{\alpha_L\bar{\theta}_{\alpha_L}\bar{W}_{S'}}{2}$

[R (Definition A.30 at S'); (L18), (L21); ln of a product and of a power]

(L23) $\Rightarrow\ \ln R \le \mathfrak{L}_B + \mathfrak{L}_{\bar{\delta}} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$

[(L10), (L22); $\bar{W}_{S'} \le W^\circ_{S'}$ ((L1)); $\bar{\theta}_{\alpha_L} \ge 0$ (Definition A.30); $\mathfrak{L}_B$, $\mathfrak{L}_{\bar{\delta}}$, $\mathfrak{L}_\Delta$, $\mathfrak{L}_\Phi$ (the statement, precondition 1)]

(L24) $\mathfrak{L}_B + \mathfrak{L}_{\bar{\delta}} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi = A$

[precondition 1]

(L25) $\Rightarrow\ \ln R \le A$

[(L23), (L24)]

(L26) $\Rightarrow$ item 1

[(L25)]

□ (items 1 and 2)

Proof of item 3.

Corollary G.75, (L6) at p'_τ	This proof
Shared: $\alpha,\ \bar{p}_C,\ \epsilon_i, \epsilon_{i,+}$ Shared: $n \in \{512, 1024\},\ N := 2n,\ \tau > 1,\ \alpha_L := 2\alpha - 1,\ \alpha > 1$	
(I5) p'_τ $p'_\tau \in \mathbb{R}$	p'_τ (the statement) The statement
Assumption A4	(L16)
Its conclusion: $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i \setminus C_i) \ge 1 - p'_\tau - \bar{p}_C$	

(L27) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i \setminus C_i) \ge \beta$

[(I5); β (the proof's block)]

(L28) $\bar{p}_C \ge 0$

[$\bar{p}_C = \max_{i\le N} \sup_{z_{<i}\in S_{<i}} \widetilde{B}_i(C_i)$ and $\sup\emptyset := 0$ (Definition A.28); $\widetilde{B}_i(C_i) \ge 0$ (Fact A.45, item 12); Fact A.41, item 20]

(L29) $\beta > 0$

[β (the proof's block); $p'_\tau + \bar{p}_C < 1$ (assumption A5)]

(L30) $p'_\tau < 1$

[$p'_\tau + \bar{p}_C < 1$ (assumption A5); (L28)]

(L31) $\forall i \le N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i) = 1 - \widetilde{B}_i(\mathcal{Z}_i^c)$

[Fact A.45, item 5, at $P := \widetilde{B}_i$, $A := \mathcal{Z}_i$]

(L32) $\forall i \le N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i) > 0$

[(L16), (L30), (L31)]

(L33) $\forall i \le N\ \forall z_{<i} :\ \mathcal{Z}_i \ne \emptyset$

[(L32); $\widetilde{B}_i(\emptyset) = 0$ (Fact A.45, item 12)]

(L34) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \sigma_i > 0$

[(L2); $\sigma_{\min} > 0$ (assumption A1)]

	Lemma G.78 at τ and β	This proof
	Shared: $\tau,\ \beta,\ S_0$	
	Shared: $n \in \{512, 1024\},\ N := 2n,\ \tau > 1$	
	P, Q	P, Q (L14), (L15)
	$\beta > 0$	(L29)
(I6)	Assumption A1	(L27)
	Assumption A2	(L34)
	Assumption A3	(L9)
	Assumption A4	(L33)
	Its item 2: $P(S_0) > 0$	
	Its item 3: $Q(S_0) > 0$	

(L35) $P(S_0) > 0$

[item 2 of (I6)]

(L36) $Q(S_0) > 0$

[item 3 of (I6)]

(L37) $S'_0 = S_0$

[$S' := S$ (item 3); S'_k and S_k at $k := 0$ (Definition A.26)]

	Theorem 4.4, item 1 at α, τ, $S' := S$, $\bar{\delta} := \bar{\delta}_{S'}$ and $\bar{\phi}$	This proof
	Shared: $\alpha, \tau, N,\ C_i,\ \bar{\rho}_B$ (Definition A.28), $\bar{W}_{\alpha_L}, \bar{\theta}_{\alpha_L}$	
	Shared: $n \in \{512, 1024\},\ N := 2n,\ \alpha > 1,\ \tau > 1,\ \alpha_L := 2\alpha - 1$	
	S'	S (item 3)
	$S'_0, P_{S'_0}, Q_{S'_0}$	S_0, P_{S_0}, Q_{S_0} (L37); the statement
	$\bar{\delta}$	$\bar{\delta}_{S'}$ (L4)
	$\bar{\phi}$	$\bar{\phi}$ (L12), (L13)
(I7)	R	R (Definition A.30 at $\bar{\rho}_B$, $\bar{\phi}$, $\bar{\delta}_{S'}$ and $\bar{W}_{S'}$; (L1))
	P, Q	P, Q (L14), (L15)
	$S' \subseteq S$	$S' := S$ (the rows above)
	Assumption A1	(L11)
	Assumption A2	(L9)
	Assumption A3	(L18)
	Assumption A4	(L35), (L37)
	Assumption A5	(L36), (L37)
	Its conclusion: $R_\alpha(P_{S'_0} \,\|\, Q_{S'_0}) \le R\,(1 - P((S'_0)^c))^{-\alpha/(\alpha-1)}$	

(L38) $\Rightarrow\ R_\alpha(P_{S_0} \,\|\, Q_{S_0}) \le R\,(1 - P(S_0^c))^{-\alpha/(\alpha-1)}$

[(I7)]

(L39) $\Rightarrow$ item 3

[(L38)]

□ (item 3)

Lemma G.79 (Nonnegativity of the sum A [to table])**.** *The sum A of the four terms of* $\ln R$ *of Theorem 4.11 is nonnegative. Define:*

- $\theta_{\alpha_L}(\delta) := 1/(\alpha_L + (1 - \alpha_L)(1 + \delta)^2)$ *(Definition A.30).*

Let:

- $M_{2\alpha}, p_\tau \in \mathbb{R}$ *with* $p_\tau \ge 0$*;*
- $\bar{\delta}_{S'} \in [0, 1)$*;*
- $W^\circ_{S'} \ge 0$*;*
- $\bar{\theta}_{\alpha_L} \ge 0$ *with* $\forall \delta > -1,\ |\delta| \le \bar{\delta}_{S'} :\ \theta_{\alpha_L}(\delta) \le \bar{\theta}_{\alpha_L}$ *(Definition A.30 at* $\bar{\delta}_{S'}$*);*
- $\bar{W}_{\alpha_L} > 0$ *with* $\forall \delta > -1,\ |\delta| \le \bar{\delta}_{S'} :\ \theta_{\alpha_L}(\delta)^{1/2}(1 + \delta)^{1-\alpha_L} \le \bar{W}_{\alpha_L}$ *(Definition A.30 at* $\bar{\delta}_{S'}$*).*

Define:

- $\sigma_{\max} := 1.17^2\sigma_{\min}$ *(Theorem 4.11);*
- $\bar{\Delta} := \sigma_{\max}(W^\circ_{S'})^{1/2}$ *(Theorem 4.11);*
- ε°_0 *and* $\bar{\phi}_{\mathrm{u}}$*, those of Definition A.40 at* $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \bar{\delta}_{S'}, \bar{\Delta})$*;*
- $\mathfrak{L}_B$*,* $\mathfrak{L}_{\bar{\delta}}$*,* $\mathfrak{L}_\Delta$*,* $\mathfrak{L}_\Phi$ *and* A*, those of Theorem 4.11, precondition 1, at* $M_{2\alpha}$*,* p_τ*,* $\bar{\delta}_{S'}$*,* $W^\circ_{S'}$*,* $\bar{\theta}_{\alpha_L}$ *and* $\bar{W}_{\alpha_L}$*.*

Assume:

(A1) $\sigma_{\min} > 0$*;*

(A2) $M_{2\alpha} \geq 0$*;*

(A3) $(1+\bar{\delta}_{S'})^2 < \alpha_L/(\alpha_L - 1)$*;*

(A4) $\varepsilon^\circ_0 < 1$*.*

Then

$$A \geq 0.$$

Proof. (L1) $\alpha_L > 1$

[$\alpha_L = 2\alpha - 1$ and $\alpha > 1$ (the statement)]

(L2) $N\alpha_L/(2(\alpha-1)) > 0$

[$N = 2n$ and $n \in \{512, 1024\}$ (the statement); (L1); $\alpha > 1$ (the statement)]

(L3) $\alpha M_{2\alpha} + 2p_\tau \geq 0$

[assumption A2; $p_\tau \geq 0$ (the statement); $\alpha > 1$ (the statement); Fact A.41, item 26, at $a := 0$]

(L4) $\mathfrak{L}_B = N\alpha_L(\alpha M_{2\alpha} + 2p_\tau)/(2(\alpha-1))$

[$\mathfrak{L}_B$ of Theorem 4.11, precondition 1, at $M_{2\alpha}$ and p_τ; $\mathfrak{L}_B$ (the statement)]

(L5) $\Rightarrow$ $\mathfrak{L}_B \geq 0$

[(L2), (L3), (L4); Fact A.41, item 26, at $a := 0$ and $c := N\alpha_L/(2(\alpha-1))$]

(L6) $\theta_{\alpha_L}(0) = 1$

[θ_{α_L} (the statement) at $\delta := 0$; expand]

(L7) $\theta_{\alpha_L}(0)^{1/2}(1+0)^{1-\alpha_L} = 1$

[(L6); $1^a = 1$ (Fact A.41, item 43) at $a := 1/2$ and at $a := 1 - \alpha_L$]

(L8) $\bar{W}_{\alpha_L} \geq 1$

[(L7); the bound of $\bar{W}_{\alpha_L}$ (the statement) at $\delta := 0$; $\bar{\delta}_{S'} \geq 0$ (the statement)]

(L9) $\ln \bar{W}_{\alpha_L} \geq 0$

[(L8); $\forall y \geq 1 :\ \ln y \geq 0$ (Fact A.41, item 28)]

(L10) $\mathfrak{L}_{\bar{\delta}} = N \ln \bar{W}_{\alpha_L}/(2(\alpha-1))$

[$\mathfrak{L}_{\bar{\delta}}$ of Theorem 4.11, precondition 1, at $\bar{W}_{\alpha_L}$; $\mathfrak{L}_{\bar{\delta}}$ (the statement)]

(L11) $\Rightarrow$ $\mathfrak{L}_{\bar{\delta}} \geq 0$

[(L9), (L10); $N = 2n$ and $\alpha > 1$ (the statement); Fact A.41, item 26, at $a := 0$ and $c := N/(2(\alpha-1))$]

(L12) $\bar{\theta}_{\alpha_L} W^\circ_{S'} \geq 0$

[$\bar{\theta}_{\alpha_L} \geq 0$ (the statement); $W^\circ_{S'} \geq 0$ (the statement); Fact A.41, item 8, at $(a, a', b, b') := (0, \bar{\theta}_{\alpha_L}, 0, W^\circ_{S'})$]

(L13) $\mathfrak{L}_\Delta = \alpha_L \bar{\theta}_{\alpha_L} W^\circ_{S'}/2$

[$\mathfrak{L}_\Delta$ of Theorem 4.11, precondition 1, at $\bar{\theta}_{\alpha_L}$ and $W^\circ_{S'}$; $\mathfrak{L}_\Delta$ (the statement)]

(L14) $\Rightarrow$ $\mathfrak{L}_\Delta \geq 0$

[(L1), (L12), (L13); Fact A.41, item 26, at $a := 0$ and $c := \alpha_L/2$]

(L15) $\sigma_{\max} \geq \sigma_{\min}$

[$\sigma_{\max} = 1.17^2\sigma_{\min}$ (the statement); assumption A1; Fact A.41, item 26, at $(a, b) := (1, 1.17^2)$ and $c := \sigma_{\min}$]

(L16) $\bar{\Delta} \geq 0$

[$\bar{\Delta} = \sigma_{\max}(W^\circ_{S'})^{1/2}$ (the statement); (L15); assumption A1; $(W^\circ_{S'})^{1/2} \geq 0$ (Fact A.41, item 40); Fact A.41, item 8, at $(a, a', b, b') := (0, \sigma_{\max}, 0, (W^\circ_{S'})^{1/2})$]

	Corollary E.13 at $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \bar{\delta}_{S'}, \bar{\Delta})$ and $(s, \delta, c', \Delta) := (\sigma_{\min}, 0, 0, 0)$	This proof
	Shared: $\varepsilon_0^\circ, \bar{\phi}_{\mathrm{u}}$	
	α	α_L (the statement)
	$s_{\mathrm{lo}}, s_{\mathrm{hi}}$	$\sigma_{\min}, \sigma_{\max}$ (the statement)
	$\bar{\delta}, \bar{\Delta}$	$\bar{\delta}_{S'}, \bar{\Delta}$ (the statement)
	s, δ, c', Δ	$\sigma_{\min}, 0, 0, 0$
	$\Phi(s, \delta, c', \Delta)$	$\Phi(\sigma_{\min}, 0, 0, 0)$ (Definition A.39)
	$\alpha > 1$	(L1)
(I1)	$s_{\mathrm{lo}} > 0$	Assumption A1
	$s_{\mathrm{lo}} \le s_{\mathrm{hi}}$	(L15)
	$\bar{\delta} \in [0, 1)$	$\bar{\delta}_{S'} \in [0, 1)$ (the statement)
	$\bar{\Delta} \ge 0$	(L16)
	$s \in [s_{\mathrm{lo}}, s_{\mathrm{hi}}]$	(L15)
	$\lvert\delta\rvert \le \bar{\delta}$	$\bar{\delta}_{S'} \ge 0$ (the statement)
	$c' \in \mathbb{R}$	$c' := 0$ (the rows above)
	$\lvert\Delta\rvert \le \bar{\Delta}$	(L16)
	Assumption A1	Assumption A3
	Assumption A2	Assumption A4
	Its conclusion: $\forall s \in [s_{\mathrm{lo}}, s_{\mathrm{hi}}]\ \forall \delta \in [-\bar{\delta}, \bar{\delta}]\ \forall c' \in \mathbb{R}\ \forall \Delta \in [-\bar{\Delta}, \bar{\Delta}] :\ \lvert\ln \Phi(s, \delta, c', \Delta)\rvert \le \bar{\phi}_{\mathrm{u}}$	

(L17) $\lvert\ln \Phi(\sigma_{\min}, 0, 0, 0)\rvert \le \bar{\phi}_{\mathrm{u}}$ at $\alpha := \alpha_L$

[(I1)]

(L18) $\bar{\phi}_{\mathrm{u}} \ge 0$

[(L17); $\lvert x\rvert \ge 0$ (Fact A.41, item 1)]

(L19) $\mathfrak{L}_\Phi = N\bar{\phi}_{\mathrm{u}}/(2(\alpha - 1))$

[$\mathfrak{L}_\Phi$ of Theorem 4.11, precondition 1, at $\bar{\phi} := \bar{\phi}_{\mathrm{u}}$; $\mathfrak{L}_\Phi$ (the statement)]

(L20) $\Rightarrow\ \mathfrak{L}_\Phi \ge 0$

[(L18), (L19); $N = 2n$ and $\alpha > 1$ (the statement); Fact A.41, item 26, at $a := 0$ and $c := N/(2(\alpha - 1))$]

(L21) $A = \mathfrak{L}_B + \mathfrak{L}_{\bar{\delta}} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$

[precondition 1]

(L22) $\Rightarrow\ A \ge 0$

[(L5), (L11), (L14), (L20), (L21)]

(L23) $\Rightarrow$ the statement

[(L22)]

□

Corollary 4.10 (*Base sampler of a Falcon-type signer [to table]*) [to statement].

At leaf standard deviations within $\bar{\delta}$, the base sampler's row bounds bound its divergence, its factor κ_C, the tail of the tail-cut event and the masses of the fringe leaves. Let:

- *$\mathcal{F} \subset \mathcal{A}$ be the realization of a Falcon-type signer at (u, ζ), the signer (Definition 4.5);*
- *$e_{+,k} \ge 0$, $k \le 18$, and $e_{\mathrm{ccs}} \in [0, 1)$, the row bounds of the signer's base sampler;*
- *$\epsilon \in [0, 1)$;*
- *$\bar{\delta} \ge 0$ with $\forall z \in S\ \forall i \le N :\ \lvert\delta_i\rvert \le \bar{\delta}$, δ_i of Definition A.27.*

Define:

- *The signer's parameters*
  - *$\sigma_0 := 1.8205$ (Lemma G.64);*
  - *$\sigma_{\max} := 1.17^2\sigma_{\min}$;*
- *The prefix sets*
  - *$\forall i \le N :\ S_{<i} := \{\, z_{<i} : z \in S \,\}$ (Definition A.26);*
- *The leaf measures*

– $\widetilde{B}_i$, $\widetilde{D}_i$ *and* $\bar{\rho}_B$, *those of Definition A.28 at the signer's base sampler;*
– $\epsilon_{\mathrm{hi}} \geq 0$ *with* $\forall i \leq N\ \forall z_{<i}\ \forall z_i \notin C_i :\ \widetilde{B}_i(z_i) \leq (1+\epsilon_{\mathrm{hi}})\,\widetilde{D}_i(z_i)$ *(Definition A.28).*

Define:

Precondition 1. $M_{2\alpha} := (\sqrt{\bar{M}_{\mathrm{tab}}} + \sqrt{\bar{M}_{\mathrm{ar}}})^2$, *with* $\bar{M}_{\mathrm{tab}}$ *and* $\bar{M}_{\mathrm{ar}}$ *of Lemma G.73 at order* 2α, $\sigma_{\min}$, $\sigma_{\max}(1+\bar{\delta})$, τ, *the row bounds* $e_{+,k}$ *and* e_{ccs}, *and* ϖ, $\bar{e}_{\mathrm{norm}}$ *that lemma's at these;*

Precondition 2. $p_\tau := \frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}\,\epsilon_{\mathcal{Z}} + p_C^D$, *with* $\epsilon_{\mathcal{Z}} \in [0,1]$ *bounding* $\epsilon_{\mathcal{Z}_i \setminus C_i}$ *at every* $i \leq N$ *and* $z_{<i} \in S_{<i}$ *(Corollary G.75),* $\widetilde{D}_i(\mathcal{Z}_i^c)$ *bounded by Lemma E.18, item 2, at* $(\widetilde{\sigma}_i, \widetilde{t}_i)$ *under assumptions A2, A4 and A7, and* $p_C^D \geq 0$ *bounding* $\widetilde{D}_i(C_i)$ *at every* $i \leq N$ *and* $z_{<i} \in S_{<i}$, $p_C^D = 0$ *when every* C_i *is empty;*

Precondition 3. $p'_\tau := (1+\epsilon_{\mathrm{hi}})\,\frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$ *(Corollary E.21), at which* κ_C *is read (Corollary G.75, item 3:* $\kappa_C \leq \bar{U}^\alpha (1 - p'_\tau - \bar{p}_C)^{-\alpha}$*).*

Assume:

(A1) $e_{+,k}$ *and* e_{ccs} *bound the base sampler's relative perturbation of the acceptance on the row* k *at every leaf, and the relative rounding of its computed* $\widetilde{ccs}$*, as Lemma G.73 assumes, on* $\mathcal{Y} := \mathcal{Z}_i \setminus C_i$ *(Definitions A.26, A.28);*
(A2) $\sigma_{\min} > 0$*;*
(A3) $\forall i \leq N\ \forall z_{<i} \in S_{<i} :\ \sigma_i \in [\sigma_{\min}, \sigma_{\max}]$, *with* σ_i *that of Definition A.25;*
(A4) $\forall i \leq N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i \geq \sigma_{\min}$*;*
(A5) $\sigma_{\max}(1+\bar{\delta}) \leq \sigma_0$*;*
(A6) $\bar{\delta} < 1$*;*
(A7) $\forall i \leq N\ \forall z_{<i}\ \forall c \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$*;*
(A8) $\varpi < 1$, *with* ϖ *that of precondition 1;*
(A9) $\bar{e}_{\mathrm{norm}} < 1$, *with* $\bar{e}_{\mathrm{norm}}$ *that of precondition 1;*
(A10) $p'_\tau + \bar{p}_C < 1$.

Then the leaves' divergence and the factor κ_C *are bounded, the computed leaves' mass off* $\mathcal{Z}_i$ *is at most* p'_τ*, the tail and the fringe masses are bounded, each leaf's divergence on* $\mathcal{Z}_i \setminus C_i$ *is bounded, and* p_τ *is nonnegative:*

1. $\ln \bar{\rho}_B \leq \alpha\, M_{2\alpha} + 2\, p_\tau$*;*
2. $\bar{\rho}_B \geq (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$*;*
3. $\kappa_C \leq \bar{U}^\alpha\, (1 - p'_\tau - \bar{p}_C)^{-\alpha}$*;*
4. $\forall i \leq N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \leq p'_\tau$*;*
5. $P(S^c) \leq N\, p'_\tau$*;*
6. $\forall S' \subseteq S\ \forall I \subseteq \{1, \ldots, N\} :\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \leq \bar{p}_C^{|I|}$*;*
7. $\forall i \leq N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \leq 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}$*;*
8. $p_\tau \geq 0$.

Proof.

DEFINES $\epsilon_i := \widetilde{B}_i / \widetilde{D}_i - 1$ and $\epsilon_{i,+} := \max(\epsilon_i, 0)$ (Corollary G.75)

Proof of items 1 to 8.

(L1) $\forall i \leq N\ \forall z_{<i} \in S_{<i} :\ |\delta_i| \leq \bar{\delta}$

[the statement, at the $z \in S$ of each prefix; $S_{<i}$ (Definition A.26)]

(L2) $\bar{\delta} \in [0, 1)$

[$\bar{\delta} \geq 0$ (the statement); assumption A6]

(L3) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \sigma_i \le \sigma_{\max}$
[assumption A3]

(L4) $\forall i \le N :\ (\mathcal{Z}_i \setminus C_i)^c = \mathcal{Z}_i^c \cup C_i$
[Fact A.41, item 17, at $(A, B) := (\mathcal{Z}_i, C_i)$]

(L5) $\forall i \le N\ \forall z_{<i} :\ \widetilde{D}_i((\mathcal{Z}_i \setminus C_i)^c) \le \widetilde{D}_i(\mathcal{Z}_i^c) + \widetilde{D}_i(C_i)$
[(L4); Fact A.45, item 5]

(L6) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \epsilon_{\mathcal{Z}_i \setminus C_i} \le \epsilon_{\mathcal{Z}}$
[$\epsilon_{\mathcal{Z}}$ (precondition 2)]

(L7) $\epsilon_{\mathcal{Z}} \le 1$
[$\epsilon_{\mathcal{Z}} \in [0, 1]$ (precondition 2)]

(L8) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \widetilde{\sigma}_i \in [\sigma_{\min}, \sigma_{\max}(1 + \bar{\delta})]$
[assumption A4; (L1), (L3); δ_i (Definition A.27)]

(L9) $\sigma_{\max}(1 + \bar{\delta}) \le \sigma_0$
[assumption A5]

(L10) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ \mathcal{Z}_i \setminus C_i \subseteq \mathcal{Z}_i$
[Fact A.41, item 17, at $(A, B) := (\mathcal{Z}_i, C_i)$]

(L11) $\forall i \le N\ \forall z_{<i} \in S_{<i} :$ assumptions A3, A6 and A7 of Lemma G.73 at $(\widetilde{\sigma}_i, \widetilde{t}_i)$, $\mathcal{Y} := \mathcal{Z}_i \setminus C_i$
[assumption A1]

(L12) $\varpi < 1$
[assumption A8]

(L13) $\bar{e}_{\text{norm}} < 1$
[assumption A9]

(L14) $\forall i \le N\ \forall z_{<i} \in \mathbb{Z}^{i-1} :\ \widetilde{\sigma}_i > 0$
[assumption A4; $\sigma_{\min} > 0$ (assumption A2)]

Lemma G.73, item 3 at order 2α, at every $i \le N$ and $z_{<i} \in S_{<i}$	This proof
Shared: $\sigma_{\min},\ e_{+,k}, e_{\text{ccs}}$ Shared: $\tau > 1,\ e_{+,k} \ge 0,\ e_{\text{ccs}} \in [0, 1)$	
α	2α (the statement)
$\sigma_{\max}$	$\sigma_{\max}(1 + \bar{\delta})$ (the statement)
$\widetilde{\sigma}, \widetilde{t}$	$\widetilde{\sigma}_i, \widetilde{t}_i$ (Definition A.25)
$\mathcal{Y}$	$\mathcal{Z}_i \setminus C_i$ (Definitions A.26 and A.28)
$\widetilde{D}$	$\widetilde{D}_i$ (Definition A.28)
ϵ, ϵ_+	$\epsilon_i, \epsilon_{i,+}$ (the proof's block)
$\bar{M}_{\text{tab}}, \bar{M}_{\text{ar}}$	$\bar{M}_{\text{tab}}, \bar{M}_{\text{ar}}$ (precondition 1)
$\varpi, \bar{e}_{\text{norm}}$	$\varpi, \bar{e}_{\text{norm}}$ (precondition 1)
$\alpha \ge 2$	$2\alpha \ge 2$ ($\alpha > 1$, the statement)
(I1) $\sigma_{\min} > 0$	Assumption A2
$\sigma_{\max} \in [\sigma_{\min}, \sigma_0]$	$\sigma_{\max}(1 + \bar{\delta}) \ge \sigma_{\min}$ ((L2); assumption A3); (L9)
$\widetilde{\sigma} > 0$	(L14)
$\widetilde{t} \in \mathbb{R}$	$\widetilde{t}_i$ (Definition A.25)
$\mathcal{Y} \subseteq \mathbb{Z}$	$\mathcal{Z}_i$ (Definition A.28)
$\epsilon_{\text{ar}} = 0$ off $\text{Supp}(P_0)$	ϵ_{ar} (Lemma G.73)
Assumption A1	(L10)
Assumption A2	(L8)
Assumption A3	(L11)
Assumption A4	(L12)
Assumption A5	(L13)
Assumption A6	(L11)
Assumption A7	(L11)
Its conclusion: $\sum_{y \in \mathcal{Y}} \widetilde{D}(1 + \epsilon_+)^{\alpha-2}\epsilon^2 \le \left(\sqrt{\bar{M}_{\text{tab}}} + \sqrt{\bar{M}_{\text{ar}}}\right)^2$	

(L15) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ \sum_{z_i \in \mathcal{Z}_i \setminus C_i} \widetilde{D}_i(1+\epsilon_{i,+})^{2\alpha-2}\epsilon_i^2 \le \left(\sqrt{\bar{M}_{\text{tab}}} + \sqrt{\bar{M}_{\text{ar}}}\right)^2$

[(I1)]

(L16) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ \sum_{z_i \in \mathcal{Z}_i \setminus C_i} \widetilde{D}_i(1+\epsilon_{i,+})^{2\alpha-2}\epsilon_i^2 \le M_{2\alpha}$

[(L15); $M_{2\alpha}$ (precondition 1)]

Lemma E.18, item 2 at every $i \le N$ and $z_{<i}$	This proof
Shared: $\tau > 1,\ \epsilon \in [0,1)$	
s, t	$\widetilde{\sigma}_i, \widetilde{t}_i$ (Definition A.25)
z	$z_i \leftarrow \widetilde{D}_i$ (Definition A.28)
τ, ϵ	τ, ϵ (the statement)
(I2) $\rho_{s,c}(\mathbb{Z})$	$\rho_{\widetilde{\sigma}_i,c}(\mathbb{Z})$ (assumption A7)
$s > 0$	(L14)
$t \in \mathbb{R}$	$\widetilde{t}_i$ (Definition A.25)
$z \leftarrow D_{\mathbb{Z},s,t}$	$\widetilde{D}_i = D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$ (Definition A.28)
Assumption A1	Assumption A7
Its conclusion: $\Pr[\lvert z - t\rvert > \tau s] \le \frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$	

(L17) $\forall i \le N\ \forall z_{<i}:\ \widetilde{D}_i(\mathcal{Z}_i^c) \le \frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$

[(I2); $\mathcal{Z}_i$ (Definition A.28)]

(L18) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ \widetilde{D}_i(C_i) \le p_C^D$

[precondition 2]

(L19) $p_\tau \ge 0$

[p_τ (precondition 2): a sum of products of $(1+\epsilon)/(1-\epsilon) > 0$, $\tau > 1$, $e^{(1-\tau^2)/2} > 0$, $\epsilon_{\mathcal{Z}} \ge 0$ and $p_C^D \ge 0$; $\epsilon \in [0,1)$ (the statement)]

(L20) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ \widetilde{D}_i((\mathcal{Z}_i \setminus C_i)^c)\,\epsilon_{\mathcal{Z}_i \setminus C_i} \le p_\tau$

[(L5), (L6), (L7), (L17), (L18); p_τ (precondition 2)]

(L21) $\forall i \le N\ \forall z_{<i}:\ P(z_i \in \cdot \mid z_{<i}) = \widetilde{B}_i$

[P of Definition A.25 at the signer's ffSampling$^{\mathcal{F}}$, its item 1; $\widetilde{B}_i$ (Definition A.28)]

(L22) $\forall i \le N\ \forall z_{<i}:\ C_i \subseteq \mathcal{Z}_i$

[(L14); C_i (Definition A.26); $\mathcal{Z}_i$ (Definition A.28)]

(L23) $\forall i \le N\ \forall z_{<i}\ \forall z_i \in \mathcal{Z}_i^c:\ \widetilde{B}_i(z_i) \le (1+\epsilon_{\text{hi}})\,\widetilde{D}_i(z_i)$

[(L22); ϵ_{hi} (Definition A.28) at $z_i \notin C_i$]

(L24) $\forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i^c) \le (1+\epsilon_{\text{hi}})\,\widetilde{D}_i(\mathcal{Z}_i^c)$

[(L23); Fact A.45, item 9, at $f := \widetilde{B}_i$, $g := (1+\epsilon_{\text{hi}})\widetilde{D}_i$ on $\mathcal{Z}_i^c$]

(L25) $\forall i \le N\ \forall z_{<i}:\ (1+\epsilon_{\text{hi}})\,\widetilde{D}_i(\mathcal{Z}_i^c) \le p'_\tau$

[(L17); $\epsilon_{\text{hi}} \ge 0$ (Definition A.28); Fact A.41, item 26, at $c := 1+\epsilon_{\text{hi}}$; p'_τ (precondition 3)]

(L26) $\Rightarrow\ \forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$

[(L24), (L25)]

(L27) $\Rightarrow$ item 4

[(L26)]

	Corollary G.75, item 1 at order 2α	This proof
	Shared: $\alpha,\ \bar{p}_C,\ \epsilon_i, \epsilon_{i,+},\ \bar{\rho}_B$ (Definition A.28)	
	Shared: $n \in \{512, 1024\},\ N := 2n,\ \tau > 1,\ \alpha_L := 2\alpha - 1,\ \alpha > 1$	
	$M_{2\alpha}$	$M_{2\alpha}$ (precondition 1)
	p_τ	p_τ (precondition 2)
(I3)	$M_{2\alpha}, p_\tau \in \mathbb{R}$	Preconditions 1 and 2
	Assumption A1	(L16)
	Assumption A2	(L19)
	Assumption A3	(L20)
	Assumption A4	(L26)
	Assumption A5	Assumption A10
	Its conclusion: $\ln \bar{\rho}_B \leq \alpha\, M_{2\alpha} + 2\, p_\tau$	
(L28)	$\ln \bar{\rho}_B \leq \alpha\, M_{2\alpha} + 2\, p_\tau$	
		[(I3)]
(L29)	$\Rightarrow$ item 1	
		[(L28)]

	Corollary G.75, item 2 at order 2α, at p'_τ and $\bar{p}_C$	This proof
	Shared: $\alpha,\ \bar{p}_C,\ \bar{\rho}_B$ (Definition A.28)	
	Shared: $n \in \{512, 1024\},\ N := 2n,\ \tau > 1,\ \alpha_L := 2\alpha - 1,\ \alpha > 1$	
	$M_{2\alpha}$	$M_{2\alpha}$ (precondition 1)
	p_τ	p_τ (precondition 2)
	p'_τ	p'_τ (precondition 3)
(I4)	$M_{2\alpha}, p_\tau, p'_\tau \in \mathbb{R}$	Preconditions 1, 2 and 3
	Assumption A1	(L16)
	Assumption A2	(L19)
	Assumption A3	(L20)
	Assumption A4	(L26)
	Assumption A5	Assumption A10
	Its item 2: $\bar{\rho}_B \geq (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$	
	Its item 3: $\kappa_C \leq \bar{U}^\alpha\, (1 - p'_\tau - \bar{p}_C)^{-\alpha}$	
(L30)	$\bar{\rho}_B \geq (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$	
		[item 2 of (I4)]
(L31)	$\Rightarrow$ item 2	
		[(L30)]
(L32)	$\kappa_C \leq \bar{U}^\alpha\, (1 - p'_\tau - \bar{p}_C)^{-\alpha}$	
		[item 3 of (I4)]
(L33)	$\Rightarrow$ item 3	
		[(L32)]
(L34)	$\forall i \leq N\ \forall z_{<i}\ \forall c \in \mathbb{R}:\ \rho_{\widetilde{\sigma}_{i,c}}(\mathbb{Z}) \geq (1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i$	
		[assumption A7]
(L35)	$\forall i \leq N\ \forall z_{<i}\ \forall c \in \mathbb{R}:\ \rho_{\widetilde{\sigma}_{i,c}}(\mathbb{Z}) \leq (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i$	
		[assumption A7]

	Corollary E.21 at τ	This proof
	Shared: $\epsilon,\ \tau, N,\ S^c$ (Definition A.26), $C_i, \epsilon_{\text{hi}},\ P$ (L21)	
	Shared: $n \in \{512, 1024\},\ N := 2n,\ \tau > 1,\ \epsilon \in [0, 1)$	
	$\epsilon_{\text{hi}} \geq 0$	ϵ_{hi} (Definition A.28)
(I5)	$\forall i \leq N\ \forall z_{<i}\ \forall z_i \notin C_i :\ \widetilde{B}_i(z_i) \leq (1+\epsilon_{\text{hi}})\,\widetilde{D}_i(z_i)$	ϵ_{hi} (Definition A.28)
	Assumption A1	(L14)
	Assumption A2	(L34), (L35)
	Its conclusion: $P(S^c) \leq N\,(1+\epsilon_{\text{hi}})\,\frac{1+\epsilon}{1-\epsilon}\,\tau\,e^{(1-\tau^2)/2}$	

(L36) $P(S^c) \leq N\,p'_\tau$

[(I5); p'_τ (precondition 3)]

(L37) $\Rightarrow$ item 5

[(L36)]

(L38) $\forall S' \subseteq S\ \forall i \leq N :\ S'_{<i} \subseteq S_{<i}$

[$S'_{<i}$ and $S_{<i}$ at $S' \subseteq S$ (Definition A.26)]

(L39) $\forall S' \subseteq S\ \forall I \subseteq \{1, \ldots, N\} :\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \leq \bar{p}_C^{|I|}$

[$\Pr_P[z_i \in C_i \mid z_{<i}] = \widetilde{B}_i(C_i)$ ((L21)), $\widetilde{B}_i(C_i) \leq \bar{p}_C$ at $z_{<i} \in S_{<i}$ (Definition A.28) and $z \in S' \Rightarrow\ z_{<i} \in S'_{<i}$ ($S'_{<i}$, Definition A.26), (L38); the $|I|$ conditionals along $z_1, \ldots, z_N$ (Fact A.45, item 1)]

(L40) $\Rightarrow$ item 6

[(L39)]

	Corollary G.75, (L1), (L2) at order 2α	This proof
	Shared: $\alpha,\ \bar{p}_C,\ \epsilon_i, \epsilon_{i,+}$	
	Shared: $n \in \{512, 1024\},\ N := 2n,\ \tau > 1,\ \alpha_L := 2\alpha - 1,\ \alpha > 1$	
(I6)	$M_{2\alpha}$ p_τ $M_{2\alpha}, p_\tau \in \mathbb{R}$	$M_{2\alpha}$ (precondition 1) p_τ (precondition 2) Preconditions 1 and 2
	Assumption A1	(L16)
	Assumption A2	(L19)
	Assumption A3	(L20)
	Its conclusion: $\forall i \leq N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \leq 1 + 2\alpha\,p_\tau + \alpha\,\alpha_L M_{2\alpha}$	

(L41) $\forall i \leq N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \leq 1 + 2\alpha\,p_\tau + \alpha\,\alpha_L M_{2\alpha}$

[(I6)]

(L42) $\Rightarrow$ item 7

[(L41)]

(L43) $\Rightarrow$ item 8

[(L19)]

□ (items 1 to 8)

The fixed-point signer's rejection at the saturated exponent removes the fringe terms of the theorem and of the loss.

Lemma G.80 (Rejection of the fringe candidates [to table])**.** *Rejecting every fringe candidate leaves every fringe set empty, so the fringe terms of the loss vanish. Let:*

- *The signer be a Falcon-type signer (Definition 4.5) whose* BerExp *(Algorithm 9) executes line 15, $z_{\text{acc}} \leftarrow 0$ at every $si \geq 64$, in place of the word of line 13 at $s_x = 63$.*

Define:

- $\sigma_0 := 1.8205$*, line 9 of* SamplerZ *(Algorithm 8).*

Assume:

(A1) $\forall i \le N\ \forall z_{<i} :\ \widetilde{\sigma}_i \in [\sigma_{\min}, \sigma_0]$.
Then the fringe sets and the fringe terms are empty:

1. $\forall i \le N :\ C_i = \emptyset$;
2. $\bar{U} = 0$;
3. $\bar{p}_C = 0$;
4. $\kappa_C = 0$.

Proof. Proof of item 1.

(L1) $\forall i \le N\ \forall z_{<i}\ \forall z_i,\ si(z_i - \lfloor \widetilde{t}_i \rfloor) \ge 64 :\ \Pr[\text{accept}] = 0$
[$z_{\text{acc}} = 0$ (line 15) at the candidate $z_i - \lfloor \widetilde{t}_i \rfloor$ of the sample z_i (SamplerZ (Algorithm 8), lines 1 and 18); Fact G.66 at the candidate's computed si and r' (lines 2 and 4); assumption A1 of Fact G.66 at $si \ge 64$]

(I1)

Lemma G.64, item 2 at $(\sigma, t) := (\widetilde{\sigma}_i, \widetilde{t}_i)$	This proof
Shared: $\sigma_{\min},\ \sigma_0, P_0$	
σ, t	$\widetilde{\sigma}_i, \widetilde{t}_i$ (the scope)
Assumption A1 Assumption A2	Assumption A1 Assumption A1
Its conclusion: $P_0(s+z) = \frac{\rho_\sigma(z-r)\, w(\bar{z}_0(z))}{\sum_{z'} \rho_\sigma(z'-r)\, w(\bar{z}_0(z'))}$	

(L2) $\Rightarrow\ \forall i \le N\ \forall z_{<i}\ \forall z_i,\ si(z_i - \lfloor \widetilde{t}_i \rfloor) \ge 64 :\ \widetilde{B}_i(z_i) = 0$
[(L1); (I1); Fact A.45, item 4, at the acceptance 0]

(L3) $\forall i \le N :\ C_i = \{\, z_i \in \mathcal{Z}_i \cap \mathrm{Supp}(\widetilde{B}_i) : si(z_i - \lfloor \widetilde{t}_i \rfloor) \ge 64 \,\}$
[C_i (Definition A.26)]

(L4) $\Rightarrow\ \forall i \le N :\ C_i = \emptyset$
[(L2), (L3)]

(L5) $\Rightarrow$ item 1
[(L4)]

□ (item 1)

Proof of items 2 to 4.

(L6) $\sup \emptyset := 0$ in $\bar{U}$
[$\bar{U}$ (Definition A.28)]

(L7) $\Rightarrow\ \bar{U} = 0$
[(L4), (L6); $\bar{U}$ (Definition A.28)]

(L8) $\Rightarrow$ item 2
[(L7)]

(L9) $\bar{p}_C = 0$
[(L4); $\widetilde{B}_i(\emptyset) = 0$ (Fact A.45, item 12); $\bar{p}_C$ (Definition A.28)]

(L10) $\Rightarrow$ item 3
[(L9)]

(L11) $\kappa_C = \bar{U}^{\alpha} \bar{\rho}_B^{-\alpha_L/2}$
[κ_C (Definition A.28)]

(L12) $\Rightarrow\ \kappa_C = 0$
[(L7), (L11)]

(L13) $\Rightarrow$ item 4
[(L12)]

□ (items 2 to 4)

G.8 The tail of the leaf sum

Lemma 4.13 (*Linear form of the leaf center shift [to table]*) [to statement].
The leaf center shift at either center is the leaf offsets times a matrix the key and the center fix, plus the remainder times $I_N + K$. Let:

- $\mathcal{F} \subset \mathcal{A}$ *be the realization of a Falcon-type signer at* (u, ζ) *(Definition 4.5);*
- (f, g, F, G) *be a key of degree* n *of the signer (Definition 4.6);*
- $t_c \in \{t, t_{\text{frac}}\}$ *be a center,* t *and* t_{frac} *those of Definition 4.5 at the key and* $\mathsf{h}(\mathsf{m})$*;*
- $z \in \mathbb{Z}^{2n}$.

Define:

- $\mathcal{G}$ *and* T*, those of Definition 4.6 at the key;*
- $\widetilde{T}$, $\mathcal{L}$, $\widetilde{\mathcal{L}}$, $\widetilde{\mathcal{L}}^{-1}$, I_N, K, σ_i, $\widetilde{\sigma}_i$, t_{leaf}, $\widetilde{t}_{\text{leaf}}$, $\widetilde{c}$, Δ, e *and* r*, those of Definition 4.12 at* $\mathcal{F}$*, the key,* $\mathsf{h}(\mathsf{m})$, t_c *and* z.

Assume:

(A1) $\sigma_{\min} > 0$.

Then the shift is e *times* K *plus the remainder times* $I_N + K$*,* K *is strictly lower triangular in the sampling order, and the leaf standard deviations do not depend on the sample:*

1. $\Delta = eK + r(I_N + K)$;
2. $\forall i, j \le N,\ j \ge i :\ K_{ji} = 0$;
3. $\forall i \le N\ \forall z' \in \mathbb{Z}^N :\ (\sigma_i, \widetilde{\sigma}_i)(z'_{<i}) = (\sigma_i, \widetilde{\sigma}_i)(z_{<i})$.

Proof.

DEFINES $c = (c_i)_{i \le N}$, the leaf centers of ffSampling(t_c, T) with the sample z (Definition G.9)

DEFINES (g_{00}, g_{01}, g_{11}): the entries of $\mathcal{G}$ over $\mathbb{R}$ at the root node

DEFINES $d_{11} = g_{11} - |g_{01}|^2/g_{00}$, the second diagonal LDL† (Algorithm 5), line 19, computes over $\mathbb{R}$ on $\mathcal{G}$

DEFINES d_{11}^{root}: the root node's second diagonal ffsamp (Algorithm 6) reads over $\mathbb{R}$ at the center t_c

COMPUTES $\widetilde{d}_{(i)}$, $i \le N$: the computed diagonal of the leaf of position i, in the LDL$^\dagger(\widetilde{\mathcal{G}})$ of the calls of ffsamp (Algorithm 6), lines 6, 15 and 29

COMPUTES $\widetilde{\sigma}(d)$, $d \in \mathcal{F}$: the standard deviation deepest (Algorithm 7), lines 1 and 3, or their counterparts at $\widetilde{d}_{00}$, computes from the diagonal d

Proof of item 1.

(L1) `INV_SIGMA` $= 1/s$
[ffSampling$^{\mathbb{R}}$ over $\mathbb{R}$ at s (Definition A.25)]

(L2) $T =$ ffLDL$^\dagger(\mathcal{G})$
[T (the statement; Definition 4.6)]

(L3) $d_{11}^{\text{root}} \in \{d_{11}, q^2/g_{00}\}$
[ffsamp (Algorithm 6), line 4 at `root` $= 0$ and line 7 at `root` $= 1$; d_{11}^{root} (the proof's block)]

(L4) $d_{11} = q^2/g_{00}$
[Fact A.33, item 4]

(L5) $\Rightarrow\ d_{11}^{\text{root}} = d_{11}$
[(L3), (L4)]

	Fact G.5 at z	This proof
	Shared: $\mathcal{G}, s$	
(I1)	t	t_{c} (the statement)
	T	T (L2)
	$\mathcal{G} \in \mathrm{Gram}_n$	$g_{00} > 0$, $g_{00}g_{11} - \lvert g_{01}\rvert^2 = q^2$, $q^2 > 0$ (Fact A.33, items 3 and 2); Definition A.14
	$t \in \mathcal{R}_n \times \mathcal{R}_n$	t_{c} (the statement; Definition 4.5)
	$s > 0$	$s = 1.17\sqrt{q}\,\sigma_{\min}$ (Definition A.25); assumption A1
	Assumption A1	(L1)
	Its conclusion: $\forall z \in \mathbb{Z}^N\ \forall i \le N:\ (\sigma_i', c_i')(z_{<i}) = (\sigma_i, c_i)(z_{<i})$	
(L6)	$t_{\mathrm{leaf}} = c$	
		[(I1), the root's second diagonal by (L5); c (the proof's block)]
	Proposition G.48, item 1 at (T, t_{c}, z)	This proof
	Shared: $T,\ z,\ c$	
(I2)	t	t_{c} (the statement)
	$\mathcal{L}_T$	$\mathcal{L}$ (the statement)
	$T \in \mathcal{T}_n$	(L2)
	$t \in \mathcal{R}_n \times \mathcal{R}_n$	t_{c} (the statement; Definition 4.5)
	z a sample of ffSampling(t, T)	$\rho_{s',c'}(z_i) > 0$ (Fact A.41, item 12)
	Its item 1: $c - z = (t - z)\mathcal{L}_T$	
(L7)	$\Rightarrow\ t_{\mathrm{leaf}} - z = (t_{\mathrm{c}} - z)\mathcal{L}$	
		[(L6); (I2)]
	Proposition G.48, item 1 at $(\widetilde{T}, t_{\mathrm{c}}, z)$	This proof
	Shared: z	
(I3)	T	$\widetilde{T}$ (the statement)
	t	t_{c} (the statement)
	c	$\widetilde{c}$ (the statement)
	$\mathcal{L}_T$	$\widetilde{\mathcal{L}}$ (the statement)
	$t \in \mathcal{R}_n \times \mathcal{R}_n$	t_{c} (the statement; Definition 4.5)
	z a sample of ffSampling(t, T)	$\rho_{s',c'}(z_i) > 0$ (Fact A.41, item 12)
	Its item 1: $c - z = (t - z)\mathcal{L}_T$	
(L8)	$\widetilde{c} - z = (t_{\mathrm{c}} - z)\widetilde{\mathcal{L}}$	
		[(I3)]
(L9)	$\Rightarrow\ t_{\mathrm{c}} - z = (\widetilde{c} - z)\widetilde{\mathcal{L}}^{-1}$	
		[(L8); $\widetilde{\mathcal{L}}^{-1}$ (the statement)]
(L10)	$\Rightarrow\ t_{\mathrm{leaf}} - z = (\widetilde{c} - z)\widetilde{\mathcal{L}}^{-1}\mathcal{L}$	
		[(L7), (L9)]
(L11)	$\widetilde{c} - z = -e - r$	
		[e and r (the statement)]
(L12)	$\Rightarrow\ t_{\mathrm{leaf}} - z = -(e + r)(I_N + K)$	
		[(L10), (L11); $\widetilde{\mathcal{L}}^{-1}\mathcal{L} = I_N + K$ (K, the statement)]
(L13)	$\Delta = (\widetilde{t}_{\mathrm{leaf}} - z) - (t_{\mathrm{leaf}} - z)$	
		[Δ (the statement)]
(L14)	$\widetilde{t}_{\mathrm{leaf}} - z = -e$	
		[e (the statement)]
(L15)	$\Rightarrow\ \Delta = -e + (e + r)(I_N + K)$	
		[(L12), (L13), (L14)]
(L16)	$\Rightarrow\ \Delta = eK + r(I_N + K)$	

[(L15); expand]

(L17) $\Rightarrow$ item 1

[(L16)]

□ (item 1)

Proof of item 2.

Lemma G.11 at T	This proof
Shared: T	
(I4) $\mathcal{L}_T$	$\mathcal{L}$ (the statement)
$T \in \mathcal{T}_n$	(L2)
Its conclusion: $\forall x \in \mathcal{R}_n \times \mathcal{R}_n\ \forall i \le N:\ (x\mathcal{L}_T)_i = x_i + \sum_{j<i} x_j (\mathcal{L}_T)_{ji}$	

(L18) $\forall i, j \le N,\ j \ge i:\ \mathcal{L}_{ji} = [j = i]$

[(I4); the matrix of the tree map (Definition G.6)]

Lemma G.11 at $\widetilde{T}$	This proof
(I5) T	$\widetilde{T}$ (the statement)
$\mathcal{L}_T$	$\widetilde{\mathcal{L}}$ (the statement)
Its conclusion: $\forall x \in \mathcal{R}_n \times \mathcal{R}_n\ \forall i \le N:\ (x\mathcal{L}_T)_i = x_i + \sum_{j<i} x_j (\mathcal{L}_T)_{ji}$	

(L19) $\forall i, j \le N,\ j \ge i:\ \widetilde{\mathcal{L}}_{ji} = [j = i]$

[(I5); Definition G.6]

(L20) $\widetilde{\mathcal{L}} K = \mathcal{L} - \widetilde{\mathcal{L}}$

[K and $\widetilde{\mathcal{L}}^{-1}$ (the statement)]

(L21) $\forall i, j \le N,\ j \ge i:\ (\mathcal{L} - \widetilde{\mathcal{L}})_{ji} = 0$

[(L18), (L19)]

(L22) $\forall i, j \le N:\ (\widetilde{\mathcal{L}} K)_{ji} = K_{ji} + \sum_{j<k\le N} \widetilde{\mathcal{L}}_{jk} K_{ki}$

[(L19); expand]

(L23) $\forall i \le N\ \forall j \in \{i, \dots, N\}:\ (\forall k \in \{j+1, \dots, N\}:\ K_{ki} = 0) \Rightarrow\ K_{ji} = 0$

[(L20), (L21), (L22)]

(L24) $\Rightarrow\ \forall i, j \le N,\ j \ge i:\ K_{ji} = 0$

[induction on j from N down to i: (L23) at $j = N$, no k, the base; (L23) the step]

(L25) $\Rightarrow$ item 2

[(L24)]

□ (item 2)

Proof of item 3.

(L26) $\forall i \le N\ \forall z' \in \mathbb{Z}^N:\ \sigma_i(z'_{<i}) = \sigma_i(z_{<i})$

[Fact G.5 as at (L6); Definition A.21, item 1, at d_i of Definition A.19 at T]

(L27) $\forall i \le N\ \forall z' \in \mathbb{Z}^N:\ \widetilde{\sigma}_i(z'_{<i}) = \widetilde{\sigma}(\widetilde{d}_{(i)})$

[$\widetilde{\sigma}_i$ (Definition A.25); $\widetilde{d}_{(i)}$ and $\widetilde{\sigma}$ (the proof's block)]

(L28) $\forall i \le N\ \forall z' \in \mathbb{Z}^N:\ \widetilde{\sigma}_i(z'_{<i}) = \widetilde{\sigma}_i(z_{<i})$

[(L27) at z' and at z]

(L29) $\Rightarrow\ \forall i \le N\ \forall z' \in \mathbb{Z}^N:\ (\sigma_i, \widetilde{\sigma}_i)(z'_{<i}) = (\sigma_i, \widetilde{\sigma}_i)(z_{<i})$

[(L26), (L28)]

(L30) $\Rightarrow$ item 3

[(L29)]

□ (item 3)

Lemma 4.14 (*The leaf sum's tail [to table]*) [to statement].

At a key whose three quantities lie within D, M and B, the leaf sum of one signature at either

center exceeds W^{tail} on the tail-cut event with probability at most η_1. Let:

- $\mathcal{F} \subset \mathcal{A}$ *be the realization of a Falcon-type signer at* (u, ζ) *(Definition 4.5);*
- (f, g, F, G) *be a key of degree* n *of the signer (Definition 4.6);*
- $t_{\mathrm{c}} \in \{t, t_{\mathrm{frac}}\}$ *be a center,* t *and* t_{frac} *those of Definition 4.5 at the key and* $\mathsf{h}(\mathsf{m})$*;*
- $D \in [0, 1)$*;*
- $M \geq 0$*;*
- $B \geq 0$*;*
- $\eta_1 \in (0, 1)$*;*
- $\epsilon \in [0, 1)$*.*

Define:

- *The leaf perturbations*
  - N*,* σ_i*,* $\widetilde{\sigma}_i$*,* $\widetilde{t}_i$*,* I_N*,* K*,* Δ*,* e*,* r*,* δ_i*,* $\bar{\delta}_K$*,* μ_{key} *and* $\bar{B}_K$*, those of Definition 4.12 at* $\mathcal{F}$*, the key,* $\mathsf{h}(\mathsf{m})$*,* t_{c} *and* $\tau_K := \tau$*;*
  - $W(z) := \sum_{i \leq N} \Delta_i^2 / \sigma_i^2$ *for* $z \in \mathbb{Z}^N$*;*
- *The probability measures*
  - $P(A) := \Pr[z \in A]$*,* z *the output of* $\mathrm{ffSampling}^{\mathcal{F}}$ *(Definition A.25 at the key,* $\mathsf{h}(\mathsf{m})$ *and* t_{c}*);*
  - $\epsilon_{\mathrm{hi}} \geq 0$ *with* $\forall i \leq N\ \forall z_{<i}\ \forall z_i \notin C_i :\ \widetilde{B}_i(z_i) \leq (1 + \epsilon_{\mathrm{hi}})\, \widetilde{D}_i(z_i)$ *(Definition A.28);*
- *The tail-cut event*
  - $S := \{\, z \in \mathbb{Z}^N : \forall i \leq N\ |z_i - \widetilde{t}_i(z_{<i})| \leq \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$ *(Definition A.26);*
- *The terms*
  - $\kappa := (1 + \epsilon)/(1 - \epsilon)$*;*
  - $\eta' := \eta_1 / (2N(1 + \epsilon_{\mathrm{hi}})^N \kappa^N)$*;*
  - $W^{\mathrm{tail}} := (1 + D)^2 \left((2M \ln(1/\eta'))^{1/2} + B^{1/2} \right)^2$*.*

Assume:

(A1) $\bar{\delta}_K \leq D$*;*
(A2) $\mu_{\mathrm{key}} \leq M$*;*
(A3) $\bar{B}_K \leq B$*;*
(A4) $\forall i \leq N\ \forall z_{<i}\ \forall c \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1 - \epsilon)\sqrt{2\pi}\, \widetilde{\sigma}_i, (1 + \epsilon)\sqrt{2\pi}\, \widetilde{\sigma}_i]$*;*
(A5) $\forall i \leq N\ \forall z_{<i} :\ C_i(z_{<i}) = \emptyset$*;*
(A6) $\sigma_{\min} > 0$*;*
(A7) $\forall i \leq N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$*.*

Then

$$P(S \cap \{z \in \mathbb{Z}^N : W(z) > W^{\mathrm{tail}}\}) \leq \eta_1.$$

Proof.

DEFINES

$$\xi := (2 \ln(1/\eta'))^{1/2}$$
$$R_i := \left(\sum_{j<i} K_{ji}^2 \widetilde{\sigma}_j^2 \right)^{1/2} / \widetilde{\sigma}_i \text{ for } i \leq N$$
$$U_i := \{z \in \mathbb{Z}^N : |(eK)_i| > \widetilde{\sigma}_i R_i \xi\} \text{ for } i \leq N$$
$$U := \bigcup_{i \leq N} U_i$$
$$\rho := r(I_N + K)$$
$$\widetilde{B}_i := B^{\mathcal{F}}_{\widetilde{\sigma}_i(z_{<i}), \widetilde{t}_i(z_{<i})} \text{ (Definition A.28)}$$
$$\widetilde{D}_i := D_{\mathbb{Z}, \widetilde{\sigma}_i, \widetilde{t}_i} \text{ (Definition A.28)}$$
$$P_D(z) := \prod_{i \leq N} D_{\mathbb{Z}, \widetilde{\sigma}_i(z_{<i}), \widetilde{t}_i(z_{<i})}(z_i) \text{ for } z \in \mathbb{Z}^N \text{ (Definition A.28)}$$

(L1) $\forall i \leq N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$

[assumption A7]

(L2) $\sigma_{\min} > 0$

[assumption A6]

	Lemma 4.13 at every $z \in \mathbb{Z}^N$	This proof
	Shared: $\mathcal{F},\ (f,g,F,G),\ t_{\mathrm{c}},\ z,\ \Delta, e, r, K, I_N,\ \sigma_i, \widetilde{\sigma}_i$	
(I1)	$\mathcal{F}$ the realization of a Falcon-type signer at (u,ζ)	The statement
	(f,g,F,G) a key of degree n of the signer	The statement
	$t_{\mathrm{c}} \in \{t, t_{\mathrm{frac}}\}$	The statement
	Assumption A1	Assumption A6
	Its item 1: $\Delta = eK + r(I_N + K)$	
	Its item 2: $\forall i,j \le N,\ j \ge i:\ K_{ji} = 0$	
	Its item 3: $\forall i \le N\ \forall z' \in \mathbb{Z}^N:\ (\sigma_i, \widetilde{\sigma}_i)(z'_{<i}) = (\sigma_i, \widetilde{\sigma}_i)(z_{<i})$	

(L3) $\forall z \in \mathbb{Z}^N:\ \Delta = eK + \rho$

[item 1 of (I1); ρ (the proof's block)]

(L4) $\forall z \in \mathbb{Z}^N\ \forall i \le N:\ 1/\sigma_i = (1+\delta_i)/\widetilde{\sigma}_i$

[δ_i (Definition A.27); (L1), (L2)]

(L5) $\forall i \le N\ \forall z_{<i}:\ |\delta_i(z_{<i})| \le D$

[$\bar{\delta}_K$ (Definition 4.12, item 1); assumption A1]

(L6) $\Rightarrow\ \forall z \in \mathbb{Z}^N\ \forall i \le N:\ 1/\sigma_i \le (1+D)/\widetilde{\sigma}_i$

[(L4), (L5); (L1), (L2)]

(L7) $\Rightarrow\ \forall z \in \mathbb{Z}^N:\ W(z) \le (1+D)^2 \sum_{i \le N} \Delta_i^2/\widetilde{\sigma}_i^2$

[(L6); W (the statement); $t \mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L8) $\forall z \in \mathbb{Z}^N:\ \left(\sum_{i \le N} \Delta_i^2/\widetilde{\sigma}_i^2\right)^{1/2} \le \left(\sum_{i \le N} (eK)_i^2/\widetilde{\sigma}_i^2\right)^{1/2} + \left(\sum_{i \le N} \rho_i^2/\widetilde{\sigma}_i^2\right)^{1/2}$

[(L3); $\|X+Y\|_w \le \|X\|_w + \|Y\|_w$ at $w_i := 1/\widetilde{\sigma}_i^2$ (Fact A.41, item 3)]

(L9) $\forall z \in S:\ \sum_{i \le N} \rho_i^2/\widetilde{\sigma}_i^2 \le B$

[$\bar{B}_K$ (Definition 4.12, item 3, at $\tau_K := \tau$); assumption A3; ρ (the proof's block)]

(L10) $\forall z \in S:\ \left(\sum_{i \le N} \rho_i^2/\widetilde{\sigma}_i^2\right)^{1/2} \le B^{1/2}$

[(L9); $t \mapsto \sqrt{t}$ nondecreasing (Fact A.41, item 5)]

(L11) $\forall z \notin U\ \forall i \le N:\ (eK)_i^2/\widetilde{\sigma}_i^2 \le R_i^2 \xi^2$

[U and U_i (the proof's block)]

(L12) $\sum_{i \le N} R_i^2 = \mu_{\mathrm{key}}$

[R_i (the proof's block); μ_{key} (Definition 4.12, item 2)]

(L13) $\Rightarrow\ \forall z \notin U:\ \sum_{i \le N} (eK)_i^2/\widetilde{\sigma}_i^2 \le \mu_{\mathrm{key}} \xi^2$

[(L11), (L12)]

(L14) $\xi \ge 0$

[ξ (the proof's block)]

(L15) $\Rightarrow\ \forall z \notin U:\ \left(\sum_{i \le N} (eK)_i^2/\widetilde{\sigma}_i^2\right)^{1/2} \le M^{1/2}\xi$

[(L13), (L14); assumption A2; $t \mapsto \sqrt{t}$ nondecreasing (Fact A.41, item 5)]

(L16) $\Rightarrow\ \forall z \in S \setminus U:\ \left(\sum_{i \le N} \Delta_i^2/\widetilde{\sigma}_i^2\right)^{1/2} \le M^{1/2}\xi + B^{1/2}$

[(L8), (L10), (L15)]

(L17) $\Rightarrow\ \forall z \in S \setminus U:\ \sum_{i \le N} \Delta_i^2/\widetilde{\sigma}_i^2 \le (M^{1/2}\xi + B^{1/2})^2$

[(L16); $t \mapsto t^2$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L18) $\Rightarrow\ \forall z \in S \setminus U:\ W(z) \le (1+D)^2 (M^{1/2}\xi + B^{1/2})^2$

[(L7), (L17)]

(L19) $(1+D)^2 (M^{1/2}\xi + B^{1/2})^2 = W^{\mathrm{tail}}$

[ξ (the proof's block); W^{tail} (the statement)]

(L20) $\Rightarrow\ S \cap \{z : W(z) > W^{\mathrm{tail}}\} \subseteq U$

[(L18), (L19)]

(L21) $\forall z \in \mathbb{Z}^N :\ P(z) = \prod_{i \le N} \widetilde{B}_i(z_i)$

[Fact A.45, item 1; Definition A.25, item 1; $\widetilde{B}_i$ (the proof's block)]

(L22) $\forall i \le N\ \forall z_{<i}\ \forall z_i \in \mathbb{Z} :\ \widetilde{B}_i(z_i) \le (1+\epsilon_{\text{hi}})\, \widetilde{D}_i(z_i)$

[ϵ_{hi} (Definition A.28) at $C_i(z_{<i}) = \emptyset$ (assumption A5)]

(L23) $\Rightarrow\ \forall z \in \mathbb{Z}^N :\ P(z) \le (1+\epsilon_{\text{hi}})^N P_D(z)$

[(L21), (L22); P_D and $\widetilde{D}_i$ (Definition A.28); Fact A.41, item 8, over the N factors]

(L24) $\Rightarrow\ P(U) \le (1+\epsilon_{\text{hi}})^N P_D(U)$

[(L23); Fact A.45, item 9]

(L25) $\forall j \le N\ \forall z_{<j} :\ \widetilde{\sigma}_j > 0$

[(L1), (L2)]

(L26) $\epsilon \in [0, 1)$

[ϵ (the statement)]

(L27) $\forall j \le N\ \forall z_{<j}\ \forall c' \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_j, c'}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_j, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_j]$

[assumption A4]

(I2)

Lemma B.4, item 2 at every $j \le N$, $z_{<j}$ and $\ell \in \mathbb{R}$	This proof
s, c	$\widetilde{\sigma}_j, \widetilde{t}_j(z_{<j})$ (Definition A.25)
ℓ	ℓ (the scope)
ϵ	ϵ (the statement)
$D_{\mathbb{Z},s,c}$	$\widetilde{D}_j$ (Definition A.28)
$s > 0$	(L25)
$c \in \mathbb{R}$	$\widetilde{t}_j$ (Definition A.25)
$\ell \in \mathbb{R}$	The scope
$\epsilon \in [0, 1)$	(L26)
Assumption A1	(L27)
Its conclusion: $M_{s,c}(\ell) \le \frac{1+\epsilon}{1-\epsilon}\, e^{\ell^2 s^2/2}$	

(L28) $\forall j \le N\ \forall z_{<j}\ \forall \ell \in \mathbb{R} :\ \sum_{z_j \in \mathbb{Z}} \widetilde{D}_j(z_j)\, e^{\ell(z_j - \widetilde{t}_j)} \le \frac{1+\epsilon}{1-\epsilon}\, e^{\ell^2 \widetilde{\sigma}_j^2/2}$

[(I2)]

(L29) $\forall j \le N\ \forall z_{<j}\ \forall \ell \in \mathbb{R} :\ \sum_{z_j \in \mathbb{Z}} \widetilde{D}_j(z_j)\, e^{\ell(z_j - \widetilde{t}_j)} \le \kappa\, e^{\ell^2 \widetilde{\sigma}_j^2/2}$

[(L28); κ (the statement)]

(L30) $\forall z \in \mathbb{Z}^N\ \forall i \le N :\ (eK)_i = \sum_{j \le N} K_{ji} e_j$

[expand]

(L31) $\forall i \le N :\ \sum_{j \le N} K_{ji}^2 \widetilde{\sigma}_j^2 = \widetilde{\sigma}_i^2 R_i^2$

[R_i (the proof's block); item 2 of (I1)]

(L32) $\forall j \le N\ \forall z, z' \in \mathbb{Z}^N :\ \widetilde{\sigma}_j(z'_{<j}) = \widetilde{\sigma}_j(z_{<j})$

[item 3 of (I1)]

(L33) $\forall z \in \mathbb{Z}^N :\ P_D(z) = \prod_{j \le N} \widetilde{D}_j(z_j)$

[P_D (the proof's block); Fact A.45, item 1]

(L34) $\forall i \le N,\ R_i > 0 :\ \widetilde{\sigma}_i^2 R_i^2 > 0$

[(L1), (L2)]

Lemma B.5, item 2 at every $i \le N$ with $R_i > 0$	This proof
Shared: N, κ	
P_j	$\widetilde{D}_j$ (Definition A.28)
$g_j(z_{\le j})$	e_j (the statement)
a_j	K_{ji} (the statement)
s_j	$\widetilde{\sigma}_j$ (L32)
t	$\widetilde{\sigma}_i R_i \xi$ (the proof's block)
P	P_D (L33)
X	$(eK)_i$ (L30)
V	$\widetilde{\sigma}_i^2 R_i^2$ (L31)
(I3) $N \in \mathbb{Z}_{>0}$	N (the statement)
$P_j(\cdot \mid y_{<j}) : \mathbb{Z} \to [0,1]$, $\sum_{x \in \mathbb{Z}} P_j(x \mid y_{<j}) = 1$	$\widetilde{D}_i$ (Definition A.28) at $i := j$
$g_j : \mathbb{Z}^j \to \mathbb{R}$	e_j (the statement)
$a \in \mathbb{R}^N$	K (the statement)
$s \in (0,\infty)^N$	(L25), (L32)
$\kappa \ge 1$	κ (the statement); (L26)
$t \ge 0$	(L14), (L25); R_i (the proof's block)
Assumption A1	(L29)
Assumption A2	(L34)
Its conclusion: $P(\{y \in \mathbb{Z}^N : \lvert X(y)\rvert > t\}) \le 2\kappa^N e^{-t^2/(2V)}$	

(L35) $\forall i \le N,\ R_i > 0 :\ P_D(U_i) \le 2\kappa^N e^{-(\widetilde{\sigma}_i R_i \xi)^2/(2\widetilde{\sigma}_i^2 R_i^2)}$

[(I3); U_i (the proof's block)]

(L36) $\forall i \le N,\ R_i > 0 :\ (\widetilde{\sigma}_i R_i \xi)^2/(2\widetilde{\sigma}_i^2 R_i^2) = \xi^2/2$

[expand]

(L37) $\forall i \le N,\ R_i = 0\ \forall j < i :\ K_{ji} = 0$

[R_i (the proof's block); (L1), (L2)]

(L38) $\Rightarrow\ \forall i \le N,\ R_i = 0\ \forall z \in \mathbb{Z}^N :\ (eK)_i = 0$

[(L30), (L37); item 2 of (I1)]

(L39) $\Rightarrow\ \forall i \le N,\ R_i = 0 :\ U_i = \emptyset$

[(L38); U_i (the proof's block)]

(L40) $\Rightarrow\ \forall i \le N :\ P_D(U_i) \le 2\kappa^N e^{-\xi^2/2}$

[(L35), (L36) at $R_i > 0$; (L39) at $R_i = 0$; Fact A.45, item 12]

(L41) $e^{-\xi^2/2} = \eta'$

[ξ (the proof's block); Fact A.41, item 28, at $y := 1/\eta'$]

(L42) $\Rightarrow\ P_D(U) \le 2N\kappa^N \eta'$

[(L40), (L41); U (the proof's block); Fact A.45, item 5]

(L43) $\Rightarrow\ P(U) \le (1+\epsilon_{\text{hi}})^N 2N\kappa^N \eta'$

[(L24), (L42)]

(L44) $(1+\epsilon_{\text{hi}})^N 2N\kappa^N \eta' = \eta_1$

[η' (the statement)]

(L45) $\Rightarrow\ P(S \cap \{z : W(z) > W^{\text{tail}}\}) \le \eta_1$

[(L20), (L43), (L44); Fact A.45, item 12]

(L46) $\Rightarrow$ the statement

[(L45)]

□

H Proofs of Section 5

This appendix proves the statements of Section 5. The proofs follow the conventions of Appendix D. Section H.1 proves the bit security over Q_s signatures; Section H.2 proves the checked key's bounds.

How each statement is verified. Table 22 lists this appendix's definitions, and Table 23 how each fact, lemma and proposition placed here is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Def. H.1	✓				
Fact H.4	✓				

Table 22: Appendix H: its definitions and facts.

Table 23: Appendix H: how each lemma and proposition is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma H.2	✓				
Lemma H.3	✓				
Lemma H.5	✓				
Lemma H.6	✓				
Prop. H.7	✓				
Lemma H.8	✓				
Lemma H.9	✓				
Lemma H.10	✓				
Lemma H.11	✓				
Lemma H.12	✓				
Lemma H.13	✓				
Lemma H.14	✓				
Lemma H.15	✓				
Lemma H.16	✓		✓		
Lemma H.17	✓				
Lemma H.18	✓				
Lemma H.19	✓				
Lemma H.20	✓				
Lemma H.21	✓				
Lemma H.22	✓				
Lemma H.23	✓				
Lemma H.24	✓				
Lemma H.25	✓		✓		
Lemma H.26	✓				

H.1 The bit security over Q_s signatures

Theorem 5.11 (*Bit cost of the fringe leaves [to table]*) [to statement].

The level $\lambda_{\mathcal{F}}$ with fringe leaves is the level $\lambda_{\mathcal{F}}^{\emptyset}$ at empty fringe sets less $\log_2(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}} \Pi_C(y))$ bits. Each fringe leaf multiplies the probability-preservation bound y in $\Pi_C(y)$ by at most g_C. The union bound of m fringe leaves is at most $\mu_C^m/m!$. Let:

- $\lambda \in \mathbb{R}$;
- $Q_s \in \mathbb{Z}_{>0}$;
- $A \in \mathbb{R}$;
- $M_C \in \mathbb{Z}_{\geq 0}$.

Define:

- *y and $\lambda_{\mathcal{F}}$, those of Definition 5.3 at (λ, Q_s, A, M_C);*
- *$\Pi_C(y)$, that of Definition 5.2 at (Q_s, M_C);*
- *$\lambda_{\mathcal{F}}^{\emptyset}$ by $2^{-\lambda_{\mathcal{F}}^{\emptyset}} := Q_s\, P(S'^c) + y$;*

- $g_C := (Q_s N)^{1/\alpha}\, \bar{U}\, \bar{\rho}_B^{-\alpha_L/(2\alpha)}$;
- $\mu_C := Q_s N\, \bar{p}_C$.

Assume:

(A1) $\bar{\rho}_B > 0$;

(A2) $\bar{U} < \infty$.

Then the fringe leaves' cost in bits is exact, bounded in g_C and μ_C, and zero at empty fringe sets:

1. $\lambda_{\mathcal{F}}^{\emptyset} - \lambda_{\mathcal{F}} = \log_2\!\big(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}}\, \Pi_C(y)\big)$;
2. $\Pi_C(y) \le \sum_{m=1}^{M_C} \min\!\big(g_C^m\, y,\ \mu_C^m/m!\big) + \mu_C^{M_C+1}/(M_C+1)!$;
3. $\lambda_{\mathcal{F}}^{\emptyset} - \lambda_{\mathcal{F}} \le \log_2\!\Big(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}} \Big(\sum_{m=1}^{M_C} \min\!\big(g_C^m\, y,\ \mu_C^m/m!\big) + \mu_C^{M_C+1}/(M_C+1)!\Big)\Big)$;
4. *Assume:*

   (A3) $\bar{p}_C = 0$.

   Then $\lambda_{\mathcal{F}} = \lambda_{\mathcal{F}}^{\emptyset}$.

Proof. Proof of items 1 to 3.

(L1) $\bar{U} \in [0, \infty)$

[$\widetilde{B}_i(z) \ge 0$ ($\widetilde{B}_i$ a probability measure, Definition A.28); $\widetilde{D}_i(z) > 0$ ($\widetilde{D}_i = D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$, Definition A.2, items 2 and 1; Fact A.41, item 12); $\sup\emptyset := 0$ and $\bar{U}$ (Definition A.28); Fact A.41, item 20; $\bar{U} < \infty$ (assumption A2)]

(L2) $\kappa_C \ge 0$

[(L1); $\bar{\rho}_B > 0$ (assumption A1); $t^a \ge 0$ at $t \ge 0$ (Fact A.41, item 40); $\kappa_C = \bar{U}^{\alpha}\, \bar{\rho}_B^{-\alpha_L/2}$ (Definition A.28); Fact A.41, item 8]

(L3) $\bar{p}_C \ge 0$

[$\widetilde{B}_i(C_i) \ge 0$ ($\widetilde{B}_i$ a probability measure, Definition A.28); $\sup\emptyset := 0$ and $\bar{p}_C$ (Definition A.28); Fact A.41, item 20]

(L4) $y > 0$

[$2^{-\lambda} > 0$ and $e^{Q_s A} > 0$ (Fact A.41, item 12); $t^a > 0$ at $t > 0$ (Fact A.41, items 12 and 28); y (Definition 5.3)]

(L5) $Q_s\, P(S'^c) \ge 0$

[P a probability measure (Definition A.25); $Q_s \in \mathbb{Z}_{>0}$ (the statement)]

(L6) $2^{-\lambda_{\mathcal{F}}} = 2^{-\lambda_{\mathcal{F}}^{\emptyset}} + \Pi_C(y)$

[$\lambda_{\mathcal{F}}$ (Definition 5.3); $\lambda_{\mathcal{F}}^{\emptyset}$ (the statement)]

(L7) $2^{-\lambda_{\mathcal{F}}^{\emptyset}} > 0$

[(L4), (L5); $\lambda_{\mathcal{F}}^{\emptyset}$ (the statement)]

(L8) $\forall m \in \mathbb{Z}_{\ge 0}:\ \binom{Q_s N}{m} \in [0, (Q_s N)^m/m!]$

[$Q_s N \in \mathbb{Z}_{\ge 0}$ ($Q_s \in \mathbb{Z}_{>0}$, the statement); Fact A.41, item 37]

(L9) $\forall m \in \{1, \dots, M_C\}:\ \binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha}\, y \ge 0$

[(L2), (L4), (L8); $t^a \ge 0$ at $t \ge 0$ (Fact A.41, item 40); Fact A.41, item 8]

(L10) $\forall m \in \mathbb{Z}_{\ge 0}:\ \binom{Q_s N}{m} \bar{p}_C^m \ge 0$

[(L3), (L8); $t^a \ge 0$ at $t \ge 0$ (Fact A.41, item 40); Fact A.41, item 8]

(L11) $\forall m \in \{1, \dots, M_C\}:\ \min\left(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha}\, y,\ \binom{Q_s N}{m} \bar{p}_C^m\right) \ge 0$

[(L9), (L10); Fact A.41, item 47, at $c := 0$]

(L12) $\Pi_C(y) \ge 0$

[(L10) at $m := M_C + 1$, (L11); $\Pi_C(y)$ (Definition 5.2)]

(L13) $2^{-\lambda_{\mathcal{F}}} = 2^{-\lambda_{\mathcal{F}}^{\emptyset}} \big(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}}\, \Pi_C(y)\big)$

[(L6); $2^{-a}\, 2^a = 1$ ($2^t = e^{t \ln 2}$, $e^x e^y = e^{x+y}$, Fact A.41, item 12); expand]

(L14) $1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}} \Pi_C(y) > 0$

[(L12); $2^{\lambda_{\mathcal{F}}^{\emptyset}} > 0$ (Fact A.41, item 12)]

(L15) $-\lambda_{\mathcal{F}} = -\lambda_{\mathcal{F}}^{\emptyset} + \log_2\bigl(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}} \Pi_C(y)\bigr)$

[(L7), (L13), (L14); $\log_2 2^t = t$ and $\log_2(st) = \log_2 s + \log_2 t$ at $s, t > 0$ ($\log_2 = \ln / \ln 2$; Fact A.41, items 29 and 30)]

(L16) $\Rightarrow$ item 1

[(L15)]

(L17) $\kappa_C^{1/\alpha} = \bar{U}\, \bar{\rho}_B^{-\alpha_L/(2\alpha)}$

[$\kappa_C = \bar{U}^{\alpha}\, \bar{\rho}_B^{-\alpha_L/2}$ (Definition A.28); (L1); assumption A1; $t^a \geq 0$ at $t \geq 0$ (Fact A.41, item 40); $(st)^a = s^a t^a$ at $s, t \geq 0$ (Fact A.41, item 45); $(t^a)^b = t^{ab}$ at $t \geq 0$ (Fact A.41, item 46) at $(a, b) := (\alpha, 1/\alpha)$ and at $(a, b) := (-\alpha_L/2, 1/\alpha)$; $t^1 = t$ at $t \geq 0$ (Fact A.41, item 42); expand]

(L18) $\forall m \in \mathbb{Z}_{\geq 0} :\ \binom{Q_s N}{m} \leq (Q_s N)^m$

[(L8); $K^m/m! \leq K^m$ at $K := Q_s N$ (Fact A.41, item 38)]

(L19) $\forall m \in \mathbb{Z}_{\geq 0} :\ \binom{Q_s N}{m}^{1/\alpha} \leq ((Q_s N)^m)^{1/\alpha}$

[(L8), (L18); $t \mapsto t^{1/\alpha}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5) at $\alpha > 1$ (the statement)]

(L20) $\forall m \in \{1, \ldots, M_C\} :\ \binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha}\, y \leq ((Q_s N)^m)^{1/\alpha} \kappa_C^{m/\alpha}\, y$

[(L19); (L2), (L4); $t^a \geq 0$ at $t \geq 0$ (Fact A.41, item 40); Fact A.41, item 8]

(L21) $\forall m \in \mathbb{Z}_{\geq 0} :\ ((Q_s N)^m)^{1/\alpha} = ((Q_s N)^{1/\alpha})^m$

[$(t^a)^b = t^{ab}$ at $t \geq 0$ (Fact A.41, item 46) at $(a, b) := (m, 1/\alpha)$ and at $(a, b) := (1/\alpha, m)$]

(L22) $\forall m \in \mathbb{Z}_{\geq 0} :\ \kappa_C^{m/\alpha} = (\kappa_C^{1/\alpha})^m$

[(L2); $(t^a)^b = t^{ab}$ at $t \geq 0$ (Fact A.41, item 46) at $(a, b) := (1/\alpha, m)$]

(L23) $\forall m \in \mathbb{Z}_{\geq 0} :\ ((Q_s N)^{1/\alpha})^m (\kappa_C^{1/\alpha})^m = ((Q_s N)^{1/\alpha} \kappa_C^{1/\alpha})^m$

[(L2); $t^a \geq 0$ at $t \geq 0$ (Fact A.41, item 40); $(st)^a = s^a t^a$ at $s, t \geq 0$ (Fact A.41, item 45) at $a := m$]

(L24) $(Q_s N)^{1/\alpha} \kappa_C^{1/\alpha} = g_C$

[(L17); g_C (the statement)]

(L25) $\Rightarrow\ \forall m \in \{1, \ldots, M_C\} :\ \binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha}\, y \leq g_C^m\, y$

[(L20), (L21), (L22), (L23), (L24)]

(L26) $\forall m \in \mathbb{Z}_{\geq 0} :\ \binom{Q_s N}{m} \bar{p}_C^m \leq ((Q_s N)^m/m!)\, \bar{p}_C^m$

[(L3), (L8); $t^a \geq 0$ at $t \geq 0$ (Fact A.41, item 40); Fact A.41, item 8]

(L27) $\forall m \in \mathbb{Z}_{\geq 0} :\ ((Q_s N)^m/m!)\, \bar{p}_C^m = \mu_C^m/m!$

[(L3); $(st)^a = s^a t^a$ at $s, t \geq 0$ (Fact A.41, item 45) at $a := m$; μ_C (the statement)]

(L28) $\Rightarrow\ \forall m \in \mathbb{Z}_{\geq 0} :\ \binom{Q_s N}{m} \bar{p}_C^m \leq \mu_C^m/m!$

[(L26), (L27)]

(L29) $\forall m \in \{1, \ldots, M_C\} :\ \min\left(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha}\, y,\ \binom{Q_s N}{m} \bar{p}_C^m\right) \leq \min\bigl(g_C^m\, y,\ \mu_C^m/m!\bigr)$

[(L25), (L28); Fact A.41, item 25]

(L30) $\binom{Q_s N}{M_C+1} \bar{p}_C^{M_C+1} \leq \mu_C^{M_C+1}/(M_C+1)!$

[(L28) at $m := M_C + 1$]

(L31) $\Pi_C(y) \leq \sum_{m=1}^{M_C} \min\bigl(g_C^m\, y,\ \mu_C^m/m!\bigr) + \mu_C^{M_C+1}/(M_C+1)!$

[(L29), (L30); $\Pi_C(y)$ (Definition 5.2)]

(L32) $\Rightarrow$ item 2

[(L31)]

(L33) $1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}} \Pi_C(y) \leq 1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}} \Bigl(\sum_{m=1}^{M_C} \min\bigl(g_C^m\, y,\ \mu_C^m/m!\bigr) + \mu_C^{M_C+1}/(M_C+1)!\Bigr)$

[(L31); $2^{\lambda_{\mathcal{F}}^{\emptyset}} > 0$ (Fact A.41, item 12); Fact A.41, item 26]

(L34) $\log_2\bigl(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}} \Pi_C(y)\bigr) \leq \log_2\Bigl(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}} \Bigl(\sum_{m=1}^{M_C} \min\bigl(g_C^m\, y,\ \mu_C^m/m!\bigr) + \mu_C^{M_C+1}/(M_C+1)!\Bigr)\Bigr)$

[(L14), (L33); $\log_2$ increasing on $(0, \infty)$ ($\log_2 = \ln / \ln 2$; $e^{\ln t} = t$ at $t > 0$, Fact A.41, item 28; exp increasing on $\mathbb{R}$, Fact A.41, item 5)]

(L35) $\Rightarrow\ \lambda_{\mathcal{F}}^{\emptyset} - \lambda_{\mathcal{F}} \leq \log_2\Bigl(1 + 2^{\lambda_{\mathcal{F}}^{\emptyset}} \Bigl(\sum_{m=1}^{M_C} \min\bigl(g_C^m\, y,\ \mu_C^m/m!\bigr) + \mu_C^{M_C+1}/(M_C+1)!\Bigr)\Bigr)$

[(L15), (L34)]

(L36) $\Rightarrow$ item 3

[(L35)]

□ (items 1 to 3)

Proof of item 4.

(L37) $\forall m \in \{1, \dots, M_C\}:\ \binom{Q_sN}{m}\bar{p}_C^m = 0$

[$\bar{p}_C = 0$ (assumption A3); $0^a = 0$ at $a > 0$ (Fact A.41, item 44) at $a := m$]

(L38) $\forall m \in \{1, \dots, M_C\}:\ \min\left(\binom{Q_sN}{m}^{1/\alpha}\kappa_C^{m/\alpha}\, y,\ \binom{Q_sN}{m}\bar{p}_C^m\right) \le 0$

[(L37); $\min(a, b) \le b$ (Fact A.41, item 20)]

(L39) $\Rightarrow\ \forall m \in \{1, \dots, M_C\}:\ \min\left(\binom{Q_sN}{m}^{1/\alpha}\kappa_C^{m/\alpha}\, y,\ \binom{Q_sN}{m}\bar{p}_C^m\right) = 0$

[(L11), (L38)]

(L40) $\binom{Q_sN}{M_C+1}\bar{p}_C^{M_C+1} = 0$

[$\bar{p}_C = 0$ (assumption A3); $0^a = 0$ at $a > 0$ (Fact A.41, item 44) at $a := M_C + 1$]

(L41) $\Pi_C(y) = 0$

[(L39), (L40); $\Pi_C(y)$ (Definition 5.2)]

(L42) $2^{-\lambda_{\mathcal{F}}} = 2^{-\lambda_{\mathcal{F}}^{\emptyset}}$

[(L6), (L41)]

(L43) $\lambda_{\mathcal{F}} = \lambda_{\mathcal{F}}^{\emptyset}$

[(L42); $t \mapsto 2^{-t}$ injective ($2^{-t} = e^{-t \ln 2}$, exp increasing on $\mathbb{R}$, Fact A.41, items 12 and 5)]

(L44) $\Rightarrow$ item 4

[(L43)]

□ (item 4)

Lemma 5.4 (*Fringe bounds over Q_s signatures [to table]*) [to statement].

The bounds of one signature on its fringe classes and on its fringe leaves' masses hold, compounded, on the tuples of Q_s independent signatures. Let:

- $Q_s \in \mathbb{Z}_{>0}$;
- $R > 0$;
- $S' \subseteq S$ *be a sub-event (Definition A.26);*
- κ_C *and* $\bar{p}_C$ *be the fringe quantities (Definition A.28).*

Define:

- $\mathcal{K}(z)$ *and* S'_k, *those of Definition A.26;*
- $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$, *the probability measures of* Q_s *independent signatures on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1);*
- $\mathcal{E} := \{\, w \in (\mathbb{Z}^N)^{Q_s} : \forall j \le Q_s\ w_j \in S' \,\}$;
- $\forall m \le Q_sN:\ E_m := \{\, w \in \mathcal{E} : \sum_{j \le Q_s} |\mathcal{K}(w_j)| = m \,\}$;
- $R_\alpha^{S'_k}(P \,\|\, Q)$ *and* $R_\alpha^{E_m}(P^{\otimes Q_s} \,\|\, Q^{\otimes Q_s})$, *those of Definition A.28 at* $\mathcal{Y} := S'_k$ *and at* $\mathcal{Y} := E_m$.

Assume:

(A1) $\forall k \le N:\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k}\kappa_C^k R^{\alpha-1}$;

(A2) $\forall I \subseteq \{1, \dots, N\}:\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$.

Then

1. $\forall m \le Q_sN:\ R_\alpha^{E_m}(P^{\otimes Q_s} \,\|\, Q^{\otimes Q_s})^{\alpha-1} \le \binom{Q_sN}{m}\kappa_C^m R^{(\alpha-1)Q_s}$;
2. $\forall I \subseteq \{1, \dots, Q_s\} \times \{1, \dots, N\}:\ P^{\otimes Q_s}(\{w \in \mathcal{E} : \forall (j,i) \in I\ (w_j)_i \in C_i\}) \le \bar{p}_C^{|I|}$;
3. $\forall m \le Q_sN:\ P^{\otimes Q_s}(E_m) \le \binom{Q_sN}{m}\bar{p}_C^m$.

Proof.

DEFINES $E_{(k_j)} := \{w \in \mathcal{E} : \forall j \le Q_s\ w_j \in S'_{k_j}\}$, $(k_1, \dots, k_{Q_s}) \in \{0, \dots, N\}^{Q_s}$ ($\mathcal{E}$, S'_k of the statement)

DEFINES $I_j := \{i \le N : (j,i) \in I\}$, $I \subseteq \{1, \dots, Q_s\} \times \{1, \dots, N\}$, $j \le Q_s$

(L1) $\forall (k_1, \dots, k_{Q_s}),\ k_j \le N :$

$$\sum_{w \in E_{(k_j)}} P^{\otimes Q_s}(w)^\alpha Q^{\otimes Q_s}(w)^{1-\alpha} = \prod_{j \le Q_s} \sum_{z \in S'_{k_j}} P^\alpha Q^{1-\alpha}$$

[$P^{\otimes Q_s}(w) = \prod_j P(w_j)$, $Q^{\otimes Q_s}(w) = \prod_j Q(w_j)$ (Fact A.45, item 1); the indicator of $E_{(k_j)}$ the product of the indicators of S'_{k_j} at $j \le Q_s$ (the proof's block)]

(L2) $\Rightarrow\ \forall (k_1, \dots, k_{Q_s}),\ k_j \le N :\ \sum_{w \in E_{(k_j)}} P^{\otimes Q_s}(w)^\alpha Q^{\otimes Q_s}(w)^{1-\alpha} \le \prod_{j \le Q_s} \binom{N}{k_j} \kappa_C^{k_j}\ R^{(\alpha-1)Q_s}$

[(L1); assumption A1 at $k := k_j$; $R_\alpha^{S'_k}(P \,\|\, Q)$ (Definition A.28)]

(L3) $\forall m \le Q_s N :\ \sum_{k_1 + \cdots + k_{Q_s} = m} \prod_{j \le Q_s} \binom{N}{k_j} = \binom{Q_s N}{m}$

[the coefficient of x^m on both sides of $((1+x)^N)^{Q_s} = (1+x)^{Q_s N}$; expand]

(L4) $\forall m \le Q_s N :\ \sum_{w \in E_m} P^{\otimes Q_s}(w)^\alpha Q^{\otimes Q_s}(w)^{1-\alpha} \le \binom{Q_s N}{m} \kappa_C^m R^{(\alpha-1)Q_s}$

[E_m the union of the classes $E_{(k_j)}$ with $\sum_j k_j = m$, pairwise disjoint (the statement; the proof's block); (L2) at each; (L3)]

(L5) $\Rightarrow$ item 1

[(L4); $R_\alpha^{E_m}(P^{\otimes Q_s} \,\|\, Q^{\otimes Q_s})$ (Definition A.28)]

(L6) $\forall I \subseteq \{1, \dots, Q_s\} \times \{1, \dots, N\} :\ P^{\otimes Q_s}(\{w \in \mathcal{E} : \forall (j,i) \in I\ (w_j)_i \in C_i\}) = \prod_{j \le Q_s} P(\{z \in S' : \forall i \in I_j\ z_i \in C_i\})$

[$\mathcal{E}$ (the statement); I_j (the proof's block); Fact A.45, item 1, over the Q_s independent signatures]

(L7) $\Rightarrow\ \forall I \subseteq \{1, \dots, Q_s\} \times \{1, \dots, N\} :\ P^{\otimes Q_s}(\{w \in \mathcal{E} : \forall (j,i) \in I\ (w_j)_i \in C_i\}) \le \prod_{j \le Q_s} \bar{p}_C^{|I_j|}$

[(L6); assumption A2 at $I := I_j$, $j \le Q_s$; Fact A.41, item 8]

(L8) $\forall I \subseteq \{1, \dots, Q_s\} \times \{1, \dots, N\} :\ \prod_{j \le Q_s} \bar{p}_C^{|I_j|} = \bar{p}_C^{|I|}$

[I_j (the proof's block); add the exponents]

(L9) $\Rightarrow$ item 2

[(L7), (L8)]

(L10) $\forall m \le Q_s N :\ E_m \subseteq \bigcup_{I \subseteq \{1,\dots,Q_s\} \times \{1,\dots,N\},\ |I| = m} \{w \in \mathcal{E} : \forall (j,i) \in I\ (w_j)_i \in C_i\}$

[E_m, $\mathcal{E}$ (the statement); $\mathcal{K}$ (Definition A.26), at the set $I := \{(j,i) : i \in \mathcal{K}(w_j)\}$ of the m fringe leaves of w]

(L11) $\forall m \le Q_s N :\ P^{\otimes Q_s}(E_m) \le \binom{Q_s N}{m} \bar{p}_C^m$

[(L9), (L10) over the $\binom{Q_s N}{m}$ sets I of m of the $Q_s N$ leaves; Fact A.45, item 5]

(L12) $\Rightarrow$ item 3

[(L11)]

□ (items 1, 2 and 3)

Theorem 1.2 (*Bit security over Q_s signatures [to table]*) [to statement].

Over Q_s independent signatures, the Rényi divergences on the fringe classes S'_k of a sub-event S' of the tail-cut event, to the power $\alpha - 1$, and the masses of its fringe leaves bound the computed signer's probability of the adversary's event by $2^{-\lambda_{\mathcal{F}}}$. Let:

- $\lambda \in \mathbb{R}$;
- $Q_s \in \mathbb{Z}_{>0}$;
- $A \ge 0$;
- $M_C \in \mathbb{Z}_{\ge 0}$;
- $R > 0$.

Define:

- $y := (2^{-\lambda} e^{Q_s A})^{(\alpha-1)/\alpha}$ *(Definition 5.3)*;
- S'_k, *that of Definition A.26*;
- $R_\alpha^{S'_k}(P \,\|\, Q)$, *that of Definition A.28 at* $\mathcal{Y} := S'_k$;

- $\lambda_{\mathcal{F}}$, *that of Definition 5.3 at* (λ, Q_s, A, M_C);
- $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$, *the probability measures of* Q_s *independent signatures on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1).*

Let:

- $A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s}$, *an adversary's event (Definition 5.1) at* (λ, Q_s).

Assume:

(A1) $\ln R \le A$;

(A2) $\forall k \le N:\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k R^{\alpha-1}$;

(A3) $\forall I \subseteq \{1, \dots, N\}:\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$.

Then

$$P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}.$$

Proof.

DEFINES $\mathcal{E}$ and E_m, those of Lemma 5.4 at Q_s, R, S', κ_C and $\bar{p}_C$ (the statement)

(L1) $\mathcal{E}^c \subseteq \bigcup_{j \le Q_s} \{w : w_j \notin S'\}$

[$\mathcal{E}$ (the proof's block)]

(L2) $P^{\otimes Q_s}(\mathcal{E}^c) \le Q_s\, P(S'^c)$

[(L1); Fact A.45, item 5, over the Q_s coordinates]

(I1)

Lemma 5.4	This proof
Shared: Q_s, R, S', κ_C, $\bar{p}_C$, $P^{\otimes Q_s}$, $Q^{\otimes Q_s}$	
Assumption A1 Assumption A2	Assumption A2 Assumption A3
Its item 1: $\forall m \le Q_s N:\ R_\alpha^{E_m}(P^{\otimes Q_s} \,\|\, Q^{\otimes Q_s})^{\alpha-1} \le \binom{Q_s N}{m} \kappa_C^m R^{(\alpha-1)Q_s}$	
Its item 2: $\forall I \subseteq \{1, \dots, Q_s\} \times \{1, \dots, N\}:\ P^{\otimes Q_s}(\{w \in \mathcal{E} : \forall (j,i) \in I\ (w_j)_i \in C_i\}) \le \bar{p}_C^{|I|}$	
Its item 3: $\forall m \le Q_s N:\ P^{\otimes Q_s}(E_m) \le \binom{Q_s N}{m} \bar{p}_C^m$	

(L3) $\forall m \le Q_s N:\ R_\alpha^{E_m}(P^{\otimes Q_s} \,\|\, Q^{\otimes Q_s})^{\alpha-1} \le \binom{Q_s N}{m} \kappa_C^m R^{(\alpha-1)Q_s}$

[item 1 of (I1)]

(L4) $\forall m:\ Q^{\otimes Q_s}(A_{\text{adv}} \cap E_m) \le Q^{\otimes Q_s}(A_{\text{adv}})$

[Fact A.45, item 12, at $A_{\text{adv}} \cap E_m \subseteq A_{\text{adv}}$ (Fact A.41, item 17)]

(L5) $Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda}$

[A_{adv} (Definition 5.1)]

(L6) $R^{Q_s} \le e^{Q_s A}$

[$\ln R \le A$ (assumption A1); $R > 0$, $Q_s \in \mathbb{Z}_{>0}$ (the statement)]

(L7) $\forall m \le M_C:\ P^{\otimes Q_s}(A_{\text{adv}} \cap E_m) \le \binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} (R^{Q_s}\, Q^{\otimes Q_s}(A_{\text{adv}}))^{(\alpha-1)/\alpha}$

[Fact A.45, item 7 at $\mu := P^{\otimes Q_s}$, $\nu := Q^{\otimes Q_s}$, $B := A_{\text{adv}} \cap E_m$; (L3); $R_\alpha^{E_m}(P^{\otimes Q_s} \,\|\, Q^{\otimes Q_s})$ (Definition A.28)]

(L8) $\forall m \le M_C:\ \binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} (R^{Q_s}\, Q^{\otimes Q_s}(A_{\text{adv}}))^{(\alpha-1)/\alpha} \le \binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha}\, y$

[(L4), (L5), (L6); y (Definition 5.3); $x \mapsto x^{(\alpha-1)/\alpha}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L9) $\forall m \le Q_s N:\ P^{\otimes Q_s}(E_m) \le \binom{Q_s N}{m} \bar{p}_C^m$

[item 3 of (I1)]

(L10) $\forall m > M_C\ \forall w \in E_m:\ |\{(j,i) : (w_j)_i \in C_i\}| = m$

[E_m (Lemma 5.4)]

(L11) $\forall m > M_C:\ m \ge M_C + 1$

[$m \in \mathbb{Z}$]

(L12) $\bigcup_{M_C < m \le Q_s N} E_m \subseteq \bigcup_{|I| = M_C+1} \{w \in \mathcal{E} : \forall (j,i) \in I\ (w_j)_i \in C_i\}$

[(L10), (L11), at a set I of $M_C + 1$ of the fringe leaves of w; E_m, $\mathcal{E}$ (Lemma 5.4)]

(L13) $P^{\otimes Q_s}(\bigcup_{M_C < m \le Q_s N} E_m) \le \binom{Q_s N}{M_C+1} \bar{p}_C^{M_C+1}$

[(L12); Fact A.45, item 5; item 2 of (I1) at $|I| := M_C + 1$]

(L14) $(\mathbb{Z}^N)^{Q_s} = \mathcal{E}^c \cup \bigcup_{m \le Q_s N} E_m$

[$\mathcal{E}$, E_m (the proof's block); $\mathcal{K}$ (Definition A.26)]

(L15) $\Rightarrow$ $P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$

[(L14); (L2); (L7), (L8) at $m := 0$; $\binom{Q_s N}{0} = 1$ (Fact A.41, item 39); $1^a = 1$ (Fact A.41, item 43); $\kappa_C^0 = 1$ (Fact A.41, item 41); (L7), (L8) and (L9) at $m \in \{1, \dots, M_C\}$; (L13) beyond; $\lambda_{\mathcal{F}}$ (the statement), $2^{-\lambda_{\mathcal{F}}}$ at A, M_C (Definition 5.3); $\Pi_C(y)$ (Definition 5.2)]

(L16) $\Rightarrow$ the statement

[(L15)]

□

H.2 The induced form, the computed FFT entry, the checked key's bounds and the acceptance word

Structure. This subsection proves the statements of Section 5.2 and the steps an instantiation takes. Section H.2.1 states the induced form; Section H.2.2 the FFT; Section H.2.3 the checked key; Section H.2.4 the acceptance word.

H.2.1 The induced form

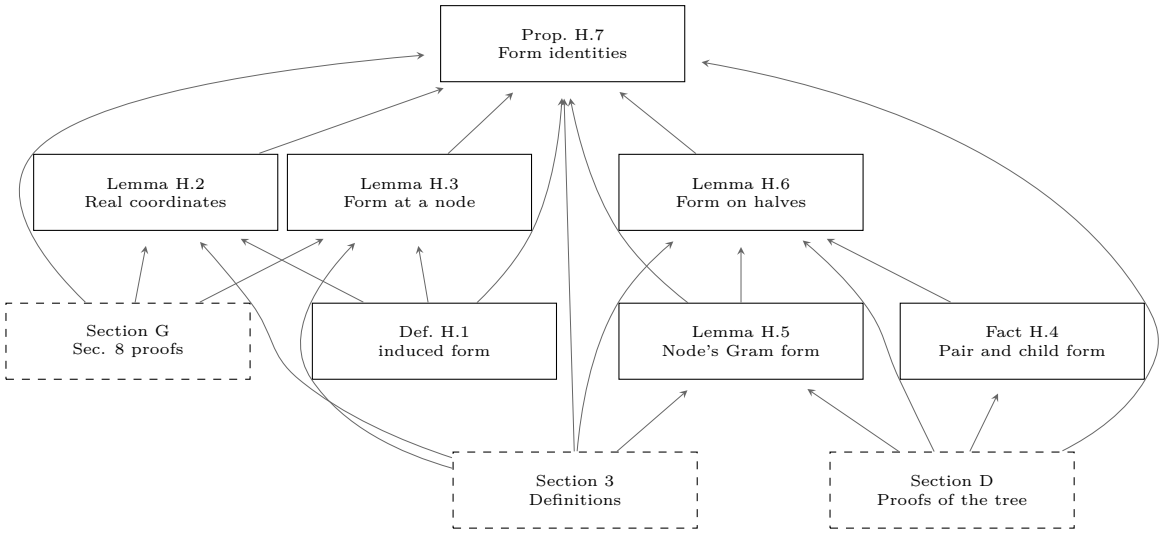


Figure 61: Dependencies, Section H.2.1.

Figure 62 describes the symbols of this subsection on the tree; Definition H.1 states the induced form; Proposition H.7 its identities.

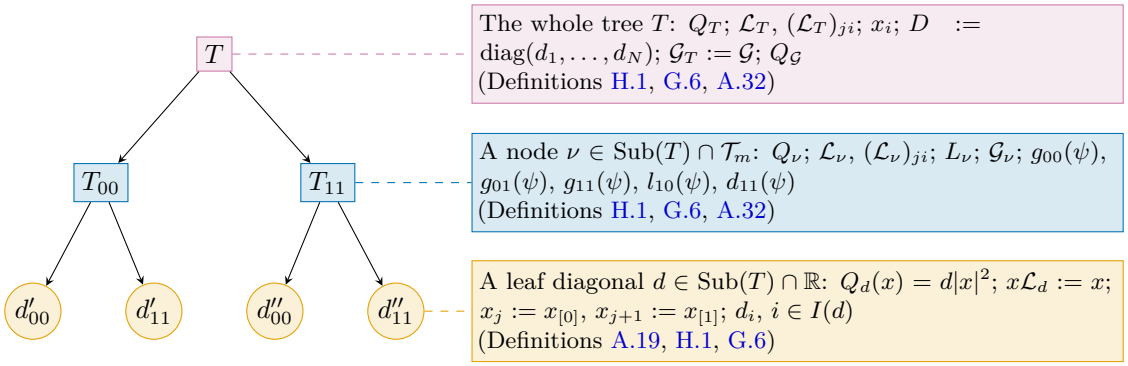


Figure 62: The objects of Section H.2.1 by the part of the tree of Figure 22 that carries them.

Definition H.1 (Induced form [to table])**.** A tree induces on each subtree the form of its leaf diagonals along the tree map. Let:

- $T \in \mathcal{T}_n$;
- $m \in \mathbb{Z}_{>0}$;
- $T' \in \mathrm{Sub}(T) \cap \mathcal{T}_m$;
- $d \in \mathrm{Sub}(T) \cap \mathbb{R}$.

Define:

- $\mathrm{split}(a) := (a_0, a_1)$ for $a \in \mathcal{R}_m$, $m \geq 4$ (Definition A.15);
- $a_0 := \sum_{i<m/2} a_{[2i]} x^i$ and $a_1 := \sum_{i<m/2} a_{[2i+1]} x^i$ (Definition A.15);
- $d_v^{T'}$, the leaf diagonals of T' (Definition A.19 at T');
- $Q_d(x) := d|x|^2$ for $x \in \mathcal{R}_2$;
- $\mathcal{L}_{T'}$, the tree map at T' (Definition G.6);
- $Q_{T'}(x) := \sum_{v \leq m} d_v^{T'} |(x\mathcal{L}_{T'})_v|^2$ for $x \in \mathcal{R}_m^2$;
- $Q_{T'}(f) := Q_{T'}(\mathrm{split}(f))$ for $f \in \mathcal{R}_{2m}$ if $m \geq 2$.

```
noncomputable def Q {k : Nat} (T : FTree k) (x : SlotVec k x SlotVec k) : Real :=
  (List.zipWith (fun d c => d * ||c|| ^ 2) T.weights (T.coords x)).sum

def weights : {k : Nat} -> FTree k -> List Real
  | _, base d0 d1 _ => [d1, d0]
  | _, node _ _ T0 T1 => T1.weights ++ T0.weights
```

Figure 63: The Lean declarations carrying Definition H.1: `FTree.Q`, `FTree.weights` (`TreeRec.lean`); with `SlotVec`, `FTree` of Figure 21; with `FTree.coords` of Figure 49; Lean's symbols in ASCII.

Lemma H.2 (The induced form in the real coordinates [to table])**.** *The induced form of a tree is the sum, over the real coordinates of its tree map, of each coordinate's square weighted by the leaf diagonal at its position. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18).*

Define:

- $Q_T(x) := \sum_{v \leq n} d_v^T |(x\mathcal{L}_T)_v|^2$ *for* $x \in \mathcal{R}_n^2$, d_v^T *the leaf diagonals of* T *(Definition H.1);*
- $(x\mathcal{L}_T)_v \in \mathcal{R}_2$, $v \leq n$, *the entries of* $x\mathcal{L}_T \in \mathcal{R}_2^n$ *(Definition G.6);*
- $(x\mathcal{L}_T)_{2v-1} := \mathrm{Re}\,(x\mathcal{L}_T)_v$ *and* $(x\mathcal{L}_T)_{2v} := \mathrm{Im}\,(x\mathcal{L}_T)_v$ *(Definition G.6);*
- $d_i := d$ *for* $i \in I(d)$, *the leaf diagonal at the position* i *(Definition A.19);*
- $\forall v \leq n:\ d_v := d_{2v-1}$ *(Definition A.19).*

Then

$$\forall x \in \mathcal{R}_n \times \mathcal{R}_n: \quad Q_T(x) = \sum_{i \leq N} d_i (x\mathcal{L}_T)_i^2.$$

Proof. (L1) $Q_T(x) = \sum_{v \leq n} d_v |(x\mathcal{L}_T)_v|^2$

[Definition H.1 at $T' := T$]

(L2) $\forall v \leq n:\ |(x\mathcal{L}_T)_v|^2 = (\mathrm{Re}\,(x\mathcal{L}_T)_v)^2 + (\mathrm{Im}\,(x\mathcal{L}_T)_v)^2$

[Fact A.41, item 1: $|a+ib|^2 = a^2 + b^2$]

(L3) $\forall v \leq n:\ (\mathrm{Re}\,(x\mathcal{L}_T)_v, \mathrm{Im}\,(x\mathcal{L}_T)_v) = ((x\mathcal{L}_T)_{2v-1}, (x\mathcal{L}_T)_{2v})$

[Definition G.6]

(L4) $\forall v \leq n:\ (d_{2v-1}, d_{2v}) = (d_v, d_v)$

[Definition A.19]

(L5) $\Rightarrow\ \forall v \leq n:\ d_v |(x\mathcal{L}_T)_v|^2 = d_{2v-1}(x\mathcal{L}_T)_{2v-1}^2 + d_{2v}(x\mathcal{L}_T)_{2v}^2$

[(L2), (L3), (L4)]

(L6) $\{2v-1 : v \leq n\} \sqcup \{2v : v \leq n\} = \{1, \ldots, N\}$

[$N = 2n$ (the statement)]

(L7) $\Rightarrow$ $\sum_{v\le n} d_v|(x\mathcal{L}_T)_v|^2 = \sum_{i\le N} d_i(x\mathcal{L}_T)_i^2$

[(L5), (L6)]

(L8) $\Rightarrow$ the statement

[(L1), (L7)]

□

Lemma H.3 (The induced form at a node [to table])**.** *At a node, the induced form is the first child's form at the first coordinate of the node factor's image plus the second child's form at the second coordinate. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18).*

Define:

- $Q_d(x) := d|x|^2$ *for* $d \in \mathrm{Sub}(T) \cap \mathbb{R}$ *and* $x \in \mathcal{R}_2$ *(Definition H.1);*
- $Q_{T'}(x) := \sum_{v\le m} d_v^{T'} |(x\mathcal{L}_{T'})_v|^2$ *for* $T' \in \mathrm{Sub}(T) \cap \mathcal{T}_m$ *and* $x \in \mathcal{R}_m^2$ *(Definition H.1);*
- $Q_{T'}(f) := Q_{T'}(\mathrm{split}(f))$ *for* $f \in \mathcal{R}_{2m}$ *(Definition H.1);*
- $d_v^{T'}$*, the leaf diagonals of* T' *(Definition A.19 at* T'*).*

Then the form satisfies, at a node of degree 2 *and at a node of a larger degree:*

1. $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T)\ \forall x \in \mathcal{R}_2^2 :\ Q_\nu(x) = Q_{d_{00}}(x_0 + x_1 l_{10}) + Q_{d_{11}}(x_1)$;
2. $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \ge 4\ \forall x \in \mathcal{R}_m^2 :\ Q_\nu(x) = Q_{T_{00}}(x_0 + x_1 l_{10}) + Q_{T_{11}}(x_1)$.

Proof.

DEFINES ν, x: those of the item's quantifiers, in each item

DEFINES $d_v^{T'}$, $I(T')$, $T' \in \mathrm{Sub}(T)$, those of Definition A.19

DEFINES $x\mathcal{L}_{T'}$, $T' \in \mathrm{Sub}(T)$, that of Definition G.6

Proof of item 1.

(L1) $Q_\nu(x) = d_1^\nu|(x\mathcal{L}_\nu)_1|^2 + d_2^\nu|(x\mathcal{L}_\nu)_2|^2$

[Definition H.1 at $T' := \nu$, $m = 2$]

(L2) $x\mathcal{L}_\nu = (x_1,\ x_0 + x_1 l_{10})$

[Definition G.6]

(L3) $(d_1^\nu, d_2^\nu) = (d_{11}, d_{00})$

[Definition A.19: $I(T_{11})$ precedes $I(T_{00})$]

(L4) $\Rightarrow$ $Q_\nu(x) = d_{11}|x_1|^2 + d_{00}|x_0 + x_1 l_{10}|^2$

[(L1), (L2), (L3)]

(L5) $\Rightarrow$ $Q_\nu(x) = Q_{d_{00}}(x_0 + x_1 l_{10}) + Q_{d_{11}}(x_1)$

[(L4); $Q_d(y) = d|y|^2$ (Definition H.1)]

(L6) $\Rightarrow$ item 1

[(L5)]

□ (item 1)

Proof of item 2.

(L7) $Q_\nu(x) = \sum_{v\le m} d_v^\nu|(x\mathcal{L}_\nu)_v|^2$

[Definition H.1 at $T' := \nu$]

(L8) $x\mathcal{L}_\nu = (\mathrm{split}(x_1)\mathcal{L}_{T_{11}},\ \mathrm{split}(x_0 + x_1 l_{10})\mathcal{L}_{T_{00}})$

[Definition G.6: $xL_\nu = (x_0 + x_1 l_{10},\ x_1)$]

(L9) $\forall v \le m/2 :\ d_v^\nu = d_v^{T_{11}}$

[Definition A.19: $I(T_{11})$ precedes $I(T_{00})$]

(L10) $\forall v \le m/2 :\ d_{m/2+v}^\nu = d_v^{T_{00}}$

[Definition A.19: $I(T_{11})$ precedes $I(T_{00})$]

(L11) $\Rightarrow$ $Q_\nu(x) = \sum_{v\le m/2} d_v^{T_{11}}|(\mathrm{split}(x_1)\mathcal{L}_{T_{11}})_v|^2 + \sum_{v\le m/2} d_v^{T_{00}}|(\mathrm{split}(x_0 + x_1 l_{10})\mathcal{L}_{T_{00}})_v|^2$

[(L7) to (L10)]

(L12) $\Rightarrow$ $Q_\nu(x) = Q_{T_{11}}(\mathrm{split}(x_1)) + Q_{T_{00}}(\mathrm{split}(x_0 + x_1 l_{10}))$

[(L11); Definition H.1 at $T' := T_{11}$ and at $T' := T_{00}$]

(L13) $\Rightarrow$ $Q_\nu(x) = Q_{T_{00}}(x_0 + x_1 l_{10}) + Q_{T_{11}}(x_1)$

[(L12); $Q_{T'}(f) = Q_{T'}(\mathrm{split}(f))$ (Definition H.1) at $T' \in \{T_{00}, T_{11}\}$, $\{T_{00}, T_{11}\} \subseteq \mathcal{T}_{m/2}$, $f \in \mathcal{R}_m$]

(L14) $\Rightarrow$ item 2

[(L13)]

□ (item 2)

Fact H.4 (The parent's weighted sum and the child's Gram form [to table])**.** The parent's diagonal values $d(\psi)$ and $d(-\psi)$ weight the squared moduli $|y_0 + \psi y_1|^2$ and $|y_0 - \psi y_1|^2$, and the weighted sum is twice the child's Gram form on (y_0, y_1). Let:

- $m \geq 2$, a power of two;
- $d \in \mathcal{R}_m$;
- $\psi \in \mathbb{C}$ with $\psi^m = -1$;
- $y_0, y_1 \in \mathbb{C}$.

Define:

- $a := d(\psi)$ and $b := d(-\psi)$ (Fact D.1);
- (d_0, d_1), the values of $\mathrm{split}_{\mathrm{sa}}$ (Algorithm 3) at d and ψ (Fact D.1);
- $y_+ := y_0 + \psi y_1$;
- $y_- := y_0 - \psi y_1$;
- $y' := (y_0, y_1)$;
- $\mathcal{G}_{\mathrm{child}} := \begin{pmatrix} d_0 & d_1 \\ \mathrm{conj}\, d_1 & d_0 \end{pmatrix}$, that of lines 16, 30 of ffsamp (Algorithm 6).

Assume:

(A1) $d(\psi) > 0$;

(A2) $d(-\psi) > 0$.

Then

$$a|y_+|^2 + b|y_-|^2 = 2\, y' \mathcal{G}_{\mathrm{child}} y'^{\dagger}. \qquad \text{[derived]}$$

Proof. (L1) $|\psi| = 1$

[Fact A.42, item 1]

(L2) $\forall s \in \{1, -1\}:\ |y_0 + s\psi y_1|^2 = |y_0|^2 + |\psi y_1|^2 + 2s\,\mathrm{Re}(y_0\, \mathrm{conj}\, \psi\, \mathrm{conj}\, y_1)$

[expand $(y_0 + s\psi y_1)\, \mathrm{conj}\, (y_0 + s\psi y_1)$; Fact A.41, item 1: $w\, \mathrm{conj}\, w = |w|^2$, $w + \mathrm{conj}\, w = 2\,\mathrm{Re}\, w$]

(L3) $\Rightarrow$ $\forall s \in \{1, -1\}:\ |y_0 + s\psi y_1|^2 = |y_0|^2 + |y_1|^2 + 2s\,\mathrm{Re}(y_0\, \mathrm{conj}\, \psi\, \mathrm{conj}\, y_1)$

[(L1), (L2); Fact A.41, item 1: $|xy| = |x||y|$]

(L4) $\Rightarrow$ $a|y_+|^2 + b|y_-|^2 = (a+b)(|y_0|^2 + |y_1|^2) + 2(a-b)\,\mathrm{Re}(y_0\, \mathrm{conj}\, \psi\, \mathrm{conj}\, y_1)$

[(L3) at $s := 1$ and at $s := -1$; $y_\pm$ (the statement)]

(L5) $d_0 = \mathrm{AM}(a, b)$

[Fact D.1, item 1, at (m, d, ψ); $a = d(\psi)$, $d(\psi) > 0$, $b = d(-\psi)$, $d(-\psi) > 0$ (assumptions A1, A2)]

(L6) $\mathrm{AM}(a, b) = (a+b)/2$

[Definition A.46]

(L7) $d_1 = ((a-b)/2)\ \mathrm{conj}\, \psi$

[Fact D.1, item 2, at (m, d, ψ); $a, b > 0$ (assumptions A1, A2)]

(L8) $\Rightarrow$ $a|y_+|^2 + b|y_-|^2 = 2\left(d_0(|y_0|^2 + |y_1|^2) + 2\,\mathrm{Re}(y_0 d_1\, \mathrm{conj}\, y_1)\right)$

[(L4), (L5), (L6), (L7)]

(L9) $2\left(d_0(|y_0|^2 + |y_1|^2) + 2\,\mathrm{Re}(y_0 d_1\, \mathrm{conj}\, y_1)\right) = 2\, y' \mathcal{G}_{\mathrm{child}} y'^{\dagger}$

[Fact A.44, item 1, at $(g_{00}, g_{01}, g_{11}) := (d_0, d_1, d_0)$, $x := y'$; $\mathcal{G}_{\mathrm{child}}$, y' (the statement)]

(L10) $\Rightarrow$ the statement

[(L8), (L9)]

□

Lemma H.5 (A node's Gram form [to table])**.** *The Gram form of a node's matrix is its first diagonal times the squared node factor's image plus its Schur complement times the squared second coordinate. Let:*

- $\mathcal{G} \in \mathrm{Gram}_n$ *(Definition A.14).*

Define:

- $T := \mathrm{ffLDL}^\dagger(\mathcal{G})$ *(Definition A.20);*
- $\mathcal{G}_\nu$*, that of Definition A.32;*
- (g_{00}, g_{01}, g_{11})*, the entries of* $\mathcal{G}_\nu(\psi)$ *(Definition A.14);*
- $l_{10}(\psi) := \operatorname{conj} g_{01}(\psi)/g_{00}(\psi)$ *and* $d_{11}(\psi) := g_{11}(\psi) - |g_{01}(\psi)|^2/g_{00}(\psi)$ *(Definition A.17);*
- $y := x_0(\psi) + x_1(\psi) l_{10}$.

Then

$$\forall m\ \forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m\ \forall \psi,\ \psi^m = -1\ \forall x \in \mathcal{R}_m \times \mathcal{R}_m : \quad x(\psi)\mathcal{G}_\nu(\psi)x(\psi)^\dagger = g_{00}|y|^2 + d_{11}|x_1(\psi)|^2.$$

Proof. (L1) $x(\psi)\mathcal{G}_\nu(\psi)x(\psi)^\dagger = g_{00}|x_0(\psi)|^2 + 2\,\mathrm{Re}(x_0(\psi) g_{01} \operatorname{conj} x_1(\psi)) + g_{11}|x_1(\psi)|^2$
[Fact A.44, item 1, at $\mathcal{G} := \mathcal{G}_\nu(\psi)$ (Definition A.32), $x := (x_0(\psi), x_1(\psi))$]

(L2) $2\,\mathrm{Re}(x_0(\psi) g_{01} \operatorname{conj} x_1(\psi)) = g_{01} x_0(\psi) \operatorname{conj} x_1(\psi) + \operatorname{conj} g_{01}\ \operatorname{conj} x_0(\psi) x_1(\psi)$
[Fact A.41, item 1: $w + \operatorname{conj} w = 2\,\mathrm{Re}\, w$ at $w := x_0(\psi) g_{01} \operatorname{conj} x_1(\psi)$]

(L3) $g_{00}|x_0(\psi)+x_1(\psi)l_{10}|^2 = g_{00}|x_0(\psi)|^2 + g_{00} \operatorname{conj} l_{10}\, x_0(\psi) \operatorname{conj} x_1(\psi) + g_{00} l_{10}\ \operatorname{conj} x_0(\psi) x_1(\psi) + g_{00} l_{10} \operatorname{conj} l_{10}\, |x_1(\psi)|^2$
[expand $(x_0(\psi) + x_1(\psi) l_{10})\ \operatorname{conj}(x_0(\psi) + x_1(\psi) l_{10})$; Fact A.41, item 1: $w \operatorname{conj} w = |w|^2$]

(L4) $g_{00} \operatorname{conj} l_{10} = g_{01}$
[Lemma D.4, items 1 and 2: $d_{00} = g_{00}$, $d_{00} \operatorname{conj} l_{10} = g_{01}$]

(L5) $g_{00} l_{10} = \operatorname{conj} g_{01}$
[Lemma D.4, items 1 and 3: $l_{10} d_{00} = \operatorname{conj} g_{01}$]

(L6) $\operatorname{conj} l_{10} = g_{01}/g_{00}$
[(L4); $g_{00} > 0$ (Lemma D.6, item 1)]

(L7) $\Rightarrow$ $g_{00} l_{10} \operatorname{conj} l_{10} = \operatorname{conj} g_{01}\, g_{01}/g_{00}$
[(L5), (L6)]

(L8) $\Rightarrow$ $g_{00} l_{10} \operatorname{conj} l_{10} = |g_{01}|^2/g_{00}$
[(L7); Fact A.41, item 1: $w \operatorname{conj} w = |w|^2$]

(L9) $\Rightarrow$ $g_{00}|x_0(\psi) + x_1(\psi) l_{10}|^2 = g_{00}|x_0(\psi)|^2 + g_{01} x_0(\psi) \operatorname{conj} x_1(\psi) + \operatorname{conj} g_{01}\ \operatorname{conj} x_0(\psi) x_1(\psi) + (|g_{01}|^2/g_{00})|x_1(\psi)|^2$
[(L3), (L4), (L5), (L8)]

(L10) $d_{11}|x_1(\psi)|^2 = g_{11}|x_1(\psi)|^2 - (|g_{01}|^2/g_{00})|x_1(\psi)|^2$
[$d_{11}(\psi) := g_{11}(\psi) - |g_{01}(\psi)|^2/g_{00}(\psi)$ (Definition A.17)]

(L11) $\Rightarrow$ $g_{00}|x_0(\psi) + x_1(\psi) l_{10}|^2 + d_{11}|x_1(\psi)|^2$
$= g_{00}|x_0(\psi)|^2 + g_{01} x_0(\psi) \operatorname{conj} x_1(\psi) + \operatorname{conj} g_{01}\ \operatorname{conj} x_0(\psi) x_1(\psi) + g_{11}|x_1(\psi)|^2$
[(L9), (L10)]

(L12) $\Rightarrow$ $x(\psi)\mathcal{G}_\nu(\psi)x(\psi)^\dagger = g_{00}|y|^2 + d_{11}|x_1(\psi)|^2$
[(L1), (L2), (L11); $y = x_0(\psi) + x_1(\psi) l_{10}$ (the statement)]

(L13) $\Rightarrow$ the statement
[(L12)]

□

Lemma H.6 (A node's Gram form on the split halves [to table])**.** *At a node of degree at least* 4*, the Gram form of the node's matrix is the first child's Gram form on the split of the node factor's image plus the second child's Gram form on the split of the second coordinate. Let:*

- $\mathcal{G} \in \mathrm{Gram}_n$ *(Definition A.14);*
- $T = \mathrm{ffLDL}^\dagger(\mathcal{G})$ *(Definition A.20).*

Define:

- $\mathcal{G}_\nu$, $\mathcal{G}_{T_{00}}$ *and* $\mathcal{G}_{T_{11}}$, *those of Definition A.32;*
- $\psi_k := e^{i\pi(2k+1)/m}$ *for* $k < m/2$ *(Definition A.32);*
- $Q_{\mathcal{G}}(x) := \frac{2}{m}\sum_{k<m/2} x(\psi_k)\mathcal{G}(\psi_k)x(\psi_k)^\dagger$ *(Definition A.32);*
- $\mathrm{split}(a) := (a_0, a_1)$ *for* $a \in \mathcal{R}_m$, $m \geq 4$ *(Definition A.15);*
- $a_0 := \sum_{i<m/2} a_{[2i]}x^i$ *and* $a_1 := \sum_{i<m/2} a_{[2i+1]}x^i$ *(Definition A.15);*
- $l_{10} \in \mathcal{R}_m$, *that of Definition A.20, item 1, at* $\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11})$*;*
- $Y := x_0 + x_1 l_{10} \in \mathcal{R}_m$, *for* $x := (x_0, x_1) \in \mathcal{R}_m^2$.

Then

$$\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall x \in \mathcal{R}_m \times \mathcal{R}_m :$$
$$Q_{\mathcal{G}_\nu}(x) = Q_{\mathcal{G}_{T_{00}}}(\mathrm{split}(Y)) + Q_{\mathcal{G}_{T_{11}}}(\mathrm{split}(x_1)).$$

Proof.

DEFINES $(f_0, f_1) := \mathrm{split}(f)$, $f \in \mathcal{R}_m$ (split (Algorithm 2))

DEFINES $f' := (f_0, f_1)$, $f \in \mathcal{R}_m$

DEFINES g_{00}, the first entry of $\mathcal{G}_\nu$ (Definition A.14), the first diagonal of ν

DEFINES $d_{11} \in \mathcal{R}_m$, the second diagonal of ν (Definition A.20, item 1)

(L1) $\forall f \in \mathcal{R}_m\ \forall \psi,\ \psi^m = -1 :\ f_0(\psi^2) = (f(\psi) + f(-\psi))/2$

[split (Algorithm 2), line 5]

(L2) $\forall f \in \mathcal{R}_m\ \forall \psi,\ \psi^m = -1 :\ f_1(\psi^2) = ((f(\psi) - f(-\psi))/2)\ \mathrm{conj}\,\psi$

[split (Algorithm 2), line 7]

(L3) $\forall \psi,\ \psi^m = -1 :\ \psi\,\mathrm{conj}\,\psi = 1$

[Fact A.42, item 1]

(L4) $\Rightarrow\ \forall f\ \forall \psi,\ \psi^m = -1 :\ f(\psi) = f_0(\psi^2) + \psi f_1(\psi^2)$

[(L1), (L2), (L3)]

(L5) $\Rightarrow\ \forall f\ \forall \psi,\ \psi^m = -1 :\ f(-\psi) = f_0(\psi^2) - \psi f_1(\psi^2)$

[(L1), (L2), (L3)]

(L6) $\forall d \in \{g_{00}, d_{11}\}\ \forall \psi,\ \psi^m = -1 :\ \mathcal{G}_d(\psi^2) = \begin{pmatrix} d_0(\psi^2) & d_1(\psi^2) \\ \mathrm{conj}\, d_1(\psi^2) & d_0(\psi^2) \end{pmatrix}$

[$\mathcal{G}_d$ (Definition A.23)]

(L7) $\Rightarrow\ \forall f\ \forall d \in \{g_{00}, d_{11}\}\ \forall \psi,\ \psi^m = -1 :$

$$d(\psi)|f(\psi)|^2 + d(-\psi)|f(-\psi)|^2 = 2\, f'(\psi^2)\mathcal{G}_d(\psi^2)f'(\psi^2)^\dagger$$

[Fact H.4 at $(d, \psi, y_0, y_1) := (d, \psi, f_0(\psi^2), f_1(\psi^2))$; (L4), (L5), (L6); $d(\pm\psi) > 0$ (Lemma D.6, items 1 and 2)]

(L8) $\forall k < m/4 :\ \psi_{m/2-1-k} = e^{i\pi(m-2k-1)/m}$

[$\psi_k = e^{i\pi(2k+1)/m}$ (Definition A.32)]

(L9) $\Rightarrow\ \forall k < m/4 :\ \psi_{m/2-1-k} = \mathrm{conj}\,(-\psi_k)$

[(L8); Fact A.41, item 12: $e^{i\pi} = -1$, $\mathrm{conj}\, e^{i\theta} = e^{-i\theta}$]

(L10) $\forall f \in \{x_0, x_1, g_{00}, g_{01}, g_{11}\}\ \forall \psi,\ \psi^m = -1 :\ f(\mathrm{conj}\,\psi) = \mathrm{conj}\, f(\psi)$

[Fact A.42, item 2]

(L11) $\Rightarrow\ \forall \psi,\ \psi^m = -1 :\ x(\mathrm{conj}\,\psi)\mathcal{G}_\nu(\mathrm{conj}\,\psi)x(\mathrm{conj}\,\psi)^\dagger = \mathrm{conj}\, x(\psi)\mathcal{G}_\nu(\psi)x(\psi)^\dagger$

[(L10); Fact A.44, item 1]

(L12) $\forall \psi,\ \psi^m = -1 :\ x(\psi)\mathcal{G}_\nu(\psi)x(\psi)^\dagger \in \mathbb{R}$

[Fact A.44, item 1]

(L13) $\Rightarrow\ \forall \psi,\ \psi^m = -1 :\ x(\mathrm{conj}\,\psi)\mathcal{G}_\nu(\mathrm{conj}\,\psi)x(\mathrm{conj}\,\psi)^\dagger = x(\psi)\mathcal{G}_\nu(\psi)x(\psi)^\dagger$

[(L11), (L12)]

(L14) $\Rightarrow\ \sum_{k<m/2} x(\psi_k)\mathcal{G}_\nu(\psi_k)x(\psi_k)^\dagger =$

$$\sum_{k<m/4} [x(\psi_k)\mathcal{G}_\nu(\psi_k)x(\psi_k)^\dagger + x(-\psi_k)\mathcal{G}_\nu(-\psi_k)x(-\psi_k)^\dagger]$$

[(L9); (L13) at $\psi := -\psi_k$]

	Lemma H.5 at every $k < m/4$	This proof
	Shared: $n,\ \mathcal{G},\ T,\ m, \nu,\ \mathcal{G}_\nu,\ x$	
	ψ	$\pm\psi_k$
(I1)	g_{00}, l_{10}, d_{11}	$g_{00}(\pm\psi_k), l_{10}(\pm\psi_k), d_{11}(\pm\psi_k)$
	y	$Y(\pm\psi_k)$
	$\psi^m = -1$	ψ_k (Definition A.32); Fact A.43, item 3, at m

Its conclusion:
$\forall m\ \forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m\ \forall \psi,\ \psi^m = -1\ \forall x \in \mathcal{R}_m \times \mathcal{R}_m :\ x(\psi)\mathcal{G}_\nu(\psi)x(\psi)^\dagger = g_{00}|y|^2 + d_{11}|x_1|^2$

(L15) $\Rightarrow\ Q_{\mathcal{G}_\nu}(x) = \dfrac{2}{m}\displaystyle\sum_{k<m/4} \big[g_{00}(\psi_k)|Y(\psi_k)|^2 + g_{00}(-\psi_k)|Y(-\psi_k)|^2 + d_{11}(\psi_k)|x_1(\psi_k)|^2 + d_{11}(-\psi_k)|x_1(-\psi_k)|^2\big]$
[$Q_\mathcal{G}$ (Definition A.32); (L14); (I1); Y (the statement)]

(L16) $\Rightarrow\ Q_{\mathcal{G}_\nu}(x) = \frac{4}{m}\sum_{k<m/4}\big[Y'(\psi_k^2)\mathcal{G}_{g_{00}}(\psi_k^2)Y'(\psi_k^2)^\dagger + x_1'(\psi_k^2)\mathcal{G}_{d_{11}}(\psi_k^2)x_1'(\psi_k^2)^\dagger\big]$
[(L15); (L7) at ψ_k with $(f,d) := (Y, g_{00})$ and with $(f,d) := (x_1, d_{11})$]

(L17) $\forall k < m/4 :\ \psi_k^2 = e^{i\pi(2k+1)/(m/2)}$
[ψ_k (Definition A.32)]

(L18) $\mathcal{G}_{T_{00}} = \mathcal{G}_{g_{00}}$
[Definition A.32: $\mathcal{G}_{T_{00}} = \mathcal{G}_{d_{00}}$; $d_{00} = g_{00}$ (Lemma D.4, item 1)]

(L19) $\mathcal{G}_{T_{11}} = \mathcal{G}_{d_{11}}$
[Definition A.32]

(L20) $2/(m/2) = 4/m$
[expand]

(L21) $\Rightarrow\ Q_{\mathcal{G}_\nu}(x) = Q_{\mathcal{G}_{T_{00}}}(Y') + Q_{\mathcal{G}_{T_{11}}}(x_1')$
[(L16) to (L20); $Q_\mathcal{G}$ (Definition A.32) over $\mathcal{R}_{m/2}$]

(L22) $\Rightarrow\ Q_{\mathcal{G}_\nu}(x) = Q_{\mathcal{G}_{T_{00}}}(\mathrm{split}(Y)) + Q_{\mathcal{G}_{T_{11}}}(\mathrm{split}(x_1))$
[(L21); $f' = \mathrm{split}(f)$ (the proof's block)]

(L23) $\Rightarrow$ the statement
[(L22)]

□

Proposition H.7 (Identities of the induced form [to table])**.** *The induced form of a tree has three readings: the quadratic form of the tree map's $LDL^\dagger$ product, the exponent of the product of the leaf Gaussians, and the Gram form of the matrix the tree decomposes. Let:*

- $T \in \mathcal{T}_n$ *(Definition A.18);*
- $s > 0$*;*
- $t \in \mathcal{R}_n^2$*;*
- $\mathcal{G} \in \mathrm{Gram}_n$ *(Definition A.14).*

Define:

- (σ_i, c_i)*, those of* ffSampling(t, T) *(Definition G.9);*
- $\mathcal{L}_T$*, the tree map at T, and x_j, the coordinate of x at j (Definition G.6);*
- $Q_T(x) := \sum_{v \le n} d_v^T\, |(x\mathcal{L}_T)_v|^2$ *for $x \in \mathcal{R}_n^2$, d_v^T the leaf diagonals of T (Definition H.1);*
- $(\mathcal{L}_T)_{ji} := (e^{(j)}\mathcal{L}_T)_i$ *for $j, i \le N$, with $e_i^{(j)} = [i = j]$ (Definition G.6);*
- $x^{(b)} \in \mathcal{R}_n^2$*, the element with $(x_i^{(b)})_{i \le N} = b$, $b \in \mathbb{R}^N$ (Definition G.6);*
- d_i*, the leaf diagonals of T (Definition A.19);*
- $Q_\mathcal{G}(x) := \frac{2}{n}\sum_{k<n/2} x(\psi_k)\mathcal{G}(\psi_k)x(\psi_k)^\dagger$ *at $\psi_k := e^{i\pi(2k+1)/n}$ (Definition A.32);*
- $(\mathcal{L}_T D \mathcal{L}_T^\dagger)_{jk} := \sum_{i \le N} (\mathcal{L}_T)_{ji}\, d_i\, (\mathcal{L}_T)_{ki}$*, $j, k \le N$.*

Then the induced form is the $LDL^\dagger$ form, the Gaussian exponent and, on the tree of $\mathcal{G}$, the Gram form:

1. $\forall x \in \mathcal{R}_n^2 :\ Q_T(x) = \sum_{j,k \le N} x_j \, (\mathcal{L}_T D \mathcal{L}_T^\dagger)_{jk} \, x_k$;

2. $\forall z \in \mathbb{Z}^N :\ \prod_{i \le N} \rho_{\sigma_i, c_i}(z_i) = \exp(-Q_T(t - x^{(z)})/(2s^2))$;

3. *Assume:*

   (A1) $T = \mathrm{ffLDL}^\dagger(\mathcal{G})$.

   Then $\forall x \in \mathcal{R}_n^2 :\ Q_T(x) = Q_{\mathcal{G}}(x)$.

Proof.

DEFINES $x \in \mathcal{R}_n^2$: that of item 1; $z \in \mathbb{Z}^N$: that of item 2

DEFINES $\mathrm{Sub}(d) = \{d\}$, $d \in \mathbb{R}$, and $\mathrm{Sub}(\nu) = \{\nu\} \cup \mathrm{Sub}(L(\nu)) \cup \mathrm{Sub}(R(\nu))$ (Definition A.18)

DEFINES $I(T')$, $T' \in \mathrm{Sub}(T)$, that of Definition A.19

DEFINES $e^{(j)} \in \mathcal{R}_n^2$, $j \le N$, given by $e_i^{(j)} = [i = j]$ (Definition G.6)

DEFINES $t_{T'}$, $\hat{z}_{T'}$, $T' \in \mathrm{Sub}(T)$, and tb_0, z_0, z_1 at a node of degree at least 4, those of ffSampling (Definition A.21) at (t, T)

DEFINES $z_0 := \hat{z}_{T_{00}}$, $z_1 := \hat{z}_{T_{11}}$ at a node $\mathrm{node}(l_{10};\ T_{00}, T_{11})$ of degree 2

DEFINES g_{00}^ν, d_{11}^ν, $\nu \in \mathrm{Sub}(T)$, the g_{00} and d_{11} of $\mathcal{G}_\nu$ (Definitions A.32 and A.17)

DEFINES $z_{T'} := (z_i)_{i \in I(T')}$ and $\varrho_{T'}(t_{T'}, z_{T'}) := \prod_{i \in I(T')} \rho_{\sigma_i, c_i}(z_i)$ (Definition G.9)

DEFINES $\mathcal{G}_\nu$, $\nu \in \mathrm{Sub}(T)$, that of Definition A.32

DEFINES $\psi_k := e^{i\pi(2k+1)/m}$ for $k < m/2$ (Definition A.32)

DEFINES $Y_\nu := x_0 + x_1 l_{10}$, $x = (x_0, x_1) \in \mathcal{R}_m^2$, $\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathcal{T}_m$

Proof of item 1.

(L1) $Q_T(x) = \sum_{i \le N} d_i (x\mathcal{L}_T)_i^2$

[Lemma H.2]

(L2) $x = \sum_{j \le N} x_j e^{(j)}$

[Fact G.7, item 4; $e^{(j)}$ (Definition G.6)]

(L3) $x \mapsto x\mathcal{L}_T$ is $\mathbb{R}$-linear

[Fact G.8]

(L4) $\Rightarrow\ \forall i \le N :\ (x\mathcal{L}_T)_i = \sum_{j \le N} x_j (\mathcal{L}_T)_{ji}$

[(L2), (L3); $(\mathcal{L}_T)_{ji} = (e^{(j)}\mathcal{L}_T)_i$ (Definition G.6)]

(L5) $\Rightarrow\ Q_T(x) = \sum_{i \le N} d_i \Big(\sum_{j \le N} x_j (\mathcal{L}_T)_{ji} \Big) \Big(\sum_{k \le N} x_k (\mathcal{L}_T)_{ki} \Big)$

[(L1), (L4)]

(L6) $\Rightarrow\ Q_T(x) = \sum_{j,k \le N} x_j \Big(\sum_{i \le N} (\mathcal{L}_T)_{ji} \, d_i \, (\mathcal{L}_T)_{ki} \Big) x_k$

[(L5); expand the product of the two finite sums]

(L7) $\Rightarrow$ item 1

[(L6); $(\mathcal{L}_T D \mathcal{L}_T^\dagger)_{jk}$ (the statement)]

□ (item 1)

Proof of item 2.

(L8) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\} :\ \varrho_d(t_d, z_d) = \rho_{\sigma_j, c_j}(z_j) \, \rho_{\sigma_{j+1}, c_{j+1}}(z_{j+1})$

[$\varrho_{T'}$ (Definition G.9) at $T' := d$]

(L9) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\} :\ (\sigma_j, \sigma_{j+1}) = (s/\sqrt{d}, s/\sqrt{d})$

[Definition A.21, item 1]

(L10) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\} :\ (c_j, c_{j+1}) = (\mathrm{Re}\, t_d, \mathrm{Im}\, t_d)$

[Definition A.21, item 2]

(L11) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\} :\ \hat{z}_d = z_j + i z_{j+1}$

[Definition A.21, item 4]

(L12) $\Rightarrow\ \forall d \in \mathrm{Sub}(T) \cap \mathbb{R} :\ \varrho_d(t_d, z_d) = \exp(-d|t_d - \hat{z}_d|^2/(2s^2))$

[(L8) to (L11); Definition A.2, item 1, at $(s, c) := (\sigma_j, c_j)$ and at (σ_{j+1}, c_{j+1}); Fact A.41, item 1: $|a + ib|^2 = a^2 + b^2$; Fact A.41, item 12: $e^a e^b = e^{a+b}$]

(L13) $\Rightarrow$ $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R}:\ \varrho_d(t_d, z_d) = \exp(-Q_d(t_d - \hat{z}_d)/(2s^2))$

[(L12); $Q_d(y) = d|y|^2$ (Definition H.1)]

(L14) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T):\ \varrho_\nu(t_\nu, z_\nu) = \varrho_{T_{11}}(t_{T_{11}}, z_{T_{11}})\, \varrho_{T_{00}}(t_{T_{00}}, z_{T_{00}})$

[$\varrho_{T'}$ (Definition G.9); $I(\nu) = I(T_{11}) \sqcup I(T_{00})$ (Fact A.31, item 2)]

(L15) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ t_{T_{11}} = \mathrm{split}(t_1)$

[Definition A.21, item 13]

(L16) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ t_{T_{00}} = \mathrm{split}(tb_0)$

[Definition A.21, item 17]

(L17) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ t_{T_{11}} - \hat{z}_{T_{11}} = \mathrm{split}(t_1 - z_1)$

[(L15); Lemma G.10, item 1; Fact A.42, item 4]

(L18) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4:\ t_{T_{00}} - \hat{z}_{T_{00}} = \mathrm{split}(tb_0 - z_0)$

[(L16); Lemma G.10, item 2; Fact A.42, item 4]

(L19) $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T):\ t_{T_{11}} - \hat{z}_{T_{11}} = t_1 - \hat{z}_{T_{11}}$

[Definition A.21, item 7]

(L20) $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T):\ t_{T_{00}} - \hat{z}_{T_{00}} = tb_0 - \hat{z}_{T_{00}}$

[Definition A.21, item 10]

(L21) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m:\ tb_0 - z_0 = (t_0 - z_0) + (t_1 - z_1)\, l_{10}$

[$tb_0 = t_0 + (t_1 - z_1)\, l_{10}$ (Definition A.21, items 16, 9; the proof's block)]

(L22) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T):\ t_\nu - \hat{z}_\nu = (t_0 - z_0,\ t_1 - z_1)$

[Definition A.21, items 6, 20, 12]

Lemma H.3 at every $\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T)$	This proof
Shared: $T,\ \nu, l_{10}, T_{00}, T_{11},\ Q_{T'}$	
x	$t_\nu - \hat{z}_\nu$
(I1) d_{00}, d_{11}	T_{00}, T_{11}
$x \in \mathcal{R}_m^2$	(L22)
Its item 1: $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T)\ \forall x \in \mathcal{R}_2^2:\ Q_\nu(x) = Q_{d_{00}}(x_0 + x_1 l_{10}) + Q_{d_{11}}(x_1)$	
Its item 2: $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall x \in \mathcal{R}_m^2:\ Q_\nu(x) = Q_{T_{00}}(x_0 + x_1 l_{10}) + Q_{T_{11}}(x_1)$	

(L23) $\Rightarrow$ $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T):\ Q_{T_{11}}(t_{T_{11}} - \hat{z}_{T_{11}}) + Q_{T_{00}}(t_{T_{00}} - \hat{z}_{T_{00}}) = Q_\nu(t_\nu - \hat{z}_\nu)$

[(L17) to (L22); $Q_{T'}(f) = Q_{T'}(\mathrm{split}(f))$ (Definition H.1); items 1 and 2 of (I1)]

(L24) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T):$

$$\left[\forall T' \in \{T_{00}, T_{11}\}:\ \varrho_{T'}(t_{T'}, z_{T'}) = \exp(-Q_{T'}(t_{T'} - \hat{z}_{T'})/(2s^2))\right] \Rightarrow$$
$$\varrho_\nu(t_\nu, z_\nu) = \exp(-Q_\nu(t_\nu - \hat{z}_\nu)/(2s^2))$$

[(L14), (L23); Fact A.41, item 12: $e^a e^b = e^{a+b}$]

(L25) $\Rightarrow$ $\forall T' \in \mathrm{Sub}(T):\ \varrho_{T'}(t_{T'}, z_{T'}) = \exp(-Q_{T'}(t_{T'} - \hat{z}_{T'})/(2s^2))$

[induction on the depth from the leaves: base (L13), step (L24)]

(L26) $t_T = t$

[Definition A.21, item 5]

(L27) $\varrho_T(t, z) = \prod_{i \leq N} \rho_{\sigma_i, c_i}(z_i)$

[$\varrho_{T'}$ (Definition G.9) at $T' := T$; $I(T) = \{1, \ldots, N\}$ (Definition A.19)]

(L28) $\Rightarrow$ item 2

[(L25) at $T' := T$; Lemma G.10, item 4; (L26), (L27)]

□ (item 2)

Proof of item 3.

(L29) $\forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T):\ \{\psi \in \mathbb{C} : \psi^2 = -1,\ \mathrm{Im}\,\psi > 0\} = \{\psi_0\}$

[ψ_k (Definition A.32) at $m = 2$]

(L30) $\forall f \in \mathcal{R}_2:\ |f| = |f(\psi_0)|$

[$\mathcal{R}_2 = \mathbb{C}$ at $x := \psi_0 = i$ (Definition A.1)]

Lemma H.5 at every $\nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T)$	This proof
Shared: $n,\ \mathcal{G}, T,\ \nu,\ \mathcal{G}_\nu,\ x$	
m	2
ψ	ψ_0
(I2) g_{00}, l_{10}, d_{11}	$g^\nu_{00}(\psi_0), l_{10}(\psi_0), d^\nu_{11}(\psi_0)$
y	$Y_\nu(\psi_0)$
$T = \mathrm{ffLDL}^\dagger(\mathcal{G})$	Assumption A1
$\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m$	The scope; Definition A.18
$\psi^m = -1$	(L29)

Its conclusion:
$\forall m\ \forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m\ \forall \psi,\ \psi^m = -1\ \forall x \in \mathcal{R}_m \times \mathcal{R}_m :\ x(\psi)\mathcal{G}_\nu(\psi)x(\psi)^\dagger = g_{00}|y|^2 + d_{11}|x_1|^2$

(L31) $\Rightarrow\ \forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T)\ \forall x :\ Q_{\mathcal{G}_\nu}(x) = d_{00}|Y_\nu|^2 + d_{11}|x_1|^2$

[$Q_\mathcal{G}$ (Definition A.32) at $m = 2$; Lemma D.6, items 1 and 2; (L29); (I2); (L30); $d_{00} = g_{00}$ (Lemma D.4, item 1)]

(L32) $\Rightarrow\ \forall \nu = \mathrm{node}(l_{10};\ d_{00}, d_{11}) \in \mathrm{Sub}(T)\ \forall x :\ Q_{\mathcal{G}_\nu}(x) = Q_\nu(x)$

[(L31); Lemma H.3, item 1; $Q_d(y) = d|y|^2$ (Definition H.1)]

(L33) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall x :\ Q_{\mathcal{G}_\nu}(x) = Q_{\mathcal{G}_{T_{00}}}(\mathrm{split}(Y_\nu)) + Q_{\mathcal{G}_{T_{11}}}(\mathrm{split}(x_1))$

[Lemma H.6]

(L34) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4 :$
$\big[\forall T' \in \{T_{00}, T_{11}\}\ \forall y :\ Q_{\mathcal{G}_{T'}}(y) = Q_{T'}(y)\big] \Rightarrow$
$\forall x :\ Q_{\mathcal{G}_\nu}(x) = Q_{T_{00}}(\mathrm{split}(Y_\nu)) + Q_{T_{11}}(\mathrm{split}(x_1))$

[(L33); the bracket at $(T', y) := (T_{00}, \mathrm{split}(Y_\nu))$ and at $(T_{11}, \mathrm{split}(x_1))$]

(L35) $\forall \nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m,\ m \geq 4\ \forall x :\ Q_{T_{00}}(\mathrm{split}(Y_\nu)) + Q_{T_{11}}(\mathrm{split}(x_1)) = Q_\nu(x)$

[$Q_{T'}(f) = Q_{T'}(\mathrm{split}(f))$ (Definition H.1); Lemma H.3, item 2; Y_ν (the proof's block)]

(L36) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T)\ \forall x :\ Q_{\mathcal{G}_\nu}(x) = Q_\nu(x)$

[induction on the depth from the leaves: base (L32), step (L34), (L35)]

(L37) $\Rightarrow\ \forall x :\ Q_\mathcal{G}(x) = Q_T(x)$

[(L36) at $\nu := T$; $\mathcal{G}_T = \mathcal{G}$ (Definition A.32); $T = \mathrm{ffLDL}^\dagger(\mathcal{G})$ (assumption A1)]

(L38) $\Rightarrow$ item 3

[(L37)]

□ (item 3)

H.2.2 The FFT

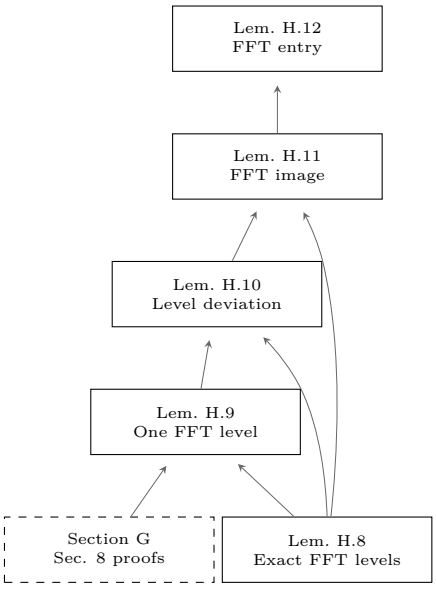


Figure 64: Dependencies, Section H.2.2.

Algorithm 14 FFT(f), the coefficients to $(f(\psi_k))_{k<n/2}$ [L0: `sign_fpoly.c:1242-1267`] [L0: `fxp/sign_fxpoly.c:11-40`]

Input: $f = \sum_{p<n} f_{[p]} x^p \in \mathbb{R}[x]/(x^n+1)$, $f_{[p]} \in \mathcal{F}$; $\psi_k \in \mathbb{C}$, $\widetilde{\psi}_k \in C_{\mathcal{F}}$ (Definition A.8, item 1)
Precondition: $n = 2^h$, $h \in \{1, \dots, 10\}$ (Definition A.8, item 1).
Output (code): $\widetilde{\hat{f}} \in C_{\mathcal{F}}^{n/2}$
Output (idealized): $\hat{f} = (f(\psi))_{\psi} \in \mathbb{C}^{n/2}$
Postcondition: $\forall p < n/2 :\ \hat{f}_p = f(\psi)$, ψ the root at position p of the code's order [gate: `verify/gates/tree/tower_index.py`]
In the proofs: P, $\widetilde{\text{in}}_j$, in_j, $\widetilde{\Lambda}_j$, Λ_j

1: $P \leftarrow n/4$ ▷ the pairs per level
2: $\widetilde{\text{in}}_0 \leftarrow (f_{[p]} + i\, f_{[p+n/2]})_{p<n/2}$
3: $\text{in}_0 \leftarrow (f_{[p]} + i\, f_{[p+n/2]})_{p<n/2}$ ▷ the array read as pairs, exact
4: $a \leftarrow \text{in}_0$ ▷ the working array
5: $t \leftarrow n/2$
6: **for** $j = 0, \dots, h-2$ **do**
7: $m \leftarrow 2^{j+1}$
8: **for** $i = 0, \dots, m/2-1$ **do**
9: $s \leftarrow \psi_{m+i}$ ▷ GM$[m+i]$; $\widetilde{s} \leftarrow \widetilde{\psi}_{m+i}$ in $\mathcal{F}$
10: **for** $j' = 0, \dots, t/2-1$ **do**
11: $j_1 \leftarrow it + j'$
12: $j_2 \leftarrow j_1 + t/2$
13: $x \leftarrow a_{j_1}$
14: $z \leftarrow a_{j_2}\, s$ ▷ merge (Algorithm 4) at the pair
15: $a_{j_1} \leftarrow x + z$
16: $a_{j_2} \leftarrow x - z$
17: **end for**
18: **end for**
19: $\widetilde{\Lambda}_j : C_{\mathcal{F}}^{n/2} \to C_{\mathcal{F}}^{n/2}$, $\widetilde{\Lambda}_j(a)_{j_1} := a_{j_1} \oplus (a_{j_2} \otimes \widetilde{s})$, $\widetilde{\Lambda}_j(a)_{j_2} := a_{j_1} \ominus (a_{j_2} \otimes \widetilde{s})$ ▷ $\widetilde{\text{merge}}$ (Algorithm 4) at each pair, $\widetilde{s} = \widetilde{\psi}_{2^{j+1}+i}$
20: $\Lambda_j : \mathbb{C}^{n/2} \to \mathbb{C}^{n/2}$, $\Lambda_j(a)_{j_1} := a_{j_1} + a_{j_2}\, s$, $\Lambda_j(a)_{j_2} := a_{j_1} - a_{j_2}\, s$ ▷ the P pairs of the level, lines 6 to 14
21: $\widetilde{\text{in}}_{j+1} \leftarrow \widetilde{\Lambda}_j(\widetilde{\text{in}}_j)$
22: $\text{in}_{j+1} \leftarrow \Lambda_j(\text{in}_j)$
23: $t \leftarrow t/2$
24: **end for**
25: $\widetilde{\hat{f}} \leftarrow \widetilde{\text{in}}_{h-1}$
26: $\hat{f} \leftarrow \text{in}_{h-1}$
27: **return** $\widetilde{\hat{f}}$
28: **return** $\hat{f}$

Lemma H.8 (The exact FFT levels [to table])**.** *Each level of the exact FFT is linear and multiplies the Euclidean norm by $\sqrt{2}$, so the image's norm is $\sqrt{n/2}$ times the coefficient norm. Let:*

- *h and $n = 2^h$, as FFT (Algorithm 14) takes them (Precondition).*

Define:

- *$\|f\| := (\sum_{i<n} f_{[i]}^2)^{1/2}$ (Definition A.1 at $m := n$);*
- *in_0, Λ_j, in_{j+1} and $\hat{f}$, those of FFT (Algorithm 14), lines 3, 20, 22 and 26.*

Then the levels and the image satisfy:

1. *$\forall f \in \mathbb{R}[x]/(x^n+1) :\ \|\text{in}_0\| = \|f\|$;*
2. *$\forall j < h-1\ \forall x \in \mathbb{C}^{n/2} :\ \|\Lambda_j x\| = \sqrt{2}\,\|x\|$;*

3. $\forall j < h-1\ \forall x, y \in \mathbb{C}^{n/2}:\ \Lambda_j(x-y) = \Lambda_j x - \Lambda_j y$;

4. $\forall f \in \mathbb{R}[x]/(x^n+1)\ \forall j \le h-1:\ \|\mathrm{in}_j\| = 2^{j/2}\|f\|$;

5. $\forall f \in \mathbb{R}[x]/(x^n+1):\ \|\hat{f}\| = \sqrt{n/2}\,\|f\|$.

Proof.

DEFINES (j_1, j_2), s: a pair of level j and its root, those of FFT (Algorithm 14), lines 6 to 14

DEFINES Π_j: the P pairs (j_1, j_2) of level j

Proof of item 1.

(L1) $\|\mathrm{in}_0\|^2 = \sum_{p<n/2} |f_{[p]} + i f_{[p+n/2]}|^2$

[in_0 (FFT (Algorithm 14), line 3); $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead)]

(L2) $\sum_{p<n/2} |f_{[p]} + i f_{[p+n/2]}|^2 = \sum_{p<n/2} (f_{[p]}^2 + f_{[p+n/2]}^2)$

[Fact A.41, item 1: $|a+ib|^2 = a^2+b^2$]

(L3) $\{p + n/2 : p < n/2\} = \{p : n/2 \le p < n\}$

[$p \mapsto p + n/2$]

(L4) $\{p : p < n/2\} \sqcup \{p : n/2 \le p < n\} = \{p : p < n\}$

[$n/2 \le n$]

(L5) $\Rightarrow\ \|\mathrm{in}_0\|^2 = \sum_{p<n} f_{[p]}^2$

[(L1) to (L4)]

(L6) $\sum_{p<n} f_{[p]}^2 = \|f\|^2$

[$\|f\|$ (Definition A.1)]

(L7) $\Rightarrow\ \|\mathrm{in}_0\| = \|f\|$

[(L5), (L6); Fact A.41, item 5: $t \mapsto \sqrt{t}$ nondecreasing]

(L8) $\Rightarrow$ item 1

[(L7)]

□ (item 1)

Proof of item 2.

(L9) $\forall j < h-1\ \forall x\ \forall (j_1, j_2):\ |(\Lambda_j x)_{j_1}|^2 + |(\Lambda_j x)_{j_2}|^2 = |x_{j_1} + x_{j_2} s|^2 + |x_{j_1} - x_{j_2} s|^2$

[Λ_j (FFT (Algorithm 14), line 20)]

(L10) $\forall j < h-1\ \forall x\ \forall (j_1, j_2):\ |x_{j_1} + x_{j_2} s|^2 + |x_{j_1} - x_{j_2} s|^2 = 2(|x_{j_1}|^2 + |x_{j_2} s|^2)$

[Fact A.41, item 2, at $(x, y) := (x_{j_1}, x_{j_2} s)$]

(L11) $|s| = 1$

[Fact A.42, item 1: $s = \psi_{m+i}$ a root]

(L12) $\Rightarrow\ \forall j < h-1\ \forall x\ \forall (j_1, j_2):\ |(\Lambda_j x)_{j_1}|^2 + |(\Lambda_j x)_{j_2}|^2 = 2(|x_{j_1}|^2 + |x_{j_2}|^2)$

[(L9), (L10), (L11); Fact A.41, item 1: $|xy| = |x||y|$]

(L13) $\forall j < h-1:\ \bigsqcup_{(j_1,j_2)\in\Pi_j} \{j_1, j_2\} = \{0, \ldots, n/2-1\}$

[FFT (Algorithm 14), lines 1 to 14: $j_1 = it + j'$, $j_2 = j_1 + t/2$, $i < m/2$, $j' < t/2$, $mt = n$]

(L14) $\Rightarrow\ \forall j < h-1\ \forall x:\ \|\Lambda_j x\|^2 = 2\|x\|^2$

[(L12), (L13); $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead)]

(L15) $\Rightarrow\ \forall j < h-1\ \forall x:\ \|\Lambda_j x\| = \sqrt{2}\,\|x\|$

[(L14); Fact A.41, item 5: $t \mapsto \sqrt{t}$ nondecreasing]

(L16) $\Rightarrow$ item 2

[(L15)]

□ (item 2)

Proof of item 3.

(L17) $\forall j < h-1\ \forall x, y:\ \Lambda_j(x-y) = \Lambda_j x - \Lambda_j y$

[Λ_j (FFT (Algorithm 14), line 20)]

(L18) $\Rightarrow$ item 3

[(L17)]

□ (item 3)

Proof of item 4.

	Lemma H.8, item 2 at every $j < h-1$	This proof
	Shared: $h, n,\ j,\ \Lambda_j$	
(I1)	x	in_j
	$x \in \mathbb{C}^{n/2}$	in_j (FFT (Algorithm 14), lines 3, 20 and 22)
	Its conclusion: $\forall j < h-1\ \forall x \in \mathbb{C}^{n/2}:\ \|\Lambda_j x\| = \sqrt{2}\,\|x\|$	

(L19) $\forall j < h-1:\ \|\mathrm{in}_{j+1}\| = \sqrt{2}\,\|\mathrm{in}_j\|$

[$\mathrm{in}_{j+1} = \Lambda_j(\mathrm{in}_j)$ (FFT (Algorithm 14), line 22); (I1)]

(L20) $\Rightarrow\ \forall j \le h-1:\ \|\mathrm{in}_j\| = 2^{j/2}\|f\|$

[induction on j: base item 1, step (L19)]

(L21) $\Rightarrow$ item 4

[(L20)]

□ (item 4)

Proof of item 5.

(L22) $\hat{f} = \mathrm{in}_{h-1}$

[FFT (Algorithm 14), line 26]

(L23) $2^{(h-1)/2} = \sqrt{n/2}$

[$n = 2^h$ (the statement)]

	Lemma H.8, item 4	This proof
	Shared: $h, n,\ f,\ \mathrm{in}_j$	
(I2)	j	$h-1$
	Its conclusion: $\forall f \in \mathbb{R}[x]/(x^n+1)\ \forall j \le h-1:\ \|\mathrm{in}_j\| = 2^{j/2}\|f\|$	

(L24) $\Rightarrow\ \|\hat{f}\| = \sqrt{n/2}\,\|f\|$

[(I2); (L22), (L23)]

(L25) $\Rightarrow$ item 5

[(L24)]

□ (item 5)

Lemma H.9 (One computed FFT level [to table])**.** *At each level, the computed FFT's deviation from the exact one grows by at most the factor $\sqrt{2}(1+c_{\mathrm{merge}})$ plus a term in the exact level's norm and in ζ. Let:*

- *$\mathcal{F}$ be a realization at (u,ζ) (Definition A.4);*
- *h and $n = 2^h$, as FFT (Algorithm 14) takes them (Precondition);*
- *$f \in \mathbb{R}[x]/(x^n+1)$ with every coefficient in $\mathcal{F}$ (FFT (Algorithm 14), Require).*

Define:

- *in_j and Λ_j, the values of FFT (Algorithm 14), lines 3, 20 and 22;*
- *P, that of FFT (Algorithm 14), line 1;*
- *$c_{\mathrm{merge}} := u + (1+u)((1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1)$ (Lemma G.18);*
- *$k_E := 2\sqrt{2}((3+2u)(1+u)+1)$ (Lemma G.18);*
- *$\widetilde{\mathrm{in}}_j$, the values FFT (Algorithm 14) computes at lines 2 and 21;*
- *$\widetilde{\Lambda}_j : C_{\mathcal{F}}^{n/2} \to C_{\mathcal{F}}^{n/2}$, that of FFT (Algorithm 14), line 19;*
- *$E_j := \|\widetilde{\mathrm{in}}_j - \mathrm{in}_j\|$, $j \le h-1$.*

Then

$$\forall j < h-1:\quad E_{j+1} \le \sqrt{2}(1+c_{\mathrm{merge}})E_j + \sqrt{2}\,c_{\mathrm{merge}}\|\mathrm{in}_j\| + k_E\,\zeta\sqrt{P}.$$

Proof.

DEFINES (j_1, j_2), s and $\widetilde{s}$: a pair of level j, its root and its stored root, those of FFT (Algorithm 14), lines 6 to 19

DEFINES $y_{(j_1,j_2)} := (y_{j_1}, y_{j_2})$, $y \in \mathbb{C}^{n/2}$

Definition A.8, item 1 at every $j < h-1$ and $i < 2^j$	This proof
Shared: $\mathcal{F}, u, \zeta$	
(I1) $\psi, \widetilde{\psi}$ $\psi^{2^{11}} = 1,\ \operatorname{Im}\psi > 0$	$s, \widetilde{s}$ $s = \psi_{2^{j+1}+i}$, $j < h-1$, $i < 2^j$ (the scope); $h \le 10$ (FFT (Algorithm 14), Precondition)
Its conclusion: $\exists\, u_\circ \in \mathbb{C},\ \lvert u_\circ\rvert \le u + \sqrt{2}\,\zeta :\ \widetilde{s} = s(1+u_\circ)$	

Lemma G.18 at every $j < h-1$ and every pair (j_1, j_2) of level j	This proof
Shared: $\mathcal{F}, u, \zeta,\ c_{\text{merge}}, k_E$	
f_0, f_1 $\psi, \widetilde{\psi}$ (a, b) (I2) $(\tilde{a}, \tilde{b})$ $f_0, f_1 \in C_{\mathcal{F}}$ $\psi \in \mathbb{C}$ $\widetilde{\psi} \in C_{\mathcal{F}}$	$(\widetilde{\text{in}}_j)_{j_1}, (\widetilde{\text{in}}_j)_{j_2}$ $s, \widetilde{s}$ $(\Lambda_j \widetilde{\text{in}}_j)_{(j_1,j_2)}$ (FFT (Algorithm 14), line 20) $(\widetilde{\Lambda}_j \widetilde{\text{in}}_j)_{(j_1,j_2)}$ (FFT (Algorithm 14), line 19) $\widetilde{\text{in}}_j$ (the statement); FFT (Algorithm 14), lines 2 and 19 s (the proof's block) $\widetilde{s}$ (the proof's block); FFT (Algorithm 14), Require
Assumption A1 Assumption A2	$s = \psi_{m+i}$ (the proof's block); Fact A.42, item 1 (I1); Definition A.10
Its conclusion: $(\tilde{a}, \tilde{b})\ \mathcal{N}\,(c_{\text{merge}}, k_E\zeta)\ (a, b)$	

(L1) $\forall j < h-1\ \forall (j_1, j_2) :\ \|(\widetilde{\Lambda}_j \widetilde{\text{in}}_j)_{(j_1,j_2)} - (\Lambda_j \widetilde{\text{in}}_j)_{(j_1,j_2)}\| \le c_{\text{merge}} \|(\Lambda_j \widetilde{\text{in}}_j)_{(j_1,j_2)}\| + k_E\,\zeta$

[(I1), (I2)]

(L2) $\forall j < h-1 :\ \|\widetilde{\Lambda}_j \widetilde{\text{in}}_j - \Lambda_j \widetilde{\text{in}}_j\| \le \|(c_{\text{merge}} \|(\Lambda_j \widetilde{\text{in}}_j)_{(j_1,j_2)}\|)_{(j_1,j_2)}\| + \|(k_E\,\zeta)_{(j_1,j_2)}\|$

[(L1); the P pairs of level j: a partition of $\{0, \dots, n/2-1\}$ (FFT (Algorithm 14), lines 1 to 14); Fact A.41, item 3]

(L3) $\forall j < h-1 :\ \|(c_{\text{merge}} \|(\Lambda_j \widetilde{\text{in}}_j)_{(j_1,j_2)}\|)_{(j_1,j_2)}\| = c_{\text{merge}} \|\Lambda_j \widetilde{\text{in}}_j\|$

[$\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead) over the partition]

(L4) $\|(k_E\,\zeta)_{(j_1,j_2)}\| = k_E\,\zeta\sqrt{P}$

[$\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead) over the P pairs]

(L5) $\Rightarrow\ \forall j < h-1 :\ \|\widetilde{\Lambda}_j \widetilde{\text{in}}_j - \Lambda_j \widetilde{\text{in}}_j\| \le c_{\text{merge}} \|\Lambda_j \widetilde{\text{in}}_j\| + k_E\,\zeta\sqrt{P}$

[(L2), (L3), (L4)]

Lemma H.8, item 3 at every $j < h-1$	This proof
Shared: $h, n,\ j,\ \Lambda_j$	
(I3) x, y $x, y \in \mathbb{C}^{n/2}$	$\widetilde{\text{in}}_j, \text{in}_j$ $\widetilde{\text{in}}_j$, in_j (the statement); FFT (Algorithm 14), lines 2 to 22
Its conclusion: $\forall j < h-1\ \forall x, y \in \mathbb{C}^{n/2} :\ \Lambda_j(x-y) = \Lambda_j x - \Lambda_j y$	

Lemma H.8, item 2 at every $j < h-1$	This proof
Shared: $h, n,\ j,\ \Lambda_j$	
(I4) x $x \in \mathbb{C}^{n/2}$	$\widetilde{\mathrm{in}}_j - \mathrm{in}_j$ $\widetilde{\mathrm{in}}_j$, in_j (the statement); FFT (Algorithm 14), lines 2 to 22
Its conclusion: $\forall j < h-1\ \forall x \in \mathbb{C}^{n/2}:\ \|\Lambda_j x\| = \sqrt{2}\,\|x\|$	

(L6) $\forall j < h-1:\ \|\Lambda_j \widetilde{\mathrm{in}}_j - \Lambda_j \mathrm{in}_j\| = \sqrt{2}\,E_j$

[(I3), (I4); E_j (the statement)]

Lemma H.8, item 2 at every $j < h-1$	This proof
Shared: $h, n,\ j,\ \Lambda_j$	
(I5) x $x \in \mathbb{C}^{n/2}$	$\widetilde{\mathrm{in}}_j$ $\widetilde{\mathrm{in}}_j$ (the statement); FFT (Algorithm 14), lines 2 and 19
Its conclusion: $\forall j < h-1\ \forall x \in \mathbb{C}^{n/2}:\ \|\Lambda_j x\| = \sqrt{2}\,\|x\|$	

(L7) $\forall j < h-1:\ \|\Lambda_j \widetilde{\mathrm{in}}_j\| = \sqrt{2}\,\|\widetilde{\mathrm{in}}_j\|$

[(I5)]

(L8) $\forall j < h-1:\ \|\widetilde{\mathrm{in}}_j\| \le \|\mathrm{in}_j\| + E_j$

[$\widetilde{\mathrm{in}}_j = \mathrm{in}_j + (\widetilde{\mathrm{in}}_j - \mathrm{in}_j)$; Fact A.41, item 3; E_j (the statement)]

(L9) $\Rightarrow\ \forall j < h-1:\ \|\Lambda_j \widetilde{\mathrm{in}}_j\| \le \sqrt{2}(\|\mathrm{in}_j\| + E_j)$

[(L7), (L8)]

(L10) $\forall j < h-1:\ E_{j+1} = \|\widetilde{\Lambda}_j \widetilde{\mathrm{in}}_j - \Lambda_j \mathrm{in}_j\|$

[E_{j+1} (the statement); FFT (Algorithm 14), lines 21, 22]

(L11) $\forall j < h-1:\ \widetilde{\Lambda}_j \widetilde{\mathrm{in}}_j - \Lambda_j \mathrm{in}_j = (\widetilde{\Lambda}_j \widetilde{\mathrm{in}}_j - \Lambda_j \widetilde{\mathrm{in}}_j) + (\Lambda_j \widetilde{\mathrm{in}}_j - \Lambda_j \mathrm{in}_j)$

[$x - z = (x - y) + (y - z)$ at $y := \Lambda_j \widetilde{\mathrm{in}}_j$]

(L12) $\Rightarrow\ \forall j < h-1:\ E_{j+1} \le \|\widetilde{\Lambda}_j \widetilde{\mathrm{in}}_j - \Lambda_j \widetilde{\mathrm{in}}_j\| + \|\Lambda_j \widetilde{\mathrm{in}}_j - \Lambda_j \mathrm{in}_j\|$

[(L10), (L11); Fact A.41, item 3]

(L13) $\Rightarrow\ \forall j < h-1:\ E_{j+1} \le c_{\mathrm{merge}} \|\Lambda_j \widetilde{\mathrm{in}}_j\| + k_E\,\zeta\sqrt{P} + \sqrt{2}\,E_j$

[(L12); (L5) on the first norm, (L6) on the second]

(L14) $(1 + u + \sqrt{2}\,\zeta)(1 + \sqrt{2}\,u(2+u)) \ge 1$

[$u, \zeta \ge 0$ (Definition A.4); Fact A.41, item 8]

(L15) $c_{\mathrm{merge}} \ge 0$

[$c_{\mathrm{merge}} = u + (1+u)((1 + u + \sqrt{2}\,\zeta)(1 + \sqrt{2}\,u(2+u)) - 1)$ (Lemma G.18); (L14); $u \ge 0$ (Definition A.4)]

(L16) $\Rightarrow\ \forall j < h-1:\ E_{j+1} \le c_{\mathrm{merge}}\sqrt{2}(\|\mathrm{in}_j\| + E_j) + k_E\,\zeta\sqrt{P} + \sqrt{2}\,E_j$

[(L13), (L9), (L15)]

(L17) $\forall a, b, c \in \mathbb{R}:\ c\sqrt{2}(a+b) + \sqrt{2}\,b = \sqrt{2}(1+c)b + \sqrt{2}\,ca$

[expand]

(L18) $\Rightarrow\ \forall j < h-1:\ E_{j+1} \le \sqrt{2}(1 + c_{\mathrm{merge}})E_j + \sqrt{2}\,c_{\mathrm{merge}}\|\mathrm{in}_j\| + k_E\,\zeta\sqrt{P}$

[(L16); (L17) at $(a, b, c) := (\|\mathrm{in}_j\|, E_j, c_{\mathrm{merge}})$]

(L19) $\Rightarrow$ the statement

[(L18)]

□

Lemma H.10 (The computed FFT's deviation by level [to table])**.** *The per-level growth of Lemma H.9 sums to a closed bound at every level: a relative part in the coefficient norm and an absolute part A_j. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *h and $n = 2^h$, as FFT (Algorithm 14) takes them (Precondition);*
- *$f \in \mathbb{R}[x]/(x^n + 1)$ with every coefficient in $\mathcal{F}$ (FFT (Algorithm 14), Require).*

Define:

- *The signer's words and parameters*
  - P, *that of* FFT *(Algorithm 14), line 1;*
- *The coefficient norm*
  - $\|f\| := (\sum_{i<n} f_{[i]}^2)^{1/2}$ *(Definition A.1 at* $m := n$*);*
- *The center shifts*
  - $c_{\text{merge}} := u + (1+u)((1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1)$ *(Lemma G.18);*
  - $k_E := 2\sqrt{2}((3+2u)(1+u)+1)$ *(Lemma G.18);*
  - $A_0 := 0$*;*
  - $A_{j+1} := \sqrt{2}(1+c_{\text{merge}})A_j + k_E\,\zeta\sqrt{P}$*,* $j < h-1$*;*
- *The images*
  - in_j*, the values of* FFT *(Algorithm 14), lines 3, 20 and 22;*
  - $\widetilde{\text{in}}_j$*, the values* FFT *(Algorithm 14) computes at lines 2 and 21 (Lemma H.9);*
  - $E_j := \|\widetilde{\text{in}}_j - \text{in}_j\|$*,* $j \le h-1$ *(Lemma H.9).*

Then

$$\forall j \le h-1: \quad E_j \le 2^{j/2}\|f\|\left((1+c_{\text{merge}})^j - 1\right) + A_j.$$

Proof.

DEFINES $B_j := 2^{j/2}\|f\|((1+c_{\text{merge}})^j - 1) + A_j$, $j \le h-1$

(L1) $\widetilde{\text{in}}_0 = \text{in}_0$

[FFT (Algorithm 14), lines 2, 3: $f_{[p]} \in \mathcal{F}$ (the statement)]

(L2) $\Rightarrow$ $E_0 = 0$

[(L1); E_0 (the statement)]

(L3) $B_0 = 0$

[$A_0 = 0$ (the statement); B_0 (the proof's block)]

(L4) $\Rightarrow$ $E_0 \le B_0$

[(L2), (L3)]

(L5) $\forall j < h-1:\ E_{j+1} \le \sqrt{2}(1+c_{\text{merge}})E_j + \sqrt{2}\,c_{\text{merge}}\|\text{in}_j\| + k_E\,\zeta\sqrt{P}$

[Lemma H.9]

(L6) $\forall j \le h-1:\ \|\text{in}_j\| = 2^{j/2}\|f\|$

[Lemma H.8, item 4]

(L7) $1 + c_{\text{merge}} \ge 0$

[Lemma H.9's c_{merge}, that of Lemma G.18, at $u, \zeta \ge 0$ (Definition A.4)]

(L8) $\Rightarrow$ $\forall j < h-1:\ [E_j \le B_j] \Rightarrow\ E_{j+1} \le \sqrt{2}(1+c_{\text{merge}})B_j + \sqrt{2}\,c_{\text{merge}}\,2^{j/2}\|f\| + k_E\,\zeta\sqrt{P}$

[(L5), (L6), (L7)]

(L9) $\forall j:\ \sqrt{2}\,2^{j/2} = 2^{(j+1)/2}$

[expand]

(L10) $\forall c \in \mathbb{R}\ \forall j:\ (1+c)((1+c)^j - 1) + c = (1+c)^{j+1} - 1$

[expand]

(L11) $\forall j:\ \sqrt{2}(1+c_{\text{merge}})\,2^{j/2}\|f\|((1+c_{\text{merge}})^j - 1) + \sqrt{2}\,c_{\text{merge}}\,2^{j/2}\|f\| = 2^{(j+1)/2}\|f\|((1+c_{\text{merge}})^{j+1} - 1)$

[(L9); (L10) at $c := c_{\text{merge}}$]

(L12) $\forall j < h-1:\ \sqrt{2}(1+c_{\text{merge}})A_j + k_E\,\zeta\sqrt{P} = A_{j+1}$

[A_{j+1} (the statement)]

(L13) $\Rightarrow$ $\forall j < h-1:\ [E_j \le B_j] \Rightarrow\ E_{j+1} \le B_{j+1}$

[(L8), (L11), (L12); B_j (the proof's block)]

(L14) $\Rightarrow$ $\forall j \le h-1:\ E_j \le 2^{j/2}\|f\|((1+c_{\text{merge}})^j - 1) + A_j$

[induction on j: base (L4), step (L13); B_j (the proof's block)]

(L15) $\Rightarrow$ the statement

[(L14)]

□

Lemma H.11 (The computed FFT image's deviation [to table])**.** *The computed FFT of a polynomial with coefficients in $\mathcal{F}$ deviates from the exact image by a relative part in the image's norm and an absolute part. Let:*

- *$\mathcal{F}$ be a realization at (u, ζ) (Definition A.4);*
- *h and $n = 2^h$, as FFT (Algorithm 14) takes them (Precondition);*
- *$f \in \mathbb{R}[x]/(x^n + 1)$ with every coefficient in $\mathcal{F}$ (FFT (Algorithm 14), Require).*

Define:

- *$\hat{f}$, that of FFT (Algorithm 14), line 26;*
- *$\widetilde{\hat{f}} := \widetilde{\mathrm{FFT}}(f)$, the value FFT (Algorithm 14) computes at line 25;*
- *$c_{\mathrm{merge}} := u + (1+u)((1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1)$ (Lemma G.18);*
- *$k_E := 2\sqrt{2}((3+2u)(1+u)+1)$ (Lemma G.18);*
- *P, that of FFT (Algorithm 14), line 1;*
- *$R_{h-1} := (1 + c_{\mathrm{merge}})^{h-1} - 1$;*
- *$A_0 := 0$;*
- *$A_{j+1} := \sqrt{2}(1 + c_{\mathrm{merge}})A_j + k_E\,\zeta\sqrt{P}$, $j < h - 1$.*

Then

$$\|\widetilde{\hat{f}} - \hat{f}\| \le R_{h-1}\|\hat{f}\| + A_{h-1}.$$

Proof.

COMPUTES $\widetilde{\mathrm{in}}_j$: FFT (Algorithm 14), lines 2, 21
DEFINES in_j: FFT (Algorithm 14), lines 3, 22
DEFINES $E_j := \|\widetilde{\mathrm{in}}_j - \mathrm{in}_j\|$

(L1) $\widetilde{\hat{f}} = \widetilde{\mathrm{in}}_{h-1}$

[FFT (Algorithm 14), line 25]

(L2) $\hat{f} = \mathrm{in}_{h-1}$

[FFT (Algorithm 14), line 26]

(L3) $\Rightarrow$ $\|\widetilde{\hat{f}} - \hat{f}\| = E_{h-1}$

[(L1), (L2); E_j (the proof's block)]

(I1)

Lemma H.10	This proof
Shared: $\mathcal{F}, u, \zeta,\ h, n,\ f,\ \|f\|$ (Definition A.1), $\mathrm{in}_j, \widetilde{\mathrm{in}}_j, E_j,\ P, c_{\mathrm{merge}}, k_E, A_j$	
j	$h - 1$
Its conclusion: $\forall j \le h-1:\ E_j \le 2^{j/2}\|f\|\left((1+c_{\mathrm{merge}})^j - 1\right) + A_j$	

(L4) $E_{h-1} \le 2^{(h-1)/2}\|f\|((1 + c_{\mathrm{merge}})^{h-1} - 1) + A_{h-1}$

[(I1)]

(I2)

Lemma H.8	This proof
Shared: $h, n,\ f,\ \|f\|$ (Definition A.1), $\mathrm{in}_j, \hat{f}$	
j	$h - 1$
Its item 4: $\forall f \in \mathbb{R}[x]/(x^n+1)\ \forall j \le h-1:\ \|\mathrm{in}_j\| = 2^{j/2}\|f\|$	
Its item 5: $\forall f \in \mathbb{R}[x]/(x^n+1):\ \|\hat{f}\| = \sqrt{n/2}\,\|f\|$	

(L5) $2^{(h-1)/2}\|f\| = \|\hat{f}\|$

[items 4 and 5 of (I2); $n = 2^h$ (the statement)]

(L6) $\Rightarrow$ $\|\widetilde{\hat{f}} - \hat{f}\| \le R_{h-1}\|\hat{f}\| + A_{h-1}$

[(L3), (L4), (L5); R_{h-1} (the statement)]

(L7) $\Rightarrow$ the statement

[(L6)]

□

Lemma H.12 (A computed FFT entry's deviation [to table])**.** *Every entry of the computed FFT image deviates from the exact entry by at most the image's bound of Lemma H.11. Let:*

- $\mathcal{F}$ *be a realization at* (u, ζ) *(Definition A.4);*
- h *and* $n = 2^h$*, as* FFT *(Algorithm 14) takes them (Precondition);*
- $f \in \mathbb{R}[x]/(x^n + 1)$ *with every coefficient in* $\mathcal{F}$ *(*FFT *(Algorithm 14), Require).*

Define:

- $\hat{f}$ *and* $\widetilde{\hat{f}}$*, the exact and the computed outputs of* FFT *(Algorithm 14), lines 26 and 25;*
- $P := n/4$*, that of* FFT *(Algorithm 14), line 1;*
- $c_{\text{merge}} := u + (1+u)((1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1)$ *(Lemma G.18);*
- $k_E := 2\sqrt{2}((3+2u)(1+u)+1)$ *(Lemma G.18);*
- $R_{h-1} := (1 + c_{\text{merge}})^{h-1} - 1$*;*
- $A_0 := 0$*;*
- $A_{j+1} := \sqrt{2}(1 + c_{\text{merge}})A_j + k_E\zeta\sqrt{P}$*,* $j < h - 1$*.*

Then

$$\forall k < n/2 : \quad |\widetilde{\hat{f}}_k - \hat{f}_k| \le R_{h-1}\|\hat{f}\| + A_{h-1}.$$

Proof. (L1) $\forall k < n/2 : |\widetilde{\hat{f}}_k - \hat{f}_k| \le \|\widetilde{\hat{f}} - \hat{f}\|$

[Fact A.41, item 3: $|X_i| \le \|X\|$]

(L2) $\|\widetilde{\hat{f}} - \hat{f}\| \le R_{h-1}\|\hat{f}\| + A_{h-1}$

[Lemma H.11]

(L3) $\Rightarrow \forall k < n/2 : |\widetilde{\hat{f}}_k - \hat{f}_k| \le R_{h-1}\|\hat{f}\| + A_{h-1}$

[(L1), (L2)]

(L4) $\Rightarrow$ the statement

[(L3)]

□

H.2.3 The checked key and its floors

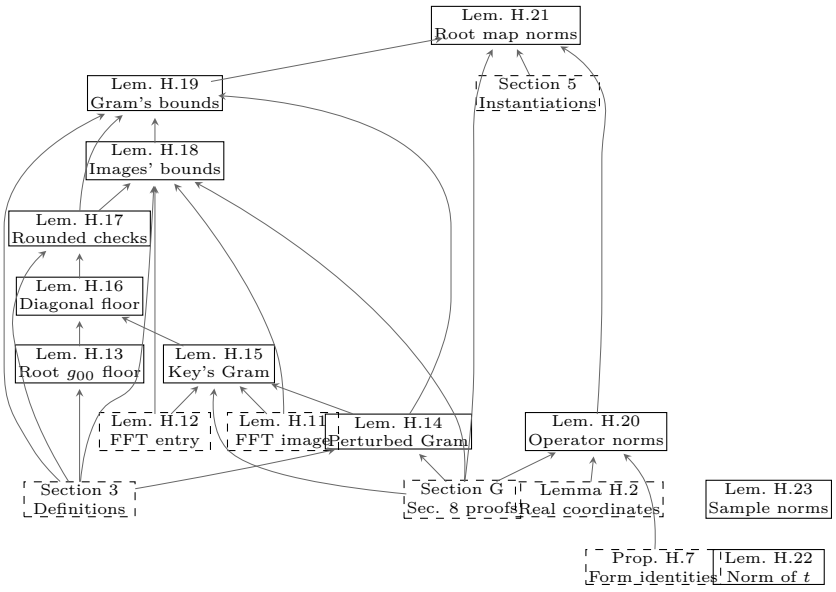


Figure 65: Dependencies, Section H.2.3.

Lemma H.13 (The floor of the root's first diagonal [to table])**.** *The NTRU equation and the small coefficients of F and G bound the root's first Gram diagonal from below at every root. Let:*

- *(f, g, F, G) be a key (line 3 of* keygen *(Algorithm 11)) of degree $n = 2^h$;*
- *ψ be a root of $x^n + 1$.*

Define:

- *$g_{00} := |f(\psi)|^2 + |g(\psi)|^2$ and $g_{11} := |F(\psi)|^2 + |G(\psi)|^2$ (Fact A.33);*
- *$g_{01} := g(\psi)\,\mathrm{conj}\,G(\psi) + f(\psi)\,\mathrm{conj}\,F(\psi)$ (Fact A.33).*

Assume:

(A1) $\forall a < n:\ F_{[a]}, G_{[a]} \in [-127, 127]$ *[L0: kgen_nstru.c:1887-1895].*

Then

$$g_{00} \geq q^2/(2(127n)^2).$$

Proof.

(L1) $g_{00}g_{11} - |g_{01}|^2 = q^2$
[Fact A.33, item 2]

(L2) $\forall p \in \{F, G\}:\ |p(\psi)| \leq \sum_{a<n}|p_{[a]}|$
[Fact A.42, item 3]

(L3) $\forall p \in \{F, G\}:\ \sum_{a<n}|p_{[a]}| \leq 127n$
[assumption A1]

(L4) $g_{11} = |F(\psi)|^2 + |G(\psi)|^2$
[g_{11} (Fact A.33)]

(L5) $\Rightarrow$ $g_{11} \leq 2(127n)^2$
[(L2), (L3), (L4); Fact A.41, item 5: $t \mapsto t^2$ nondecreasing on $[0, \infty)$]

(L6) $g_{11} \geq 0$
[(L4)]

(L7) $|g_{01}|^2 \geq 0$
[Fact A.41, item 13: $t^{2j} \geq 0$ at $(t, j) := (|g_{01}|, 1)$]

(L8) $g_{00}g_{11} \geq q^2$
[(L1), (L7)]

(L9) $q^2 > 0$
[$q = 12289$ (the statement)]

(L10) $\Rightarrow$ $g_{11} > 0$
[(L6), (L8), (L9)]

(L11) $\Rightarrow$ $g_{00} \geq q^2/g_{11}$
[(L8), (L10)]

(L12) $q^2/g_{11} \geq q^2/(2(127n)^2)$
[(L5), (L10); Fact A.41, item 5: $t \mapsto 1/t$ nonincreasing on $(0, \infty)$]

(L13) $\Rightarrow$ $g_{00} \geq q^2/(2(127n)^2)$
[(L11), (L12)]

(L14) $\Rightarrow$ the statement
[(L13)]

□

Lemma H.14 (A Gram matrix from perturbed images [to table])**.** *On the images of a key, a computed Gram is within the rounding of* Gram *plus the images' perturbation of the exact Gram.*

Define:

- *$\Psi_n := \{\psi_k : k < n/2\}$, that of Fact A.43 at $m := n$.*

Let:

- *$\psi \in \Psi_n$;*
- *$\gamma_{fg}, \gamma_{FG}, \delta_{fg}, \delta_{FG} \in \mathbb{R}$;*
- *$\widetilde{f}, \widetilde{g}, \widetilde{F}, \widetilde{G} \in \mathbb{C}$, with real and imaginary parts in $2^{-64}\mathbb{Z}$.*

Define:

- $\zeta := 2^{-64}$;
- $\hat{f} := f(\psi)$, $\hat{g} := g(\psi)$, $\hat{F} := F(\psi)$, $\hat{G} := G(\psi)$;
- $\Gamma := \{(f, \gamma_{fg}, \delta_{fg}), (g, \gamma_{fg}, \delta_{fg}), (F, \gamma_{FG}, \delta_{FG}), (G, \gamma_{FG}, \delta_{FG})\}$;
- $g_{00} := |f(\psi)|^2 + |g(\psi)|^2$ *and* $g_{11} := |F(\psi)|^2 + |G(\psi)|^2$ *(Fact A.33);*
- $g_{01} := g(\psi)\operatorname{conj} G(\psi) + f(\psi)\operatorname{conj} F(\psi)$ *(Fact A.33);*
- $\mathcal{F}_{\text{fx}} := 2^{-64}\mathbb{Z}$ *(Definition A.4, item 8, at the precision* 64*);*
- $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$*, the Gram* Gram *(Algorithm 13) computes in* $\mathcal{F}_{\text{fx}}$ *from* $\begin{pmatrix} \widetilde{\hat{g}} & -\widetilde{\hat{f}} \\ \widetilde{\hat{G}} & -\widetilde{\hat{F}} \end{pmatrix}$;
- $k_H := 7$ *(Lemma G.22 at* $u = 0$*) and* $k'_H := 7\sqrt{2}$ *(Lemma G.23 at* $u = 0$*).*

Assume:

(A1) $\forall (p, \gamma, \delta) \in \Gamma : \ |\hat{p}| \le \gamma$;

(A2) $\forall (p, \gamma, \delta) \in \Gamma : \ |\widetilde{\hat{p}} - \hat{p}| \le \delta$.

Then the computed Gram is within the three bounds:

1. $|\widetilde{g}_{00} - g_{00}| \le k_H\zeta + 4\gamma_{fg}\delta_{fg} + 2\delta_{fg}^2$;
2. $|\widetilde{g}_{11} - g_{11}| \le k_H\zeta + 4\gamma_{FG}\delta_{FG} + 2\delta_{FG}^2$;
3. $|\widetilde{g}_{01} - g_{01}| \le k'_H\zeta + 2(\gamma_{fg}\delta_{FG} + \gamma_{FG}\delta_{fg} + \delta_{fg}\delta_{FG})$.

Proof. (L1) $\forall x, e \in \mathbb{C} : \ |x + e|^2 - |x|^2 = 2\operatorname{Re}(\operatorname{conj} xe) + |e|^2$

[expand $(x + e)\operatorname{conj}(x + e)$; Fact A.41, item 1: $w \operatorname{conj} w = |w|^2$, $w + \operatorname{conj} w = 2\operatorname{Re} w$]

(L2) $\forall x, e \in \mathbb{C} : \ |2\operatorname{Re}(\operatorname{conj} xe)| \le 2|x||e|$

[Fact A.41, item 1: $|\operatorname{Re} w| \le |w|$, $|xy| = |x||y|$, $|\operatorname{conj} x| = |x|$]

(L3) $\Rightarrow \ \forall (p, \gamma, \delta) \in \Gamma : \ \big||\widetilde{\hat{p}}|^2 - |\hat{p}|^2\big| \le 2\gamma\delta + \delta^2$

[(L1), (L2) at $(x, e) := (\hat{p}, \widetilde{\hat{p}} - \hat{p})$; assumptions A1, A2]

(I1)

Lemma G.22	This proof
Shared: ζ, $\widetilde{g}_{00}, \widetilde{g}_{11}$, k_H	
$\mathcal{F}$	$2^{-64}\mathbb{Z}$
u	0
$b_{00}, b_{01}, b_{10}, b_{11}$	$\widetilde{\hat{g}}, -\widetilde{\hat{f}}, \widetilde{\hat{G}}, -\widetilde{\hat{F}}$
g_{00}, g_{11}	$\lvert\widetilde{\hat{f}}\rvert^2 + \lvert\widetilde{\hat{g}}\rvert^2, \lvert\widetilde{\hat{F}}\rvert^2 + \lvert\widetilde{\hat{G}}\rvert^2$
$\mathcal{F}$ realization at (u, ζ)	$2^{-64}\mathbb{Z}$ at $(0, 2^{-64})$ (Definition A.4, item 8)
$b_{00}, b_{01}, b_{10}, b_{11} \in C_{\mathcal{F}}$	The statement
Assumption A1	Definition A.4, item 8
Its item 1: $\tilde{g}_{00}\ \mathcal{I}\left(((1+u)^3 - 1)^{\pm}, k_H\zeta^{\pm}\right)\ g_{00}$	
Its item 2: $\tilde{g}_{11}\ \mathcal{I}\left(((1+u)^3 - 1)^{\pm}, k_H\zeta^{\pm}\right)\ g_{11}$	

(L4) $|\widetilde{g}_{00} - (|\widetilde{\hat{f}}|^2 + |\widetilde{\hat{g}}|^2)| \le k_H\zeta$

[item 1 of (I1); k_H (the statement)]

(L5) $g_{00} = |\hat{f}|^2 + |\hat{g}|^2$

[g_{00} (Fact A.33)]

(L6) $\Rightarrow \ |\widetilde{g}_{00} - g_{00}| \le k_H\zeta + 4\gamma_{fg}\delta_{fg} + 2\delta_{fg}^2$

[(L3) at $p := f$ and at $p := g$; (L4), (L5); Fact A.41, item 1: $|x + y| \le |x| + |y|$]

(L7) $\Rightarrow$ item 1

[(L6)]

(L8) $|\widetilde{g}_{11} - (|\widetilde{\hat{F}}|^2 + |\widetilde{\hat{G}}|^2)| \le k_H\zeta$

[item 2 of (I1); k_H (the statement)]

(L9) $g_{11} = |\hat{F}|^2 + |\hat{G}|^2$

[g_{11} (Fact A.33)]

(L10) $\Rightarrow$ $|\widetilde{g}_{11} - g_{11}| \le k_H\zeta + 4\gamma_{FG}\delta_{FG} + 2\delta_{FG}^2$

[(L3) at $p := F$ and at $p := G$; (L8), (L9); Fact A.41, item 1: $|x+y| \le |x| + |y|$]

(L11) $\Rightarrow$ item 2

[(L10)]

(L12) $\forall x, y, \widetilde{x}, \widetilde{y} \in \mathbb{C}:\ \widetilde{x}\operatorname{conj}\widetilde{y} - x\operatorname{conj} y = x\operatorname{conj}(\widetilde{y} - y) + (\widetilde{x} - x)\operatorname{conj} y + (\widetilde{x} - x)\operatorname{conj}(\widetilde{y} - y)$

[expand]

(L13) $\Rightarrow$ $\forall x, y, \widetilde{x}, \widetilde{y} \in \mathbb{C}:\ |\widetilde{x}\operatorname{conj}\widetilde{y} - x\operatorname{conj} y| \le |x||\widetilde{y} - y| + |y||\widetilde{x} - x| + |\widetilde{x} - x||\widetilde{y} - y|$

[(L12); Fact A.41, item 1: $|x+y| \le |x| + |y|$, $|xy| = |x||y|$, $|\operatorname{conj} x| = |x|$]

(I2)

Lemma G.23	This proof
Shared: ζ, $\widetilde{g}_{01}$, k'_H	
$\mathcal{F}$	$2^{-64}\mathbb{Z}$
u	0
$b_{00}, b_{01}, b_{10}, b_{11}$	$\widetilde{\hat{g}}, -\widetilde{\hat{f}}, \widetilde{\hat{G}}, -\widetilde{\hat{F}}$
g_{00}, g_{11}	$\lvert\widetilde{\hat{f}}\rvert^2 + \lvert\widetilde{\hat{g}}\rvert^2, \lvert\widetilde{\hat{F}}\rvert^2 + \lvert\widetilde{\hat{G}}\rvert^2$
g_{01}	$\widetilde{\hat{g}}\operatorname{conj}\widetilde{\hat{G}} + \widetilde{\hat{f}}\operatorname{conj}\widetilde{\hat{F}}$
$\mathcal{F}$ realization at (u, ζ)	$2^{-64}\mathbb{Z}$ at $(0, 2^{-64})$ (Definition A.4, item 8)
$b_{00}, b_{01}, b_{10}, b_{11} \in C_{\mathcal{F}}$	The statement
Its conclusion: $\tilde{g}_{01}\ \mathcal{N}\left(u, (1+u)\sqrt{2}u(2+u)\sqrt{g_{00}g_{11}} + k'_H\zeta\right)\ g_{01}$	

(L14) $|\widetilde{g}_{01} - (\widetilde{\hat{g}}\operatorname{conj}\widetilde{\hat{G}} + \widetilde{\hat{f}}\operatorname{conj}\widetilde{\hat{F}})| \le k'_H\zeta$

[(I2); k'_H (the statement)]

(L15) $g_{01} = \hat{g}\operatorname{conj}\hat{G} + \hat{f}\operatorname{conj}\hat{F}$

[g_{01} (Fact A.33)]

(L16) $\Rightarrow$ $|\widetilde{g}_{01} - g_{01}| \le k'_H\zeta + 2(\gamma_{fg}\delta_{FG} + \gamma_{FG}\delta_{fg} + \delta_{fg}\delta_{FG})$

[(L13) at $(x, y) := (\hat{g}, \hat{G})$ and at $(\hat{f}, \hat{F})$; assumptions A1, A2; (L14), (L15); Fact A.41, item 1: $|x+y| \le |x| + |y|$]

(L17) $\Rightarrow$ item 3

[(L16)]

□ (items 1, 2 and 3)

Lemma H.15 (The Gram's perturbation from the key alone [to table])**.** *The coefficient ranges of the key bound the exact images, and the FFT's bound then bounds the Gram the fixed-point code computes against the exact Gram. Define:*

- $\Psi_n := \{\psi_k : k < n/2\}$*, that of Fact A.43 at* $m := n$*.*

Let:

- (f, g, F, G) *be a key (line 3 of* keygen *(Algorithm 11)) of degree* $n = 2^h$*;*
- $B_{fg} \in \mathbb{R}$*;*
- $\psi \in \Psi_n$*.*

Define:

- *The signer's words and parameters*
  - $\zeta := 2^{-64}$*;*
  - $\mathcal{F}_{\text{fx}} := 2^{-64}\mathbb{Z}$ *(Definition A.4, item 8, at the precision* 64*);*
- *The Gram deltas*
  - $R_{h-1} := (1 + \sqrt{2}\,\zeta)^{h-1} - 1$ *(Lemma H.11 at* $(0, \zeta)$*);*
  - $A_0 := 0$ *and* $A_{j+1} := \sqrt{2}(1 + \sqrt{2}\,\zeta)A_j + 4\sqrt{2}\,\zeta\sqrt{n}$ *for* $j < h - 1$ *(Lemma H.11 at* $(0, \zeta)$*);*
  - $\gamma^*_{fg} := B_{fg}n$*;*
  - $\gamma^*_{FG} := 127n$*;*
  - $\delta^*_{fg} := R_{h-1}\gamma^*_{fg}\sqrt{n/2} + A_{h-1}$*;*

13005 – $\delta^*_{FG} := R_{h-1}\gamma^*_{FG}\sqrt{n/2} + A_{h-1}$;
13006 – $E^*_{00} := 7\zeta + 4\gamma^*_{fg}\delta^*_{fg} + 2\delta^{*2}_{fg}$;
13007 – $E^*_{11} := 7\zeta + 4\gamma^*_{FG}\delta^*_{FG} + 2\delta^{*2}_{FG}$;
13008 – $E^*_{01} := 7\sqrt{2}\,\zeta + 2(\gamma^*_{fg}\delta^*_{FG} + \gamma^*_{FG}\delta^*_{fg} + \delta^*_{fg}\delta^*_{FG})$;
13009 • *The Gram matrix entries*
13010 – $g_{00} := |f(\psi)|^2 + |g(\psi)|^2$ *and* $g_{11} := |F(\psi)|^2 + |G(\psi)|^2$ *(Fact A.33);*
13011 – $g_{01} := g(\psi)\operatorname{conj} G(\psi) + f(\psi)\operatorname{conj} F(\psi)$ *(Fact A.33);*
13012 – $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$, *the Gram* Gram *(Algorithm 13) computes in* $\mathcal{F}_{\mathrm{fx}}$ *on the images* $\widetilde{\mathrm{FFT}}$
13013 *(Algorithm 14) writes.*
13014 *Assume:*
13015 *(A1)* $\forall a < n:\ f_{[a]}, g_{[a]} \in [-B_{fg}, B_{fg}]$ *[L0: fxp/sign_fxcore.c:128-141];*
13016 *(A2)* $\forall a < n:\ F_{[a]}, G_{[a]} \in [-127, 127]$ *[L0: kgen_nstru.c:1887-1895].*
13017 *Then the computed Gram is within the three bounds:*

13018 1. $|\widetilde{g}_{00} - g_{00}| \le E^*_{00}$;
13019 2. $|\widetilde{g}_{11} - g_{11}| \le E^*_{11}$;
13020 3. $|\widetilde{g}_{01} - g_{01}| \le E^*_{01}$.

13021 *Proof.*
DEFINES $\Gamma := \{(f, \gamma^*_{fg}, \delta^*_{fg}), (g, \gamma^*_{fg}, \delta^*_{fg}), (F, \gamma^*_{FG}, \delta^*_{FG}), (G, \gamma^*_{FG}, \delta^*_{FG})\}$
13022 COMPUTES $\widetilde{\hat{p}}$, $p \in \{f, g, F, G\}$: $\widetilde{\mathrm{FFT}}$ (Algorithm 14) at $(0, \zeta)$, the images Gram (Algorithm 13) reads

13023 (L1) $\forall(p, \gamma, \delta) \in \Gamma\ \forall\psi:\ |\hat{p}(\psi)| \le \sum_{a<n}|p_{[a]}|$
13024 [Fact A.42, item 3]
13025 (L2) $\forall(p, \gamma, \delta) \in \Gamma:\ \sum_{a<n}|p_{[a]}| \le \gamma$
13026 [assumptions A1, A2; γ^*_{fg}, γ^*_{FG} (the statement)]
13027 (L3) $\Rightarrow\ \forall(p, \gamma, \delta) \in \Gamma\ \forall\psi:\ |\hat{p}(\psi)| \le \gamma$
13028 [(L1), (L2)]
13029 (L4) $\Rightarrow\ \forall(p, \gamma, \delta) \in \Gamma:\ \|\hat{p}\| \le \gamma\sqrt{n/2}$
13030 [(L3); $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead) over the $n/2$ roots]
13031 (L5) $\forall(p, \gamma, \delta) \in \Gamma\ \forall a < n:\ p_{[a]} \in 2^{-64}\mathbb{Z}$
13032 [$f, g, F, G \in \mathbb{Z}[x]/(x^n + 1)$ (keygen (Algorithm 11), line 3); $\mathbb{Z} \subseteq 2^{-64}\mathbb{Z}$]

Lemma H.12 at every $(p, \gamma, \delta) \in \Gamma$	This proof
Shared: $\zeta,\ h, n,\ k,\ R_{h-1}, A_{h-1}$	
$\mathcal{F}$	$2^{-64}\mathbb{Z}$
u	0
f	p
(I1) $\hat{f}_k, \widetilde{\hat{f}}_k$	$\hat{p}(\psi), \widetilde{\hat{p}}(\psi)$ (FFT (Algorithm 14), Post)
$\mathcal{F}$ realization at (u, ζ)	$2^{-64}\mathbb{Z}$ at $(0, 2^{-64})$ (Definition A.4, item 8)
$h \in \{1, \ldots, 10\}$	$n \in \{512, 1024\}$ (keygen (Algorithm 11), Require)
$f_{[a]} \in \mathcal{F},\ a < n$	(L5)
$k < n/2$	k (the statement)
Its conclusion: $\forall k < n/2:\ \lvert\widetilde{\hat{f}}_k - \hat{f}_k\rvert \le R_{h-1}\lVert\hat{f}\rVert + A_{h-1}$	

13033

13034 (L6) $\forall(p, \gamma, \delta) \in \Gamma\ \forall\psi:\ |\widetilde{\hat{p}}(\psi) - \hat{p}(\psi)| \le R_{h-1}\|\hat{p}\| + A_{h-1}$
13035 [(I1)]
13036 (L7) $\Rightarrow\ \forall(p, \gamma, \delta) \in \Gamma\ \forall\psi:\ |\widetilde{\hat{p}}(\psi) - \hat{p}(\psi)| \le \delta$
13037 [(L4), (L6); $R_{h-1} \ge 0$ (Lemma H.11); δ^*_{fg}, δ^*_{FG} (the statement)]
13038 (L8) $k_H = 7$ at $u = 0$
13039 [$k_H = 4(1+u)^2 + 2(1+u) + 1$ (Lemma G.22) at $u = 0$; assumption A1 by Definition A.4, item 8]

(L9) $k'_H = 7\sqrt{2}$ at $u = 0$

[$k'_H = \sqrt{2}(2(3+2u)(1+u)+1)$ (Lemma G.23) at $u = 0$]

Lemma H.14 at $(\gamma_{fg}, \gamma_{FG}, \delta_{fg}, \delta_{FG}) :=$ $(\gamma^*_{fg}, \gamma^*_{FG}, \delta^*_{fg}, \delta^*_{FG})$ and the images $\widetilde{\text{FFT}}$ writes	This proof
Shared: $\zeta,\ \psi,\ (g_{00}, g_{01}, g_{11}),\ (\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11}),\ \widetilde{f}, \widetilde{g}, \widetilde{F}, \widetilde{G},\ k_H, k'_H$	
$\gamma_{fg}, \gamma_{FG}, \delta_{fg}, \delta_{FG}$	$\gamma^*_{fg}, \gamma^*_{FG}, \delta^*_{fg}, \delta^*_{FG}$ (the scope)
(I2) $\gamma_{fg}, \gamma_{FG}, \delta_{fg}, \delta_{FG} \in \mathbb{R}$	$\gamma^*_{fg}, \gamma^*_{FG}, \delta^*_{fg}, \delta^*_{FG}$ (the statement)
Assumption A1	(L3)
Assumption A2	(L7)
Its item 1: $\lvert\widetilde{g}_{00} - g_{00}\rvert \le k_H\zeta + 4\gamma_{fg}\delta_{fg} + 2\delta^2_{fg}$	
Its item 2: $\lvert\widetilde{g}_{11} - g_{11}\rvert \le k_H\zeta + 4\gamma_{FG}\delta_{FG} + 2\delta^2_{FG}$	
Its item 3: $\lvert\widetilde{g}_{01} - g_{01}\rvert \le k'_H\zeta + 2(\gamma_{fg}\delta_{FG} + \gamma_{FG}\delta_{fg} + \delta_{fg}\delta_{FG})$	

(L10) $\forall\psi:\ \lvert\widetilde{g}_{00} - g_{00}\rvert \le E^*_{00}$

[item 1 of (I2); (L8); E^*_{00} (the statement)]

(L11) $\Rightarrow$ item 1

[(L10)]

(L12) $\forall\psi:\ \lvert\widetilde{g}_{11} - g_{11}\rvert \le E^*_{11}$

[item 2 of (I2); (L8); E^*_{11} (the statement)]

(L13) $\Rightarrow$ item 2

[(L12)]

(L14) $\forall\psi:\ \lvert\widetilde{g}_{01} - g_{01}\rvert \le E^*_{01}$

[item 3 of (I2); (L9); E^*_{01} (the statement)]

(L15) $\Rightarrow$ item 3

[(L14)]

□ (items 1, 2 and 3)

Lemma H.16 (The floor of the computed first diagonal [to table])**.** *At both degrees, the floor of Lemma H.13 less the perturbation of Lemma H.15 keeps the computed first diagonal above* 2^{-8} *and above that perturbation. Define:*

- $\Psi_n := \{\psi_k : k < n/2\}$*, that of Fact A.43 at* $m := n$*.*

Let:

- (f, g, F, G) *be a key (line 3 of* keygen *(Algorithm 11)) of degree* $n = 2^h$*;*
- $\psi \in \Psi_n$*.*

Define:

- $\zeta := 2^{-64}$ *(Lemma H.15);*
- $\mathcal{F}_{\text{fx}} := 2^{-64}\mathbb{Z}$ *(Definition A.4, item 8, at the precision* 64*);*
- $\widetilde{g}_{00}$*, the first diagonal* Gram *(Algorithm 13) computes in* $\mathcal{F}_{\text{fx}}$ *on the images* $\widetilde{\text{FFT}}$ *(Algorithm 14) writes;*
- $B_{fg} := \begin{cases} 31 & n = 512 \\ 15 & n = 1024 \end{cases}$ *[LO: kgen_gauss.c:14-16];*
- $R_{h-1} := (1 + \sqrt{2}\,\zeta)^{h-1} - 1$ *(Lemma H.11 at* $(0, \zeta)$*);*
- $A_0 := 0$ *and* $A_{j+1} := \sqrt{2}(1 + \sqrt{2}\,\zeta)A_j + 4\sqrt{2}\,\zeta\sqrt{n}$ *for* $j < h - 1$ *(Lemma H.11 at* $(0, \zeta)$*);*
- $\gamma^*_{fg} := B_{fg}n$ *(Lemma H.15 at* B_{fg}*);*
- $\delta^*_{fg} := R_{h-1}\gamma^*_{fg}\sqrt{n/2} + A_{h-1}$ *(Lemma H.15);*
- $E^*_{00} := 7\zeta + 4\gamma^*_{fg}\delta^*_{fg} + 2\delta^{*2}_{fg}$ *(Lemma H.15).*

Assume:

(A1) $\forall a < n:\ f_{[a]}, g_{[a]} \in [-B_{fg}, B_{fg}]$ *[LO: fxp/sign_fxcore.c:128-141];*

(A2) $\forall a < n:\ F_{[a]}, G_{[a]} \in [-127, 127]$ *[L0: kg en_n tr u. c: 1887-1895].*
Measured [gate: ve ri fy /g at es /f x/ gr am_f lo or .p y]:

- $q^2/(2(127n)^2) - E^*_{00} > 2^{-8}$ *at* $n = 512$ *and at* $n = 1024$*;*
- $E^*_{00} \le 2^{-24}$ *at* $n = 512$ *and at* $n = 1024$.

Then the computed first diagonal exceeds 2^{-8} *and* E^*_{00}*:*

1. $\widetilde{g}_{00} > 2^{-8}$*;*
2. $E^*_{00} < \widetilde{g}_{00}$.

Proof. Proof of item 1.

	Lemma H.15, item 1	This proof
	Shared: $(f, g, F, G), n,\ \psi, k,\ B_{fg},\ g_{00}$ (Fact A.33), $\widetilde{g}_{00},\ E^*_{00}$	
(I1)	Shared: assumptions A1, A2	
	$B_{fg} \in \mathbb{R}$	B_{fg} (the statement)
	Its conclusion: $\lvert\widetilde{g}_{00} - g_{00}\rvert \le E^*_{00}$	

(L1) $\widetilde{g}_{00} \ge g_{00} - E^*_{00}$ [(I1)]

(L2) $g_{00} \ge q^2/(2(127n)^2)$ [Lemma H.13; its range of F and G (assumption A2)]

(L3) $\Rightarrow\ \widetilde{g}_{00} \ge q^2/(2(127n)^2) - E^*_{00}$ [(L1), (L2)]

(L4) $q^2/(2(127n)^2) - E^*_{00} > 2^{-8}$ [the first measured row]

(L5) $\Rightarrow\ \widetilde{g}_{00} > 2^{-8}$ [(L3), (L4)]

(L6) $\Rightarrow$ item 1 [(L5)]

□ (item 1)

Proof of item 2.

(L7) $E^*_{00} \le 2^{-24}$ [the second measured row]

(L8) $2^{-24} < 2^{-8}$ [$\forall t \in \mathbb{R}:\ 2^t = e^{t \ln 2}$ (Fact A.41, item 12); exp increasing on $\mathbb{R}$ (Fact A.41, item 5), at $t := -24$ and $t := -8$]

(L9) $\Rightarrow\ E^*_{00} < 2^{-8}$ [(L7), (L8)]

(L10) $\Rightarrow\ E^*_{00} < \widetilde{g}_{00}$ [(L5), (L9)]

(L11) $\Rightarrow$ item 2 [(L10)]

□ (item 2)

Lemma H.17 (The rounded checks' bounds [to table])**.** *A key that passes the four rounded checks has its computed images below the checks' thresholds and its computed first Gram diagonal and off-diagonal entry within the thresholds' ranges, each threshold enlarged by the checks' rounding. Define:*

- $\Psi_n := \{\psi_k : k < n/2\}$*, that of Fact A.43 at* $m := n$.

Let:

- (f, g, F, G) *be a checked key (Definition 5.5) of degree* n*;*
- $\psi \in \Psi_n$.

Define:

- $(\gamma_{fg}, \gamma_{\text{hyb}}, \gamma_{FG}, \gamma_{\text{root}}) := \begin{cases} (275, 4.75, 4500, 27) & n = 512 \\ (280, 5.75, 6800, 34) & n = 1024 \end{cases}$ *(*keygen *(Algorithm 11), Require [L0: fxp/kgen_fx.c:97-111];*
- $\check{\gamma}_{fg} := (\gamma_{fg}^2 + 2^{-64})^{1/2}$ *and* $\check{\gamma}_{FG} := (\gamma_{FG}^2 + 2^{-64})^{1/2}$ *(Definition A.35);*
- $\check{\gamma}_{\text{hyb}} := (\gamma_{\text{hyb}}^2 + 2^{-65})^{1/2}$ *(Definition A.35);*
- $\check{\gamma}_{\text{root}} := ((\gamma_{\text{root}}^2 + 2^{-65})(1 + 2^{-65}\check{\gamma}_{\text{hyb}}^4/q^2) + 2^{-64}\check{\gamma}_{\text{hyb}}^4/q^2)^{1/2}$ *(Definition A.35);*
- $\widetilde{\hat{p}}$, $p \in \{f, g, F, G\}$, $\widetilde{g}_{00}$ *and* $\widetilde{g}_{01}$*, the values* keychecks *computes in* $\mathcal{F}_{\text{fx}}$*, lines 1 to 11.*

Then the computed images and Gram matrix entries satisfy:

1. $\forall p \in \{f, g\} : \ |\widetilde{\hat{p}}(\psi)| \le \check{\gamma}_{fg}$;
2. $\forall p \in \{F, G\} : \ |\widetilde{\hat{p}}(\psi)| \le \check{\gamma}_{FG}$;
3. $\widetilde{g}_{00}(\psi) \in [q/\check{\gamma}_{\text{hyb}}^2, \ q\check{\gamma}_{\text{hyb}}^2]$;
4. $|\widetilde{g}_{01}(\psi)| \le \check{\gamma}_{\text{root}}\, \widetilde{g}_{00}(\psi)$.

Proof.

COMPUTES *lo*, *hi* and num_ψ, the values keychecks computes in $\mathcal{F}_{\text{fx}}$, lines 1 to 11

Proof of items 1 and 2.

(L1) $\forall \gamma \in \{\gamma_{fg}, \gamma_{\text{hyb}}, \gamma_{FG}, \gamma_{\text{root}}\} : \ \gamma \in 2^{-2}\mathbb{Z}$
[keygen (Algorithm 11), Require [L0: fxp/kgen_fx.c:97-111]]

(L2) $\Rightarrow \ \forall \gamma \in \{\gamma_{fg}, \gamma_{\text{hyb}}, \gamma_{FG}, \gamma_{\text{root}}\} : \ \gamma^2 \in 2^{-4}\mathbb{Z}$
[(L1)]

(L3) $2^{-4}\mathbb{Z} \subset 2^{-64}\mathbb{Z}$
[$2^{-4} = 2^{60} \cdot 2^{-64}$]

(L4) $\Rightarrow \ \forall \gamma \in \{\gamma_{fg}, \gamma_{\text{hyb}}, \gamma_{FG}, \gamma_{\text{root}}\} : \ \text{fl}(\gamma^2) = \gamma^2$
[(L2), (L3); $\text{fl}(x)$ the element of $2^{-64}\mathbb{Z}$ within 2^{-65} of x (Definition A.4)]

(L5) $\forall x \in \mathcal{F}_{\text{fx}} : \ \text{fl}(x^2) \ge x^2 - 2^{-65}$
[Definition A.4]

(L6) $\forall x, y \in \mathcal{F}_{\text{fx}}, \ y \ne 0 : \ \text{fl}(x/y) \ge x/y - 2^{-65}$
[Definition A.4]

(L7) $\forall p \in \{f, g, F, G\} : \ |\widetilde{\hat{p}}|^2 = \widetilde{\hat{p}}_r^2 + \widetilde{\hat{p}}_i^2$
[Fact A.41, item 1: $|a + ib|^2 = a^2 + b^2$]

(L8) $\forall p \in \{f, g, F, G\} : \ \widetilde{\hat{p}}_r^2 + \widetilde{\hat{p}}_i^2 \le \text{fl}(\widetilde{\hat{p}}_r^2) + \text{fl}(\widetilde{\hat{p}}_i^2) + 2^{-64}$
[(L5) at $x := \widetilde{\hat{p}}_r$ and at $x := \widetilde{\hat{p}}_i$]

(L9) $\forall p \in \{f, g\} : \ \text{fl}(\widetilde{\hat{p}}_r^2) + \text{fl}(\widetilde{\hat{p}}_i^2) \le \gamma_{fg}^2$
[Definition 5.5, item 4, at the key (the statement); line 5; (L4)]

(L10) $\forall p \in \{F, G\} : \ \text{fl}(\widetilde{\hat{p}}_r^2) + \text{fl}(\widetilde{\hat{p}}_i^2) \le \gamma_{FG}^2$
[Definition 5.5, item 6, at the key (the statement); line 9; (L4)]

(L11) $\check{\gamma}_{fg}^2 = \gamma_{fg}^2 + 2^{-64}$
[Definition A.35, item 1]

(L12) $\check{\gamma}_{FG}^2 = \gamma_{FG}^2 + 2^{-64}$
[Definition A.35, item 2]

(L13) $\Rightarrow \ \forall p \in \{f, g\} : \ |\widetilde{\hat{p}}(\psi)| \le \check{\gamma}_{fg}$
[(L7), (L8), (L9), (L11); Fact A.41, item 5: $t \mapsto \sqrt{t}$ nondecreasing]

(L14) $\Rightarrow$ item 1
[(L13)]

(L15) $\Rightarrow\ \forall p \in \{F, G\} :\ |\widetilde{\hat{p}}(\psi)| \le \check{\gamma}_{FG}$

[(L7), (L8), (L10), (L12); Fact A.41, item 5: $t \mapsto \sqrt{t}$ nondecreasing]

(L16) $\Rightarrow$ item 2

[(L15)]

□ (items 1 and 2)

Proof of item 3.

Lemma H.16, item 1 at every $\psi' \in \Psi_n$	This proof
$(f, g, F, G), n$	$(f, g, F, G), n$ (the statement)
ψ	ψ' (the proof's block)
$n \in \{512, 1024\}$	Definition 5.5, item 1
(I1) (f, g, F, G) key of degree n	The statement
Assumption A1	Definition 5.5, item 2
Assumption A2	Definition 5.5, item 3
Its conclusion: $\widetilde{g}_{00} > 2^{-8}$	

(L17) $\forall \psi' \in \Psi_n :\ \widetilde{g}_{00}(\psi') > 2^{-8}$

[(I1)]

(L18) $\Rightarrow\ lo > 0$

[(L17); line 6]

(L19) $hi/q \le \mathrm{fl}(hi/q) + 2^{-65}$

[(L6) at $(x, y) := (hi, q)$]

(L20) $\mathrm{fl}(hi/q) \le \gamma_{\mathrm{hyb}}^2$

[Definition 5.5, item 5, at the key (the statement); line 8; (L4)]

(L21) $q/lo \le \mathrm{fl}(q/lo) + 2^{-65}$

[(L6) at $(x, y) := (q, lo)$; (L18)]

(L22) $\mathrm{fl}(q/lo) \le \gamma_{\mathrm{hyb}}^2$

[Definition 5.5, item 5, at the key (the statement); line 8; (L4)]

(L23) $\gamma_{\mathrm{hyb}}^2 + 2^{-65} = \check{\gamma}_{\mathrm{hyb}}^2$

[Definition A.35, item 3]

(L24) $\Rightarrow\ hi \le q\check{\gamma}_{\mathrm{hyb}}^2$

[(L19), (L20), (L23)]

(L25) $\Rightarrow\ lo \ge q/\check{\gamma}_{\mathrm{hyb}}^2$

[(L18), (L21), (L22), (L23)]

(L26) $lo \le \widetilde{g}_{00}(\psi)$

[line 6]

(L27) $\widetilde{g}_{00}(\psi) \le hi$

[line 7]

(L28) $\Rightarrow\ \widetilde{g}_{00}(\psi) \in [q/\check{\gamma}_{\mathrm{hyb}}^2,\ q\check{\gamma}_{\mathrm{hyb}}^2]$

[(L24) to (L27)]

(L29) $\Rightarrow$ item 3

[(L28)]

□ (item 3)

Proof of item 4.

(L30) $num_\psi \ge |\widetilde{g}_{01}(\psi)|^2 - 2^{-64}$

[line 10; (L5) at $x := \widetilde{g}_{01,r}$ and at $x := \widetilde{g}_{01,i}$; Fact A.41, item 1: $|a + ib|^2 = a^2 + b^2$]

(L31) $\mathrm{fl}(\widetilde{g}_{00}(\psi)^2) \le \widetilde{g}_{00}(\psi)^2 + 2^{-65}$

[Definition A.4]

(L32) $\mathrm{fl}(\widetilde{g}_{00}(\psi)^2) \ge \widetilde{g}_{00}(\psi)^2 - 2^{-65}$

[(L5) at $x := \widetilde{g}_{00}$]

(L33) $\widetilde{g}_{00}(\psi)^2 - 2^{-65} > 0$

[(L17) at $\psi' := \psi$]

(L34) $\Rightarrow$ $\mathrm{fl}(\widetilde{g}_{00}(\psi)^2) > 0$

[(L32), (L33)]

(L35) $num_\psi / \mathrm{fl}(\widetilde{g}_{00}(\psi)^2) \le \mathrm{fl}(num_\psi / \mathrm{fl}(\widetilde{g}_{00}(\psi)^2)) + 2^{-65}$

[(L6) at $(x, y) := (num_\psi, \mathrm{fl}(\widetilde{g}_{00}^2))$; (L34)]

(L36) $\mathrm{fl}(num_\psi / \mathrm{fl}(\widetilde{g}_{00}(\psi)^2)) \le \gamma_{\mathrm{root}}^2$

[Definition 5.5, item 7, at the key (the statement); line 11; (L4)]

(L37) $\Rightarrow$ $|\widetilde{g}_{01}(\psi)|^2 \le (\gamma_{\mathrm{root}}^2 + 2^{-65})(\widetilde{g}_{00}(\psi)^2 + 2^{-65}) + 2^{-64}$

[(L30), (L31), (L34), (L35), (L36)]

(L38) $1/\widetilde{g}_{00}(\psi)^2 \le \check{\gamma}_{\mathrm{hyb}}^4 / q^2$

[item 3; Fact A.41, item 5: $t \mapsto 1/t$ nonincreasing on $(0, \infty)$]

(L39) $\Rightarrow$ $|\widetilde{g}_{01}(\psi)|^2 \le \widetilde{g}_{00}(\psi)^2((\gamma_{\mathrm{root}}^2 + 2^{-65})(1 + 2^{-65}\check{\gamma}_{\mathrm{hyb}}^4/q^2) + 2^{-64}\check{\gamma}_{\mathrm{hyb}}^4/q^2)$

[(L37), (L38)]

(L40) $(\gamma_{\mathrm{root}}^2 + 2^{-65})(1 + 2^{-65}\check{\gamma}_{\mathrm{hyb}}^4/q^2) + 2^{-64}\check{\gamma}_{\mathrm{hyb}}^4/q^2 = \check{\gamma}_{\mathrm{root}}^2$

[Definition A.35, item 4]

(L41) $\Rightarrow$ $|\widetilde{g}_{01}(\psi)|^2 \le \check{\gamma}_{\mathrm{root}}^2 \widetilde{g}_{00}(\psi)^2$

[(L39), (L40)]

(L42) $\Rightarrow$ $|\widetilde{g}_{01}(\psi)| \le \check{\gamma}_{\mathrm{root}}\, \widetilde{g}_{00}(\psi)$

[(L41), (L17) at $\psi' := \psi$; Fact A.41, item 5: $t \mapsto \sqrt{t}$ nondecreasing]

(L43) $\Rightarrow$ item 4

[(L42)]

□ (item 4)

Lemma H.18 (The images' bounds at a checked key [to table])**.** *A key that passes the four rounded checks has its exact images within bounds computed from the thresholds and the FFT's bound, and its computed images within a deviation of them. Define:*

- $\Psi_n := \{\psi_k : k < n/2\}$*, that of Fact A.43 at* $m := n$*.*

Let:

- (f, g, F, G) *be a checked key (Definition 5.5) of degree* n*;*
- h *with* $n = 2^h$*, as* FFT *(Algorithm 14) takes them (Precondition);*
- $\psi \in \Psi_n$*.*

Define:

- $\hat{f}$*,* $\hat{g}$*,* $\hat{F}$*,* $\hat{G}$*, the exact images,* keychecks *(Algorithm 12), line 2;*
- $\widetilde{\hat{f}}$*,* $\widetilde{\hat{g}}$*,* $\widetilde{\hat{F}}$*,* $\widetilde{\hat{G}}$*, the images* keychecks *computes in* $\mathcal{F}_{\mathrm{fx}}$*, line 1;*
- γ_{fg} *and* γ_{FG}*, those of Definition A.35;*
- $\check{\gamma}_{fg} := (\gamma_{fg}^2 + 2^{-64})^{1/2}$ *and* $\check{\gamma}_{FG} := (\gamma_{FG}^2 + 2^{-64})^{1/2}$ *(Definition A.35);*
- R_{h-1} *and* A_{h-1}*, those of Definition A.36;*
- $\delta_{fg} := R_{h-1}(\check{\gamma}_{fg}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$ *(Definition A.36);*
- $\delta_{FG} := R_{h-1}(\check{\gamma}_{FG}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$ *(Definition A.36);*
- $\gamma'_{fg} := \check{\gamma}_{fg} + \delta_{fg}$ *and* $\gamma'_{FG} := \check{\gamma}_{FG} + \delta_{FG}$ *(Definition A.36).*

Then the exact images and the computed images' deviation are bounded:

1. $\forall p \in \{f, g\} : \ |\hat{p}(\psi)| \le \gamma'_{fg}$*;*
2. $\forall p \in \{F, G\} : \ |\hat{p}(\psi)| \le \gamma'_{FG}$*;*
3. $\forall (p, \delta) \in \{(f, \delta_{fg}), (g, \delta_{fg}), (F, \delta_{FG}), (G, \delta_{FG})\} : \ |\widetilde{\hat{p}}(\psi) - \hat{p}(\psi)| \le \delta$*.*

Proof.

DEFINES $\zeta = 2^{-64}$

DEFINES $c_{\text{merge}} := \sqrt{2} \cdot 2^{-64}$ and $k_E := 8\sqrt{2}$ (Lemma G.18 at $(u, \zeta) = (0, 2^{-64})$)

DEFINES P, that of FFT (Algorithm 14), line 1

DEFINES $R_{h-1} = (1 + c_{\text{merge}})^{h-1} - 1$

DEFINES $A_0 = 0$

DEFINES $A_{j+1} = \sqrt{2}(1 + c_{\text{merge}})A_j + k_E\,\zeta\sqrt{P}$, $j < h - 1$

MEASURED $R_{h-1} < 1$ at both degrees `verify/reports/fx/terms.py`

DEFINES $\Gamma := \{(f, \check{\gamma}_{fg}, \delta_{fg}, \gamma'_{fg}), (g, \check{\gamma}_{fg}, \delta_{fg}, \gamma'_{fg}), (F, \check{\gamma}_{FG}, \delta_{FG}, \gamma'_{FG}), (G, \check{\gamma}_{FG}, \delta_{FG}, \gamma'_{FG})\}$

Proof of items 1 to 3.

(L1) $\forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ \|\hat{p}\| \le \|\widetilde{\hat{p}}\| + \|\widetilde{\hat{p}} - \hat{p}\|$

[Fact A.41, item 3, at $(X, Y) := (\widetilde{\hat{p}}, \hat{p} - \widetilde{\hat{p}})$]

Lemma H.11 at every $(p, \check{\gamma}, \delta, \gamma') \in \Gamma$	This proof
Shared: $\zeta,\ h, n,\ c_{\text{merge}}, k_E, P,\ R_{h-1}, A_j$	
$\mathcal{F}$	$\mathcal{F}_{\text{fx}}$
u	0
f	p
$\hat{f}, \widetilde{\hat{f}}$	$\hat{p}, \widetilde{\hat{p}}$
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\text{fx}}$ at $(0, 2^{-64})$ (Definition A.4, item 8)
$f_{[a]} \in \mathcal{F},\ a < n$	$p \in \mathbb{Z}[x]/(x^n + 1)$ (keygen (Algorithm 11), line 3); Definition A.4, item 8
Its conclusion: $\|\widetilde{\hat{f}} - \hat{f}\| \le R_{h-1}\|\hat{f}\| + A_{h-1}$	

(I1)

(L2) $\forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ \|\widetilde{\hat{p}} - \hat{p}\| \le R_{h-1}\|\hat{p}\| + A_{h-1}$

[(I1)]

(L3) $\forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ \|\widetilde{\hat{p}}\| \le \check{\gamma}\sqrt{n/2}$

[Lemma H.17, items 1 and 2; $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead) over the $n/2$ roots, at the checked key (the statement)]

(L4) $\Rightarrow\ \forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ \|\hat{p}\| \le \check{\gamma}\sqrt{n/2} + R_{h-1}\|\hat{p}\| + A_{h-1}$

[(L1), (L2), (L3)]

(L5) $\Rightarrow\ \forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ \|\hat{p}\| \le \frac{\check{\gamma}\sqrt{n/2} + A_{h-1}}{1 - R_{h-1}}$

[(L4); $R_{h-1} < 1$ (the proof's block)]

Lemma H.12 at every $(p, \check{\gamma}, \delta, \gamma') \in \Gamma$	This proof
Shared: $\zeta,\ h, n,\ c_{\text{merge}}, k_E, P,\ R_{h-1}, A_j$	
$\mathcal{F}$	$\mathcal{F}_{\text{fx}}$
u	0
f	p
$\hat{f}_k, \widetilde{\hat{f}}_k$	$\hat{p}(\psi), \widetilde{\hat{p}}(\psi)$ (FFT (Algorithm 14), Post)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\text{fx}}$ at $(0, 2^{-64})$ (Definition A.4, item 8)
$f_{[a]} \in \mathcal{F},\ a < n$	$p \in \mathbb{Z}[x]/(x^n + 1)$ (keygen (Algorithm 11), line 3); Definition A.4, item 8
$k < n/2$	ψ (the statement)
Its conclusion: $\forall k < n/2 :\ \|\widetilde{\hat{f}}_k - \hat{f}_k\| \le R_{h-1}\|\hat{f}\| + A_{h-1}$	

(I2)

(L6) $\forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ |\widetilde{\hat{p}}(\psi) - \hat{p}(\psi)| \le R_{h-1}\|\hat{p}\| + A_{h-1}$

[(I2)]

(L7) $\Rightarrow\ \forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ |\widetilde{\hat{p}}(\psi) - \hat{p}(\psi)| \le \delta$

[(L5), (L6); $R_{h-1} \ge 0$ (the proof's block); δ_{fg}, δ_{FG} (Definition A.36, items 1 and 2)]

(L8) $\Rightarrow$ item 3

[(L7)]

(L9) $\forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ |\hat{p}(\psi)| \le |\widetilde{\hat{p}}(\psi)| + |\widetilde{\hat{p}}(\psi) - \hat{p}(\psi)|$

[Fact A.41, item 1: $|x+y| \le |x| + |y|$]

(L10) $\forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ |\hat{p}(\psi)| \le \check{\gamma} + \delta$

[(L7), (L9); Lemma H.17, items 1 and 2]

(L11) $\forall (p, \check{\gamma}, \delta, \gamma') \in \Gamma :\ \check{\gamma} + \delta = \gamma'$

[γ'_{fg}, γ'_{FG} (Definition A.36, items 3 and 4)]

(L12) $\Rightarrow\ \forall p \in \{f, g\} :\ |\hat{p}(\psi)| \le \gamma'_{fg}$

[(L10), (L11); Γ (the proof's block)]

(L13) $\Rightarrow$ item 1

[(L12)]

(L14) $\Rightarrow\ \forall p \in \{F, G\} :\ |\hat{p}(\psi)| \le \gamma'_{FG}$

[(L10), (L11); Γ (the proof's block)]

(L15) $\Rightarrow$ item 2

[(L14)]

□ (items 1 to 3)

Lemma H.19 (The Gram's bounds at a checked key [to table])**.** *A key that passes the four rounded checks has its computed Gram within bounds of the exact one, its exact first diagonal between two bounds and its second at most a bound. Define:*

- $\Psi_n := \{\psi_k : k < n/2\}$, *that of Fact A.43 at* $m := n$.

Let:

- (f, g, F, G) *be a checked key (Definition 5.5) of degree* n;
- h *with* $n = 2^h$, *as* FFT *(Algorithm 14) takes them (Precondition);*
- $\psi \in \Psi_n$.

Define:

- *The signer's words and parameters*
  - $\zeta := 2^{-64}$ *(Definition I.1 at* $\zeta_{\text{op}} := 2^{-65}$*);*
  - γ_{hyb}, *that of Definition A.35;*
- *The Gram deltas*
  - $\check{\gamma}_{fg}$, $\check{\gamma}_{FG}$, R_{h-1} *and* A_{h-1}, *those of Definition A.36;*
  - $k_H := 7$ *(Lemma G.22 at* $u = 0$*) and* $k'_H := 7\sqrt{2}$ *(Lemma G.23 at* $u = 0$*);*
  - $\delta_{fg} := R_{h-1}(\check{\gamma}_{fg}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$ *(Definition A.36);*
  - $\delta_{FG} := R_{h-1}(\check{\gamma}_{FG}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$ *(Definition A.36);*
  - $\gamma'_{fg} := \check{\gamma}_{fg} + \delta_{fg}$ *and* $\gamma'_{FG} := \check{\gamma}_{FG} + \delta_{FG}$ *(Definition A.36);*
  - $E_{00} := k_H\zeta + 4\gamma'_{fg}\delta_{fg} + 2\delta^2_{fg}$ *and* $E_{11} := k_H\zeta + 4\gamma'_{FG}\delta_{FG} + 2\delta^2_{FG}$ *(Definition A.36);*
  - $E_{01} := k'_H\zeta + 2(\gamma'_{fg}\delta_{FG} + \gamma'_{FG}\delta_{fg} + \delta_{fg}\delta_{FG})$ *(Definition A.36);*
- *The key bounds*
  - $\check{\gamma}_{\text{hyb}} := (\gamma^2_{\text{hyb}} + 2^{-65})^{1/2}$ *(Definition A.35);*
  - $m_0 := q/\check{\gamma}^2_{\text{hyb}} - E_{00}$, $M_0 := q\check{\gamma}^2_{\text{hyb}} + E_{00}$ *and* $\bar{g}_{11} := 2\gamma'^2_{FG}$ *(Definition A.37);*
- *The Gram matrix entries*
  - g_{00}, g_{01}, g_{11}, *the exact Gram matrix entries,* keychecks *(Algorithm 12), line 4;*
  - $\widetilde{g}_{00}$, $\widetilde{g}_{01}$ *and* $\widetilde{g}_{11}$, *the values* keychecks *computes in* $\mathcal{F}_{\text{fx}}$, *lines 1 to 11* [LO: `fxp/kgen_fx.c: 81`].

Then the computed Gram's perturbation and the exact diagonals are bounded:

1. $|\widetilde{g}_{00}(\psi) - g_{00}(\psi)| \le E_{00}$;
2. $|\widetilde{g}_{11}(\psi) - g_{11}(\psi)| \le E_{11}$;
3. $|\widetilde{g}_{01}(\psi) - g_{01}(\psi)| \le E_{01}$;
4. $g_{00}(\psi) \in [m_0, M_0]$;

5. $g_{11}(\psi) \le \bar{g}_{11}$.

Proof.

DEFINES $q = 12289$

DEFINES $\hat{F}$, $\hat{G}$, the exact images, keychecks (Algorithm 12), line 2

Proof of items 1 to 5.

(I1)

Lemma H.18	This proof
Shared: $h, n,\ (f, g, F, G),\ \psi$	
(f, g, F, G) checked key of degree n	The statement
Its item 1: $\forall p \in \{f, g\} :\ \lvert\hat{p}(\psi)\rvert \le \gamma'_{fg}$	
Its item 2: $\forall p \in \{F, G\} :\ \lvert\hat{p}(\psi)\rvert \le \gamma'_{FG}$	
Its item 3: $\forall (p, \delta) \in \{(f, \delta_{fg}), (g, \delta_{fg}), (F, \delta_{FG}), (G, \delta_{FG})\} :\ \lvert\widetilde{\hat{p}}(\psi) - \hat{p}(\psi)\rvert \le \delta$	

(L1) $\forall p \in \{f, g\} :\ \lvert\hat{p}(\psi)\rvert \le \gamma'_{fg}$

[item 1 of (I1)]

(L2) $\forall p \in \{F, G\} :\ \lvert\hat{p}(\psi)\rvert \le \gamma'_{FG}$

[item 2 of (I1)]

(L3) $\forall (p, \delta) \in \{(f, \delta_{fg}), (g, \delta_{fg}), (F, \delta_{FG}), (G, \delta_{FG})\} :\ \lvert\widetilde{\hat{p}}(\psi) - \hat{p}(\psi)\rvert \le \delta$

[item 3 of (I1)]

(I2)

Lemma H.14	This proof
$\gamma_{fg}, \gamma_{FG}, \delta_{fg}, \delta_{FG}$	$\gamma'_{fg}, \gamma'_{FG}, \delta_{fg}, \delta_{FG}$ (the statement)
$\widetilde{\hat{f}}, \widetilde{\hat{g}}, \widetilde{\hat{F}}, \widetilde{\hat{G}}$	$\widetilde{\hat{f}}(\psi), \widetilde{\hat{g}}(\psi), \widetilde{\hat{F}}(\psi), \widetilde{\hat{G}}(\psi)$ (keychecks, line 3)
$\gamma_{fg}, \gamma_{FG}, \delta_{fg}, \delta_{FG} \in \mathbb{R}$	The statement
$\widetilde{\hat{f}}, \widetilde{\hat{g}}, \widetilde{\hat{F}}, \widetilde{\hat{G}} \in 2^{-64}\mathbb{Z} + i\,2^{-64}\mathbb{Z}$	keychecks, line 1, in $\mathcal{F}_{\text{fx}}$ (the statement)
Assumption A1	(L1), (L2)
Assumption A2	(L3)
Its item 1: $\lvert\widetilde{g}_{00} - g_{00}\rvert \le k_H\zeta + 4\gamma_{fg}\delta_{fg} + 2\delta_{fg}^2$	
Its item 2: $\lvert\widetilde{g}_{11} - g_{11}\rvert \le k_H\zeta + 4\gamma_{FG}\delta_{FG} + 2\delta_{FG}^2$	
Its item 3: $\lvert\widetilde{g}_{01} - g_{01}\rvert \le k'_H\zeta + 2(\gamma_{fg}\delta_{FG} + \gamma_{FG}\delta_{fg} + \delta_{fg}\delta_{FG})$	

(L4) $\lvert\widetilde{g}_{00}(\psi) - g_{00}(\psi)\rvert \le k_H\zeta + 4\gamma'_{fg}\delta_{fg} + 2\delta_{fg}^2$

[item 1 of (I2)]

(L5) $k_H\zeta + 4\gamma'_{fg}\delta_{fg} + 2\delta_{fg}^2 = E_{00}$

[E_{00} (Definition A.36, item 5)]

(L6) $\Rightarrow$ item 1

[(L4), (L5)]

(L7) $\lvert\widetilde{g}_{11}(\psi) - g_{11}(\psi)\rvert \le k_H\zeta + 4\gamma'_{FG}\delta_{FG} + 2\delta_{FG}^2$

[item 2 of (I2)]

(L8) $k_H\zeta + 4\gamma'_{FG}\delta_{FG} + 2\delta_{FG}^2 = E_{11}$

[E_{11} (Definition A.36, item 6)]

(L9) $\Rightarrow$ item 2

[(L7), (L8)]

(L10) $\lvert\widetilde{g}_{01}(\psi) - g_{01}(\psi)\rvert \le k'_H\zeta + 2(\gamma'_{fg}\delta_{FG} + \gamma'_{FG}\delta_{fg} + \delta_{fg}\delta_{FG})$

[item 3 of (I2)]

(L11) $k'_H\zeta + 2(\gamma'_{fg}\delta_{FG} + \gamma'_{FG}\delta_{fg} + \delta_{fg}\delta_{FG}) = E_{01}$

[E_{01} (Definition A.36, item 7)]

(L12) $\Rightarrow$ item 3

[(L10), (L11)]

(L13) $g_{00}(\psi) \ge \widetilde{g}_{00}(\psi) - E_{00}$

[(L4), (L5)]

(L14) $g_{00}(\psi) \le \widetilde{g}_{00}(\psi) + E_{00}$

[(L4), (L5)]

(L15) $\widetilde{g}_{00}(\psi) \in [q/\check{\gamma}^2_{\mathrm{hyb}},\ q\check{\gamma}^2_{\mathrm{hyb}}]$

[Lemma H.17, item 3, at the checked key (the statement)]

(L16) $g_{00}(\psi) \ge m_0$

[(L13), (L15); $m_0 = q/\check{\gamma}^2_{\mathrm{hyb}} - E_{00}$ (Definition A.37, item 1)]

(L17) $g_{00}(\psi) \le M_0$

[(L14), (L15); $M_0 = q\check{\gamma}^2_{\mathrm{hyb}} + E_{00}$ (Definition A.37, item 2)]

(L18) $\Rightarrow$ $g_{00}(\psi) \in [m_0, M_0]$

[(L16), (L17)]

(L19) $\Rightarrow$ item 4

[(L18)]

(L20) $g_{11}(\psi) = |\hat{F}(\psi)|^2 + |\hat{G}(\psi)|^2$

[g_{11} (Fact A.33; keychecks (Algorithm 12), line 4)]

(L21) $g_{11}(\psi) \le 2\gamma'^2_{FG}$

[(L2) at $p := F$ and at $p := G$; (L20); Fact A.41, item 5: $t \mapsto t^2$ nondecreasing on $[0, \infty)$]

(L22) $2\gamma'^2_{FG} = \bar{g}_{11}$

[$\bar{g}_{11}$ (Definition A.37, item 6)]

(L23) $\Rightarrow$ $g_{11}(\psi) \le \bar{g}_{11}$

[(L21), (L22)]

(L24) $\Rightarrow$ item 5

[(L23)]

□ (items 1 to 5)

Lemma H.20 (Operator norms of a Gram matrix's tree map [to table])**.** *The tree map of a Gram matrix's tree and its inverse are bounded by the matrix's eigenvalues against the tree's leaf diagonals. Let:*

- $m = 2^{h'}$ *with* $h' \ge 1$*;*
- $\mathcal{G} \in \mathrm{Gram}_m$ *(Definition A.14);*
- $\lambda_{\mathrm{lo}} > 0$*;*
- $\lambda_{\mathrm{hi}} > 0$*;*
- $d_{\mathrm{lo}} > 0$*;*
- $d_{\mathrm{hi}} > 0$.

Define:

- $T := \mathrm{ffLDL}^{\dagger}(\mathcal{G})$ *(Definition A.20);*
- $N := 2m$*;*
- d_i*,* $i \le N$*, the leaf diagonals of* T *(Definition A.19);*
- $\mathcal{L}_T$*, the tree map at* T*, and* $\mathcal{L}_T^{-1}$*, its inverse (Definition 4.6, item 7, at* T*);*
- $\|A\| := \max_{x \ne 0} \|xA\|/\|x\|$ *for* $A \in \{\mathcal{L}_T, \mathcal{L}_T^{-1}\}$*,* $\|x\|$ *the coefficient norm (Definition 4.6, items 7 and 6, at* T*);*
- $Z_m := \{\psi \in \mathbb{C} : \psi^m = -1\}$ *(Fact A.43);*
- (g_{00}, g_{01}, g_{11})*, the entries of* $\mathcal{G}(\psi)$*, for* $\psi \in Z_m$*;*
- $\lambda_{\pm}(\psi) := (g_{00} + g_{11})/2 \pm (((g_{00} - g_{11})/2)^2 + |g_{01}|^2)^{1/2}$*,* $\psi \in Z_m$ *(Fact A.44 at* $\mathcal{G} := \mathcal{G}(\psi)$*).*

Assume:

(A1) $\forall \psi \in Z_m :\ \lambda_-(\psi) \ge \lambda_{\mathrm{lo}}$*;*

(A2) $\forall \psi \in Z_m :\ \lambda_+(\psi) \le \lambda_{\mathrm{hi}}$*;*

(A3) $\forall i \le N :\ d_i \ge d_{\mathrm{lo}}$*;*

(A4) $\forall i \le N :\ d_i \le d_{\mathrm{hi}}$.

Then the tree map and its inverse are bounded:

1. $\|\mathcal{L}_T\| \le (\lambda_{\text{hi}}/d_{\text{lo}})^{1/2}$;

2. $\|\mathcal{L}_T^{-1}\| \le (d_{\text{hi}}/\lambda_{\text{lo}})^{1/2}$.

Proof.

DEFINES $x \in \mathcal{R}_m^2$
$Q_T(x) := \sum_{v \le m} d_v^T \, |(x\mathcal{L}_T)_v|^2$, d_v^T the leaf diagonals of T (Definition H.1)
$Q_{\mathcal{G}}(x) := \frac{2}{m} \sum_{k<m/2} x(\psi_k)\mathcal{G}(\psi_k)x(\psi_k)^\dagger$ (Definition A.32)
$\psi_k := e^{i\pi(2k+1)/m} \in Z_m$ for $k < m/2$ (Definition A.32; Fact A.43, item 2)

	Lemma H.2	This proof
	Shared: $T,\ N,\ Q_T,\ \mathcal{L}_T, d_i$	
(I1)	n $T \in \mathcal{T}_n$	m $T := \text{ffLDL}^\dagger(\mathcal{G})$, $\mathcal{G} \in \text{Gram}_m$ (the statement); Definition A.20
	Its conclusion: $\forall x \in \mathcal{R}_n \times \mathcal{R}_n :\ Q_T(x) = \sum_{i \le N} d_i (x\mathcal{L}_T)_i^2$	
(L1)	$\forall x :\ Q_T(x) = \sum_{i \le N} d_i (x\mathcal{L}_T)_i^2$	[(I1)]
(L2)	$\Rightarrow\ \forall x :\ d_{\text{lo}} \|x\mathcal{L}_T\|^2 \le Q_T(x)$	[(L1); assumption A3; $\|X\|^2 := \sum_i \|X_i\|^2$ (Fact A.41, its lead)]
(L3)	$\Rightarrow\ \forall x :\ Q_T(x) \le d_{\text{hi}} \|x\mathcal{L}_T\|^2$	[(L1); assumption A4; $\|X\|^2 := \sum_i \|X_i\|^2$ (Fact A.41, its lead)]
	Proposition H.7, item 3 at $n := m$ and $\mathcal{G}$	This proof
	Shared: $T,\ \mathcal{G},\ Q_T, Q_{\mathcal{G}},\ \mathcal{L}_T, d_i$	
(I2)	n $\mathcal{G} \in \text{Gram}_n$	m (the scope) $\mathcal{G} \in \text{Gram}_m$ (the statement)
	Assumption A1	$T = \text{ffLDL}^\dagger(\mathcal{G})$ (the statement)
	Its conclusion: $\forall x \in \mathcal{R}_n^2 :\ Q_T(x) = Q_{\mathcal{G}}(x)$	
(L4)	$\forall x :\ Q_T(x) = Q_{\mathcal{G}}(x)$	[(I2)]
(L5)	$\forall x :\ Q_{\mathcal{G}}(x) = \frac{2}{m} \sum_{k<m/2} x(\psi_k)\, \mathcal{G}(\psi_k)\, x(\psi_k)^\dagger$	[$Q_{\mathcal{G}}$ (Definition A.32)]
(L6)	$\forall \psi \in Z_m\ \forall y \in \mathbb{C}^2 :\ \lambda_-(\psi)(\|y_0\|^2 + \|y_1\|^2) \le y\, \mathcal{G}(\psi)\, y^\dagger$	[Fact A.44, item 3]
(L7)	$\forall \psi \in Z_m\ \forall y \in \mathbb{C}^2 :\ y\, \mathcal{G}(\psi)\, y^\dagger \le \lambda_+(\psi)(\|y_0\|^2 + \|y_1\|^2)$	[Fact A.44, item 3]
	Proposition G.15 at $f := x_0$ and at $f := x_1$	This proof
	Shared: ψ_k (Definition A.32)	
(I3)	n, h f $n = 2^h,\ h \ge 1$ $f \in \mathbb{R}[x]/(x^n + 1)$	m, h' x_0, x_1 $m = 2^{h'},\ h' \ge 1$ (the statement) $x \in \mathcal{R}_m^2$ (the proof's block); $\mathcal{R}_m$ (Definition A.1)
	Its conclusion: $\sum_{p<n} f_{[p]}^2 = \frac{2}{n} \sum_{k<n/2} \|f(\psi_k)\|^2$	
(L8)	$\forall x :\ \frac{2}{m} \sum_{k<m/2} (\|x_0(\psi_k)\|^2 + \|x_1(\psi_k)\|^2) = \|x\|^2$	[(I3); $\|(X,Y)\|^2 := \|X\|^2 + \|Y\|^2$ (Fact A.41, its lead)]
(L9)	$\forall x :\ \lambda_{\text{lo}} \frac{2}{m} \sum_{k<m/2} (\|x_0(\psi_k)\|^2 + \|x_1(\psi_k)\|^2) \le Q_{\mathcal{G}}(x)$	[(L5), (L6) at $\psi := \psi_k$, $y := x(\psi_k)$; assumption A1]

(L10) $\Rightarrow$ $\forall x:\ \lambda_{\mathrm{lo}}\|x\|^2 \le Q_{\mathcal{G}}(x)$

[(L8), (L9)]

(L11) $\forall x:\ Q_{\mathcal{G}}(x) \le \lambda_{\mathrm{hi}}\frac{2}{m}\sum_{k<m/2}(|x_0(\psi_k)|^2 + |x_1(\psi_k)|^2)$

[(L5), (L7) at $\psi := \psi_k$, $y := x(\psi_k)$; assumption A2]

(L12) $\Rightarrow$ $\forall x:\ Q_{\mathcal{G}}(x) \le \lambda_{\mathrm{hi}}\|x\|^2$

[(L8), (L11)]

(L13) $\Rightarrow$ $\forall x:\ d_{\mathrm{lo}}\|x\mathcal{L}_T\|^2 \le \lambda_{\mathrm{hi}}\|x\|^2$

[(L2), (L4), (L12)]

(L14) $\Rightarrow$ $\|\mathcal{L}_T\| \le (\lambda_{\mathrm{hi}}/d_{\mathrm{lo}})^{1/2}$

[(L13); $d_{\mathrm{lo}} > 0$ (the statement); $\lambda_{\mathrm{hi}} > 0$ (the statement); $\|\cdot\|$ of Definition 4.6, item 7, at T and $A := \mathcal{L}_T$; $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L15) $\Rightarrow$ item 1

[(L14)]

(L16) $\forall y \in \mathbb{R}^N:\ (y\mathcal{L}_T^{-1})\mathcal{L}_T = y$

[$\mathcal{L}_T^{-1}$ (Definition 4.6, item 7, at T)]

(L17) $\Rightarrow$ $\forall y \in \mathbb{R}^N:\ \lambda_{\mathrm{lo}}\|y\mathcal{L}_T^{-1}\|^2 \le d_{\mathrm{hi}}\|y\|^2$

[(L3), (L4), (L10) at $x := y\mathcal{L}_T^{-1}$; (L16)]

(L18) $\Rightarrow$ $\|\mathcal{L}_T^{-1}\| \le (d_{\mathrm{hi}}/\lambda_{\mathrm{lo}})^{1/2}$

[(L17); $\lambda_{\mathrm{lo}} > 0$ (the statement); $d_{\mathrm{hi}} > 0$ (the statement); $\|\cdot\|$ of Definition 4.6, item 7, at T and $A := \mathcal{L}_T^{-1}$; $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L19) $\Rightarrow$ item 2

[(L18)]

□ (items 1 and 2)

Proposition 5.8 (*The tree's bounds at a checked key [to table]*) [to statement].

A key that passes the four rounded checks has every diagonal of its tree, κ_k and κ_{root} of the LDL subtractions $d_{11} = g_{11} - |g_{01}|^2/g_{00}$ at its nodes, the off-diagonal factors and the norms of the tree maps below the root within bounds computed from the thresholds and the FFT's bound. Let:

- *(f, g, F, G) be a checked key (Definition 5.5) of degree n;*
- *h with $n = 2^h$, as FFT (Algorithm 14) takes them (Precondition).*

Define:

- *The Gram deltas*
  - *$c_{\mathrm{merge}} := \sqrt{2}\cdot 2^{-64}$ (Lemma G.18 at $(u,\zeta) = (0, 2^{-64})$);*
  - *$R_{h-1} := (1 + c_{\mathrm{merge}})^{h-1} - 1$;*
  - *E_{00} and E_{01}, those of Definition A.36, items 5 and 7;*
  - *γ'_{FG}, that of Definition A.37;*
- *The key bounds*
  - *γ_{hyb}, that of Definition A.35;*
  - *$\check{\gamma}_{\mathrm{hyb}} := (\gamma_{\mathrm{hyb}}^2 + 2^{-65})^{1/2}$ and $\check{\gamma}_{\mathrm{root}}$, its root threshold (Definition A.35);*
  - *$m_0 := q/\check{\gamma}_{\mathrm{hyb}}^2 - E_{00}$, $M_0 := q\check{\gamma}_{\mathrm{hyb}}^2 + E_{00}$ and $\bar{g}_{11} := 2\gamma'^2_{FG}$ (Definition A.37);*
  - *$d_{\mathrm{lo}} := \min(m_0, q^2/M_0)$, $d_{\mathrm{hi}} := \max(M_0, q^2/m_0)$ and $\bar{\varsigma} := d_{\mathrm{hi}}/d_{\mathrm{lo}}$ (Definition A.37);*
- *The Gram matrix entries*
  - *g_{00}, g_{01}, g_{11}, the exact Gram matrix entries, keychecks (Algorithm 12), line 4;*
  - *$\mathcal{G} := \begin{pmatrix} g_{00} & g_{01} \\ \mathrm{conj}\, g_{01} & g_{11} \end{pmatrix}$;*
  - *$\widetilde{g}_{00}$ and $\widetilde{g}_{01}$, the values keychecks computes in $\mathcal{F}_{\mathrm{fx}}$, lines 1 to 11 [LO: fxp/kgen_fx.c:81];*
- *The tree*
  - *$T :=$ ffLDL$^\dagger(\mathcal{G})$ (Definition A.20);*
  - *d_{00}^{ν} and d_{11}^{ν}, those of Proposition G.38 at $\mathcal{G}$ and at $\nu \in \mathrm{Sub}(T)$;*
  - *l_{10}, that of LDL† (Algorithm 5), line 13, at the root node of T;*

- *The key constants*
  - κ_k, *that of Definition 4.6 at the key;*
  - $\kappa_{\mathrm{root}} := \max_\psi |g_{01}|^2/q^2$ *(Definition 4.6);*
  - Ξ', Ξ *and* ℓ, *those of Definition 4.6 at the key.*

Measured `verify/reports/fx/terms.py`*:*

- $R_{h-1} < 1$ *at both degrees;*
- $E_{00} < q/\check{\gamma}^2_{\mathrm{hyb}}$ *at both degrees.*

Then the diagonals, κ_k *and* κ_{root}*, the factors and the tree maps' norms satisfy:*

1. $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi :\ d^\nu_j(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$;
2. $\forall k \in \{1, \dots, h-1\} :\ \kappa_k \le (\bar{\varsigma} - 1)^2/(4\bar{\varsigma})$;
3. $\kappa_{\mathrm{root}} \le (\check{\gamma}_{\mathrm{root}}\, q \check{\gamma}^2_{\mathrm{hyb}} + E_{01})^2/q^2$;
4. $\max_\psi |l_{10}| \le \check{\gamma}_{\mathrm{root}}/(1 - E_{00}\check{\gamma}^2_{\mathrm{hyb}}/q) + E_{01}/m_0$;
5. $\Xi' \le \bar{\varsigma}^{1/2}$;
6. $\Xi \le \bar{\varsigma}^{1/2}$;
7. $\ell \le \max(1,\ \check{\gamma}_{\mathrm{root}}/(1 - E_{00}\check{\gamma}^2_{\mathrm{hyb}}/q) + E_{01}/m_0)$;
8. $m_0 > 0$.

Proof.

DEFINES $d_{00} := d^T_{00}$, $d_{11} := d^T_{11}$, the root node's diagonals
g^ν_{00}, $\nu \in \mathrm{Sub}(T)$, the g_{00} of $\mathcal{G}_\nu$ (Definitions A.32 and A.17)
$k \in \{1, \dots, h-1\}$
$\nu \in \mathrm{Sub}(T)$ with $\mathrm{depth}(\nu) = k$ (Definition A.18), of degree $m' := n/2^k$
π, the parent node of ν: $\nu \in \{L(\pi), R(\pi)\}$, the children of Definition A.18
$d \in \{d^\pi_{00}, d^\pi_{11}\}$ with $\mathcal{G}_\nu = \mathcal{G}_d$ (Definition A.32)
ψ' with $\psi'^{m'} = -1$
$\psi \in \Psi_{2m'}$ with $\psi^2 = \psi'$ (Fact A.43, item 5, at $2m'$)
$a := d(\psi)$
$b := d(-\psi)$
(d_0, d_1), the values of $\mathrm{split}_{\mathrm{sa}}$ (Algorithm 3) at d and ψ (Fact D.1)
$\lambda_\pm := (g_{00} + g_{11})/2 \pm (((g_{00} - g_{11})/2)^2 + |g_{01}|^2)^{1/2}$ (Fact A.44)
(g_{00}, g_{01}, g_{11}), the entries of $\mathcal{G}_\nu(\psi')$

DEFINES Ψ_n and Z_n, those of Fact A.43 at $m := n$

Proof of items 1 and 2.

(L1) $\forall \psi \in \Psi_n :\ |\widetilde{g}_{01}(\psi) - g_{01}(\psi)| \le E_{01}$
[Lemma H.19, item 3, at the checked key (the statement)]

(L2) $\forall \psi \in \Psi_n :\ |\widetilde{g}_{00}(\psi) - g_{00}(\psi)| \le E_{00}$
[Lemma H.19, item 1, at the checked key (the statement)]

(L3) $\forall \psi \in \Psi_n :\ \widetilde{g}_{00}(\psi) \in [q/\check{\gamma}^2_{\mathrm{hyb}},\ q\check{\gamma}^2_{\mathrm{hyb}}]$
[Lemma H.17, item 3, at the checked key (the statement)]

(L4) $\forall \psi \in \Psi_n :\ g_{00}(\psi) \in [m_0, M_0]$
[Lemma H.19, item 4, at the checked key (the statement)]

(L5) $\forall \psi \in Z_n\ \exists \psi' \in \Psi_n :\ (g_{00}(\psi), |g_{01}(\psi)|) = (g_{00}(\psi'), |g_{01}(\psi')|)$
[$Z_n = \Psi_n \sqcup \mathrm{conj}\,\Psi_n$ (Fact A.43, item 2, at $m := n$); $g_{00}(\mathrm{conj}\,\psi) = \mathrm{conj}\, g_{00}(\psi)$ and $g_{01}(\mathrm{conj}\,\psi) = \mathrm{conj}\, g_{01}(\psi)$, $g_{00}, g_{01} \in \mathcal{R}_n$ (Fact A.42, item 2, at $m := n$); $g_{00}(\psi) \in \mathbb{R}$ (Fact A.33); $|\mathrm{conj}\, x| = |x|$ (Fact A.41, item 1)]

(L6) $\forall \psi :\ d_{00}(\psi) = g_{00}(\psi)$

[Lemma D.4, item 1]

(L7) $\forall \psi :\ d_{11}(\psi) = q^2 / g_{00}(\psi)$

[Fact A.33, item 4]

(L8) $\forall \psi :\ d_{00}(\psi) \in [m_0, M_0]$

[(L4), (L5), (L6)]

(L9) $m_0 > 0$

[$m_0 = q/\check{\gamma}^2_{\mathrm{hyb}} - E_{00}$ (Definition A.37, item 1); $E_{00} < q/\check{\gamma}^2_{\mathrm{hyb}}$ (the statement's measured row)]

(L10) $\forall \psi :\ d_{11}(\psi) \in [q^2/M_0, q^2/m_0]$

[(L4), (L5), (L7), (L9); Fact A.41, item 5: $t \mapsto 1/t$ nonincreasing on $(0, \infty)$]

(L11) $\forall \psi :\ d_{00}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$

[(L8); $d_{\mathrm{lo}} = \min(m_0, q^2/M_0)$, $d_{\mathrm{hi}} = \max(M_0, q^2/m_0)$ (Definition A.37, items 3 and 4)]

(L12) $\forall \psi :\ d_{11}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$

[(L10); $d_{\mathrm{lo}} = \min(m_0, q^2/M_0)$, $d_{\mathrm{hi}} = \max(M_0, q^2/m_0)$ (Definition A.37, items 3 and 4)]

(L13) $d_{\mathrm{lo}} > 0$

[(L4), (L9); $d_{\mathrm{lo}} = \min(m_0, q^2/M_0)$ (Definition A.37, item 3)]

(L14) $[d_{\mathrm{lo}}, d_{\mathrm{hi}}] \subseteq (0, \infty)$

[(L13)]

(L15) $\mathcal{G} \in \mathrm{Gram}_n$

[$g_{00} > 0$, $g_{00} g_{11} - |g_{01}|^2 = q^2$, $q^2 > 0$ (Fact A.33, items 3 and 2); Definition A.14]

(L16) $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d^\nu_{00}(\psi) = g^\nu_{00}(\psi)$

[d^ν_{00} (Proposition G.38); g^ν_{00} (the proof's block)]

(I1)

Lemma D.5	This proof
Shared: T, g^ν_{00}	
$\mathcal{G}$	$\mathcal{G}$ (the statement)
I	$[d_{\mathrm{lo}}, d_{\mathrm{hi}}]$
d^ν_{11}	d^ν_{11} (the statement; Proposition G.38)
$n \in \{512, 1024\}$	Definition 5.5, item 1
$\mathcal{G} \in \mathrm{Gram}_n$	(L15)
$I \subseteq (0, \infty)$	(L14); $[d_{\mathrm{lo}}, d_{\mathrm{hi}}]$, an interval
Assumption A1	(L11), (L16) at $\nu := T$; $d_{00} = d^T_{00}$ (the proof's block)
Assumption A2	(L12); $d_{11} = d^T_{11}$ (the proof's block)
Its item 1: $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ g^\nu_{00}(\psi) \in I$	
Its item 2: $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d^\nu_{11}(\psi) \in I$	

(L17) $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ g^\nu_{00}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$

[item 1 of (I1)]

(L18) $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi :\ d^\nu_{11}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$

[item 2 of (I1)]

(L19) $\Rightarrow\ \forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi :\ d^\nu_j(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$

[(L16), (L17), (L18)]

(L20) $\Rightarrow$ item 1

[(L19)]

	Proposition G.38 at every $k \in \{1, \dots, h-1\}$	This proof
	Shared: $h, n,\ k$	
(I2)	$\mathcal{G}$	$\mathcal{G}$ (the statement)
	$h \geq 1$	$n \in \{512, 1024\}$ (Definition 5.5, item 1)
	$\mathcal{G} \in \mathrm{Gram}_n,\ n := 2^h$	(L15); $n = 2^h$ (the statement)
	$k \in \{1, \dots, h-1\}$	The scope
	Its conclusion: $\kappa_k \leq (\varsigma_k - 1)^2/(4\varsigma_k)$	

(L21) $\forall k \in \{1, \dots, h-1\} :\ \kappa_k \leq (\varsigma_k - 1)^2/(4\varsigma_k)$

[(I2)]

(L22) $\forall k \in \{1, \dots, h-1\} :\ \varsigma_k \geq 1$

[ς_k (Proposition G.38), a maximum of the ratios $\max_\psi d_j^\pi(\psi)/\min_\psi d_j^\pi(\psi)$; (L19), (L13)]

(L23) $\forall k \in \{1, \dots, h-1\} :\ \varsigma_k \leq \bar{\varsigma}$

[(L19); ς_k (Proposition G.38); $\bar{\varsigma} = d_{\mathrm{hi}}/d_{\mathrm{lo}}$ (Definition A.37, item 5)]

(L24) $\forall x > 0 :\ (x-1)^2/(4x) = (x - 2 + 1/x)/4$

[expand]

(L25) $x \mapsto (x-1)^2/(4x)$ is nondecreasing on $[1, \infty)$

[(L24); Fact A.41, item 5]

(L26) $\Rightarrow\ \forall k \in \{1, \dots, h-1\} :\ \kappa_k \leq (\bar{\varsigma} - 1)^2/(4\bar{\varsigma})$

[(L21), (L22), (L23), (L25)]

(L27) $\Rightarrow$ item 2

[(L26)]

□ (items 1 and 2)

Proof of item 3.

(L28) $\forall \psi \in \Psi_n :\ |g_{01}(\psi)| \leq |\widetilde{g}_{01}(\psi)| + E_{01}$

[(L1); Fact A.41, item 1: $|x+y| \leq |x| + |y|$]

(L29) $\forall \psi \in \Psi_n :\ |\widetilde{g}_{01}(\psi)| \leq \check{\gamma}_{\mathrm{root}} \widetilde{g}_{00}(\psi)$

[Lemma H.17, item 4, at the checked key (the statement)]

(L30) $\Rightarrow\ \forall \psi :\ |g_{01}(\psi)| \leq \check{\gamma}_{\mathrm{root}}\, q \check{\gamma}_{\mathrm{hyb}}^2 + E_{01}$

[(L28), (L29), (L3); (L5)]

(L31) $\kappa_{\mathrm{root}} = \max_\psi |g_{01}|^2/q^2$

[Fact A.33, item 6]

(L32) $\Rightarrow\ \kappa_{\mathrm{root}} \leq (\check{\gamma}_{\mathrm{root}}\, q \check{\gamma}_{\mathrm{hyb}}^2 + E_{01})^2/q^2$

[(L30), (L31); Fact A.41, item 5: $t \mapsto t^2$ nondecreasing on $[0, \infty)$]

(L33) $\Rightarrow$ item 3

[(L32)]

□ (item 3)

Proof of item 4.

(L34) $\forall \psi :\ |l_{10}(\psi)| = |g_{01}(\psi)|/g_{00}(\psi)$

[Lemma D.4, items 3 and 1: $l_{10} d_{00} = \mathrm{conj}\, g_{01}$, $d_{00} = g_{00}$; Fact A.41, item 1: $|\mathrm{conj}\, x| = |x|$, $|xy| = |x||y|$]

(L35) $\forall \psi \in \Psi_n :\ \widetilde{g}_{00}(\psi) - E_{00} \geq m_0$

[(L3); $m_0 = q/\check{\gamma}_{\mathrm{hyb}}^2 - E_{00}$ (Definition A.37, item 1)]

(L36) $\Rightarrow\ \forall \psi \in \Psi_n :\ |l_{10}(\psi)| \leq \frac{\check{\gamma}_{\mathrm{root}} \widetilde{g}_{00}(\psi) + E_{01}}{\widetilde{g}_{00}(\psi) - E_{00}}$

[(L2), (L9), (L28), (L29), (L34), (L35)]

(L37) $\forall \psi \in \Psi_n :\ \frac{\check{\gamma}_{\mathrm{root}} \widetilde{g}_{00}(\psi)}{\widetilde{g}_{00}(\psi) - E_{00}} = \frac{\check{\gamma}_{\mathrm{root}}}{1 - E_{00}/\widetilde{g}_{00}(\psi)}$

[divide by $\widetilde{g}_{00} > 0$ (L3)]

(L38) $\forall \psi \in \Psi_n :\ E_{00}/\widetilde{g}_{00}(\psi) \leq E_{00} \check{\gamma}_{\mathrm{hyb}}^2/q$

[(L3); Fact A.41, item 5: $t \mapsto 1/t$ nonincreasing on $(0, \infty)$]

(L39) $E_{00}\check{\gamma}_{\mathrm{hyb}}^2/q < 1$

[$E_{00} < q/\check{\gamma}_{\mathrm{hyb}}^2$ (the statement's measured row)]

(L40) $\forall \psi \in \Psi_n : \ \frac{\check{\gamma}_{\mathrm{root}}}{1-E_{00}/\widetilde{g}_{00}(\psi)} \le \frac{\check{\gamma}_{\mathrm{root}}}{1-E_{00}\check{\gamma}_{\mathrm{hyb}}^2/q}$

[(L38), (L39); Fact A.41, item 5: $t \mapsto 1/t$ nonincreasing on $(0,\infty)$]

(L41) $\forall \psi \in \Psi_n : \ \frac{E_{01}}{\widetilde{g}_{00}(\psi)-E_{00}} \le \frac{E_{01}}{m_0}$

[(L9), (L35); Fact A.41, item 5: $t \mapsto 1/t$ nonincreasing on $(0,\infty)$]

(L42) $\Rightarrow \ \max_\psi |l_{10}| \le \check{\gamma}_{\mathrm{root}}/(1 - E_{00}\check{\gamma}_{\mathrm{hyb}}^2/q) + E_{01}/m_0$

[(L36), (L37), (L40), (L41); (L34), (L5)]

(L43) $\Rightarrow$ item 4

[(L42)]

□ (item 4)

Proof of items 5, 6 and 7.

(L44) $\mathcal{G}_\nu(\psi') = \begin{pmatrix} d_0 & d_1 \\ \mathrm{conj}\, d_1 & d_0 \end{pmatrix}$

[$\mathcal{G}_\nu = \mathcal{G}_d$ (the proof's block); $\mathcal{G}_d$ (Definition A.23) at $\psi' = \psi^2$; (d_0, d_1) (the proof's block)]

Proposition 5.8, item 1 at ψ and at $-\psi$	This proof
Shared: $T,\ d_{\mathrm{lo}}, d_{\mathrm{hi}}$	
ν	π
d_j^ν	d
(I3) $\nu \in \mathrm{Sub}(T)$	π (the proof's block)
$j \in \{00, 11\}$	$d \in \{d_{00}^\pi, d_{11}^\pi\}$ (the proof's block)
$\psi, -\psi \in Z_{2m'}$	$\psi \in \Psi_{2m'}$ (the proof's block); Fact A.43, items 2 and 3, at $2m'$
Its conclusion: $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00,11\}\ \forall \psi : \ d_j^\nu(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$	

(L45) $a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$

[(I3); a, b (the proof's block)]

(L46) $a, b > 0$

[(L45), (L13)]

Fact D.1	This proof
Shared: $d,\ \psi,\ a, b, d_0, d_1$	
m	$2m'$ (the proof's block)
$m \in \{2^k : k \ge 1\}$	$m' = n/2^k$ (the proof's block)
$d \in \mathcal{R}_m$	$d \in \{d_{00}^\pi, d_{11}^\pi\}$, π of degree $2m'$ (the proof's block)
(I4) $\psi^m = -1$	$\psi \in \Psi_{2m'}$ (the proof's block)
Assumption A1	(L46)
Assumption A2	(L46)
Its item 1: $d_0 = \mathrm{AM}(a, b)$	
Its item 3: $\lvert d_1\rvert = \lvert a - b\rvert/2$	

(L47) $d_0 = \mathrm{AM}(a, b)$

[item 1 of (I4)]

(L48) $|d_1| = |a - b|/2$

[item 3 of (I4)]

(L49) $\lambda_\pm = d_0 \pm |d_1|$

[Fact A.44, item 2, at $\mathcal{G} := \mathcal{G}_\nu(\psi')$, $g_{00} := d_0$ and $g_{11} := d_0$ by (L44)]

(L50) $d_0 + |d_1| = \max(a, b)$

[(L47), (L48); $\mathrm{AM}(a, b) = (a + b)/2$ (Definition A.46)]

(L51) $d_0 - |d_1| = \min(a, b)$

[(L47), (L48); $\mathrm{AM}(a, b) = (a + b)/2$ (Definition A.46)]

(L52) $\Rightarrow\ \lambda_+ \le d_{\mathrm{hi}}$

[(L45), (L49), (L50)]

(L53) $\Rightarrow\ \lambda_- \ge d_{\mathrm{lo}}$

[(L45), (L49), (L51)]

(L54) $\forall i \in I(\nu):\ d_i \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$

[item 1 ((L19)): each d_i a diagonal of a node of degree 2 of T (Definition A.19; Definition A.20, item 2)]

(L55) $d_0^2 - |d_1|^2 = \max(a,b)\min(a,b)$

[(L50), (L51); expand]

(L56) $\max(a,b)\min(a,b) \ge d_{\mathrm{lo}}^2$

[(L45), (L13)]

(L57) $d_0 > 0$

[(L46), (L47); $\mathrm{AM}(a,b) = (a+b)/2$ (Definition A.46)]

(L58) $d_0^2 - |d_1|^2 > 0$

[(L55), (L56), (L13)]

(L59) $\mathcal{G}_\nu \in \mathrm{Gram}_{m'}$

[(L44), (L57), (L58), $\forall\psi'$; Definition A.14]

(L60) $\nu = \mathrm{ffLDL}^\dagger(\mathcal{G}_\nu)$

[Definition A.32]

	Lemma H.20	This proof
	m	m' (the proof's block)
	$\mathcal{G}$	$\mathcal{G}_\nu$ (the proof's block)
	$\lambda_{\mathrm{lo}}, \lambda_{\mathrm{hi}}, d_{\mathrm{lo}}, d_{\mathrm{hi}}$	$d_{\mathrm{lo}}, d_{\mathrm{hi}}, d_{\mathrm{lo}}, d_{\mathrm{hi}}$ (the statement)
	T	ν (L60)
	$\lambda_\pm$	$\lambda_\pm$ (the proof's block)
	$m = 2^{h'},\ h' \ge 1$	$m' = n/2^k,\ k \le h-1$ (the proof's block)
	$\mathcal{G} \in \mathrm{Gram}_m$	(L59)
	$\lambda_{\mathrm{lo}} > 0$	(L13)
(I5)	$\lambda_{\mathrm{hi}} > 0$	(L13), (L45)
	$d_{\mathrm{lo}} > 0$	(L13)
	$d_{\mathrm{hi}} > 0$	(L13), (L45)
	Assumption A1	(L53), $\forall\psi'$
	Assumption A2	(L52), $\forall\psi'$
	Assumption A3	(L54)
	Assumption A4	(L54)
	Its item 1: $\|\mathcal{L}_T\| \le (\lambda_{\mathrm{hi}}/d_{\mathrm{lo}})^{1/2}$	
	Its item 2: $\|\mathcal{L}_T^{-1}\| \le (d_{\mathrm{hi}}/\lambda_{\mathrm{lo}})^{1/2}$	

(L61) $\|\mathcal{L}_\nu\| \le (d_{\mathrm{hi}}/d_{\mathrm{lo}})^{1/2}$

[item 1 of (I5)]

(L62) $\|\mathcal{L}_\nu^{-1}\| \le (d_{\mathrm{hi}}/d_{\mathrm{lo}})^{1/2}$

[item 2 of (I5)]

(L63) $(d_{\mathrm{hi}}/d_{\mathrm{lo}})^{1/2} = \bar{\varsigma}^{1/2}$

[$\bar{\varsigma} = d_{\mathrm{hi}}/d_{\mathrm{lo}}$ (Definition A.37, item 5)]

(L64) $\bar{\varsigma} \ge 1$

[(L45), (L13), (L63)]

(L65) $\forall k \in \{1,\dots,h-1\}:\ \Xi'_k \le \bar{\varsigma}^{1/2}$

[(L61), (L63) at every ν of depth k; $\Xi'_k := \max_{\mathrm{depth}(\nu)=k}\|\mathcal{L}_\nu\|$ (Definition 4.6)]

(L66) $\Rightarrow\ \Xi' \le \bar{\varsigma}^{1/2}$

[(L64), (L65); $\Xi' := \max(\{1\} \cup \{\Xi'_k : 1 \le k \le h-1\})$ (Definition 4.6); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L67) $\Rightarrow$ item 5

[(L66)]

(L68) $\forall k \in \{1, \dots, h-1\}: \ \Xi_k \le \bar{\varsigma}^{1/2}$

[(L62), (L63) at every ν of depth k; $\Xi_k := \max_{\mathrm{depth}(\nu)=k} \|\mathcal{L}_\nu^{-1}\|$ (Definition 4.6)]

(L69) $\Rightarrow \ \Xi \le \bar{\varsigma}^{1/2}$

[(L64), (L68); $\Xi := \max(\{1\} \cup \{\Xi_k : 1 \le k \le h-1\})$ (Definition 4.6); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L70) $\Rightarrow$ item 6

[(L69)]

(L71) $|l_{10}^\nu(\psi')| = |d_1|/d_0$

[$l_{10} := \mathrm{conj}\, g_{01}/g_{00}$ (Definition A.17) at $\mathcal{G}_\nu(\psi')$ (L44); $|\mathrm{conj}\, x| = |x|$, $|x/y| = |x|/|y|$ (Fact A.41, item 1); (L57)]

(L72) $|d_1|/d_0 = |a-b|/(a+b)$

[(L47), (L48); $\mathrm{AM}(a,b) = (a+b)/2$ (Definition A.46)]

(L73) $|a-b| \le a+b$

[(L46); $|x+y| \le |x| + |y|$ (Fact A.41, item 1)]

(L74) $\Rightarrow \ |l_{10}^\nu(\psi')| \le 1$

[(L71), (L72), (L73); $a+b > 0$ by (L46)]

(L75) $\Rightarrow \ \ell \le \max(1, \ \check{\gamma}_{\mathrm{root}}/(1 - E_{00}\check{\gamma}_{\mathrm{hyb}}^2/q) + E_{01}/m_0)$

[(L74), $\forall k \in \{1, \dots, h-1\}$ $\forall \nu$, $\mathrm{depth}(\nu) = k$ $\forall \psi'$; item 4 ((L42)) at the root node; $\ell := \max_\psi |l_{10}|$ over the nodes (Definition 4.6)]

(L76) $\Rightarrow$ item 7

[(L75)]

□ (items 5, 6 and 7)

Proof of item 8.

(L77) $\Rightarrow$ item 8

[(L9)]

□ (item 8)

Lemma H.21 (The norms of the root's tree map [to table])**.** *The passed checks bound the norms of the root's tree map and of its inverse. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5) of degree* n*;*
- h *with* $n = 2^h$*, as* FFT *(Algorithm 14) takes them (Precondition).*

Define:

- g_{00}*,* g_{01}*,* g_{11}*, the exact Gram matrix entries,* keychecks *(Algorithm 12), line 4;*
- $\mathcal{G} := \begin{pmatrix} g_{00} & g_{01} \\ \mathrm{conj}\, g_{01} & g_{11} \end{pmatrix}$ *(Proposition 5.8);*
- $T := \mathrm{ffLDL}^\dagger(\mathcal{G})$ *(Proposition 5.8);*
- $\check{\gamma}_{\mathrm{hyb}}$*,* E_{00} *and* γ'_{FG}*, those of Definition A.37;*
- $m_0 := q/\check{\gamma}_{\mathrm{hyb}}^2 - E_{00}$ *(Definition A.37);*
- $M_0 := q\check{\gamma}_{\mathrm{hyb}}^2 + E_{00}$ *(Definition A.37);*
- $\bar{g}_{11} := 2\gamma'^2_{FG}$ *(Definition A.37);*
- $d_{\mathrm{lo}} := \min(m_0, q^2/M_0)$ *(Definition A.37);*
- $d_{\mathrm{hi}} := \max(M_0, q^2/m_0)$ *(Definition A.37);*
- $\Xi_0 := \|\mathcal{L}_T^{-1}\|$ *(Definition 4.6 at* $k = 0$*);*
- $\Xi'_{\mathrm{root}} := \|\mathcal{L}_T\|$ *(Definition 4.6);*
- $\bar{\Xi}_0 := (d_{\mathrm{hi}}(M_0 + \bar{g}_{11}))^{1/2}/q$*;*
- $\bar{\Xi}'_{\mathrm{root}} := ((M_0 + \bar{g}_{11})/d_{\mathrm{lo}})^{1/2}$*.*

Then the root's tree map and its inverse are bounded:

1. $\Xi_0 \le \bar{\Xi}_0$*;*

2. $\Xi'_{\mathrm{root}} \in [1, \bar{\Xi}'_{\mathrm{root}}]$.

Proof.

DEFINES $N := 2n$

d_i, $i \le N$, the leaf diagonals of T (Definition A.19)

(g_{00}, g_{01}, g_{11}), the entries of $\mathcal{G}(\psi)$, $\psi \in \mathbb{C}$ with $\psi^n = -1$

$\lambda_\pm := (g_{00} + g_{11})/2 \pm (((g_{00} - g_{11})/2)^2 + |g_{01}|^2)^{1/2}$ (Fact A.44)

DEFINES Ψ_n and Z_n, those of Fact A.43 at $m := n$

(L1) $\forall i \le N : \ d_i \le d_{\mathrm{hi}}$

[Proposition 5.8, item 1: each d_i a diagonal of a node of degree 2 (Definition A.19; Definition A.20, item 2), at the checked key (the statement)]

(L2) $\forall i \le N : \ d_i \ge d_{\mathrm{lo}}$

[Proposition 5.8, item 1: each d_i a diagonal of a node of degree 2 (Definition A.19; Definition A.20, item 2), at the checked key (the statement)]

(L3) $\forall \psi : \ \lambda_+(\psi)\lambda_-(\psi) = g_{00}g_{11} - |g_{01}|^2$

[$\lambda_\pm$, the two roots of $(\lambda - g_{00})(\lambda - g_{11}) = |g_{01}|^2$ (Fact A.44, item 2): the product of the roots]

(L4) $\forall \psi : \ g_{00}g_{11} - |g_{01}|^2 = q^2$

[Fact A.33, item 2]

(L5) $q > 0$

[$q = 12289$ (the statement)]

(L6) $\forall \psi \in Z_n \ \exists \psi' \in \Psi_n : \ (g_{00}(\psi), g_{11}(\psi)) = (g_{00}(\psi'), g_{11}(\psi'))$

[$Z_n = \Psi_n \sqcup \operatorname{conj} \Psi_n$ (Fact A.43, item 2, at $m := n$); $g_{00}(\operatorname{conj} \psi) = \operatorname{conj} g_{00}(\psi)$ and $g_{11}(\operatorname{conj} \psi) = \operatorname{conj} g_{11}(\psi)$, $g_{00}, g_{11} \in \mathcal{R}_n$ (Fact A.42, item 2, at $m := n$); $g_{00}(\psi), g_{11}(\psi) \in \mathbb{R}$ (Fact A.33)]

(L7) $\forall \psi : \ g_{00} > 0$

[$g_{00} \ge m_0$ (Lemma H.19, item 4, at every $\psi' \in \Psi_n$); (L6); $m_0 > 0$ (Proposition 5.8, item 8), at the checked key (the statement)]

(L8) $\forall \psi : \ g_{11} \ge 0$

[$g_{11} = |F(\psi)|^2 + |G(\psi)|^2$ (Fact A.33)]

(L9) $\forall \psi : \ \lambda_-(\psi) \ge 0$

[Fact A.44, item 4, by (L4), (L7), (L8)]

(L10) $\forall \psi : \ \lambda_+(\psi) \le g_{00} + g_{11}$

[Fact A.44, item 4, by (L4), (L7), (L8)]

(L11) $\forall \psi : \ g_{00} + g_{11} \le M_0 + \bar{g}_{11}$

[Lemma H.19, items 4 and 5, at the checked key (the statement) and at every $\psi' \in \Psi_n$; (L6)]

(L12) $\Rightarrow \ \forall \psi : \ \lambda_+(\psi) \le M_0 + \bar{g}_{11}$

[(L10), (L11)]

(L13) $\forall \psi : \ \lambda_+(\psi)\lambda_-(\psi) > 0$

[(L3), (L4), (L5)]

(L14) $\Rightarrow \ \forall \psi : \ \lambda_+(\psi) > 0$

[(L9), (L13)]

(L15) $\forall \psi : \ \lambda_-(\psi) = q^2/\lambda_+(\psi)$

[(L3), (L4), (L14)]

(L16) $\Rightarrow \ \forall \psi : \ \lambda_-(\psi) \ge q^2/(M_0 + \bar{g}_{11})$

[(L12), (L14), (L15); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L17) $M_0 + \bar{g}_{11} > 0$

[(L7), (L8), (L11)]

(L18) $d_{\mathrm{lo}} > 0$

[Proposition 5.8, (L13)]

(L19) $d_{\mathrm{lo}} \le d_{\mathrm{hi}}$

[(L1), (L2) at $i := 1$]

(L20) $\mathcal{G} \in \mathrm{Gram}_n$

[(L4), (L5), (L7); Definition A.14]

Lemma H.20	This proof
m, h'	n, h (the statement)
$\mathcal{G}$	$\mathcal{G}$ (the statement)
$\lambda_{\mathrm{lo}}, \lambda_{\mathrm{hi}}, d_{\mathrm{lo}}, d_{\mathrm{hi}}$	$q^2/(M_0+\bar{g}_{11}), M_0+\bar{g}_{11}, d_{\mathrm{lo}}, d_{\mathrm{hi}}$ (the statement)
T	T (Proposition 5.8)
$d_i, \lambda_\pm$	$d_i, \lambda_\pm$ (the proof's block)
$\|\mathcal{L}_T^{-1}\|, \|\mathcal{L}_T\|$	$\Xi_0, \Xi'_{\mathrm{root}}$ (the statement)
$m = 2^{h'},\ h' \geq 1$	$n = 2^h$ (the statement); $n \in \{512, 1024\}$ (Definition 5.5, item 1)
$\mathcal{G} \in \mathrm{Gram}_m$	(L20)
(I1) $\lambda_{\mathrm{lo}} > 0$	(L5), (L17)
$\lambda_{\mathrm{hi}} > 0$	(L17)
$d_{\mathrm{lo}} > 0$	(L18)
$d_{\mathrm{hi}} > 0$	(L18), (L19)
Assumption A1	(L16)
Assumption A2	(L12)
Assumption A3	(L2)
Assumption A4	(L1)
Its item 1: $\|\mathcal{L}_T\| \leq (\lambda_{\mathrm{hi}}/d_{\mathrm{lo}})^{1/2}$	
Its item 2: $\|\mathcal{L}_T^{-1}\| \leq (d_{\mathrm{hi}}/\lambda_{\mathrm{lo}})^{1/2}$	

(L21) $\Xi_0 \leq \left(d_{\mathrm{hi}}/(q^2/(M_0+\bar{g}_{11}))\right)^{1/2}$

[item 2 of (I1)]

(L22) $d_{\mathrm{hi}}/(q^2/(M_0+\bar{g}_{11})) = d_{\mathrm{hi}}(M_0+\bar{g}_{11})/q^2$

[(L5), (L17)]

(L23) $\Rightarrow\ \Xi_0 \leq \bar{\Xi}_0$

[(L21), (L22); $\bar{\Xi}_0$ (the statement)]

(L24) $\Rightarrow$ item 1

[(L23)]

(L25) $\Xi'_{\mathrm{root}} \leq ((M_0+\bar{g}_{11})/d_{\mathrm{lo}})^{1/2}$

[item 1 of (I1)]

(L26) $\Rightarrow\ \Xi'_{\mathrm{root}} \leq \bar{\Xi}'_{\mathrm{root}}$

[(L25); $\bar{\Xi}'_{\mathrm{root}}$ (the statement)]

(L27) $\exists x \in \mathcal{R}_n^2 :\ x_N = 1,\ \forall i < N :\ x_i = 0$

[Fact G.7, item 4, at $T' := T$]

(L28) $\|x\| = 1$

[(L27); $x_i := (x_{c_{i,1}})_{[p_i]}$ (Definition G.6) at $T' := T$, a bijection onto the coefficients of x (Fact G.7, item 4); $\|x\|$, the coefficient norm (Definition A.1)]

(L29) $\forall i \leq N :\ (x\mathcal{L}_T)_i = x_i$

[Lemma G.11; (L27)]

(L30) $\|x\mathcal{L}_T\| = 1$

[(L27), (L29); $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead)]

(L31) $\|\mathcal{L}_T\| = \max_{x \neq 0} \|x\mathcal{L}_T\|/\|x\|$

[Definition 4.6, item 7, at $A := \mathcal{L}_T$]

(L32) $\Rightarrow\ \Xi'_{\mathrm{root}} \geq 1$

[(L28), (L30), (L31); $\Xi'_{\mathrm{root}} = \|\mathcal{L}_T\|$ (the statement)]

(L33) $\Rightarrow\ \Xi'_{\mathrm{root}} \in [1, \bar{\Xi}'_{\mathrm{root}}]$

[(L26), (L32)]

(L34) $\Rightarrow$ item 2

[(L33)]

□ (items 1 and 2)

Lemma H.22 (The norm of the center t [to table])**.** *The passed checks bound the norm of the center t of every hashed message. Let:*

- *(f, g, F, G) be a checked key (Definition 5.5) of degree n;*
- *h with $n = 2^h$, as FFT (Algorithm 14) takes them (Precondition);*
- *$\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ be a hashed message (Definition A.25).*

Define:

- *$t := (t_0, t_1)$, that of ffSampling$^{\mathcal{F}}$ (Algorithm 10) at $\mathsf{h}(\mathsf{m})$, lines 9 to 19;*
- *$\check{\gamma}_{fg}$, $\check{\gamma}_{FG}$, δ_{fg} and δ_{FG}, those of Definition A.36;*
- *$\gamma'_{fg} := \check{\gamma}_{fg} + \delta_{fg}$ and $\gamma'_{FG} := \check{\gamma}_{FG} + \delta_{FG}$ (Definition A.36);*
- *$\forall a \in \mathbb{R}[x]/(x^n+1) : \ \|a\| := (\sum_{i<n} a_{[i]}^2)^{1/2}$ (Definition A.1);*
- *$\bar{T} := (n(\gamma'^2_{FG} + \gamma'^2_{fg}))^{1/2}$.*

Then

$$\|t\| \le \bar{T}.$$

Proof.

DEFINES $\hat{f}$ and $\hat{F}$, the exact images, keychecks (Algorithm 12), line 2

DEFINES $\hat{h}$, that of ffSampling$^{\mathcal{F}}$ (Algorithm 10) at $\mathsf{h}(\mathsf{m})$, line 10

DEFINES Ψ_n and Z_n, those of Fact A.43 at $m := n$

(L1) $\forall \psi : \ t_0(\psi) = \hat{h}(\psi)(-\hat{F}(\psi))(1/q)$

[line 17 of ffSampling$^{\mathcal{F}}$ (Algorithm 10)]

(L2) $\forall \psi : \ t_1(\psi) = (-\hat{f}(\psi))\hat{h}(\psi)(-1/q)$

[line 19 of ffSampling$^{\mathcal{F}}$]

(L3) $\forall \psi \in \Psi_n : \ |\hat{F}(\psi)| \le \gamma'_{FG}$

[Lemma H.18, item 2, at the checked key (the statement) and at every $\psi \in \Psi_n$ (the proof's block)]

(L4) $\forall \psi \in \Psi_n : \ |\hat{f}(\psi)| \le \gamma'_{fg}$

[Lemma H.18, item 1, at the checked key (the statement) and at every $\psi \in \Psi_n$ (the proof's block)]

(L5) $\forall \psi \in \Psi_n : \ |t_0(\psi)|^2 + |t_1(\psi)|^2 \le (\gamma'^2_{FG} + \gamma'^2_{fg})|\hat{h}(\psi)|^2/q^2$

[(L1) to (L4); $|xy| = |x||y|$ (Fact A.41, item 1); $t \mapsto t^2$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

Proposition G.15 at $f := t_0$ and at $f := t_1$	This proof
Shared: n, h	
(I1) f	t_0, t_1
$h \ge 1$	$n \in \{512, 1024\}$ (Definition 5.5, item 1)
$f \in \mathbb{R}[x]/(x^n+1)$	t (ffSampling$^{\mathcal{F}}$ (Algorithm 10), lines 9 to 19)
Its conclusion: $\sum_{p<n} f_{[p]}^2 = \frac{2}{n}\sum_{k<n/2}\lvert f(\psi_k)\rvert^2$	

(L6) $\|t\|^2 = \frac{2}{n}\sum_{\psi \in \Psi_n}(|t_0(\psi)|^2 + |t_1(\psi)|^2)$

[(I1); $\Psi_n = \{\psi \in Z_n : \operatorname{Im}\psi > 0\}$ (Fact A.43, item 2, at $m := n$); $\|(X, Y)\|^2 := \|X\|^2 + \|Y\|^2$ (Fact A.41, its lead)]

Proposition G.15 at $f := \mathsf{h}(\mathsf{m})$	This proof
Shared: n, h	
(I2) f	$\mathsf{h}(\mathsf{m})$
$h \ge 1$	$n \in \{512, 1024\}$ (Definition 5.5, item 1)
$f \in \mathbb{R}[x]/(x^n+1)$	$\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ (the statement)
Its conclusion: $\sum_{p<n} f_{[p]}^2 = \frac{2}{n}\sum_{k<n/2}\lvert f(\psi_k)\rvert^2$	

(L7) $\sum_{\psi \in \Psi_n}|\hat{h}(\psi)|^2 = (n/2)\|\mathsf{h}(\mathsf{m})\|^2$

[(I2); $\Psi_n = \{\psi \in Z_n : \operatorname{Im}\psi > 0\}$ (Fact A.43, item 2, at $m := n$); $\hat{h} = \mathrm{FFT}(\mathsf{h}(\mathsf{m}))$ (ffSampling$^{\mathcal{F}}$, line 10)]

(L8) $\|t\|^2 \le (\gamma'^2_{FG} + \gamma'^2_{fg})\|\mathsf{h}(\mathsf{m})\|^2/q^2$

[(L5), (L6), (L7)]

(L9) $\|\mathsf{h}(\mathsf{m})\|^2 \le nq^2$

[$\mathsf{h}(\mathsf{m}) \in \{0,\dots,q-1\}^n$ (the statement)]

(L10) $\Rightarrow$ $\|t\|^2 \le n(\gamma'^2_{FG} + \gamma'^2_{fg})$

[(L8), (L9)]

(L11) $\Rightarrow$ $\|t\| \le \bar{T}$

[(L10); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5); $\bar{T}$ (the statement)]

(L12) $\Rightarrow$ the statement

[(L11)]

□

Lemma H.23 (Sample norms on the tail-cut event [to table])**.** *On the tail-cut event, the sample's norm is at most $\bar{Z}$, from bounds on the center's norm, its shift at the root node's entry, the leaves' standard deviations and the inverse tree map. Let:*

- *$\mathcal{F}$ be a realization at (u,ζ) (Definition A.4);*
- *$h \ge 1$;*
- *$T \in \mathcal{T}_n$ at $n := 2^h$;*
- *$t \in \mathcal{R}_n \times \mathcal{R}_n$;*
- *$\bar{T} \in [0,\infty)$;*
- *$\bar{e} \in [0,\infty)$;*
- *$\bar{\sigma} \in [0,\infty)$;*
- *$\bar{\Xi}_0 \in [0,\infty)$;*
- *$\bar{\delta} \in [0,\infty)$.*

Define:

- *The signer's words and parameters*
  - *$N := 2n$;*
- *The key constants*
  - *$\Xi_0 := \|\mathcal{L}_T^{-1}\|$, that of Definition 4.6, item 9, at T and $k = 0$;*
  - *Ξ, Ξ'_{root} and Ξ'_k, those of Definition 4.6, items 13, 10 and 8, at T;*
- *The centers and the samples*
  - *$\widetilde{t}_T$, σ_i, $\widetilde{\sigma}_i$ and $\widetilde{t}_i$, $i \le N$, those of Corollary G.62;*
  - *$\widetilde{t} := (\widetilde{t}_i)_{i \le N}$;*
  - *$z' := (z_0, z_1)$, the sample* ffsamp *(Algorithm 6) returns at t (*ffSampling$^{\mathcal{F}}$ *(Algorithm 10), line 24), the sample z read as a pair;*
- *The tail-cut event*
  - *$\tau > 1$, the radius of the tail-cut event (Definition A.26);*
  - *$S := \{\, z \in \mathbb{Z}^N : \forall i \le N \ |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$ (Definition A.26);*
- *The center shifts*
  - *γ, γ_S, c_{split}, G_X, G_Z, M_k, Θ_k and Υ_k, those of Corollary G.62 at $\bar{\delta}$;*
  - *$R^\circ := \sqrt{2}\,\Xi\tau\bar{\sigma}(1+\bar{\delta})(n/2)^{1/2}$;*
- *The terms*
  - *$D_0^\circ := \Xi'_{\mathrm{root}}\bar{e} + \sum_{k=1}^h \Xi'_k[(c_{\mathrm{split}} + G_X)\bar{T} + \Upsilon_k R^\circ + \Theta_k]$;*
  - *$D_Z^\circ := \sum_{k=1}^h \Xi'_k G_Z M_k$;*
  - $\bar{Z} := \dfrac{\bar{T} + \bar{\Xi}_0\left(\tau\bar{\sigma}(1+\bar{\delta})\sqrt{N} + D_0^\circ/(1-\gamma-\gamma_S)\right)}{1 - \bar{\Xi}_0 D_Z^\circ/(1-\gamma-\gamma_S)}$.

Assume:

(A1) $\|t\| \le \bar{T}$;

(A2) $\|\widetilde{t}_T - t\| \le \bar{e}$;

(A3) $\forall i \le N\ \exists\, \delta_i \in \mathbb{R},\ |\delta_i| \le \bar{\delta} :\ \widetilde{\sigma}_i = \sigma_i(1+\delta_i)$;

13849 *(A4)* $\forall i \le N:\ \sigma_i \le \bar\sigma$;
13850 *(A5)* $\Xi_0 \le \bar\Xi_0$;
13851 *(A6)* $\gamma + \gamma_S < 1$;
13852 *(A7)* $\bar\Xi_0 D^\circ_Z < 1 - \gamma - \gamma_S$.
13853 *Then*
13854 $$\forall z \in S:\ \|z'\| \le \bar Z.$$

13855 *Proof.*
DEFINES $c = (c_i)_{i\le N}$, the leaf centers with the sample z' (Proposition G.48)
13856 $\sigma_{\max} = \max_i \sigma_i$ (Corollary G.62)
$R^\circ_{\max}$ and D°, those of Corollary G.62 at $\bar\delta$, $\bar T$, $e_{\text{root}} := \widetilde t_T - t$ and $Z := \|z'\|$

Proposition G.48, item 2 at every $z \in S$	This proof
Shared: $T,\ t,\ c$	
13857 (I1) z	z' (the statement)
$t \in \mathcal{R}_n \times \mathcal{R}_n$	t (the statement)
$z \in \mathbb{Z}^N$	z', a sample of ffSampling(t, T) (the statement)
Its conclusion: $t - z = (c - z)\mathcal{L}_T^{-1}$	

13858 (L1) $\forall z \in S:\ t - z' = (c - z')\mathcal{L}_T^{-1}$
13859 [(I1)]
13860 (L2) $\forall z \in S:\ \|z'\| \le \|t\| + \Xi_0\|c - z'\|$
13861 [(L1); $\|x + y\| \le \|x\| + \|y\|$ (Fact A.41, item 3); $\|y\mathcal{L}_T^{-1}\| \le \Xi_0\|y\|$ (Definition 4.6, items 7 and 9, at T)]
13862 (L3) $\Rightarrow\ \forall z \in S:\ \|z'\| \le \bar T + \bar\Xi_0\|c - z'\|$
13863 [(L2); assumptions A1, A5]
13864 (L4) $\forall z \in S\ \forall i \le N:\ |z'_i - \widetilde t_i| \le \tau\widetilde\sigma_i$
13865 [Definition A.26]
13866 (L5) $\forall i \le N:\ \widetilde\sigma_i \le \bar\sigma(1 + \bar\delta)$
13867 [assumptions A3, A4; $\sigma_i > 0$ (Definition A.25)]
13868 (L6) $\forall z \in S:\ \|\widetilde t - z'\|^2 \le N(\tau\bar\sigma(1 + \bar\delta))^2$
13869 [(L4), (L5); $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead); $\widetilde t$ (the statement)]
13870 (L7) $\Rightarrow\ \forall z \in S:\ \|\widetilde t - z'\| \le \tau\bar\sigma(1 + \bar\delta)\sqrt{N}$
13871 [(L6); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

Corollary G.62 at every $z \in S$	This proof
Shared: $\mathcal{F}, u, \zeta,\ h, n,\ T,\ t,\ \bar T,\ S, \tau, \bar\delta,\ \gamma, \gamma_S,\ D^\circ$	
Shared: $h \ge 1,\ T \in \mathcal{T}_n,\ \bar T \in \mathbb{R},\ \bar\delta \in \mathbb{R}$	
z	z' (the statement)
Z	$\|z'\|$ (the proof's block)
e_{root}	$\widetilde t_T - t$ (the proof's block)
Δ	$\widetilde t - c$ (Proposition G.48)
$\mathcal{F}$ realization at (u, ζ)	The statement
13872 (I2) $t \in \mathcal{R}_n \times \mathcal{R}_n$	t (the statement)
$z \in \mathbb{Z}^N$	z' (the statement)
$Z \ge 0$	$\|z'\| \ge 0$ (Fact A.41, item 3)
$e_{\text{root}} \in \mathcal{R}_n \times \mathcal{R}_n$	$\widetilde t_T,\ t$ (the statement)
Assumption A1	The scope
Assumption A2	$Z := \|z'\|$ (the proof's block)
Assumption A3	Assumption A1
Assumption A4	$e_{\text{root}} := \widetilde t_T - t$ (the proof's block)
Assumption A5	Assumption A3
Its conclusion: $(1 - \gamma - \gamma_S)\|\Delta\| \le D^\circ$	

13873 (L8) $\forall z \in S:\ (1 - \gamma - \gamma_S)\|\widetilde t - c\| \le D^\circ$

[(I2)]

(L9) $\sigma_{\max} \le \bar{\sigma}$

[$\sigma_{\max} = \max_i \sigma_i$ (Corollary G.62); assumption A4]

(L10) $R^\circ_{\max} \le R^\circ$

[(L9); $R^\circ_{\max} = \sqrt{2}\,\Xi\tau\sigma_{\max}(1+\bar{\delta})(n/2)^{1/2}$ (Corollary G.62); $\Xi \ge 0$ (Definition 4.6, item 13, at T); $\tau > 1$ (the statement); $\bar{\delta} \ge 0$ (the statement); R° (the statement)]

(L11) $G_X \ge 0$

[G_X (Theorem G.59); $u \ge 0$ (Definition A.4); $c_{\text{split}} \ge 0$ (Lemma G.53)]

(L12) $G_R \ge 0$

[G_R and K_0 (Theorem G.59); (L11); E_l and $\widetilde{\ell}$, maxima of moduli (Theorem G.59); $|x| \ge 0$ (Fact A.41, item 1); $e_{\text{mul}} \ge 0$ (Lemma B.2, item 3)]

(L13) $\forall k \in \{1, \dots, h\} : \ \Upsilon_k \ge 0$

[Υ_k (Corollary G.62); (L11), (L12); $c_{\text{split}} \ge 0$ (Lemma G.53); $\ell \ge 0$ (Lemma G.42)]

(L14) $\forall z \in S : \ D^\circ \le D^\circ_0 + D^\circ_Z \|z'\|$

[(L10); assumption A2; D° (the proof's block); D°_0, D°_Z (the statement); $\Xi'_{\text{root}}, \Xi'_k \ge 0$ (Definition 4.6, items 10 and 8, at T); (L13)]

(L15) $1 - \gamma - \gamma_S > 0$

[assumption A6]

(L16) $\Rightarrow \ \forall z \in S : \ \|\widetilde{t} - c\| \le \frac{D^\circ_0 + D^\circ_Z \|z'\|}{1-\gamma-\gamma_S}$

[(L8), (L14), (L15)]

(L17) $\Rightarrow \ \forall z \in S : \ \|c - z'\| \le \tau\bar{\sigma}(1+\bar{\delta})\sqrt{N} + \frac{D^\circ_0 + D^\circ_Z \|z'\|}{1-\gamma-\gamma_S}$

[(L7), (L16); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3)]

(L18) $\Rightarrow \ \forall z \in S : \ \|z'\| \le \bar{T} + \bar{\Xi}_0 \left(\tau\bar{\sigma}(1+\bar{\delta})\sqrt{N} + \frac{D^\circ_0}{1-\gamma-\gamma_S}\right) + \frac{\bar{\Xi}_0 D^\circ_Z}{1-\gamma-\gamma_S}\|z'\|$

[(L3), (L17); $\bar{\Xi}_0 \ge 0$ (the statement); expand]

(L19) $1 - \bar{\Xi}_0 D^\circ_Z/(1-\gamma-\gamma_S) > 0$

[assumption A7; (L15)]

(L20) $\Rightarrow \ \forall z \in S : \ \|z'\| \le \bar{Z}$

[(L18), (L19); $\bar{Z}$ (the statement)]

(L21) $\Rightarrow$ the statement

[(L20)]

□

H.2.4 The exponent's inputs, the polynomial and the acceptance word

Structure. Lemma H.24 states the exponent's input ranges; Lemma H.25 the polynomial's relative precision; Lemma H.26 the acceptance word's rounding.

Lemma H.24 (The exponent's input ranges [to table])**.** *The distance of a candidate to the center, the squared table row and the scaled inverse variance of the base sampler are bounded by constants.*
Let:

- `isigma` *be an input of* SamplerZ *(Algorithm 8).*

Define:

- $\sigma := 1/\texttt{isigma}$*;*
- z*, that of line 10 of* SamplerZ *(Algorithm 8);*
- r*, that of line 3;*
- z_0*, that of line 9;*
- $\sigma_{\min}$*, that of* SamplerZ *(Algorithm 8), Require;*
- dss*, that of* SamplerZ *(Algorithm 8) over* $\mathbb{R}$*.*

Assume:
(A1) $\sigma \ge \sigma_{\min}$*.*

Then

1. $|z - r| \le 19.5$;
2. $z_0^2 \le 324$;
3. $dss \le 1/(2\sigma_{\min}^2)$.

Proof. (L1) $z_0 \in \{0, \dots, 18\}$
[z_0 (the statement; SamplerZ (Algorithm 8), line 9); m (Lemma G.64)]

(L2) $z \in [-18, 19]$
[(L1); $z = b + (2b-1)z_0$, $b \in \{0, 1\}$ (SamplerZ (Algorithm 8), lines 9 and 10)]

(L3) $r \in [0, 1)$
[$r = \mu - \lfloor \mu \rfloor$ (SamplerZ (Algorithm 8), lines 1 and 3); Fact A.41, item 22]

(L4) $|z - r| \le 19.5$
[(L2), (L3)]

(L5) $\Rightarrow$ item 1
[(L4)]

(L6) $z_0^2 \le 324$
[(L1)]

(L7) $\Rightarrow$ item 2
[(L6)]

(L8) $dss = \texttt{isigma}^2/2$
[dss (SamplerZ (Algorithm 8))]

(L9) $\texttt{isigma}^2/2 = 1/(2\sigma^2)$
[σ (the statement)]

(L10) $\Rightarrow$ $dss = 1/(2\sigma^2)$
[(L8), (L9)]

(L11) $dss \le 1/(2\sigma_{\min}^2)$
[(L10); $\sigma \ge \sigma_{\min}$ (assumption A1)]

(L12) $\Rightarrow$ item 3
[(L11)]

□ (items 1 to 3)

Lemma H.25 (The polynomial's relative precision [to table])**.** *The integer Horner scheme of* BerExp *approximates the scaled exponential within a relative* $2^{-51.05}$ *on the covered interval. Let:*

- $r', ccs \in \mathbb{R}$.

Define:

- *The stored words*
  - $C_0, \dots, C_{12}$, *the words of* `EXPM_COEFFS` *[L0: sign_sampler.c: 787-801];*
- *The covered interval*
  - $L := 0.6931471805599453095 + 2^{-30}$;
  - $t_j := jL/4096$, $0 \le j \le 4096$;
  - $\rho := L/8192$;
- *The polynomial*
  - $P(t) := \sum_{k=0}^{12} (-1)^k C_{12-k} 2^{-63} t^k$;
  - $\epsilon(t) := P(t)e^t - 1$;
  - $D_0 := P$;
  - $D_m := \frac{d}{dt} D_{m-1} + D_{m-1}$, $m \ge 1$;
  - $K_3 := e^L \sum_k |d_k| L^k$ *over the coefficients* d_k *of* D_3;
- *The bounds*
  - $\bar{\epsilon} := 2^{-51.0549} + 2^{-66.754}$;

13970 – $s_{\text{even}} := \sum_{k\le 11,\ k\ even} L^k$;
13971 – $s_{\text{odd}} := \sum_{k\le 11,\ k\ odd} L^k$;
13972 – $e_{\text{up}} := (1+\bar\epsilon)(1+2^{-62}) + s_{\text{even}}2^{-63}e^L - 1$;
13973 – $e_{\text{down}} := 1-(1-2^{-62})(1-\bar\epsilon - s_{\text{odd}}2^{-63}e^L) + 2^{-62}e^L$;
13974 • *The words*
13975 – $y := \texttt{expm_p63}(r', ccs)/2^{63}$, *the value the word of Fact G.66 carries.*
13976 *Assume:*
13977 *(A1)* $r' \in [0, L]$;
13978 *(A2)* $ccs \in [1/2, 1)$.
13979 *Measured [gate: verify/gates/sampler/poly_bound.py]:*
13980 • $L > \ln 2$;
13981 • $\max_j \sum_{m=0}^{2} |\epsilon^{(m)}(t_j)|\rho^m/m! \le 2^{-51.0549}$, *each* $\epsilon^{(m)}(t_j)$ *at 100 digits;*
13982 • $K_3\rho^3/3! \le 2^{-66.754}$;
13983 • *Every partial value of the Horner scheme lies in* $[0, 2^{64})$ *on* $[0, L]$;
13984 • $\max(e_{\text{up}}, e_{\text{down}}) \le 2^{-51.05}$.
13985 *Then*

13986 $$|y/(e^{-r'}ccs) - 1| \le 2^{-51.05}.$$

13987 *Proof.*

DEFINES $x' = \text{trunc}(r'2^{63})/2^{63}$
DEFINES $w = 2\,\text{trunc}(ccs\,2^{63})$
COMPUTES y_i, $0 \le i \le 12$: the Horner loop's word after i steps (line 8)
13988 DEFINES $\delta_i = y_i - (C_i - x'y_{i-1})$, $1 \le i \le 12$
DEFINES $e = \sum_{i=1}^{12} \delta_i(-x')^{12-i}$
COMPUTES $Z = 2\,\text{trunc}(r'2^{63})$, the code's word [L0: `sign_sampler.c:810`]

13989 (L1) $x' \in (r' - 2^{-63}, r']$
13990 [x' (the proof's block); trunc toward 0 at $r' \ge 0$ (assumption A1)]
13991 (L2) $Z = x'2^{64}$
13992 [the code's $Z = 2\,\text{trunc}(r'2^{63})$ [L0: `sign_sampler.c:810`]; x' (the proof's block)]
13993 (L3) $\forall i \in \{1, \dots, 12\}:\ \delta_i \in [0, 1)$
13994 [line 8: $y_i = C_i - \lfloor Zy_{i-1}/2^{64} \rfloor$; (L2); $\lfloor a \rfloor \in (a-1, a]$ (Fact A.41, item 22); $y_i \in [0, 2^{64})$ (the fourth
13995 measured row)]
13996 (L4) $y_0 = C_0$
13997 [BerExp (Algorithm 9)]
13998 (L5) $\forall i \in \{1, \dots, 12\} : y_{i-1} = \sum_{k=0}^{i-1}(-x')^k C_{i-1-k} + \sum_{j=1}^{i-1}\delta_j(-x')^{i-1-j} \Rightarrow y_i =$
13999 $\sum_{k=0}^{i}(-x')^k C_{i-k} + \sum_{j=1}^{i}\delta_j(-x')^{i-j}$
14000 [δ_i (the proof's block)]
14001 (L6) $y_{12} = 2^{63}P(x') + e$
14002 [induction on i: (L4) the base, (L5) the step; P (the statement); e (the proof's block)]
14003 (L7) $e \in [-s_{\text{odd}}, s_{\text{even}}]$
14004 [(L1), (L3); e (the proof's block); $x' \in [0, L]$ ((L1); assumption A1); s_{odd}, s_{even} (the statement)]
14005 (L8) $\forall t \in [0, L]\ \exists j:\ |t - t_j| \le \rho$
14006 [t_j, ρ (the statement)]
14007 (L9) $\forall t \in [0, L]\ \forall j:\ |\epsilon(t)| \le \sum_{m=0}^{2}|\epsilon^{(m)}(t_j)|\frac{|t-t_j|^m}{m!} + \max_{[0,L]}|\epsilon'''|\frac{|t-t_j|^3}{3!}$
14008 [the expansion of ϵ of order 2 at t_j with its remainder]
14009 (L10) $\epsilon' = e^t(\frac{d}{dt}D_0 + D_0)$
14010 [$\epsilon = Pe^t - 1$, $D_0 = P$ (the statement); differentiate]
14011 (L11) $\forall m \ge 1:\ (e^t D_m)' = e^t D_{m+1}$
14012 [$D_{m+1} = \frac{d}{dt}D_m + D_m$ (the statement); differentiate]
14013 (L12) $\forall m \ge 1:\ \epsilon^{(m)} = e^t D_m$
14014 [induction on m: (L10) the base, $D_1 = \frac{d}{dt}D_0 + D_0$ (the statement); (L11) the step]

(L13) $\max_{[0,L]}|\epsilon'''| \le K_3$

[(L12) at $m := 3$; D_m, K_3 (the statement)]

(L14) $\forall t \in [0, L] :\ |\epsilon(t)| \le \bar{\epsilon}$

[(L8), (L9), (L13); the second and third measured rows; $\bar{\epsilon}$ (the statement)]

(L15) $2^{63}y = \lfloor wy_{12}/2^{64} \rfloor$

[line 12; w (the proof's block) [L0: `sign_sampler.c:857-862`]]

(L16) $w/2^{64} \in (ccs - 2^{-63}, ccs]$

[w (the proof's block); trunc toward 0 at $ccs > 0$]

(L17) $r' - x' < 2^{-63}$

[(L1)]

(L18) $\ln(1 + 2^{-62}) \ge 2^{-62} - 2^{-124}/(2(1 - 2^{-62}))$

[Fact A.41, item 15, at $\epsilon := 2^{-62}$, $x := 2^{-62}$]

(L19) $2^{-62} - 2^{-124}/(2(1 - 2^{-62})) \ge 2^{-63}$

[expand]

(L20) $\Rightarrow\ r' - x' < \ln(1 + 2^{-62})$

[(L17), (L18), (L19)]

(L21) $\Rightarrow\ e^{r'-x'} \le 1 + 2^{-62}$

[(L20); exp increasing on $\mathbb{R}$ (Fact A.41, item 5); $e^{\ln y} = y$ (Fact A.41, item 28)]

(L22) $e^{r'} \le e^{L}$

[$r' \le L$ (assumption A1); Fact A.41, item 5]

(L23) $2^{-51.05} < 1$

[$-51.05 < 0$]

(L24) $1 - \bar{\epsilon} - s_{\text{odd}}2^{-63}e^{L} \ge 0$

[(L23); the last measured row; e_{down} (the statement); $1 - 2^{-62} > 0$]

(L25) $y_{12}/2^{63} = P(x') + e/2^{63}$

[(L6)]

(L26) $P(x') \in [(1 - \bar{\epsilon})e^{-x'}, (1 + \bar{\epsilon})e^{-x'}]$

[(L14) at $t := x' \in [0, L]$ ((L1); $r' \le L$, assumption A1); ϵ (the statement)]

(L27) $e^{-x'} \in [e^{-r'}, (1 + 2^{-62})e^{-r'}]$

[(L1), (L21)]

(L28) $y_{12}/2^{63} \le (1 + \bar{\epsilon})(1 + 2^{-62})e^{-r'} + s_{\text{even}}2^{-63}$

[(L7), (L25), (L26), (L27)]

(L29) $y_{12}/2^{63} \ge (1 - \bar{\epsilon})e^{-r'} - s_{\text{odd}}2^{-63}$

[(L7), (L24) to (L27)]

(L30) $y \le ccs\, y_{12}/2^{63}$

[(L15), (L16); $y_{12} \ge 0$ (the fourth measured row)]

(L31) $y \ge (ccs - 2^{-63})\, y_{12}/2^{63} - 2^{-63}$

[(L15), (L16); $y_{12} \ge 0$ (the fourth measured row)]

(L32) $y/(e^{-r'}ccs) - 1 \le e_{\text{up}}$

[(L22), (L28), (L30); e_{up} (the statement)]

(L33) $1 - y/(e^{-r'}ccs) \le e_{\text{down}}$

[(L22), (L24), (L29), (L31); $ccs \ge 1/2$ (assumption A2); e_{down} (the statement)]

(L34) $|y/(e^{-r'}ccs) - 1| \le 2^{-51.05}$

[(L32), (L33); the last measured row]

(L35) $\Rightarrow$ the statement

[(L34)]

□

The code's own estimate of the polynomial. The code's own estimate of the polynomial, "precision only 51 bits or so" [L0: `sign_sampler.c:893`], is confirmed and sharpened by Lemma H.25.

Lemma H.26 (The acceptance word's rounding [to table])**.** *The acceptance word of* BerExp *holds the saturated acceptance rounded down by less than* $2 \cdot 2^{-64}$*, is* 0 *below* 2^{-64}*, and at* $si \le 63$ *the saturated acceptance carries the shift. Let:*

- $si \in \mathbb{Z}$*;*
- $r' \in \mathbb{R}$*;*
- *ccs be the scale* BerExp *(Algorithm 9) takes (line 6 of* SamplerZ *(Algorithm 8)).*

Define:

- $s_x := \min(si, 63)$ *and* $z_{\mathrm{acc}} := ((\texttt{expm_p63}(r', ccs) \ll 1) - 1) \gg s_x$ *(Fact G.66);*
- $P := \texttt{expm_p63}(r', ccs)$*;*
- $acc_c := \texttt{expm_p63}(r', ccs)/2^{63+s_x}$*;*
- $\widetilde{acc}_c := z_{\mathrm{acc}}/2^{64}$.

Assume:

(A1) $si \ge 0$*;*

(A2) $P \ge 1$.

Then

1. $\dfrac{\widetilde{acc}_c}{acc_c} - 1 \in \left[-\dfrac{2 \cdot 2^{-64}}{acc_c},\ 0\right]$.
2. *Assume:*

   (A3) $acc_c < 2^{-64}$.

   Then $z_{\mathrm{acc}} = 0$.
3. *Assume:*

   (A4) $si \le 63$.

   Then $acc_c = \texttt{expm_p63}(r', ccs)/2^{63+si}$.

Proof.

DEFINES $y' = (2P - 1)/2^{s_x}$

(L1) $z_{\mathrm{acc}} = ((P \ll 1) - 1) \gg s_x$
[Fact G.66 at si, r' and ccs (the statement); $si \ge 0$ (assumption A1), assumption A1 of Fact G.66; P (the statement)]

(L2) $z_{\mathrm{acc}} = \lfloor y' \rfloor$
[(L1); $a \ll 1 = 2a$ (Definition A.5), $a \gg s = \lfloor a/2^s \rfloor$ (Definition A.5); $P \ge 1$ (assumption A2); y' (the proof's block)]

(L3) $z_{\mathrm{acc}} \in (y' - 1, y']$
[(L2); $\lfloor a \rfloor \in (a - 1, a]$ (Fact A.41, item 22)]

(L4) $\widetilde{acc}_c \in (\frac{2P-1}{2^{64+s_x}} - 2^{-64}, \frac{2P-1}{2^{64+s_x}}]$
[(L3); $\widetilde{acc}_c$ (the statement)]

(L5) $\frac{2P-1}{2^{64+s_x}} = acc_c - 2^{-64-s_x}$
[$acc_c = P/2^{63+s_x}$ (the statement)]

(L6) $2^{-64-s_x} \le 2^{-64}$
[$s_x \ge 0$ ($s_x = \min(si, 63)$, the statement; $si \ge 0$, assumption A1; Fact A.41, item 47, at $c := 0$)]

(L7) $\widetilde{acc}_c \in (acc_c - 2 \cdot 2^{-64}, acc_c]$
[(L4), (L5), (L6)]

(L8) $acc_c > 0$
[$P \ge 1$ (assumption A2); acc_c (the statement)]

(L9) $\frac{\widetilde{acc}_c}{acc_c} - 1 \in \left[-\frac{2 \cdot 2^{-64}}{acc_c},\ 0\right]$
[(L7), (L8)]

(L10) $\Rightarrow$ item 1

[(L9)]

(L11) $z_{\text{acc}} < 1$

[(L7); $\widetilde{acc}_c = z_{\text{acc}}/2^{64}$ (the statement); $acc_c < 2^{-64}$ (assumption A3)]

(L12) $z_{\text{acc}} = 0$

[(L11); $z_{\text{acc}} \in \mathbb{Z}_{\geq 0}$ (Fact G.66); $\mathbb{Z}_{\geq 0}$ (Definition A.1)]

(L13) $\Rightarrow$ item 2

[(L12)]

(L14) $s_x = \min(si, 63)$

[s_x (the statement)]

(L15) $s_x = si$

[(L14); $si \leq 63$ (assumption A4)]

(L16) $acc_c = \texttt{expm_p63}(r', ccs)/2^{63+si}$

[(L15); acc_c (the statement)]

(L17) $\Rightarrow$ item 3

[(L16)]

□ (items 1 to 3)

I The fixed-point signer

Table 24 lists this section's definitions and hypotheses, Table 25 how each lemma, proposition and corollary of this section is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Def. I.1	✓		✓		
Def. I.13					
Def. I.14					
Def. I.15					
Def. I.16					
Def. I.17					
Def. I.18					
Def. I.19	✓				
Def. I.20	✓		✓		
Hyp. I.21				code alignment	
Hyp. I.22				code alignment	
Stat. I.23					L2: BFLP26, Alg. 2
Def. I.28	✓				
Def. I.32	✓				
Fact I.45	✓				
Def. I.62					
Def. I.74					
Def. I.82					
Hyp. I.91			✓	code alignment	

Table 24: Appendix I: its definitions, facts, hypotheses and statistics.

Table 25: Appendix I: how each lemma, proposition, corollary and theorem is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma I.2	✓	✓			
Lemma I.3	✓	✓			
Lemma I.4	✓	✓			

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma I.5	✓	✓			
Lemma I.6	✓	✓			
Lemma I.7	✓	✓			
Lemma I.8	✓	✓			
Cor. I.9	✓				
Lemma I.10	✓	✓			
Lemma I.11	✓	✓			
Lemma I.12	✓				
Cor. I.24	✓				
Lemma I.25	✓				
Lemma I.26	✓				L2: BFLP26, Sec. 7.3, item 3(a)
Lemma I.27	✓				
Lemma I.29	✓				
Lemma I.30	✓				
Lemma I.31	✓				
Cor. I.33	✓				
Lemma I.34	✓		✓		
Lemma I.35	✓				
Lemma I.36	✓				
Lemma I.37	✓		✓		
Lemma I.38	✓		✓		
Lemma I.39	✓		✓		
Lemma I.40	✓		✓		
Lemma I.41	✓				
Lemma I.42	✓				
Lemma I.43	✓		✓		
Lemma I.44	✓				
Lemma I.46	✓				
Lemma I.47	✓				
Lemma I.48	✓				
Lemma I.49	✓		✓		
Lemma I.50	✓		✓		
Lemma I.51	✓		✓		
Lemma I.52	✓		✓		
Lemma I.53	✓		✓		
Thm. I.54	✓		✓		
Lemma I.55	✓		✓		
Lemma I.56	✓		✓		
Cor. I.57	✓				
Lemma I.58	✓				
Lemma I.59	✓				
Lemma I.60	✓		✓		
Lemma I.61	✓				
Lemma I.63	✓			**I.21**, **I.22**	
Lemma I.64	✓		✓		
Lemma I.65			✓		
Lemma I.66	✓		✓		
Lemma I.67	✓		✓		
Lemma I.68			✓		
Lemma I.69	✓		✓		
Lemma I.70			✓		
Lemma I.71	✓		✓	**I.21**, **I.22**	
Prop. I.72	✓			**I.21**, **I.22**	
Lemma I.73	✓				
Lemma I.75	✓		✓		
Lemma I.76	✓				
Lemma I.77	✓		✓	**I.21**, **I.22**	
Cor. I.78			✓		
Cor. I.79			✓		
Cor. I.80			✓	**I.21**, **I.22**	
Lemma I.81	✓		✓	**I.21**, **I.22**	
Lemma I.83	✓				

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma I.84	✓				
Prop. I.85	✓				
Lemma I.86	✓				
Cor. I.87			✓		
Cor. I.88			✓		
Cor. I.89			✓	**I.21**, **I.22**	

Standing symbols. The standing symbols of this appendix are:

- $\mathcal{F}_{\mathrm{fx}}$, the realization (Definition I.1);
- $u := 0$ and $\zeta := 2^{-64}$, its bounds (Definition I.1).

What the machine-checked proofs cover. The kernels the sampling recursion calls are proved on their compiled code at both degrees (Lemma I.10). The recursion's compiled code makes their calls as ffsamp (Algorithm 6) states, and returns its algorithm's words, at both degrees (Lemma I.11). **Hypothesis I.21, item 2**, assumes the composition outside the recursion.

The result of this appendix. The appendix's result is Theorem 1.3, restated with its tables in Section 5.5, a lower bound on the fixed-point signer's bit security under **Hypotheses I.21, I.22 and I.91**, the three code-alignment hypotheses, at each center and every key the key generation accepts at that center. Its tables are Table 31, the sample maxima W^* and $\bar{\delta}^*$ of the leaf perturbations at both centers (Statistics I.23, items 13 and 14), and Table 34, the bit security $\lambda_{\mathcal{F}}$ at the tail W^{tail} at both centers. Table 51 (Appendix L) lists this signer's routines, the algorithm each one is and the lemma that bounds it.

The fixed-point signer. The fixed-point signer, the realization of Definition A.4, item 8, is the code under `fxp/`: the signing path of `c-fn-dsa` mirrored file by file on a 64.64 fixed-point type, with the four key checks of [L2: BFLP26, Alg. 2]. Under **Hypotheses I.21 and I.22**, it is the Falcon-type signer of Definition 4.5 at $(u, \zeta) = (0, 2^{-64})$ (Lemma I.63), and this appendix instantiates the phase statements and Theorem 4.11 at it (Proposition 5.9, Corollary 5.10), in two versions that differ in the center of the tree recursion: $\mathrm{ffSampling}^{\mathcal{F}}(B, s, t)$ at the center $t = (\mathsf{h}(\mathsf{m}), 0)B^{-1}$ of the lattice Gaussian, computed as the reference computes it (Appendix I.6), and $\mathrm{ffSampling}^{\mathcal{F}}(B, s, t_{\mathrm{frac}})$ at its fractional part t_{frac} in the split $t = t_{\mathrm{int}} + t_{\mathrm{frac}}$ of [L2: BFLP26, Alg. 7] (Appendix I.7; what the split buys, Remark I.90). Both versions compute the root node's second diagonal by the NTRU identity $\mathrm{fl}(q^2/\widetilde{g}_{00})$ (Lemma I.27; [L2: BFLP26, Sec. 7.3, item 3(a)]) in place of the $LDL^{\dagger}$ step's.

Structure. This appendix proves a lower bound on the fixed-point signer's bit security. Appendix I.1 states the realization; Appendix I.2 the checked key; the subsection after it the tree at $u = 0$; Appendix I.4 the base sampler's perturbation budget; the subsection after it the terms of $\ln R$; Appendices I.6 and I.7 the two versions $\mathrm{ffSampling}^{\mathcal{F}}(B, s, t)$ and $\mathrm{ffSampling}^{\mathcal{F}}(B, s, t_{\mathrm{frac}})$; Appendix I.8 the tail checks' hypothesis; Appendix I.9 the result.

No word overflows. No word of the key check, the tree or the recursion's center lines overflows, at every checked key and every sample (Theorem I.54): the base sampler's bounded support bounds each sample's distance to its center, where [L2: BFLP26, Lemma 11] bounds these words with a failure probability, the samples modeled as a discrete Gaussian.

The tables and the sampled measurements. Every table names in its caption the center it reports. The code's sampled measurements are Statistics I.23, with Table 26 the key checks'

acceptance, Table 27 the tail checks' time, Table 29 the signatures and Table 30 the tail checks on the checked keys.

The key is a checked key. Every statement of this appendix that reads the key takes a checked key (Definition 5.5), and its key constants are taken at the bounds every checked key meets (Definition I.62), never at a sample's maxima; the leaf-perturbation sample of this section is measured on checked keys.

I.1 The realization

Structure. Appendix I.1.1 states the arithmetic; Appendix I.1.2 the interval arithmetic of the tail checks; Appendix I.1.3 the tail checks in code; Appendix I.1.4 ffSampling$^{\mathcal{F}}$ in $\mathcal{F}_{\text{fx}}$.

I.1.1 The arithmetic

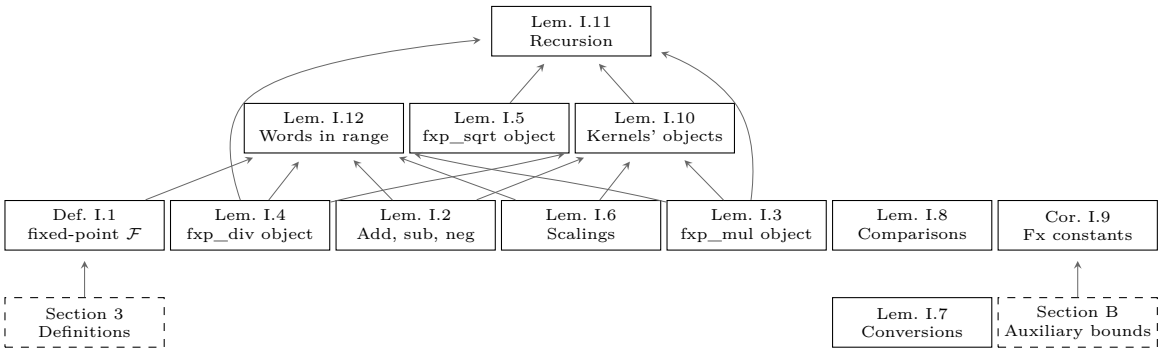


Figure 66: Dependencies, Appendix I.1.1.

Definition I.1 (The fixed-point realization [to table])**.** The fixed-point signer computes in $2^{-64}\mathbb{Z}$, each operation rounded to nearest, a tie away from 0. Define:

- $\mathcal{F}_{\text{fx}} := 2^{-64}\mathbb{Z}$, the fixed-point signer's realization;
- $\forall x \in \mathcal{V}_{\text{fx}}:\ W_x$, the word of Definition A.5 that stores it [L0: `fxp/sign_fxp.h:28-30`];
- $\zeta_{\text{op}} := 2^{-65}$;
- $\zeta := 2\zeta_{\text{op}}$;
- $u := 0$;
- $\forall v \in \mathbb{R}:\ \text{roundAway}(v) := \text{sgn}(v)\,\lfloor |v| + 1/2 \rfloor$;
- $\forall v \in \mathbb{Z}\ \forall d > 0:\ \text{roundAway}(v, d) := \text{roundAway}(v/d)$;
- $\forall v \in \mathbb{R}:\ \text{roundEven}(v) := \begin{cases} \lfloor v + 1/2 \rfloor & v - \lfloor v \rfloor \neq 1/2 \\ 2\lfloor v/2 + 1/4 \rfloor & v - \lfloor v \rfloor = 1/2 \end{cases}$;
- $\forall k < 1024:\ \text{rev}_{10}(k) := \sum_{j<10} (\lfloor k/2^j \rfloor \bmod 2)\, 2^{9-j}$ (Lemma G.14);
- $\forall k < 1024:\ \psi_k := \exp(i\pi\, \text{rev}_{10}(k)/1024)$ (Lemma G.14).

Every statement of this appendix is at $(u, \zeta) = (0, 2^{-64})$. We define the realization by

1. fl (Definition A.4 at $(u, \zeta) = (0, \zeta_{\text{op}})$) [L0: `fxp/sign_fxp.c:101`] [L0: `fxp/sign_fxp.c:148`] [L0: `fxp/sign_fxp.c:180`]:
   - $\forall x, y \in \mathcal{F}_{\text{fx}}:\ \text{fl}(x \times y) = 2^{-64}\text{roundAway}(x_{\text{fx64}} y_{\text{fx64}}, 2^{64})$;
   - $\forall x, y \in \mathcal{F}_{\text{fx}},\ y \neq 0:\ \text{fl}(x/y) = 2^{-64}\text{roundAway}(x_{\text{fx64}} 2^{64}/y_{\text{fx64}})$;
   - $\forall x \in \mathcal{F}_{\text{fx}},\ x \geq 0:\ \text{fl}(\sqrt{x}) = 2^{-64}\text{roundAway}(\sqrt{x_{\text{fx64}} 2^{64}})$;
   - $\forall \circ \in \{\times, /\}\ \forall x, y \in \mathcal{F}_{\text{fx}},\ y \neq 0$ at $/\ \exists \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \leq \zeta_{\text{op}}:\ \text{fl}(x \circ y) = x \circ y + \zeta_\circ$, with `fxp_inv`$(x)$ = `fxp_div`$(1, x)$ [L0: `fxp/sign_fxp.h:412`];
   - $\forall x \in \mathcal{F}_{\text{fx}},\ x \geq 0\ \exists \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \leq \zeta_{\text{op}}:\ \text{fl}(\sqrt{x}) = \sqrt{x} + \zeta_\circ$;
   - $\forall x, y \in \mathcal{F}_{\text{fx}}:\ \text{fl}(x \pm y) = x \pm y$ and $\text{fl}(-x) = -x$ [L0: `fxp/sign_fxp.h:194-227`];

2. $\forall x \in \mathcal{F}_{\mathrm{fx}},\ x_{\mathrm{fx64}} \in [-2^{127}, 2^{127}) :\ \mathrm{fl}(x/2) := 2^{-64}\mathrm{roundAway}(x_{\mathrm{fx64}}/2)$ (Definition A.4 at $(0, \zeta)$; Fact A.6, item 2; Lemmas B.3, G.32) [L0: `fxp/sign_fxp.h:316-318`]:
   - $\forall x, y \in \mathcal{F}_{\mathrm{fx}}\ \exists \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \le \zeta_{\mathrm{op}} :\ \mathrm{fl}((x+y)/2) = (x+y)/2 + \zeta_\circ$;
3. $\lfloor \cdot \rfloor$, trunc, rint, those of Fact A.6, item 5 [L0: `fxp/sign_fxp.h:345-378`];
4. $\forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\}\ \forall k < 1024 :\ \mathfrak{p}(\widetilde{\psi}_k) := 2^{-64}\mathrm{roundEven}(2^{64}\mathfrak{p}(\psi_k))$ [L0: `fxp/gen_consts.py:145`] [gate: `verify/gates/fx/consts.py`];
5. $\forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\}\ \forall k < 1024 :\ W_{\mathfrak{p}(\widetilde{\psi}_k)} = \mathfrak{p}(\widetilde{\psi}_k)_{\mathrm{fx64}} \bmod 2^{128}$, the stored twiddles' words in `FXP_GM`, the words of Definition A.5 that store $\widetilde{\psi}_k$ [L0: `fxp/gen_consts.py:182`] [gate: `verify/gates/fx/consts.py`];
6. $\forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\}\ \forall k < 1024 :\ W_{\mathfrak{p}(\mathrm{conj}\,\widetilde{\psi}_k)} = \mathfrak{p}(\mathrm{conj}\,\widetilde{\psi}_k)_{\mathrm{fx64}} \bmod 2^{128}$, the conjugates' words the inverse FFT reads, the imaginary part's by `fxp_neg` [L0: `fxp/sign_fxpoly.c:58`].

```
theorem fxAdd_rounds {zeta : Real} (hzeta : 0 <= zeta) (f : Nat) (X Y : Int) :
    Rounds 0 zeta (fxVal f X + fxVal f Y) (fxVal f (X + Y)) := by

def roundAway (num den : Int) : Int :=
  if num < 0 then -roundUpHalf (-num) den else roundUpHalf num den

theorem roundAway_real {num den : Int} (hden : 0 < den) :
    |(roundAway num den : Real) - num / den| <= 1 / 2 := by

theorem fxMul_rounds (f : Nat) (X Y : Int) :
    Rounds 0 (zetaOp f) (fxVal f X * fxVal f Y) (fxVal f (fxMul f X Y)) := by

theorem fxDiv_rounds (f : Nat) (X Y : Int) (hY : Y != 0) :
    Rounds 0 (zetaOp f) (fxVal f X / fxVal f Y) (fxVal f (fxDiv f X Y)) := by

theorem fxSqrt_rounds (f : Nat) (X : Int) (hX : 0 <= X) :
    Rounds 0 (zetaOp f) (Real.sqrt (fxVal f X)) (fxVal f (fxSqrt f X)) := by

theorem fxHalf_rounds (f : Nat) (X : Int) :
    Rounds 0 (zetaOp f) (fxVal f X / 2) (fxVal f (fxHalf X)) := by

theorem fxDiv2e_rounds (f : Nat) (X : Int) (e : Nat) :
    Rounds 0 (zetaOp f) (fxVal f X / 2 ^ e) (fxVal f (fxDiv2e X e)) := by

theorem halved_sum_rounds {zeta x y h : Real} (hr : Rounds 0 zeta ((x + y) / 2) h) :
    exists s : Real, Rounds 0 (2 * zeta) (x + y) s /\ h = s / 2 := by

theorem fxHalf_add_rounds (f : Nat) (X Y : Int) :
    exists s : Real, Rounds 0 (1 / 2 ^ f) (fxVal f X + fxVal f Y) s /\ fxVal f (fxHalf (X + Y))
        = s / 2 := by

theorem fxCAdd_cadd {zeta : Real} (hzeta : 0 <= zeta) (f : Nat) (a b : Int x Int) :
    CAdd 0 zeta (fxCVal f a) (fxCVal f b) (fxCVal f (a + b)) := by

theorem fxCMul_cmul (f : Nat) (a b : Int x Int) :
    CMul 0 (zetaOp f) (fxCVal f a) (fxCVal f b) (fxCVal f (fxCMul f a b)) := by

theorem roundAway_eq_formula {num den : Int} (hd : 0 < den) :
    roundAway num den = SignType.sign ((num : Real) / den) * floor(|(num : Real) / den| + 1 /
        2) := by

theorem isqrtNearest_eq_formula (n : Nat) : (isqrtNearest n : Int) = floor(Real.sqrt n + 1 / 2)
    := by

def roundUpHalf (a den : Int) : Int :=
  if den <= 2 * (a % den) then a / den + 1 else a / den
```

Figure 67: The Lean declarations carrying Definition I.1: `fxAdd_rounds`, `roundAway`, `roundAway_real`, `fxMul_rounds`, `fxDiv_rounds`, `fxSqrt_rounds`, `fxHalf_rounds`, `fxDiv2e_rounds`, `halved_sum_rounds`, `fxHalf_add_rounds`, `fxCAdd_cadd`, `fxCMul_cmul`, `roundAway_eq_formula`, `isqrtNearest_eq_formula`, `roundUpHalf` (`FixedFormat.lean`, `MachineWords.lean`); Lean's symbols in ASCII.

The code's operations on its words, each proved on its compiled object by CryptoLine (Section 2.2), are the following lemmas.

Lemma I.2 (The objects of the additive operations [to table]). *The objects of* `fxp_add`, `fxp_sub` *and* `fxp_neg` *return the sum, the difference and the negation of their words modulo* 2^{128}. *Let:*

- $x, y \in 2^{-64}\mathbb{Z}$.

Define:

- $W_x := x_{\text{fx64}} \bmod 2^{128}$ *and* $W_y := y_{\text{fx64}} \bmod 2^{128}$;

- *$\mathcal{O}$, the aarch64 `-O3` objects of the routines below, each through its `noinline` wrapper (Homebrew clang 22.1.8, QEMU `virt` Cortex-A72);*
- *W_z, the word each object returns.*

Then:

1. *The object of `fxp_add` in $\mathcal{O}$ returns $W_z = (W_x + W_y) \bmod 2^{128}$ [CryptoLine: `lemmas/fxp64_64/ops/add/lem_add.cl`].*
2. *The object of `fxp_sub` in $\mathcal{O}$ returns $W_z = (W_x - W_y) \bmod 2^{128}$ [CryptoLine: `lemmas/fxp64_64/ops/sub/lem_sub.cl`].*
3. *The object of `fxp_neg` in $\mathcal{O}$ returns $W_z = (-W_x) \bmod 2^{128}$ [CryptoLine: `lemmas/fxp64_64/ops/neg/lem_neg.cl`].*

Proof. (L1) $\forall a \in \mathbb{Z} :\ \mathrm{u}_{128}(a) = a \bmod 2^{128}$

[u_w (Definition A.5)]

Proof of item 1.

(L2) $W_z = \mathrm{u}_{128}(W_x + W_y)$

[[CryptoLine: `lemmas/fxp64_64/ops/add/lem_add.cl`]]

(L3) $W_z = (W_x + W_y) \bmod 2^{128}$

[(L1), (L2)]

(L4) $\Rightarrow$ item 1

[(L3)]

□ (item 1)

Proof of item 2.

(L5) $W_z = \mathrm{u}_{128}(W_x - W_y)$

[[CryptoLine: `lemmas/fxp64_64/ops/sub/lem_sub.cl`]]

(L6) $W_z = (W_x - W_y) \bmod 2^{128}$

[(L1), (L5)]

(L7) $\Rightarrow$ item 2

[(L6)]

□ (item 2)

Proof of item 3.

(L8) $W_z = \mathrm{u}_{128}(0 - W_x)$

[[CryptoLine: `lemmas/fxp64_64/ops/neg/lem_neg.cl`]]

(L9) $W_z = (-W_x) \bmod 2^{128}$

[(L1), (L8)]

(L10) $\Rightarrow$ item 3

[(L9)]

□ (item 3)

Lemma I.3 (The object of `fxp_mul` [to table])**.** *The object of `fxp_mul` returns the product of two numbers of $2^{-64}\mathbb{Z}$, rounded to the nearest element of $2^{-64}\mathbb{Z}$, a tie away from 0, as a word modulo 2^{128}. Let:*

- *$x, y \in 2^{-64}\mathbb{Z}$ with $x_{\mathrm{fx64}}, y_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (Definition A.5).*

Define:

- *$W_x := x_{\mathrm{fx64}} \bmod 2^{128}$ and $W_y := y_{\mathrm{fx64}} \bmod 2^{128}$;*
- *W_z, the word the aarch64 `-O3` object of `fxp_mul` (Homebrew clang 22.1.8, QEMU `virt` Cortex-A72) returns on (W_x, W_y);*
- *$\forall v \in \mathbb{R} :\ \mathrm{roundAway}(v) := \mathrm{sgn}(v)\,\lfloor |v| + 1/2 \rfloor$ (Definition I.1);*

- $\forall v \in \mathbb{Z}\ \forall d > 0:\ \text{roundAway}(v, d) := \text{roundAway}(v/d)$ *(Definition I.1);*
- $z := \text{roundAway}(x_{\text{fx64}} y_{\text{fx64}}, 2^{64}) 2^{-64}$.

Then

$$W_z = z_{\text{fx64}} \bmod 2^{128}.$$

[CryptoLine: `lemmas/fxp64_64/mul_rounding/lem_mul.cl`]

Proof.

DEFINES $s_x = [x_{\text{fx64}} < 0]$: the sign bit of W_x
DEFINES $s_y = [y_{\text{fx64}} < 0]$: the sign bit of W_y
DEFINES $s = s_x \oplus s_y$
COMPUTES $M \in \{0, \ldots, 2^{128} - 1\}$: limbs 1 to 2 of $|x_{\text{fx64}}||y_{\text{fx64}}| + 2^{63}$
COMPUTES $\rho \in \{0, \ldots, 2^{64} - 1\}$: limb 0 of $|x_{\text{fx64}}||y_{\text{fx64}}| + 2^{63}$
MEASURED the object: 94 instructions and no branch, one path for every input

(L1) $M 2^{64} + \rho \equiv |x_{\text{fx64}}||y_{\text{fx64}}| + 2^{63} \pmod{2^{192}}$
[[CryptoLine: `lemmas/fxp64_64/mul_rounding/lem_mul.cl`], its algebraic claim; $x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L2) $\rho \in [0, 2^{64})$
[[CryptoLine: `lemmas/fxp64_64/mul_rounding/lem_mul.cl`], the 64-bit type of its ρ]

(L3) $W_z \equiv (1 - 2s)M \pmod{2^{128}}$
[[CryptoLine: `lemmas/fxp64_64/mul_rounding/lem_mul.cl`], its algebraic claim]

(L4) $\exists k \in \mathbb{Z}:\ |x_{\text{fx64}}||y_{\text{fx64}}| + 2^{63} = (M + k2^{128})2^{64} + \rho$
[(L1)]

(L5) $\lfloor (|x_{\text{fx64}}||y_{\text{fx64}}| + 2^{63})/2^{64} \rfloor = M + k2^{128}$
[(L4), (L2)]

(L6) $\forall v \geq 0\ \forall d > 0:\ \text{roundAway}(v, d) = \lfloor (v + d/2)/d \rfloor$
[Definition I.1]

(L7) $\text{roundAway}(|x_{\text{fx64}}||y_{\text{fx64}}|, 2^{64}) \equiv M \pmod{2^{128}}$
[(L5), (L6)]

(L8) $W_z \equiv (1 - 2s)\,\text{roundAway}(|x_{\text{fx64}}||y_{\text{fx64}}|, 2^{64}) \pmod{2^{128}}$
[(L3), (L7)]

(L9) $x_{\text{fx64}} y_{\text{fx64}} = (1 - 2s)|x_{\text{fx64}}||y_{\text{fx64}}|$
[s (the proof's block)]

(L10) $\forall v \in \mathbb{Z}\ \forall d > 0:\ \text{roundAway}(-v, d) = -\text{roundAway}(v, d)$
[Definition I.1]

(L11) $(1 - 2s)\,\text{roundAway}(|x_{\text{fx64}}||y_{\text{fx64}}|, 2^{64}) = \text{roundAway}(x_{\text{fx64}} y_{\text{fx64}}, 2^{64})$
[(L9), (L10)]

(L12) $W_z = \text{roundAway}(x_{\text{fx64}} y_{\text{fx64}}, 2^{64}) \bmod 2^{128}$
[(L8), (L11); $0 \leq W_z < 2^{128}$]

(L13) $z_{\text{fx64}} = \text{roundAway}(x_{\text{fx64}} y_{\text{fx64}}, 2^{64})$
[the statement's z; $z_{\text{fx64}} = 2^{64} z$ (Definition A.5)]

(L14) $W_z = z_{\text{fx64}} \bmod 2^{128}$
[(L12), (L13)]

(L15) $\Rightarrow$ the statement
[(L14)]

□

Lemma I.4 (The object of `fxp_div` [to table])**.** *The object of `fxp_div` returns the quotient of two numbers of $2^{-64}\mathbb{Z}$, rounded to the nearest element of $2^{-64}\mathbb{Z}$, a tie away from 0, as a word modulo 2^{128}. Let:*

- $x, y \in 2^{-64}\mathbb{Z}$ *with* $x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$ *(Definition A.5).*

Define:

- $W_x := x_{\mathrm{fx64}} \bmod 2^{128}$ *and* $W_y := y_{\mathrm{fx64}} \bmod 2^{128}$*;*
- W_z*, the word the aarch64* `-O3` *object of* `fxp_div` *(Homebrew clang 22.1.8, QEMU* `virt` *Cortex-A72) returns on* (W_x, W_y)*;*
- $\forall v \in \mathbb{R}:\ \mathrm{roundAway}(v) := \mathrm{sgn}(v)\,\lfloor |v| + 1/2 \rfloor$ *(Definition I.1);*
- $\forall v \in \mathbb{Z}\ \forall d > 0:\ \mathrm{roundAway}(v, d) := \mathrm{roundAway}(v/d)$ *(Definition I.1);*
- $z := \mathrm{roundAway}(x_{\mathrm{fx64}} 2^{64} / y_{\mathrm{fx64}}) 2^{-64}$.

Assume:

(A1) $y \neq 0$.

Then

$$W_z = z_{\mathrm{fx64}} \bmod 2^{128}.$$

[CryptoLine: `lemmas/fxp64_64/div/lem_div.cl`*]*

Proof.

DEFINES	$s_x = [x_{\mathrm{fx64}} < 0]$: the sign bit of W_x
DEFINES	$s_y = [y_{\mathrm{fx64}} < 0]$: the sign bit of W_y
DEFINES	$s = s_x \oplus s_y$
COMPUTES	A: the magnitude of x_{fx64} the object's prologue computes
COMPUTES	D: the magnitude of y_{fx64} the object's prologue computes
COMPUTES	$Q \in \{0, \ldots, 2^{128} - 1\}$: the loop's final quotient
COMPUTES	$R \in \{0, \ldots, 2^{256} - 1\}$: the loop's final remainder
MEASURED	the object: a branchless restoring division of 256 iterations, one bit of $A2^{64}$ each, 8508 instructions for every input

(L1) $QD + R \equiv A2^{64} \pmod{2^{128}D}$
[[CryptoLine: `lemmas/fxp64_64/div/lem_div.cl`], its algebraic claim; the loop body a contract, applied at each of the 256 iterations; assumption A1]

(L2) $A = |x_{\mathrm{fx64}}|$
[[CryptoLine: `lemmas/fxp64_64/div/lem_div.cl`], its range claims; $x_{\mathrm{fx64}}, y_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L3) $D = |y_{\mathrm{fx64}}|$
[[CryptoLine: `lemmas/fxp64_64/div/lem_div.cl`], its range claims; $x_{\mathrm{fx64}}, y_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L4) $R \in [0, D)$
[[CryptoLine: `lemmas/fxp64_64/div/lem_div.cl`], its range claims]

(L5) $W_z \equiv (1 - 2s)(Q + [2R \geq D]) \pmod{2^{128}}$
[[CryptoLine: `lemmas/fxp64_64/div/lem_div.cl`], its range claims]

(L6) $\exists\, k \in \mathbb{Z}:\ A2^{64} = (Q + k2^{128})D + R$
[(L1)]

(L7) $\lfloor A2^{64}/D \rfloor = Q + k2^{128}$
[(L6), (L4)]

(L8) $A2^{64} - D\lfloor A2^{64}/D \rfloor = R$
[(L6), (L7)]

(L9) $\forall v \geq 0\ \forall d > 0:\ \mathrm{roundAway}(v, d) = \lfloor (v + d/2)/d \rfloor$
[Definition I.1]

(L10) $\lfloor (R + D/2)/D \rfloor = [2R \geq D]$
[(L4)]

(L11) $\mathrm{roundAway}(A2^{64}, D) = \lfloor A2^{64}/D \rfloor + [2R \geq D]$
[(L8), (L9), (L10)]

(L12) $\mathrm{roundAway}(A2^{64}, D) \equiv Q + [2R \geq D] \pmod{2^{128}}$
[(L7), (L11)]

(L13) $W_z \equiv (1-2s)\,\mathrm{roundAway}(A2^{64}, D) \pmod{2^{128}}$

[(L5), (L12)]

(L14) $x_{\mathrm{fx64}}/y_{\mathrm{fx64}} = (1-2s)A/D$

[(L2), (L3); s (the proof's block)]

(L15) $\forall v \in \mathbb{Z}\ \forall d > 0:\ \mathrm{roundAway}(-v, d) = -\mathrm{roundAway}(v, d)$

[Definition I.1]

(L16) $(1-2s)\,\mathrm{roundAway}(A2^{64}, D) = \mathrm{roundAway}(x_{\mathrm{fx64}}2^{64}/y_{\mathrm{fx64}})$

[(L14), (L15)]

(L17) $W_z = \mathrm{roundAway}(x_{\mathrm{fx64}}2^{64}/y_{\mathrm{fx64}}) \bmod 2^{128}$

[(L13), (L16); $0 \le W_z < 2^{128}$]

(L18) $z_{\mathrm{fx64}} = \mathrm{roundAway}(x_{\mathrm{fx64}}2^{64}/y_{\mathrm{fx64}})$

[the statement's z; $z_{\mathrm{fx64}} = 2^{64}z$ (Definition A.5)]

(L19) $W_z = z_{\mathrm{fx64}} \bmod 2^{128}$

[(L17), (L18)]

(L20) $\Rightarrow$ the statement

[(L19)]

□

Lemma I.5 (The object of `fxp_sqrt` [to table])**.** *The object of* ***`fxp_sqrt`*** *returns the square root of a nonnegative number of $2^{-64}\mathbb{Z}$, rounded to the nearest element of $2^{-64}\mathbb{Z}$, as a word. Let:*

- *$x \in 2^{-64}\mathbb{Z}$ with $x_{\mathrm{fx64}} \in \{0, \dots, 2^{128}-1\}$ (Definition A.5).*

Define:

- *$W_x := x_{\mathrm{fx64}}$;*
- *W_z, the word the aarch64 `-O3` object of* ***`fxp_sqrt`*** *(Homebrew clang 22.1.8, QEMU* ***`virt`*** *Cortex-A72) returns on W_x;*
- *$\forall v \in \mathbb{R}:\ \mathrm{roundAway}(v) := \mathrm{sgn}(v)\,\lfloor |v| + 1/2 \rfloor$ (Definition I.1);*
- *$\forall v \in \mathbb{Z}\ \forall d > 0:\ \mathrm{roundAway}(v, d) := \mathrm{roundAway}(v/d)$ (Definition I.1);*
- *$z := \mathrm{roundAway}\big(\sqrt{x_{\mathrm{fx64}}2^{64}}\big)2^{-64}$.*

Then

$$W_z = z_{\mathrm{fx64}}.$$

[CryptoLine: `lemmas/fxp64_64/sqrt/lem_sqrt.cl`]

Proof.

COMPUTES $S \in \{0, \dots, 2^{128}-1\}$: the loop's final root
COMPUTES $R \in \{0, \dots, 2^{256}-1\}$: the loop's final remainder
MEASURED the object: a branchless restoring square root of 128 iterations, two bits of W_x2^{64} each, 6050 instructions for every input

(L1) $S^2 + R = W_x2^{64}$

[[CryptoLine: `lemmas/fxp64_64/sqrt/lem_sqrt.cl`], its algebraic claim; the loop body a contract, applied at each of the 128 iterations]

(L2) $0 \le R$

[[CryptoLine: `lemmas/fxp64_64/sqrt/lem_sqrt.cl`], the unsigned type of its R]

(L3) $R \le 2S$

[[CryptoLine: `lemmas/fxp64_64/sqrt/lem_sqrt.cl`], its range claims]

(L4) $W_z \equiv S + [R > S] \pmod{2^{128}}$

[[CryptoLine: `lemmas/fxp64_64/sqrt/lem_sqrt.cl`], its range claims]

(L5) $S^2 \le W_x2^{64}$

[(L1), (L2)]

(L6) $W_x2^{64} \le S^2 + 2S$

[(L1), (L3)]

(L7) $(S+1)^2 = S^2 + 2S + 1$ [the expansion]

(L8) $S^2 + 2S < (S+1)^2$ [(L7)]

(L9) $S = \lfloor \sqrt{W_x 2^{64}} \rfloor$ [(L5), (L6), (L8); $S \geq 0$ (the proof's block)]

(L10) $(S + 1/2)^2 = S^2 + S + 1/4$ [the expansion]

(L11) $\sqrt{W_x 2^{64}} \geq S + 1/2 \iff R \geq S + 1/4$ [(L1), (L10)]

(L12) $R \geq S + 1/4 \iff R > S$ [$R, S \in \mathbb{Z}$]

(L13) $\forall v \geq 0 :\ \mathrm{roundAway}(v) = \lfloor v + 1/2 \rfloor$ [Definition I.1]

(L14) $\mathrm{roundAway}(\sqrt{W_x 2^{64}}) = S + [R > S]$ [(L9), (L11), (L12), (L13)]

(L15) $W_x 2^{64} < 2^{192}$ [$W_x < 2^{128}$ (the statement)]

(L16) $S \leq 2^{96}$ [(L5), (L15)]

(L17) $S + 1 < 2^{128}$ [(L16)]

(L18) $W_z = \mathrm{roundAway}(\sqrt{W_x 2^{64}})$ [(L4), (L14), (L17); $0 \leq W_z < 2^{128}$]

(L19) $z_{\mathrm{fx64}} = \mathrm{roundAway}(\sqrt{x_{\mathrm{fx64}} 2^{64}})$ [the statement's z; $z_{\mathrm{fx64}} = 2^{64} z$ (Definition A.5)]

(L20) $W_z = z_{\mathrm{fx64}}$ [(L18), (L19); $W_x = x_{\mathrm{fx64}}$ (the statement)]

(L21) $\Rightarrow$ the statement [(L20)]

□

Lemma I.6 (The objects of the power-of-two scalings [to table])**.** *The objects of* `fxp_half` *and* `fxp_div2e` *return a number divided by* 2 *or by* 2^e*, rounded to the nearest element of* $2^{-64}\mathbb{Z}$*, a tie away from* 0*. The object of* `fxp_mul2e` *returns a word multiplied by* 2^e *modulo* 2^{128}*. Let:*

- $x \in 2^{-64}\mathbb{Z}$ *with* $x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ *(Definition A.5);*
- $e \in \{1, \ldots, 63\}$.

Define:

- $W_x := x_{\mathrm{fx64}} \bmod 2^{128}$*;*
- $\mathcal{O}$*, the aarch64* `-O3` *objects of the routines below, each through its* `noinline` *wrapper (Homebrew clang 22.1.8, QEMU* `virt` *Cortex-A72);*
- W_z*, the word each object returns on* W_x *and* e*;*
- $z_{\mathrm{fx64}} := \mathrm{s}_{128}(W_z)$ *(Definition A.5);*
- $\forall v \in \mathbb{R} :\ \mathrm{roundAway}(v) := \mathrm{sgn}(v)\, \lfloor |v| + 1/2 \rfloor$ *(Definition I.1);*
- $\forall v \in \mathbb{Z}\ \forall d > 0 :\ \mathrm{roundAway}(v, d) := \mathrm{roundAway}(v/d)$ *(Definition I.1).*

Then:

1. *The object of* `fxp_half` *in* $\mathcal{O}$ *returns* $z_{\mathrm{fx64}} = \mathrm{roundAway}(x_{\mathrm{fx64}}/2)$ *[CryptoLine:* `lemmas/fxp64_64/ops/half/lem_half.cl`*].*

2. *The object of* `fxp_div2e` *in* $\mathcal{O}$ *returns* $z_{\text{fx64}} = \text{roundAway}(x_{\text{fx64}}/2^e)$ *[CryptoLine:* `lemmas/fxp64_64/ops/div2e/lem_div2e.cl`*].*

3. *The object of* `fxp_mul2e` *in* $\mathcal{O}$ *returns* $W_z = W_x 2^e \bmod 2^{128}$ *[CryptoLine:* `lemmas/fxp64_64/ops/mul2e/lem_mul2e.cl`*].*

Proof. (L1) $\forall v \in \mathbb{Z},\ v \geq 0\ \forall e \geq 0 :\ v \gg e = \lfloor v/2^e \rfloor$

[$\gg$ (Definition A.5)]

(L2) $\forall v \in \mathbb{Z}\ \forall d > 0 :\ \text{roundAway}(-v, d) = -\text{roundAway}(v, d)$

[Definition I.1]

(L3) $\forall v \in \mathbb{Z},\ v \geq 0\ \forall e \geq 1 :\ \text{roundAway}(v, 2^e) = \lfloor (v + 2^{e-1})/2^e \rfloor$

[Definition I.1]

(L4) $\forall v \in \mathbb{Z},\ |v| < 2^{255} :\ \text{s}_{256}(v) = v$

[s_w (Definition A.5)]

Proof of item 1.

(L5) $x_{\text{fx64}} \geq 0 \Rightarrow\ z_{\text{fx64}} = (x_{\text{fx64}} + 1) \gg 1$

[[CryptoLine: `lemmas/fxp64_64/ops/half/lem_half.cl`], its claim on 256 bits; (L4) at its operands, $x_{\text{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L6) $x_{\text{fx64}} < 0 \Rightarrow\ z_{\text{fx64}} = -((-x_{\text{fx64}} + 1) \gg 1)$

[[CryptoLine: `lemmas/fxp64_64/ops/half/lem_half.cl`], its claim on 256 bits; (L4) at its operands, $x_{\text{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L7) $z_{\text{fx64}} = \text{roundAway}(x_{\text{fx64}}/2)$

[(L1) to (L6) at $e = 1$]

(L8) $\Rightarrow$ item 1

[(L7)]

$\square$ (item 1)

Proof of item 2.

(L9) $x_{\text{fx64}} \geq 0 \Rightarrow\ z_{\text{fx64}} = (x_{\text{fx64}} + 2^{e-1}) \gg e$

[[CryptoLine: `lemmas/fxp64_64/ops/div2e/lem_div2e.cl`], its claim on 256 bits; (L4) at its operands, $x_{\text{fx64}} \in [-2^{127}, 2^{127})$ and $e \in \{1, \ldots, 63\}$ (the statement), the claim's precondition]

(L10) $x_{\text{fx64}} < 0 \Rightarrow\ z_{\text{fx64}} = -((-x_{\text{fx64}} + 2^{e-1}) \gg e)$

[[CryptoLine: `lemmas/fxp64_64/ops/div2e/lem_div2e.cl`], its claim on 256 bits; (L4) at its operands, $x_{\text{fx64}} \in [-2^{127}, 2^{127})$ and $e \in \{1, \ldots, 63\}$ (the statement), the claim's precondition]

(L11) $z_{\text{fx64}} = \text{roundAway}(x_{\text{fx64}}/2^e)$

[(L1) to (L3), (L9), (L10)]

(L12) $\Rightarrow$ item 2

[(L11)]

$\square$ (item 2)

Proof of item 3.

(L13) $W_z = \text{u}_{128}(W_x \ll e)$

[[CryptoLine: `lemmas/fxp64_64/ops/mul2e/lem_mul2e.cl`]; $e \in \{1, \ldots, 63\}$ (the statement)]

(L14) $\forall a \in \mathbb{Z} :\ \text{u}_{128}(a \ll e) = a 2^e \bmod 2^{128}$

[$\ll$, u_w (Definition A.5)]

(L15) $W_z = W_x 2^e \bmod 2^{128}$

[(L13), (L14)]

(L16) $\Rightarrow$ item 3

[(L15)]

$\square$ (item 3)

Lemma I.7 (The objects of the integer conversions [to table])**.** *The object of* `fxp_of` *turns an integer into its number exactly. The objects of* `fxp_floor`*,* `fxp_trunc` *and* `fxp_rint` *return the floor, the truncation and the nearest integer of a number. Let:*

- $x \in 2^{-64}\mathbb{Z}$ *with* $x_{\text{fx64}} \in [-2^{127}, 2^{127})$ *(Definition A.5);*
- $i \in \{-2^{63}, \dots, 2^{63}-1\}$.

Define:

- $W_x := x_{\text{fx64}} \bmod 2^{128}$;
- $\mathcal{O}$*, the aarch64* `-O3` *objects of the routines below, each through its* `noinline` *wrapper (Homebrew clang 22.1.8, QEMU* `virt` *Cortex-A72);*
- W_z*, the word the object of* `fxp_of` *returns on* i*;*
- $z_{\text{fx64}} := \mathrm{s}_{128}(W_z)$ *(Definition A.5);*
- $z := 2^{-64} z_{\text{fx64}}$;
- j*, the integer each of* `fxp_floor`*,* `fxp_trunc` *and* `fxp_rint` *returns on* W_x*;*
- $\forall v \in \mathbb{R}:\ \operatorname{trunc} v := \operatorname{sgn}(v)\lfloor |v| \rfloor$ *(Fact A.6, item 5);*
- rint*, that of Fact A.6, item 5.*

Then:

1. *The object of* `fxp_of` *in* $\mathcal{O}$ *returns* $z = i$ *[CryptoLine:* `lemmas/fxp64_64/ops/of/lem_of.cl`*].*
2. *The object of* `fxp_floor` *in* $\mathcal{O}$ *returns* $j = \lfloor x \rfloor$ *[CryptoLine:* `lemmas/fxp64_64/ops/floor/lem_floor.cl`*].*
3. *The object of* `fxp_trunc` *in* $\mathcal{O}$ *returns* $j = \operatorname{trunc} x$ *[CryptoLine:* `lemmas/fxp64_64/ops/trunc/lem_trunc.cl`*].*
4. *The object of* `fxp_rint` *in* $\mathcal{O}$ *returns* $j \equiv \operatorname{rint} x \pmod{2^{64}}$ *[CryptoLine:* `lemmas/fxp64_64/ops/rint/lem_rint.cl`*].*

Proof.

COMPUTES w: the operand $(x_{\text{fx64}} + 2^{63}) \gg_{\mathrm{a}} 64$ of `fxp_rint`'s object

(L1) $\forall a \in \mathbb{Z}:\ a \gg_{\mathrm{a}} 64 = \lfloor a/2^{64} \rfloor$
[$\gg_{\mathrm{a}}$ (Definition A.5)]

(L2) $\forall a \in \mathbb{Z},\ a \geq 0:\ a \gg 64 = \lfloor a/2^{64} \rfloor$
[$\gg$ (Definition A.5)]

(L3) $x = x_{\text{fx64}} 2^{-64}$
[Definition A.5]

(L4) $\forall v \in \mathbb{Z},\ |v| < 2^{255}:\ \mathrm{s}_{256}(v) = v$
[s_w (Definition A.5)]

Proof of item 1.

(L5) $z_{\text{fx64}} = \mathrm{s}_{256}(i \ll 64)$
[[CryptoLine: `lemmas/fxp64_64/ops/of/lem_of.cl`]]

(L6) $|i2^{64}| \leq 2^{127}$
[$i \in \{-2^{63}, \dots, 2^{63}-1\}$]

(L7) $\forall a \in \mathbb{Z},\ |a2^{64}| < 2^{255}:\ \mathrm{s}_{256}(a \ll 64) = a2^{64}$
[$\ll$ (Definition A.5); (L4)]

(L8) $z_{\text{fx64}} = i2^{64}$
[(L5), (L6), (L7)]

(L9) $z = i$
[(L8); $z_{\text{fx64}} = 2^{64} z$ (Definition A.5)]

(L10) $\Rightarrow$ item 1
[(L9)]

□ (item 1)

Proof of item 2.

(L11) $j = x_{\mathrm{fx64}} \gg_{\mathrm{a}} 64$
[[CryptoLine: `lemmas/fxp64_64/ops/floor/lem_floor.cl`]; $x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L12) $j = \lfloor x \rfloor$
[(L1), (L3), (L11)]

(L13) $\Rightarrow$ item 2
[(L12)]

□ (item 2)

Proof of item 3.

(L14) $x \geq 0 \Rightarrow\ j = x_{\mathrm{fx64}} \gg 64$
[[CryptoLine: `lemmas/fxp64_64/ops/trunc/lem_trunc.cl`], its claim on 256 bits; (L4) at its operands, $x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L15) $x < 0 \Rightarrow\ j = -((-x_{\mathrm{fx64}}) \gg 64)$
[[CryptoLine: `lemmas/fxp64_64/ops/trunc/lem_trunc.cl`], its claim on 256 bits; (L4) at its operands, $x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L16) $j = \mathrm{sgn}(x)\lfloor |x| \rfloor$
[(L2), (L3), (L14), (L15)]

(L17) $\mathrm{sgn}(x)\lfloor |x| \rfloor = \mathrm{trunc}\, x$
[Fact A.6, item 5]

(L18) $j = \mathrm{trunc}\, x$
[(L16), (L17)]

(L19) $\Rightarrow$ item 3
[(L18)]

□ (item 3)

Proof of item 4.

(L20) $w \,\&\, 1 = w \bmod 2$
[& (Definition A.5)]

(L21) $x_{\mathrm{fx64}} \bmod 2^{64} = 2^{63} \Rightarrow\ j \equiv w - (w \bmod 2) \pmod{2^{64}}$
[[CryptoLine: `lemmas/fxp64_64/ops/rint/lem_rint.cl`]; (L20); $x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L22) $x_{\mathrm{fx64}} \bmod 2^{64} \neq 2^{63} \Rightarrow\ j \equiv w \pmod{2^{64}}$
[[CryptoLine: `lemmas/fxp64_64/ops/rint/lem_rint.cl`]; $x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L23) $w = \lfloor x + 1/2 \rfloor$
[(L1), (L3)]

(L24) $x_{\mathrm{fx64}} \bmod 2^{64} = 2^{63} \iff x - \lfloor x \rfloor = 1/2$
[(L3)]

(L25) $x - \lfloor x \rfloor = 1/2 \Rightarrow\ w = \lfloor x \rfloor + 1$
[(L23)]

(L26) $w - (w \bmod 2) \in \{w - 1, w\} \cap 2\mathbb{Z}$
[$w \in \mathbb{Z}$]

(L27) $x - \lfloor x \rfloor = 1/2 \Rightarrow\ \mathrm{rint}\, x = w - (w \bmod 2)$
[(L25), (L26); Fact A.6, item 5]

(L28) $x - \lfloor x \rfloor \neq 1/2 \Rightarrow\ \mathrm{rint}\, x = w$
[(L23); Fact A.6, item 5]

(L29) $j \equiv \mathrm{rint}\, x \pmod{2^{64}}$
[(L21), (L22), (L24), (L27), (L28)]

(L30) $\Rightarrow$ item 4
[(L29)]

□ (item 4)

Lemma I.8 (The objects of the comparisons [to table])**.** *The objects of* `fxp_lt`*,* `fxp_max` *and* `fxp_min` *compare two numbers of* $2^{-64}\mathbb{Z}$ *whose difference fits a word. Let:*

- $x, y \in 2^{-64}\mathbb{Z}$ *with* $x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$ *(Definition A.5).*

Define:

- $W_x := x_{\text{fx64}} \bmod 2^{128}$ *and* $W_y := y_{\text{fx64}} \bmod 2^{128}$*;*
- $\mathcal{O}$*, the aarch64* `-O3` *objects of the routines below, each through its* `noinline` *wrapper (Homebrew clang 22.1.8, QEMU* `virt` *Cortex-A72);*
- $j \in \{0, 1\}$*, the value* `fxp_lt` *returns on* (W_x, W_y)*;*
- W_z*, the word each of* `fxp_max` *and* `fxp_min` *returns on* (W_x, W_y)*;*
- $z_{\text{fx64}} := \mathrm{s}_{128}(W_z)$ *(Definition A.5);*
- $z := 2^{-64} z_{\text{fx64}}$*.*

Assume:

(A1) $-2^{127} \le x_{\text{fx64}} - y_{\text{fx64}} < 2^{127}$*.*

Then:

1. *The object of* `fxp_lt` *in* $\mathcal{O}$ *returns* $j = [x < y]$ *[CryptoLine:* `lemmas/fxp64_64/ops/lt/lem_lt.cl`*].*
2. *The object of* `fxp_max` *in* $\mathcal{O}$ *returns* $z = \max(x, y)$ *[CryptoLine:* `lemmas/fxp64_64/ops/max/lem_max.cl`*].*
3. *The object of* `fxp_min` *in* $\mathcal{O}$ *returns* $z = \min(x, y)$ *[CryptoLine:* `lemmas/fxp64_64/ops/min/lem_min.cl`*].*

Proof.

DEFINES $W_x <_{\mathrm{s}} W_y :\Leftrightarrow x_{\text{fx64}} < y_{\text{fx64}}$

DEFINES $W_y \le_{\mathrm{s}} W_x :\Leftrightarrow y_{\text{fx64}} \le x_{\text{fx64}}$

(L1) $W_x <_{\mathrm{s}} W_y \iff x < y$

[$<_{\mathrm{s}}$ (the proof's block); $x = x_{\text{fx64}} 2^{-64}$, $y = y_{\text{fx64}} 2^{-64}$ (Definition A.5)]

Proof of item 1.

(L2) $W_x <_{\mathrm{s}} W_y \Rightarrow\ j = 1$

[[CryptoLine: `lemmas/fxp64_64/ops/lt/lem_lt.cl`], under assumption A1; $x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L3) $W_y \le_{\mathrm{s}} W_x \Rightarrow\ j = 0$

[[CryptoLine: `lemmas/fxp64_64/ops/lt/lem_lt.cl`], under assumption A1; $x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L4) $j = [x < y]$

[(L1) to (L3)]

(L5) $\Rightarrow$ item 1

[(L4)]

□ (item 1)

Proof of item 2.

(L6) $W_x <_{\mathrm{s}} W_y \Rightarrow\ W_z = W_y$

[[CryptoLine: `lemmas/fxp64_64/ops/max/lem_max.cl`], under assumption A1; $x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L7) $W_y \le_{\mathrm{s}} W_x \Rightarrow\ W_z = W_x$

[[CryptoLine: `lemmas/fxp64_64/ops/max/lem_max.cl`], under assumption A1; $x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L8) $z = \max(x, y)$

[(L1), (L6), (L7); the number a word stores (Definition A.5)]

(L9) $\Rightarrow$ item 2

[(L8)]

□ (item 2)

Proof of item 3.

(L10) $W_x <_{\mathrm{s}} W_y \Rightarrow\ W_z = W_x$

[[CryptoLine: `lemmas/fxp64_64/ops/min/lem_min.cl`], under assumption A1; $x_{\mathrm{fx64}}, y_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L11) $W_y \leq_{\mathrm{s}} W_x \Rightarrow\ W_z = W_y$

[[CryptoLine: `lemmas/fxp64_64/ops/min/lem_min.cl`], under assumption A1; $x_{\mathrm{fx64}}, y_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$ (the statement)]

(L12) $z = \min(x, y)$

[(L1), (L10), (L11); the number a word stores (Definition A.5)]

(L13) $\Rightarrow$ item 3

[(L12)]

□ (item 3)

Corollary I.9 (The fixed-point arithmetic's constants [to table])**.** *At $u = 0$, the constants of the complex product, the split and the merge take the values below. Define:*

- $k_B := \sqrt{2}(3 + 2u)$ *(Lemma B.2);*
- $c_{\mathrm{split}} := (1 + u)(1 + u + \sqrt{2}\,\zeta)(1 + \sqrt{2}\,u(2 + u)) - 1$ *(Lemma G.16);*
- $k_D := (\sqrt{2}/2)(1 + u + \sqrt{2}\,\zeta)(1 + \sqrt{2}\,u(2 + u)) + k_B$ *(Lemma G.16);*
- $c_{\mathrm{merge}} := u + (1 + u)((1 + u + \sqrt{2}\,\zeta)(1 + \sqrt{2}\,u(2 + u)) - 1)$ *(Lemma G.18);*
- $k_E := 2\sqrt{2}((3 + 2u)(1 + u) + 1)$ *(Lemma G.18);*
- $e := (1 + u + \sqrt{2}\,\zeta)(1 + \sqrt{2}\,u(2 + u)) - 1$*;*
- $e_{\mathrm{mul}} := \sqrt{2}\,u(2 + u)$ *(Lemma B.2, item 3).*

Then

1. $k_B = 3\sqrt{2}$*;*
2. $c_{\mathrm{split}} = \sqrt{2}\,\zeta$*;*
3. $k_D = \frac{\sqrt{2}}{2}(1 + \sqrt{2}\,\zeta) + 3\sqrt{2}$*;*
4. $e = \sqrt{2}\,\zeta$*;*
5. $c_{\mathrm{merge}} = \sqrt{2}\,\zeta$*;*
6. $k_E = 8\sqrt{2}$*;*
7. $e_{\mathrm{mul}} = 0$.

Proof. (L1) $k_B = 3\sqrt{2}$

[$k_B = \sqrt{2}(3 + 2u)$ (Lemma B.2); Definition I.1: $u = 0$]

(L2) $\Rightarrow$ item 1

[(L1)]

(L3) $c_{\mathrm{split}} = \sqrt{2}\,\zeta$

[$c_{\mathrm{split}} = (1 + u)(1 + u + \sqrt{2}\,\zeta)(1 + \sqrt{2}\,u(2 + u)) - 1$ (Lemma G.16); Definition I.1: $u = 0$]

(L4) $\Rightarrow$ item 2

[(L3)]

(L5) $k_D = \frac{\sqrt{2}}{2}(1+\sqrt{2}\,\zeta) + 3\sqrt{2}$
$[k_D = (\sqrt{2}/2)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) + k_B$ (Lemma G.16); (L1); Definition I.1: $u = 0]$

(L6) $\Rightarrow$ item 3
[(L5)]

(L7) $e = \sqrt{2}\,\zeta$
[e (the statement); Definition I.1: $u = 0$]

(L8) $\Rightarrow$ item 4
[(L7)]

(L9) $c_{\text{merge}} = \sqrt{2}\,\zeta$
$[c_{\text{merge}} = u + (1+u)((1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1)$ (Lemma G.18); Definition I.1: $u = 0]$

(L10) $\Rightarrow$ item 5
[(L9)]

(L11) $k_E = 8\sqrt{2}$
$[k_E = 2\sqrt{2}((3+2u)(1+u)+1)$ (Lemma G.18); Definition I.1: $u = 0]$

(L12) $\Rightarrow$ item 6
[(L11)]

(L13) $e_{\text{mul}} = 0$
[e_{mul} (the statement); Definition I.1: $u = 0$]

(L14) $\Rightarrow$ item 7
[(L13)]

□ (items 1 to 7)

Lemma I.10 (The objects of the sampling's kernels [to table])**.** *Each kernel's object returns the words its algorithm's lines compute on its input words, with the operations of the word lemmas. Let:*

- $h \in \{2, \ldots, 10\}$*;*
- `g00`*, the array* g_{00} *each of* `fxpoly_LDL_fft`*,* `fxpoly_LDL_root_fft` *and* `fxp_ffsamp_fft` *reads;*
- `hm`*, the message array of* `fxpoly_apply_basis`*;*
- `qtfrac0` *and* `qtfrac1`*, the two input arrays of* `fxpoly_target_fft`*;*
- *Each input array holds any words of Definition A.5.*

Define:

- $W_{\widetilde{\psi_k}}$*, the words of* `FXP_GM`*;*
- $\mathcal{O}$*, the aarch64* `-O3` *objects (Homebrew clang 22.1.8, QEMU* `virt` *Cortex-A72) at* `logn` $= h$*, each call of* `fxp_mul`*,* `fxp_div` *and* `fxp_sqrt` *in them applied as its lemma;*
- $\oplus$*,* $\ominus$*,* $\otimes$ *and* fl*, the operations of Lemmas I.2, I.3, I.4, I.5 and I.6 on words modulo* 2^{128}*;*
- $\forall W \in \{0, \ldots, 2^{128}-1\} : Q(W)$*, the word the object of* `fxp_sqrt` *returns on* W *(Lemma I.5).*

Then

1. *Assume:*

   (A1) $h \geq 3$.

   The object of `fxpoly_FFT` *in* $\mathcal{O}$ *returns the words of lines 2 to 25 of* $\widetilde{\text{FFT}}$ *(Algorithm 14)* [CryptoLine: `lemmas/fxp64_64/fft_compose`].

2. *The object of* `fxpoly_split_fft` *in* $\mathcal{O}$ *returns the words of lines 4 and 6 of* $\widetilde{\text{split}}$ *(Algorithm 2)* [CryptoLine: `lemmas/fxp64_64/split_compose`].

3. *The object of* `fxpoly_split_selfadj_fft` *in* $\mathcal{O}$ *returns the words of lines 4 and 6 of* $\widetilde{\text{split}}_{\text{sa}}$ *(Algorithm 3)* [CryptoLine: `lemmas/fxp64_64/selfadj_compose`].

4. *The object of* `fxpoly_merge_fft` *in* $\mathcal{O}$ *returns the words of line 4 of* $\widetilde{\text{merge}}$ *(Algorithm 4) and of the sum and the difference after it [CryptoLine:* `lemmas/fxp64_64/merge_compose`*].*

5. *Assume:*

   (A2) $\forall k:\ \mathsf{g00}[k] \neq 0$.

   The object of `fxpoly_LDL_fft` *in* $\mathcal{O}$ *returns the words of lines 7 to 18 of* LDL† *(Algorithm 5) [CryptoLine:* `lemmas/fxp64_64/ldl_compose`*]; Figure 68 quotes its lemma's conditions at* $h = 2$.

6. *Assume:*

   (A3) $\forall k:\ \mathsf{g00}[k] \neq 0$.

   The object of `fxpoly_LDL_root_fft` *in* $\mathcal{O}$ *returns the words of lines 7 to 12 of* LDL† *and of line 6 of* ffsamp *(Algorithm 6) [CryptoLine:* `lemmas/fxp64_64/ldlroot_compose`*].*

7. *Assume:*

   (A4) $\forall k:\ \mathsf{g00}[k] \neq 0$.

   At a node of degree 2, the object of `fxp_ffsamp_fft` *in* $\mathcal{O}$ *returns the words of lines 7 to 18 of* LDL† *and of lines 1 to 18 of* deepest *(Algorithm 7), each square root* $\mathrm{fl}(\sqrt{x})$ *of those lines the word* $Q(W_x)$ *on the word* W_x *of* x*, each call of* SamplerZ *(Algorithm 8) left opaque [CryptoLine:* `lemmas/fxp64_64/ffsamp_compose`*].*

8. *On their input words* a *and* b *at each of the* 2^{h-1} *roots, the objects of* `fxpoly_mul_fft`*,* `fxpoly_add` *and* `fxpoly_sub` *in* $\mathcal{O}$ *return* $a \otimes b$*,* $a \oplus b$ *and* $a \ominus b$ *(Definition A.8) [CryptoLine:* `lemmas/fxp64_64/mul_fft_compose`*] [CryptoLine:* `lemmas/fxp64_64/addsub_compose`*].*

9. *Let:*

   - $f \in \{-128, \ldots, 127\}^{2^h}$*, an int8 array.*

   On f*, the object of* `fxpoly_set_small` *in* $\mathcal{O}$ *returns the words* $W_{f_{[k]}} = f_{[k],\mathrm{fx64}} \bmod 2^{128}$ *[CryptoLine:* `lemmas/fxp64_64/setsmall_compose`*].*

10. *On each of its* 2^h *input words* W_a*, the object of* `fxpoly_neg` *in* $\mathcal{O}$ *returns* $-W_a \bmod 2^{128}$ *[CryptoLine:* `lemmas/fxp64_64/neg_compose`*].*

11. *The object of* `fxpoly_gram_fft` *in* $\mathcal{O}$ *returns the words of lines 2 to 18 of* Gram *(Algorithm 13) at each of the* 2^{h-1} *roots [CryptoLine:* `lemmas/fxp64_64/gram_compose`*]. Its conjugates' imaginary parts are the words* $0 - b_{10,i}$ *and* $0 - b_{11,i}$ *of* `fxp_neg`*.*

12. *Assume:*

    (A5) $h \geq 3$*;*
    (A6) $\mathtt{hm} \in \{0, \ldots, 2^{16} - 1\}^{2^h}$*;*
    (A7) $\mathtt{qtfrac0}, \mathtt{qtfrac1} \in \{-2^{15}, \ldots, 2^{15} - 1\}^{2^h}$.

    The two objects of the center's first computation in $\mathcal{O}$ *return their algorithms' words [CryptoLine:* `lemmas/fxp64_64/center_compose`*].*

    - *Each coefficient is loaded as the word* $(0, \mathsf{h}(\mathsf{m})_{[k]})$.
    - *The harness's* `memmove` *copies 8-byte words.*
    - *The object of* `fxpoly_apply_basis` *in* $\mathcal{O}$ *returns the words of lines 9, 16 and 18 of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10).*
    - *Each residue is loaded as the word* $(0, qt_{\mathrm{frac},j,[k]})$*, sign-extended.*
    - *The object of* `fxpoly_target_fft` *in* $\mathcal{O}$ *returns the words of lines 7 and 12 of* $\text{center}_{\text{frac}}$ *(Algorithm 17).*

13. Assume:

(A8) $h \geq 3$.

The object of `fxpoly_iFFT` *in* $\mathcal{O}$ *writes, at each of its* $h-1$ *stages [L0:* `fxp/sign_fxpoly.c:52-75`*], at each pair* (x, y) *of the stage and its twiddle's conjugate* $\widetilde{s}$*, the words of* $x \oplus y$ *and* $(x \ominus y) \otimes \widetilde{s}$*; then the word of* $\mathrm{fl}(x/2^{h-1})$ *at each of its* 2^h *words* x *[L0:* `fxp/sign_fxpoly.c:76-80`*] [CryptoLine:* `lemmas/fxp64_64/ifft_compose`*].*

14. Assume:

(A9) $h = 3$.

The object of the harness's `caller` *in* $\mathcal{O}$ *calls* `fxpoly_split_fft` *on its own arrays, the call applied as the contract form of the CryptoLine lemma of item 2 at* $h = 3$*. At that call it returns the words of lines 4 and 6 of* split *(Algorithm 2) on its arrays [CryptoLine:* `lemmas/fxp64_64/splitcall_compose`*].*

Proof.

DEFINES $M(W_x, W_y)$, $D(W_x, W_y)$: the words `fxp_mul` (Lemma I.3) and `fxp_div` (Lemma I.4) return at the words W_x, W_y

DEFINES $\forall W \in \{0, \ldots, 2^{128}-1\}: \ H(W) := \mathrm{u}_{128}((\mathrm{s}_{128}(W) \gg_{\mathrm{a}} 1) + (W \,\&\, 1)(1 - (W \gg 127)))$, the claims' halving

DEFINES $W_{\texttt{INV}}$: the word of `FXP_INV_SIGMA` the code reads

DEFINES S_j, $j \in \{1, \ldots, 4\}$: the integer the j-th call of SamplerZ (Algorithm 8) in the line order of deepest returns

DEFINES $W_x \cdot_M W_y = (M(W_{x_r}, W_{y_r}) - M(W_{x_i}, W_{y_i})) + i\,(M(W_{x_r}, W_{y_i}) + M(W_{x_i}, W_{y_r})) \bmod 2^{128}$ for pairs of words W_x, W_y

DEFINES $\mathrm{FFT}_M(W_x)$: the words of line (L14)'s stages on the input words W_x, j from 0 to $h-2$

DEFINES $\widetilde{\mathrm{in}}_j$, j_1, j_2, $\widetilde{s}$: those of $\widetilde{\mathrm{FFT}}$ (Algorithm 14), in the lines of item 1

DEFINES $a := f(\psi)$, $b := f(-\psi)$ and $\widetilde{s}$, those of $\widetilde{\mathrm{split}}$ (Algorithm 2) and $\widetilde{\mathrm{split}}_{\mathrm{sa}}$ (Algorithm 3), in the lines of items 2, 3 and 14

DEFINES f_0, f_1, ψ, $\widetilde{s}$, $\widetilde{z}$, $\widetilde{a}$, $\widetilde{b}$: those of $\widetilde{\mathrm{merge}}$ (Algorithm 4), in the lines of item 4

DEFINES g_{00}, g_{01}, g_{11}, $\widetilde{\mu}$, $\widetilde{\mu}_r$, $\widetilde{\mu}_i$, $\widetilde{l}_{10}$, $\widetilde{d}_{11}$: those of LDL† (Algorithm 5) at the node, in the lines of items 5, 6 and 7; at item 6, $\widetilde{d}_{11}$ and q, those of ffsamp (Algorithm 6), line 6

DEFINES $\widetilde{t}_0$, $\widetilde{t}_1$, $\widetilde{z}_0$, $\widetilde{z}_1$, $\widetilde{tb}_0$, $1/\widetilde{\sigma}_1$, $1/\widetilde{\sigma}_0$: those of deepest (Algorithm 7), in the lines of item 7

DEFINES b_{jk}, $j, k \in \{0, 1\}$, $\widetilde{g}_{00}$, $\widetilde{g}_{01}$, $\widetilde{g}_{11}$: those of Gram (Algorithm 13), in the lines of item 11

DEFINES $\widetilde{t}_0$, $\widetilde{t}_1$, $\widetilde{b}_{01}$, $\widetilde{b}_{11}$, $\widetilde{(1/q)}$, $\widetilde{(-1/q)}$: those of ffSampling$^{\mathcal{F}}$ (Algorithm 10), and $\widetilde{t}_{\mathrm{frac},j}$, $qt_{\mathrm{frac},j}$: those of $\widetilde{\mathrm{center}}_{\mathrm{frac}}$ (Algorithm 17), in the lines of item 12

DEFINES W'_x: the word the scaling of `fxpoly_iFFT` writes at its word W_x, in the lines of item 13

Lemma I.3 at every pair of words W_x, W_y	This proof
Shared: x, y, W_x, W_y	
(I1) W_z $x, y \in 2^{-64}\mathbb{Z}$, $x_{\mathrm{fx64}}, y_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$	$M(W_x, W_y)$ (the proof's block) W_x, W_y, words (Definition A.5)
Its conclusion: $W_z = z_{\mathrm{fx64}} \bmod 2^{128}$	

(L1) $\forall W_x, W_y \in \{0, \ldots, 2^{128}-1\}: \ M(W_x, W_y) = \mathrm{fl}(W_x W_y)$

[(I1); z (Lemma I.3); Definition I.1, item 1, at $\times$; fl (the statement)]

(L2) $\forall W_x, W_y \in \{0, \ldots, 2^{128}-1\}: \ \mathrm{fl}(W_x W_y) = \mathrm{fl}(W_y W_x)$

[Definition I.1, item 1, at $\times$]

	Lemma I.2 at every pair of words W_x, W_y	This proof
	Shared: x, y, W_x, W_y W_z	$\mathrm{fl}(W_x + W_y)$, $\mathrm{fl}(W_x - W_y)$, $\mathrm{fl}(-W_x)$ (the statement)
(I2)	Its item 1: $W_z = (W_x + W_y) \bmod 2^{128}$	
	Its item 2: $W_z = (W_x - W_y) \bmod 2^{128}$	
	Its item 3: $W_z = (-W_x) \bmod 2^{128}$	

(L3) $\forall W_x, W_y \in \{0, \dots, 2^{128} - 1\} : \ \mathrm{fl}(W_x + W_y) = (W_x + W_y) \bmod 2^{128}$

[item 1 of (I2)]

(L4) $\forall W_x, W_y \in \{0, \dots, 2^{128} - 1\} : \ \mathrm{fl}(W_x - W_y) = (W_x - W_y) \bmod 2^{128}$

[item 2 of (I2)]

(L5) $\forall W_x \in \{0, \dots, 2^{128} - 1\} : \ \mathrm{fl}(-W_x) = (-W_x) \bmod 2^{128}$

[item 3 of (I2)]

(L6) $W_x \oplus W_y = (W_x + W_y) \bmod 2^{128}$ per part

[$\oplus$ (Definition A.8); (L3)]

(L7) $W_x \ominus W_y = (W_x - W_y) \bmod 2^{128}$ per part

[$\ominus$ (Definition A.8); (L3), (L5)]

(L8) $W_x \cdot_M W_y = W_x \otimes W_y$

[$\cdot_M$ (the proof's block); $\otimes$ (Definition A.8); (L1), (L3), (L4)]

(L9) $W_x \cdot_M W_y = W_y \cdot_M W_x$

[$\cdot_M$ (the proof's block); (L1), (L2)]

(L10) $\forall c \in \mathcal{F}_{\mathrm{fx}} : \ W_x \cdot_M W_c = W_x \otimes W_c$

[(L8) at $y := c$, $c_i = 0$; Definition I.1, item 1; (L2); $c \otimes a$, $a \otimes c$ (Definition A.8)]

	Lemma I.6 at every word W_x, at $e := h - 1$	This proof
	Shared: x, W_x W_z	$\mathrm{fl}(W_x/2)$, $\mathrm{fl}(W_x/2^{h-1})$ (the statement)
(I3)	e	$h - 1$ (the statement)
	$x \in 2^{-64}\mathbb{Z}$, $x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$	W_x, a word (Definition A.5)
	$e \in \{1, \dots, 63\}$	$h \in \{2, \dots, 10\}$ (the statement)
	Its item 1: $z_{\mathrm{fx64}} = \mathrm{roundAway}(x_{\mathrm{fx64}}/2)$	
	Its item 2: $z_{\mathrm{fx64}} = \mathrm{roundAway}(x_{\mathrm{fx64}}/2^e)$	

(L11) $\forall W \in \{0, \dots, 2^{128} - 1\} : \ \mathrm{s}_{128}(H(W)) = \mathrm{roundAway}(\mathrm{s}_{128}(W)/2)$

[H (the proof's block); $\gg_{\mathrm{a}}$, $\gg$, &, s_w, u_w (Definition A.5); roundAway (Definition I.1)]

(L12) $\forall W_x \in \{0, \dots, 2^{128} - 1\} : \ H(W_x) = \mathrm{fl}(W_x/2)$

[(L11); item 1 of (I3); $z_{\mathrm{fx64}} = \mathrm{s}_{128}(W_z)$ (Lemma I.6); s_w (Definition A.5)]

	Lemma I.4 at every pair of words W_x, W_y, $W_y \neq 0$	This proof
	Shared: x, y, W_x, W_y W_z	$D(W_x, W_y)$ (the proof's block)
(I4)	$x, y \in 2^{-64}\mathbb{Z}$, $x_{\mathrm{fx64}}, y_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$	W_x, W_y, words (Definition A.5)
	Assumption A1	The scope; s_w (Definition A.5)
	Its conclusion: $W_z = z_{\mathrm{fx64}} \bmod 2^{128}$	

(L13) $\forall W_x, W_y \in \{0, \dots, 2^{128} - 1\}, \ W_y \neq 0 : \ D(W_x, W_y) = \mathrm{fl}(W_x/W_y)$

[(I4); z (Lemma I.4); Definition I.1, item 1, at /; fl (the statement)]

Proof of item 1.

(L14) $\forall j \leq h - 2 : \ W_{\widetilde{\mathrm{in}}_{j+1}(j_1)} = W_{\widetilde{\mathrm{in}}_j(j_1)} + W_{\widetilde{\mathrm{in}}_j(j_2)} \cdot_M W_{\widetilde{s}} \bmod 2^{128}$

[[CryptoLine: `lemmas/fxp64_64/fft_compose`], $h = 3$ to 10; assumption A1]

(L15) $\forall j \le h-2:\ W_{\widetilde{\mathrm{in}}_{j+1}(j_2)} = W_{\widetilde{\mathrm{in}}_j(j_1)} - W_{\widetilde{\mathrm{in}}_j(j_2)} \cdot_M W_{\widetilde{s}} \bmod 2^{128}$

[[CryptoLine: `lemmas/fxp64_64/fft_compose`], $h = 3$ to 10; assumption A1]

(L16) $\Rightarrow$ item 1

[(L14), (L15); (L6), (L7), (L8)]

□ (item 1)

Proof of item 2.

(L17) $W_{\widetilde{f_0}} = H((W_a + W_b) \bmod 2^{128})$ per part

[[CryptoLine: `lemmas/fxp64_64/split_compose`], $h = 2$ to 10]

(L18) $W_{\widetilde{f_1}} = H(((W_a - W_b) \bmod 2^{128}) \cdot_M W_{\mathrm{conj}(\widetilde{s})})$ per part

[[CryptoLine: `lemmas/fxp64_64/split_compose`], $h = 2$ to 10]

(L19) $\Rightarrow$ item 2

[(L17), (L18); (L6), (L7), (L8), (L12)]

□ (item 2)

Proof of item 3.

(L20) $W_{\mathrm{Re}\,\widetilde{f_0}} = H((W_a + W_b) \bmod 2^{128})$

[[CryptoLine: `lemmas/fxp64_64/selfadj_compose`], $h = 2$ to 10]

(L21) $W_{\mathrm{Im}\,\widetilde{f_0}} = 0$

[[CryptoLine: `lemmas/fxp64_64/selfadj_compose`], $h = 2$ to 10]

(L22) $W_{\widetilde{f_1}} = M(H((W_a - W_b) \bmod 2^{128}), W_{\mathrm{Re}\,\widetilde{s}}) + i\,M(H((W_a - W_b) \bmod 2^{128}), W_{\mathrm{Im\ conj}(\widetilde{s})})$

[[CryptoLine: `lemmas/fxp64_64/selfadj_compose`], $h = 2$ to 10]

(L23) $\Rightarrow$ item 3

[(L20), (L21), (L22); (L1), (L3), (L4), (L12); $c \otimes a$ (Definition A.8)]

□ (item 3)

Proof of item 4.

(L24) $W_{\widetilde{z}} = W_{f_1(\psi^2)} \cdot_M W_{\widetilde{s}} \bmod 2^{128}$

[[CryptoLine: `lemmas/fxp64_64/merge_compose`], $h = 2$ to 10]

(L25) $W_{\widetilde{a}} = W_{f_0(\psi^2)} + W_{\widetilde{z}} \bmod 2^{128}$

[[CryptoLine: `lemmas/fxp64_64/merge_compose`], $h = 2$ to 10]

(L26) $W_{\widetilde{b}} = W_{f_0(\psi^2)} - W_{\widetilde{z}} \bmod 2^{128}$

[[CryptoLine: `lemmas/fxp64_64/merge_compose`], $h = 2$ to 10]

(L27) $\Rightarrow$ item 4

[(L24), (L25), (L26); (L6), (L7), (L8)]

□ (item 4)

Proof of item 5.

(L28) $W_{\widetilde{\mu_r}} = D(W_{g_{01,r}}, W_{g_{00}})$

[[CryptoLine: `lemmas/fxp64_64/ldl_compose`], $h = 2$ to 10; assumption A2]

(L29) $W_{\widetilde{\mu_i}} = D(W_{g_{01,i}}, W_{g_{00}})$

[[CryptoLine: `lemmas/fxp64_64/ldl_compose`], $h = 2$ to 10; assumption A2]

(L30) $W_{\widetilde{l_{10}}} = \mathrm{conj}\, W_{\widetilde{\mu}}$

[[CryptoLine: `lemmas/fxp64_64/ldl_compose`], $h = 2$ to 10; assumption A2]

(L31) $W_{\widetilde{d_{11}}} = W_{g_{11}} - (M(W_{\widetilde{\mu_r}}, W_{g_{01,r}}) + M(W_{\widetilde{\mu_i}}, W_{g_{01,i}})) \bmod 2^{128}$

[[CryptoLine: `lemmas/fxp64_64/ldl_compose`], $h = 2$ to 10; assumption A2]

(L32) $\forall x \in \{g_{01,r}, g_{01,i}\}:\ D(W_x, W_{g_{00}}) = \mathrm{fl}(W_x / W_{g_{00}})$

[(L13); assumption A2]

(L33) $\Rightarrow$ item 5

[(L28) to (L32); (L1), (L3), (L4), (L5)]

□ (item 5)

Proof of item 6.

(L34) $W_{\widetilde{\mu_r}} = D(W_{g_{01,r}}, W_{g_{00}})$
[[CryptoLine: `lemmas/fxp64_64/ldlroot_compose`], $h = 2$ to 10; assumption A3]

(L35) $W_{\widetilde{\mu_i}} = D(W_{g_{01,i}}, W_{g_{00}})$
[[CryptoLine: `lemmas/fxp64_64/ldlroot_compose`], $h = 2$ to 10; assumption A3]

(L36) $W_{\widetilde{l_{10}}} = \operatorname{conj} W_{\widetilde{\mu}}$
[[CryptoLine: `lemmas/fxp64_64/ldlroot_compose`], $h = 2$ to 10; assumption A3]

(L37) $W_{\widetilde{d_{11}}} = D(W_{q^2}, W_{g_{00}})$
[[CryptoLine: `lemmas/fxp64_64/ldlroot_compose`], $h = 2$ to 10; assumption A3]

(L38) $\forall x \in \{g_{01,r}, g_{01,i}, q^2\} :\ D(W_x, W_{g_{00}}) = \mathrm{fl}(W_x / W_{g_{00}})$
[(L13); assumption A3]

(L39) $\Rightarrow$ item 6
[(L34) to (L38); (L5)]

□ (item 6)

Proof of item 7.

(L40) $W_{\widetilde{\mu_r}} = D(W_{g_{01,r}}, W_{g_{00}})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L41) $W_{\widetilde{\mu_i}} = D(W_{g_{01,i}}, W_{g_{00}})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L42) $W_{\widetilde{l_{10}}} = \operatorname{conj} W_{\widetilde{\mu}}$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L43) $W_{\widetilde{d_{11}}} = W_{g_{11}} - (M(W_{\widetilde{\mu_r}}, W_{g_{01,r}}) + M(W_{\widetilde{\mu_i}}, W_{g_{01,i}})) \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L44) $\forall x \in \{g_{01,r}, g_{01,i}\} :\ D(W_x, W_{g_{00}}) = \mathrm{fl}(W_x / W_{g_{00}})$
[(L13); assumption A4]

(L45) $W_{1/\widetilde{\sigma_1}} = M(Q(W_{\widetilde{d_{11}}}), W_{\mathtt{INV}})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L46) $S_1 \leftarrow \mathrm{SamplerZ}(W_{\mathrm{Re}\,\widetilde{t_1}}, W_{1/\widetilde{\sigma_1}})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L47) $S_2 \leftarrow \mathrm{SamplerZ}(W_{\mathrm{Im}\,\widetilde{t_1}}, W_{1/\widetilde{\sigma_1}})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L48) $W_{\widetilde{z_1}} = (S_1 2^{64} \bmod 2^{128},\ S_2 2^{64} \bmod 2^{128})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L49) $W_{\widetilde{tb_0}} = W_{\widetilde{t_0}} + ((W_{\widetilde{t_1}} - W_{\widetilde{z_1}}) \bmod 2^{128}) \cdot_M W_{\widetilde{l_{10}}} \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L50) $W_{1/\widetilde{\sigma_0}} = M(Q(W_{g_{00}}), W_{\mathtt{INV}})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L51) $S_3 \leftarrow \mathrm{SamplerZ}(W_{\mathrm{Re}\,\widetilde{tb_0}}, W_{1/\widetilde{\sigma_0}})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L52) $S_4 \leftarrow \mathrm{SamplerZ}(W_{\mathrm{Im}\,\widetilde{tb_0}}, W_{1/\widetilde{\sigma_0}})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L53) $W_{\widetilde{z_0}} = (S_3 2^{64} \bmod 2^{128},\ S_4 2^{64} \bmod 2^{128})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_compose`], at a node of degree 2; assumption A4]

(L54) $\Rightarrow$ item 7
[(L40) to (L53); Q (the statement); (L1), (L3) to (L8)]

□ (item 7)

Proof of item 8.

(L55) $\texttt{mul_fft}(W_a, W_b) = W_a \cdot_M W_b \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/mul_fft_compose`], $\forall \psi$, $h = 2$ to 10]

(L56) $\texttt{add}(W_a, W_b) = W_a + W_b \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/addsub_compose`], $h = 2$ to 10]

(L57) $\texttt{sub}(W_a, W_b) = W_a - W_b \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/addsub_compose`], $h = 2$ to 10]

(L58) $\Rightarrow$ item 8
[(L55), (L56), (L57); (L6), (L7), (L8)]

□ (item 8)

Proof of items 9 and 10.

(L59) $\texttt{fxpoly_set_small}(f)_{[k]} = (0,\ f_{[k]} \bmod 2^{64})$
[[CryptoLine: `lemmas/fxp64_64/setsmall_compose`], $h = 2$ to 10; (W_0, W_1), the limbs (Definition A.5)]

(L60) $\texttt{fxpoly_neg}(W_a)_{[k]} = 0 - W_{a_{[k]}} \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/neg_compose`], $h = 2$ to 10]

(L61) $\Rightarrow$ item 9
[(L59); $W = W_0 + 2^{64} W_1$ (Definition A.5); $2^{64} \cdot 2^{64} = 2^{128}$]

(L62) $\Rightarrow$ item 10
[(L60)]

□ (items 9 and 10)

Proof of item 11.

(L63) $W_{\widetilde{g_{00}}} = \sum_{x \in \{b_{00,r}, b_{00,i}, b_{01,r}, b_{01,i}\}} M(W_x, W_x) \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/gram_compose`]; $h = 2$ to 10]

(L64) $W_{\widetilde{g_{01}}} = W_{b_{00}} \cdot_M (W_{b_{10,r}}, 0 - W_{b_{10,i}}) + W_{b_{01}} \cdot_M (W_{b_{11,r}}, 0 - W_{b_{11,i}}) \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/gram_compose`]; $h = 2$ to 10]

(L65) $W_{\widetilde{g_{11}}} = \sum_{x \in \{b_{10,r}, b_{10,i}, b_{11,r}, b_{11,i}\}} M(W_x, W_x) \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/gram_compose`]; $h = 2$ to 10]

(L66) $\operatorname{conj} W_b = (W_{b_r}, (0 - W_{b_i}) \bmod 2^{128})$
[$\operatorname{conj} a$ (Definition A.8); (L5)]

(L67) $\Rightarrow$ item 11
[(L63) to (L66); (L1) at $W_y := W_x$; (L3), (L6), (L8)]

□ (item 11)

Proof of item 12.

(L68) $W_{\widetilde{t_0}} = (\mathrm{FFT}_M(W_{\mathsf{h(m)}}) \cdot_M W_{\widetilde{b_{11}}}) \cdot_M W_{\widetilde{(1/q)}} \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/center_compose`], $h = 3$ to 10; FFT_M (the proof's block); assumptions A5, A6, A7]

(L69) $W_{\widetilde{t_1}} = (W_{\widetilde{b_{01}}} \cdot_M \mathrm{FFT}_M(W_{\mathsf{h(m)}})) \cdot_M W_{\widetilde{(-1/q)}} \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/center_compose`], $h = 3$ to 10; FFT_M (the proof's block); assumptions A5, A6, A7]

(L70) $W_{\widetilde{t_{\mathrm{frac},j}}} = \mathrm{FFT}_M(W_{qt_{\mathrm{frac},j}}) \cdot_M W_{\widetilde{(1/q)}} \bmod 2^{128}$
[[CryptoLine: `lemmas/fxp64_64/center_compose`], $h = 3$ to 10; FFT_M (the proof's block); assumptions A5, A6, A7]

(L71) $\Rightarrow$ item 12
[(L68), (L69), (L70); (L14), (L15), (L16) at the loaded words; (L8), (L9), (L10)]

□ (item 12)

Proof of item 13.

(L72) $W_{x \oplus y} = W_x + W_y \bmod 2^{128}$ per part
[[CryptoLine: `lemmas/fxp64_64/ifft_compose`], $h = 3$ to 10; assumption A8]

(L73) $W_{(x \ominus y) \otimes \widetilde{s}} = ((W_x - W_y) \bmod 2^{128}) \cdot_M W_{\widetilde{s}}$
[[CryptoLine: `lemmas/fxp64_64/ifft_compose`], $h = 3$ to 10; assumption A8]

(L74) $\mathrm{s}_{128}(W'_x) = (\mathrm{s}_{128}(W_x) + 2^{h-2} - [\mathrm{s}_{128}(W_x) < 0]) \gg_\mathrm{a} (h-1)$ per part
[[CryptoLine: `lemmas/fxp64_64/ifft_compose`], its scaling on 192 bits; assumption A8]

(L75) $\forall v \in \mathbb{Z}\ \forall e \geq 1 :\ (v + 2^{e-1} - [v < 0]) \gg_\mathrm{a} e = \mathrm{roundAway}(v/2^e)$
[$\gg_\mathrm{a}$ (Definition A.5); roundAway (Definition I.1)]

(L76) $\mathrm{s}_{128}(W'_x) = \mathrm{roundAway}(\mathrm{s}_{128}(W_x)/2^{h-1})$ per part
[(L74); (L75) at $e := h - 1$]

(L77) $W'_x = \mathrm{fl}(W_x/2^{h-1})$ per part
[(L76); item 2 of (I3); $z_{\mathrm{fx64}} = \mathrm{s}_{128}(W_z)$ (Lemma I.6); s_w (Definition A.5)]

(L78) $\Rightarrow$ item 13
[(L72), (L73), (L77); (L6), (L7), (L8)]

□ (item 13)

Proof of item 14.

(L79) $W_{\widetilde{f_0}} = H((W_a + W_b) \bmod 2^{128})$ per part
[[CryptoLine: `lemmas/fxp64_64/splitcall_compose`], on the caller's arrays, the call applied as the contract form of `lemmas/fxp64_64/split_compose` at $h = 3$; assumption A9]

(L80) $W_{\widetilde{f_1}} = H(((W_a - W_b) \bmod 2^{128}) \cdot_M W_{\mathrm{conj}(\widetilde{s})})$ per part
[[CryptoLine: `lemmas/fxp64_64/splitcall_compose`], on the caller's arrays, the call applied as the contract form of `lemmas/fxp64_64/split_compose` at $h = 3$; assumption A9]

(L81) $\Rightarrow$ item 14
[(L79), (L80); (L6), (L7), (L8), (L12)]

□ (item 14)

```
const hn = 2;
array uint64[2] g00[2] @ 0x400805c8;
array uint64[2] g01[4] @ 0x40080608;
array uint64[2] g11[2] @ 0x400805e8;

{ true && x0 = 0x2@64 /\ x1 = 0x400805c8@64 /\ x2 = 0x40080608@64 /\ x3 = 0x400805e8@64
      /\ and [ g00[$i] > 0@128 for i = 0 .. $hn - 1 ] }

{ forall i < $hn {
    let mu_re[$i] = limbs 64 [r0, r1] from apply d.main (limbs 64 [x0, x1] = g01[$i],
      limbs 64 [x2, x3] = g00[$i]) at div_re$i;
    let mu_im[$i] = limbs 64 [r0, r1] from apply d.main (limbs 64 [x0, x1] = g01[$i + $hn],
      limbs 64 [x2, x3] = g00[$i]) at div_im$i;
    let m_re[$i] = limbs 64 [r0, r1] from apply m.main (limbs 64 [x0, x1] = mu_re[$i],
      limbs 64 [x2, x3] = g01[$i]) at mul_re$i;
    let m_im[$i] = limbs 64 [r0, r1] from apply m.main (limbs 64 [x0, x1] = mu_im[$i],
      limbs 64 [x2, x3] = g01[$i + $hn]) at mul_im$i;
    claim true && g11'[$i] = g11[$i] - (m_re[$i] + m_im[$i]) /\ g01'[$i] = mu_re[$i]
      /\ g01'[$i + $hn] = 0@128 - mu_im[$i];
  } }
```

Figure 68: The declarations, the precondition and the postcondition of the CryptoLine lemma of item 5 at $h = 2$, as its file states them (`lemmas/fxp64_64/ldl_compose/lem_ldln_2.cl`); a line longer than the page is wrapped at a space.

Lemma I.11 (The object of the sampling recursion [to table])**.** *The recursion's object makes the calls of its algorithm's lines on the cells they state; with the kernels' objects, it returns its algorithm's words. Let:*

- $h \in \{2, \ldots, 10\}$;
- $\texttt{root} \in \{0, 1\}$;
- $\texttt{tmp}$, *the area* `fxp_ffsamp_fft_inner` *reads and writes, of any words of Definition A.5;*
- $\texttt{g00}$, *the array* g_{00} *each call of* `fxpoly_LDL_fft` *and* `fxpoly_LDL_root_fft` *and each deepest level reads.*

Define:

- $\mathcal{O}_{\text{rec}}$, *the aarch64* `-O3` *object of* `fxp_ffsamp_fft_inner` *(Homebrew clang 22.1.8, QEMU* `virt` *Cortex-A72), each call in it of a kernel, of* `fxp_mul`, `fxp_div`, `fxp_sqrt`, *of* `fxp_sampler_next` *and of* `fxp_ffsamp_fft_inner` *an interface, its outputs free;*
- $W_{\texttt{INV}} := \texttt{FXP_INV_SIGMA}[h]$, *the stored words;*
- $\forall W \in \{0, \ldots, 2^{128} - 1\} : \; Q(W)$, *the word the object of* `fxp_sqrt` *returns on* W *(Lemma I.5).*

Then

1. *At* $\texttt{logn} = h$ *and* $\texttt{root}$, *on every* $\texttt{tmp}$, *the object* $\mathcal{O}_{\text{rec}}$ *makes the calls of lines 3 to 35 of* ffsamp *(Algorithm 6) on the cells they state and returns the words of the last merge [CryptoLine:* `lemmas/fxp64_64/ffsamp_dataflow`*].*
   - `fxpoly_LDL_fft` *is called at line 3; at* $\texttt{root} = 1$, `fxpoly_LDL_root_fft` *at lines 3 and 6.*
   - `fxpoly_splitself_adj_fft` *is called at lines 13 and 27.*
   - `fxpoly_split_fft` *and the recursive call, at* $\texttt{logn} = h - 1$ *and* $\texttt{root} = 0$ *on the area from chunk* 14, *are called at lines 19 and 33.*
   - `fxpoly_merge_fft` *is called at lines 21 and 35.*
   - `fxpoly_sub`, `fxpoly_mul_fft` *and* `fxpoly_add` *are called at line 25.*
2. *At* $\texttt{logn} = 1$ *inside* $\mathcal{O}_{\text{rec}}$ *at* $\texttt{logn} = h$, *on every* $\texttt{tmp}$, *the deepest level makes the calls of* `fxp_div`, `fxp_mul`, `fxp_sqrt` *and* `fxp_sampler_next` *of lines 7 to 18 of* LDL† *(Algorithm 5) and of lines 1 to 18 of* deepest *(Algorithm 7) at* $\texttt{INV_SIGMA} := W_{\texttt{INV}}$ *on the words they state, and returns the words of its samples [CryptoLine:* `lemmas/fxp64_64/ffsamp_dataflow`*].*
3. *Assume:*

   (A1) $\forall k : \; \texttt{g00}[k] \neq 0$.

   With each call the object of Lemma I.10, items 2, 3, 4, 5, 6 and 8, or of Lemmas I.3, I.4 and I.5, the object of `fxp_ffsamp_fft_inner` *at* $\texttt{logn} = h$ *and* $\texttt{root}$ *returns the words of* ffsamp *(Algorithm 6) in* $\mathcal{F}_{\text{fx}}$ *at* $\texttt{INV_SIGMA} := W_{\texttt{INV}}$ *on every* $\texttt{tmp}$, *each square root* $\text{fl}(\sqrt{x})$ *of its lines the word* $Q(W_x)$ *on the word* W_x *of* x, *each call of* SamplerZ *(Algorithm 8) left opaque [CryptoLine:* `lemmas/fxp64_64/ffsamp_dataflow`*].*

Proof.

DEFINES $\mathcal{O}(h', r)$, $h' \leq h$, $r \in \{0, 1\}$: the words $\mathcal{O}_{\text{rec}}$ returns at $\texttt{logn} = h'$ and $\texttt{root} = r$ on $\texttt{tmp}$, each interface any function

DEFINES level$(h', r, \mathcal{P})$: the words lines 3 to 35 of ffsamp (Algorithm 6) return at $m = 2^{h'}$ and $\texttt{root} = r$ on $\texttt{tmp}$, each call of a kernel the function of its interface in $\mathcal{O}(h', r)$, each recursive call $\mathcal{P}$

DEFINES deep(w): the words lines 7 to 18 of LDL† (Algorithm 5) and deepest (Algorithm 7) return at $\texttt{INV_SIGMA} := w$ on $\texttt{tmp}$, each call of `fxp_div`, `fxp_mul`, `fxp_sqrt` and of SamplerZ the function of its interface in $\mathcal{O}(1, 0)$

DEFINES alg(h', r): the words ffsamp returns in $\mathcal{F}_{\text{fx}}$ at $m = 2^{h'}$, $\texttt{root} = r$ and $\texttt{INV_SIGMA} := W_{\texttt{INV}}$ on $\texttt{tmp}$, each square root $\text{fl}(\sqrt{x})$ the word $Q(W_x)$ on the word W_x of x, each call of SamplerZ opaque

Proof of item 1.

(L1) $\forall h' \in [2,h]\ \forall r \in \{0,1\}:\ \mathcal{O}(h',r) = \mathrm{level}(h',r,\mathcal{O}(h'-1,0))$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_dataflow`], $h = 2$ to 10, `root` $= 0$ and 1, each call an interface]

(L2) $\Rightarrow$ item 1
[(L1); level (the proof's block)]

□ (item 1)

Proof of item 2.

(L3) $\mathcal{O}(1,0) = \mathrm{deep}(W_{\mathtt{INV}})$
[[CryptoLine: `lemmas/fxp64_64/ffsamp_dataflow`], the deepest level inside the recursion at $h = 2$ to 10, each call an interface]

(L4) $\Rightarrow$ item 2
[(L3); deep (the proof's block)]

□ (item 2)

Proof of item 3.

(I1)

Lemma I.4 at each division of the deepest level, $x \in \{g_{01,r}, g_{01,i}\}$	This proof
x	x (the scope)
y	g_{00} (the statement)
W_z	$W_{\widetilde{\mu_r}}, W_{\widetilde{\mu_i}}$ (line 7 of LDL† (Algorithm 5))
$x, y \in 2^{-64}\mathbb{Z},\ x_{\mathrm{fx64}}, y_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$	W_x, $W_{g_{00}}$, words (Definition A.5); the statement
Assumption A1	Assumption A1
Its conclusion: $W_z = z_{\mathrm{fx64}} \bmod 2^{128}$	

(I2)

Lemma I.3 at each call of `fxp_mul` of the deepest level, on its words W_x, W_y	This proof
Shared: x, y, W_x, W_y, W_z (the scope)	
$x, y \in 2^{-64}\mathbb{Z},\ x_{\mathrm{fx64}}, y_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$	W_x, W_y, words (Definition A.5)
Its conclusion: $W_z = z_{\mathrm{fx64}} \bmod 2^{128}$	

(L5) $\mathrm{deep}(W_{\mathtt{INV}}) = \mathrm{alg}(1,0)$
[(I1); (I2); ffsamp (Algorithm 6) at $m = 2$; Definition I.1, item 1, at $\times$ and /; Q (the statement; Lemma I.5); deep, each interface of $\mathcal{O}(1,0)$ the object of (I1), of (I2) or of `fxp_sqrt`, and alg (the proof's block)]

(L6) $\mathcal{O}(1,0) = \mathrm{alg}(1,0)$
[(L3) at the interfaces of (L5); (L5)]

(L7) $\forall h' \in [2,h]:\ h' \le 10$
[the statement]

Lemma I.10 at $\texttt{logn} = h'$, every $h' \in [2, h]$	This proof
h	h' (the scope)
$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
`g00`	`g00` (the statement)
$h \in \{2, \ldots, 10\}$	(L7)
each input array of words	The statement; Definition A.5
Assumption A2	Assumption A1
Assumption A3	Assumption A1

Its item 2: The object of `fxpoly_split_fft` in $\mathcal{O}$ returns the words of lines 4 and 6 of $\widetilde{\text{split}}$ (Algorithm 2).

(I3) Its item 3: The object of `fxpoly_split_selfadj_fft` in $\mathcal{O}$ returns the words of lines 4 and 6 of $\widetilde{\text{split}}_{\text{sa}}$ (Algorithm 3).

Its item 4: The object of `fxpoly_merge_fft` in $\mathcal{O}$ returns the words of line 4 of $\widetilde{\text{merge}}$ (Algorithm 4) and of the sum and the difference after it.

Its item 5: The object of `fxpoly_LDL_fft` in $\mathcal{O}$ returns the words of lines 7 to 18 of LDL† (Algorithm 5).

Its item 6: The object of `fxpoly_LDL_root_fft` in $\mathcal{O}$ returns the words of lines 7 to 12 of LDL† and of line 6 of ffsamp (Algorithm 6).

Its item 8: On their input words a and b at each of the 2^{h-1} roots, the objects of `fxpoly_mul_fft`, `fxpoly_add` and `fxpoly_sub` in $\mathcal{O}$ return $a \otimes b$, $a \oplus b$ and $a \ominus b$ (Definition A.8).

(L8) $\forall h' \in [2, h]\ \forall r \in \{0, 1\} :\ \text{level}(h', r, \text{alg}(h' - 1, 0)) = \text{alg}(h', r)$
[items 2, 3, 4, 5, 6 and 8 of (I3); ffsamp (Algorithm 6) at $m = 2^{h'}$; level, each interface of a kernel in $\mathcal{O}(h', r)$ the object of (I3), and alg (the proof's block)]

(L9) $\forall h' \in [2, h]\ \forall r \in \{0, 1\} :\ \mathcal{O}(h' - 1, 0) = \text{alg}(h' - 1, 0) \Rightarrow\ \mathcal{O}(h', r) = \text{alg}(h', r)$
[(L1) at the interfaces of (L8); (L8)]

(L10) $\Rightarrow\ \forall r \in \{0, 1\} :\ \mathcal{O}(h, r) = \text{alg}(h, r)$
[induction on h': (L6) the base, (L9) the step]

(L11) $\Rightarrow$ item 3
[(L10); alg (the proof's block)]

□ (item 3)

Lemma I.12 (Words in range and rounded results [to table])**.** *A word congruent to a value in range reads as that value, and each operation's rounded result is bounded by its exact one. Let:*

- $W_x \in \{0, \ldots, 2^{128} - 1\}$*, a word of Definition A.5;*
- $W_y \in \{0, \ldots, 2^{128} - 1\}$*, a word of Definition A.5;*
- $V \in \mathbb{Z}$*.*

Define:

- $x_{\text{fx64}} := \text{s}_{128}(W_x)$ *(Definition A.5);*
- $y_{\text{fx64}} := \text{s}_{128}(W_y)$ *(Definition A.5);*
- $\forall v \in \mathbb{R} :\ \text{roundAway}(v) := \text{sgn}(v)\ \lfloor |v| + 1/2 \rfloor$ *(Definition I.1);*
- $\forall v \in \mathbb{Z}\ \forall d > 0 :\ \text{roundAway}(v, d) := \text{roundAway}(v/d)$ *(Definition I.1).*

Then

1. *Assume:*

   (A1) $W_x \equiv V \pmod{2^{128}}$*;*

   (A2) $V \in [-2^{127}, 2^{127})$*.*

   Then $x_{\text{fx64}} = V$*.*

2. $|\text{roundAway}(x_{\text{fx64}}y_{\text{fx64}}, 2^{64})| \le |x_{\text{fx64}}||y_{\text{fx64}}|/2^{64} + 1/2$.

3. *Assume:*

   (A3) $y_{\text{fx64}} \neq 0$.

   Then $|\text{roundAway}(x_{\text{fx64}}2^{64}/y_{\text{fx64}})| \le |x_{\text{fx64}}|2^{64}/|y_{\text{fx64}}| + 1/2$.

4. $|\text{roundAway}(x_{\text{fx64}}/2)| \le |x_{\text{fx64}}|/2 + 1/2$.

5. *Let:*

   - $o \in \{\text{add}, \text{sub}, \text{neg}, \text{mul}, \text{div}, \text{half}\}$.

   Define:

   - W_{z_o}*, the word* `fxp_`o *returns on* (W_x, W_y)*, the* W_z *at* o *(Lemma I.2, items 1 to 3; Lemmas I.3 and I.4; Lemma I.6, item 1);*
   - $z_{o,\text{fx64}} := \text{s}_{128}(W_{z_o})$ *(Definition A.5);*
   - V_o*, by*

$$V_{\text{add}} := x_{\text{fx64}} + y_{\text{fx64}}, \qquad V_{\text{sub}} := x_{\text{fx64}} - y_{\text{fx64}}, \qquad V_{\text{neg}} := -x_{\text{fx64}},$$
$$V_{\text{mul}} := \text{roundAway}(x_{\text{fx64}}y_{\text{fx64}}, 2^{64}), \qquad V_{\text{div}} := \text{roundAway}(x_{\text{fx64}}2^{64}/y_{\text{fx64}}),$$
$$V_{\text{half}} := \text{roundAway}(x_{\text{fx64}}/2).$$

   Assume:

   (A4) $o = \text{div} \Rightarrow\ y_{\text{fx64}} \neq 0$*;*
   (A5) $V_o \in [-2^{127}, 2^{127})$.

   Then $z_{o,\text{fx64}} = V_o$.

Proof. (L1) $x_{\text{fx64}} \equiv W_x \pmod{2^{128}}$
[Definition A.5]

(L2) $W_x \equiv V \pmod{2^{128}}$
[assumption A1]

(L3) $\Rightarrow\ x_{\text{fx64}} \equiv V \pmod{2^{128}}$
[(L1), (L2)]

(L4) $\Rightarrow\ x_{\text{fx64}} = V$
[(L3); $x_{\text{fx64}} \in [-2^{127}, 2^{127})$ (Definition A.5); assumption A2]

(L5) $\Rightarrow$ item 1
[(L4)]

(L6) $\forall v \in \mathbb{Z}\ \forall d > 0 :\ |\text{roundAway}(v, d)| \le |v|/d + 1/2$
[roundAway (Definition I.1); Fact A.41, item 22]

(L7) $\Rightarrow$ item 2
[(L6) at $(v, d) = (x_{\text{fx64}}y_{\text{fx64}}, 2^{64})$]

(L8) $\Rightarrow$ item 3
[(L6) at $(v, d) = (x_{\text{fx64}}2^{64}, |y_{\text{fx64}}|)$; roundAway (Definition I.1); assumption A3]

(L9) $\Rightarrow$ item 4
[(L6) at $(v, d) = (x_{\text{fx64}}, 2)$]

(I1)

Lemma I.2 at every $o \in \{\text{add}, \text{sub}, \text{neg}\}$	This proof
Shared: $x_{\text{fx64}}, y_{\text{fx64}}, W_x, W_y$ W_z	W_{z_o} (the statement)
Its item 1: $W_z = (W_x + W_y) \bmod 2^{128}$	
Its item 2: $W_z = (W_x - W_y) \bmod 2^{128}$	
Its item 3: $W_z = (-W_x) \bmod 2^{128}$	

(L10) $\forall o \in \{\text{add}, \text{sub}, \text{neg}\} : \ W_{z_o} \equiv V_o \pmod{2^{128}}$

[(I1); (L1); Definition A.5; V_o (the statement)]

(I2)

Lemma I.3 at (W_x, W_y)	This proof
Shared: $x_{\text{fx64}}, y_{\text{fx64}}, W_x, W_y$	
W_z	$W_{z_{\text{mul}}}$ (the statement)
$x, y \in 2^{-64}\mathbb{Z}, \ x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$	W_x, W_y, words (Definition A.5)
Its conclusion: $W_z = z_{\text{fx64}} \bmod 2^{128}$	

(L11) $W_{z_{\text{mul}}} \equiv V_{\text{mul}} \pmod{2^{128}}$

[(I2); (L1); Definition A.5; V_{mul} (the statement)]

(I3)

Lemma I.4 at (W_x, W_y)	This proof
Shared: $x_{\text{fx64}}, y_{\text{fx64}}, W_x, W_y$	
W_z	$W_{z_{\text{div}}}$ (the statement)
$x, y \in 2^{-64}\mathbb{Z}, \ x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$	W_x, W_y, words (Definition A.5)
Assumption A1	Assumption A4
Its conclusion: $W_z = z_{\text{fx64}} \bmod 2^{128}$	

(L12) $W_{z_{\text{div}}} \equiv V_{\text{div}} \pmod{2^{128}}$

[(I3); (L1); Definition A.5; V_{div} (the statement)]

(I4)

Lemma I.6, item 1 at W_x	This proof
Shared: x_{fx64}, W_x	
W_z	$W_{z_{\text{half}}}$ (the statement)
z_{fx64}	$z_{\text{half,fx64}}$ (the statement)
$x \in 2^{-64}\mathbb{Z}, \ x_{\text{fx64}} \in [-2^{127}, 2^{127})$	W_x, a word (Definition A.5)
Its item 1: $z_{\text{fx64}} = \text{roundAway}(x_{\text{fx64}}/2)$	

(I5)

Lemma I.12, item 1 at every $o \in \{\text{add}, \text{sub}, \text{neg}, \text{mul}, \text{div}\}$	This proof
W_x	W_{z_o} (the statement)
V	V_o (the statement)
Assumption A1	(L10), (L11), (L12)
Assumption A2	Assumption A5
Its conclusion: $x_{\text{fx64}} = V$	

(L13) $\Rightarrow \ \forall o \in \{\text{add}, \text{sub}, \text{neg}, \text{mul}, \text{div}\} : \ z_{o,\text{fx64}} = V_o$

[(I5)]

(L14) $\Rightarrow \ z_{\text{half,fx64}} = V_{\text{half}}$

[(I4); V_{half} (the statement)]

(L15) $\Rightarrow$ item 5

[(L13), (L14)]

□

I.1.2 The interval arithmetic of the tail checks

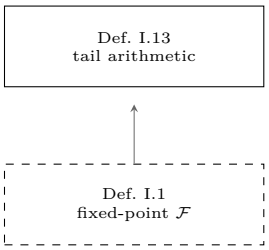


Figure 69: Dependencies, Appendix I.1.2.

Definition I.13 (The arithmetic of the tail checks [to table])**.** The tail checks compute on endpoints in $2^{-160}\mathbb{Z}$: in intervals rounded outward, in compact intervals rounded outward, and in upper bounds rounded up. Define:

- The formats
  - $\upsilon := 2^{-160}$;
  - $\mathcal{W} := \{x \in \upsilon\mathbb{Z} : -2^{159} \le x < 2^{159}\}$ [L0: `fxp/fxi.h:26-28`];
  - $\forall x \in \mathbb{R}:\ \lfloor x \rfloor_\upsilon := \upsilon\lfloor x/\upsilon \rfloor$;
  - $\forall x \in \mathbb{R}:\ \lceil x \rceil_\upsilon := \upsilon\lceil x/\upsilon \rceil$;
  - $\mathcal{J} := \{[a,b] : a, b \in \mathcal{W},\ a \le b\}$ [L0: `fxp/fxi.h:37-40`];
  - $\mathcal{J}_\mathrm{c} := \{[\ell, \ell + w\upsilon] : \ell \in \upsilon\mathbb{Z},\ -2^{31} \le \ell < 2^{31},\ w \in \mathbb{Z},\ 0 \le w < 2^{64}\}$ [L0: `fxp/fxi.h:600-603`];
  - $\zeta_\mathrm{op} := 2^{-65}$ (Definition I.1);
  - W_x, that of Definition A.5;
- The conversions
  - $\forall i \in \mathbb{Z},\ -2^{63} \le i < 2^{63}:$ `fxw_of_int`$(i) := i \in \mathcal{W}$ [L0: `fxp/fxi.h:223`];
  - $\forall x \in \mathcal{F}_\mathrm{fx},\ -2^{63} \le x < 2^{63}:$ `fxw_of_fxp`$(W_x) := x \in \mathcal{W}$ [L0: `fxp/fxi.h:205`].

We define the arithmetic by

1. $\forall x \in \mathcal{W}:$ `fxi_point`$(x) := [x, x]$ [L0: `fxp/fxi.h:337`];
2. $\forall [a,b], [c,d] \in \mathcal{J},\ a + c, b + d \in \mathcal{W}:$ `fxi_add`$([a,b],[c,d]) := [a + c, b + d]$ [L0: `fxp/fxi.h:352`];
3. $\forall [a,b], [c,d] \in \mathcal{J},\ a - d, b - c \in \mathcal{W}:$ `fxi_sub`$([a,b],[c,d]) := [a - d, b - c]$ [L0: `fxp/fxi.h:367`];
4. $\forall [a,b] \in \mathcal{J},\ -a \in \mathcal{W}:$ `fxi_neg`$([a,b]) := [-b, -a]$ [L0: `fxp/fxi.h:381`];
5. $\forall [a,b] \in \mathcal{J},\ b + \upsilon \in \mathcal{W}:$ `fxi_half`$([a,b]) := [\lfloor a/2 \rfloor_\upsilon, \lceil b/2 \rceil_\upsilon]$ [L0: `fxp/fxi.h:395`];
6. $\forall [a,b], [c,d] \in \mathcal{J},\ \max(|a|,|b|)\max(|c|,|d|) < 2^{158}:$

   $$\texttt{fxi_mul}([a,b],[c,d]) := [\lfloor \min(ac, ad, bc, bd) \rfloor_\upsilon, \lceil \max(ac, ad, bc, bd) \rceil_\upsilon]$$

   [L0: `fxp/fxi.c:30`];
7. $\forall [a,b] \in \mathcal{J},\ a^2, b^2 < 2^{158}$ [L0: `fxp/fxi.c:34`]:
   - At $a < 0 \le b$: `fxi_sqr`$([a,b]) := [0, \lceil \max(a^2, b^2) \rceil_\upsilon]$;
   - At $0 \le a \vee b < 0$: `fxi_sqr`$([a,b]) := [\lfloor \min(a^2, b^2) \rfloor_\upsilon, \lceil \max(a^2, b^2) \rceil_\upsilon]$;
8. $\forall [a,b], [c,d] \in \mathcal{J},\ c > 0,\ |a|, |b| < 2^{158}c:$ `fxi_div`$([a,b],[c,d]) := [\lfloor \min(a/c, a/d) \rfloor_\upsilon, \lceil \max(b/c, b/d) \rceil_\upsilon]$ [L0: `fxp/fxi.c:130`];
9. $\forall [c,d] \in \mathcal{J},\ c > 0:$ `fxi_inv`$([c,d]) := [\lfloor 1/d \rfloor_\upsilon, \lceil 1/c \rceil_\upsilon]$ [L0: `fxp/fxi.c:141`];
10. $\forall [a,b] \in \mathcal{J},\ a \ge 0:$ `fxi_sqrt`$([a,b]) := [\lfloor \sqrt{a} \rfloor_\upsilon, \lceil \sqrt{b} \rceil_\upsilon]$ [L0: `fxp/fxi.c:203`];

11. $\forall x_r, x_i, y_r, y_i \in \mathcal{J},\ \max_{x\in x_r\cup x_i}|x|\max_{y\in y_r\cup y_i}|y| < 2^{157}$: $\texttt{xcmul}(x_r, x_i, y_r, y_i) := (\texttt{fxi_sub}(\texttt{fxi_mul}(x_r, y_r), \texttt{fxi_mul}(x_i, y_i)), \texttt{fxi_add}(\texttt{fxi_mul}(x_r, y_i), \texttt{fxi_mul}(x_i, y_r)))$ [L0: `fxp/fxi.c:212`];

12. $\forall [a, b] \in \mathcal{J},\ |a|, |b| < 2^{158}$: $\texttt{fxi_mag}([a, b]) := \max(|a|, |b|)$ [L0: `fxp/fxi.h:436`];

13. $\forall x, y \in \mathcal{W},\ 0 \le x, y < 2^{31}$: $\texttt{fxw_mulu}(x, y) := \lceil xy \rceil_\upsilon$ [L0: `fxp/fxi.c:15`];

14. $\forall x \in \mathcal{W},\ x \ge 0,\ x + \upsilon \in \mathcal{W}$: $\texttt{fxw_halfu}(x) := \lceil x/2 \rceil_\upsilon$ [L0: `fxp/fxi.c:21`];

15. $\texttt{FXW_U65} := \zeta_{\text{op}}$ [L0: `fxp/fxi.c:13`];

16. $\forall [a, b] \in \mathcal{J},\ [a, b] \in \mathcal{J}_\text{c}$: $\texttt{fxc_of_fxi}([a, b]) := [a, b]$ [L0: `fxp/fxi.h:615`];

17. $\forall [\ell, \ell + w\upsilon], [\ell', \ell' + w'\upsilon] \in \mathcal{J}_\text{c}$: $\texttt{fxc_add}([\ell, \ell + w\upsilon], [\ell', \ell' + w'\upsilon]) := [\ell + \ell', \ell + \ell' + (w + w')\upsilon]$ and $\texttt{fxc_sub}([\ell, \ell + w\upsilon], [\ell', \ell' + w'\upsilon]) := [\ell - \ell' - w'\upsilon, \ell - \ell' + w\upsilon]$ [L0: `fxp/fxi.h:671`] [L0: `fxp/fxi.h:698`];

18. $\forall [\ell, \ell + w\upsilon] \in \mathcal{J}_\text{c}$: $\texttt{fxc_half}([\ell, \ell + w\upsilon]) := [\lfloor \ell/2 \rfloor_\upsilon, \lceil (\ell + w\upsilon)/2 \rceil_\upsilon]$ [L0: `fxp/fxi.h:732`];

19. $\forall [\ell, \ell + w\upsilon] \in \mathcal{J}_\text{c}\ \forall W \in \mathcal{F}_\text{fx}$: $\texttt{fxc_mulw}([\ell, \ell + w\upsilon], W) := [\lfloor \min(\ell W, (\ell + w\upsilon)W) \rfloor_\upsilon, \lceil \max(\ell W, (\ell + w\upsilon)W) \rceil_\upsilon]$ [L0: `fxp/fxi.h:825`];

20. $\forall [\ell, \ell + w\upsilon], [\ell', \ell' + w'\upsilon] \in \mathcal{J}_\text{c}$: $\texttt{fxc_mult}([\ell, \ell + w\upsilon], [\ell', \ell' + w'\upsilon]) := [\lfloor \min(\ell\ell', (\ell + w\upsilon)\ell') - (|\ell| + w\upsilon)w'\upsilon \rfloor_\upsilon, \lceil \max(\ell\ell', (\ell + w\upsilon)\ell') + (|\ell| + w\upsilon)w'\upsilon \rceil_\upsilon]$ [L0: `fxp/fxi.h:855`];

21. $\forall [\ell, \ell + w\upsilon] \in \mathcal{J}_\text{c}$: $\texttt{fxc_mag}([\ell, \ell + w\upsilon]) := |\ell| + w\upsilon$ [L0: `fxp/fxi.h:750`];

22. e [L0: `fxp/fxi.h:37-40`], over the operations of a check since its start, where $e = 0$: $e := 1$ at an operation on one of the causes below, and $e := 0$ otherwise:
    - At $x \notin [-2^{31}, 2^{31}) \vee y \notin [-2^{31}, 2^{31})$ (item 13);
    - At $|\ell| + w\upsilon \ge 2^{31}$ (item 20);
    - At $\ell' + w'\upsilon \ge 2^{31}$ (item 17, `fxc_sub`);
    - At $w = 2^{64} - 1$ (item 18);
    - At $c \le 0$ (items 8 and 9);
    - At $a < 0$ (item 10);
    - At a product or a quotient of magnitude at least 2^{159} (items 6, 7, 8, 9 and 11);
    - At $[a, b] \notin \mathcal{J}_\text{c}$ (item 16);
    - At a compact interval outside $\mathcal{J}_\text{c}$ (items 17, 19 and 20).

I.1.3 The tail checks in code

Algorithm 15 describes the three tail checks of a key at one center; Algorithm 16 the bounds $\mu^\uparrow$ and $B^\uparrow$; Definition I.14 states the thresholds M_n, D_n and B_n; Definitions I.15, I.16, I.17, I.18 and I.19 the quantities the checks compute.

How each quantity is computed. Each quantity is computed in the style its bound needs, on endpoints in $2^{-160}\mathbb{Z}$ (Definition I.13). The exact objects are computed in intervals that hold them: the twiddles, the key's images and Gram matrix entries, the exact tree's l_{10} and leaf diagonals, and the leaves' deviations (lines 3 to 15). The message rounding sites are computed as upper bounds, ζ_{op} per site (tailbounds (Algorithm 16), lines 4 to 11). The columns of the remainder and of $K^\mathcal{J}$ are computed in compact intervals, and the row sums take their magnitudes (lines 13 to 22 of tailbounds). The signer's own words, its computed tree and its leaves' $\texttt{isigma}_i$, are taken as points, read exactly (lines 9 and 10 of tailcheck).

The checks trust no rounding of the signer. The checks trust no rounding of the signer's fixed point: every endpoint is an exact rational, and each operation rounds its result outward or up (Definition I.13). That the C functions do, and that each of the three computed bounds lies at or above its quantity, is **Hypothesis I.91**, a code-alignment hypothesis, tested on a sample of keys (Statistics I.23, item 12).

The error word. The error word e records a failed operation: an operand beyond its length, a divisor at most 0, a negative radicand or a result beyond its limbs sets it, and no operation clears it (Definition I.13, item 22). A nonzero e makes the three verdicts 0 (lines 20 to 22), and the key generation regenerates the key. A sum, a difference or a negation whose result leaves $\mathcal{W}$ sets no bit: items 2, 3 and 4 of Definition I.13 take a result in $\mathcal{W}$ as a precondition.

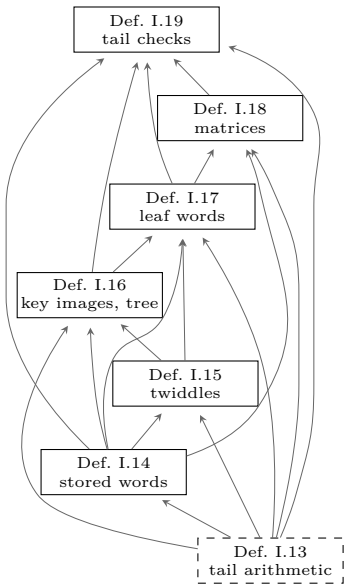


Figure 70: Dependencies, Appendix I.1.3.

Algorithm 15 tailcheck(f, g, F, G, c), the three tail checks of a key at one center, in the arithmetic of Definition I.13 [L0: `fxp/kgen_fx.c:516-618`] [L0: `fxp/kgen_fx.c:1690-1785`]

Input: (f, g, F, G) (keygen (Algorithm 11), line 3); $n \in \{512, 1024\}$; $c \in \{t, t_{\text{frac}}\}$ (Definition A.25); $M_n, D_n, B_n, \tau_K^{\uparrow} \in \upsilon\mathbb{Z}$ and $(1/s)^{\mathcal{J}} \in \mathcal{J}$, the words stored at n and c [L0: `fxp/fxp_consts.h: 2098-2117`]

Output (code): $(ok_\mu, ok_\delta, ok_B) \in \{0,1\}^3$; `tail_check_at` $= ok_\mu \wedge ok_\delta \wedge ok_B$ [L0: `fxp/kgen_fx.c: 1783-1784`]

Postcondition: $ok_\mu = 1 \Rightarrow \ \mu^{\uparrow} \le M_n$; $ok_\delta = 1 \Rightarrow \ \delta^{\uparrow} \le D_n$; $ok_B = 1 \Rightarrow \ B^{\uparrow} \le B_n$

Postcondition: under **Hypothesis I.91**, (f, g, F, G) a checked key (Definition 5.5), `tail_check_at` $= 1$, $\forall \mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$: $\delta^{\uparrow} \ge \bar{\delta}_K$ (**item 5**); $\mu^{\uparrow} \ge \mu_{\text{key}}$ (**item 4**); $B^{\uparrow} \ge \bar{B}_K$ (**item 6**); $\bar{\delta}_K$, μ_{key} and $\bar{B}_K$, those of Definition 4.12, items 1, 2 and 3, at $\mathcal{F}_{\text{fx}}$, the key, c, $\mathsf{h}(\mathsf{m})$ and the τ_K of Definition I.14

In the proofs: e, Ψ_k, $\hat{p}^{\mathcal{J}}$, $g_{00}^{\mathcal{J}}$, $g_{01}^{\mathcal{J}}$, $g_{11}^{\mathcal{J}}$, $l_{10,\nu}^{\mathcal{J}}$, $d_i^{\mathcal{J}}$, $\widetilde{B}$, $\widetilde{l}_{10,\nu}$, $\mathtt{isigma}_i$, Σ_i, $\delta^{\uparrow}$, $\mu^{\uparrow}$, $B^{\uparrow}$

1: $e \leftarrow 0$ ▷ [L0: `fxp/kgen_fx.c:325`]

2: $N \leftarrow 2n$

3: $(\Psi_k)_{k<1024} \leftarrow \mathtt{fxi_twiddles}()$ ▷ [L0: `fxp/kgen_fx.c:530`] [L0: `fxp/fxi.c:237-260`]

4: $\forall p \in \{f, g, F, G\} : \ \hat{p}^{\mathcal{J}} \leftarrow \text{FFT}^{\mathcal{J}}(p)$ ▷ Definition I.13, item 1 [L0: `fxp/kgen_fx.c:345-346`] [L0: `fxp/kgen_fx.c:550-553`]

5: $(g_{00}^{\mathcal{J}}, g_{01}^{\mathcal{J}}, g_{11}^{\mathcal{J}}) \leftarrow \text{Gram}^{\mathcal{J}} \begin{pmatrix} \hat{g}^{\mathcal{J}} & -\hat{f}^{\mathcal{J}} \\ \hat{G}^{\mathcal{J}} & -\hat{F}^{\mathcal{J}} \end{pmatrix}$ ▷ [L0: `fxp/kgen_fx.c:558-567`]

6: $((l_{10,\nu}^{\mathcal{J}})_\nu, (d_i^{\mathcal{J}})_{i \le N}) \leftarrow \text{ffLDL}^{\dagger\mathcal{J}}(g_{00}^{\mathcal{J}}, g_{01}^{\mathcal{J}}, g_{11}^{\mathcal{J}})$ ▷ [L0: `fxp/kgen_fx.c:568`]

7: $\widetilde{B} \leftarrow \widetilde{\text{FFT}} \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}$ ▷ [L0: `fxp/kgen_fx.c:1701-1710`]

8: $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11}) \leftarrow \text{Gram}(\widetilde{B})$ ▷ [L0: `fxp/kgen_fx.c:1711`]

9: $((\widetilde{l}_{10,\nu})_\nu, (\mathtt{isigma}_i)_{i \le N}) \leftarrow \mathtt{ctree}(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$ ▷ LDL†, line 12; ffsamp, line 6; deepest, line 3 [L0: `fxp/kgen_fx.c:1715`]

10: $\forall i \le N : \ \Sigma_i \leftarrow \mathtt{fxi_inv}([\mathtt{isigma}_i, \mathtt{isigma}_i])$ ▷ Definition I.13, item 1 [L0: `fxp/kgen_fx.c:1721-1722`]

11: $\forall i \le N : \ \mathtt{sig2}_i \leftarrow \mathtt{fxw_mulu}(\max \Sigma_i, \max \Sigma_i)$ ▷ [L0: `fxp/kgen_fx.c:1723`]

12: $\forall i \le N : \ \mathtt{w2}_i \leftarrow \mathtt{fxw_mulu}(\mathtt{isigma}_i, \mathtt{isigma}_i)$ ▷ [L0: `fxp/kgen_fx.c:1724`]

13: $\forall i \le N : \ y_i \leftarrow \mathtt{fxi_mul}(\mathtt{fxi_sqrt}(d_i^{\mathcal{J}}), (1/s)^{\mathcal{J}})$ ▷ [L0: `fxp/kgen_fx.c:1735-1736`]

14: $\forall i \le N : \ x_i \leftarrow \mathtt{fxi_div}(y_i, [\mathtt{isigma}_i, \mathtt{isigma}_i])$ ▷ Definition I.13, item 1 [L0: `fxp/kgen_fx.c:1737-1738`]

15: $\delta^{\uparrow} \leftarrow \max_{i \le N} \mathtt{fxi_mag}(\mathtt{fxi_sub}(x_i, [1, 1]))$ ▷ $\delta^{\uparrow} \ge \bar{\delta}_K$ (Definition 4.12, item 1; **Hypothesis I.91, item 5**) [L0: `fxp/kgen_fx.c:1739`]

16: **if** $\delta^{\uparrow} > D_n$ **then** ▷ [L0: `fxp/kgen_fx.c:1745-1746`]

17: **return** $(0, 0, 0)$

18: **end if**

19: $(\mu^{\uparrow}, B^{\uparrow}) \leftarrow \text{tailbounds}(c)$ ▷ the state of lines 3 to 15

20: $ok_\delta \leftarrow [e = 0 \wedge \delta^{\uparrow} \le D_n]$

21: $ok_\mu \leftarrow [e = 0 \wedge \mu^{\uparrow} \le M_n]$

22: $ok_B \leftarrow [e = 0 \wedge B^{\uparrow} \le B_n]$ ▷ [L0: `fxp/kgen_fx.c:1783`]

23: **return** $(ok_\mu, ok_\delta, ok_B)$

Algorithm 16 tailbounds(c), the upper bounds $\mu^\uparrow$ and $B^\uparrow$ of the tail checks at one center, in the arithmetic of Definition I.13 [L0: `fxp/kgen_fx.c:1748-1778`]

Input: $c \in \{t, t_{\text{frac}}\}$; n, N, $\tau_K^\uparrow$, $\widetilde{B}$, $(\widetilde{l}_{10,\nu})_\nu$, $(l^{\mathcal{J}}_{10,\nu})_\nu$, Ψ_k, Σ_i, $\texttt{sig2}_i$, $\texttt{w2}_i$ and e (tailcheck (Algorithm 15), line 19)

Output (code): $(\mu^\uparrow, B^\uparrow, e)$

Postcondition: under **Hypothesis I.91**, (f, g, F, G) a checked key (Definition 5.5), $\texttt{tail_check_at} = 1$ (tailcheck (Algorithm 15)), $\forall \mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$: $\mu^\uparrow \geq \mu_{\text{key}}$ (**item 4**); $B^\uparrow \geq \bar{B}_K$ (**item 6**); μ_{key} and $\bar{B}_K$, those of Definition 4.12, items 2 and 3, at $\mathcal{F}_{\text{fx}}$, the key, c, $\mathsf{h}(\mathsf{m})$ and the τ_K of Definition I.14

In the proofs: $m_i^\uparrow$, $\texttt{msg_acc}_i$, $\texttt{a_r}_i$, $\texttt{b_r}_i$, $\texttt{mu_acc}_i$, $\texttt{ka}_i$, $\texttt{kb}_i$

if $c = t_{\text{frac}}$ **then**
  $N_{\text{m}} \leftarrow 2n$
  $h_c \leftarrow \lfloor q/2 \rfloor$
  $\forall j \in \{0, 1\}$: $\texttt{a}_j \leftarrow \texttt{msb_const}(\texttt{msb_fft}(), \widetilde{(1/q)})$ ▷ [L0: `fxp/kgen_fx.c:829-832`]
else
  $N_{\text{m}} \leftarrow n$
  $h_c \leftarrow q - 1$
  $\texttt{a}_1 \leftarrow \texttt{msb_const}(\texttt{msb_cmul}(\texttt{msb_fft}(), |\widetilde{b}_{01}|), \widetilde{(-1/q)})$ ▷ [L0: `fxp/kgen_fx.c:834-841`]
  $\texttt{a}_0 \leftarrow \texttt{msb_const}(\texttt{msb_cmul}(\texttt{msb_fft}(), |\widetilde{b}_{11}|), \widetilde{(1/q)})$ ▷ [L0: `fxp/kgen_fx.c:838-842`]
end if
$(m_i^\uparrow)_{i \leq N} \leftarrow \texttt{msb_rec}(\texttt{a}_0, \texttt{a}_1)$ ▷ [L0: `fxp/kgen_fx.c:844`]
$\forall i \leq N$: $(\texttt{msg_acc}_i, \texttt{a_r}_i, \texttt{mu_acc}_i, \texttt{ka}_i, \texttt{kb}_i) \leftarrow (0, 0, 0, 0, 0)$ ▷ [L0: `fxp/kgen_fx.c:1750-1756`]
for all $j \in \{0, 8, \dots, N_{\text{m}} - 8\}$ **do**
  $V \leftarrow \texttt{exc_block}(c, j)$ ▷ $V \in \mathcal{J}_{\text{c}}^{N \times 8}$ [L0: `fxp/kgen_fx.c:1759-1761`]
  $\forall i \leq N$: $\texttt{msg_acc}_i \leftarrow \texttt{msg_acc}_i + \sum_{k<8} \texttt{fxc_mag}(V_{ik})$ ▷ [L0: `fxp/kgen_fx.c:989-993`]
end for
for all $j \in \{0, 8, \dots, N - 8\}$ **do**
  $V \leftarrow \texttt{exc_block}(c, N_{\text{m}} + j)$ ▷ [L0: `fxp/kgen_fx.c:1759-1761`]
  $\forall i \leq N$: $\texttt{a_r}_i \leftarrow \texttt{a_r}_i + \sum_{k<8} \texttt{fxw_mulu}(\texttt{fxc_mag}(V_{ik}), \max \Sigma_{j+k})$ ▷ [L0: `fxp/kgen_fx.c:995-999`]
end for
$\forall i \leq N$: $\texttt{b_r}_i \leftarrow \texttt{fxw_mulu}(h_c, \texttt{msg_acc}_i) + m_i^\uparrow + 2^{-120}$ ▷ [L0: `fxp/kgen_fx.c:1762-1766`]
for all $j \in \{0, 8, \dots, N - 8\}$ **do**
  $V \leftarrow \texttt{exd_block}(j)$ ▷ [L0: `fxp/kgen_fx.c:1768-1770`]
  $\forall i \leq N \; \forall k < 8$: $|V|_{ik} \leftarrow \texttt{fxc_mag}(V_{ik})$ ▷ [L0: `fxp/kgen_fx.c:1020`]
  $\forall i \leq N$: $\texttt{mu_acc}_i \leftarrow \texttt{mu_acc}_i + \sum_{k<8} \texttt{fxw_mulu}(\texttt{fxw_mulu}(|V|_{ik}, |V|_{ik}), \texttt{sig2}_{j+k})$
  $\forall i \leq N$: $\texttt{ka}_i \leftarrow \texttt{ka}_i + \sum_{k<8} \texttt{fxw_mulu}(|V|_{ik}, \texttt{a_r}_{j+k})$
  $\forall i \leq N$: $\texttt{kb}_i \leftarrow \texttt{kb}_i + \sum_{k<8} \texttt{fxw_mulu}(|V|_{ik}, \texttt{b_r}_{j+k})$ ▷ [L0: `fxp/kgen_fx.c:1021-1023`]
end for
$\mu^\uparrow \leftarrow \sum_{i \leq N} \texttt{fxw_mulu}(\texttt{w2}_i, \texttt{mu_acc}_i)$ ▷ $\mu^\uparrow \geq \mu_{\text{key}}$ (Definition 4.12, item 2; **Hypothesis I.91, item 4**) [L0: `fxp/kgen_fx.c:1773`]
$\forall i \leq N$: $\texttt{b_rem}_i \leftarrow \texttt{fxw_mulu}(\tau_K^\uparrow, \texttt{a_r}_i + \texttt{ka}_i) + \texttt{b_r}_i + \texttt{kb}_i$ ▷ [L0: `fxp/kgen_fx.c:1774-1775`]
$B^\uparrow \leftarrow \sum_{i \leq N} \texttt{fxw_mulu}(\texttt{w2}_i, \texttt{fxw_mulu}(\texttt{b_rem}_i, \texttt{b_rem}_i))$ ▷ $B^\uparrow \geq \bar{B}_K$ (Definition 4.12, item 3; **Hypothesis I.91, item 6**) [L0: `fxp/kgen_fx.c:1776-1777`]
return $(\mu^\uparrow, B^\uparrow)$

Definition I.14 (The tail checks' stored words [to table])**.** The tail checks read the words the code stores at the degree n and the center c. Let:

- (f, g, F, G) be a checked key (Definition 5.5) of degree n;
- $c \in \{t, t_{\text{frac}}\}$ be a center (Definition A.25).

Define:

- The arithmetic
  - $\upsilon := 2^{-160}$, $\forall x \in \mathbb{R} :\ \lfloor x \rfloor_\upsilon := \upsilon \lfloor x/\upsilon \rfloor$, $\forall x \in \mathbb{R} :\ \lceil x \rceil_\upsilon := \upsilon \lceil x/\upsilon \rceil$, $\mathcal{W} := \{x \in \upsilon\mathbb{Z} : -2^{159} \le x < 2^{159}\}$, $\mathcal{J} := \{[a,b] : a,b \in \mathcal{W},\ a \le b\}$ (Definition I.13);
- The parameters
  - $q := 12289$ (Definition A.13);
  - $N := 2n$ (Definition A.25);
  - $N_{\mathrm{m}} := \begin{cases} n & c = t \\ 2n & c = t_{\mathrm{frac}} \end{cases}$ (tailbounds (Algorithm 16)) [L0: `fxp/kgen_fx.c:1692`];
  - $h_c := \begin{cases} q-1 & c = t \\ \lfloor q/2 \rfloor & c = t_{\mathrm{frac}} \end{cases}$ (tailbounds (Algorithm 16)) [L0: `fxp/kgen_fx.c:1762`];
- The stored words
  - $M_n := \begin{cases} \lceil 2^{-112.85} \rceil_\upsilon & (n,c) = (512,t) \\ \lceil 2^{-110.64} \rceil_\upsilon & (n,c) = (1024,t) \\ \lceil 2^{-112.85} \rceil_\upsilon & (n,c) = (512,t_{\mathrm{frac}}) \\ \lceil 2^{-110.64} \rceil_\upsilon & (n,c) = (1024,t_{\mathrm{frac}}) \end{cases}$, the stored words [L0: `fxp/fxp_consts.h:2102`] [L0: `fxp/fxp_consts.h:2106`] [L0: `fxp/fxp_consts.h:2110`] [L0: `fxp/fxp_consts.h:2114`];
  - $D_n := \begin{cases} \lceil 2^{-57.95} \rceil_\upsilon & (n,c) = (512,t) \\ \lceil 2^{-57.38} \rceil_\upsilon & (n,c) = (1024,t) \\ \lceil 2^{-57.95} \rceil_\upsilon & (n,c) = (512,t_{\mathrm{frac}}) \\ \lceil 2^{-57.38} \rceil_\upsilon & (n,c) = (1024,t_{\mathrm{frac}}) \end{cases}$, the stored words [L0: `fxp/fxp_consts.h:2103`] [L0: `fxp/fxp_consts.h:2107`] [L0: `fxp/fxp_consts.h:2111`] [L0: `fxp/fxp_consts.h:2115`];
  - $B_n := \begin{cases} \lceil 2^{-73.16} \rceil_\upsilon & (n,c) = (512,t) \\ \lceil 2^{-71.19} \rceil_\upsilon & (n,c) = (1024,t) \\ \lceil 2^{-82.22} \rceil_\upsilon & (n,c) = (512,t_{\mathrm{frac}}) \\ \lceil 2^{-79.17} \rceil_\upsilon & (n,c) = (1024,t_{\mathrm{frac}}) \end{cases}$, the stored words [L0: `fxp/fxp_consts.h:2104`] [L0: `fxp/fxp_consts.h:2108`] [L0: `fxp/fxp_consts.h:2112`] [L0: `fxp/fxp_consts.h:2116`];
  - $\tau_K := \begin{cases} 17.34 & (n,c) = (512,t) \\ 21.91 & (n,c) = (1024,t) \\ 17.34 & (n,c) = (512,t_{\mathrm{frac}}) \\ 21.91 & (n,c) = (1024,t_{\mathrm{frac}}) \end{cases}$ [L0: `fxp/fxp_consts.h:2105`] [L0: `fxp/fxp_consts.h:2109`] [L0: `fxp/fxp_consts.h:2113`] [L0: `fxp/fxp_consts.h:2117`];
  - $\tau_K^{\uparrow} := \lceil \tau_K \rceil_\upsilon$, the stored words [L0: `fxp/fxp_consts.h:2105`] [L0: `fxp/fxp_consts.h:2109`] [L0: `fxp/fxp_consts.h:2113`] [L0: `fxp/fxp_consts.h:2117`];
  - $(1/s)^{\mathcal{J}} := [\lfloor 1/s \rfloor_\upsilon, \lceil 1/s \rceil_\upsilon]$, the stored words (Definition A.25) [L0: `fxp/fxp_consts.h:2098-2101`];
  - $\widetilde{(1/q)}$, $\widetilde{(-1/q)}$, the stored words [L0: `fxp/fxp_consts.h:2090`] [L0: `fxp/fxp_consts.h:2091`].

Definition I.15 (The interval twiddles [to table])**.** The interval twiddles are the roots of the FFT as the code computes them in intervals. Define:

- The components
  - $\mathcal{J}$, that of Definition I.14;
  - $\forall x,y \in \mathcal{J} :\ (x,y)_r := x$, $(x,y)_i := y$, $\forall z \in \mathbb{C} :\ z_r := \operatorname{Re} z$, $z_i := \operatorname{Im} z$, $\forall m \ge 1\ \forall a \in (\mathcal{J}^2)^m \cup \mathbb{C}^m\ \forall k < m :\ a_{k,r} := (a_k)_r$, $a_{k,i} := (a_k)_i$;
- The indices
  - $\forall k < 1024 :\ \mathrm{rev}_{10}(k) := \sum_{b<10} (\lfloor k/2^b \rfloor \bmod 2)\, 2^{9-b}$ [L0: `fxp/fxi.c:229-235`];
  - $\forall j \in \{1,\ldots,1023\} :\ \mathrm{low}(j) := \max\{b < 10 : j \in 2^b\mathbb{Z}\}$ [L0: `fxp/fxi.c:252-255`];
- The twiddles
  - $\mathtt{bc}_1 := [0,0]$ [L0: `fxp/fxi.c:240-242`];

- $\mathtt{bs}_1 := [1,1]$ [L0: `fxp/fxi.c:240-242`];
- $\forall m \in \{1,\ldots,9\}$: $\mathtt{bc}_{m+1} := \mathtt{fxi_sqrt}(\mathtt{fxi_half}(\mathtt{fxi_add}([1,1],\mathtt{bc}_m)))$ (Definition I.13, items 10, 5 and 2) [L0: `fxp/fxi.c:244-245`];
- $\forall m \in \{1,\ldots,9\}$: $\mathtt{bs}_{m+1} := \mathtt{fxi_sqrt}(\mathtt{fxi_half}(\mathtt{fxi_sub}([1,1],\mathtt{bc}_m)))$ (Definition I.13, items 10, 5 and 3) [L0: `fxp/fxi.c:246-247`];
- $\Psi_0 := ([1,1],[0,0])$ [L0: `fxp/fxi.c:249-250`];
- $\forall j \in \{1,\ldots,1023\}$: $\Psi_{\mathrm{rev}_{10}(j)} := \mathtt{xcmul}(\Psi_{\mathrm{rev}_{10}(j-2^{\mathrm{low}(j)}),r}, \Psi_{\mathrm{rev}_{10}(j-2^{\mathrm{low}(j)}),i}, \mathtt{bc}_{10-\mathrm{low}(j)}, \mathtt{bs}_{10-\mathrm{low}(j)})$ (Definition I.13, item 11) [L0: `fxp/fxi.c:251-259`].

The code computes, along tailcheck (Algorithm 15):

1. $(\Psi_k)_{k<1024} \in (\mathcal{J}^2)^{1024}$; line 3 [L0: `fxp/fxi.c:237-260`].

Definition I.16 (The key's images and tree over the intervals [to table])**.** The key's images and tree over the intervals are the key's FFT, its Gram matrix entries and their tree as the code computes them in intervals. Let:

- (f,g,F,G) be a checked key (Definition 5.5) of degree n.

Define:

- The images
  - $\mathcal{J}$, N, those of Definition I.14;
  - Ψ_k, $a_{k,r}$, $a_{k,i}$, those of Definition I.15;
  - $\mathtt{fxw_of_int}$, that of Definition I.13;
  - $\forall p \in \{f,g,F,G\}$:

$$\mathrm{in}_0^{\mathcal{J}}(p) := \big((\mathtt{fxi_point}(\mathtt{fxw_of_int}(p_{[k]})), \mathtt{fxi_point}(\mathtt{fxw_of_int}(p_{[k+n/2]}))\big)\big)_{k<n/2}$$

    (Definition I.13, item 1) [L0: `fxp/kgen_fx.c:344-347`];
  - $\forall \ell \le \log_2 n - 2\ \forall a \in (\mathcal{J}^2)^{n/2}\ \forall i < 2^\ell\ \forall j < n/2^{\ell+2}$:

$$\begin{aligned} j_1 &:= i\,n/2^{\ell+1} + j, \quad j_2 := j_1 + n/2^{\ell+2}, \\ (z_r, z_i) &:= \mathtt{xcmul}(a_{j_2,r}, a_{j_2,i}, \Psi_{2^{\ell+1}+i,r}, \Psi_{2^{\ell+1}+i,i}), \\ \Lambda_\ell^{\mathcal{J}}(a)_{j_1} &:= (\mathtt{fxi_add}(a_{j_1,r}, z_r), \mathtt{fxi_add}(a_{j_1,i}, z_i)), \\ \Lambda_\ell^{\mathcal{J}}(a)_{j_2} &:= (\mathtt{fxi_sub}(a_{j_1,r}, z_r), \mathtt{fxi_sub}(a_{j_1,i}, z_i)) \end{aligned}$$

    (Definition I.13, items 2, 3 and 11; FFT (Algorithm 14), lines 6 to 20) [L0: `fxp/kgen_fx.c:348-367`];
  - $\forall p \in \{f,g,F,G\}$: $\hat{p}^{\mathcal{J}} := \Lambda^{\mathcal{J}}_{\log_2 n-2}(\cdots \Lambda_0^{\mathcal{J}}(\mathrm{in}_0^{\mathcal{J}}(p)) \cdots)$ (tailcheck (Algorithm 15), line 4) [L0: `fxp/kgen_fx.c:550-553`];
  - $\forall k < n/2$:

$$g^{\mathcal{J}}_{00,k} := \mathtt{fxi_add}(\mathtt{fxi_add}(\mathtt{fxi_sqr}(\hat{g}^{\mathcal{J}}_{k,r}), \mathtt{fxi_sqr}(\hat{g}^{\mathcal{J}}_{k,i})), \mathtt{fxi_add}(\mathtt{fxi_sqr}(\hat{f}^{\mathcal{J}}_{k,r}), \mathtt{fxi_sqr}(\hat{f}^{\mathcal{J}}_{k,i})))$$

    (Definition I.13, items 2 and 7) [L0: `fxp/kgen_fx.c:559-560`];
  - $\forall k < n/2$:

$$g^{\mathcal{J}}_{11,k} := \mathtt{fxi_add}(\mathtt{fxi_add}(\mathtt{fxi_sqr}(\hat{G}^{\mathcal{J}}_{k,r}), \mathtt{fxi_sqr}(\hat{G}^{\mathcal{J}}_{k,i})), \mathtt{fxi_add}(\mathtt{fxi_sqr}(\hat{F}^{\mathcal{J}}_{k,r}), \mathtt{fxi_sqr}(\hat{F}^{\mathcal{J}}_{k,i})))$$

    (Definition I.13, items 2 and 7) [L0: `fxp/kgen_fx.c:561-562`];
  - $\forall k < n/2$: $\mathtt{xg}_k := \mathtt{xcmul}(\hat{g}^{\mathcal{J}}_{k,r}, \hat{g}^{\mathcal{J}}_{k,i}, \hat{G}^{\mathcal{J}}_{k,r}, \mathtt{fxi_neg}(\hat{G}^{\mathcal{J}}_{k,i}))$ (Definition I.13, items 11 and 4) [L0: `fxp/kgen_fx.c:563`];

- $\forall k < n/2$: $\mathtt{xf}_k := \mathtt{xcmul}(\hat{f}^{\mathcal{J}}_{k,r}, \hat{f}^{\mathcal{J}}_{k,i}, \hat{F}^{\mathcal{J}}_{k,r}, \mathtt{fxi_neg}(\hat{F}^{\mathcal{J}}_{k,i}))$ (Definition I.13, items 11 and 4) [L0: fxp/kgen_fx.c:564];
- $\forall k < n/2$: $g^{\mathcal{J}}_{01,k} := (\mathtt{fxi_add}(\mathtt{xg}_{k,r}, \mathtt{xf}_{k,r}), \mathtt{fxi_add}(\mathtt{xg}_{k,i}, \mathtt{xf}_{k,i}))$ (Definition I.13, item 2) [L0: fxp/kgen_fx.c:565-566];

- The tree
  - $\forall a, b \in \mathbb{Z}_{\geq 0}\ \forall u = (u_1, \ldots, u_a)\ \forall v = (v_1, \ldots, v_b)$: $u \parallel v := (u_1, \ldots, u_a, v_1, \ldots, v_b)$;
  - $\forall \ell \in \{1, \ldots, \log_2 n\}\ \forall a, d \in \mathcal{J}^{2^{\ell-1}}\ \forall b \in (\mathcal{J}^2)^{2^{\ell-1}}\ \forall j < 2^{\ell-1}$:

$$\begin{aligned}\mathtt{xl}(a,b)_j &:= (\mathtt{fxi_mul}(b_{j,r}, \mathtt{fxi_inv}(a_j)),\ \mathtt{fxi_neg}(\mathtt{fxi_mul}(b_{j,i}, \mathtt{fxi_inv}(a_j)))),\\ \mathtt{xd}(a,b,d)_j &:= \mathtt{fxi_sub}(d_j,\ \mathtt{fxi_mul}(\mathtt{fxi_add}(\mathtt{fxi_sqr}(b_{j,r}), \mathtt{fxi_sqr}(b_{j,i})),\\ &\qquad \mathtt{fxi_inv}(a_j)))\end{aligned}$$

    (Definition I.13, items 9, 6, 4, 7, 2 and 3) [L0: fxp/kgen_fx.c:418-426];
  - $\forall \ell \in \{2, \ldots, \log_2 n\}\ \forall d \in \mathcal{J}^{2^{\ell-1}}\ \forall j < 2^{\ell-2}$:

$$\begin{aligned}\mathtt{xs}^0(d)_j &:= \mathtt{fxi_half}(\mathtt{fxi_add}(d_{2j}, d_{2j+1})),\\ \mathtt{xu}_j &:= \mathtt{fxi_half}(\mathtt{fxi_sub}(d_{2j}, d_{2j+1})),\\ \mathtt{xs}^1(d)_j &:= (\mathtt{fxi_mul}(\mathtt{xu}_j, \Psi_{j+2^{\ell-1},r}),\\ &\qquad \mathtt{fxi_neg}(\mathtt{fxi_mul}(\mathtt{xu}_j, \Psi_{j+2^{\ell-1},i})))\end{aligned}$$

    (Definition I.13, items 5, 2, 3, 6 and 4) [L0: fxp/kgen_fx.c:383-393];
  - $\forall \ell \in \{1, \ldots, \log_2 n\}\ \forall a, d \in \mathcal{J}^{2^{\ell-1}}\ \forall b \in (\mathcal{J}^2)^{2^{\ell-1}}$:

$$\begin{aligned}(L', D') &:= \mathtt{xtree}(\mathtt{xs}^0(\mathtt{xd}(a,b,d)), \mathtt{xs}^1(\mathtt{xd}(a,b,d)),\\ &\qquad \mathtt{xs}^0(\mathtt{xd}(a,b,d))),\\ (L'', D'') &:= \mathtt{xtree}(\mathtt{xs}^0(a), \mathtt{xs}^1(a), \mathtt{xs}^0(a)),\\ \mathtt{xtree}(a,b,d) &:= \begin{cases} ((\mathtt{xl}(a,b)),\ (\mathtt{xd}(a,b,d)_0, \mathtt{xd}(a,b,d)_0, a_0, a_0)) & \ell = 1\\ ((\mathtt{xl}(a,b)) \parallel L' \parallel L'',\ D' \parallel D'') & \ell \geq 2 \end{cases}\end{aligned}$$

    (Definition A.20) [L0: fxp/kgen_fx.c:412-440];
  - $((l^{\mathcal{J}}_{10,\nu})_\nu, (d^{\mathcal{J}}_i)_{i \leq N}) := \mathtt{xtree}(g^{\mathcal{J}}_{00}, g^{\mathcal{J}}_{01}, g^{\mathcal{J}}_{11})$ at $\ell := \log_2 n$ (item 1; tailcheck (Algorithm 15), line 6) [L0: fxp/kgen_fx.c:568].

The code computes, at the key, along tailcheck (Algorithm 15):

1. $\hat{p}^{\mathcal{J}}$, $p \in \{f, g, F, G\}$, $g^{\mathcal{J}}_{00}$, $g^{\mathcal{J}}_{01}$, $g^{\mathcal{J}}_{11}$; lines 4 and 5 [L0: fxp/kgen_fx.c:550-553] [L0: fxp/kgen_fx.c:559];
2. $(l^{\mathcal{J}}_{10,\nu})_\nu$, $(d^{\mathcal{J}}_i)_{i \leq N}$; line 6 [L0: fxp/kgen_fx.c:568].

Definition I.17 (The leaf words and the message bound [to table])**.** The leaf words are the signer's leaves read exactly, and the message bound is the upper bound of the message rounding sites. Let:

- (f, g, F, G) be a checked key (Definition 5.5) of degree n;
- $c \in \{t, t_{\mathrm{frac}}\}$ be a center (Definition A.25).

Define:

- The leaf words
  - $\mathcal{W}$, N, $\widetilde{(1/q)}$, $\widetilde{(-1/q)}$, those of Definition I.14;
  - $\mathtt{fxw_of_fxp}$, that of Definition I.13;
  - $\widetilde{g}_{00}$, $\widetilde{g}_{01}$, $\widetilde{g}_{11}$, $\widetilde{f}$, $\widetilde{F}$, those of Definition 5.5;
  - $((\widetilde{l}_{10,\nu})_\nu, (\mathtt{isigma}_i)_{i \leq N}) := \mathtt{ctree}(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$ (tailcheck (Algorithm 15), line 9) [L0: fxp/kgen_fx.c:460-498] [L0: fxp/kgen_fx.c:1715];
  - $\forall i \leq N$: $\Sigma_i := \mathtt{fxi_inv}(\mathtt{fxi_point}(\mathtt{fxw_of_fxp}(\mathtt{isigma}_i)))$ (Definition I.13, items 9 and 1) [L0: fxp/kgen_fx.c:1721-1722];

- The message bound
  - $\widetilde{\psi}_k$, $k < 1024$, those of Definition I.1, item 4;
  - $a_{k,r}$, $a_{k,i}$, those of Definition I.15;
  - $\|$, that of Definition I.16;
  - $\forall u, v, w:\ \pi_1(u, v, w) := u$;
  - $\forall a_r, a_i, b_r, b_i \in \mathcal{W},\ a_r, a_i, b_r, b_i \geq 0:\ \texttt{msb_cmul}(a_r, a_i, b_r, b_i) := (\texttt{fxw_mulu}(b_r, a_r) + \texttt{fxw_mulu}(b_i, a_i) + 2\,\texttt{FXW_U65},\ \texttt{fxw_mulu}(b_i, a_r) + \texttt{fxw_mulu}(b_r, a_i) + 2\,\texttt{FXW_U65})$ (Definition I.13, items 13 and 15) [L0: fxp/kgen_fx.c:635-639];
  - $\forall C \in \mathcal{F}_{\text{fx}}\ \forall a \in \mathcal{W}^n\ \forall k < n:\ \texttt{msb_const}(a, C)_k := \texttt{fxw_mulu}(|C|, a_k) + \texttt{FXW_U65}$ (Definition I.13, items 13 and 15) [L0: fxp/kgen_fx.c:801-807];
  - $\forall \ell \leq \log_2 n - 2\ \forall a \in \mathcal{W}^n\ \forall i < 2^\ell\ \forall j < n/2^{\ell+2}:$

$$
\begin{gathered}
j_1 := i\,n/2^{\ell+1} + j, \quad j_2 := j_1 + n/2^{\ell+2}, \\
(y_r, y_i) := \texttt{msb_cmul}(a_{j_2}, a_{j_2+n/2}, |\widetilde{\psi}_{2^{\ell+1}+i,r}|, |\widetilde{\psi}_{2^{\ell+1}+i,i}|), \\
\Lambda^{\uparrow}_\ell(a)_{j_1} := a_{j_1} + y_r, \quad \Lambda^{\uparrow}_\ell(a)_{j_2} := a_{j_1} + y_r, \\
\Lambda^{\uparrow}_\ell(a)_{j_1+n/2} := a_{j_1+n/2} + y_i, \quad \Lambda^{\uparrow}_\ell(a)_{j_2+n/2} := a_{j_1+n/2} + y_i
\end{gathered}
$$

    [L0: fxp/kgen_fx.c:760-788];
  - $\texttt{msb_fft} := \Lambda^{\uparrow}_{\log_2 n-2}(\cdots \Lambda^{\uparrow}_0(0) \cdots),\ 0 \in \mathcal{W}^n$ [L0: fxp/kgen_fx.c:760-788];
  - $\forall h \in \{2, 4, \ldots, n/2\}\ \forall a \in \mathcal{W}^{2h}\ \forall j < h/2:$

$$
\begin{gathered}
\texttt{tr}_j := a_{2j} + a_{2j+1}, \quad \texttt{ti}_j := a_{2j+h} + a_{2j+1+h}, \\
(\texttt{ur}_j, \texttt{ui}_j) := \texttt{msb_cmul}(\texttt{tr}_j, \texttt{ti}_j, |\widetilde{\psi}_{j+h,r}|, |\widetilde{\psi}_{j+h,i}|), \\
a^0_j := \texttt{fxw_halfu}(\texttt{tr}_j) + \texttt{FXW_U65}, \quad a^0_{j+h/2} := \texttt{fxw_halfu}(\texttt{ti}_j) + \texttt{FXW_U65}, \\
a^1_j := \texttt{fxw_halfu}(\texttt{ur}_j) + \texttt{FXW_U65}, \quad a^1_{j+h/2} := \texttt{fxw_halfu}(\texttt{ui}_j) + \texttt{FXW_U65}, \\
\texttt{msb_split}(a) := (a^0, a^1)
\end{gathered}
$$

    (Definition I.13, items 14 and 15) [L0: fxp/kgen_fx.c:653-666];
  - $\forall h \in \{2, 4, \ldots, n/2\}\ \forall a^0, a^1 \in \mathcal{W}^h\ \forall j < h/2:$

$$
\begin{gathered}
(\texttt{cr}_j, \texttt{ci}_j) := \texttt{msb_cmul}(a^1_j, a^1_{j+h/2}, |\widetilde{\psi}_{j+h,r}|, |\widetilde{\psi}_{j+h,i}|), \\
\texttt{msb_merge}(a^0, a^1)_{2j} := a^0_j + \texttt{cr}_j, \quad \texttt{msb_merge}(a^0, a^1)_{2j+1} := a^0_j + \texttt{cr}_j, \\
\texttt{msb_merge}(a^0, a^1)_{2j+h} := a^0_{j+h/2} + \texttt{ci}_j, \quad \texttt{msb_merge}(a^0, a^1)_{2j+1+h} := a^0_{j+h/2} + \texttt{ci}_j
\end{gathered}
$$

    [L0: fxp/kgen_fx.c:680-693];
  - $\forall \ell \in \{1, \ldots, \log_2 n\}\ \forall a^0, a^1 \in \mathcal{W}^{2^\ell}\ \forall \lambda = (\lambda_1, \ldots, \lambda_{2^\ell-1}),\ \lambda_1 \in \mathbb{C}^{2^{\ell-1}}:$

$$
\begin{gathered}
(\texttt{pr}, \texttt{pi}) := \texttt{msb_cmul}(a^1_0, a^1_1, |\lambda_{1,0,r}|, |\lambda_{1,0,i}|), \\
(M', y^0, y^1) := \texttt{msb_rec}(\texttt{msb_split}(a^1), (\lambda_2, \ldots, \lambda_{2^{\ell-1}})), \\
z := \texttt{msb_merge}(y^0, y^1), \\
\forall k < 2^{\ell-1}: \quad (\texttt{pr}_k, \texttt{pi}_k) := \texttt{msb_cmul}(a^1_k + z_k, a^1_{k+2^{\ell-1}} + z_{k+2^{\ell-1}}, \\
|\lambda_{1,k,r}|, |\lambda_{1,k,i}|), \\
\forall k < 2^{\ell-1}: \quad b^0_k := a^0_k + \texttt{pr}_k, \quad b^0_{k+2^{\ell-1}} := a^0_{k+2^{\ell-1}} + \texttt{pi}_k, \\
(M'', w^0, w^1) := \texttt{msb_rec}(\texttt{msb_split}(b^0), (\lambda_{2^{\ell-1}+1}, \ldots, \lambda_{2^\ell-1})), \\
\texttt{msb_rec}(a^0, a^1, \lambda) := \begin{cases} ((a^1_0, a^1_1, a^0_0 + \texttt{pr}, a^0_1 + \texttt{pi}),\ 0,\ 0) & \ell = 1 \\ (M' \parallel M'',\ \texttt{msb_merge}(w^0, w^1),\ z) & \ell \geq 2 \end{cases}
\end{gathered}
$$

    (tailbounds (Algorithm 16), line 11) [L0: fxp/kgen_fx.c:710-749];

– $\forall P \in \{\widetilde{\hat{f}}, \widetilde{\hat{F}}\}\ \forall k < n/2$:

$$(\texttt{msb_key}(P)_k, \texttt{msb_key}(P)_{k+n/2}) := \texttt{msb_cmul}(\texttt{msb_fft}_k, \texttt{msb_fft}_{k+n/2}, |P_{k,r}|, |P_{k,i}|)$$

[L0: fxp/kgen_fx.c:834-840];

– $\mathtt{a}_0 := \begin{cases} \texttt{msb_const}(\texttt{msb_key}(\widetilde{\hat{F}}), \widetilde{(1/q)}) & c = t \\ \texttt{msb_const}(\texttt{msb_fft}, \widetilde{(1/q)}) & c = t_{\text{frac}} \end{cases}$ (tailbounds (Algorithm 16), line 4) [L0: fxp/kgen_fx.c:829-842];

– $\mathtt{a}_1 := \begin{cases} \texttt{msb_const}(\texttt{msb_key}(\widetilde{\hat{f}}), \widetilde{(-1/q)}) & c = t \\ \texttt{msb_const}(\texttt{msb_fft}, \widetilde{(1/q)}) & c = t_{\text{frac}} \end{cases}$ (tailbounds (Algorithm 16), line 4) [L0: fxp/kgen_fx.c:829-841];

– $(m_i^{\uparrow})_{i \le N} := \pi_1(\texttt{msb_rec}(\mathtt{a}_0, \mathtt{a}_1, (\widetilde{l}_{10,\nu})_\nu))$ (tailbounds (Algorithm 16), line 11) [L0: fxp/kgen_fx.c:844].

The code computes, at the key and c, along tailcheck (Algorithm 15):

1. $(\mathtt{isigma}_i)_{i \le N}$, $(\Sigma_i)_{i \le N}$; lines 9 and 10 [L0: fxp/kgen_fx.c:1715] [L0: fxp/kgen_fx.c:1722];
2. $(m_i^{\uparrow})_{i \le N}$; lines 4 to 11 of tailbounds (Algorithm 16) [L0: fxp/kgen_fx.c:819].

Definition I.18 (The remainder's matrices [to table])**.** The remainder's matrices are the columns of the remainder and of $K^{\mathcal{J}}$ in compact intervals, with their row sums. Let:

- (f, g, F, G) be a checked key (Definition 5.5) of degree n;
- $c \in \{t, t_{\text{frac}}\}$ be a center (Definition A.25).

Define:

- $\lceil \cdot \rceil_\upsilon$, N, N_{m}, h_c, those of Definition I.14;
- $\mathcal{J}_{\text{c}}$, that of Definition I.13;
- $\forall i \le N$: Σ_i, $m_i^{\uparrow}$, those of Definition I.17;
- $K^{\mathcal{J}} \in \mathcal{J}_{\text{c}}^{N \times N}$:

$$\forall j \in \{0, 8, \ldots, N-8\}\ \forall i \le N\ \forall k < 8 : \quad K^{\mathcal{J}}_{i,j+k} := \texttt{exd_block}(j)_{ik}$$

(tailbounds (Algorithm 16), line 22) [L0: fxp/kgen_fx.c:1768-1770];

- $R^{\text{m}} \in \mathcal{J}_{\text{c}}^{N \times N_{\text{m}}}$, $R^{\text{z}} \in \mathcal{J}_{\text{c}}^{N \times N}$:

$$\forall j \in \{0, 8, \ldots, N_{\text{m}}-8\}\ \forall i \le N\ \forall k < 8 : \quad R^{\text{m}}_{i,j+k} := \texttt{exc_block}(c, j)_{ik},$$
$$\forall j \in \{0, 8, \ldots, N-8\}\ \forall i \le N\ \forall k < 8 : \quad R^{\text{z}}_{i,j+k} := \texttt{exc_block}(c, N_{\text{m}} + j)_{ik}$$

(tailbounds (Algorithm 16), lines 13 and 17) [L0: fxp/kgen_fx.c:1759-1761];

- $\forall i \le N$: $\mathtt{a_r}_i := \sum_{k \le N} \lceil \texttt{fxc_mag}(R^{\text{z}}_{ik}) \max \Sigma_k \rceil_\upsilon$ (Definition I.13, items 21 and 13; Definition I.17, item 1) [L0: fxp/kgen_fx.c:995-999] [L0: fxp/kgen_fx.c:1764];
- $\forall i \le N$: $\mathtt{b_r}_i := \left\lceil h_c \sum_{k \le N_{\text{m}}} \texttt{fxc_mag}(R^{\text{m}}_{ik}) \right\rceil_\upsilon + m_i^{\uparrow} + 2^{-120}$ (Definition I.13, items 21 and 13; Definition I.17, item 2) [L0: fxp/kgen_fx.c:989-993] [L0: fxp/kgen_fx.c:1765].

The code computes, at the key and c, along tailcheck (Algorithm 15):

1. R^{m}, R^{z}, $K^{\mathcal{J}}$, $(\mathtt{a_r}_i)_{i \le N}$, $(\mathtt{b_r}_i)_{i \le N}$; lines 13 to 22 of tailbounds (Algorithm 16) [L0: fxp/kgen_fx.c:1759-1770].

Definition I.19 (The tail checks [to table])**.** The tail checks compute, from the key, the three upper bounds at the center c in the arithmetic of Definition I.13, along tailcheck (Algorithm 15). Let:

- (f, g, F, G) be a checked key (Definition 5.5) of degree n;
- $c \in \{t, t_{\text{frac}}\}$ be a center (Definition A.25).

Define:

- The bounds
  - $\lceil\cdot\rceil_v$, N, M_n, D_n, B_n, $\tau_K^{\uparrow}$, $(1/s)^{\mathcal{J}}$, those of Definition I.14;
  - e, `fxw_of_fxp`, those of Definition I.13;
  - $\forall i \le N:\ d_i^{\mathcal{J}}$, those of Definition I.16;
  - $\forall i \le N:\ \texttt{isigma}_i$, Σ_i, those of Definition I.17;
  - $K^{\mathcal{J}}$, $\forall i \le N:\ \texttt{a_r}_i$, $\texttt{b_r}_i$, those of Definition I.18;
  - $\forall i \le N$:
$$x_i := \texttt{fxi_div}(\texttt{fxi_mul}(\texttt{fxi_sqrt}(d_i^{\mathcal{J}}), (1/s)^{\mathcal{J}}), \texttt{fxi_point}(\texttt{fxw_of_fxp}(\texttt{isigma}_i)))$$
    (Definition I.13, items 8, 6, 10 and 1; Definition I.16, item 2; Definition I.17, item 1) [L0: `fxp/kgen_fx.c:1735-1738`];
  - $\delta^{\uparrow} := \max_{i\le N} \texttt{fxi_mag}(\texttt{fxi_sub}(x_i, [1,1]))$ (Definition I.13, items 12 and 3) [L0: `fxp/kgen_fx.c:1739`];
  - $\mu^{\uparrow} := \sum_{i\le N}\left\lceil \lceil \texttt{isigma}_i^2\rceil_v \sum_{j\le N}\left\lceil \lceil \texttt{fxc_mag}(K_{ij}^{\mathcal{J}})^2\rceil_v \lceil (\max \Sigma_j)^2\rceil_v\right\rceil_v\right\rceil_v$ (Definition I.13, items 21 and 13; Definition I.17, item 1; Definition I.18, item 1) [L0: `fxp/kgen_fx.c:1773`];
  - $\forall i \le N:\ \texttt{b_rem}_i := \left\lceil \tau_K^{\uparrow}\left(\texttt{a_r}_i + \sum_{j\le N}\lceil \texttt{fxc_mag}(K_{ij}^{\mathcal{J}})\,\texttt{a_r}_j\rceil_v\right)\right\rceil_v + \texttt{b_r}_i + \sum_{j\le N}\lceil \texttt{fxc_mag}(K_{ij}^{\mathcal{J}})\,\texttt{b_r}_j\rceil_v$ (Definition I.13, items 21 and 13) [L0: `fxp/kgen_fx.c:1774-1775`];
  - $B^{\uparrow} := \sum_{i\le N}\left\lceil \lceil \texttt{isigma}_i^2\rceil_v \lceil \texttt{b_rem}_i^2\rceil_v\right\rceil_v$ (Definition I.13, item 13) [L0: `fxp/kgen_fx.c:1776-1777`];
- The verdicts
  - $ok_\delta := \begin{cases} 1 & e = 0 \wedge \delta^{\uparrow} \le D_n \\ 0 & e \ne 0 \vee \delta^{\uparrow} > D_n \end{cases}$ [L0: `fxp/kgen_fx.c:1745-1746`] [L0: `fxp/kgen_fx.c:1783`];
  - $ok_\mu := \begin{cases} 1 & \delta^{\uparrow} \le D_n \wedge e = 0 \wedge \mu^{\uparrow} \le M_n \\ 0 & \delta^{\uparrow} > D_n \vee e \ne 0 \vee \mu^{\uparrow} > M_n \end{cases}$ [L0: `fxp/kgen_fx.c:1783`];
  - $ok_B := \begin{cases} 1 & \delta^{\uparrow} \le D_n \wedge e = 0 \wedge B^{\uparrow} \le B_n \\ 0 & \delta^{\uparrow} > D_n \vee e \ne 0 \vee B^{\uparrow} > B_n \end{cases}$ [L0: `fxp/kgen_fx.c:1783`].

The code computes, at the key and c, along tailcheck (Algorithm 15):

1. $(x_i)_{i\le N}$, $\delta^{\uparrow}$; lines 13 to 15 [L0: `fxp/kgen_fx.c:1735-1739`];
2. $\mu^{\uparrow}$, $(\texttt{b_rem}_i)_{i\le N}$, $B^{\uparrow}$; lines 29 to 31 of tailbounds (Algorithm 16), called at line 19 of tailcheck [L0: `fxp/kgen_fx.c:1773-1777`];
3. $ok_\delta \in \{0,1\}$; lines 16 and 20 [L0: `fxp/kgen_fx.c:1745-1746`] [L0: `fxp/kgen_fx.c:1783`];
4. $ok_\mu \in \{0,1\}$; lines 16 and 21 [L0: `fxp/kgen_fx.c:1783`];
5. $ok_B \in \{0,1\}$; lines 16 and 22 [L0: `fxp/kgen_fx.c:1783`].

```
noncomputable def tailVerdict (p : Prop) : Nat := if p then 1 else 0
```

Figure 71: The Lean declarations carrying Definition I.19: `tailVerdict` (`LeafTail.lean`); Lean's symbols in ASCII.

I.1.4 ffSampling$^{\mathcal{F}}$ in $\mathcal{F}_{\text{fx}}$

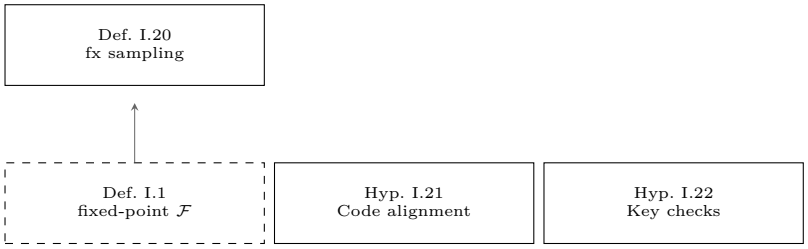


Figure 72: Dependencies, Appendix I.1.4.

Definition I.20 (The fixed-point signer's sampling [to table])**.** The fixed-point signer stores its constants rounded to $2^{-64}\mathbb{Z}$, chooses its center by a mode, and rejects the candidates at which the shift of BerExp saturates. Define:

- $\zeta_{\text{op}} := 2^{-65}$ and roundEven, those of Definition I.1;
- $\sigma_0 := 1.8205$, that of SamplerZ (Algorithm 8).

The code:

- Stores $\widetilde{c} := 2^{-64}\text{roundEven}(2^{64}c)$ [L0: `fxp/gen_consts.py:145`] [gate: `verify/gates/fx/consts.py`], for
$$c \in \{\texttt{INV_SIGMA}, \texttt{SIGMA_MIN}, \ln 2, 1/\ln 2, 1/(2\sigma_0^2), 1/q\};$$
- Centers at t at `fractional_mode` $= 0$ (line 17 of ffSampling$^{\mathcal{F}}$ (Algorithm 10); Lemma I.75) and at t_{frac} at `fractional_mode` $= 1$ (line 7; Lemma I.81);
- Computes d_{11} at the root node by line 6 of ffsamp (Algorithm 6) at both centers (Lemma I.27) [L0: `fxp/sign_fxsampler.c:338`].

We define the sampling by

1. $\forall x \geq 0,\ si(x) \geq 64 :\ z_{\text{acc}} := 0$ (BerExp (Algorithm 9), line 2) [L0: `fxp/sign_fxsampler.c:169`], a deviation from line 13 of the reference.

Hypothesis I.21 (Code alignment of the base sampler and the composition [to table])**.** A code-alignment hypothesis on the C functions of `fxp/` that the CryptoLine lemmas of Lemmas I.10 and I.11 do not cover: the base sampler and the composition of the signature outside the recursion's levels they compose. The gate measures the C base sampler against its Haskell core, word for word, on sampled inputs. The core is read against the algorithms. We assume:

1. The C base sampler, `fxp_sampler_next` and the BerExp it calls, returns the words of SamplerZ (Algorithm 8) and BerExp (Algorithm 9) in $\mathcal{F}_{\text{fx}}$ at every input **[hypothesis, sampled gate: `fxp/gate_c_functions_vs_core`]**;

2. `fxp_sign_core` composes the kernels' calls and the signature as ffSampling$^{\mathcal{F}}$ (Algorithm 10) states, at every `logn`, outside the recursion `fxp_ffsamp_fft_inner`. The top wrapper `fxp_ffsamp_fft` calls the recursion once, at the signer's `logn` and `root` $= 1$, on its area.

[L3: code alignment] Not discharged.

Hypothesis I.22 (Code alignment of the C key checks [to table])**.** A code-alignment hypothesis on the C key checks of `fxp/`, the four coefficient checks a checked key passes (Definition 5.5). Nothing in it is sampled. We assume:

1. The C key checks, `fxp_keygen_checked` and `fxp_key_bounds_of`, compute lines 5 to 11 of keychecks (Algorithm 12) in $\mathcal{F}_{\text{fx}}$.

[L3: code alignment] Not discharged.

Statistics I.23 (Measurements of the fixed-point signer [to table])**.** The statement reports sampled measurements of the fixed-point signer. No statement rests on them. Measured:

1. On the sample of the reference's seeded key generation of Table 26, the share the C key checks of keychecks (Algorithm 12) accept at the thresholds of Proposition 5.8 `verify/reports/key/keychecks.py`;
2. On the sample of item 1, the share they accept with the key checks of [L2: BFLP26, Alg. 2] (Table 26) `verify/reports/key/keychecks.py`;
3. On the sample of item 1, the share the tail checks of Definition 5.6 accept at t, at t_{frac} and at both centers, and at both centers on the keys the four key checks accept (Table 26) `verify/reports/fx/tail_accept.py`;
4. On the sample of item 1, the time per key of the tail checks at both centers (Table 27) `verify/reports/fx/tail_accept.py`;
5. 16 keys per degree and center of the checked key generation, keygen (Algorithm 11) at the thresholds of Proposition 5.8 with the tail checks of Definition 5.6 at the center: the attempts it takes and the attempts each check rejects (Table 28) `fxp/gate_signature_scheme_vs_reference`;
6. $\max \widetilde{sq}_{fg}^{1/2}$, $\max \widetilde{sq}_{\mathrm{hyb}}^{1/2}$, $\max \widetilde{sq}_{FG}^{1/2}$ and $\max \widetilde{sq}_{\mathrm{root}}^{1/2}$ over the keys of item 5, the values the four checks compare (Definition 5.5; Table 28) `fxp/gate_signature_scheme_vs_reference`;
7. At each center, every signature of the sample of Table 29 verifies under the reference's `fndsa_verify` **[statistics, sampled gate: `fxp/gate_signature_scheme_vs_reference`]**;
8. At each center, a tampered copy of each signature of item 7 is rejected (Table 29) **[statistics, sampled gate: `fxp/gate_signature_scheme_vs_reference`]**;
9. At each center, the mean of $\|s_1\|^2 + \|s_2\|^2$ over the signatures of item 7 is within 2% of $2n\sigma^2$ (Table 29) **[statistics, sampled gate: `fxp/gate_signature_scheme_vs_reference`]**;
10. At the center t, the checked keys of Table 30 that meet the thresholds M_n, D_n and B_n of Definition I.14 at t, their μ_{key} computed from the exact K of Definition 4.12 and their remainder bound exact in the constants **[statistics, sampled gate: `verify/gates/fx/leafsum_accept.py`]**;
11. At the center t_{frac}, the checked keys that meet the thresholds M_n, D_n and B_n of Definition I.14 at t_{frac}, their μ_{key} computed from the exact K of Definition 4.12 and their remainder bound exact in the constants (Table 30) **[statistics, sampled gate: `verify/gates/fx/leafsum_accept.py`]**;
12. $\mu^{\uparrow}$, $\delta^{\uparrow}$ and $B^{\uparrow}$ (Definition I.19), at each center, on the checked keys of Table 30, lie at or above the key's μ_{key}, $\max_i|\delta_i|$ and remainder bound that `verify/reports/fx/leafsum_key.py` computes, to its binary64 rounding (Table 30) **[statistics, sampled gate: `verify/gates/fx/tail_bounds.py`]**;
13. W^{*}, at each center, over the sample of 16 keys and 16 messages per degree, is below the W^{tail} at $Q_s = 2^{64}$ of Corollary I.80 at t and of Corollary I.89 at t_{frac} (Table 31) **[statistics, sampled gate: `verify/gates/tree/leafmax.py`]**;
14. $\bar{\delta}^{*}$, the largest $|\delta_i|$ over the sample of item 13, at each center, is at most the D_n of Corollaries I.80 and I.89 (Table 31) **[statistics, sampled gate: `verify/gates/tree/leafdelta.py`]**.

Keys accepted (%)	$n = 512$	$n = 1024$
keychecks, the thresholds of Proposition 5.8	1838/2000 (91.9%)	1843/2000 (92.1%)
keychecks, the thresholds of [L2: BFLP26, Alg. 2]	1332/2000 (66.6%)	148/2000 (7.4%)
Tail checks at t	2000/2000 (100.0%)	2000/2000 (100.0%)
Tail checks at t_{frac}	1999/2000 (99.9%)	2000/2000 (100.0%)
Tail checks at both centers	1999/2000 (99.9%)	2000/2000 (100.0%)
Tail checks at both centers, on the keys keychecks accepts	1837/1838 (99.9%)	1843/1843 (100.0%)

Table 26: Fixed-point signer: the key checks' acceptance on 2000 keys per degree of the reference's seeded key generation, the seeds `keychecks-9-0` to `keychecks-9-1999` and `keychecks-10-0` to `keychecks-10-1999`; the rates rounded down to 0.1%. Gate (sampled): `verify/reports/key/keychecks.py` for the four key checks' rows, `verify/reports/fx/tail_accept.py -keys 2000` for the tail checks' rows.

Seconds per key	$n = 512$	$n = 1024$
Tail checks at both centers	7.3	32.5

Table 27: Fixed-point signer: the tail checks' time per key at both centers, the mean over the sample of Table 26, 8 keys at once. Gate (sampled): `verify/reports/fx/tail_accept.py -keys 2000`.

Checked key generation	$n = 512$	$n = 1024$
Keys	16	16
Attempts	16	18
Rejected by the check on $\widetilde{sq}_{fg}$	0	2
Rejected by the check on $\widetilde{sq}_{\text{hyb}}$	0	0
Rejected by the check on $\widetilde{sq}_{FG}$	0	0
Rejected by the check on $\widetilde{sq}_{\text{root}}$	0	0
Rejected by the tail checks at t	0	0
Rejected by the tail checks at t_{frac}	0	0
$\max \widetilde{sq}_{fg}^{1/2}$	253.54	263.09
$\max \widetilde{sq}_{\text{hyb}}^{1/2}$	4.117	5.194
$\max \widetilde{sq}_{FG}^{1/2}$	3304.70	4714.13
$\max \widetilde{sq}_{\text{root}}^{1/2}$	17.797	31.075

Table 28: Fixed-point signer, both centers: the checked key generation at the degree's thresholds (Proposition 5.8) with the tail checks at its center (Definition 5.6), on 16 keys per degree and center: the attempts, the attempts each check rejects and the maxima over the keys of the values the four checks compare (Definition 5.5). Gate (sampled): `fxp/gate_signature_scheme_vs_reference`.

Quantity	$n = 512$, t	$n = 512$, t_{frac}	$n = 1024$, t	$n = 1024$, t_{frac}
Signatures	256	256	256	256
Verified by `fndsa_verify`	256	256	256	256
Tampered copies rejected	256	256	256	256
Mean of $\|s_1\|^2 + \|s_2\|^2$ over $2n\sigma^2$	0.9992	0.9992	1.0032	1.0032

Table 29: Fixed-point signer, both centers: the signatures of 16 checked keys times 16 messages per degree against the reference. Gate (sampled): `fxp/gate_signature_scheme_vs_reference`.

Checked keys	$n = 512$	$n = 1024$
M_n, D_n, B_n met at t	16/16	16/16
M_n, D_n, B_n met at t_{frac}	16/16	16/16
$\mu^{\uparrow}$, $\delta^{\uparrow}$, $B^{\uparrow}$ at or above the exact bounds at t	16/16	16/16
$\mu^{\uparrow}$, $\delta^{\uparrow}$, $B^{\uparrow}$ at or above the exact bounds at t_{frac}	16/16	16/16

Table 30: Fixed-point signer, both centers: the tail checks' thresholds and upper bounds on the 16 checked keys per degree (Definitions I.14 and I.19). Gate (sampled): `verify/gates/fx/leafsum_accept.py -center t` for the thresholds at t, `verify/gates/fx/leafsum_accept.py` at t_{frac}, `verify/gates/fx/tail_bounds.py` for the upper bounds.

Center	n	**Signatures**	W^*	$W^{\text{tail}}(2^{64})$	$\bar{\delta}^*$	D_n
t	512	256	-83.07	-73.16	-58.95	-57.95
t	1024	256	-82.16	-71.19	-58.38	-57.38
t_{frac}	512	256	-92.51	-82.22	-58.95	-57.95
t_{frac}	1024	256	-90.65	-79.17	-58.38	-57.38

Table 31: Fixed-point signer, both centers: the sample maxima of the leaf sum W and of $|\delta_i|$ over 16 keys and 16 messages per degree and center, W^* and $\bar{\delta}^*$, against the tail W^{tail} of Lemma 4.14 at $Q_s = 2^{64}$ and the threshold D_n of each center (Corollaries I.80 and I.89), $\log_2$. Gate (sampled): `verify/gates/tree/leafmax.py`, `verify/gates/tree/leafdelta.py`.

I.2 The checked key

The thresholds are chosen here. [L2: BFLP26, Alg. 2] states one set, $(255, 4, 3500, 24)$ for Falcon-512. The sets of Proposition 5.8 follow one rule at both degrees: γ_{FG} and γ_{root} above every sampled key, as checks 13 and 15 reject no key of the 1000 of [L2: BFLP26, Table 1]; γ_{fg} and γ_{hyb} at the quantile $\sqrt{0.9}$ of the sampled $\max_\psi |\widetilde{\hat{f}}|, |\widetilde{\hat{g}}|$ and of the sampled $\max_\psi \max(\widetilde{g}_{00}/q, q/\widetilde{g}_{00})^{1/2}$, rounded up to a multiple of 5 and of $1/4$, so that at least 90% of the sample passes all four. The tail checks of Definition 5.6 add the thresholds M_n, D_n and B_n of Definition I.14, by one rule at both degrees and both centers: the $\log_2$ of the maximum over the 16 checked keys of `verify/reports/fx/leafsum_key.py`, rounded up to 0.01 and raised by the margin, 1 for M_n, 1 for D_n and 0.1 for B_n, stored as words. The acceptance of each set on a sample of keys of the reference's key generation is Statistics I.23, items 2, 1 and 3, and the checked key generation's attempts and maxima are its items 5 and 6.

I.3 The tree at $u = 0$

Structure. Appendix I.3.1 states the diagonals; Appendix I.3.2 no overflow in the key check; Appendix I.3.3 in the tree; Appendix I.3.4 in the center's first computation; Appendix I.3.5 in the recursion; Appendix I.3.6 in the base sampler; Appendix I.3.7 in the inverse FFT; Appendix I.3.8 the sample's integers; Appendix I.3.9 the entry shifts.

I.3.1 The diagonals in $\mathcal{F}_{\text{fx}}$

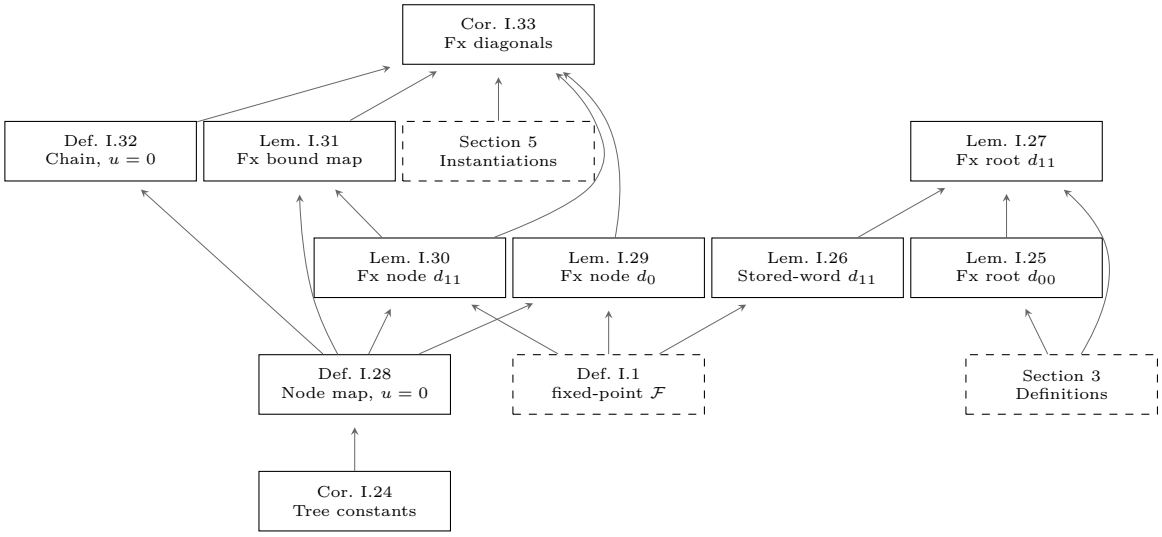


Figure 73: Dependencies, Appendix I.3.1.

Corollary I.24 (The fixed-point tree's constants [to table])**.** *At $u = 0$, the constants of the LDL† step's Schur product and of the self-adjoint split take the values below. Define:*

- *g_{01}, that of Lemma G.24;*
- *$k_{zo} := \sqrt{2}\,|g_{01}|^2(1+u)^3 + \sqrt{2}\,|g_{01}|(1+u)^2 + 2(1+u) + 1$ (Lemma G.24);*
- *$c_{\text{sa}} := (1+u)^2(1+u+\sqrt{2}\,\zeta) - 1$ and $k_{\text{sa}} := (1+u)(1+u+\sqrt{2}\,\zeta)/2 + \sqrt{2}$ (Lemma G.26).*

Then

1. *$k_{zo} = \sqrt{2}|g_{01}|^2 + \sqrt{2}|g_{01}| + 3$;*
2. *$c_{\text{sa}} = \sqrt{2}\,\zeta$;*
3. *$k_{\text{sa}} = \frac{1+\sqrt{2}\,\zeta}{2} + \sqrt{2}$.*

Proof. (L1) $k_{zo} = \sqrt{2}|g_{01}|^2 + \sqrt{2}|g_{01}| + 3$
$[k_{zo} = \sqrt{2}\,|g_{01}|^2(1+u)^3 + \sqrt{2}\,|g_{01}|(1+u)^2 + 2(1+u) + 1$ (Lemma G.24); Definition I.1: $u = 0]$

(L2) $\Rightarrow$ item 1
[(L1)]

(L3) $c_{\text{sa}} = \sqrt{2}\,\zeta$
$[c_{\text{sa}} = (1+u)^2(1+u+\sqrt{2}\,\zeta) - 1$ (Lemma G.26); Definition I.1: $u = 0]$

(L4) $\Rightarrow$ item 2
[(L3)]

(L5) $k_{\text{sa}} = \frac{1+\sqrt{2}\,\zeta}{2} + \sqrt{2}$
$[k_{\text{sa}} = (1+u)(1+u+\sqrt{2}\,\zeta)/2 + \sqrt{2}$ (Lemma G.26); Definition I.1: $u = 0]$

(L6) $\Rightarrow$ item 3
[(L5)]

□ (items 1 to 3)

Lemma I.25 (The fixed-point root's first diagonal [to table])**.** *The root node's computed first diagonal lies within a relative bound of its value over $\mathbb{R}$. Define:*

- *h and $n := 2^h$, those of FFT (Algorithm 14), Precondition;*
- *$\Psi_n := \{\psi_k : k < n/2\}$, that of Fact A.43 at $m := n$.*

Let:

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $\psi \in \Psi_n$.

Define:

- g_{00}*, the first diagonal* Gram *(Algorithm 13) outputs at line 4 of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10);*
- k_H*,* γ'_{fg} *and* δ_{fg}*, those of Definition A.36;*
- $E_{00} := k_H\zeta + 4\gamma'_{fg}\delta_{fg} + 2\delta_{fg}^2$ *(Definition A.36);*
- $\check{\gamma}_{\mathrm{hyb}}$*, that of Definition A.35;*
- $m_0 := q/\check{\gamma}_{\mathrm{hyb}}^2 - E_{00}$ *(Definition A.37);*
- $\widetilde{g}_{00}$*, the value* keychecks *computes in* $\mathcal{F}_{\mathrm{fx}}$ *(lines 1 to 11);*
- $e_{00} := E_{00}/m_0 \in [0, \infty)$*;*
- $\widetilde{d}_{00} := \widetilde{g}_{00} \in \mathcal{F}_{\mathrm{fx}}$.

Measured `verify/reports/fx/terms.py`*:*

- $m_0 > 0$.

Then

$$\widetilde{d}_{00}(\psi)\ \mathcal{I}\left(e_{00}^{\pm}, 0\right)\ g_{00}(\psi).$$

Proof. (L1) $|\widetilde{g}_{00}(\psi) - g_{00}(\psi)| \le E_{00}$
[Lemma H.19, item 1, at ψ (the statement)]

(L2) $m_0 \le g_{00}(\psi)$
[Lemma H.19, item 4, at ψ (the statement)]

(L3) $m_0 > 0$
[the measured row]

(L4) $E_{00} = e_{00}m_0$
[e_{00} (the statement); (L3)]

(L5) $e_{00}m_0 \le e_{00}g_{00}(\psi)$
[(L2), (L3); e_{00} (the statement); $E_{00}/m_0 \in [0, \infty)$ (the statement); Fact A.41, item 8]

(L6) $\Rightarrow$ $|\widetilde{g}_{00}(\psi) - g_{00}(\psi)| \le e_{00}g_{00}(\psi)$
[(L1), (L4), (L5)]

(L7) $g_{00}(\psi) > 0$
[(L2), (L3)]

(L8) $\Rightarrow$ $\left|\frac{\widetilde{g}_{00}(\psi)}{g_{00}(\psi)} - 1\right| \le e_{00}$
[(L6), (L7); $|xy| = |x||y|$ (Fact A.41, item 1)]

(L9) $\widetilde{d}_{00} = \widetilde{g}_{00}$
[$\widetilde{d}_{00}$ (the statement)]

(L10) $\Rightarrow$ $\widetilde{d}_{00}(\psi)\ \mathcal{I}\left(e_{00}^{\pm}, 0\right)\ g_{00}(\psi)$
[(L7), (L8), (L9); Definition A.10 at $u_\circ := \widetilde{g}_{00}/g_{00} - 1$, $\zeta_\circ := 0$]

(L11) $\Rightarrow$ the statement
[(L10)]

□

Lemma I.26 (The root's second diagonal on the stored word [to table])**.** *In* ffSampling$^{\mathcal{F}}(B, s, t)$ *and in* ffSampling$^{\mathcal{F}}(B, s, t_{\mathrm{frac}})$*, the root's second diagonal computed on the stored* $\widetilde{g}_{00}$ *lies within* $Z_I - 1$ *of* $q^2/\widetilde{g}_{00}$*. Let:*

- $\widetilde{g}_{00} \in \mathcal{F}_{\mathrm{fx}}$*;*
- $G \in \mathbb{R}$.

Define:

- $\widetilde{d}_{11} := \mathrm{fl}(q^2/\widetilde{g}_{00})$*, the value line 6 of* ffsamp *(Algorithm 6) computes in* $\mathcal{F}_{\mathrm{fx}}$ *(Fact A.33, item 4; [L2: BFLP26, Sec. 7.3, item 3(a)]);*
- $Z_I := 1 + \zeta G/q^2$.

Assume:

(A1) $\widetilde{g}_{00} \in (0, G]$.
Then

$$\left|\frac{\widetilde{d}_{11}\,\widetilde{g}_{00}}{q^2} - 1\right| \le Z_I - 1.$$

Proof. (L1) $\exists \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \le \zeta :\ \widetilde{d}_{11} = q^2/\widetilde{g}_{00} + \zeta_\circ$
[Definition I.1, item 1, for /; $\zeta := 2\zeta_{\mathrm{op}}$ (Definition I.1); $\widetilde{d}_{11} = \mathrm{fl}(q^2/\widetilde{g}_{00})$ (the statement); $\widetilde{g}_{00} > 0$ (assumption A1)]
(L2) $\Rightarrow$ $\frac{\widetilde{d}_{11}\widetilde{g}_{00}}{q^2} - 1 = \zeta_\circ \widetilde{g}_{00}/q^2$
[(L1); expand]
(L3) $\Rightarrow$ $\left|\frac{\widetilde{d}_{11}\widetilde{g}_{00}}{q^2} - 1\right| \le \zeta G/q^2$
[(L1), (L2); $\widetilde{g}_{00} \in (0, G]$ (assumption A1); $|xy| = |x||y|$ (Fact A.41, item 1); Fact A.41, item 8]
(L4) $\Rightarrow$ $\left|\frac{\widetilde{d}_{11}\widetilde{g}_{00}}{q^2} - 1\right| \le Z_I - 1$
[(L3); $Z_I = 1 + \zeta G/q^2$ (the statement)]
(L5) $\Rightarrow$ the statement
[(L4)]
□

Lemma I.27 (The fixed-point root's second diagonal [to table])**.** *In* ffSampling$^{\mathcal{F}}(B, s, t)$ *and in* ffSampling$^{\mathcal{F}}(B, s, t_{\mathrm{frac}})$*, the root node's second diagonal computed by the NTRU identity lies within* $Z_I/(1 - e_{00}) - 1$ *of* d_{11}*. Define:*

- *h and* $n := 2^h$*, those of* FFT *(Algorithm 14), Precondition;*
- $\Psi_n := \{\psi_k : k < n/2\}$*, that of Fact A.43 at* $m := n$*.*

Let:

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $\psi \in \Psi_n$*.*

Define:

- *The key bounds*
  - k_H*,* γ'_{fg} *and* δ_{fg}*, those of Definition A.36;*
  - $\check{\gamma}_{\mathrm{hyb}}$*, that of Definition A.35;*
  - $E_{00} := k_H\zeta + 4\gamma'_{fg}\delta_{fg} + 2\delta_{fg}^2$ *(Definition A.36);*
  - $m_0 := q/\check{\gamma}_{\mathrm{hyb}}^2 - E_{00}$ *and* $M_0 := q\check{\gamma}_{\mathrm{hyb}}^2 + E_{00}$ *(Definition A.37);*
- *The Gram matrix entries*
  - g_{00}*, the output of* Gram *(Algorithm 13) at line 4 of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10);*
  - $\widetilde{g}_{00}$*, the value* keychecks *computes in* $\mathcal{F}_{\mathrm{fx}}$ *(lines 1 to 11);*
- *The diagonals*
  - $d_{11} := q^2/g_{00}$*;*
  - $\widetilde{d}_{11}(\psi) := \mathrm{fl}(q^2/\widetilde{g}_{00}(\psi))$*, the value line 6 of* ffsamp *(Algorithm 6) computes in* $\mathcal{F}_{\mathrm{fx}}$ *(Lemma I.26 at* ψ*);*
- *The error chain*
  - $e_{00} := E_{00}/m_0$ *(Lemma I.25);*
  - $\bar{G} := M_0(1 + e_{00}) \in [0, \infty)$*;*
  - $Z_I := 1 + \zeta\bar{G}/q^2$ *(Lemma I.26 at* $G := \bar{G}$*).*

Assume:

(A1) $m_0 > 0$*;*
(A2) $e_{00} < 1$*.*
Then

$$\widetilde{d}_{11}(\psi)\ \mathcal{I}\left((Z_I/(1 - e_{00}) - 1)^{\pm}, 0\right)\ d_{11}(\psi).$$

Proof. (L1) $\widetilde{g}_{00}(\psi) \in (0, M_0 + E_{00}]$

[Lemma H.19, items 4 and 1, at ψ (the statement); Lemma H.17, item 3, at the checked key]

(L2) $M_0 + E_{00} \le \bar{G}$

[$\bar{G} = M_0(1 + e_{00})$, $e_{00} = E_{00}/m_0$ (the statement); e_{00} (Lemma I.25); $m_0 \le M_0$ (Lemma H.19, item 4, at the checked key and ψ); $m_0 > 0$ (assumption A1)]

(L3) $\Rightarrow$ $\widetilde{g}_{00}(\psi) \in (0, \bar{G}]$

[(L1), (L2)]

Lemma I.26 at $G := \bar{G}$	This proof
Shared: Z_I	
$\widetilde{g}_{00}$	$\widetilde{g}_{00}(\psi)$ (the statement)
$\widetilde{d}_{11}$	$\widetilde{d}_{11}(\psi)$ (the statement)
(I1) G	$\bar{G}$ (the statement)
$\widetilde{g}_{00} \in \mathcal{F}_{\mathrm{fx}}$	$\widetilde{g}_{00}$, computed in $\mathcal{F}_{\mathrm{fx}}$ (the statement)
$G \in \mathbb{R}$	$\bar{G}$ (the statement)
Assumption A1	(L3)
Its conclusion: $\left\lvert \frac{\widetilde{d}_{11}\,\widetilde{g}_{00}}{q^2} - 1 \right\rvert \le Z_I - 1$	

(L4) $\Rightarrow$ $\left\lvert \frac{\widetilde{d}_{11}(\psi)\,\widetilde{g}_{00}(\psi)}{q^2} - 1 \right\rvert \le Z_I - 1$

[(I1)]

(L5) $\frac{\widetilde{d}_{11}(\psi)}{d_{11}(\psi)} = \frac{\widetilde{d}_{11}(\psi)\widetilde{g}_{00}(\psi)/q^2}{\widetilde{g}_{00}(\psi)/g_{00}(\psi)}$

[$d_{11} = q^2/g_{00}$ (the statement); (L3); $g_{00}(\psi) \ge m_0$ (Lemma H.19, item 4, at the checked key and ψ); $m_0 > 0$ (assumption A1)]

(L6) $\left\lvert \frac{\widetilde{g}_{00}(\psi)}{g_{00}(\psi)} - 1 \right\rvert \le e_{00}$

[Lemma I.25, at the checked key and ψ (the statement); $\widetilde{d}_{00} = \widetilde{g}_{00}$ (Lemma I.25); Definition A.10; $g_{00}(\psi) \ge m_0$ (Lemma H.19, item 4, at the checked key and ψ); $m_0 > 0$ (assumption A1)]

(L7) $e_{00} \in [0, 1)$

[e_{00} (Lemma I.25); assumption A2]

Fact A.41, item 10	This proof
x	$\widetilde{d}_{11}(\psi)\,\widetilde{g}_{00}(\psi)/q^2$ (L4)
y	$\widetilde{g}_{00}(\psi)/g_{00}(\psi)$ (L6)
A	$Z_I - 1$ (L4)
b	e_{00} (the statement)
(I2) $x, y, A, b \in \mathbb{R}$	(L4), (L6); Z_I, e_{00} (the statement)
$\lvert x - 1 \rvert \le A$	(L4)
$\lvert y - 1 \rvert \le b$	(L6)
$b < 1$	(L7)
Its conclusion: $\lvert x/y - 1 \rvert \le (1 + A)/(1 - b) - 1$	

(L8) $\left\lvert \frac{\widetilde{d}_{11}(\psi)}{d_{11}(\psi)} - 1 \right\rvert \le \frac{1+(Z_I-1)}{1-e_{00}} - 1$

[(I2); (L5)]

(L9) $d_{11}(\psi) > 0$

[d_{11} (the statement); $g_{00}(\psi) \ge m_0$ (Lemma H.19, item 4, at the checked key and ψ); assumption A1]

(L10) $\frac{1+(Z_I-1)}{1-e_{00}} - 1 = Z_I/(1 - e_{00}) - 1$

[expand]

(L11) $\Rightarrow$ $\widetilde{d}_{11}(\psi)\ \mathcal{I}\left((Z_I/(1 - e_{00}) - 1)^{\pm}, 0\right)\ d_{11}(\psi)$

[(L8), (L9), (L10); Definition A.10 at $u_\circ := \widetilde{d}_{11}/d_{11} - 1$, $\zeta_\circ := 0$]

(L12) $\Rightarrow$ the statement

[(L11)]
□

Definition I.28 (The node map at $u = 0$ [to table])**.** Let:

- $d_{\mathrm{lo}}, d_{\mathrm{hi}} \in (0, \infty)$ with $d_{\mathrm{lo}} \le d_{\mathrm{hi}}$;
- $\chi \in [0, 1)$;
- $\kappa \in [0, \infty)$.

Define:

- The node bounds
  - $c_{\mathrm{sa}} := \sqrt{2}\,\zeta$ and $k_{\mathrm{sa}} := (1 + \sqrt{2}\,\zeta)/2 + \sqrt{2}$ (Corollary I.24 at $u := 0$);
  - $\forall x \ge 0:\ k_{zo}(x) := \sqrt{2}\,x^2 + \sqrt{2}\,x + 3$ (Corollary I.24 at $u := 0$, $|g_{01}| := x$);
  - $m_1 := d_{\mathrm{lo}}(1 - \chi) \in [0, \infty)$;
  - $u_0 := \zeta/(2m_1) \in [0, \infty)$;
  - $M_1 := d_{\mathrm{hi}}(1 + \chi)/2 \in [0, \infty)$;
  - $M_2 := M_1(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta \in [0, \infty)$;
- The terms
  - $r' := (1 + c_{\mathrm{sa}})^2 - 1 \in [0, \infty)$;
  - $\mathcal{Q}_0 := \left(2(1 + c_{\mathrm{sa}})k_{\mathrm{sa}}\zeta + k_{zo}(M_2)\,\zeta\,(1 + u_0)\right)/m_1 + (k_{\mathrm{sa}}\zeta)^2/m_1^2 \in [0, \infty)$;
  - $\mathcal{U}^0_\kappa(\chi) := \left(1 + \dfrac{\chi + \chi^2}{1 - \chi}\right)\left(1 + (1 + \kappa)((1 + u_0)^2 - 1) + \kappa r' + \mathcal{Q}_0\right)\left(1 + \dfrac{u_0}{1 - u_0}\right) - 1 + \dfrac{\zeta}{d_{\mathrm{lo}}} \in \mathbb{R}$, the node map.

```
noncomputable def PhiM0 (zeta m M kappa eps : Real) : Real :=
  (1 + (eps + eps ^ 2) / (1 - eps))
    * (1 + (1 + kappa) * ((1 + nodeU0 (0:Real) zeta eps m) ^ 2 - 1) + kappa * nodeR (0:Real)
        zeta + nodeQ0 zeta eps m M)
    * (1 + ((0:Real) + nodeU0 (0:Real) zeta eps m) / (1 - nodeU0 (0:Real) zeta eps m)) - 1 +
        zeta / m

noncomputable def nodeQ0 (zeta eps m M : Real) : Real :=
  (2 * (1 + cSa 0 zeta) * (kSa 0 zeta * zeta) + kGzo 0 (nodeM2 0 zeta eps M) * zeta * (1 +
      nodeU0 0 zeta eps m))
      / (m * (1 - eps))
    + (kSa 0 zeta * zeta) ^ 2 / (m * (1 - eps)) ^ 2

noncomputable def nodeU0 (u zeta eps m : Real) : Real :=
  (1 + u) * (1 + zeta / (2 * (m * (1 - eps) * (1 - u)))) - 1

noncomputable def nodeR (u zeta : Real) : Real := (1 + cSa u zeta) ^ 2 * (1 + u) ^ 4 - 1
```

Figure 74: The Lean declarations carrying Definition I.28: `PhiM0`, `nodeQ0`, `nodeU0`, `nodeR` (`FixedNode.lean`, `NodeMixed.lean`); Lean's symbols in ASCII.

Lemma I.29 (The fixed-point node's first diagonal [to table])**.** *Let:*

- $d_{\mathrm{lo}}, d_{\mathrm{hi}} \in (0, \infty)$*;*
- $a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$*;*
- $\psi \in \mathbb{C}$*;*
- $\chi \in [0, 1)$*;*
- $\omega_a, \omega_b \in \mathbb{R}$.

Define:

- $m_1 := d_{\mathrm{lo}}(1 - \chi)$ *and* $u_0 := \zeta/(2m_1)$ *(Definition I.28);*
- $\widetilde{a} := a(1 + \omega_a)$*;*

- $\widetilde{b} := b(1+\omega_b)$;
- $\widetilde{d}_0$, *the value* $\mathrm{split}_{\mathrm{sa}}$ *(Algorithm 3) computes in* $\mathcal{F}_{\mathrm{fx}}$ *from* $(f(\psi), f(-\psi)) := (\widetilde{a}, \widetilde{b})$ *(line 4).*

Assume:

(A1) $\widetilde{a}, \widetilde{b} \in \mathcal{F}_{\mathrm{fx}}$;

(A2) $|\psi| = 1$;

(A3) $u_0 < 1$;

(A4) $|\omega_a|, |\omega_b| \le \chi$.

Then

$$\widetilde{d}_0 \; \mathcal{I}\left(((1+\chi)(1+u_0)-1)^{\pm}, 0\right) \mathrm{AM}(a,b).$$

Proof.

DEFINES $u := 0$ (Definition I.1)

DEFINES $m_1' = d_{\mathrm{lo}}(1-\chi)(1-u)$, the m_1 of Lemma G.32, item 1

DEFINES $u_0' = (1+u)(1+\zeta/(2m_1')) - 1$, the u_0 of Lemma G.32, item 1

(L1) $u = 0 \Rightarrow \; m_1' = m_1$

[Definition I.1: $u = 0$; m_1' (the proof's block); m_1, u_0 (Definition I.28)]

(L2) $u = 0 \Rightarrow \; u_0' = u_0$

[Definition I.1: $u = 0$; (L1); u_0' (the proof's block); m_1, u_0 (Definition I.28)]

(I1)

Lemma G.32, item 1	This proof
Shared: $d_{\mathrm{lo}}, d_{\mathrm{hi}}$, a, b, ψ, χ, ω_a, ω_b, $\widetilde{a}, \widetilde{b}$, $\widetilde{d}_0$ Shared: assumption A2	
$\mathcal{F}, (u, \zeta)$	$\mathcal{F}_{\mathrm{fx}}, (0, 2^{-64})$ (Definition I.1)
m_1, u_0	m_1', u_0' (the proof's block)
$\mathcal{F}$ a realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
$d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$	The statement
Assumption A1	Assumption A1
Assumption A2	$u = 0$ (Definition I.1)
Assumption A3	Assumption A4
Assumption A4	Assumption A4
Assumption A6	Lemma G.14
Assumption A7	Assumption A3; (L2)
Its conclusion: $\widetilde{d}_0 \; \mathcal{I}\left(((1+\chi)(1+u_0)-1)^{\pm}, 0\right) \mathrm{AM}(a,b)$	

(L3) $\widetilde{d}_0 \; \mathcal{I}\left(((1+\chi)(1+u_0')-1)^{\pm}, 0\right) \mathrm{AM}(a,b)$

[(I1); u_0', m_1' (the proof's block)]

(L4) $\Rightarrow \; \widetilde{d}_0 \; \mathcal{I}\left(((1+\chi)(1+u_0)-1)^{\pm}, 0\right) \mathrm{AM}(a,b)$

[(L1), (L2), (L3)]

(L5) $\Rightarrow$ the statement

[(L4)]

□

Lemma I.30 (The fixed-point node's second diagonal [to table])**.** *Let:*

- $d_{\mathrm{lo}}, d_{\mathrm{hi}} \in (0, \infty)$;
- $a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$;
- $\psi \in \mathbb{C}$;
- $\chi \in [0, 1)$;
- $\omega_a, \omega_b \in \mathbb{R}$.

Define:

- $m_1 := d_{\mathrm{lo}}(1-\chi)$ *and* $u_0 := \zeta/(2m_1)$ *(Definition I.28);*
- $\mathcal{U}_\kappa^0$, *the node map of Definition I.28;*

- $\mathcal{U}^{\zeta}_{\kappa}$, *that of Lemma G.33 in* $\mathcal{F}_{\mathrm{fx}}$ *(Definition I.1).*

Then

1. *Define:*
   - $\widetilde{a} := a(1+\omega_a)$;
   - $\widetilde{b} := b(1+\omega_b)$;
   - $\widetilde{D} := |\widetilde{a}-\widetilde{b}|/2 \in [0,\infty)$.

   Assume:

   (A1) $\widetilde{a},\widetilde{b} \in \mathcal{F}_{\mathrm{fx}}$;
   (A2) $|\psi| = 1$;
   (A3) $u_0 < 1$;
   (A4) $|\omega_a|, |\omega_b| \le \chi$.

   Define:
   - $(\widetilde{d}_0, \widetilde{d}_1)$, *the values* $\mathrm{split}_{\mathrm{sa}}$ *(Algorithm 3) computes in* $\mathcal{F}_{\mathrm{fx}}$ *from* $(f(\psi), f(-\psi)) := (\widetilde{a},\widetilde{b})$ *(lines 4, 6);*
   - $\widetilde{d}_{11}$, *the value* $\mathrm{LDL}^{\dagger}$ *(Algorithm 5) computes in* $\mathcal{F}_{\mathrm{fx}}$ *at* $(g_{00},g_{01},g_{11}) := (\widetilde{d}_0,\widetilde{d}_1,\widetilde{d}_0)$ *(line 18);*
   - $\widetilde{\kappa} := \widetilde{D}^2/(\widetilde{a}\widetilde{b}) \in [0,\infty)$.

   Then $\widetilde{d}_{11}\ \mathcal{I}\left(\left(\mathcal{U}^{0}_{\widetilde{\kappa}}(\chi)\right)^{\pm}, 0\right)\ \mathrm{HM}(a,b)$;

2. $\forall \kappa \ge 0:\ \mathcal{U}^{\zeta}_{\kappa}(\chi) = \mathcal{U}^{0}_{\kappa}(\chi)$.

Proof.

DEFINES $u := 0$ (Definition I.1)
DEFINES $m'_1 = d_{\mathrm{lo}}(1-\chi)(1-u)$, the m_1 of Lemma G.32
DEFINES $u'_0 = (1+u)(1+\zeta/(2m'_1)) - 1$, the u_0 of Lemma G.32 and the $u_0(\chi)$ of Lemma G.33
DEFINES r'' and $\mathcal{Q}'$, the r' and the $\mathcal{Q}(\chi)$ of Lemma G.33

(L1) $u = 0 \Rightarrow\ m'_1 = m_1$

[Definition I.1: $u = 0$; m'_1 (the proof's block); m_1 (the statement)]

(L2) $u = 0 \Rightarrow\ u'_0 = u_0$

[Definition I.1: $u = 0$; (L1); u'_0 (the proof's block); u_0 (the statement)]

Lemma G.32, item 2	This proof
Shared: $d_{\mathrm{lo}}, d_{\mathrm{hi}},\ a, b,\ \psi,\ \chi,\ \omega_a, \omega_b,\ \widetilde{a}, \widetilde{b},\ \widetilde{\kappa},\ \widetilde{d}_{11}$	
Shared: assumption A2	
$\mathcal{F}, (u,\zeta)$	$\mathcal{F}_{\mathrm{fx}}, (0, 2^{-64})$ (Definition I.1)
c_H	$\mathcal{U}^{\zeta}_{\widetilde{\kappa}}(\chi)$
$\mathcal{F}$ a realization at (u,ζ)	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
(I1) $d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$	The statement
Assumption A1	Assumption A1
Assumption A2	$u = 0$ (Definition I.1)
Assumption A3	Assumption A4
Assumption A4	Assumption A4
Assumption A6	Lemma G.14
Assumption A7	Assumption A3; (L2)
Its conclusion: $\widetilde{d}_{11}\ \mathcal{I}\left(c_H^{\pm}, 0\right)\ \mathrm{HM}(a,b)$	

(L3) $\widetilde{d}_{11}\ \mathcal{I}\left(\left(\mathcal{U}^{\zeta}_{\widetilde{\kappa}}(\chi)\right)^{\pm}, 0\right)\ \mathrm{HM}(a,b)$

[(I1); $\mathcal{U}^{\zeta}_{\kappa}$ (Lemma G.33)]

(L4) $u = 0 \Rightarrow\ r'' = r'$

[Definition I.1: $u = 0$; r'' (the proof's block); c_{sa} (Lemma G.33); r', c_{sa} (Definition I.28)]

(L5) $u = 0 \Rightarrow \ \mathcal{Q}' = \mathcal{Q}_0$

[Definition I.1: $u = 0$; (L1), (L2); $\mathcal{Q}'$ (the proof's block); c_{sa}, k_{sa}, $M_2(\chi)$, $\bar{k}_{zo}(\chi)$ (Lemma G.33); $\mathcal{Q}_0$, c_{sa}, k_{sa}, M_2, k_{zo} (Definition I.28)]

(L6) $u = 0 \Rightarrow \ 1 + \dfrac{u + u_0}{1 - u_0} = 1 + \dfrac{u_0}{1 - u_0}$

[Definition I.1: $u = 0$]

(L7) $\Rightarrow \ \forall \kappa \geq 0 : \ \mathcal{U}^{\zeta}_{\kappa}(\chi) = \mathcal{U}^{0}_{\kappa}(\chi)$

[(L2), (L4), (L5), (L6); $\mathcal{U}^{\zeta}_{\kappa}$ (Lemma G.33); $\mathcal{U}^{0}_{\kappa}$ (Definition I.28)]

(L8) $\Rightarrow \ \widetilde{d}_{11}\, \mathcal{I}\left(\left(\mathcal{U}^{0}_{\widetilde{\kappa}}(\chi)\right)^{\pm}, 0\right) \text{HM}(a, b)$

[(L3), (L7) at $\kappa := \widetilde{\kappa}$; $\widetilde{\kappa}$ (the statement)]

(L9) $\Rightarrow$ item 1

[(L8)]

(L10) $\Rightarrow$ item 2

[(L7)]

□ (items 1 and 2)

Lemma I.31 (Monotonicity of the fixed-point bound map [to table])**.** *At $u = 0$ the bound map grows with its two arguments. Let:*

- $d_{\text{lo}} > 0$*;*
- $d_{\text{hi}} \geq d_{\text{lo}}$*.*

Define:

- $\mathcal{U}^{0}_{\kappa}$*, that of Definition I.28;*
- $\forall \chi \in [0, 1) : \ m_1(\chi) := d_{\text{lo}}(1 - \chi)$ *and* $u_0(\chi) := \zeta/(2m_1(\chi))$ *(Definition I.28).*

Then

$$\forall 0 \leq \chi \leq \chi' < 1, \ u_0(\chi') < 1 \ \forall 0 \leq \kappa \leq \kappa' : \quad \mathcal{U}^{0}_{\kappa}(\chi) \leq \mathcal{U}^{0}_{\kappa'}(\chi').$$

Proof.

DEFINES $\mathcal{U}^{\zeta}_{\kappa}(\chi)$ and $u'_0(\chi)$, the $\mathcal{U}^{\zeta}_{\kappa}(\chi)$ and the $u_0(\chi)$ of Lemma G.33 at $u := 0$ (Definition I.1)

(L1) $\forall \chi \in [0, 1) : \ u'_0(\chi) = u_0(\chi)$

[u'_0 (the proof's block); $u = 0$ (Definition I.1); m_1, u_0 (the statement)]

Lemma G.33 at $u := 0$ and at every χ, χ', κ, κ' of the statement's quantifier	This proof
Shared: ζ (Definition I.1), $d_{\text{lo}}, d_{\text{hi}}$, $\chi, \chi', \kappa, \kappa'$ (the scope)	
u	0 (Definition I.1)
$\mathcal{U}^{\zeta}_{\kappa}, u_0$	$\mathcal{U}^{\zeta}_{\kappa}, u'_0$ (the proof's block)
$u \in [0, 1)$	$u = 0$ (Definition I.1)
$\zeta \geq 0$	$\zeta := 2\zeta_{\text{op}}$ (Definition I.1)
(I1) $d_{\text{lo}}, d_{\text{hi}} > 0$	The statement
$\chi, \chi', \kappa, \kappa' \in \mathbb{R}$	The scope
Assumption A1	The scope; (L1)
Assumption A2	The scope
Assumption A3	The scope
Assumption A4	The scope
Assumption A5	The scope
Its conclusion: $\mathcal{U}^{\zeta}_{\kappa}(\chi) \leq \mathcal{U}^{\zeta}_{\kappa'}(\chi')$	

(L2) $\forall 0 \leq \chi \leq \chi' < 1, \ u_0(\chi') < 1 \ \forall 0 \leq \kappa \leq \kappa' : \ \mathcal{U}^{\zeta}_{\kappa}(\chi) \leq \mathcal{U}^{\zeta}_{\kappa'}(\chi')$

[(I1)]

	Lemma I.30, item 2 at χ and at χ' of the statement's quantifier	This proof
	Shared: $d_{\mathrm{lo}}, d_{\mathrm{hi}}$, $\mathcal{U}^0_\kappa$, $\mathcal{U}^\zeta_\kappa$ (the proof's block)	
	χ	χ, χ' (the scope)
(I2)	$a, b, \psi, \omega_a, \omega_b$	$d_{\mathrm{lo}}, d_{\mathrm{lo}}, 1, 0, 0$ (the scope)
	$d_{\mathrm{lo}}, d_{\mathrm{hi}} \in (0, \infty)$	The statement
	$a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$	$d_{\mathrm{lo}} \le d_{\mathrm{hi}}$ (the statement)
	$\psi \in \mathbb{C},\ \omega_a, \omega_b \in \mathbb{R}$	The scope
	$\chi \in [0, 1)$	The scope
	Its item 2: $\forall \kappa \ge 0 :\ \mathcal{U}^\zeta_\kappa(\chi) = \mathcal{U}^0_\kappa(\chi)$	
(L3)	$\Rightarrow$ the statement	
		[(L2); (I2)]
		□

Definition I.32 (The chain of the leaf diagonals at $u = 0$ [to table])**.** Let:

- $d_{\mathrm{lo}}, d_{\mathrm{hi}} \in (0, \infty)$ with $d_{\mathrm{lo}} \le d_{\mathrm{hi}}$;
- $h \ge 1$;
- $T \in \mathcal{T}_n$ with $n = 2^h$;
- $(\nu_k)_{0 \le k \le h-1}$ be a path: $\nu_0 = T$ and $\forall k \in \{1, \dots, h-1\} :\ \nu_k \in \{L(\nu_{k-1}), R(\nu_{k-1})\}$ (Definition A.18);
- $\forall k \in \{1, \dots, h-1\} :\ \kappa_k \in \mathbb{R}$;
- $\chi_0 \in [0, 1)$.

Define:

- $\forall \chi \in [0, 1) :\ m_1(\chi) := d_{\mathrm{lo}}(1 - \chi)$ (Definition I.28);
- $\forall \chi \in [0, 1) :\ u_0(\chi) := \zeta/(2m_1(\chi))$ (Definition I.28);
- $\mathcal{U}^0_\kappa$, the node map of Definition I.28;
- $\mathcal{A} := \{\chi : 0 \le \chi < 1,\ u_0(\chi) < 1\}$;
- $\forall k \in \{1, \dots, h-1\} :\ \vartheta_{k-1} := (1 + \chi_{k-1})/(1 - \chi_{k-1})$;
- $\forall k \in \{1, \dots, h-1\} :\ \hat{\kappa}_k := \vartheta_{k-1}\kappa_k + (\vartheta_{k-1} - 1)/2$;
- $\forall k \in \{1, \dots, h-1\} :\ \chi_k := \mathcal{U}^0_{\hat{\kappa}_k}(\chi_{k-1})$.

```
noncomputable abbrev fxChain (zeta m M : Real) (kappa : Nat -> Real) (chi0 : Real) : Nat ->
    Real :=
  iterMap (fun kappa' chi' => PhiM0 zeta m M (kappaHat chi' kappa') chi') kappa chi0

noncomputable def iterMap (Psi : Real -> Real -> Real) (kappa : Nat -> Real) (eps0 : Real) :
    Nat -> Real
  | 0 => eps0
  | k + 1 => Psi (kappa (k + 1)) (iterMap Psi kappa eps0 k)

noncomputable def kappaHat (chi kappa : Real) : Real := (1 + chi) / (1 - chi) * kappa + ((1 +
    chi) / (1 - chi) - 1) / 2
```

Figure 75: The Lean declarations carrying Definition I.32: `fxChain`, `iterMap`, `kappaHat` (`Depth.lean`, `FixedNode.lean`); with `PhiM0` of Figure 74; Lean's symbols in ASCII.

Corollary I.33 (The computed diagonals of the fixed-point signer [to table])**.** *The chain χ_k bounds the computed diagonals at every depth, and its last term bounds the leaves'. Let:*

- *(f, g, F, G) be a checked key (Definition 5.5) of degree $n = 2^h$;*
- *$(\nu_k)_{0 \le k \le h-1}$ be a path of the key's tree T (Definition I.32; T below);*
- $\chi_0 \in [0, 1)$.

Define:

- *The key bounds*
  - m_0 *and* M_0*, those of Definition A.37;*
  - $d_{\mathrm{lo}} := \min(m_0, q^2/M_0)$ *(Definition A.37);*
  - $d_{\mathrm{hi}} := \max(M_0, q^2/m_0)$ *(Definition A.37);*
  - $\bar{\varsigma} := d_{\mathrm{hi}}/d_{\mathrm{lo}}$ *(Definition A.37);*
  - $\forall k \in \{1, \dots, h-1\}:\ \bar{\kappa}_k := (\bar{\varsigma}-1)^2/(4\bar{\varsigma}) \in [0, \infty)$ *(Proposition 5.8, item 2);*
- *The tree*
  - $\mathcal{G}$*, that of Proposition 5.8;*
  - $T :=$ ffLDL$^\dagger(\mathcal{G})$ *(Definition A.20);*
  - $\forall \nu \in \mathrm{Sub}(T):\ \mathcal{G}_\nu$*, that of Definition A.32;*
  - $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi:\ (g_{00}, g_{01}, g_{11})$*, the entries of* $\mathcal{G}_\nu(\psi)$ *(Definition A.14);*
- *The key constants*
  - $\forall k \in \{1, \dots, h-1\}:\ \kappa_k := \max_{\nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu)=k}\ \max_\psi |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$ *(Definition 4.6 at the key);*
- *The diagonals*
  - $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi:\ d^\nu_{00}(\psi) := g_{00}$ *and* $d^\nu_{11}(\psi) := g_{11} - |g_{01}|^2/g_{00}$ *(Corollary G.36);*
  - $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}:\ \widetilde{d}^\nu_j$*, the diagonal* ffLDL† *computes in* $\mathcal{F}_{\mathrm{fx}}$ *at* ν *in place of* d^ν_j *(Corollary G.36);*
  - d_{00} *and* d_{11}*, the root's diagonals;*
- *The node bounds*
  - $\forall \chi \in [0, 1):\ m_1(\chi) := d_{\mathrm{lo}}(1-\chi)$ *(Definition I.28);*
  - $\forall \chi \in [0, 1):\ u_0(\chi) := \zeta/(2m_1(\chi))$ *(Definition I.28);*
  - $\mathcal{U}^0_\kappa$*, the node map of Definition I.28;*
  - $\mathcal{A} := \{\chi : 0 \le \chi < 1,\ u_0(\chi) < 1\}$ *(Definition I.32 at* d_{lo} *and* ζ*);*
- *The error chain*
  - $\forall k \in \{1, \dots, h-1\}:\ \vartheta_{k-1} := (1+\chi_{k-1})/(1-\chi_{k-1})$ *(Definition I.32);*
  - $\forall k \in \{1, \dots, h-1\}:\ \hat{\kappa}_k := \vartheta_{k-1}\bar{\kappa}_k + (\vartheta_{k-1}-1)/2$ *(Definition I.32 at* $\kappa_k := \bar{\kappa}_k$*);*
  - $\forall k \in \{1, \dots, h-1\}:\ \chi_k := \mathcal{U}^0_{\hat{\kappa}_k}(\chi_{k-1})$ *(Definition I.32 at* $\kappa_k := \bar{\kappa}_k$*);*
  - $\chi_{\mathrm{leaf}} := \max_{\nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu)=h-1}\ \max_{j \in \{00,11\}}\ \max_\psi |\widetilde{d}^\nu_j(\psi)/d^\nu_j(\psi) - 1|$ *(Corollary G.36).*

Assume:

(A1) $\forall \psi:\ \widetilde{d}_{00}(\psi)\ \mathcal{I}\left(\chi_0^{\pm}, 0\right) d_{00}(\psi)$ *at the root node;*

(A2) $\forall \psi:\ \widetilde{d}_{11}(\psi)\ \mathcal{I}\left(\chi_0^{\pm}, 0\right) d_{11}(\psi)$ *at the root node;*

(A3) $\forall k \le h-1:\ \chi_k \in \mathcal{A}$.

Then

1. $\forall k \le h-1\ \forall j \in \{00, 11\}\ \forall \psi:\ \widetilde{d}^{\nu_k}_j(\psi)\ \mathcal{I}\left(\chi_k^{\pm}, 0\right) d^{\nu_k}_j(\psi)$;
2. $\chi_{\mathrm{leaf}} \le \chi_{h-1}$.

Proof.

DEFINES $\widetilde{\kappa}_k := \widetilde{D}^2/(\widetilde{a}\widetilde{b})$ at ν_k (Lemma I.30), with $\widetilde{D}$, $\widetilde{a}$ and $\widetilde{b}$ that lemma's at ν_k

DEFINES $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi:\ \kappa_\nu(\psi) := |g_{01}|^2/(g_{00}g_{11} - |g_{01}|^2)$ (Corollary G.36)

DEFINES $\forall k \in \{1, \dots, h-1\}:\ j(k) := \begin{cases} 00 & \nu_k = L(\nu_{k-1}) \\ 11 & \nu_k = R(\nu_{k-1}) \end{cases}$, the diagonal of ν_{k-1} the child ν_k splits (Definition A.20, items 5 to 7; Definition A.18)

(L1) $\forall k \in \{1, \dots, h-1\}\ \forall j \in \{00, 11\}\ \forall \psi:\ d^{\nu_{k-1}}_j(\psi), d^{\nu_{k-1}}_j(-\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$
[Proposition 5.8, item 1, at the checked key (the statement)]

(L2) $d_{\mathrm{lo}} > 0$
[Proposition 5.8, (L13), at the checked key (the statement)]

(L3) $\forall\psi:\ |\psi|=1$

[Fact A.42, item 1]

(L4) $\forall k\in\{1,\dots,h-1\}:\ \chi_{k-1}\in[0,1)$

[assumption A3; $\mathcal{A}$ (Definition I.32)]

(L5) $\forall k\in\{1,\dots,h-1\}:\ u_0(\chi_{k-1})<1$

[assumption A3; $\mathcal{A}$ (Definition I.32)]

Fact D.1 $\forall k\in\{1,\dots,h-1\}\ \forall\psi$	This proof
m	$n/2^{k-1}$ (the statement)
d	$d_{j(k)}^{\nu_{k-1}}$ (the statement; the proof's block)
ψ	ψ (the scope)
d_0	$d_{00}^{\nu_k}(\psi^2)$ (Definition A.32; Definition A.20, items 3 to 6, at $j(k)$)
(I1) $m\in\{2^i:i\geq 1\}$	$n=2^h$, $k\leq h-1$ (the statement)
(I1) $d\in\mathcal{R}_m$	$d_{j(k)}^{\nu_{k-1}}$ (the statement)
(I1) $\psi^m=-1$	The scope
Assumption A1	(L1), (L2)
Assumption A2	(L1), (L2)
Its item 1: $d_0=\mathrm{AM}(a,b)$	
Its item 3: $\lvert d_1\rvert=\lvert a-b\rvert/2$	

Lemma I.29 $\forall k\in\{1,\dots,h-1\}\ \forall\psi$, under $\forall\psi:\ \lvert\widetilde{d}_{j(k)}^{\nu_{k-1}}(\psi)/d_{j(k)}^{\nu_{k-1}}(\psi)-1\rvert\leq\chi_{k-1}$	This proof
Shared: $d_{\mathrm{lo}},d_{\mathrm{hi}},\ \psi$ (the scope)	
a,b	$d_{j(k)}^{\nu_{k-1}}(\psi), d_{j(k)}^{\nu_{k-1}}(-\psi)$ (the statement)
χ	χ_{k-1} (the statement)
u_0	$u_0(\chi_{k-1})$ (the statement)
ω_a,ω_b	$\widetilde{d}_{j(k)}^{\nu_{k-1}}(\psi)/d_{j(k)}^{\nu_{k-1}}(\psi)-1, \widetilde{d}_{j(k)}^{\nu_{k-1}}(-\psi)/d_{j(k)}^{\nu_{k-1}}(-\psi)-1$ (the statement)
(I2) $\widetilde{d}_0$	$\widetilde{d}_{00}^{\nu_k}(\psi^2)$ (Definition A.20, items 3 to 6, at $j(k)$)
(I2) $d_{\mathrm{lo}},d_{\mathrm{hi}}\in(0,\infty)$	(L2), (L1)
(I2) $a,b\in[d_{\mathrm{lo}},d_{\mathrm{hi}}]$	(L1)
(I2) $\psi\in\mathbb{C}$	The scope
(I2) $\chi\in[0,1)$	(L4)
(I2) $\omega_a,\omega_b\in\mathbb{R}$	$\widetilde{d}_j^{\nu}$, d_j^{ν} (the statement)
Assumption A1	$\widetilde{d}_{j(k)}^{\nu_{k-1}}$, computed in $\mathcal{F}_{\mathrm{fx}}$ (the statement)
Assumption A2	(L3)
Assumption A3	(L5)
Assumption A4	The scope
Its conclusion: $\widetilde{d}_0\ \mathcal{I}\left(((1+\chi)(1+u_0)-1)^{\pm},0\right)\ \mathrm{AM}(a,b)$	

(L6) $\forall k\in\{1,\dots,h-1\}:\ [\forall\psi:\ |\widetilde{d}_{j(k)}^{\nu_{k-1}}(\psi)/d_{j(k)}^{\nu_{k-1}}(\psi)-1|\leq\chi_{k-1}]$

$\Rightarrow\ \forall\psi:\ \widetilde{d}_{00}^{\nu_k}(\psi^2)\ \mathcal{I}\left(((1+\chi_{k-1})(1+u_0(\chi_{k-1}))-1)^{\pm},0\right)\ \mathrm{AM}(d_{j(k)}^{\nu_{k-1}}(\psi),d_{j(k)}^{\nu_{k-1}}(-\psi))$

[(I2)]

(L7) $\forall k\in\{1,\dots,h-1\}:\ [\forall\psi:\ |\widetilde{d}_{j(k)}^{\nu_{k-1}}(\psi)/d_{j(k)}^{\nu_{k-1}}(\psi)-1|\leq\chi_{k-1}]\Rightarrow\ \forall\psi:\ |\widetilde{d}_{00}^{\nu_k}(\psi^2)/d_{00}^{\nu_k}(\psi^2)-1|\leq(1+\chi_{k-1})(1+u_0(\chi_{k-1}))-1$

[(L6); item 1 of (I1); Definition A.10]

Lemma I.30, item 1 $\forall k \in \{1,\dots,h-1\}\ \forall\psi$, under $\forall\psi:\ \lvert\widetilde{d}^{\nu_{k-1}}_{j(k)}(\psi)/d^{\nu_{k-1}}_{j(k)}(\psi)-1\rvert \le \chi_{k-1}$	This proof
Shared: $d_{\mathrm{lo}}, d_{\mathrm{hi}},\ \psi$ (the scope)	
a, b	$d^{\nu_{k-1}}_{j(k)}(\psi), d^{\nu_{k-1}}_{j(k)}(-\psi)$ (the statement)
χ	χ_{k-1} (the statement)
ω_a, ω_b	$\widetilde{d}^{\nu_{k-1}}_{j(k)}(\psi)/d^{\nu_{k-1}}_{j(k)}(\psi)-1, \widetilde{d}^{\nu_{k-1}}_{j(k)}(-\psi)/d^{\nu_{k-1}}_{j(k)}(-\psi)-1$ (the statement)
$\widetilde{\kappa}$	$\widetilde{\kappa}_k$ (the proof's block)
$\widetilde{d}_{11}$	$\widetilde{d}^{\nu_k}_{11}(\psi^2)$ (Definition A.20, items 3 to 6, at $j(k)$)
(I3) $d_{\mathrm{lo}}, d_{\mathrm{hi}} \in (0,\infty)$	(L2), (L1)
$a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$	(L1)
$\psi \in \mathbb{C}$	The scope
$\chi \in [0,1)$	(L4)
$\omega_a, \omega_b \in \mathbb{R}$	$\widetilde{d}^{\nu}_{j}$, d^{ν}_{j} (the statement)
Assumption A1	$\widetilde{d}^{\nu_{k-1}}_{j(k)}$, computed in $\mathcal{F}_{\mathrm{fx}}$ (the statement)
Assumption A2	(L3)
Assumption A3	(L5)
Assumption A4	The scope
Its conclusion: $\widetilde{d}_{11}\ \mathcal{I}\left(\left(\mathcal{U}^0_{\widetilde{\kappa}}(\chi)\right)^{\pm}, 0\right)\ \mathrm{HM}(a,b)$	

(L8) $\forall k \in \{1,\dots,h-1\}:\ [\forall\psi:\ \lvert\widetilde{d}^{\nu_{k-1}}_{j(k)}(\psi)/d^{\nu_{k-1}}_{j(k)}(\psi)-1\rvert \le \chi_{k-1}]$
$\Rightarrow\ \forall\psi:\ \widetilde{d}^{\nu_k}_{11}(\psi^2)\ \mathcal{I}\left(\left(\mathcal{U}^0_{\kappa_k}(\chi_{k-1})\right)^{\pm}, 0\right)\ \mathrm{HM}(d^{\nu_{k-1}}_{j(k)}(\psi), d^{\nu_{k-1}}_{j(k)}(-\psi))$

[(I3)]

Fact D.2 $\forall k \in \{1,\dots,h-1\}\ \forall\psi$	This proof
m	$n/2^{k-1}$ (the statement)
d	$d^{\nu_{k-1}}_{j(k)}$ (the statement; the proof's block)
ψ	ψ (the scope)
d_{11}	$d^{\nu_k}_{11}(\psi^2)$ (Definition A.32; Definition A.20, items 3 to 6, at $j(k)$)
(I4) $m \in \{2^i : i \ge 1\}$	$n = 2^h$, $k \le h-1$ (the statement)
$d \in \mathcal{R}_m$	$d^{\nu_{k-1}}_{j(k)}$ (the statement)
$\psi^m = -1$	The scope
Assumption A1	(L1), (L2)
Assumption A2	(L1), (L2)
Its conclusion: $d_{11} = \mathrm{HM}(a,b)$	

(L9) $\forall k \in \{1,\dots,h-1\}:\ [\forall\psi:\ \lvert\widetilde{d}^{\nu_{k-1}}_{j(k)}(\psi)/d^{\nu_{k-1}}_{j(k)}(\psi)-1\rvert \le \chi_{k-1}] \Rightarrow\ \forall\psi:\ \lvert\widetilde{d}^{\nu_k}_{11}(\psi^2)/d^{\nu_k}_{11}(\psi^2)-1\rvert \le \mathcal{U}^0_{\kappa_k}(\chi_{k-1})$

[(L8); (I4); Definition A.10]

(L10) $\Rightarrow\ \forall k \in \{1,\dots,h-1\}:\ [\forall j \in \{00,11\}\ \forall\psi:\ \lvert\widetilde{d}^{\nu_{k-1}}_{j}(\psi)/d^{\nu_{k-1}}_{j}(\psi)-1\rvert \le \chi_{k-1}] \Rightarrow\ \forall j \in \{00,11\}\ \forall\psi:\ \lvert\widetilde{d}^{\nu_k}_{j}(\psi^2)/d^{\nu_k}_{j}(\psi^2)-1\rvert \le \max\big((1+\chi_{k-1})(1+u_0(\chi_{k-1}))-1,\ \mathcal{U}^0_{\kappa_k}(\chi_{k-1})\big)$

[(L7) at $j = 00$, (L9) at $j = 11$, each at $j(k) \in \{00,11\}$ (the proof's block); Definition I.32; Fact A.41, item 20]

(L11) $\forall k \in \{1,\dots,h-1\}:\ \bar{\kappa}_k \ge 0$

[(L1), (L2); $\bar{\kappa}_k$, $\bar{\varsigma}$ (the statement)]

(L12) $\forall k \in \{1,\dots,h-1\}:\ \hat{\kappa}_k \ge 0$

[(L11), (L4); $\hat{\kappa}_k$, ϑ_{k-1} (Definition I.32, at $\kappa_k := \bar{\kappa}_k$)]

	Lemma G.34 at every $k \in \{1, \dots, h-1\}$	This proof
	Shared: ζ (Definition I.1), $d_{\mathrm{lo}}, d_{\mathrm{hi}}$	
	u	0
	χ	χ_{k-1} (the statement)
	κ	$\hat{\kappa}_k$ (Definition I.32)
(I5)	$\mathcal{U}_\kappa^\zeta, u_0$	$\mathcal{U}_\kappa^0, u_0$ (Lemma I.30, item 2)
	$u \in [0, 1)$	$u = 0$ (Definition I.1)
	$\zeta \geq 0$	ζ (Definition I.1)
	$d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$	(L2), (L1)
	$\chi, \kappa \in \mathbb{R}$	(L4), (L12)
	Assumption A1 Assumption A2	Assumption A3 (L12)
	Its conclusion: $(1+\chi)(1+u_0(\chi)) - 1 \leq \mathcal{U}_\kappa^\zeta(\chi)$	

(L13) $\forall k \in \{1, \dots, h-1\} : \ (1+\chi_{k-1})(1+u_0(\chi_{k-1})) - 1 \leq \mathcal{U}_{\hat{\kappa}_k}^0(\chi_{k-1})$

[(I5)]

(L14) $\forall k \in \{1, \dots, h-1\} : \ \kappa_k \leq \bar{\kappa}_k$

[Proposition 5.8, item 2, at the checked key (the statement)]

	Lemma G.35 $\forall k \in \{1, \dots, h-1\}$ $\forall \psi$, under $\forall \psi : \ \lvert \widetilde{d}_{j(k)}^{\nu_{k-1}}(\psi) / d_{j(k)}^{\nu_{k-1}}(\psi) - 1 \rvert \leq \chi_{k-1}$	This proof
	a, b	$d_{j(k)}^{\nu_{k-1}}(\psi), d_{j(k)}^{\nu_{k-1}}(-\psi)$ (the statement)
	χ	χ_{k-1} (the statement)
	ω_a, ω_b	$\widetilde{d}_{j(k)}^{\nu_{k-1}}(\psi) / d_{j(k)}^{\nu_{k-1}}(\psi) - 1, \widetilde{d}_{j(k)}^{\nu_{k-1}}(-\psi) / d_{j(k)}^{\nu_{k-1}}(-\psi) - 1$ (the statement)
(I6)	$\widetilde{\kappa}$	$\widetilde{\kappa}_k$ (the proof's block)
	ϑ	ϑ_{k-1} (Definition I.32)
	$a, b > 0$	(L1), (L2)
	$\chi \in [0, 1)$	(L4)
	$\omega_a, \omega_b \in \mathbb{R}$	$\widetilde{d}_j^\nu$, d_j^ν (the statement)
	Assumption A1 Assumption A2	The scope The scope
	Its conclusion: $\widetilde{\kappa} \leq \vartheta\kappa + (\vartheta - 1)/2$	

(L15) $\forall k \in \{1, \dots, h-1\} : \ [\forall \psi : \ \lvert \widetilde{d}_{j(k)}^{\nu_{k-1}}(\psi) / d_{j(k)}^{\nu_{k-1}}(\psi) - 1 \rvert \leq \chi_{k-1}]$

$$\Rightarrow \ \forall \psi : \ \widetilde{\kappa}_k \leq \vartheta_{k-1} \frac{(d_{j(k)}^{\nu_{k-1}}(\psi) - d_{j(k)}^{\nu_{k-1}}(-\psi))^2}{4 d_{j(k)}^{\nu_{k-1}}(\psi) d_{j(k)}^{\nu_{k-1}}(-\psi)} + (\vartheta_{k-1} - 1)/2$$

[(I6)]

(L16) $\forall k \in \{1, \dots, h-1\} \ \forall \psi : \ \kappa_{\nu_k}(\psi^2) = \frac{(d_{j(k)}^{\nu_{k-1}}(\psi) - d_{j(k)}^{\nu_{k-1}}(-\psi))^2}{4 d_{j(k)}^{\nu_{k-1}}(\psi) d_{j(k)}^{\nu_{k-1}}(-\psi)}$

[items 1 and 3 of (I1); $\mathcal{G}_\nu$ (Definition A.32); Definition A.20, items 3 to 6, at $j(k)$; κ_ν (the proof's block); expand]

(L17) $\forall k \in \{1, \dots, h-1\} \ \forall \psi : \ \kappa_{\nu_k}(\psi^2) \leq \kappa_k$

[κ_ν (the proof's block); κ_k (the statement); ν_k (Definition I.32); depth (Definition A.18)]

(L18) $\forall k \in \{1, \dots, h-1\} : \ [\forall \psi : \ \lvert \widetilde{d}_{j(k)}^{\nu_{k-1}}(\psi) / d_{j(k)}^{\nu_{k-1}}(\psi) - 1 \rvert \leq \chi_{k-1}] \Rightarrow \ \forall \psi : \ \widetilde{\kappa}_k \leq \hat{\kappa}_k$

[(L15), (L16), (L17), (L14), (L4); ϑ_{k-1}, $\hat{\kappa}_k$ (Definition I.32); Fact A.41, item 8]

	Lemma I.31	This proof
	$d_{\mathrm{lo}}, d_{\mathrm{hi}}$	$d_{\mathrm{lo}}, d_{\mathrm{hi}}$ (the statement)
(I7)	$d_{\mathrm{lo}} > 0$	(L2)
	$d_{\mathrm{hi}} \geq d_{\mathrm{lo}}$	(L1)
	Its conclusion: $\forall 0 \leq \chi \leq \chi' < 1,\ u_0(\chi') < 1\ \forall 0 \leq \kappa \leq \kappa' :\ \mathcal{U}^0_{\kappa}(\chi) \leq \mathcal{U}^0_{\kappa'}(\chi')$	

(L19) $\forall 0 \leq \chi \leq \chi' < 1,\ u_0(\chi') < 1\ \forall 0 \leq \kappa \leq \kappa' :\ \mathcal{U}^0_{\kappa}(\chi) \leq \mathcal{U}^0_{\kappa'}(\chi')$

[(I7)]

(L20) $\forall k \in \{1, \ldots, h-1\} :\ [\forall \psi :\ |\widetilde{d}^{\nu_{k-1}}_{j(k)}(\psi)/d^{\nu_{k-1}}_{j(k)}(\psi) - 1| \leq \chi_{k-1}] \Rightarrow\ \max\big((1+\chi_{k-1})(1+u_0(\chi_{k-1})) - 1,\ \mathcal{U}^0_{\widetilde{\kappa}_k}(\chi_{k-1})\big) \leq \mathcal{U}^0_{\hat{\kappa}_k}(\chi_{k-1})$

[(L19) at $\chi, \chi' := \chi_{k-1}$, $\kappa := \widetilde{\kappa}_k$ and $\kappa' := \hat{\kappa}_k$ by (L18); (L13), (L4), (L5); Fact A.41, item 24]

(L21) $\Rightarrow\ \forall k \in \{1, \ldots, h-1\} :\ [\forall \psi :\ |\widetilde{d}^{\nu_{k-1}}_{j(k)}(\psi)/d^{\nu_{k-1}}_{j(k)}(\psi) - 1| \leq \chi_{k-1}] \Rightarrow\ \max\big((1+\chi_{k-1})(1+u_0(\chi_{k-1})) - 1,\ \mathcal{U}^0_{\widetilde{\kappa}_k}(\chi_{k-1})\big) \leq \chi_k$

[(L20); χ_k (Definition I.32)]

(L22) $\forall j \in \{00, 11\}\ \forall \psi :\ \widetilde{d}^{\nu_0}_j(\psi)\ \mathcal{I}\left(\chi_0^{\pm}, 0\right)\ d^{\nu_0}_j(\psi)$

[assumptions A1, A2; $\nu_0 = T$ (Definition I.32); d_{00}, d_{11} (the statement)]

(L23) $\forall k \in \{1, \ldots, h-1\} :\ [\forall j \in \{00, 11\}\ \forall \psi :\ |\widetilde{d}^{\nu_{k-1}}_j(\psi)/d^{\nu_{k-1}}_j(\psi) - 1| \leq \chi_{k-1}] \Rightarrow\ \forall j \in \{00, 11\}\ \forall \psi :\ |\widetilde{d}^{\nu_k}_j(\psi^2)/d^{\nu_k}_j(\psi^2) - 1| \leq \chi_k$

[(L10); (L21) at $j(k) \in \{00, 11\}$ (the proof's block)]

(L24) $\forall k \in \{1, \ldots, h-1\} :\ \{\psi^2 : \psi \text{ a root of } \nu_{k-1}\text{'s ring}\} = \{\text{the roots of } \nu_k\text{'s ring}\}$

[Fact A.43, item 5, at $m := n/2^{k-1}$]

(L25) $\Rightarrow\ \forall k \leq h-1\ \forall j \in \{00, 11\}\ \forall \psi :\ \widetilde{d}^{\nu_k}_j(\psi)\ \mathcal{I}\left(\chi_k^{\pm}, 0\right)\ d^{\nu_k}_j(\psi)$

[induction on k: (L22) the base; (L23), (L24) the step; Definition A.10]

(L26) $\Rightarrow$ item 1

[(L25)]

(L27) $\forall (\nu'_k)_{0 \leq k \leq h-1}$ a path of $T\ \forall k \leq h-1\ \forall j \in \{00, 11\}\ \forall \psi :\ \widetilde{d}^{\nu'_k}_j(\psi)\ \mathcal{I}\left(\chi_k^{\pm}, 0\right)\ d^{\nu'_k}_j(\psi)$

[(L25) at the statement's path $(\nu_k) := (\nu'_k)$; χ_k (Definition I.32 at $\kappa_k := \bar{\kappa}_k$)]

(L28) $\forall \nu \in \mathrm{Sub}(T),\ \mathrm{depth}(\nu) = h-1\ \exists (\nu'_k)_{0 \leq k \leq h-1}$ a path of $T :\ \nu'_{h-1} = \nu$

[a path (Definition I.32); depth, L, R (Definition A.18)]

(L29) $\Rightarrow\ \chi_{\mathrm{leaf}} \leq \chi_{h-1}$

[(L27) at $k = h-1$, (L28); Definition A.10; χ_{leaf} (the statement)]

(L30) $\Rightarrow$ item 2

[(L29)]

□ (items 1 and 2)

I.3.2 No overflow in the key check

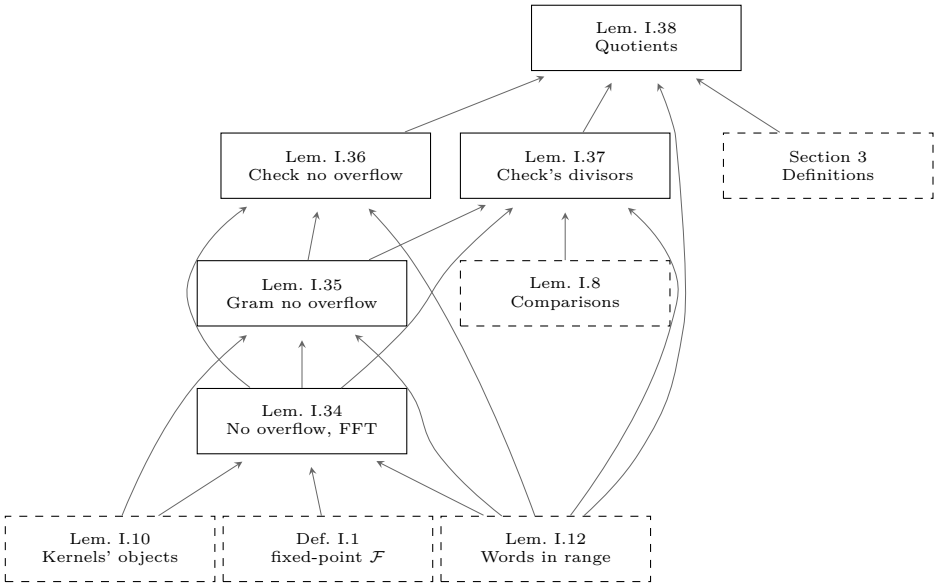


Figure 76: Dependencies, Appendix I.3.2.

Lemma I.34 (No overflow in the FFT expansion [to table])**.** *The expansion of an int8 array keeps every word's value within M_j at stage j, below 2^{81}; a product's modulus is at most the product of the moduli over 2^{64} plus $\sqrt{2}$; the stages on any input whose words hold their values within M keep them within $c^{h-1}(M+2)-2$. Let:*

- $h \in \{3, \dots, 10\}$;
- $p \in \{-128, \dots, 127\}^{2^h}$, *an int8 array;*
- $B \in [0, 127]$;
- $W_x = (W_{x_r}, W_{x_i})$ *be a pair of words written at stage j of the expansion of p, a root's real and imaginary parts: of* `fxpoly_set_small` *on p, of the $h-1$ stages of* FFT *(Algorithm 14, lines 2 to 25) after it, or of* `fxpoly_neg` *on the words of the last stage.*

Define:

- $n := 2^h$;
- $x := x_r + ix_i$, *the complex number the line of W_x computes in $\mathcal{F}_{\text{fx}}$ (Definition I.1);*
- $\forall j \leq h-1$: X_j, *the numbers x of the pairs written at stage j, X_0 those of* `fxpoly_set_small`;
- X^-, *the numbers x of the pairs* `fxpoly_neg` *writes on pairs of X_{h-1};*
- $M_0 := \sqrt{2}\, B 2^{64}$;
- $\forall j \leq h-2:\ M_{j+1} := M_j(1 + (2^{64}+1)/2^{64}) + \sqrt{2}$;
- $c := 2(1 + 2^{-65})$.

Then

1. *Assume:*

   (A1) $\forall k < n:\ p_{[k]} \in [-B, B]$.

   Then, at each part, $\forall j \leq h-1\ \forall x \in X_j:\ W_x = x_{\text{fx64}} \bmod 2^{128}$;

2. *Under assumption A1,* $\forall j \leq h-1\ \forall x \in X_j:\ |x_{\text{fx64}}| \leq M_j$;

3. *Under assumption A1, at each part,* $\forall x \in X^-:\ W_x = x_{\text{fx64}} \bmod 2^{128}$;

4. *Under assumption A1,* $\forall x \in X^-:\ |x_{\text{fx64}}| \leq M_{h-1}$;

5. $\forall j \leq h-1:\ M_j \leq c^{h-1}(1.4143\, B 2^{64} + 2) - 2$;

6. $c^{h-1}(1.4143\,B2^{64}+2)-2<2^{81}$;

7. $\forall v,w\in C_{\mathcal{F}_{\mathrm{fx}}}:\ |(v\otimes w)_{\mathrm{fx64}}|\le |v_{\mathrm{fx64}}||w_{\mathrm{fx64}}|/2^{64}+\sqrt{2}$;

8. *Let:*

   - $M\ge 0$;
   - $\forall j\in\{0,\dots,h-1\}:\ Y_j$, *the numbers of the pairs written at stage* j *of* $\widetilde{\mathrm{FFT}}$ *(Algorithm 14, lines 2 to 25) on an input array of pairs of words,* Y_0 *those of the input.*

   Assume:

   (A2) $\forall \mathfrak{p}\in\{\mathrm{Re},\mathrm{Im}\}\ \forall y\in Y_0:\ W_{\mathfrak{p}(y)}=\mathfrak{p}(y)_{\mathrm{fx64}} \bmod 2^{128}$;
   (A3) $\forall y\in Y_0:\ |y_{\mathrm{fx64}}|\le M$;
   (A4) $c^{h-1}(M+2)-2<2^{127}$.

   Then, at each part, $\forall j\le h-1\ \forall y\in Y_j:\ W_y=y_{\mathrm{fx64}} \bmod 2^{128}$;

9. *Under assumptions A2 to A4, at* M *and* Y_j *of item 8,* $\forall j\le h-1\ \forall y\in Y_j:\ |y_{\mathrm{fx64}}|\le c^{h-1}(M+2)-2$.

Proof. (L1) $127\cdot 2^{64}<2^{127}$ [expand]

Lemma I.10, item 9	This proof
f	p (the statement)
(I1) $\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
$h\in\{2,\dots,10\}$	$h\in\{3,\dots,10\}$ (the statement)
Its item 9: $W_{f_{[k]}}=f_{[k],\mathrm{fx64}} \bmod 2^{128}$	

Lemma I.12, item 1 at every $x\in X_0$, at each part	This proof
Shared: W_x	
V	$p_{[k],\mathrm{fx64}}, p_{[k+n/2],\mathrm{fx64}}$ (Lemma I.10, item 9)
(I2) $W_x\in\{0,\dots,2^{128}-1\}$	The word `fxpoly_set_small` writes (Definition A.5)
$V\in\mathbb{Z}$	$p_{[k],\mathrm{fx64}}$, $p_{[k+n/2],\mathrm{fx64}}$, integers
Assumption A1	Item 9 of (I1)
Assumption A2	(L1); assumption A1; $B\le 127$ (the statement)
Its conclusion: $x_{\mathrm{fx64}}=V$	

(L2) $\forall x\in X_0:\ W_x=x_{\mathrm{fx64}} \bmod 2^{128}$ [(I1); (I2)]

(L3) $\forall x\in X_0:\ x_{\mathrm{fx64}}=2^{64}(p_{[k]}+ip_{[k+n/2]})$ [(I1)]

(L4) $\forall x\in X_0:\ |x_{\mathrm{fx64}}|\le\sqrt{2}\,B2^{64}$
[(L3); assumption A1; $\forall a,b\in\mathbb{R}:\ |a+ib|^2=a^2+b^2$ (Fact A.41, item 1); Fact A.41, item 5]

(L5) $\Rightarrow\ \forall x\in X_0:\ |x_{\mathrm{fx64}}|\le M_0$ [(L4); M_0 (the statement)]

(L6) $\forall k:\ |\widetilde{\psi}_{k,\mathrm{fx64}}|\le 2^{64}+1$
[[gate: `verify/gates/fx/twiddle_pairs.py`], the 1024 stored pairs of Definition I.1, item 4]

(L7) $\forall x,y\in C_{\mathcal{F}_{\mathrm{fx}}}:\ |(x\otimes y)_{\mathrm{fx64}}-x_{\mathrm{fx64}}y_{\mathrm{fx64}}/2^{64}|\le\sqrt{2}$
[Definition A.8: two products per part; Definition I.1, item 1, at $\times$; $\forall a,b\in\mathbb{R}:\ |a+ib|^2=a^2+b^2$ (Fact A.41, item 1)]

(L8) $\forall x,y\in C_{\mathcal{F}_{\mathrm{fx}}}:\ |(x\otimes y)_{\mathrm{fx64}}|\le|x_{\mathrm{fx64}}||y_{\mathrm{fx64}}|/2^{64}+\sqrt{2}$
[(L7); $|x+y|\le|x|+|y|$, $|xy|=|x||y|$ (Fact A.41, item 1)]

		Lemma I.10, item 1	This proof
		Shared: h	
		$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
15969	(I3)	$h \in \{2, \dots, 10\}$	$h \in \{3, \dots, 10\}$ (the statement)
		each input array of words	The words of X_0 (the statement)
		Assumption A1	$h \in \{3, \dots, 10\}$ (the statement)
		Its conclusion: the object of `fxpoly_FFT` in $\mathcal{O}$ returns the words of lines 2 to 25 of $\widetilde{\text{FFT}}$	
		Lemma I.12, item 1 at each part of every $x \in X_j$, $j \le h-2$, under $[\forall x \in X_j : W_x = x_{\text{fx64}} \bmod 2^{128} \wedge \lvert x_{\text{fx64}}\rvert \le M_j] \wedge M_{j+1} < 2^{127}$	This proof
		Shared: W_x (the scope)	
15970	(I4)	V	x_{fx64} (the scope)
		$W_x \in \{0, \dots, 2^{128}-1\}$	W_x, a word (Definition A.5)
		$V \in \mathbb{Z}$	x_{fx64} (Definition A.5)
		Assumption A1	The scope
		Assumption A2	The scope; M_{j+1} (the statement); $\lvert\text{Re}\, x\rvert, \lvert\text{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
		Its conclusion: $x_{\text{fx64}} = V$	
		Lemma I.12, item 1 at each part of every stored twiddle $\widetilde{s}$ of $\widetilde{\text{FFT}}$, line 19	This proof
		W_x	$W_{\widetilde{s}}$ ($\widetilde{\text{FFT}}$, line 19)
		V	$\widetilde{s}_{\text{fx64}}$ (Definition A.5)
		$W_x \in \{0, \dots, 2^{128}-1\}$	$W_{\widetilde{s}}$, a word of `FXP_GM` (Lemma I.10)
15971	(I5)	$V \in \mathbb{Z}$	$\widetilde{\psi}_k \in 2^{-64}\mathbb{Z}$ $(\text{roundEven}(2^{64}\text{Re}\,\psi_k), \text{roundEven}(2^{64}\text{Im}\,\psi_k) \in \mathbb{Z}$, Definition I.1, item 4); $\widetilde{s}$ ($\widetilde{\text{FFT}}$, line 19)
		Assumption A1	Definition I.1, item 5
		Assumption A2	(L6); $\lvert\text{Re}\, x\rvert, \lvert\text{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
		Its conclusion: $x_{\text{fx64}} = V$	
		Lemma I.12, item 5 at each part of each operation of $\widetilde{\text{FFT}}$, line 19, at every $x \in X_{j+1}$, $j \le h-2$, under $[\forall x \in X_j : W_x = x_{\text{fx64}} \bmod 2^{128} \wedge \lvert x_{\text{fx64}}\rvert \le M_j] \wedge M_{j+1} < 2^{127}$	This proof
		W_x, W_y	$W_{a_{j_2}}, W_{\widetilde{s}}$ at $\otimes$; $W_{a_{j_1}}, W_{a_{j_2}\otimes\widetilde{s}}$ at $\oplus, \ominus$ ($\widetilde{\text{FFT}}$, line 19; Definition A.8)
15972	(I6)	o	mul, sub, add ($\widetilde{\text{FFT}}$, line 19; Definition A.8)
		W_{z_o}	$W_{a_{j_2}\otimes\widetilde{s}}$ at $\otimes$; W_x at $\oplus, \ominus$ ($\widetilde{\text{FFT}}$, line 19; Definition A.8)
		$W_x, W_y \in \{0, \dots, 2^{128}-1\}$	$W_{a_{j_1}}$, $W_{a_{j_2}}$, $W_{a_{j_2}\otimes\widetilde{s}}$, $W_{\widetilde{s}}$, words (Definition A.5)
		$o \in \{\text{add}, \text{sub}, \text{neg}, \text{mul}, \text{div}, \text{half}\}$	$\widetilde{\text{FFT}}$, line 19
		Assumption A4	$o \in \{\text{add}, \text{sub}, \text{mul}\}$ ($\widetilde{\text{FFT}}$, line 19)
		Assumption A5	The scope; (L6), (L8); M_{j+1} (the statement); $\lvert\text{Re}\, x\rvert, \lvert\text{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
		Its conclusion: $z_{o,\text{fx64}} = V_o$	
15973	(L9)	$\forall j \le h-2 : [\forall x \in X_j : W_x = x_{\text{fx64}} \bmod 2^{128} \wedge \lvert x_{\text{fx64}}\rvert \le M_j] \wedge M_{j+1} < 2^{127} \Rightarrow \forall x \in$	
15974		$X_{j+1} : W_x = x_{\text{fx64}} \bmod 2^{128} \wedge \lvert x_{\text{fx64}}\rvert \le M_{j+1}$	

15975 [(I3); (I4); (I5); (I6); (L6), (L8); Definition I.1, item 1; $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \le |x|$ (Fact A.41, item 1); M_{j+1} (the
15976 statement)]

15977 (L10) $\forall j:\ M_{j+1} = cM_j + \sqrt{2}$

15978 [M_{j+1}, c (the statement)]

15979 (L11) $2c - \sqrt{2} \ge 2$

15980 [c (the statement); expand]

15981 (L12) $M_0 + 2 = c^0(M_0 + 2)$

15982 [expand]

15983 (L13) $\forall j:\ M_{j+1} + 2 \le c(M_j + 2)$

15984 [(L10), (L11)]

15985 (L14) $\forall j:\ M_j + 2 \le c^j(M_0 + 2)$

15986 [induction on j: (L12) the base, (L13) the step]

15987 (L15) $\forall j \le h-1:\ M_j \le c^{h-1}(1.4143\, B2^{64} + 2) - 2$

15988 [(L14); M_0, c (the statement); Fact A.41, items 23 and 26; expand]

15989 (L16) $c^{h-1}(1.4143\, B2^{64} + 2) - 2 < 2^{81}$

15990 [expand at $h \le 10$ and $B \le 127$ (the statement)]

15991 (L17) $\Rightarrow\ \forall j \le h-1:\ M_j < 2^{81}$

15992 [(L15), (L16)]

15993 (L18) $\forall j \le h-1\ \forall x \in X_j:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

15994 [induction on j: (L2), (L5) the base; (L9) the step, its premise $M_{j+1} < 2^{127}$ by (L17)]

15995 (L19) $\forall j \le h-1\ \forall x \in X_j:\ |x_{\mathrm{fx64}}| \le M_j$

15996 [induction on j: (L2), (L5) the base; (L9) the step, its premise $M_{j+1} < 2^{127}$ by (L17)]

Lemma I.10, item 10	This proof
Shared: h	
$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
(I7) $h \in \{2, \dots, 10\}$	$h \in \{3, \dots, 10\}$ (the statement)
each input array of words	The words of X_{h-1} (the statement)
Its conclusion: on each of its 2^h input words W_a, the object of `fxpoly_neg` in $\mathcal{O}$ returns $-W_a \bmod 2^{128}$	

15997

Lemma I.12, item 1 at each part of every $x' \in X_{h-1}$	This proof
W_x	$W_{x'}$ (the scope)
V	x'_{fx64} (the scope)
(I8) $W_x \in \{0, \dots, 2^{128} - 1\}$	$W_{x'}$, a word (Definition A.5)
$V \in \mathbb{Z}$	x'_{fx64} (Definition A.5)
Assumption A1	(L18) at $j = h-1$
Assumption A2	(L17); (L19) at $j = h-1$; $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
Its conclusion: $x_{\mathrm{fx64}} = V$	

15998

Lemma I.12, item 5 at each part, at every $x \in X^-$ and the pair $x' \in X_{h-1}$ `fxpoly_neg` writes it on	This proof
W_x	$W_{x'}$ (the scope)
o	neg (the scope)
W_{z_o}	W_x (the scope)
(I9) $W_x \in \{0, \dots, 2^{128} - 1\}$	$W_{x'}$, a word (Definition A.5)
$o \in \{\text{add}, \text{sub}, \text{neg}, \text{mul}, \text{div}, \text{half}\}$	X^- (the statement)
Assumption A4	$o = \text{neg}$ (X^-, the statement)
Assumption A5	(L17); (L19) at $j = h - 1$; $\lvert -z\rvert = \lvert z\rvert$ (Fact A.41, item 1); $\lvert\text{Re}\, x\rvert, \lvert\text{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
Its conclusion: $z_{o,\text{fx64}} = V_o$	

(L20) $\forall x \in X^- :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[(I7); (I8); (I9); $\text{fl}(-x) = -x$ (Definition I.1, item 1)]

(L21) $\forall x \in X^- :\ |x_{\text{fx64}}| \le M_{h-1}$

[(L20); (L19) at $j = h - 1$; $|-z| = |z|$ (Fact A.41, item 1)]

(L22) $\Rightarrow$ item 1

[(L18)]

(L23) $\Rightarrow$ item 2

[(L19)]

(L24) $\Rightarrow$ item 3

[(L20)]

(L25) $\Rightarrow$ item 4

[(L21)]

(L26) $\Rightarrow$ item 5

[(L15)]

(L27) $\Rightarrow$ item 6

[(L16)]

(L28) $\Rightarrow$ item 7

[(L8) at $(x, y) := (v, w)$]

(L29) $c^0(M + 2) - 2 = M$

[expand]

(L30) $\forall j :\ c(c^j(M + 2) - 2) + \sqrt{2} \le c^{j+1}(M + 2) - 2$

[(L11); expand]

(L31) $\forall j \le h - 1 :\ c^j(M + 2) - 2 \le c^{h-1}(M + 2) - 2$

[$c > 1$ (c, the statement); $M \ge 0$ (the statement); Fact A.41, items 23 and 26]

Lemma I.10, item 1	This proof
Shared: h	
$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
(I10) $h \in \{2, \dots, 10\}$	$h \in \{3, \dots, 10\}$ (the statement)
each input array of words	The words of Y_0 (the statement)
Assumption A1	$h \in \{3, \dots, 10\}$ (the statement)
Its conclusion: the object of `fxpoly_FFT` in $\mathcal{O}$ returns the words of lines 2 to 25 of $\widetilde{\text{FFT}}$	

	Lemma I.12, item 1 at each part of every $y \in Y_j$, $j \le h-2$, under $[\forall y \in Y_j :\ W_y = y_{\mathrm{fx64}} \bmod 2^{128} \wedge \lvert y_{\mathrm{fx64}}\rvert \le c^j(M+2)-2] \wedge c^{j+1}(M+2)-2 < 2^{127}$	This proof
(I11)	W_x V $W_x \in \{0,\dots,2^{128}-1\}$ $V \in \mathbb{Z}$	W_y (the scope) y_{fx64} (the scope) W_y, a word (Definition A.5) y_{fx64} (Definition A.5)
	Assumption A1 Assumption A2	The scope The scope; (L30); $c > 1$ (c, the statement); $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
	Its conclusion: $x_{\mathrm{fx64}} = V$	
	Lemma I.12, item 1 at each part of every stored twiddle $\widetilde{s}$ of $\widetilde{\mathrm{FFT}}$, line 19	This proof
(I12)	W_x V $W_x \in \{0,\dots,2^{128}-1\}$ $V \in \mathbb{Z}$	$W_{\widetilde{s}}$ ($\widetilde{\mathrm{FFT}}$, line 19) $\widetilde{s}_{\mathrm{fx64}}$ (Definition A.5) $W_{\widetilde{s}}$, a word of `FXP_GM` (Lemma I.10) $\widetilde{\psi}_k \in 2^{-64}\mathbb{Z}$ $(\mathrm{roundEven}(2^{64}\mathrm{Re}\,\psi_k), \mathrm{roundEven}(2^{64}\mathrm{Im}\,\psi_k) \in \mathbb{Z}$, Definition I.1, item 4); $\widetilde{s}$ ($\widetilde{\mathrm{FFT}}$, line 19)
	Assumption A1 Assumption A2	Definition I.1, item 5 (L6); $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
	Its conclusion: $x_{\mathrm{fx64}} = V$	
	Lemma I.12, item 5 at each part of each operation of $\widetilde{\mathrm{FFT}}$, line 19, at every $y \in Y_{j+1}$, $j \le h-2$, under $[\forall y \in Y_j :\ W_y = y_{\mathrm{fx64}} \bmod 2^{128} \wedge \lvert y_{\mathrm{fx64}}\rvert \le c^j(M+2)-2] \wedge c^{j+1}(M+2)-2 < 2^{127}$	This proof
(I13)	W_x, W_y o W_{z_o} $W_x, W_y \in \{0,\dots,2^{128}-1\}$ $o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	$W_{a_{j_2}}, W_{\widetilde{s}}$ at $\otimes$; $W_{a_{j_1}}, W_{a_{j_2}\otimes\widetilde{s}}$ at $\oplus, \ominus$ ($\widetilde{\mathrm{FFT}}$, line 19; Definition A.8) $\mathrm{mul}, \mathrm{sub}, \mathrm{add}$ ($\widetilde{\mathrm{FFT}}$, line 19; Definition A.8) $W_{a_{j_2}\otimes\widetilde{s}}$ at $\otimes$; W_y at $\oplus, \ominus$ ($\widetilde{\mathrm{FFT}}$, line 19; Definition A.8) $W_{a_{j_1}}, W_{a_{j_2}}, W_{a_{j_2}\otimes\widetilde{s}}, W_{\widetilde{s}}$, words (Definition A.5) $\widetilde{\mathrm{FFT}}$, line 19
	Assumption A4 Assumption A5	$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{mul}\}$ ($\widetilde{\mathrm{FFT}}$, line 19) The scope; (L6), (L8), (L10), (L30); $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
	Its conclusion: $z_{o,\mathrm{fx64}} = V_o$	

(L32) $\forall j \le h-2 :\ [\forall y \in Y_j :\ W_y = y_{\mathrm{fx64}} \bmod 2^{128} \wedge \lvert y_{\mathrm{fx64}}\rvert \le c^j(M+2)-2] \wedge c^{j+1}(M+2)-2 < 2^{127} \Rightarrow\ \forall y \in Y_{j+1} :\ W_y = y_{\mathrm{fx64}} \bmod 2^{128} \wedge \lvert y_{\mathrm{fx64}}\rvert \le c^{j+1}(M+2)-2$
[(I10); (I11); (I12); (I13); (L6), (L8), (L10), (L30); Definition I.1, item 1; $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)]

(L33) $\forall j \le h-1\ \forall y \in Y_j :\ W_y = y_{\mathrm{fx64}} \bmod 2^{128} \wedge \lvert y_{\mathrm{fx64}}\rvert \le c^j(M+2)-2$
[induction on j: assumptions A2 and A3 and (L29) the base; (L32) the step, its premise by (L31) and assumption A4]

(L34) $\Rightarrow$ item 8
[(L33)]

(L35) $\Rightarrow$ item 9

[(L33), (L31)]

□ (items 1 to 9)

Lemma I.35 (No overflow in the Gram matrix [to table])**.** *The Gram's words hold their values when the basis pairs' moduli stay below* 2^{81}*. Let:*

- $\forall j,k \in \{0,1\}:\ b_{jk}$ *be arrays of pairs of words* ffSampling$^{\mathcal{F}}$ *(Algorithm 10), line 1, writes, or the same without the negations (*keychecks *(Algorithm 12));*
- $\forall j \in \{0,1\}:\ M_j \geq 0$*;*
- W_x *be a word of lines 2 to 18 of* Gram *(Algorithm 13) on the* b_{jk}*.*

Define:

- $\forall j \in \{0,1\}:\ Y_j$*, the numbers of the pairs of* b_{j0} *and* b_{j1}*;*
- x*, the number the line of* W_x *computes in* $\mathcal{F}_{\text{fx}}$*;*
- $\widetilde{g}_{00}$*,* $\widetilde{g}_{01}$ *and* $\widetilde{g}_{11}$*, the values lines 2 to 18 of* Gram *compute on the* b_{jk} *in* $\mathcal{F}_{\text{fx}}$*;*
- $p_0 := b_{00} \otimes \text{conj}(b_{10})$ *and* $p_1 := b_{01} \otimes \text{conj}(b_{11})$*, the two products line 12 adds.*

Assume:

(A1) $\forall \mathfrak{p} \in \{\text{Re},\text{Im}\}\ \forall j \in \{0,1\}\ \forall y \in Y_j:\ W_{\mathfrak{p}(y)} = \mathfrak{p}(y)_{\text{fx64}} \bmod 2^{128}$*;*

(A2) $\forall j \in \{0,1\}\ \forall y \in Y_j:\ |y_{\text{fx64}}| \leq M_j$*;*

(A3) $M_0, M_1 < 2^{81}$*.*

Then

1. $W_x = x_{\text{fx64}} \bmod 2^{128}$*;*
2. $|\widetilde{g}_{00,\text{fx64}}| \leq 4(M_0^2/2^{64} + 1/2)$*;*
3. $|\widetilde{g}_{11,\text{fx64}}| \leq 4(M_1^2/2^{64} + 1/2)$*;*
4. $|\widetilde{g}_{01,\text{fx64}}| \leq 2M_0M_1/2^{64} + 2\sqrt{2}$*;*
5. $4(M_0^2/2^{64} + 1/2),\ 4(M_1^2/2^{64} + 1/2),\ 2M_0M_1/2^{64} + 2\sqrt{2} < 2^{101}$*;*
6. $|x_{\text{fx64}}| < 2^{127}$*.*

Proof. (L1) $|b_{jk,r,\text{fx64}}|,\ |b_{jk,i,\text{fx64}}| \leq |b_{jk,\text{fx64}}|$

[$|\text{Re}\, x|, |\text{Im}\, x| \leq |x|$ (Fact A.41, item 1)]

(L2) $|b_{jk,\text{fx64}}| \leq M_j$

[assumption A2]

(L3) $\Rightarrow\ |b_{jk,r,\text{fx64}}|,\ |b_{jk,i,\text{fx64}}| \leq M_j$

[(L1), (L2)]

(L4) $\widetilde{g}_{00,\text{fx64}} = \sum_{x \in \{b_{00,r}, b_{00,i}, b_{01,r}, b_{01,i}\}} \text{roundAway}(x_{\text{fx64}}^2, 2^{64})$

[Gram (Algorithm 13), lines 2 to 18; Definition I.1, item 1, at $\times$ and at $+$]

(L5) $\widetilde{g}_{11,\text{fx64}} = \sum_{x \in \{b_{10,r}, b_{10,i}, b_{11,r}, b_{11,i}\}} \text{roundAway}(x_{\text{fx64}}^2, 2^{64})$

[Gram (Algorithm 13), lines 2 to 18; Definition I.1, item 1, at $\times$ and at $+$]

	Lemma I.12, items 1, 2 and 5 at the word $W_{\mathfrak{p}(y)}$ of each part of every $y \in Y_0 \cup Y_1$, at $W_y := W_x$ and at $o := \text{neg}$	This proof
(I1)	W_x, W_y	$W_{\mathfrak{p}(y)}, W_{\mathfrak{p}(y)}$ (the scope)
	V	$\mathfrak{p}(y)_{\text{fx64}}$ (the scope)
	o	neg (the scope)
	$W_x, W_y \in \{0, \dots, 2^{128}-1\}$	$W_{\mathfrak{p}(y)}$, a word (Definition A.5)
	$V \in \mathbb{Z}$	$\mathfrak{p}(y)_{\text{fx64}}$ (Definition A.5)
	$o \in \{\text{add}, \text{sub}, \text{neg}, \text{mul}, \text{div}, \text{half}\}$	The scope
	Assumption A1	Assumption A1
	Assumption A2	(L3); assumption A3
	Assumption A4	$o = \text{neg}$ (the scope)
	Assumption A5	(L3); assumption A3
	Its item 1: $x_{\text{fx64}} = V$	
	Its item 2: $\lvert\text{roundAway}(x_{\text{fx64}} y_{\text{fx64}}, 2^{64})\rvert \le \lvert x_{\text{fx64}}\rvert\lvert y_{\text{fx64}}\rvert/2^{64} + 1/2$	
	Its item 5: $z_{o,\text{fx64}} = V_o$	

(L6) $|\widetilde{g}_{00,\text{fx64}}| \le 4(M_0^2/2^{64} + 1/2)$

[(L3) at $j = 0$, (L4); items 1 and 2 of (I1)]

(L7) $|\widetilde{g}_{11,\text{fx64}}| \le 4(M_1^2/2^{64} + 1/2)$

[(L3) at $j = 1$, (L5); items 1 and 2 of (I1)]

(L8) $4(M_0^2/2^{64} + 1/2),\ 4(M_1^2/2^{64} + 1/2) < 2^{127}$

[$M_0, M_1 < 2^{81}$ (assumption A3)]

(L9) $\Rightarrow\ |\widetilde{g}_{00,\text{fx64}}|,\ |\widetilde{g}_{11,\text{fx64}}| < 2^{127}$

[(L6), (L7), (L8)]

(L10) $(0 - b_{10,i})_{\text{fx64}} = -b_{10,i,\text{fx64}}$

[items 1 and 5 of (I1)]

(L11) $(0 - b_{11,i})_{\text{fx64}} = -b_{11,i,\text{fx64}}$

[items 1 and 5 of (I1)]

(L12) $|(b_{10,r,\text{fx64}}, -b_{10,i,\text{fx64}})| = |b_{10,\text{fx64}}|$

[(L10); $|\text{conj}\, z| = |z|$ (Fact A.41, item 1)]

(L13) $|(b_{11,r,\text{fx64}}, -b_{11,i,\text{fx64}})| = |b_{11,\text{fx64}}|$

[(L11); $|\text{conj}\, z| = |z|$ (Fact A.41, item 1)]

(L14) $\widetilde{g}_{01,\text{fx64}} = p_{0,\text{fx64}} + p_{1,\text{fx64}}$

[$\widetilde{g}_{01}$, p_0, p_1 (the statement); Gram (Algorithm 13), line 12; Definition A.8; Definition I.1, item 1]

	Lemma I.34, item 7	This proof
(I2)	v, w	$b_{00}, \text{conj}(b_{10})$
	$v, w \in C_{\mathcal{F}_{\text{fx}}}$	The pairs of the b_{jk} (the statement)
	Its item 7: $\lvert(v \otimes w)_{\text{fx64}}\rvert \le \lvert v_{\text{fx64}}\rvert\lvert w_{\text{fx64}}\rvert/2^{64} + \sqrt{2}$	

(L15) $|p_{0,\text{fx64}}| \le M_0 M_1/2^{64} + \sqrt{2}$

[(I2); (L2), (L12); Fact A.41, item 8]

	Lemma I.34, item 7	This proof
(I3)	v, w	$b_{01}, \text{conj}(b_{11})$
	$v, w \in C_{\mathcal{F}_{\text{fx}}}$	The pairs of the b_{jk} (the statement)
	Its item 7: $\lvert(v \otimes w)_{\text{fx64}}\rvert \le \lvert v_{\text{fx64}}\rvert\lvert w_{\text{fx64}}\rvert/2^{64} + \sqrt{2}$	

(L16) $|p_{1,\text{fx64}}| \le M_0 M_1/2^{64} + \sqrt{2}$

[(I3); (L2), (L13); Fact A.41, item 8]

(L17) $|\widetilde{g}_{01,\text{fx64}}| \le |p_{0,\text{fx64}}| + |p_{1,\text{fx64}}|$

[(L14); $|x+y| \le |x| + |y|$ (Fact A.41, item 1)]

(L18) $\Rightarrow$ $|\widetilde{g}_{01,\mathrm{fx64}}| \le 2M_0M_1/2^{64} + 2\sqrt{2}$

[(L15), (L16), (L17)]

(L19) $M_0M_1 \le 2^{162}$

[$M_j \ge 0$ (the statement); $M_0, M_1 < 2^{81}$ (assumption A3); Fact A.41, item 8]

(L20) $2(M_0M_1/2^{64} + \sqrt{2}) < 2^{127}$

[(L19); expand]

(L21) $\Rightarrow$ $|\widetilde{g}_{01,\mathrm{fx64}}| < 2^{127}$

[(L18), (L20)]

Lemma I.12, item 5 at each word of lines 2 to 18	This proof
W_{z_o}	W_x (the scope)
$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	The operation computing W_x (Gram, lines 2 to 18)
(I4) $W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	The words of that operation's arguments (Definition A.5)
Assumption A4	$o \ne \mathrm{div}$ (Gram, lines 2 to 18)
Assumption A5	(L3), (L9), (L21)
Its conclusion: $z_{o,\mathrm{fx64}} = V_o$	

(L22) $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[Lemma I.10, item 11; (I4); assumption A1; Definition I.1, item 1]

(L23) $4(M_0^2/2^{64} + 1/2) < 2^{100} + 2$

[$M_0^2/2^{64} < 2^{98}$ ($M_0, M_1 < 2^{81}$, assumption A3)]

(L24) $4(M_1^2/2^{64} + 1/2) < 2^{100} + 2$

[$M_1^2/2^{64} < 2^{98}$ ($M_0, M_1 < 2^{81}$, assumption A3)]

(L25) $2M_0M_1/2^{64} + 2\sqrt{2} < 2^{99} + 3$

[(L19); $\sqrt{2} < 1.4143$]

(L26) $2^{100} + 2,\ 2^{99} + 3 < 2^{101}$

[expand]

(L27) $\forall j, k \in \{0, 1\}\ \forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\} :\ |\mathrm{fl}(\mathfrak{p}(b_{jk})^2)_{\mathrm{fx64}}| \le M_j^2/2^{64} + 1/2$

[(L3); items 1 and 2 of (I1); Definition I.1, item 1, at $\times$]

(L28) $\forall j \in \{0, \dots, 3\} :\ |\widetilde{s}_{j,\mathrm{fx64}}| \le 2(M_{\lfloor j/2 \rfloor}^2/2^{64} + 1/2)$

[(L27); Gram (Algorithm 13), lines 2 to 18; Definition I.1, item 1, at $+$; $|x+y| \le |x| + |y|$ (Fact A.41, item 1)]

(L29) $\forall (y, y') \in \{(b_{00}, \mathrm{conj}(b_{10})), (b_{01}, \mathrm{conj}(b_{11}))\}\ \forall \mathfrak{p}, \mathfrak{p}' \in \{\mathrm{Re}, \mathrm{Im}\} :\ |\mathrm{fl}(\mathfrak{p}(y)\,\mathfrak{p}'(y'))_{\mathrm{fx64}}| \le M_0M_1/2^{64} + 1/2$

[(L3), (L10), (L11); Definition I.1, item 1, at $\times$; roundAway (Definition I.1); Fact A.41, items 22 and 8]

(L30) $M_0^2/2^{64} + 1/2,\ M_1^2/2^{64} + 1/2,\ M_0M_1/2^{64} + 1/2 < 2^{126}$

[assumption A3; (L19); expand]

(L31) $|x_{\mathrm{fx64}}| < 2^{127}$

[(L3), (L9), (L10), (L11), (L15), (L16), (L20), (L21), (L27), (L28), (L29), (L30); assumption A3; $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \le |x|$ (Fact A.41, item 1); Gram (Algorithm 13), lines 2 to 18]

(L32) $\Rightarrow$ item 1

[(L22)]

(L33) $\Rightarrow$ item 2

[(L6)]

(L34) $\Rightarrow$ item 3

[(L7)]

(L35) $\Rightarrow$ item 4

[(L18)]

(L36) $\Rightarrow$ item 5

[(L23), (L24), (L25), (L26)]

(L37) $\Rightarrow$ item 6

[(L31)]

$\square$ (items 1 to 6)

Lemma I.36 (No overflow in the key check's operands [to table])**.** *The key check's images, Gram, squared moduli and num_ψ do not overflow. Define:*

- $\Psi_n := \{\psi_k : k < n/2\}$*, that of Fact A.43 at* $m := n$*.*

Let:

- (f, g, F, G) *be a key (line 3 of* keygen *(Algorithm 11)) of degree* $n = 2^h \in \{512, 1024\}$*;*
- $\psi \in \Psi_n$*.*

Define:

- $\widetilde{g}_{01}$*, the Gram's entry* keychecks *computes, line 3;*
- num_ψ*, the number* keychecks *computes from* $\widetilde{g}_{01}(\psi)$*, line 10;*
- $\widetilde{\hat{p}}$*, the value* keychecks *computes in place of* $p(\psi)$*,* $p \in \{f, g, F, G\}$*, line 1;*
- $\widetilde{sq}_{\hat{p}} := \mathrm{fl}(\widetilde{\hat{p}}_r^2) + \mathrm{fl}(\widetilde{\hat{p}}_i^2)$ *(lines 5 and 9).*

Let:

- W_x *be a word of* keychecks *(Algorithm 12), lines 1 to 10 [L0: fxp/kgen_fx.c:60-90], one of:*
  - *The images* $\widetilde{\hat{p}}$*;*
  - *The squared moduli* $\widetilde{sq}_{\hat{p}}$*;*
  - *The Gram's entries;*
  - num_ψ*;*

Define:

- $B_{fg} := \begin{cases} 31 & n = 512 \\ 15 & n = 1024 \end{cases}$ *[L0: kgen_gauss.c:14-16] [L0: kgen_gauss.c:8-11] [L0: kgen_gauss.c:52-61];*
- x*, the number* W_x*'s line computes in* $\mathcal{F}_{\mathrm{fx}}$ *(Definition I.1);*
- $x_{\mathrm{fx64}} := 2^{64}x$ *(Definition A.5);*
- $M_{fg} := M_{h-1}$ *(Lemma I.34 at* $B := B_{fg}$*);*
- $M_{FG} := M_{h-1}$ *(Lemma I.34 at* $B := 127$*).*

Assume:

(A1) $\forall a < n:\ f_{[a]}, g_{[a]} \in [-B_{fg}, B_{fg}]$ *[L0: fxp/sign_fxcore.c:128-141];*

(A2) $\forall a < n:\ F_{[a]}, G_{[a]} \in [-127, 127]$ *[L0: kgen_ntru.c:1887-1895].*

Then

1. $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$*;*
2. $num_\psi < 2^{62}$*;*
3. $\forall \widetilde{\hat{p}}:\ \widetilde{sq}_{\hat{p}} < 2^{33}$*;*
4. $|x_{\mathrm{fx64}}| < 2^{127}$*.*

Proof.

DEFINES $\hat{P}_{fg}$, $\hat{P}_{FG}$: the images $\widetilde{\hat{p}}$ of f, g and of F, G

DEFINES $\mathcal{G}$: the numbers of the Gram's words, line 3

DEFINES $\forall j \le h - 1\ \forall B \in [0, 127]:\ M_j(B)$, the M_j of Lemma I.34 at B

	Lemma I.34 at $j := h-1$	This proof
	Shared: h	
	p	$p \in \{f, g\}$ (the statement)
	B	B_{fg} (the statement)
	W_x	$W_{\widetilde{\hat{p}}}$, $\widetilde{\hat{p}} \in \hat{P}_{fg}$ (keychecks, line 1)
	X_{h-1}	$\hat{P}_{fg}$ (the proof's block)
	M_{h-1}	M_{fg} (the statement)
(I1)	$h \in \{3, \dots, 10\}$	$n \in \{512, 1024\}$ (the statement)
	$p \in \{-128, \dots, 127\}^{2^h}$	Assumption A1; $B \le 127$ (B, the rows above)
	$B \in [0, 127]$	B_{fg} (the statement)
	W_x pair of words at stage j	$\widetilde{\hat{f}}$, $\widetilde{\hat{g}}$ (keychecks (Algorithm 12), line 1)
	Assumption A1	Assumption A1
	Its item 1: $\forall j \le h-1\ \forall x \in X_j :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 2: $\forall j \le h-1\ \forall x \in X_j :\ \lvert x_{\text{fx64}}\rvert \le M_j$	

	Lemma I.34 at $j := h-1$	This proof
	Shared: h	
	p	$p \in \{F, G\}$ (the statement)
	B	127
	W_x	$W_{\widetilde{\hat{p}}}$, $\widetilde{\hat{p}} \in \hat{P}_{FG}$ (keychecks, line 1)
	X_{h-1}	$\hat{P}_{FG}$ (the proof's block)
	M_{h-1}	M_{FG} (the statement)
	$h \in \{3, \dots, 10\}$	$n \in \{512, 1024\}$ (the statement)
(I2)	$p \in \{-128, \dots, 127\}^{2^h}$	Assumption A2; $B \le 127$ (B, the rows above)
	$B \in [0, 127]$	127
	W_x pair of words at stage j	$\widetilde{\hat{F}}$, $\widetilde{\hat{G}}$ (keychecks (Algorithm 12), line 1)
	Assumption A1	Assumption A2
	Its item 1: $\forall j \le h-1\ \forall x \in X_j :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 2: $\forall j \le h-1\ \forall x \in X_j :\ \lvert x_{\text{fx64}}\rvert \le M_j$	
	Its item 5: $\forall j \le h-1 :\ M_j \le c^{h-1}(1.4143\, B2^{64} + 2) - 2$	
	Its item 6: $c^{h-1}(1.4143\, B2^{64} + 2) - 2 < 2^{81}$	

(L1) $\forall \widetilde{\hat{p}} \in \hat{P}_{fg} \cup \hat{P}_{FG} :\ W_{\widetilde{\hat{p}}} = \widetilde{\hat{p}}_{\text{fx64}} \bmod 2^{128}$

[item 1 of (I1); item 1 of (I2)]

(L2) $\forall \widetilde{\hat{p}} \in \hat{P}_{fg} :\ \lvert\widetilde{\hat{p}}_{\text{fx64}}\rvert \le M_{fg}$

[item 2 of (I1); M_{fg} (the statement)]

(L3) $\forall \widetilde{\hat{p}} \in \hat{P}_{FG} :\ \lvert\widetilde{\hat{p}}_{\text{fx64}}\rvert \le M_{FG}$

[item 2 of (I2); M_{FG} (the statement)]

(L4) $M_0(B_{fg}) \le M_0(127)$

[$M_j(B)$ (the proof's block); M_0 (Lemma I.34); B_{fg} (the statement); Fact A.41, item 26]

(L5) $\forall j \le h-2 :\ M_j(B_{fg}) \le M_j(127) \Rightarrow\ M_{j+1}(B_{fg}) \le M_{j+1}(127)$

[$M_j(B)$ (the proof's block); M_{j+1} (Lemma I.34); Fact A.41, item 26]

(L6) $\forall j \le h-1 :\ M_j(B_{fg}) \le M_j(127)$

[induction on j: (L4) the base, (L5) the step]

(L7) $M_{fg} \le M_{FG}$

[(L6) at $j := h-1$; M_{fg}, M_{FG} (the statement)]

(L8) $M_{FG} < 2^{81}$

[items 5 and 6 of (I2)]

Lemma I.35 the key generation's form	This proof
$(b_{00}, b_{01}, b_{10}, b_{11})$	$(\widetilde{\hat{g}}, \widetilde{\hat{f}}, \widetilde{\hat{G}}, \widetilde{\hat{F}})$ (keychecks, line 1)
Y_0, Y_1	$\hat{P}_{fg}, \hat{P}_{FG}$ (the proof's block)
M_0, M_1	M_{fg}, M_{FG} (the statement)
W_x	$W_x,\ x \in \mathcal{G}$ (the proof's block)
b_{jk} arrays of pairs of words of ffSampling$^{\mathcal{F}}$, line 1, or the same without the negations	keychecks (Algorithm 12), lines 1 and 3
(I3) $M_0, M_1 \geq 0$	M_{fg}, M_{FG} (the statement)
W_x a word of Gram on the b_{jk}	$\mathcal{G}$ (the proof's block)
Assumption A1	(L1)
Assumption A2	(L2), (L3)
Assumption A3	(L7), (L8)
Its item 1: $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 4: $\lvert\widetilde{g}_{01,\mathrm{fx64}}\rvert \leq 2M_0M_1/2^{64} + 2\sqrt{2}$	
Its item 6: $\lvert x_{\mathrm{fx64}}\rvert < 2^{127}$	

(L9) $\forall x \in \mathcal{G}:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[item 1 of (I3)]

(L10) $\lvert\widetilde{g}_{01,\mathrm{fx64}}\rvert \leq 2M_{fg}M_{FG}/2^{64} + 2\sqrt{2}$

[item 4 of (I3)]

(L11) $2M_{fg}M_{FG}/2^{64} + 2\sqrt{2} < 2^{95}$

[M_{fg}, M_{FG} (the statement); expand at $h \leq 10$]

(L12) $\Rightarrow\ \lvert\widetilde{g}_{01,\mathrm{fx64}}\rvert < 2^{95}$

[(L10), (L11)]

(L13) $num_{\psi,\mathrm{fx64}} \leq \lvert\widetilde{g}_{01,\mathrm{fx64}}\rvert^2/2^{64} + 1$

[line 10 of keychecks; Definition I.1, item 1, at $\times$ twice and at $+$; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1); $\forall a, b \in \mathbb{R}:\ \lvert a + ib\rvert^2 = a^2 + b^2$ (Fact A.41, item 1)]

(L14) $\Rightarrow\ num_{\psi,\mathrm{fx64}} < 2^{126}$

[(L12), (L13)]

(L15) $\widetilde{sq}_{\hat{p},\mathrm{fx64}} \leq M_{FG}^2/2^{64} + 1$

[$\widetilde{sq}_{\hat{p}}$ (the statement); Definition I.1, item 1, at $\times$ twice and at $+$; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1); $\forall a, b \in \mathbb{R}:\ \lvert a + ib\rvert^2 = a^2 + b^2$ (Fact A.41, item 1); (L2), (L3), (L7); Fact A.41, item 5]

(L16) $M_{FG}^2/2^{64} + 1 < 2^{97}$

[M_{FG} (the statement); expand at $h \leq 10$]

(L17) $\Rightarrow\ \widetilde{sq}_{\hat{p},\mathrm{fx64}} < 2^{97}$

[(L15), (L16)]

	Lemma I.12, items 1 and 5 at each operation of line 10 on $v := \widetilde{g}_{01}(\psi)$ and of lines 5 and 9 on each $v := \widetilde{\hat{p}}$, $\mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\}$	This proof
	W_x, W_y	$W_{\mathfrak{p}(v)}, W_{\mathfrak{p}(v)}$ at mul; $W_{\mathrm{fl}(v_r^2)}, W_{\mathrm{fl}(v_i^2)}$ at add (the scope)
	V	$\mathfrak{p}(v)_{\mathrm{fx64}}$ (the scope)
	o	mul, add (the scope)
	W_{z_o}	$W_{\mathrm{fl}(\mathfrak{p}(v)^2)}$ at mul; $W_{num_\psi}, W_{\widetilde{sq}_{\hat{p}}}$ at add (the scope)
	$W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	Words (Definition A.5)
(I4)	$V \in \mathbb{Z}$	$\mathfrak{p}(v)_{\mathrm{fx64}}$ (Definition A.5)
	$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	The scope
	Assumption A1	(L9) at $v := \widetilde{g}_{01}(\psi)$; (L1) at $v := \widetilde{\hat{p}}$
	Assumption A2	(L12) at $v := \widetilde{g}_{01}(\psi)$; (L2), (L3), (L7), (L8) at $v := \widetilde{\hat{p}}$; $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
	Assumption A4	$o \neq \mathrm{div}$ (the scope)
	Assumption A5	(L12), (L14) at $v := \widetilde{g}_{01}(\psi)$; (L17) at $v := \widetilde{\hat{p}}$
	Its item 1: $x_{\mathrm{fx64}} = V$	
	Its item 5: $z_{o,\mathrm{fx64}} = V_o$	

(L18) $W_{num_\psi} = num_{\psi,\mathrm{fx64}} \bmod 2^{128}$

[(I4); Definition I.1, item 1, at $\times$ and at $+$]

(L19) $\forall \widetilde{\hat{p}}: \; W_{\widetilde{sq}_{\hat{p}}} = \widetilde{sq}_{\hat{p},\mathrm{fx64}} \bmod 2^{128}$

[(I4); Definition I.1, item 1, at $\times$ and at $+$]

(L20) $\Rightarrow$ item 1

[(L1), (L9), (L18), (L19)]

(L21) $num_\psi < 2^{62}$

[(L14); $x = x_{\mathrm{fx64}} 2^{-64}$ (Definition A.5)]

(L22) $\Rightarrow$ item 2

[(L21)]

(L23) $\widetilde{sq}_{\hat{p}} < 2^{33}$

[(L17); $x = x_{\mathrm{fx64}} 2^{-64}$ (Definition A.5)]

(L24) $\Rightarrow$ item 3

[(L23)]

(L25) $\lvert x_{\mathrm{fx64}}\rvert < 2^{127}$

[(L2), (L3), (L7), (L8) at the images; item 6 of (I3) at the Gram's entries; (L17) at $\widetilde{sq}_{\hat{p}}$; (L14) at num_ψ; x (the statement)]

(L26) $\Rightarrow$ item 4

[(L25)]

□ (items 1 to 4)

Lemma I.37 (The key check's divisors [to table])**.** *The key check's divisors are positive and do not overflow. Define:*

- $\Psi_n := \{\psi_k : k < n/2\}$, *that of Fact A.43 at* $m := n$.

Let:

- (f, g, F, G) *be a key (line 3 of* keygen *(Algorithm 11)) of degree* $n = 2^h \in \{512, 1024\}$;
- $\psi \in \Psi_n$.

Define:

- $B_{fg} := \begin{cases} 31 & n = 512 \\ 15 & n = 1024 \end{cases}$ *[L0: kg en_g au ss . c : 14 -16] [L0: kg en_g au ss . c : 8-11] [L0: kg en_g au ss . c : 52-61];*

- $\widetilde{g}_{00}$, *the Gram's entry* keychecks *computes, line 3;*
- *lo, that of* keychecks*, line 6;*
- W_x, *the word of* $\mathrm{fl}(\widetilde{g}_{00}(\psi)^2)$, *line 11* [LO: fxp/kgen_fx.c:91];
- x, *the number* W_x*'s line computes in* $\mathcal{F}_{\mathrm{fx}}$ *(Definition I.1);*
- $x_{\mathrm{fx64}} := 2^{64}x$ *(Definition A.5);*
- $M_{fg} := M_{h-1}$ *(Lemma I.34 at* $B := B_{fg}$*).*

Assume:

(A1) $\forall a < n:\ f_{[a]}, g_{[a]} \in [-B_{fg}, B_{fg}]$ [LO: fxp/sign_fxcore.c:128-141];

(A2) $\forall a < n:\ F_{[a]}, G_{[a]} \in [-127, 127]$ [LO: kgen_natru.c:1887-1895].

Then

1. $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$;
2. $\mathrm{fl}(\widetilde{g}_{00}(\psi)^2) \in (0, 2^{62})$;
3. $lo > 0$.

Proof.

DEFINES M_{FG}: the M_{h-1} of Lemma I.34 at $B := 127$

(L1) $\mathrm{fl}(\widetilde{g}_{00}(\psi)^2) \geq \widetilde{g}_{00}(\psi)^2 - 2^{-65}$

[Definition I.1, item 1, at $\times$; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1)]

Lemma H.16, item 1 at every $\psi' \in \Psi_n$	This proof
Shared: $(f, g, F, G), n,\ B_{fg}, \widetilde{g}_{00}$ Shared: assumptions A1, A2	
(I1) ψ	ψ' (the proof's block)
$n \in \{512, 1024\}$	The statement
(f, g, F, G) key of degree n	The statement
Its conclusion: $\widetilde{g}_{00} > 2^{-8}$	

(L2) $\forall \psi' \in \Psi_n:\ \widetilde{g}_{00}(\psi') > 2^{-8}$

[(I1)]

(L3) $\widetilde{g}_{00}(\psi)^2 - 2^{-65} > 0$

[(L2) at $\psi' := \psi$; Fact A.41, item 5; expand]

(L4) $\Rightarrow\ \mathrm{fl}(\widetilde{g}_{00}(\psi)^2) > 0$

[(L1), (L3)]

Lemma I.34 at $j := h - 1$	This proof
Shared: h	
p	$p \in \{f, g\}$ (the statement)
B	B_{fg} (the statement)
W_x	$W_{\widetilde{p}(\psi)}$, $\widetilde{p} \in \{\widetilde{f}, \widetilde{g}\}$ (keychecks, line 1)
X_{h-1}	$\{\widetilde{f}(\psi'), \widetilde{g}(\psi')\}_{\psi' \in \Psi_n}$ (keychecks, line 1)
M_{h-1}	M_{fg} (the statement)
$h \in \{3, \ldots, 10\}$	$n \in \{512, 1024\}$ (the statement)
(I2) $p \in \{-128, \ldots, 127\}^{2^h}$	Assumption A1; $B \leq 127$ (B, the rows above)
$B \in [0, 127]$	B_{fg} (the statement)
W_x pair of words at stage j	$\widetilde{f}$, $\widetilde{g}$ (keychecks (Algorithm 12), line 1)
Assumption A1	Assumption A1
Its item 1: $\forall j \leq h-1\ \forall x \in X_j:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 2: $\forall j \leq h-1\ \forall x \in X_j:\ \lvert x_{\mathrm{fx64}} \rvert \leq M_j$	
Its item 5: $\forall j \leq h-1:\ M_j \leq c^{h-1}(1.4143\, B 2^{64} + 2) - 2$	
Its item 6: $c^{h-1}(1.4143\, B 2^{64} + 2) - 2 < 2^{81}$	

(L5) $\forall \widetilde{\widehat{p}} \in \{\widetilde{\widehat{f}}, \widetilde{\widehat{g}}\} : \ |\widetilde{\widehat{p}}_{\mathrm{fx64}}(\psi)| \le M_{fg}$

[item 2 of (I2)]

(L6) $\forall \widetilde{\widehat{p}} \in \{\widetilde{\widehat{f}}, \widetilde{\widehat{g}}\} : \ W_{\widetilde{\widehat{p}}(\psi)} = \widetilde{\widehat{p}}_{\mathrm{fx64}}(\psi) \bmod 2^{128}$

[item 1 of (I2)]

(L7) $M_{fg} < 2^{81}$

[items 5 and 6 of (I2)]

Lemma I.34 at $j := h-1$	This proof
Shared: h	
p	$p \in \{F, G\}$ (the statement)
B	127 (the statement)
W_x	$W_{\widetilde{\widehat{p}}(\psi)}$, $\widetilde{\widehat{p}} \in \{\widetilde{\widehat{F}}, \widetilde{\widehat{G}}\}$ (keychecks, line 1)
X_{h-1}	$\{\widetilde{\widehat{F}}(\psi'), \widetilde{\widehat{G}}(\psi')\}_{\psi' \in \Psi_n}$ (keychecks, line 1)
M_{h-1}	M_{FG} (the proof's block)
$h \in \{3, \dots, 10\}$	$n \in \{512, 1024\}$ (the statement)
(I3) $p \in \{-128, \dots, 127\}^{2^h}$	Assumption A2; $B \le 127$ (B, the rows above)
$B \in [0, 127]$	127
W_x pair of words at stage j	$\widetilde{\widehat{F}}$, $\widetilde{\widehat{G}}$ (keychecks (Algorithm 12), line 1)
Assumption A1	Assumption A2
Its item 1: $\forall j \le h-1 \ \forall x \in X_j : \ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 2: $\forall j \le h-1 \ \forall x \in X_j : \ \lvert x_{\mathrm{fx64}} \rvert \le M_j$	
Its item 5: $\forall j \le h-1 : \ M_j \le c^{h-1}(1.4143\, B 2^{64} + 2) - 2$	
Its item 6: $c^{h-1}(1.4143\, B 2^{64} + 2) - 2 < 2^{81}$	

(L8) $\forall \widetilde{\widehat{p}} \in \{\widetilde{\widehat{F}}, \widetilde{\widehat{G}}\} : \ W_{\widetilde{\widehat{p}}(\psi)} = \widetilde{\widehat{p}}_{\mathrm{fx64}}(\psi) \bmod 2^{128}$

[item 1 of (I3)]

(L9) $\forall \widetilde{\widehat{p}} \in \{\widetilde{\widehat{F}}, \widetilde{\widehat{G}}\} : \ |\widetilde{\widehat{p}}_{\mathrm{fx64}}(\psi)| \le M_{FG}$

[item 2 of (I3)]

(L10) $M_{FG} < 2^{81}$

[items 5 and 6 of (I3)]

Lemma I.35, items 1, 2 and 5 at every $\psi' \in \Psi_n$	This proof
$b_{00}, b_{01}, b_{10}, b_{11}$	$\widetilde{\widehat{g}}, \widetilde{\widehat{f}}, \widetilde{\widehat{G}}, \widetilde{\widehat{F}}$ (keychecks, line 1)
Y_0, Y_1	$\{\widetilde{\widehat{g}}(\psi'), \widetilde{\widehat{f}}(\psi')\}, \{\widetilde{\widehat{G}}(\psi'), \widetilde{\widehat{F}}(\psi')\}$ (keychecks, line 1)
M_0, M_1	M_{fg}, M_{FG} (the statement; the proof's block)
W_x	$W_{\widetilde{g}_{00}(\psi')}$ (keychecks, line 3)
b_{jk} arrays of pairs of words without the negations	$\widetilde{\widehat{g}}$, $\widetilde{\widehat{f}}$, $\widetilde{\widehat{G}}$, $\widetilde{\widehat{F}}$ (keychecks, line 1)
(I4) $M_0, M_1 \ge 0$	M_{fg}, M_{FG} (the statement; the proof's block)
W_x a word of Gram on the b_{jk}	$\widetilde{g}_{00}$ (keychecks, line 3)
Assumption A1	(L6), (L8) at $\psi := \psi'$
Assumption A2	(L5), (L9) at $\psi := \psi'$
Assumption A3	(L7), (L10)
Its item 1: $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 2: $\lvert \widetilde{g}_{00,\mathrm{fx64}} \rvert \le 4(M_0^2/2^{64} + 1/2)$	
Its item 5: $4(M_0^2/2^{64} + 1/2) < 2^{101}$	

		Lemma I.8, item 3 at each step of line 6 of keychecks, on two values of $\widetilde{g}_{00}$ at $\psi', \psi'' \in \Psi_n$	This proof
		x, y	$\widetilde{g}_{00}(\psi'), \widetilde{g}_{00}(\psi'')$ (keychecks, line 6)
16289	(I5)	$x, y \in 2^{-64}\mathbb{Z},\ x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$	Items 2 and 5 of (I4); $\mathcal{F}_{\text{fx}}$ (Definition I.1)
		Assumption A1	Items 2 and 5 of (I4); $\lvert x-y\rvert \le \lvert x\rvert + \lvert y\rvert$ (Fact A.41, item 1)
		Its item 3: $z = \min(x, y)$	
16290	(L11)	$lo > 0$	
16291			[(L2); (I5); lo (keychecks, line 6)]
16292	(L12)	$\Rightarrow$ item 3	
16293			[(L11)]
16294	(L13)	$\widetilde{g}_{00,\text{fx64}} \le 4(M_{fg}^2/2^{64} + 1/2)$	
16295			[item 2 of (I4) at $\psi' := \psi$; $\widetilde{g}_{00}(\psi) > 0$ ((L2) at $\psi' := \psi$)]
16296	(L14)	$\text{fl}(\widetilde{g}_{00}(\psi)^2) \le \widetilde{g}_{00}(\psi)^2 + 2^{-65}$	
16297			[Definition I.1, item 1, at $\times$; $\zeta_{\text{op}} := 2^{-65}$ (Definition I.1)]
16298	(L15)	$\widetilde{g}_{00}(\psi)^2 + 2^{-65} < 2^{62}$	
16299			[(L13); item 5 of (I2); $\widetilde{g}_{00}(\psi) > 0$ ((L2) at $\psi' := \psi$); Definition A.5; Fact A.41, item 5;
16300			[gate: `verify/gates/fx/check_divisors.py`]]
16301	(L16)	$\Rightarrow$ $\text{fl}(\widetilde{g}_{00}(\psi)^2) < 2^{62}$	
16302			[(L14), (L15)]
16303	(L17)	$\Rightarrow$ $\text{fl}(\widetilde{g}_{00}(\psi)^2) \in (0, 2^{62})$	
16304			[(L4), (L16)]
16305	(L18)	$\Rightarrow$ item 2	
16306			[(L17)]
		Lemma I.12, items 1 and 5 at $o :=$ mul on $W_x = W_y := W_{\widetilde{g}_{00}(\psi)}$	This proof
		W_x, W_y	$W_{\widetilde{g}_{00}(\psi)}, W_{\widetilde{g}_{00}(\psi)}$ (keychecks, line 11)
		V	$\widetilde{g}_{00,\text{fx64}}(\psi)$ (Definition A.5)
		o	mul (the scope)
		W_{z_o}	W_x (the statement)
		$W_x, W_y \in \{0, \dots, 2^{128}-1\}$	$W_{\widetilde{g}_{00}(\psi)}$, a word (Definition A.5)
16307	(I6)	$V \in \mathbb{Z}$	$\widetilde{g}_{00,\text{fx64}}(\psi)$ (Definition A.5)
		$o \in \{\text{add}, \text{sub}, \text{neg}, \text{mul}, \text{div}, \text{half}\}$	The scope
		Assumption A1	Item 1 of (I4) at $\psi' := \psi$
		Assumption A2	Items 2 and 5 of (I4) at $\psi' := \psi$
		Assumption A4	$o =$ mul (the scope)
		Assumption A5	(L16); Definition I.1, item 1, at $\times$; Definition A.5
		Its item 1: $x_{\text{fx64}} = V$	
		Its item 5: $z_{o,\text{fx64}} = V_o$	
16308	(L19)	$W_x = x_{\text{fx64}} \bmod 2^{128}$	
16309			[(I6); Definition I.1, item 1, at $\times$]
16310	(L20)	$\Rightarrow$ item 1	
16311			[(L19)]
16312			$\square$ (items 1 to 3)
16313			

16314 **Lemma I.38** (No overflow in the key check's quotients [to table])**.** *The key check's quotients do*
16315 *not overflow. Define:*

- $\Psi_n := \{\psi_k : k < n/2\}$, *that of Fact A.43 at* $m := n$.

Let:

- (f, g, F, G) *be a key (line 3 of* keygen *(Algorithm 11)) of degree* $n = 2^h \in \{512, 1024\}$;
- $\psi \in \Psi_n$.

Define:

- *The signer's words and parameters*
  - $B_{fg} := \begin{cases} 31 & n = 512 \\ 15 & n = 1024 \end{cases}$ *[L0: kgen_gauss.c:14-16] [L0: kgen_gauss.c:8-11] [L0: kgen_gauss.c:52-61];*
- *The word bounds*
  - $M_{fg} := M_{h-1}$ *(Lemma I.34 at* $B := B_{fg}$*);*
  - $M_{FG} := M_{h-1}$ *(Lemma I.34 at* $B := 127$*);*
- *The Gram deltas*
  - $\gamma^*_{fg} := B_{fg} n$ *(Lemma H.15);*
  - $\gamma^*_{FG} := 127n$ *(Lemma H.15);*
  - $R_{h-1} := (1 + \sqrt{2}\,\zeta)^{h-1} - 1$ *(Lemma H.11 at* $(0, \zeta)$*);*
  - $A_0 := 0$ *and* $A_{j+1} := \sqrt{2}(1 + \sqrt{2}\,\zeta)A_j + 4\sqrt{2}\,\zeta\sqrt{n}$ *for* $j < h - 1$ *(Lemma H.11 at* $(0, \zeta)$*);*
  - $\delta^*_{fg} := R_{h-1}\gamma^*_{fg}\sqrt{n/2} + A_{h-1}$ *(Lemma H.15);*
  - $\delta^*_{FG} := R_{h-1}\gamma^*_{FG}\sqrt{n/2} + A_{h-1}$ *(Lemma H.15);*
  - $E^*_{00} := 7\zeta + 4\gamma^*_{fg}\delta^*_{fg} + 2\delta^{*2}_{fg}$ *(Lemma H.15);*
  - $E^*_{11} := 7\zeta + 4\gamma^*_{FG}\delta^*_{FG} + 2\delta^{*2}_{FG}$ *(Lemma H.15);*
  - $E^*_{01} := 7\sqrt{2}\,\zeta + 2(\gamma^*_{fg}\delta^*_{FG} + \gamma^*_{FG}\delta^*_{fg} + \delta^*_{fg}\delta^*_{FG})$ *(Lemma H.15);*
- *The computed values*
  - $\widetilde{g}_{00}$*, the Gram's first diagonal* keychecks *computes, line 3;*
  - $\widetilde{g}_{11}$*, the Gram's second diagonal* keychecks *computes, line 3;*
  - num_ψ*, the number* keychecks *computes from* $\widetilde{g}_{01}(\psi)$*, line 10;*
  - lo*, that of* keychecks*, line 6;*
  - hi*, that of* keychecks*, line 7;*
- *The words*
  - W_x*, the word of one of* $\mathrm{fl}(num_\psi / \mathrm{fl}(\widetilde{g}^2_{00}))$, $\mathrm{fl}(q/lo)$ *and* $\mathrm{fl}(hi/q)$*, lines 8 and 11 [L0: fxp/kgen_fx.c:91] [L0: fxp/kgen_fx.c:93];*
  - x*, the number* W_x*'s line computes in* $\mathcal{F}_{\mathrm{fx}}$ *(Definition I.1);*
  - $x_{\mathrm{fx64}} := 2^{64}x$ *(Definition A.5).*

Assume:

(A1) $\forall a < n:\ f_{[a]}, g_{[a]} \in [-B_{fg}, B_{fg}]$ *[L0: fxp/sign_fxcore.c:128-141];*

(A2) $\forall a < n:\ F_{[a]}, G_{[a]} \in [-127, 127]$ *[L0: kgen_ntru.c:1887-1895].*

Then

1. $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$;
2. $\mathrm{fl}(num_\psi / \mathrm{fl}(\widetilde{g}_{00}(\psi)^2)) < 2^{62}$;
3. $\mathrm{fl}(q/lo),\ \mathrm{fl}(hi/q) < 2^{62}$.

Proof.

DEFINES $g_{00} = |f(\psi)|^2 + |g(\psi)|^2$ and $g_{11} = |F(\psi)|^2 + |G(\psi)|^2$ (Fact A.33)

DEFINES $g_{01} = g(\psi)\,\mathrm{conj}\,G(\psi) + f(\psi)\,\mathrm{conj}\,F(\psi)$ (Fact A.33)

DEFINES $\hat{P}_{fg}$, $\hat{P}_{FG}$: the images $\widehat{p}$ of f, g and of F, G (keychecks, line 1)

Lemma I.36, (L13)	This proof
(I1) Shared: $(f, g, F, G), n,\ \psi,\ B_{fg},\ num_\psi,\ \widetilde{g}_{01},\ M_{fg}, M_{FG}$ Shared: assumptions A1, A2	
Its conclusion: $num_{\psi,\mathrm{fx64}} \le \lvert\widetilde{g}_{01,\mathrm{fx64}}\rvert^2/2^{64} + 1$	

(L1) $num_{\psi,\mathrm{fx64}} \le |\widetilde{g}_{01,\mathrm{fx64}}|^2/2^{64} + 1$

[(I1)]

(L2) $\Rightarrow\ num_{\psi} \le |\widetilde{g}_{01}|^2 + 2^{-64}$

[(L1); Definition A.5]

Lemma H.15 at B_{fg}	This proof
Shared: (f,g,F,G), n, B_{fg}, ψ Shared: assumptions A1, A2	
(I2) (f,g,F,G) key of degree $n = 2^h$ $B_{fg} \in \mathbb{R}$	The statement $B_{fg} = 31$ at $n = 512$, $B_{fg} = 15$ at $n = 1024$ (the statement)
ψ a root of the images at a position $k < n/2$	The statement
Its item 3: $\lvert\widetilde{g}_{01} - g_{01}\rvert \le E^*_{01}$	
Its item 1: $\lvert\widetilde{g}_{00} - g_{00}\rvert \le E^*_{00}$	
Its item 2: $\lvert\widetilde{g}_{11} - g_{11}\rvert \le E^*_{11}$	

(L3) $|\widetilde{g}_{01} - g_{01}| \le E^*_{01}$

[item 3 of (I2)]

(L4) $\Rightarrow\ |\widetilde{g}_{01}| \le |g_{01}| + E^*_{01}$

[(L3); Fact A.41, item 1]

(L5) $\forall x, y \in \mathbb{R}:\ (x+y)^2 \le 2x^2 + 2y^2$

[Fact A.41, item 2, at (x,y); Fact A.41, item 13, at $t := x - y$, $j := 1$]

(L6) $\Rightarrow\ |\widetilde{g}_{01}|^2 \le 2|g_{01}|^2 + 2E^{*2}_{01}$

[(L4), (L5); Fact A.41, item 5]

(L7) $|g_{01}|^2 \le g_{00}g_{11}$

[Fact A.33, item 2]

(L8) $g_{00} \le \widetilde{g}_{00} + E^*_{00}$

[item 1 of (I2); Fact A.41, item 1]

Lemma H.16	This proof
Shared: (f,g,F,G), n, ψ, B_{fg}, $\widetilde{g}_{00}$, E^*_{00} Shared: assumptions A1, A2	
(I3) $n \in \{512, 1024\}$	The statement
(f,g,F,G) key of degree n	The statement
Its item 2: $E^*_{00} < \widetilde{g}_{00}$	
Its item 1: $\widetilde{g}_{00} > 2^{-8}$	

(L9) $E^*_{00} < \widetilde{g}_{00}$

[item 2 of (I3)]

(L10) $\Rightarrow\ g_{00} \le 2\widetilde{g}_{00}$

[(L8), (L9)]

(L11) $g_{11} \le \widetilde{g}_{11} + E^*_{11}$

[item 2 of (I2); Fact A.41, item 1]

(L12) $\Rightarrow\ |\widetilde{g}_{01}|^2 \le 4\widetilde{g}_{00}(\widetilde{g}_{11} + E^*_{11}) + 2E^{*2}_{01}$

[(L6), (L7), (L10), (L11); Fact A.41, item 8]

(L13) $\Rightarrow\ num_{\psi} \le 4\widetilde{g}_{00}(\widetilde{g}_{11} + E^*_{11}) + 2E^{*2}_{01} + 2^{-64}$

[(L2), (L12)]

(L14) $\mathrm{fl}(\widetilde{g}^2_{00}) \ge \widetilde{g}^2_{00} - 2^{-65}$

[Definition I.1, item 1, at $\times$; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1)]

(L15) $\widetilde{g}_{00} > 2^{-8}$

[item 1 of (I3)]

(L16) $\Rightarrow\ \widetilde{g}_{00}^2 - 2^{-65} \geq \widetilde{g}_{00}^2/2$

[(L15); Fact A.41, item 5; expand]

(L17) $\Rightarrow\ \mathrm{fl}(\widetilde{g}_{00}^2) \geq \widetilde{g}_{00}^2/2$

[(L14), (L16)]

Lemma I.37, item 2	This proof
(I4) Shared: $(f, g, F, G), n,\ \psi,\ B_{fg},\ \widetilde{g}_{00}$ Shared: assumptions A1, A2	
Its conclusion: $\mathrm{fl}(\widetilde{g}_{00}(\psi)^2) \in (0, 2^{62})$	

(L18) $\Rightarrow\ num_\psi / \mathrm{fl}(\widetilde{g}_{00}^2) \leq (4\widetilde{g}_{00}(\widetilde{g}_{11} + E_{11}^*) + 2E_{01}^{*2} + 2^{-64})/(\widetilde{g}_{00}^2/2)$

[(L13), (L17); (I4); Fact A.41, item 5]

(L19) $(4\widetilde{g}_{00}(\widetilde{g}_{11} + E_{11}^*) + 2E_{01}^{*2} + 2^{-64})/(\widetilde{g}_{00}^2/2) = 8(\widetilde{g}_{11} + E_{11}^*)/\widetilde{g}_{00} + (4E_{01}^{*2} + 2^{-63})/\widetilde{g}_{00}^2$

[expand]

(L20) $\Rightarrow\ num_\psi / \mathrm{fl}(\widetilde{g}_{00}^2) \leq 8(\widetilde{g}_{11} + E_{11}^*)/\widetilde{g}_{00} + (4E_{01}^{*2} + 2^{-63})/\widetilde{g}_{00}^2$

[(L18), (L19)]

Lemma I.34 at $j := h-1$, at $B := B_{fg}$ on f, g and at $B := 127$ on F, G	This proof
Shared: h	
(I5) p	$p \in \{f, g\}$ at B_{fg}; $p \in \{F, G\}$ at 127 (the statement)
B	$B_{fg}, 127$ (the statement)
W_x	$W_{\widetilde{p}},\ \widetilde{p} \in \hat{P}_{fg} \cup \hat{P}_{FG}$ (keychecks, line 1)
X_{h-1}	$\hat{P}_{fg}, \hat{P}_{FG}$ (the proof's block)
M_{h-1}	M_{fg}, M_{FG} (the statement)
$h \in \{3, \ldots, 10\}$	$n \in \{512, 1024\}$ (the statement)
$p \in \{-128, \ldots, 127\}^{2^h}$	Assumptions A1 and A2; $B \leq 127$ (B, the rows above)
$B \in [0, 127]$	B_{fg} (the statement); 127
W_x pair of words at stage j	$\hat{P}_{fg}$, $\hat{P}_{FG}$ (the proof's block)
Assumption A1	Assumptions A1 and A2
Its item 1: $\forall j \leq h-1\ \forall x \in X_j :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 2: $\forall j \leq h-1\ \forall x \in X_j :\ \lvert x_{\mathrm{fx64}} \rvert \leq M_j$	
Its item 5: $\forall j \leq h-1 :\ M_j \leq c^{h-1}(1.4143\, B 2^{64} + 2) - 2$	
Its item 6: $c^{h-1}(1.4143\, B 2^{64} + 2) - 2 < 2^{81}$	

Lemma I.35 the key generation's form	This proof
(I6) $(b_{00}, b_{01}, b_{10}, b_{11})$	$(\widetilde{\hat{g}}, \widetilde{\hat{f}}, \widetilde{\hat{G}}, \widetilde{\hat{F}})$ (keychecks, line 1)
Y_0, Y_1	$\hat{P}_{fg}, \hat{P}_{FG}$ (the proof's block)
M_0, M_1	M_{fg}, M_{FG} (the statement)
W_x	$W_{\widetilde{g_{00}}}, W_{\widetilde{g_{11}}}$ (keychecks, line 3)
b_{jk} arrays of pairs of words of ffSampling$^{\mathcal{F}}$, line 1, or the same without the negations	keychecks (Algorithm 12), lines 1 and 3
$M_0, M_1 \geq 0$	M_{fg}, M_{FG} (the statement)
W_x a word of Gram on the b_{jk}	keychecks (Algorithm 12), line 3
Assumption A1	Item 1 of (I5) at $j = h-1$
Assumption A2	Item 2 of (I5) at $j = h-1$
Assumption A3	Items 5 and 6 of (I5)
Its item 2: $\lvert \widetilde{g}_{00,\mathrm{fx64}} \rvert \leq 4(M_0^2/2^{64} + 1/2)$	
Its item 3: $\lvert \widetilde{g}_{11,\mathrm{fx64}} \rvert \leq 4(M_1^2/2^{64} + 1/2)$	

(L21) $\lvert \widetilde{g}_{00,\mathrm{fx64}} \rvert \leq 4(M_{fg}^2/2^{64} + 1/2)$

[item 2 of (I6)]

(L22) $|\widetilde{g}_{11,\mathrm{fx64}}| \le 4(M_{FG}^2/2^{64} + 1/2)$

[item 3 of (I6)]

(L23) $\Rightarrow\ \widetilde{g}_{00} \le 4(M_{fg}^2/2^{128} + 2^{-65})$

[(L21); Definition A.5; expand]

(L24) $\Rightarrow\ \widetilde{g}_{11} \le 4(M_{FG}^2/2^{128} + 2^{-65})$

[(L22); Definition A.5; expand]

(L25) $\widetilde{g}_{00} \ge q^2/(2(127n)^2) - E_{00}^*$

[Lemma H.16, (L3)]

(L26) $8(\widetilde{g}_{11} + E_{11}^*)/\widetilde{g}_{00} + (4E_{01}^{*2} + 2^{-63})/\widetilde{g}_{00}^2 < 2^{62}$

[[gate: `verify/gates/fx/check_quotients.py`], at (L24), (L25); item 5 of (I5) at $B = 127$; Fact A.41, item 5]

(L27) $q/lo < 2^{62}$

[[gate: `verify/gates/fx/check_quotients.py`], at (L25); $lo = \min_\psi \widetilde{g}_{00}$ (keychecks, line 6); Fact A.41, item 5]

(L28) $hi/q < 2^{62}$

[[gate: `verify/gates/fx/check_quotients.py`], at (L23); item 5 of (I5) at $B = B_{fg}$; Fact A.41, item 5; $hi = \max_\psi \widetilde{g}_{00}$ (keychecks, line 7)]

Lemma I.12, items 1 and 5 at the three quotients of lines 8 and 11, at $o :=$ div	This proof
(W_x, W_y)	$(W_{num_\psi}, W_{\mathrm{fl}(\widetilde{g}_{00}(\psi)^2)})$, (W_q, W_{lo}), (W_{hi}, W_q) (keychecks, lines 8 and 11)
o	div (the scope)
W_{z_o}	W_x (the statement)
V	$num_{\psi,\mathrm{fx64}}$, $\mathrm{fl}(\widetilde{g}_{00}(\psi)^2)_{\mathrm{fx64}}$ (the scope)
$W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	Words (Definition A.5)
$V \in \mathbb{Z}$	Definition A.5
$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	The scope

(I7)

Assumption A1	W_{num_ψ} (Lemma I.36, item 1); $W_{\mathrm{fl}(\widetilde{g}_{00}^2)}$ (Lemma I.37, item 1)
Assumption A2	$num_\psi < 2^{62}$ (Lemma I.36, item 2); item 2 of (I4); Definition A.5
Assumption A4	Item 2 of (I4); $lo > 0$ (Lemma I.37, item 3); Lemma I.7, item 1, at $i := q$; W_{lo} (Lemma I.8, item 3, its assumption A1 by (L21))
Assumption A5	(L20), (L26), (L27), (L28); roundAway (Definition I.1); Fact A.41, item 22; Definition A.5

Its item 1: $x_{\mathrm{fx64}} = V$

Its item 5: $z_{o,\mathrm{fx64}} = V_o$

(L29) $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[(I7); Definition I.1, item 1, at /]

(L30) $x < 2^{62}$

[(L20), (L26), (L27), (L28)]

(L31) $\Rightarrow$ item 1

[(L29)]

(L32) $\Rightarrow$ item 2

[(L30) at $x = \mathrm{fl}(num_\psi / \mathrm{fl}(\widetilde{g}_{00}^2))$]

(L33) $\Rightarrow$ item 3

[(L30) at $x = \mathrm{fl}(q/lo)$ and at $x = \mathrm{fl}(hi/q)$]

□ (items 1 to 3)

I.3.3 No overflow in the tree

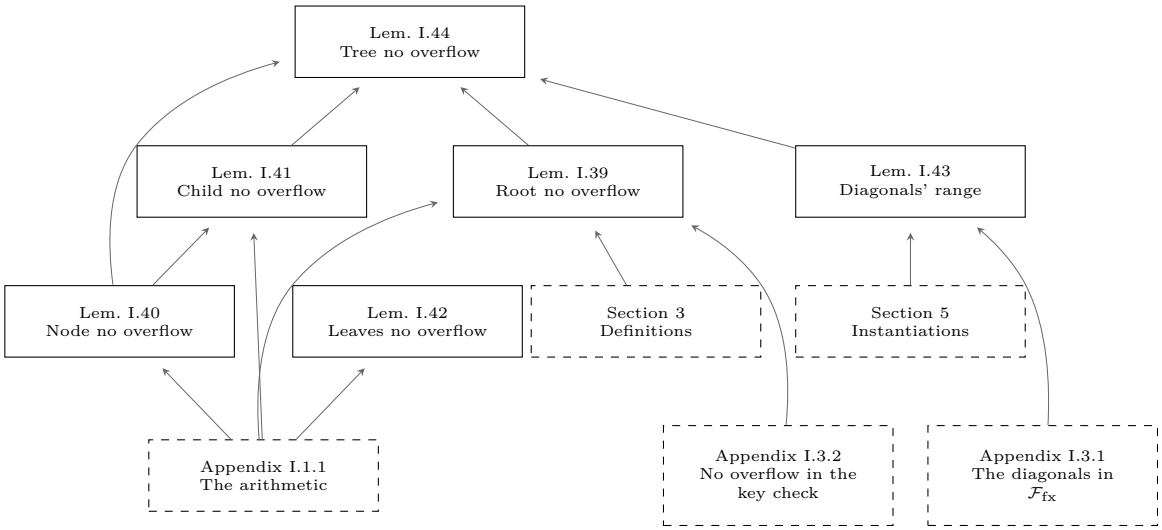


Figure 77: Dependencies, Appendix I.3.3.

Lemma I.39 (No overflow at the root [to table])**.** *The root's words $\widetilde{\mu}$, $\widetilde{l}_{10}$ and $\widetilde{d}_{11}$ hold their values, below 2^{126}. Let:*

- *(f, g, F, G) be a key (line 3 of keygen (Algorithm 11)) of degree $n = 2^h \in \{512, 1024\}$.*

Define:

- *$\widetilde{g}_{00}$, the Gram's first diagonal ffSampling$^{\mathcal{F}}$ (Algorithm 10) computes, line 3;*
- *$\widetilde{g}_{01}$, the Gram's off-diagonal entry ffSampling$^{\mathcal{F}}$ (Algorithm 10) computes, line 3.*

Let:

- *W_x be a word of the root's step on $\widetilde{g}_{00}$ and $\widetilde{g}_{01}$, one of $\widetilde{\mu}$, $\widetilde{l}_{10}$ and $\widetilde{d}_{11}$: LDL† (Algorithm 5), lines 7 to 12, and ffsamp (Algorithm 6), line 6.*

Define:

- *$B_{fg} := \begin{cases} 31 & n = 512 \\ 15 & n = 1024 \end{cases}$ [LO: kgen_gauss.c:14-16];*
- *x, the number W_x's line computes in $\mathcal{F}_{\text{fx}}$ (Definition I.1);*
- *$x_{\text{fx64}} := 2^{64}x$ (Definition A.5).*

Assume:

(A1) $\forall a < n:\ f_{[a]}, g_{[a]} \in [-B_{fg}, B_{fg}]$ [LO: fxp/sign_fxcore.c:128-141];

(A2) $\forall a < n:\ F_{[a]}, G_{[a]} \in [-127, 127]$ [LO: kgen_ntru.c:1887-1895].

Then

1. $W_x = x_{\text{fx64}} \bmod 2^{128}$;
2. $|x_{\text{fx64}}| < 2^{126}$.

Proof.

DEFINES $q = 12289$ (Fact A.33)
DEFINES γ^*_{fg}, δ^*_{fg} and ζ, those of Lemma H.15
DEFINES $E^*_{00} = 7\zeta + 4\gamma^*_{fg}\delta^*_{fg} + 2\delta^{*2}_{fg}$ (Lemma H.15)
DEFINES $g_{\min} = q^2/(2(127n)^2) - E^*_{00}$
DEFINES $\widetilde{p}$: an image of f, g, F or G, or its negation, ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 1
DEFINES b_{00}, b_{01}, b_{10}, b_{11}: the images of g, $-f$, G and $-F$ line 1 writes
DEFINES M_{FG}: the M_{h-1} of Lemma I.34 at $B := 127$
DEFINES M_{fg}: the M_{h-1} of Lemma I.34 at $B := B_{fg}$

	Lemma H.16, (L3)	This proof
	Shared: (f, g, F, G), n, B_{fg}, $\widetilde{g}_{00}$, E^*_{00}	
(I1)	Shared: assumptions A1, A2	
	$q^2/(2(127n)^2) - E^*_{00}$	$g_{\min}$ (the proof's block)
	Its conclusion: $\widetilde{g}_{00} \geq q^2/(2(127n)^2) - E^*_{00}$	
(L1)	$\widetilde{g}_{00} \geq g_{\min}$	
		[(I1); $g_{\min}$ (the proof's block)]
(L2)	$g_{\min} > 2^{-8}$	
		[$q^2/(2(127n)^2) - E^*_{00} > 2^{-8}$ (Lemma H.16, the first measured row); $g_{\min}$ (the proof's block)]
(L3)	$\widetilde{g}_{00} > 0$	
		[(L1), (L2)]

	Lemma I.34 at $j := h - 1$	This proof
	Shared: h	
	p	$p \in \{g, f, G, F\}$ (the statement)
	B	127 (the statement)
	W_x	$W_{\widetilde{p}}$, $\widetilde{p} \in \{\widetilde{g}, \widetilde{f}, -\widetilde{f}, \widetilde{G}, \widetilde{F}, -\widetilde{F}\}$ (the proof's block)
	M_{h-1}	M_{FG} (the proof's block)
	$h \in \{3, \ldots, 10\}$	$n \in \{512, 1024\}$ (the statement)
	$p \in \{-128, \ldots, 127\}^{2^h}$	Assumptions A1 and A2; $B \leq 127$ (B, the rows above)
	$B \in [0, 127]$	127
(I2)	W_x a pair of words at stage j	ffSampling$^{\mathcal{F}}$, line 1 (the proof's block)
	Assumption A1	Assumptions A1 and A2
	Its item 1: $\forall j \leq h-1\ \forall x \in X_j :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 2: $\forall j \leq h-1\ \forall x \in X_j :\ \lvert x_{\text{fx64}}\rvert \leq M_j$	
	Its item 3: $\forall x \in X^- :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 4: $\forall x \in X^- :\ \lvert x_{\text{fx64}}\rvert \leq M_{h-1}$	
	Its item 5: $\forall j \leq h-1 :\ M_j \leq c^{h-1}(1.4143\, B2^{64} + 2) - 2$	
	Its item 6: $c^{h-1}(1.4143\, B2^{64} + 2) - 2 < 2^{81}$	
(L4)	$\forall \widetilde{p} :\ W_{\widetilde{p}} = \widetilde{p}_{\text{fx64}} \bmod 2^{128}$	
		[items 1 and 3 of (I2)]
(L5)	$\forall \widetilde{p} :\ \lvert\widetilde{p}_{\text{fx64}}\rvert \leq M_{FG}$	
		[items 2 and 4 of (I2); M_{FG} (the proof's block)]
(L6)	$M_{FG} < 2^{81}$	
		[items 5 and 6 of (I2)]

Lemma I.34 at $j := h-1$	This proof
Shared: h	
p	$p \in \{g, f\}$ (the statement)
B	B_{fg} (the statement)
W_x	$W_{\widetilde{\hat{p}}}$, $\widetilde{\hat{p}} \in \{\widetilde{\hat{g}}, \widetilde{\hat{f}}, -\widetilde{\hat{f}}\}$ (the proof's block)
M_{h-1}	M_{fg} (the proof's block)
$h \in \{3, \dots, 10\}$	$n \in \{512, 1024\}$ (the statement)
(I3) $p \in \{-128, \dots, 127\}^{2^h}$	Assumption A1; $B \le 127$ (B, the rows above)
$B \in [0, 127]$	B_{fg} (the statement)
W_x a pair of words at stage j	ffSampling$^{\mathcal{F}}$, line 1 (the proof's block)
Assumption A1	Assumption A1
Its item 2: $\forall j \le h-1\ \forall x \in X_j :\ \lvert x_{\text{fx64}}\rvert \le M_j$	
Its item 4: $\forall x \in X^- :\ \lvert x_{\text{fx64}}\rvert \le M_{h-1}$	
Its item 5: $\forall j \le h-1 :\ M_j \le c^{h-1}(1.4143\, B2^{64} + 2) - 2$	
Its item 6: $c^{h-1}(1.4143\, B2^{64} + 2) - 2 < 2^{81}$	

(L7) $\lvert b_{00,\text{fx64}}\rvert,\ \lvert b_{01,\text{fx64}}\rvert \le M_{fg}$

[items 2 and 4 of (I3)]

(L8) $M_{fg} < 2^{81}$

[items 5 and 6 of (I3)]

Lemma I.35, items 1, 2, 4 and 5	This proof
Shared: b_{jk}	
Y_0, Y_1	$\{b_{00}, b_{01}\}, \{b_{10}, b_{11}\}$ (the proof's block)
M_0, M_1	M_{fg}, M_{FG} (the proof's block)
W_x	$W_{\widetilde{g_{00}}}, W_{\widetilde{g_{01}}}$ (the statement)
b_{jk} arrays of pairs of words of ffSampling$^{\mathcal{F}}$, line 1	b_{jk} (the proof's block)
$M_0, M_1 \ge 0$	M_{fg}, M_{FG} (the proof's block)
(I4) W_x a word of Gram on the b_{jk}	$\widetilde{g}_{01}$ (the statement)
Assumption A1	(L4)
Assumption A2	(L5), (L7)
Assumption A3	(L6), (L8)
Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
Its item 2: $\lvert\widetilde{g}_{00,\text{fx64}}\rvert \le 4(M_0^2/2^{64} + 1/2)$	
Its item 4: $\lvert\widetilde{g}_{01,\text{fx64}}\rvert \le 2M_0M_1/2^{64} + 2\sqrt{2}$	
Its item 5: $4(M_0^2/2^{64} + 1/2),\ 4(M_1^2/2^{64} + 1/2),\ 2M_0M_1/2^{64} + 2\sqrt{2} < 2^{101}$	

(L9) $\lvert\widetilde{g}_{01,\text{fx64}}\rvert \le 2M_{fg}M_{FG}/2^{64} + 2\sqrt{2}$

[item 4 of (I4)]

(L10) $\forall x \in \{\widetilde{g}_{00}, \widetilde{g}_{01,r}, \widetilde{g}_{01,i}\} :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[item 1 of (I4)]

(L11) $\lvert\widetilde{g}_{00,\text{fx64}}\rvert,\ \lvert\widetilde{g}_{01,\text{fx64}}\rvert < 2^{101}$

[items 2, 4 and 5 of (I4)]

	Lemma I.10, item 6	This proof
	Shared: h	
(I5)	$\mathcal{O}$ `g00` $h \in \{2, \dots, 10\}$ each input array of words	$\mathcal{O}$ (Lemma I.10) $\widetilde{g}_{00}$ (the statement) $n \in \{512, 1024\}$ (the statement) $\widetilde{g}_{00}$, $\widetilde{g}_{01}$, the Gram's words (the statement; Definition A.5)
	Assumption A3	(L3), (L10), (L11); Definition A.5

Its conclusion: The object of `fxpoly_LDL_root_fft` in $\mathcal{O}$ returns the words of lines 7 to 12 of LDL† and of line 6 of ffsamp (Algorithm 6).

(L12) $(\widetilde{\mu}_r, \widetilde{\mu}_i) = (\mathrm{fl}(\widetilde{g}_{01,r}/\widetilde{g}_{00}), \mathrm{fl}(\widetilde{g}_{01,i}/\widetilde{g}_{00}))$

[(I5); LDL† (Algorithm 5), lines 7 and 8]

	Lemma I.12, items 1 and 3 at every $x \in \{\widetilde{g}_{01,r}, \widetilde{g}_{01,i}, q^2\}$ and at $\widetilde{g}_{00}$	This proof
(I6)	W_x W_y V $W_x, W_y \in \{0, \dots, 2^{128} - 1\}$ $V \in \mathbb{Z}$	$W_{\widetilde{g}_{01,r}}, W_{\widetilde{g}_{01,i}}, W_{q^2}$ (the scope) $W_{\widetilde{g}_{00}}$ (the statement) $\widetilde{g}_{01,r,\mathrm{fx64}}, \widetilde{g}_{01,i,\mathrm{fx64}}, (q^2)_{\mathrm{fx64}}, \widetilde{g}_{00,\mathrm{fx64}}$ (Definition A.5) The words (Definition A.5) of x and $\widetilde{g}_{00}$ Definition A.5
	Assumption A1 Assumption A2 Assumption A3	(L10); Lemma I.7, item 1, at $i := q^2$ (L11); q (the proof's block) (L3); item 1 at $W_{\widetilde{g}_{00}}$
	Its item 1: $x_{\mathrm{fx64}} = V$	
	Its item 3: $\lvert\mathrm{roundAway}(x_{\mathrm{fx64}} 2^{64} / y_{\mathrm{fx64}})\rvert \le \lvert x_{\mathrm{fx64}}\rvert 2^{64} / \lvert y_{\mathrm{fx64}}\rvert + 1/2$	

(L13) $|\widetilde{\mu}_r| \le |\widetilde{g}_{01,r}|/\widetilde{g}_{00} + 2^{-65}$

[(L12); Definition I.1, item 1, at /; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1); (L3)]

(L14) $|\widetilde{\mu}_i| \le |\widetilde{g}_{01,i}|/\widetilde{g}_{00} + 2^{-65}$

[(L12); Definition I.1, item 1, at /; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1); (L3)]

(L15) $1/\widetilde{g}_{00} \le 1/g_{\min}$

[(L1), (L2); Fact A.41, item 5]

(L16) $|\widetilde{\mu}| \le \|(|\widetilde{g}_{01,r}|, |\widetilde{g}_{01,i}|)\|/g_{\min} + \|(2^{-65}, 2^{-65})\|$

[(L13), (L14), (L15); Fact A.41, items 1, 3, 5 and 26]

(L17) $\|(|\widetilde{g}_{01,r}|, |\widetilde{g}_{01,i}|)\| = |\widetilde{g}_{01}|$

[Fact A.41, item 1]

(L18) $\|(2^{-65}, 2^{-65})\| = \sqrt{2}\, 2^{-65}$

[expand]

(L19) $\Rightarrow\ |\widetilde{\mu}| \le |\widetilde{g}_{01}|/g_{\min} + \sqrt{2}\, 2^{-65}$

[(L16), (L17), (L18)]

(L20) $|\mathrm{fl}(q^2/\widetilde{g}_{00})_{\mathrm{fx64}}| \le (q^2)_{\mathrm{fx64}} 2^{64} / \widetilde{g}_{00,\mathrm{fx64}} + 1/2$

[(I5); (I6); Definition I.1, item 1, at /]

(L21) $\Rightarrow\ \mathrm{fl}(q^2/\widetilde{g}_{00}) \le q^2/\widetilde{g}_{00} + 2^{-65}$

[(L20); Definition A.5]

(L22) $q^2/\widetilde{g}_{00} \le q^2/g_{\min}$

[(L15); Fact A.41, item 26, at $c := q^2$]

(L23) $\Rightarrow\ \mathrm{fl}(q^2/\widetilde{g}_{00}) \le q^2/g_{\min} + 2^{-65}$

[(L21), (L22)]

(L24) $\Rightarrow\ |\widetilde{g}_{01}| \le 2M_{fg}M_{FG}/2^{128} + 2\sqrt{2}\, 2^{-64}$

[(L9); Definition A.5]

(L25) $\forall x \in \{\widetilde{\mu}, \mathrm{fl}(q^2/\widetilde{g}_{00})\} :\ |x| < 2^{62}$

[[gate: `verify/gates/fx/root_words.py`], at the bounds of (L19), (L23) and (L24), $g_{\min}$ (the proof's block), M_{FG} and M_{fg} at their ceilings (item 5 of (I2) and (I3))]

	Lemma I.12, items 1 and 5 at each operation of LDL† (Algorithm 5), lines 7 to 12, and of ffsamp (Algorithm 6), line 6	This proof
(I7)	(W_x, W_y)	$(W_{\widetilde{g}_{01,r}}, W_{\widetilde{g}_{00}})$, $(W_{\widetilde{g}_{01,i}}, W_{\widetilde{g}_{00}})$, $(W_{q^2}, W_{\widetilde{g}_{00}})$ at div; $W_{\widetilde{\mu}_i}$ at neg (LDL†; ffsamp)
	o	div, neg (the scope)
	W_{z_o}	W_x (the statement)
	V	$\widetilde{g}_{01,r,\mathrm{fx64}}, \widetilde{g}_{01,i,\mathrm{fx64}}, (q^2)_{\mathrm{fx64}}, \widetilde{g}_{00,\mathrm{fx64}}$ (Definition A.5)
	$W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	Words (Definition A.5)
	$V \in \mathbb{Z}$	Definition A.5
	$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	The scope
	Assumption A1	(L10); Lemma I.7, item 1, at $i := q^2$
	Assumption A2	(L11); q (the proof's block)
	Assumption A4	(L3); item 1 at $W_{\widetilde{g}_{00}}$
	Assumption A5	(L25); Definition I.1, item 1, at /; Definition A.5
	Its item 1: $x_{\mathrm{fx64}} = V$	
	Its item 5: $z_{o,\mathrm{fx64}} = V_o$	

(L26) $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[(I7); Definition I.1, item 1, at / and at −]

(L27) $|x_{\mathrm{fx64}}| = 2^{64}|x|$

[Definition A.5]

(L28) $2^{64}|x| < 2^{126}$

[(L25); $\widetilde{l}_{10} = \mathrm{conj}\,\widetilde{\mu}$ (LDL†, line 12); $|\mathrm{conj}\,z| = |z|$ (Fact A.41, item 1); $\widetilde{d}_{11} = \mathrm{fl}(q^2/\widetilde{g}_{00})$ (ffsamp, line 6)]

(L29) $\Rightarrow$ item 1

[(L26)]

(L30) $\Rightarrow$ item 2

[(L27), (L28)]

□ (items 1 and 2)

Lemma I.40 (No overflow in a node's self-adjoint split [to table])**.** *A node's self-adjoint split does not overflow. Let:*

- $h \in \{2, \dots, 10\}$*;*
- $\widetilde{d}$ *be the parent's diagonal array at* $m := 2^h$*.*

Define:

- $\forall \psi: \ (a, b) := (\widetilde{d}(\psi), \widetilde{d}(-\psi))$*;*
- W_a*,* W_b*, their words (Definition A.5);*
- $\widetilde{f}_0$*,* $\widetilde{f}_1$*, the numbers* $\widetilde{\mathrm{split}}_{\mathrm{sa}}$ *(Algorithm 3), lines 4 and 6, computes on the parent's diagonal array;*
- $\widetilde{f}_- := \mathrm{fl}((a \ominus b)/2)$*.*

Let:

- W_x *be a word* $\widetilde{\mathrm{split}}_{\mathrm{sa}}$ *(Algorithm 3), lines 4 and 6, writes on the parent's diagonal array, one of* $\widetilde{f}_0$*,* $\widetilde{f}_1$ *and* $\widetilde{f}_-$*.*

Define:

- x*, the number* W_x*'s line computes in* $\mathcal{F}_{\mathrm{fx}}$ *(Definition I.1);*
- $x_{\mathrm{fx64}} := 2^{64}x$ *(Definition A.5).*

Assume:

(A1) $\forall \psi: \ W_a = a_{\mathrm{fx64}} \bmod 2^{128}$*;*

(A2) $\forall \psi :\ a \in [2^8, 2^{19}]$.
Then

1. $W_x = x_{\text{fx64}} \bmod 2^{128}$;
2. $|x_{\text{fx64}}| < 2^{127}$.

Proof.
DEFINES $L = 2^{64} \cdot 2^8$
DEFINES $A = 2^{64} \cdot 2^{19}$

(L1) $|\widetilde{f}_{0,\text{fx64}}|,\ |\widetilde{f}_{-,\text{fx64}}| \le A + 1/2$
[$\widetilde{\text{split}}_{\text{sa}}$ (Algorithm 3), line 4; Definition I.1, items 1 and 2; $\zeta_{\text{op}} := 2^{-65}$ (Definition I.1); assumption A2; Definition A.5]

(L2) $\widetilde{f}_{0,\text{fx64}} \ge L - 1/2$
[$\widetilde{\text{split}}_{\text{sa}}$ (Algorithm 3), line 4; Definition I.1, items 1 and 2; $\zeta_{\text{op}} := 2^{-65}$ (Definition I.1); assumption A2; Definition A.5]

(L3) $|\text{Re}\, \widetilde{f}_{1,\text{fx64}}|,\ |\text{Im}\, \widetilde{f}_{1,\text{fx64}}| \le A + 1$
[$\widetilde{\text{split}}_{\text{sa}}$ (Algorithm 3), line 6; Definition A.8; Definition I.1, item 1, at $\times$; $\zeta_{\text{op}} := 2^{-65}$ (Definition I.1); (L1); the twiddle parts' words in $[-2^{64}, 2^{64}]$ ([gate: `verify/gates/fx/twiddle_parts.py`])]

(I1)

Lemma I.12, items 1 and 5 at each operation of lines 4 and 6 of $\widetilde{\text{split}}_{\text{sa}}$ (Algorithm 3) at every ψ	This proof
(W_x, W_y)	(W_a, W_b) at add, sub; $W_{a\oplus b}, W_{a\ominus b}$ at half; $(W_{\widetilde{f}_-}, W_{\text{Re}\,\widetilde{s}}), (W_{\widetilde{f}_-}, W_{\text{Im conj}\,\widetilde{s}})$ at mul ($\widetilde{\text{split}}_{\text{sa}}$, lines 4 and 6)
o	add, sub, half, mul (the scope)
V	$a_{\text{fx64}}, b_{\text{fx64}}, (\text{Re}\,\widetilde{s})_{\text{fx64}}, (\text{Im conj}\,\widetilde{s})_{\text{fx64}}$ (Definition A.5)
$W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	Words (Definition A.5)
$V \in \mathbb{Z}$	Definition A.5
$o \in \{\text{add}, \text{sub}, \text{neg}, \text{mul}, \text{div}, \text{half}\}$	The scope
Assumption A1	Assumption A1 at ψ and at $-\psi$; Definition I.1, items 5 and 6
Assumption A2	Assumption A2; Definition A.5; the twiddle parts' words in $[-2^{64}, 2^{64}]$ ([gate: `verify/gates/fx/twiddle_parts.py`])
Assumption A4	$o \ne \text{div}$ (the scope)
Assumption A5	Assumption A2; (L1), (L3); A (the proof's block); Definition A.5
Its item 1: $x_{\text{fx64}} = V$	
Its item 5: $z_{o,\text{fx64}} = V_o$	

(L4) $\forall x \in \{\widetilde{f}_0, \widetilde{f}_-\} :\ W_x = x_{\text{fx64}} \bmod 2^{128}$
[(I1); Lemma I.10, item 3; Definition I.1, item 1, at $\pm$, and item 2, at $x := a \oplus b, a \ominus b$, $\forall \psi :\ a \in [2^8, 2^{19}]$ (assumption A2); Definition A.5]

(L5) $W_{\widetilde{f}_1} = \widetilde{f}_{1,\text{fx64}} \bmod 2^{128}$
[(I1); (L4); Definition A.8; Definition I.1, item 1, at $\times$]

(L6) $\sqrt{2}(A + 1) < 2^{127}$
[A (the proof's block); expand]

(L7) $\Rightarrow$ item 1
[(L4), (L5)]

(L8) $\Rightarrow$ item 2
[(L1), (L3), (L6); $\forall a, b \in \mathbb{R} :\ |a + ib|^2 = a^2 + b^2$ (Fact A.41, item 1)]

□ (items 1 and 2)

Lemma I.41 (No overflow in the child's $LDL^\dagger$ [to table])**.** *The child's $LDL^\dagger$ does not overflow.*
Let:

- $h \in \{2, \dots, 10\}$;
- $\widetilde{d}$ *be the parent's diagonal array at* $m := 2^h$.

Define:

- $\forall \psi : \ (a, b) := (\widetilde{d}(\psi), \widetilde{d}(-\psi))$;
- W_a, W_b, *their words (Definition A.5);*
- $\widetilde{f}_0$, $\widetilde{f}_1$, *the numbers* $\widetilde{\text{split}}_{\text{sa}}$ *(Algorithm 3), lines 4 and 6, computes on the parent's diagonal array.*

Let:

- W_x *be a word of* LDL† *(Algorithm 5), lines 7 to 18, on the child's Gram* $(\widetilde{f}_0, \widetilde{f}_1, \widetilde{f}_0)$ *at* $m/2$.

Define:

- x, *the number* W_x*'s line computes in* $\mathcal{F}_{\text{fx}}$ *(Definition I.1);*
- $x_{\text{fx64}} := 2^{64} x$ *(Definition A.5).*

Assume:

(A1) $\forall \psi : \ W_a = a_{\text{fx64}} \bmod 2^{128}$;
(A2) $\forall \psi : \ a \in [2^8, 2^{19}]$.
Then

1. $W_x = x_{\text{fx64}} \bmod 2^{128}$;
2. $|x_{\text{fx64}}| < 2^{127}$.

Proof.

DEFINES $L = 2^{64} \cdot 2^8$
DEFINES $A = 2^{64} \cdot 2^{19}$
DEFINES $J = (A+1)2^{64}/(L - 1/2) + 1/2$
COMPUTES *zo*: the number LDL† (Algorithm 5) computes at line 14

Lemma I.40, (L2)	This proof
Shared: $h, \widetilde{d}, \ a, b, \ W_a, W_b, \ \widetilde{f}_0$ (I1) Shared: $h \in \{2, \dots, 10\}$ Shared: assumptions A1, A2	
Its conclusion: $\widetilde{f}_{0,\text{fx64}} \geq L - 1/2$	
(L1) $\widetilde{f}_{0,\text{fx64}} \geq L - 1/2$	
[(I1)]	

Lemma I.40, (L1)	This proof
Shared: $h, \widetilde{d}, \ a, b, \ W_a, W_b, \ \widetilde{f}_0$ (I2) Shared: $h \in \{2, \dots, 10\}$ Shared: assumptions A1, A2	
Its conclusion: $\lvert\widetilde{f}_{0,\text{fx64}}\rvert, \ \lvert\widetilde{f}_{-,\text{fx64}}\rvert \leq A + 1/2$	
(L2) $\lvert\widetilde{f}_{0,\text{fx64}}\rvert \leq A + 1/2$	
[(I2)]	

Lemma I.40, (L3)	This proof
Shared: $h, \widetilde{d}, \ a, b, \ W_a, W_b, \ \widetilde{f}_0$ (I3) Shared: $h \in \{2, \dots, 10\}$ Shared: assumptions A1, A2	
Its conclusion: $\lvert\text{Re}\,\widetilde{f}_{1,\text{fx64}}\rvert, \ \lvert\text{Im}\,\widetilde{f}_{1,\text{fx64}}\rvert \leq A + 1$	
(L3) $\lvert\text{Re}\,\widetilde{f}_{1,\text{fx64}}\rvert, \ \lvert\text{Im}\,\widetilde{f}_{1,\text{fx64}}\rvert \leq A + 1$	
[(I3)]	

(L4) $\widetilde{f}_{0,\mathrm{fx64}} > 0$

[(L1); L (the proof's block)]

Lemma I.40, item 1 at every word W_x of $\widetilde{f}_0$, $\widetilde{f}_1$, $\widetilde{f}_-$	This proof
Shared: $h, \widetilde{d},\ a, b,\ W_a, W_b,\ \widetilde{f}_0, \widetilde{f}_1$ Shared: $h \in \{2, \dots, 10\}$ Shared: assumptions A1, A2	
W_x	$W_{\widetilde{f}_0}, W_{\widetilde{f}_1}, W_{\widetilde{f}_-}$ (the scope)
Its item 1: $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	

Lemma I.10, item 5 at the child's degree 2^{h-1}	This proof
h	$h-1$ (the scope)
$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
`g00`	$\widetilde{f}_0$ (the statement)
(I5) $h \in \{2, \dots, 10\}$	$h-1$, at $h \geq 3$ (the line)
each input array of words	The child's Gram $(\widetilde{f}_0, \widetilde{f}_1, \widetilde{f}_0)$ (the statement; Definition A.5)
Assumption A2	(I4) at $W_{\widetilde{f}_0}$; (L2), (L4); Definition A.5

Its conclusion: The object of `fxpoly_LDL_fft` in $\mathcal{O}$ returns the words of lines 7 to 18 of LDL† (Algorithm 5).

(L5) $h \geq 3 \Rightarrow\ (\mathrm{Re}\,\widetilde{\mu}, \mathrm{Im}\,\widetilde{\mu}) = (\mathrm{fl}(\mathrm{Re}\,\widetilde{f}_1/\widetilde{f}_0), \mathrm{fl}(\mathrm{Im}\,\widetilde{f}_1/\widetilde{f}_0))$

[(I5); LDL† (Algorithm 5), lines 7 and 8]

Lemma I.10, item 7 at the child of degree 2	This proof
Shared: h Shared: $h \in \{2, \dots, 10\}$	
$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
`g00`	$\widetilde{f}_0$ (the statement)
(I6) each input array of words	The child's Gram $(\widetilde{f}_0, \widetilde{f}_1, \widetilde{f}_0)$ (the statement; Definition A.5)
Assumption A4	(I4) at $W_{\widetilde{f}_0}$; (L2), (L4); Definition A.5

Its conclusion: At a node of degree 2, the object of `fxp_ffsamp_fft` in $\mathcal{O}$ returns the words of lines 7 to 18 of LDL† and of lines 1 to 18 of deepest (Algorithm 7), each square root $\mathrm{fl}(\sqrt{x})$ of those lines the word $Q(W_x)$ on the word W_x of x, each call of SamplerZ (Algorithm 8) left opaque.

(L6) $h = 2 \Rightarrow\ (\mathrm{Re}\,\widetilde{\mu}, \mathrm{Im}\,\widetilde{\mu}) = (\mathrm{fl}(\mathrm{Re}\,\widetilde{f}_1/\widetilde{f}_0), \mathrm{fl}(\mathrm{Im}\,\widetilde{f}_1/\widetilde{f}_0))$

[(I6); LDL† (Algorithm 5), lines 7 and 8]

Lemma I.12, item 3 at every $x \in \{\mathrm{Re}\,\widetilde{f}_1, \mathrm{Im}\,\widetilde{f}_1\}$	This proof
x_{fx64}	x_{fx64} (the scope)
(I7) y_{fx64}	$\widetilde{f}_{0,\mathrm{fx64}}$ (the statement)
$W_x, W_y \in \{0, \dots, 2^{128}-1\}$	The words of x and $\widetilde{f}_0$ (Definition A.5)
Assumption A3	(L4)

Its conclusion: $|\mathrm{roundAway}(x_{\mathrm{fx64}} 2^{64}/y_{\mathrm{fx64}})| \leq |x_{\mathrm{fx64}}| 2^{64}/|y_{\mathrm{fx64}}| + 1/2$

(L7) $|\mathrm{Re}\,\widetilde{\mu}_{\mathrm{fx64}}|,\ |\mathrm{Im}\,\widetilde{\mu}_{\mathrm{fx64}}| \leq (A+1)2^{64}/(L-1/2) + 1/2$

[(L5), (L6); Definition I.1, item 1, at /; (I7); (L1), (L3); Fact A.41, item 5]

(L8) $\Rightarrow\ |\mathrm{Re}\,\widetilde{\mu}_{\mathrm{fx64}}|,\ |\mathrm{Im}\,\widetilde{\mu}_{\mathrm{fx64}}| \leq J$

[(L7); J (the proof's block)]

(L9) $\forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\} : \ |\mathrm{fl}(\mathfrak{p}(\widetilde{\mu})\,\mathfrak{p}(\widetilde{f}_1))_{\mathrm{fx64}}| \le (A+1)^2/(L-1/2) + (A+1)/2^{65} + 1/2$

[LDL† (Algorithm 5), line 14; Definition I.1, item 1, at $\times$; roundAway (Definition I.1); Fact A.41, item 22; (L3), (L7); Fact A.41, item 8; expand]

(L10) $|zo_{\mathrm{fx64}}| \le 2(A+1)^2/(L-1/2) + 2(A+1)/2^{65} + 1$

[LDL† (Algorithm 5), line 14; Definition I.1, item 1, at $+$; (L9); $|x+y| \le |x| + |y|$ (Fact A.41, item 1)]

(L11) $|\widetilde{d}_{11,\mathrm{fx64}}| \le A + 1/2 + |zo_{\mathrm{fx64}}|$

[LDL† (Algorithm 5), line 18; Definition I.1, item 1, at $-$; (L2), (L10); Fact A.41, item 1]

(L12) $J,\ \sqrt{2}J,\ (A+1)^2/(L-1/2) + (A+1)/2^{65} + 1/2,\ 2(A+1)^2/(L-1/2) + 2(A+1)/2^{65} + 1 + A + 1/2 < 2^{127}$

[L, A, J (the proof's block); expand]

Lemma I.12, items 1 and 5 at each operation of LDL† (Algorithm 5), lines 7 to 18, on the child's Gram $(\widetilde{f}_0, \widetilde{f}_1, \widetilde{f}_0)$	This proof
(W_x, W_y)	$(W_{\mathfrak{p}(\widetilde{f}_1)}, W_{\widetilde{f}_0})$ at div; $W_{\mathrm{Im}\,\widetilde{\mu}}$ at neg; $(W_{\mathfrak{p}(\widetilde{\mu})}, W_{\mathfrak{p}(\widetilde{f}_1)})$ at mul; $(W_{\mathrm{fl}(\mathrm{Re}\,\widetilde{\mu}\,\mathrm{Re}\,\widetilde{f}_1)}, W_{\mathrm{fl}(\mathrm{Im}\,\widetilde{\mu}\,\mathrm{Im}\,\widetilde{f}_1)})$ at add; $(W_{\widetilde{f}_0}, W_{\widetilde{zo}})$ at sub (LDL†, lines 7 to 18)
o	div, neg, mul, add, sub (the scope)
W_{z_o}	W_x (the statement)
(I8) V	$\widetilde{f}_{0,\mathrm{fx64}}, \mathfrak{p}(\widetilde{f}_1)_{\mathrm{fx64}}$ (Definition A.5)
$W_x, W_y \in \{0, \dots, 2^{128}-1\}$	Words (Definition A.5)
$V \in \mathbb{Z}$	Definition A.5
$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	The scope
Assumption A1	(I4) at $W_{\widetilde{f}_0}$, $W_{\widetilde{f}_1}$
Assumption A2	(L2), (L3); A (the proof's block)
Assumption A4	(L4); item 1 at $W_{\widetilde{f}_0}$
Assumption A5	(L8), (L9), (L10), (L11), (L12)
Its item 1: $x_{\mathrm{fx64}} = V$	
Its item 5: $z_{o,\mathrm{fx64}} = V_o$	

(L13) $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[(I8); Definition I.1, item 1]

(L14) $\Rightarrow$ item 1

[(L13)]

(L15) $\Rightarrow$ item 2

[(L2), (L8), (L9), (L10), (L11), (L12); $\widetilde{l}_{10} = \mathrm{conj}\,\widetilde{\mu}$ (LDL† (Algorithm 5), line 12); $\widetilde{d}_{00} = \widetilde{f}_0$ (LDL†); $\forall a, b \in \mathbb{R} : \ |a+ib|^2 = a^2 + b^2$ (Fact A.41, item 1)]

□ (items 1 and 2)

Lemma I.42 (No overflow at the leaves [to table])**.** *A leaf's square root and inverse standard deviation hold their numbers. Let:*

- $n = 2^h \in \{512, 1024\}$*;*
- $\widetilde{d}$ *be a diagonal* $\widetilde{d}_{00}$ *or* $\widetilde{d}_{11}$ *of* deepest *(Algorithm 7) at a node of degree* 2*;*
- W_x *be a word of line 1 or 3 of* deepest *or of their counterparts at* $\widetilde{d}_{00}$*, on* $\widetilde{d}$*.*

Define:

- W_d*, the word that stores* $\widetilde{d}$*;*
- $\widetilde{r}$*, the number line 1 of* deepest *or its counterpart computes on* $\widetilde{d}$ *in* $\mathcal{F}_{\mathrm{fx}}$ *(Definition I.1);*
- $1/\widetilde{\sigma}$*, the number line 3 of* deepest *or its counterpart computes on* $\widetilde{d}$ *in* $\mathcal{F}_{\mathrm{fx}}$ *(Definition I.1);*
- $W_{\mathtt{INV}}$*, the word of* `FXP_INV_SIGMA`$[h]$ *[LO: fxp/fxp_consts.h:2058-2070];*

- *x, the number W_x's line computes in $\mathcal{F}_{\text{fx}}$ (Definition I.1);*
- *$x_{\text{fx64}} := 2^{64}x$ (Definition A.5).*

Assume:

(A1) $W_d = \widetilde{d}_{\text{fx64}} \bmod 2^{128}$;

(A2) $\widetilde{d} \in [0, 2^{19}]$.

Then

1. $W_x = x_{\text{fx64}} \bmod 2^{128}$;
2. $|x_{\text{fx64}}| < 2^{127}$.

Proof. (L1) $\widetilde{d}_{\text{fx64}} \in [0, 2^{83}]$

[assumption A2; $\widetilde{d}_{\text{fx64}} = 2^{64}\widetilde{d}$ (Definition A.5)]

(L2) $W_d = \widetilde{d}_{\text{fx64}}$

[assumption A1; (L1)]

(L3) $W_{\widetilde{r}} = Q(W_d)$

[Lemma I.10, item 7, at line 1 of deepest or its counterpart on $\widetilde{d}$; W_d (the statement)]

(L4) $\widetilde{r} = 2^{-64}\text{roundAway}(\sqrt{\widetilde{d}_{\text{fx64}}2^{64}})$

[Definition I.1, item 1, at $x := \widetilde{d}$; $\widetilde{r}$ (the statement); assumption A2]

(I1)

Lemma I.5 at $x := \widetilde{d}$	This proof
x	$\widetilde{d}$
W_x	W_d (L2)
W_z	$W_{\widetilde{r}}$ (L3); Q (Lemma I.10)
z	$\widetilde{r}$ (L4)
$x \in 2^{-64}\mathbb{Z},\ x_{\text{fx64}} \in \{0, \dots, 2^{128} - 1\}$	(L1); W_d, a word (Definition A.5)
Its conclusion: $W_z = z_{\text{fx64}}$	

(L5) $W_{\widetilde{r}} = \widetilde{r}_{\text{fx64}}$

[(I1)]

(L6) $\widetilde{r}_{\text{fx64}} = \text{roundAway}(\sqrt{\widetilde{d}_{\text{fx64}}2^{64}})$

[(L4); Definition A.5]

(L7) $\widetilde{r}_{\text{fx64}} \le \sqrt{2^{147}} + 1/2$

[(L1), (L6); roundAway (Definition I.1); Fact A.41, item 22; Fact A.41, item 5]

(L8) $\sqrt{2^{147}} + 1/2 \le 2^{82}$

[expand]

(L9) $W_{\texttt{INV}} \in [0, 2^{57})$

[`FXP_INV_SIGMA` [L0: `fxp/fxp_consts.h:2058-2070`]]

(I2)

Lemma I.3 at line 3 of deepest or its counterpart, on $(W_{\widetilde{r}}, W_{\texttt{INV}})$	This proof
x	$\widetilde{r}$ (the statement)
y	$2^{-64}W_{\texttt{INV}}$ (the statement)
W_x	$W_{\widetilde{r}}$ (L5)
W_y	$W_{\texttt{INV}}$ (the statement)
W_z	$W_{1/\widetilde{\sigma}}$ (Lemma I.10, item 7)
$x, y \in 2^{-64}\mathbb{Z},\ x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$	(L5), (L7), (L8), (L9)
Its conclusion: $W_z = z_{\text{fx64}} \bmod 2^{128}$	

(L10) $W_{1/\widetilde{\sigma}} = (1/\widetilde{\sigma})_{\text{fx64}} \bmod 2^{128}$

[(I2); z (Lemma I.3); Definition I.1, item 1, at $\times$]

(L11) $(1/\widetilde{\sigma})_{\text{fx64}} = \text{roundAway}(\widetilde{r}_{\text{fx64}}W_{\texttt{INV}}, 2^{64})$

[deepest (Algorithm 7), line 3 or its counterpart; Definition I.1, item 1, at $\times$; (L9)]

	Lemma I.12, items 1 and 2 at $(W_x, W_y) := (W_{\widetilde{r}}, W_{\texttt{INV}})$	This proof
	W_x	$W_{\widetilde{r}}$ (L5)
	W_y	$W_{\texttt{INV}}$ (the statement)
	V	$\widetilde{r}_{\text{fx64}}, W_{\texttt{INV}}$ (Definition A.5)
(I3)	$W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	Words (Definition A.5)
	$V \in \mathbb{Z}$	Definition A.5
	Assumption A1	(L5); $W_{\texttt{INV}}$ (the statement)
	Assumption A2	(L7), (L8), (L9)
	Its item 1: $x_{\text{fx64}} = V$	
	Its item 2: $\lvert\text{roundAway}(x_{\text{fx64}} y_{\text{fx64}}, 2^{64})\rvert \le \lvert x_{\text{fx64}}\rvert\lvert y_{\text{fx64}}\rvert / 2^{64} + 1/2$	

(L12) $|(1/\widetilde{\sigma})_{\text{fx64}}| \le 2^{82} 2^{57} / 2^{64} + 1/2$

[(I3); (L7), (L8), (L9), (L11)]

(L13) $2^{82} 2^{57} / 2^{64} + 1/2 < 2^{127}$

[expand]

(L14) $\Rightarrow$ item 1

[(L5), (L10)]

(L15) $\Rightarrow$ item 2

[(L7), (L8), (L12), (L13)]

□ (items 1 and 2)

Lemma I.43 (The range of the tree's computed diagonals [to table])**.** *Every diagonal the tree recursion computes lies in* $[d_{\text{lo}}(1 - \max_k \chi_k),\ d_{\text{hi}}(1 + \max_k \chi_k)]$*, and so in* $[2^8, 2^{19}]$*. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5), of degree* $n = 2^h \in \{512, 1024\}$*;*
- $(\nu_k)_{0 \le k \le h-1}$ *be a path of the key's tree (Definition I.32).*

Define:

- *The key bounds*
  - m_0*, that of Definition A.37;*
  - M_0*, that of Definition A.37;*
  - $d_{\text{lo}} := \min(m_0, q^2/M_0)$ *(Definition A.37);*
  - $d_{\text{hi}} := \max(M_0, q^2/m_0)$ *(Definition A.37);*
  - $\bar{\varsigma} := d_{\text{hi}}/d_{\text{lo}}$ *(Definition A.37);*
  - $\forall 1 \le k \le h-1 :\ \bar{\kappa}_k := (\bar{\varsigma} - 1)^2/(4\bar{\varsigma})$ *(Proposition 5.8, item 2);*
  - E_{00}*, that of Definition A.36, item 5;*
- *The root bounds*
  - $e_{00} := E_{00}/m_0$ *(Lemma I.25);*
  - $\bar{G} := M_0(1 + e_{00})$ *(Lemma I.27);*
  - $Z_I := 1 + \zeta \bar{G}/q^2$ *(Lemma I.27);*
  - $\chi_0 := \max(e_{00},\ Z_I/(1 - e_{00}) - 1)$*;*
- *The error chain*
  - $\forall \chi \in [0, 1) :\ m_1(\chi) := d_{\text{lo}}(1 - \chi)$ *(Definition I.28);*
  - $\forall \chi \in [0, 1) :\ u_0(\chi) := \zeta/(2m_1(\chi))$ *(Definition I.28);*
  - $\mathcal{U}^0_\kappa$*, that of Definition I.28;*
  - $\mathcal{A} := \{\chi : 0 \le \chi < 1,\ u_0(\chi) < 1\}$ *(Definition I.32);*
  - $\forall 1 \le k \le h-1 :\ \vartheta_{k-1} := (1 + \chi_{k-1})/(1 - \chi_{k-1})$ *(Definition I.32);*
  - $\forall 1 \le k \le h-1 :\ \hat{\kappa}_k := \vartheta_{k-1}\bar{\kappa}_k + (\vartheta_{k-1} - 1)/2$ *(Definition I.32 at* $\kappa_k := \bar{\kappa}_k$*);*
  - $\forall 1 \le k \le h-1 :\ \chi_k := \mathcal{U}^0_{\hat{\kappa}_k}(\chi_{k-1})$ *(Definition I.32);*
- *The diagonals*
  - $\forall k \in \{0, \dots, h-1\}\ \forall j \in \{00, 11\} :\ \widetilde{d}^{\nu_k}_j$*, those of Corollary I.33.*

Measured:

- $\forall k \le h-1:\ \chi_k \in \mathcal{A}$ *at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/fx/chain_admissible.py];*
- $e_{00} < 1$ *at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/tree/general_assume.py].*

Then

1. $\forall k \in \{0, \dots, h-1\}\ \forall \psi:\ \widetilde{d}_{00}^{\nu_k}(\psi), \widetilde{d}_{11}^{\nu_k}(\psi) \in [d_{\mathrm{lo}}(1 - \max_j \chi_j),\ d_{\mathrm{hi}}(1 + \max_j \chi_j)]$;
2. $\forall k \in \{0, \dots, h-1\}\ \forall \psi:\ \widetilde{d}_{00}^{\nu_k}(\psi), \widetilde{d}_{11}^{\nu_k}(\psi) \in [2^8, 2^{19}]$.

Proof.

DEFINES g_{00}, the root node's first diagonal over $\mathbb{R}$ (Lemma I.25)
DEFINES $\widetilde{d}_{00} := \widetilde{g}_{00}$ (Lemma I.25)
DEFINES $d_{11} := q^2/g_{00}$ (Lemma I.27)
DEFINES $\widetilde{d}_{11}$, its computed value, that of Lemma I.26 at each ψ
DEFINES T, d_j^ν and $\widetilde{d}_j^\nu$, $\nu \in \mathrm{Sub}(T)$, $j \in \{00, 11\}$, those of Corollary I.33 at the checked key
DEFINES Ψ_n, that of Fact A.43 at $m := n$

(L1) $\forall k \in \{0, \dots, h-1\}\ \forall j \in \{00, 11\}\ \forall \psi:\ d_j^{\nu_k}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$
[Proposition 5.8, item 1, at the checked key (the statement)]

(I1)

Lemma I.25 at the checked key and at every $\psi' \in \Psi_n$	This proof
ψ	ψ' (the proof's block)
Its conclusion: $\widetilde{d}_{00}(\psi)\ \mathcal{I}\left(e_{00}^{\pm}, 0\right)\ g_{00}(\psi)$	

(L2) $\forall \psi' \in \Psi_n:\ \widetilde{d}_{00}(\psi')\ \mathcal{I}\left(e_{00}^{\pm}, 0\right)\ g_{00}(\psi')$
[(I1)]

(L3) $e_{00} < 1$
[the second measured row]

(L4) $m_0 > 0$
[Proposition 5.8, item 8, at the checked key]

(I2)

Lemma I.27 at the checked key and at every $\psi' \in \Psi_n$	This proof
ψ	ψ' (the proof's block)
Assumption A1	(L4)
Assumption A2	(L3)
Its conclusion: $\widetilde{d}_{11}(\psi)\ \mathcal{I}\left((Z_I/(1-e_{00}) - 1)^{\pm}, 0\right)\ d_{11}(\psi)$	

(L5) $\forall \psi' \in \Psi_n:\ \widetilde{d}_{11}(\psi')\ \mathcal{I}\left(\left(\frac{Z_I}{1-e_{00}} - 1\right)^{\pm}, 0\right)\ d_{11}(\psi')$
[(I2)]

(L6) $e_{00} \le \chi_0$
[χ_0 (the statement); $a \le \max(a, b)$ (Fact A.41, item 20)]

(L7) $Z_I/(1 - e_{00}) - 1 \le \chi_0$
[χ_0 (the statement); $b \le \max(a, b)$ (Fact A.41, item 20)]

(L8) $\forall \psi' \in \Psi_n:\ \widetilde{d}_{00}(\psi')\ \mathcal{I}\left(\chi_0^{\pm}, 0\right)\ g_{00}(\psi')$
[(L2), (L6); $\mathcal{I}\,(\mathcal{I}_0, \mathcal{I}_1)$ (Definition A.10)]

(L9) $\forall \psi' \in \Psi_n:\ \widetilde{d}_{11}(\psi')\ \mathcal{I}\left(\chi_0^{\pm}, 0\right)\ d_{11}(\psi')$
[(L5), (L7); $\mathcal{I}\,(\mathcal{I}_0, \mathcal{I}_1)$ (Definition A.10)]

(L10) $\forall k \le h-1:\ \chi_k \in \mathcal{A}$
[the first measured row]

Corollary I.33, item 1 at the path $(\nu_k)_{k\le h-1}$	This proof
Shared: $(f,g,F,G), n, h,\ T, d_j^\nu, \widetilde{d}_j^\nu,\ (\nu_k)_{0\le k\le h-1}, \chi_0$	
(f,g,F,G) checked key of degree $n=2^h$	The statement
(I3) $(\nu_k)_{0\le k\le h-1}$ a path of T $\chi_0 \in [0,1)$	The statement (L10); $\mathcal{A}$ (Definition I.32)
Assumption A1	(L8)
Assumption A2	(L9); Fact A.33, item 4
Assumption A3	(L10)
Its conclusion: $\forall k \le h-1\ \forall j \in \{00,11\}\ \forall \psi:\ \widetilde{d}_j^{\nu_k}(\psi)\ \mathcal{I}\left(\chi_k^{\pm}, 0\right)\ d_j^{\nu_k}(\psi)$	

(L11) $\forall k \le h-1\ \forall j \in \{00,11\}\ \forall \psi:\ \widetilde{d}_j^{\nu_k}(\psi)\ \mathcal{I}\left(\chi_k^{\pm}, 0\right)\ d_j^{\nu_k}(\psi)$
[(I3)]

(L12) $\max_j \chi_j \le 1/2$
[[gate: `verify/gates/fx/node_chi.py`], on the proved bounds of Proposition 5.8, items 1 to 4, in both modes, at the checked key (the statement)]

(L13) $[d_{\mathrm{lo}}(1-\max_j \chi_j),\ d_{\mathrm{hi}}(1+\max_j \chi_j)] \subset [2^8, 2^{19}]$
[[gate: `verify/gates/fx/node_diag.py`], on the proved bounds of Proposition 5.8, items 1 to 4, in both modes, at the checked key (the statement)]

(L14) $\forall k \in \{0,\dots,h-1\}\ \forall j \in \{00,11\}\ \forall \psi:\ \widetilde{d}_j^{\nu_k}(\psi) \in [d_j^{\nu_k}(\psi)(1-\chi_k),\ d_j^{\nu_k}(\psi)(1+\chi_k)]$
[(L1), (L11); $\mathcal{I}(\mathcal{I}_0, \mathcal{I}_1)$ (Definition A.10)]

(L15) $\forall k \in \{0,\dots,h-1\}\ \forall \psi:\ \widetilde{d}_{00}^{\nu_k}(\psi), \widetilde{d}_{11}^{\nu_k}(\psi) \in [d_{\mathrm{lo}}(1-\max_j \chi_j),\ d_{\mathrm{hi}}(1+\max_j \chi_j)]$
[(L1), (L12), (L14); Fact A.41, item 8]

(L16) $\forall k \in \{0,\dots,h-1\}\ \forall \psi:\ \widetilde{d}_{00}^{\nu_k}(\psi), \widetilde{d}_{11}^{\nu_k}(\psi) \in [2^8, 2^{19}]$
[(L13), (L15)]

(L17) $\Rightarrow$ item 2
[(L16)]

(L18) $\Rightarrow$ item 1
[(L15)]

□ (items 1 and 2)

Lemma I.44 (No overflow below the root [to table]). *The tree's splits and LDL steps below the root do not overflow. Let:*

- *(f,g,F,G) be a checked key (Definition 5.5), of degree $n = 2^h \in \{512, 1024\}$;*
- *W_x be a word of the tree recursion, in either center's mode, one of:*
  - *$\exists k \in \{2,\dots,h\}$: a word of $\mathrm{split}_{\mathrm{sa}}$ (Algorithm 3) at $m = 2^k$;*
  - *$\exists k \in \{1,\dots,h-1\}$: a word of $\mathrm{LDL}^\dagger$ (Algorithm 5) below the root at $m = 2^k$.*

Define:

- *x, the number W_x's line computes in $\mathcal{F}_{\mathrm{fx}}$ (Definition I.1);*
- *$x_{\mathrm{fx64}} := 2^{64}x$ (Definition A.5).*

Then

1. *$W_x = x_{\mathrm{fx64}} \bmod 2^{128}$;*
2. *$|x_{\mathrm{fx64}}| < 2^{127}$.*

Proof.

DEFINES D_k, $0 \le k \le h-1$: the numbers of the diagonals' words at the nodes of depth k

DEFINES X_k, $0 \le k \le h-2$: the numbers of the words of the self-adjoint split at a node of depth k and of the $LDL^\dagger$ steps at its children

DEFINES $B_{fg} := 31$ at $n = 512$ and 15 at $n = 1024$ [L0: `kgen_gauss.c:14-16`] (Definition 5.5)

DEFINES $\widetilde{\hat{p}}$: an image of f, g, F or G, or its negation, ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 1

DEFINES b_{00}, b_{01}, b_{10}, b_{11}: the images of g, $-f$, G and $-F$ line 1 writes

DEFINES M_{FG}: the M_{h-1} of Lemma I.34 at $B := 127$

DEFINES M_{fg}: the M_{h-1} of Lemma I.34 at $B := B_{fg}$

Lemma I.39, item 1	This proof
$(f, g, F, G), n$	$(f, g, F, G), n$ (the statement)
W_x	$W_{\widetilde{d}_{11}}$ (ffsamp, line 6)
$n \in \{512, 1024\}$	Definition 5.5, item 1
(I1) (f, g, F, G) key of degree n	The statement
W_x a word of the root's $LDL^\dagger$ step	$\widetilde{d}_{11}$ (ffsamp (Algorithm 6), line 6)
Assumption A1	Definition 5.5, item 2
Assumption A2	Definition 5.5, item 3
Its conclusion: $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	

(L1) $W_{\widetilde{d}_{11}} = \widetilde{d}_{11,\mathrm{fx64}} \bmod 2^{128}$ [(I1)]

Lemma I.34 at $j := h-1$	This proof
Shared: h	
p	$p \in \{g, f, G, F\}$ (the statement)
B	127 (the statement)
W_x	$W_{\widetilde{\hat{p}}}$, $\widetilde{\hat{p}} \in \{\widetilde{\hat{g}}, \widetilde{\hat{f}}, -\widetilde{\hat{f}}, \widetilde{\hat{G}}, \widetilde{\hat{F}}, -\widetilde{\hat{F}}\}$ (the proof's block)
M_{h-1}	M_{FG} (the proof's block)
$h \in \{3, \ldots, 10\}$	$n \in \{512, 1024\}$ (the statement)
$p \in \{-128, \ldots, 127\}^{2^h}$	Definition 5.5, items 2 and 3; $B_{fg} \le 127$ (B_{fg}, the proof's block); $B \le 127$ (B, the rows above)
$B \in [0, 127]$	127
(I2) W_x a pair of words at stage j	ffSampling$^{\mathcal{F}}$, line 1 (the proof's block)
Assumption A1	Definition 5.5, items 2 and 3; $B_{fg} \le 127$ (B_{fg}, the proof's block)
Its item 1: $\forall j \le h-1\ \forall x \in X_j :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 2: $\forall j \le h-1\ \forall x \in X_j :\ \lvert x_{\mathrm{fx64}} \rvert \le M_j$	
Its item 3: $\forall x \in X^- :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 4: $\forall x \in X^- :\ \lvert x_{\mathrm{fx64}} \rvert \le M_{h-1}$	
Its item 5: $\forall j \le h-1 :\ M_j \le c^{h-1}(1.4143\, B2^{64} + 2) - 2$	
Its item 6: $c^{h-1}(1.4143\, B2^{64} + 2) - 2 < 2^{81}$	

(L2) $\forall \widetilde{\hat{p}} :\ W_{\widetilde{\hat{p}}} = \widetilde{\hat{p}}_{\mathrm{fx64}} \bmod 2^{128}$ [items 1 and 3 of (I2)]

(L3) $\forall \widetilde{\hat{p}} :\ \lvert \widetilde{\hat{p}}_{\mathrm{fx64}} \rvert \le M_{FG}$ [items 2 and 4 of (I2); M_{FG} (the proof's block)]

(L4) $M_{FG} < 2^{81}$ [items 5 and 6 of (I2)]

Lemma I.34 at $j := h - 1$	This proof
Shared: h	
p	$p \in \{g, f\}$ (the statement)
B	B_{fg} (the proof's block)
W_x	$W_{\widetilde{\hat{p}}}$, $\widetilde{\hat{p}} \in \{\widetilde{\hat{g}}, \widetilde{\hat{f}}, -\widetilde{\hat{f}}\}$ (the proof's block)
M_{h-1}	M_{fg} (the proof's block)
$h \in \{3, \dots, 10\}$	$n \in \{512, 1024\}$ (the statement)
(I3) $p \in \{-128, \dots, 127\}^{2^h}$	Definition 5.5, item 2; $B \le 127$ (B, the rows above)
$B \in [0, 127]$	B_{fg} (the proof's block)
W_x a pair of words at stage j	ffSampling$^{\mathcal{F}}$, line 1 (the proof's block)
Assumption A1	Definition 5.5, item 2
Its item 2: $\forall j \le h-1\ \forall x \in X_j :\ \lvert x_{\text{fx64}}\rvert \le M_j$	
Its item 4: $\forall x \in X^- :\ \lvert x_{\text{fx64}}\rvert \le M_{h-1}$	
Its item 5: $\forall j \le h-1 :\ M_j \le c^{h-1}(1.4143\, B2^{64} + 2) - 2$	
Its item 6: $c^{h-1}(1.4143\, B2^{64} + 2) - 2 < 2^{81}$	
(L5) $\lvert b_{00,\text{fx64}}\rvert,\ \lvert b_{01,\text{fx64}}\rvert \le M_{fg}$	
	[items 2 and 4 of (I3)]
(L6) $M_{fg} < 2^{81}$	
	[items 5 and 6 of (I3)]

Lemma I.35, item 1 at the root node's first diagonal	This proof
Shared: b_{jk}	
Y_0, Y_1	$\{b_{00}, b_{01}\}, \{b_{10}, b_{11}\}$ (the proof's block)
M_0, M_1	M_{fg}, M_{FG} (the proof's block)
W_x	$W_{\widetilde{g_{00}}}$ (Gram (Algorithm 13), line 6)
(I4) b_{jk} arrays of pairs of words of ffSampling$^{\mathcal{F}}$, line 1	b_{jk} (the proof's block)
$M_0, M_1 \ge 0$	M_{fg}, M_{FG} (the proof's block)
W_x a word of Gram on the b_{jk}	$\widetilde{g}_{00}$ (Gram, line 6)
Assumption A1	(L2)
Assumption A2	(L3), (L5)
Assumption A3	(L4), (L6)
Its conclusion: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
(L7) $W_{\widetilde{g_{00}}} = \widetilde{g}_{00,\text{fx64}} \bmod 2^{128}$	
	[(I4)]
(L8) $\forall x \in D_0 :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
	[(L1), (L7); D_0 (the proof's block)]
(L9) $\forall k \le h-1\ \forall x \in D_k :\ x \in [2^8, 2^{19}]$	
	[Lemma I.43, item 2, at the checked key (the statement); D_k (the proof's block)]

Lemma I.40 at every $k \le h-2$, under $\forall x \in D_k :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	This proof
h	$h-k$ (the scope)
$\widetilde{d}$	$\widetilde{d},\ \forall \psi :\ \widetilde{d}(\psi) \in D_k$ (the proof's block)
W_x	$W_x,\ x \in X_k$ (the proof's block)
$h \in \{2, \ldots, 10\}$	$k \le h-2$ (the scope); $n \in \{512, 1024\}$ (Definition 5.5, item 1)
(I5) $\widetilde{d}$ a parent's diagonal array	D_k (the proof's block)
W_x a word of $\widetilde{\mathrm{split}}_{\mathrm{sa}}$	X_k (the proof's block)
Assumption A1	The scope
Assumption A2	(L9)
Its item 1: $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 2: $\lvert x_{\mathrm{fx64}} \rvert < 2^{127}$	

Lemma I.41 at every $k \le h-2$, under $\forall x \in D_k :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	This proof
h	$h-k$ (the scope)
$\widetilde{d}$	$\widetilde{d},\ \forall \psi :\ \widetilde{d}(\psi) \in D_k$ (the proof's block)
W_x	$W_x,\ x \in X_k$ (the proof's block)
$h \in \{2, \ldots, 10\}$	$k \le h-2$ (the scope); $n \in \{512, 1024\}$ (Definition 5.5, item 1)
(I6) $\widetilde{d}$ a parent's diagonal array	D_k (the proof's block)
W_x a word of $\mathrm{LDL}^{\dagger}$	X_k (the proof's block)
Assumption A1	The scope
Assumption A2	(L9)
Its item 1: $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 2: $\lvert x_{\mathrm{fx64}} \rvert < 2^{127}$	

(L10) $\forall k \le h-2 :\ [\forall x \in D_k :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}] \Rightarrow\ \forall x \in X_k :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128} \wedge \lvert x_{\mathrm{fx64}} \rvert < 2^{127}$

[items 1 and 2 of (I5); items 1 and 2 of (I6)]

(L11) $\forall k \le h-2 :\ D_{k+1} \subseteq X_k$

[$\widetilde{\mathrm{split}}_{\mathrm{sa}}$ (Algorithm 3), line 4; $\mathrm{LDL}^{\dagger}$ (Algorithm 5), line 18; D_k, X_k (the proof's block)]

(L12) $\forall k \le h-3 :\ [\forall x \in D_k :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}] \Rightarrow\ [\forall x \in D_{k+1} :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}]$

[(L10), (L11)]

(L13) $\forall k \le h-2\ \forall x \in D_k :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[induction on k: (L8) the base; (L12) the step]

(L14) $\forall k \le h-2\ \forall x \in X_k :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[(L10), (L13)]

(L15) $\forall k \le h-2\ \forall x \in X_k :\ \lvert x_{\mathrm{fx64}} \rvert < 2^{127}$

[(L10), (L13)]

(L16) $\Rightarrow$ item 1

[(L14); W_x (the statement) a word of some X_k (X_k, the proof's block)]

(L17) $\Rightarrow$ item 2

[(L15); W_x (the statement) a word of some X_k (X_k, the proof's block)]

$\square$ (items 1 and 2)

I.3.4 No overflow in the center's first computation

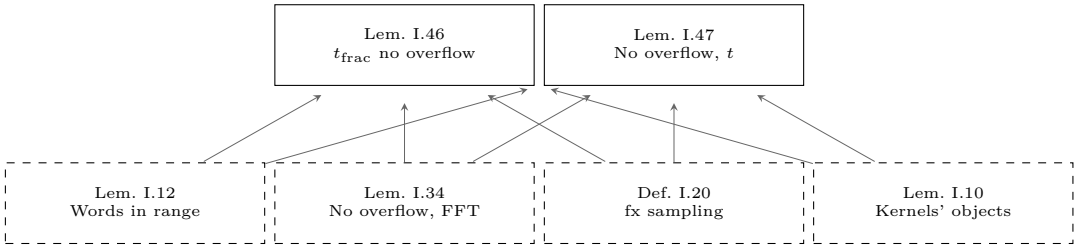


Figure 78: Dependencies, Appendix I.3.4.

Fact I.45 (The signer's 16-bit inputs [to table])**.** The hashed message's coefficients and the residues of the center t_{frac} fit in 16 bits. Let:

- $n \in \mathbb{Z}_{>0}$, a degree;
- $\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$, a hashed message, q that of Table 5, as $\text{center}_{\text{frac}}$ (Algorithm 17) takes it (Require);
- f, F, as $\text{center}_{\text{frac}}$ (Algorithm 17) takes them (Require).

Define:

- $\forall j \in \{0,1\}:\ qt_{\text{frac},j}$, the residues of $\text{center}_{\text{frac}}$ (Algorithm 17), line 4, at $(\mathsf{h}(\mathsf{m}), f, F)$.

We have

1. $\forall k < n:\ \mathsf{h}(\mathsf{m})_{[k]} \in \{0, \dots, 2^{16}-1\}$ [L0: `util.c:38-42`] [L0: `fxp/sign_fxcore.c:68-71`] $(q-1 < 2^{16})$;
2. $\forall j \in \{0,1\}\ \forall k < n:\ qt_{\text{frac},j,[k]} \in [-2^{15}, 2^{15})$ [L0: `fxp/sign_fxcore.c:75-78`] $(qt_{\text{frac},j,[k]} \in [-q/2, q/2)$, $\text{center}_{\text{frac}}$ (Algorithm 17), line 4; $q/2 < 2^{15})$.

Lemma I.46 (No overflow in the center t_{frac} [to table])**.** *The center t_{frac}'s first computation does not overflow. Let:*

- *$h \in \{3, \dots, 10\}$;*
- *(f, g, F, G) be a key (line 3 of keygen (Algorithm 11)) of degree $n = 2^h$;*
- *$\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ be a hashed message (Definition A.25);*
- *W_x be a word of $\text{center}_{\text{frac}}$ (Algorithm 17), lines 7 and 12 (`fractional_mode` $= 1$).*

Define:

- *x, the number W_x's line computes in $\mathcal{F}_{\text{fx}}$ (Definition I.1);*
- *$x_{\text{fx64}} := 2^{64}x$ (Definition A.5).*

Then

1. *$W_x = x_{\text{fx64}} \bmod 2^{128}$;*
2. *$|x_{\text{fx64}}| < 2^{127}$.*

Proof.

DEFINES $c = 2(1 + 2^{-65})$
DEFINES $M_T = c^9(1.4143\, q 2^{64} + 2) - 2$
DEFINES R_0: the residues $qt_{\text{frac},j,[k]}$ of line 4, each the number its loaded word stores
DEFINES X_{in}: the numbers of the input pairs of the FFT of line 7, each a pair of residues of R_0
DEFINES X_{FFT}: the numbers of the pairs of the FFT of line 7
DEFINES X_{sc}: the numbers of the scaled words of line 12
DEFINES $M(a, b)$: the number whose word `fxp_mul` (Lemma I.3) returns on the words of a and b, read through $\cdot_{\text{fx64}}$

(L1) $\forall r \in R_0:\ |r| < q$ [$\text{center}_{\text{frac}}$ (Algorithm 17), line 4]

(L2) $q2^{64} < 2^{127}$

[expand]

(L3) $\forall k < n :\ \mathsf{h}(\mathsf{m})_{[k]} \in \{0, \ldots, 2^{16} - 1\}$

[Fact I.45, item 1, at $\mathsf{h}(\mathsf{m})$ and the key (the statement)]

(L4) $\forall j \in \{0, 1\}\ \forall k < n :\ qt_{\mathrm{frac},j,[k]} \in [-2^{15}, 2^{15})$

[Fact I.45, item 2, at $\mathsf{h}(\mathsf{m})$ and the key (the statement)]

Lemma I.10, item 12 at $\mathtt{logn} = h$	This proof
Shared: h	
$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
$\mathtt{hm}$	$\mathsf{h}(\mathsf{m})$ (the statement)
$\mathtt{qtfrac0}, \mathtt{qtfrac1}$	$qt_{\mathrm{frac},0}, qt_{\mathrm{frac},1}$ ($\mathrm{center}_{\mathrm{frac}}$ (Algorithm 17), line 4)
$h \in \{2, \ldots, 10\}$	$h \in \{3, \ldots, 10\}$ (the statement)
each input array of words (I1)	The words the center's first computation loads (Definition A.5)
Assumption A5	$h \in \{3, \ldots, 10\}$ (the statement)
Assumption A6	(L3)
Assumption A7	(L4)
Its conclusion: The two objects of the center's first computation in $\mathcal{O}$ return their algorithms' words; each coefficient is loaded as the word $(0, \mathsf{h}(\mathsf{m})_{[k]})$, each residue as the word $(0, qt_{\mathrm{frac},j,[k]})$, sign-extended.	

(L5) $\forall r \in R_0 :\ W_r = r_{\mathrm{fx64}} \bmod 2^{128}$

[(I1): the loads; Definition A.5]

(L6) $\forall r \in R_0 :\ r_{\mathrm{fx64}} = r2^{64}$

[Definition A.5]

Lemma I.34, items 8 and 9 at the FFT of line 7	This proof
Shared: h, c	
M	$\sqrt{2}\, q2^{64}$
Y_0	X_{in} (the proof's block)
$Y_j,\ 1 \le j \le h-1$	X_{FFT} (the proof's block)
$M \ge 0$ (I2)	$q2^{64} > 0$; expand
Y_j written at stage j of $\widetilde{\mathrm{FFT}}$ on Y_0	The FFT of line 7 (I1)
Assumption A2	(L5)
Assumption A3	(L6), (L1); $\lvert a + ib\rvert^2 = a^2 + b^2$ (Fact A.41, item 1)
Assumption A4	$h - 1 \le 9$; expand
Its item 8: $\forall j \le h-1\ \forall y \in Y_j :\ W_y = y_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 9: $\forall j \le h-1\ \forall y \in Y_j :\ \lvert y_{\mathrm{fx64}}\rvert \le c^{h-1}(M+2) - 2$	

(L7) $\forall x \in X_{\mathrm{FFT}} :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[item 8 of (I2)]

(L8) $c^{h-1}(\sqrt{2}\, q2^{64} + 2) - 2 \le M_T$

[M_T, c (the proof's block); $h - 1 \le 9$; expand]

(L9) $\forall x \in X_{\mathrm{FFT}} :\ \lvert x_{\mathrm{fx64}}\rvert \le M_T$

[item 9 of (I2); (L8)]

(L10) $M_T < 2^{88}$

[M_T, c (the proof's block); expand]

(L11) $\Rightarrow\ \forall x \in X_{\mathrm{FFT}} :\ \lvert x_{\mathrm{fx64}}\rvert < 2^{88}$

[(L9), (L10)]

(L12) $\lvert\widetilde{(1/q)}_{\mathrm{fx64}}\rvert < 2^{51}$

[Definition I.20: the stored $1/q$ [L0: `fxp/fxp_consts.h:2090-2091`]]

(L13) $\forall x \in X_{\mathrm{FFT}}\ \forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\} :\ |\mathfrak{p}(x)_{\mathrm{fx64}}|2^{51}/2^{64} + 1/2 < 2^{127}$

[(L11); $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \le |x|$ (Fact A.41, item 1); expand]

Lemma I.12, items 1, 2 and 5 at each part $\mathfrak{p}(x)$ of every $x \in X_{\mathrm{FFT}}$ and the stored $\widetilde{(1/q)}$, the products of line 12	This proof
(W_x, W_y)	$(W_{\mathfrak{p}(x)}, W_{\widetilde{(1/q)}})$ ($\mathrm{center}_{\mathrm{frac}}$, line 12)
o	mul (the scope)
V	$\mathfrak{p}(x)_{\mathrm{fx64}}, \widetilde{(1/q)}_{\mathrm{fx64}}$ (Definition A.5)
$W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	Words (Definition A.5)
$V \in \mathbb{Z}$	Definition A.5
(I3) $o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	The scope
Assumption A1	(L7); the stored word of $1/q$ (Definition I.20)
Assumption A2	(L11), (L12); $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
Assumption A4	$o =$ mul (the scope)
Assumption A5	Item 2; (L12), (L13)
Its item 1: $x_{\mathrm{fx64}} = V$	
Its item 2: $\lvert\mathrm{roundAway}(x_{\mathrm{fx64}} y_{\mathrm{fx64}}, 2^{64})\rvert \le \lvert x_{\mathrm{fx64}}\rvert\lvert y_{\mathrm{fx64}}\rvert/2^{64} + 1/2$	
Its item 5: $z_{o,\mathrm{fx64}} = V_o$	

(L14) $\forall x \in X_{\mathrm{FFT}}\ \forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\} :\ |M(\mathfrak{p}(x), \widetilde{(1/q)})_{\mathrm{fx64}}| \le |\mathfrak{p}(x)_{\mathrm{fx64}}|2^{51}/2^{64} + 1/2$

[(I3); (L12); M (the proof's block)]

(L15) $\forall x \in X_{\mathrm{sc}} :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[(I1); (I3); Definition I.1, item 1, at $\times$; X_{sc} (the proof's block)]

(L16) $\Rightarrow$ item 1

[(L5), (L7), (L15); X_{in}, X_{FFT}, X_{sc} (the proof's block)]

(L17) $\Rightarrow$ item 2

[(L1), (L2), (L6), (L11), (L13), (L14); $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \le |x|$ (Fact A.41, item 1); X_{in}, X_{FFT}, X_{sc} (the proof's block)]

□ (items 1 and 2)

Lemma I.47 (No overflow in the center t [to table])**.** *The center t's first computation does not overflow. Let:*

- $h \in \{3, \dots, 10\}$*;*
- (f, g, F, G) *be a key (line 3 of* keygen *(Algorithm 11)) of degree $n = 2^h$;*
- $\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ *be a hashed message (Definition A.25);*
- W_x *be a word of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10), lines 9, 16 and 18 (*`fractional_mode` $= 0$*).*

Define:

- x*, the number W_x's line computes in $\mathcal{F}_{\mathrm{fx}}$ (Definition I.1);*
- $x_{\mathrm{fx64}} := 2^{64}x$ *(Definition A.5).*

Assume:

(A1) $\forall a < n :\ f_{[a]}, g_{[a]} \in [-127, 127]$ *[L0: `fxp/sign_fxcore.c: 128-141`];*

(A2) $\forall a < n :\ F_{[a]}, G_{[a]} \in [-127, 127]$ *[L0: `kgen_ntru.c: 1887-1895`].*

Then

1. $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$*;*
2. $|x_{\mathrm{fx64}}| < 2^{127}$*.*

Proof.

DEFINES $c = 2(1 + 2^{-65})$

DEFINES $M_T = c^9(1.4143\, q2^{64} + 2) - 2$

DEFINES $M_b = c^9(1.4143 \cdot 127 \cdot 2^{64} + 2) - 2$

DEFINES X_{in}: the numbers of the input pairs of the FFT of $\mathsf{h}(\mathsf{m})$, line 9, each a pair of coefficients of $\mathsf{h}(\mathsf{m})$

DEFINES X_{FFT}: the numbers of the pairs of the FFT of $\mathsf{h}(\mathsf{m})$, line 9

DEFINES X_{prod}: the products $x \otimes \widetilde{b}$, $x \in X_{\text{FFT}}$, $\widetilde{b}$ an image $\widetilde{b}_{01}$ or $\widetilde{b}_{11}$, lines 16 and 18

DEFINES X_{sc}: the numbers of the scaled words of lines 16 and 18

DEFINES $M(a, b)$: the number whose word `fxp_mul` (Lemma I.3) returns on the words of a and b, read through $\cdot_{\text{fx64}}$

(L1) $\forall k < n :\ \mathsf{h}(\mathsf{m})_{[k]} \in [0, q)$

[$\mathsf{h}(\mathsf{m})$ (the statement)]

(L2) $q2^{64} < 2^{127}$

[expand]

(L3) $\forall k < n :\ \mathsf{h}(\mathsf{m})_{[k]} \in \{0, \dots, 2^{16} - 1\}$

[Fact I.45, item 1, at $\mathsf{h}(\mathsf{m})$ and the key (the statement)]

(L4) $\forall j \in \{0, 1\}\ \forall k < n :\ qt_{\text{frac},j,[k]} \in [-2^{15}, 2^{15})$

[Fact I.45, item 2, at $\mathsf{h}(\mathsf{m})$ and the key (the statement)]

(I1)

Lemma I.10, item 12 at `logn` $= h$	This proof
Shared: h	
$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
`hm`	$\mathsf{h}(\mathsf{m})$ (the statement)
`qtfrac0`, `qtfrac1`	$qt_{\text{frac},0}, qt_{\text{frac},1}$ ($\text{center}_{\text{frac}}$ (Algorithm 17), line 4)
$h \in \{2, \dots, 10\}$	$h \in \{3, \dots, 10\}$ (the statement)
each input array of words	The words the center's first computation loads (Definition A.5)
Assumption A5	$h \in \{3, \dots, 10\}$ (the statement)
Assumption A6	(L3)
Assumption A7	(L4)

Its conclusion: The two objects of the center's first computation in $\mathcal{O}$ return their algorithms' words; each coefficient is loaded as the word $(0, \mathsf{h}(\mathsf{m})_{[k]})$, each residue as the word $(0, qt_{\text{frac},j,[k]})$, sign-extended.

(L5) $\forall k < n :\ W_{\mathsf{h}(\mathsf{m})_{[k]}} = \mathsf{h}(\mathsf{m})_{[k],\text{fx64}} \bmod 2^{128}$

[(I1): the loads; Definition A.5]

(L6) $\forall k < n :\ \mathsf{h}(\mathsf{m})_{[k],\text{fx64}} = \mathsf{h}(\mathsf{m})_{[k]} 2^{64}$

[Definition A.5]

Lemma I.34, items 8 and 9 at the FFT of line 9	This proof
Shared: h, c	
M	$\sqrt{2}\,q2^{64}$
Y_0	X_{in} (the proof's block)
$Y_j,\ 1 \le j \le h-1$	X_{FFT} (the proof's block)
(I2) $M \ge 0$	$q2^{64} > 0$; expand
Y_j written at stage j of $\widetilde{\text{FFT}}$ on Y_0	The FFT of line 9 (I1)
Assumption A2	(L5)
Assumption A3	(L6), (L1); $\lvert a+ib\rvert^2 = a^2+b^2$ (Fact A.41, item 1)
Assumption A4	$h-1 \le 9$; expand
Its item 8: $\forall j \le h-1\ \forall y \in Y_j :\ W_y = y_{\text{fx64}} \bmod 2^{128}$	
Its item 9: $\forall j \le h-1\ \forall y \in Y_j :\ \lvert y_{\text{fx64}}\rvert \le c^{h-1}(M+2)-2$	

(L7) $\forall x \in X_{\text{FFT}} :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[item 8 of (I2)]

(L8) $\forall B' \ge 0 :\ c^{h-1}(B'+2)-2 \le c^9(B'+2)-2$

[c (the proof's block); $h-1 \le 9$; expand]

(L9) $\forall x \in X_{\text{FFT}} :\ \lvert x_{\text{fx64}}\rvert \le M_T$

[item 9 of (I2); (L8) at $B' := \sqrt{2}\,q2^{64}$; M_T (the proof's block); expand]

(L10) $M_T < 2^{88}$

[M_T, c (the proof's block); expand]

(L11) $\Rightarrow\ \forall x \in X_{\text{FFT}} :\ \lvert x_{\text{fx64}}\rvert < 2^{88}$

[(L9), (L10)]

Lemma I.34 at $j := h-1$	This proof
Shared: h	
p	$p \in \{f, F\}$ (the statement)
B	127
W_x	$W_{\widetilde{b}},\ \widetilde{b} \in \{\widetilde{b}_{01}, \widetilde{b}_{11}\}$ (ffSampling$^{\mathcal{F}}$, line 1)
X^-	$\{\widetilde{b}_{01}, \widetilde{b}_{11}\}$ (ffSampling$^{\mathcal{F}}$, line 1)
(I3) $p \in \{-128, \dots, 127\}^{2^h}$	Assumptions A1 and A2; $B \le 127$ (B, the rows above)
$B \in [0, 127]$	127
W_x a pair of words at stage j	ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 1
Assumption A1	Assumptions A1 and A2
Its item 3: $\forall x \in X^- :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
Its item 4: $\forall x \in X^- :\ \lvert x_{\text{fx64}}\rvert \le M_{h-1}$	
Its item 5: $\forall j \le h-1 :\ M_j \le c^{h-1}(1.4143\,B2^{64}+2)-2$	

(L12) $\forall \widetilde{b} \in \{\widetilde{b}_{01}, \widetilde{b}_{11}\} :\ W_{\widetilde{b}} = \widetilde{b}_{\text{fx64}} \bmod 2^{128}$

[item 3 of (I3)]

(L13) $\forall \widetilde{b} \in \{\widetilde{b}_{01}, \widetilde{b}_{11}\} :\ \lvert \widetilde{b}_{\text{fx64}}\rvert \le M_b$

[items 4 and 5 of (I3); (L8) at $B' := 1.4143 \cdot 127 \cdot 2^{64}$; M_b (the proof's block)]

(L14) $\forall y \in X_{\text{prod}} :\ \lvert y_{\text{fx64}}\rvert \le M_T M_b/2^{64} + \sqrt{2}$

[Lemma I.34, item 7; (L9), (L13); Fact A.41, item 8]

(L15) $M_T M_b/2^{64} + \sqrt{2} < 2^{105}$

[M_T, M_b, c (the proof's block); expand]

(L16) $\Rightarrow\ \forall y \in X_{\text{prod}} :\ \lvert y_{\text{fx64}}\rvert < 2^{105}$

[(L14), (L15)]

(L17) $\forall x \in X_{\text{FFT}}\ \forall \widetilde{b} \in \{\widetilde{b}_{01}, \widetilde{b}_{11}\}\ \forall \mathfrak{p}, \mathfrak{p}' \in \{\text{Re}, \text{Im}\} :\ \lvert \mathfrak{p}(x)_{\text{fx64}} \lvert \lvert \mathfrak{p}'(\widetilde{b})_{\text{fx64}}\rvert/2^{64} + 1/2 \le M_T M_b/2^{64} + 1/2$

16950 [(L9), (L13); $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \le |x|$ (Fact A.41, item 1); Fact A.41, item 8]

16951 (L18) $2(M_T M_b/2^{64} + 1/2) < 2^{127}$

16952 [M_T, M_b, c (the proof's block); expand]

Lemma I.12, items 1, 2 and 5 at each operation of the products $x \otimes \widetilde{b}$ of lines 16 and 18, at every $x \in X_{\mathrm{FFT}}$ and $\widetilde{b} \in \{\widetilde{b}_{01}, \widetilde{b}_{11}\}$	This proof
(W_x, W_y)	$(W_{\mathfrak{p}(x)}, W_{\mathfrak{p}'(\widetilde{b})})$ at mul; the words of two of these products at add, sub (Definition A.8)
o	mul, add, sub (Definition A.8)
V	$\mathfrak{p}(x)_{\mathrm{fx64}}, \mathfrak{p}'(\widetilde{b})_{\mathrm{fx64}}$ (Definition A.5)
$W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	Words (Definition A.5)
(I4) $V \in \mathbb{Z}$	Definition A.5
$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	The scope
Assumption A1	(L7), (L12)
Assumption A2	(L11), (L13); M_b (the proof's block); $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1); expand
Assumption A4	$o \ne \mathrm{div}$ (the scope)
Assumption A5	Item 2; (L17), (L18)
Its item 1: $x_{\mathrm{fx64}} = V$	
Its item 2: $\lvert\mathrm{roundAway}(x_{\mathrm{fx64}} y_{\mathrm{fx64}}, 2^{64})\rvert \le \lvert x_{\mathrm{fx64}}\rvert\lvert y_{\mathrm{fx64}}\rvert/2^{64} + 1/2$	
Its item 5: $z_{o,\mathrm{fx64}} = V_o$	

16954 (L19) $\forall y \in X_{\mathrm{prod}} :\ W_y = y_{\mathrm{fx64}} \bmod 2^{128}$

16955 [(I1); (I4); Definition A.8; Definition I.1, item 1; X_{prod} (the proof's block)]

16956 (L20) $|\widetilde{(1/q)}_{\mathrm{fx64}}|,\ |\widetilde{(-1/q)}_{\mathrm{fx64}}| < 2^{51}$

16957 [Definition I.20: the stored $1/q$; $\widetilde{(-1/q)} = -\widetilde{(1/q)}$ [L0: `fxp/fxp_consts.h:2090-2091`]]

16958 (L21) $\forall y \in X_{\mathrm{prod}}\ \forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\} :\ |\mathfrak{p}(y)_{\mathrm{fx64}}|2^{51}/2^{64} + 1/2 < 2^{127}$

16959 [(L16); $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \le |x|$ (Fact A.41, item 1); expand]

Lemma I.12, items 1, 2 and 5 at each part $\mathfrak{p}(y)$ of every $y \in X_{\mathrm{prod}}$ and the stored $\widetilde{(\pm 1/q)}$, the scalings of lines 16 and 18	This proof
(W_x, W_y)	$(W_{\mathfrak{p}(y)}, W_{\widetilde{(\pm 1/q)}})$ (ffSampling$^{\mathcal{F}}$, lines 16 and 18)
o	mul (the scope)
V	$\mathfrak{p}(y)_{\mathrm{fx64}}, \widetilde{(\pm 1/q)}_{\mathrm{fx64}}$ (Definition A.5)
$W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	Words (Definition A.5)
(I5) $V \in \mathbb{Z}$	Definition A.5
$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	The scope
Assumption A1	(L19); the stored words of $\pm 1/q$ (Definition I.20)
Assumption A2	(L16), (L20); $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
Assumption A4	$o = \mathrm{mul}$ (the scope)
Assumption A5	Item 2; (L20), (L21)
Its item 1: $x_{\mathrm{fx64}} = V$	
Its item 2: $\lvert\mathrm{roundAway}(x_{\mathrm{fx64}} y_{\mathrm{fx64}}, 2^{64})\rvert \le \lvert x_{\mathrm{fx64}}\rvert\lvert y_{\mathrm{fx64}}\rvert/2^{64} + 1/2$	
Its item 5: $z_{o,\mathrm{fx64}} = V_o$	

16961 (L22) $\forall y \in X_{\mathrm{prod}}\ \forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\} :\ |M(\mathfrak{p}(y), \widetilde{(\pm 1/q)})_{\mathrm{fx64}}| \le |\mathfrak{p}(y)_{\mathrm{fx64}}|2^{51}/2^{64} + 1/2$

16962 [(I5); (L20); M (the proof's block)]

16963 (L23) $\forall x \in X_{\mathrm{sc}} :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[(I1); (I5); Definition I.1, item 1, at $\times$; X_{sc} (the proof's block)]

(L24) $\Rightarrow$ item 1

[(L5), (L7), (L12), (L19), (L23); X_{FFT}, X_{prod}, X_{sc} (the proof's block)]

(L25) $\Rightarrow$ item 2

[(L1), (L2), (L6), (L11), (L13), (L16), (L21), (L22); $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \leq |x|$ (Fact A.41, item 1); X_{FFT}, X_{prod}, X_{sc} (the proof's block)]

□ (items 1 and 2)

Stage	Words	Lemma	$n = 512$	$n = 1024$
expansion	$\widetilde{b}_{00}$, $\widetilde{b}_{01}$	Lemma I.34	$2^{13.46}$	$2^{13.41}$
expansion	$\widetilde{b}_{10}$, $\widetilde{b}_{11}$	Lemma I.34	$2^{15.49}$	$2^{16.49}$
Gram	$\widetilde{g}_{00}$	Lemma I.35	$2^{28.91}$	$2^{28.82}$
Gram	$\widetilde{g}_{11}$	Lemma I.35	$2^{32.98}$	$2^{34.98}$
Gram	$\widetilde{g}_{01}$	Lemma I.35	$2^{29.95}$	$2^{30.90}$
key check	$\mathrm{fl}(\widetilde{\hat{p}}_r^2) + \mathrm{fl}(\widetilde{\hat{p}}_i^2)$	Lemma I.36	$2^{30.98}$	$2^{32.98}$
key check	num_ψ	Lemma I.36	$2^{59.89}$	$2^{61.80}$
key check	$\mathrm{fl}(\widetilde{g}_{00}^2)$	Lemma I.37	$2^{57.82}$	$2^{57.63}$
key check	$\mathrm{fl}(num_\psi / \mathrm{fl}(\widetilde{g}_{00}^2))$	Lemma I.38	$2^{41.79}$	$2^{45.79}$
key check	$\mathrm{fl}(q/lo)$	Lemma I.38	$2^{19.40}$	$2^{21.40}$
key check	$\mathrm{fl}(hi/q)$	Lemma I.38	$2^{15.33}$	$2^{15.23}$
root	$\widetilde{\mu}$, $\widetilde{l}_{10}$	Lemma I.39	$2^{35.76}$	$2^{38.71}$
root	$\mathrm{fl}(q^2/\widetilde{g}_{00})$	Lemma I.39	$2^{32.98}$	$2^{34.98}$
node	$\widetilde{d}_\nu$	Lemma I.43	$[2^{9.08}, 2^{18.09}]$	$[2^{8.53}, 2^{18.64}]$
node	$\widetilde{f}_0$, $\widetilde{f}_-$	Lemma I.40	$2^{18.09}$	$2^{18.64}$
node	$\widetilde{f}_1$	Lemma I.40	$2^{18.09}$	$2^{18.64}$
node	$\widetilde{\mu}$	Lemma I.41	$2^{9.00}$	$2^{10.10}$
node	zo	Lemma I.41	$2^{28.08}$	$2^{29.73}$
node	$\widetilde{d}_{11}$	Lemma I.41	$2^{28.08}$	$2^{29.73}$
center	$\widetilde{\hat{h}}$	Lemma I.47	$2^{22.09}$	$2^{23.09}$
center	$\widetilde{h}_j$	Lemma I.46	$2^{21.09}$	$2^{22.09}$
center	$\widetilde{\hat{h}} \otimes \widetilde{b}_{11}$	Lemma I.47	$2^{37.58}$	$2^{39.58}$
center	$\widetilde{\hat{h}} \otimes \widetilde{b}_{01}$	Lemma I.47	$2^{35.54}$	$2^{36.50}$
center	$\widetilde{t}_0$	Lemma I.47	$2^{24.58}$	$2^{26.58}$
center	$\widetilde{t}_1$	Lemma I.47	$2^{22.54}$	$2^{23.50}$
center	$\widetilde{t}_{\mathrm{frac},j}$	Lemma I.46	$2^{8.09}$	$2^{9.09}$
leaf	$\widetilde{r}$	Lemma I.42	$2^{9.05}$	$2^{9.32}$
leaf	$1/\widetilde{\sigma}$	Lemma I.42	$2^{1.67}$	$2^{1.93}$
recursion	$\widetilde{l}_{10}$ at the root	Lemma I.48	$2^{4.76}$	$2^{5.09}$
recursion	$\widetilde{l}_{10}$ below the root	Lemma I.48	$2^{0.01}$	$2^{0.01}$
recursion	the centers $\widetilde{t}_0$, $\widetilde{t}_1$, $\widetilde{tb}_0$	Lemma I.49	$2^{26.34}$	$2^{28.54}$
recursion	$\widetilde{t}_0 - \widetilde{z}_0$, $\widetilde{t}_1 - \widetilde{z}_1$	Lemma I.49	$2^{25.60}$	$2^{27.92}$
recursion	the center lines' words	Lemma I.49	$2^{32.00}$	$2^{32.00}$
base sampler	$\widetilde{r}$	Lemma I.52	$2^{0.00}$	$2^{0.00}$
base sampler	$\widetilde{dss}$	Lemma I.52	$2^{2.34}$	$2^{2.85}$
base sampler	$\widetilde{ccs}$	Lemma I.52	$2^{2.03}$	$2^{2.30}$
base sampler	$\mathrm{fl}((z - \widetilde{r})^2)$	Lemma I.52	$2^{8.50}$	$2^{8.50}$
base sampler	$\widetilde{a}_x$	Lemma I.52	$2^{10.84}$	$2^{11.34}$
base sampler	$\widetilde{b}_x$	Lemma I.52	$2^{5.62}$	$2^{5.62}$
base sampler	$\widetilde{x}$	Lemma I.52	$2^{10.87}$	$2^{11.37}$
base sampler	$\mathrm{fl}(\widetilde{x} \cdot \texttt{INV_LOG2})$	Lemma I.52	$2^{11.40}$	$2^{11.90}$
base sampler	$\mathrm{fl}(si \cdot \texttt{LOG2})$	Lemma I.52	$2^{10.87}$	$2^{11.37}$
base sampler	$\widetilde{r}'$	Lemma I.52	$2^{11.87}$	$2^{12.37}$
base sampler	r'	Lemma I.52	$2^{-0.52}$	$2^{-0.52}$
inverse FFT	the stages' pairs	Lemma I.53	$2^{34.36}$	$2^{37.56}$
inverse FFT	the scaled pairs	Lemma I.53	$2^{26.36}$	$2^{28.56}$

Table 32: Fixed-point signer, both centers: the range R_x of the number x of each class of words of the key check, the tree and the recursion: the bound its lemma proves, evaluated at the degree's constants (Theorem I.54), its exponent rounded up; for the diagonals below the root, their floor, rounded down, and ceiling. Gate: `verify/gates/fx/ranges.py`.

I.3.5 No overflow in the recursion

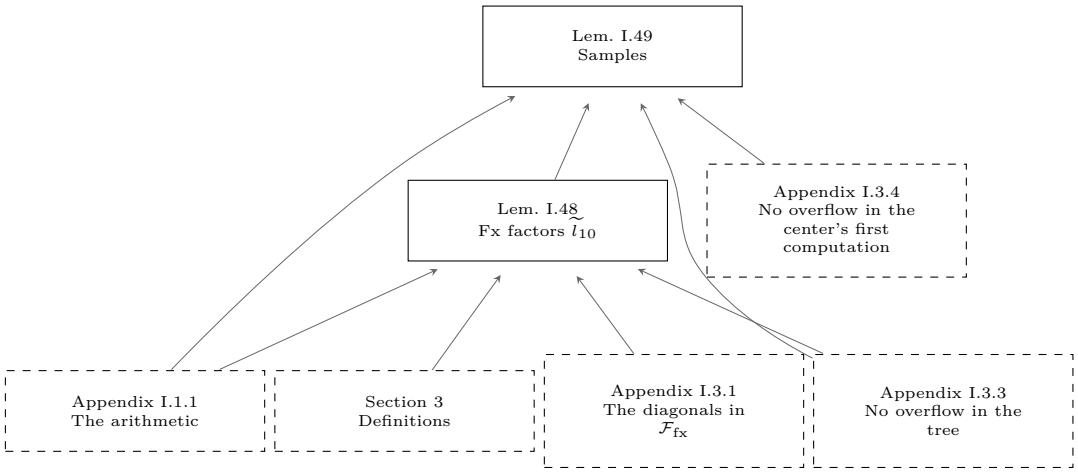


Figure 79: Dependencies, Appendix I.3.5.

Lemma I.48 (The fixed-point signer's factors $\widetilde{l}_{10}$ [to table])**.** *The key check bounds the root's computed factor, and the self-adjoint split bounds a child's. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5), of degree* $n = 2^h \in \{512, 1024\}$*;*
- ν *be a node of the tree recursion, in either center's mode.*

Define:

- $\zeta_{\mathrm{op}} := 2^{-65}$ *(Definition I.1);*
- γ_{root} *and* $\check{\gamma}_{\mathrm{hyb}}$*, those of Definition A.35;*
- $\check{\gamma}_{\mathrm{root}} := ((\gamma_{\mathrm{root}}^2 + 2^{-65})(1 + 2^{-65}\check{\gamma}_{\mathrm{hyb}}^4/q^2) + 2^{-64}\check{\gamma}_{\mathrm{hyb}}^4/q^2)^{1/2}$ *(Definition A.35);*
- $c_{\mathrm{sa}} := \sqrt{2}\,\zeta$ *and* $k_{\mathrm{sa}} := (1 + \sqrt{2}\,\zeta)/2 + \sqrt{2}$ *(Corollary I.24);*
- $\ell_{\mathrm{root}} := \check{\gamma}_{\mathrm{root}} + \sqrt{2}\,\zeta_{\mathrm{op}}$*;*
- $\ell_{\mathrm{child}} := (2^8(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta)/(2^8 - \zeta_{\mathrm{op}}) + \sqrt{2}\,\zeta_{\mathrm{op}}$*;*
- $\nu_0 := T$*;*
- $\widetilde{l}_{10}$*, the number* LDL† *(Algorithm 5) computes at* ν*, line 12.*

Then

1. *Assume:*

   (A1) $\nu = \nu_0$.

   Then $\forall \psi :\ |\widetilde{l}_{10}| \le \ell_{\mathrm{root}}$.

2. *Assume:*

   (A2) $\nu \neq \nu_0$.

   Then $\forall \psi :\ |\widetilde{l}_{10}| \le \ell_{\mathrm{child}}$.

Proof.

COMPUTES $(\widetilde{g}_{00}, \widetilde{g}_{01})$: the Gram matrix entries LDL† (Algorithm 5) takes at ν
COMPUTES $\widetilde{\mu}$: the number LDL† computes at ν, line 10
DEFINES $(\widetilde{b}_{00}, \widetilde{b}_{01}, \widetilde{b}_{10}, \widetilde{b}_{11}) = (\widetilde{\hat{g}}, \widetilde{\hat{f}}, \widetilde{\hat{G}}, \widetilde{\hat{F}})$: the images of keychecks, line 1
DEFINES $(\widetilde{b}^{\mathrm{S}}_{00}, \widetilde{b}^{\mathrm{S}}_{01}, \widetilde{b}^{\mathrm{S}}_{10}, \widetilde{b}^{\mathrm{S}}_{11})$: the images of ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 1
DEFINES $(\widetilde{g}^{\mathrm{K}}_{00}, \widetilde{g}^{\mathrm{K}}_{01})$: the Gram's entries of keychecks, line 3
DEFINES $\widetilde{d}$: at a node ν below the root, the diagonal of ν's parent $\widetilde{\mathrm{split}}_{\mathrm{sa}}$ (Algorithm 3) splits
DEFINES $a = \widetilde{d}(\psi)$, $b = \widetilde{d}(-\psi)$
DEFINES $y = (a + b)/2$

(L1) $\forall \psi :\ |\widetilde{l}_{10}| = |\widetilde{\mu}|$

[$\widetilde{l}_{10} = \operatorname{conj} \widetilde{\mu}$ (LDL† (Algorithm 5), line 12); $|\operatorname{conj} x| = |x|$ (Fact A.41, item 1)]

Lemma H.16, item 1 at the root node $\nu = \nu_0$	This proof
Shared: n, $\widetilde{g}_{00}$ (ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 3)	
(I1) (f, g, F, G) key of degree $n = 2^h$ $\psi \in \Psi_n$	The checked key (the statement) The roots ψ (the statement)
Assumption A1 Assumption A2	Definition 5.5, item 2, at the key (the statement) Definition 5.5, item 3, at the key (the statement)
Its conclusion: $\widetilde{g}_{00} > 2^{-8}$	

(L2) $\nu = \nu_0 \Rightarrow\ \forall \psi :\ \widetilde{g}_{00} > 2^{-8}$

[(I1)]

(L3) $\nu \neq \nu_0 \Rightarrow\ \forall \psi :\ W_a = a_{\text{fx64}} \bmod 2^{128}$

[Lemma I.44, (L13), at the checked key (the statement); a (the proof's block)]

(L4) $\nu \neq \nu_0 \Rightarrow\ \forall \psi :\ a \in [2^8, 2^{19}]$

[Lemma I.43, item 2, at the checked key (the statement); a (the proof's block)]

Lemma I.40, (L2) at the parent's diagonal $\widetilde{d}$ of ν	This proof
Shared: $\widetilde{f}_0$	
(I2) $\widetilde{d}$ $h \in \{2, \ldots, 10\}$	$\widetilde{d}$ (the proof's block) The parent of ν, of degree 2^h in the tree of the key of degree $n \in \{512, 1024\}$ (the statement)
Assumption A1 Assumption A2	(L3) (L4)
Its conclusion: $\widetilde{f}_{0,\text{fx64}} \geq 2^{64} 2^8 - 1/2$	

(L5) $\nu \neq \nu_0 \Rightarrow\ \forall \psi :\ \widetilde{g}_{00,\text{fx64}} \geq 2^{64} 2^8 - 1/2$

[(I2); $\widetilde{g}_{00} = \widetilde{f}_0$ at $\nu \neq \nu_0$ (ffsamp (Algorithm 6), lines 15 and 29; $\widetilde{\text{split}}_{\text{sa}}$ (Algorithm 3), line 4)]

(L6) $2^{64} 2^8 - 1/2 > 0$

[expand]

(L7) $\forall \psi :\ \widetilde{g}_{00} = 2^{-64} \widetilde{g}_{00,\text{fx64}}$

[Definition A.5]

(L8) $\Rightarrow\ \forall \psi :\ \widetilde{g}_{00} > 0$

[(L2), (L5), (L6), (L7)]

(L9) $\forall \psi :\ |\widetilde{\mu}_r - \widetilde{g}_{01,r}/\widetilde{g}_{00}|,\ |\widetilde{\mu}_i - \widetilde{g}_{01,i}/\widetilde{g}_{00}| \leq \zeta_{\text{op}}$

[Definition I.1, item 1, at / (LDL†, lines 7 and 8); $\widetilde{g}_{00} > 0$ (L8)]

(L10) $\forall \psi :\ |\widetilde{\mu}| \leq |\widetilde{g}_{01}|/\widetilde{g}_{00} + \sqrt{2}\, \zeta_{\text{op}}$

[(L8), (L9); $\widetilde{\mu} = \widetilde{\mu}_r + i\, \widetilde{\mu}_i$ (LDL† (Algorithm 5), line 10); $\forall a, b \in \mathbb{R} :\ |a + ib|^2 = a^2 + b^2$, $|x + y| \leq |x| + |y|$ (Fact A.41, item 1)]

Proof of item 1.

(L11) $(\widetilde{b}^{\text{S}}_{00}, \widetilde{b}^{\text{S}}_{01}, \widetilde{b}^{\text{S}}_{10}, \widetilde{b}^{\text{S}}_{11}) = (\widetilde{b}_{00}, -\widetilde{b}_{01}, \widetilde{b}_{10}, -\widetilde{b}_{11})$

[[L0: `fxp/kgen_fx.c:71-78`] [L0: `fxp/sign_fxcore.c:24-42`]; Lemma I.10, item 10]

(L12) $(\widetilde{g}_{00}, \widetilde{g}_{01}) = (\widetilde{g}^{\text{K}}_{00}, \widetilde{g}^{\text{K}}_{01})$

[assumption A1; (L11); Gram (Algorithm 13), lines 2 to 18; $(-x)(-y) = xy$ [L0: `fxp/kgen_fx.c:81`] [L0: `fxp/sign_fxcore.c:184`]]

(L13) $\forall \psi :\ |\widetilde{g}_{01}| \leq \check{\gamma}_{\text{root}} \widetilde{g}_{00}$

[(L12); Lemma H.17, item 4, at the checked key (the statement)]

(L14) $\forall \psi :\ |\widetilde{g}_{01}|/\widetilde{g}_{00} \leq \check{\gamma}_{\text{root}}$

[(L13); $\widetilde{g}_{00} > 0$ (L8)]

(L15) $\Rightarrow$ $\forall \psi : \ |\widetilde{l}_{10}| \le \ell_{\mathrm{root}}$

[(L1), (L10), (L14); ℓ_{root} (the statement)]

(L16) $\Rightarrow$ item 1

[(L15)]

Proof of item 2.

(L17) $(\widetilde{g}_{00}, \widetilde{g}_{01}) = (\widetilde{f}_0, \widetilde{f}_1)$

[assumption A2; ffsamp (Algorithm 6), lines 15 and 29; $\widetilde{\mathrm{split}}_{\mathrm{sa}}$ (Algorithm 3), lines 4 and 6, at (a, b) (the proof's block)]

(L18) $a, b \in [2^8, 2^{19}]$

[Lemma I.43, item 2, at the checked key (the statement)]

(L19) $\widetilde{f}_0 \ge y - \zeta_{\mathrm{op}}$

[$\widetilde{\mathrm{split}}_{\mathrm{sa}}$ (Algorithm 3), line 4; Definition I.1, items 1 and 2; y (the proof's block)]

(I3)

Lemma G.26 at $(\widetilde{a}, \widetilde{b}) := (a, b)$ and $(u, \zeta) = (0, 2^{-64})$	This proof
Shared: $\psi,\ c_{\mathrm{sa}}, k_{\mathrm{sa}}$	
$\mathcal{F}, (u, \zeta)$	$\mathcal{F}_{\mathrm{fx}}, (0, 2^{-64})$ (Definition I.1)
$\widetilde{a}, \widetilde{b}$	a, b (the scope)
$\widetilde{d}_1$	$\widetilde{f}_1$ ($\widetilde{\mathrm{split}}_{\mathrm{sa}}$ (Algorithm 3), line 6)
$\widetilde{\psi}$	$\widetilde{s}$ ($\widetilde{\mathrm{split}}_{\mathrm{sa}}$, line 6)
$\mathcal{F}$ a realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
$\psi \in \mathbb{C}$	The roots ψ
$\widetilde{\psi} \in C_{\mathcal{F}}$	$\widetilde{s}$, a stored twiddle (Definition A.8, item 1)
$\widetilde{a}, \widetilde{b} \in \mathcal{F}$	a, b (the proof's block)
Assumption A1	$\lvert\psi\rvert = 1$ (Fact A.42, item 1)
Assumption A2	Lemma G.14
Its conclusion: $\exists\, \delta_{\mathrm{sa}}, e_{\mathrm{sa}} \in \mathbb{C},\ \lvert\delta_{\mathrm{sa}}\rvert \le c_{\mathrm{sa}},\ \lvert e_{\mathrm{sa}}\rvert \le k_{\mathrm{sa}}\zeta :\ \widetilde{d}_1 = \frac{\widetilde{a}-\widetilde{b}}{2}\operatorname{conj}(\psi)(1+\delta_{\mathrm{sa}}) + e_{\mathrm{sa}}$	

(L20) $\exists\, \delta_{\mathrm{sa}}, e_{\mathrm{sa}} \in \mathbb{C},\ |\delta_{\mathrm{sa}}| \le c_{\mathrm{sa}},\ |e_{\mathrm{sa}}| \le k_{\mathrm{sa}}\zeta :\ \widetilde{f}_1 = \frac{a-b}{2}\operatorname{conj}(\psi)(1+\delta_{\mathrm{sa}}) + e_{\mathrm{sa}}$

[(I3); c_{sa}, k_{sa} (the statement; Corollary I.24)]

(L21) $|\widetilde{f}_1| \le \frac{|a-b|}{2}(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta$

[(L20); $|\psi| = 1$ (Fact A.42, item 1); $|xy| = |x||y|$, $|\operatorname{conj} x| = |x|$, $|x + y| \le |x| + |y|$ (Fact A.41, item 1)]

(L22) $|a - b|/2 \le y$

[(L18); $|x + y| \le |x| + |y|$ (Fact A.41, item 1); y (the proof's block)]

(L23) $|\widetilde{f}_1| \le y(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta$

[(L21), (L22)]

(L24) $y \ge 2^8$

[(L18); y (the proof's block)]

(L25) $y - \zeta_{\mathrm{op}},\ 2^8 - \zeta_{\mathrm{op}} > 0$

[(L24); $\zeta_{\mathrm{op}} = 2^{-65}$ (Definition I.1)]

(L26) $1/\widetilde{g}_{00} \le 1/(y - \zeta_{\mathrm{op}})$

[(L17), (L19), (L25); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L27) $|\widetilde{\mu}| \le \frac{y(1+c_{\mathrm{sa}})+k_{\mathrm{sa}}\zeta}{y-\zeta_{\mathrm{op}}} + \sqrt{2}\,\zeta_{\mathrm{op}}$

[(L10), (L17), (L23), (L26); $\forall a, a', b, b' \in \mathbb{R},\ 0 \le a \le a',\ 0 \le b \le b' :\ ab \le a'b'$ (Fact A.41, item 8)]

(L28) $(2^8(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta)(y - \zeta_{\mathrm{op}}) - (y(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta)(2^8 - \zeta_{\mathrm{op}}) = (y - 2^8)((1 + c_{\mathrm{sa}})\zeta_{\mathrm{op}} + k_{\mathrm{sa}}\zeta)$

[expand]

(L29) $(y - 2^8)((1 + c_{\mathrm{sa}})\zeta_{\mathrm{op}} + k_{\mathrm{sa}}\zeta) \ge 0$

[(L24); c_{sa}, k_{sa}, ζ_{op} (the statement); expand]

(L30) $\frac{y(1+c_{\mathrm{sa}})+k_{\mathrm{sa}}\zeta}{y-\zeta_{\mathrm{op}}} \le \frac{2^8(1+c_{\mathrm{sa}})+k_{\mathrm{sa}}\zeta}{2^8-\zeta_{\mathrm{op}}}$

[(L25), (L28), (L29)]

(L31) $\Rightarrow$ $\forall \psi :\ |\widetilde{l}_{10}| \le \ell_{\text{child}}$

[(L1), (L27), (L30); ℓ_{child} (the statement)]

(L32) $\Rightarrow$ item 2

[(L31)]

$\square$ (items 1 and 2)

Lemma I.49 (No overflow in the recursion's centers and samples [to table])**.** *Every center of the sampling recursion is at most 2^{30}, every sample within an explicit deviation of its center, and every word of the center lines holds its number. Let:*

- *(f, g, F, G) be a checked key (Definition 5.5), of degree $n = 2^h \in \{512, 1024\}$;*
- *ν be a call of the sampling recursion at depth k, $0 \le k \le h-1$, in either center's mode: of* ffsamp *(Algorithm 6) at $k \le h-2$, of* deepest *(Algorithm 7) at $k = h-1$.*

Define:

- *$(\widetilde{t}_0, \widetilde{t}_1)$, the center ν receives (line 1 of* ffsamp*);*
- *$(\widetilde{z}_0, \widetilde{z}_1)$, the sample ν returns;*
- *$\widetilde{tb}_0$, the center of line 25 of* ffsamp *at $k \le h-2$, of line 9 of* deepest *at $k = h-1$.*

Let:

- *W_x be a word of ν's center lines, one of:*
  - *At $k \le h-2$: the splits $\widetilde{\text{split}}(\widetilde{t}_1)$ and $\widetilde{\text{split}}(\widetilde{tb}_0)$ ($\widetilde{\text{split}}$ (Algorithm 2)) the calls of lines 19 and 33 take, the merges of lines 21 and 35, and line 25 with its $\widetilde{t}_1 \ominus \widetilde{z}_1$ and its product;*
  - *At $k = h-1$: line 9 of* deepest *with its $\widetilde{t}_1 \ominus \widetilde{z}_1$ and its product, and the samples' parts $\operatorname{Re} \widetilde{z}_j$, $\operatorname{Im} \widetilde{z}_j$.*

Define:

- *The signer's words and parameters*
  - *$\zeta_{\text{op}} := 2^{-65}$ (Definition I.1);*
  - *$T^* := 2^{30}$;*
- *The node bounds*
  - *$c_{\text{sa}} := \sqrt{2}\,\zeta$ and $k_{\text{sa}} := (1 + \sqrt{2}\,\zeta)/2 + \sqrt{2}$ (Corollary I.24);*
  - *$\check{\gamma}_{\text{root}}$, that of Definition A.35;*
  - *$\ell_{\text{root}} := \check{\gamma}_{\text{root}} + \sqrt{2}\,\zeta_{\text{op}}$ (Lemma I.48);*
  - *$\ell_{\text{child}} := (2^8(1 + c_{\text{sa}}) + k_{\text{sa}}\zeta)/(2^8 - \zeta_{\text{op}}) + \sqrt{2}\,\zeta_{\text{op}}$ (Lemma I.48);*
  - *$\ell_0 := \ell_{\text{root}}$;*
  - *$\forall k \in \{1, \ldots, h-1\} :\ \ell_k := \ell_{\text{child}}$;*
- *The center shifts*
  - *$c_{\text{split}} := \sqrt{2} \cdot 2^{-64}$ (Lemma G.16 at $(u, \zeta) = (0, 2^{-64})$);*
  - *$k_D := (\sqrt{2}/2)(1 + \sqrt{2} \cdot 2^{-64}) + 3\sqrt{2}$ (Lemma G.16 at $(u, \zeta) = (0, 2^{-64})$);*
  - *$c_{\text{merge}} := \sqrt{2} \cdot 2^{-64}$ and $k_E := 8\sqrt{2}$ (Lemma G.18 at $(u, \zeta) = (0, 2^{-64})$);*
  - *$e_s := c_{\text{split}} T^* + (\sqrt{2}/2 + k_D)\zeta$;*
  - *$e_m := 4c_{\text{merge}} T^* + k_E \zeta$;*
  - *$\forall \ell \ge 0 :\ e_I(\ell) := \sqrt{2}(\ell + 4)\zeta$;*
- *The centers and the samples*
  - *$H_{h-1} := 39\sqrt{2}/2$;*
  - *$D_{h-1} := (1 + \ell_{h-1})H_{h-1} + e_I(\ell_{h-1})$;*
  - *$\forall k \le h-2 :\ H_k := 2D_{k+1} + 2e_s + e_m$;*
  - *$\forall k \le h-2 :\ D_k := (1 + \ell_k)H_k + e_I(\ell_k)$;*
  - *$R := \max(R_{\widetilde{t}_0}, R_{\widetilde{t}_1}, R_{\widetilde{t}_{\text{frac},j}})$ (Table 32 at n), a bound on each part;*
  - *$T_0 := \sqrt{2}\,R$;*
  - *$\forall k \le h-2 :\ T_{k+1} := T_k + \ell_k H_k + e_I(\ell_k) + e_s$;*
  - *$T_{\text{leaf}} := T_{h-1} + \ell_{h-1} H_{h-1} + e_I(\ell_{h-1})$;*

- *The words*
  - x, *the number* W_x*'s line computes in* $\mathcal{F}_{\text{fx}}$ *(Definition I.1);*
  - $x_{\text{fx64}} := 2^{64}x$ *(Definition A.5).*

Then

1. $\forall\psi:\ |\widetilde{t}_0(\psi)|, |\widetilde{t}_1(\psi)| \le T_k$;
2. *Assume:*

   (A1) $k = h - 1$.

   Then $\forall\psi:\ |\widetilde{tb}_0(\psi)| \le T_{\text{leaf}}$.
3. $\forall\psi:\ |\widetilde{t}_1(\psi) - \widetilde{z}_1(\psi)| \le H_k$;
4. $\forall\psi:\ |\widetilde{t}_0(\psi) - \widetilde{z}_0(\psi)| \le D_k$;
5. $W_x = x_{\text{fx64}} \bmod 2^{128}$;
6. $|x| \le 4T^*$.

Proof.

DEFINES $P(k)$: every call at depth k whose center has $\forall\psi:\ |\widetilde{t}_0(\psi)|, |\widetilde{t}_1(\psi)| \le T_k$ and $\forall j \in \{0,1\}\ \forall\psi\ \forall\mathfrak{p} \in \{\text{Re}, \text{Im}\}:\ W_{\mathfrak{p}(\widetilde{t}_j(\psi))} = \mathfrak{p}(\widetilde{t}_j(\psi))_{\text{fx64}} \bmod 2^{128}$ satisfies items 3, 4, 5 and 6, item 2 at $k = h-1$, and every call below it at depth k' receives a center at most $T_{k'}$ whose words satisfy the same identity

DEFINES μ, a part Re or Im of a center of deepest's calls of SamplerZ (Algorithm 8), and w, the part of the sample that call returns

DEFINES o, an operation of the center lines, a, b its operands and $o(a,b)$ the number $\mathcal{F}_{\text{fx}}$ (Definition I.1) computes

DEFINES X_ν: the numbers of the words W_x of the statement at the call ν

DEFINES $(\widetilde{c}_0, \widetilde{c}_1) = \widetilde{\text{split}}(\widetilde{t}_1)$ and $(\widetilde{c}'_0, \widetilde{c}'_1) = \widetilde{\text{split}}(\widetilde{tb}_0)$, the centers of the calls of lines 19 and 33, at $k \le h - 2$

(L1) $\forall k:\ T_{\text{leaf}}, D_k \le T^*$

[[gate: `verify/gates/fx/samples.py`], at the degree's constants]

(L2) $\forall k:\ H_k \le D_k$

[H_k, D_k (the statement); $\ell_k, e_I(\ell_k) \ge 0$ (the statement)]

(L3) $\forall k \le h-2:\ T_k \le T_{k+1}$

[T_{k+1} (the statement); $\ell_k, H_k, e_I(\ell_k), e_s \ge 0$ (the statement)]

(L4) $T_{h-1} \le T_{\text{leaf}}$

[T_{leaf} (the statement); $\ell_{h-1}, H_{h-1}, e_I(\ell_{h-1}) \ge 0$ (the statement)]

(L5) $\forall x,\ |x| \le 4T^*:\ |x_{\text{fx64}}| \le 2^{96}$

[$T^* = 2^{30}$ (the statement); Definition A.5]

(L6) $2^{96} < 2^{127}$

[expand]

(L7) $\forall x,\ |x| \le 4T^*:\ |x_{\text{fx64}}| < 2^{127}$

[(L5), (L6)]

	Lemma I.10, items 2, 4 and 8 at the call ν at $k \le h-2$, at $\texttt{logn} = h-k$	This proof
	h	$h-k$ (the statement)
	$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
	$h \in \{2,\dots,10\}$	$k \le h-2$; $n \in \{512, 1024\}$ (the statement)
17140 (I1)	each input array of words	The words of ν's center lines (the statement; Definition A.5)
	Its item 2: the object of `fxpoly_split_fft` in $\mathcal{O}$ returns the words of lines 4 and 6 of $\widetilde{\text{split}}$	
	Its item 4: the object of `fxpoly_merge_fft` in $\mathcal{O}$ returns the words of line 4 of $\widetilde{\text{merge}}$ and of the sum and the difference after it	
	Its item 8: on their input words a and b, the objects of `fxpoly_mul_fft`, `fxpoly_add` and `fxpoly_sub` in $\mathcal{O}$ return $a \otimes b$, $a \oplus b$ and $a \ominus b$	
	Lemma I.40, (L2) at the parent's diagonal $\widetilde{d}$ of a node of degree 2 of the key's tree	This proof
	Shared: $\widetilde{f}_0$	
17141 (I2)	$\widetilde{d}$	$\widetilde{d}$ (Lemma I.40)
	$h \in \{2,\dots,10\}$	The parent, of degree 4 in the tree of the key of degree $n \in \{512, 1024\}$ (the statement)
	Assumption A1	Lemma I.44, (L13), at the checked key (the statement)
	Assumption A2	Lemma I.43, item 2, at the checked key (the statement)
	Its conclusion: $\widetilde{f}_{0,\text{fx64}} \ge 2^{64}2^8 - 1/2$	
	Lemma I.10, item 7 at the signer's $\texttt{logn} = h$	This proof
	h	h (the statement)
	$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
	g00	$\widetilde{f}_0$ (I2)
17142 (I3)	$h \in \{2,\dots,10\}$	$n \in \{512, 1024\}$ (the statement)
	each input array of words	The words of ν's center lines (the statement; Definition A.5)
	Assumption A4	(I2); expand
	Its item 7: at a node of degree 2, the object of `fxp_ffsamp_fft` in $\mathcal{O}$ returns the words of lines 7 to 18 of LDL† and of lines 1 to 18 of deepest	

17143 (L8) $\forall o:\ W_{o(a,b)} = W_{z_o}$

17144 [items 2, 4 and 8 of (I1); item 7 of (I3); W_{z_o} of Lemma I.12, item 5, at $(W_x, W_y) := (W_a, W_b)$]

17145 (L9) $\forall o:\ |a| \le 4T^* \Rightarrow\ o(a,b)_{\text{fx64}} = V_o$

17146 [Definition I.1, item 1, and item 2, at $x := a$, $a_{\text{fx64}} \in [-2^{127}, 2^{127})$ by the premise and (L7); V_o of

17147 Lemma I.12, item 5, at $(x_{\text{fx64}}, y_{\text{fx64}}) := (a_{\text{fx64}}, b_{\text{fx64}})$]

	Lemma I.12, items 1 and 5 at every operation o of ν's center lines on its operands a, b, under the premise of (L10)	This proof
	(W_x, W_y)	(W_a, W_b) (the proof's block)
	o	o (the proof's block)
	V	$a_{\mathrm{fx64}}, b_{\mathrm{fx64}}$ (Definition A.5)
	$W_x, W_y \in \{0, \dots, 2^{128} - 1\}$	Words (Definition A.5)
(I4)	$V \in \mathbb{Z}$	Definition A.5
	$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	o, an operation of the center lines (the proof's block)
	Assumption A1	The premise of (L10)
	Assumption A2	The premise of (L10); (L7)
	Assumption A4	$o \neq \mathrm{div}$ (the scope)
	Assumption A5	The premise of (L10); (L7), (L9)
	Its item 1: $x_{\mathrm{fx64}} = V$	
	Its item 5: $z_{o,\mathrm{fx64}} = V_o$	

(L10) $|a|, |b|, |o(a,b)| \le 4T^* \wedge W_a = a_{\mathrm{fx64}} \bmod 2^{128} \wedge W_b = b_{\mathrm{fx64}} \bmod 2^{128} \Rightarrow W_{o(a,b)} = o(a,b)_{\mathrm{fx64}} \bmod 2^{128}$

[(L8); (I4)]

(L11) $(z_0, b) \in \{0, \dots, 18\} \times \{0, 1\}$

[SamplerZ (Algorithm 8), line 9, its 18 rows of `GAUSS0` [L0: `fxp/sign_fxsampler.c:33-65`]]

(L12) $z \in [-18, 19]$

[(L11); $z = b + (2b-1)z_0$ (SamplerZ, line 10)]

(L13) $|\mu| \le T^* \Rightarrow \lfloor |\mu| \rfloor + 19 < 2^{31}$

[$\lfloor \mu \rfloor \in (\mu - 1, \mu]$ (Fact A.41, item 22); $T^* = 2^{30}$ (the statement)]

	Lemma I.7, items 2 and 1 at every μ and w of the proof's block, under the premise of (L14)	This proof
	x	μ (the proof's block)
	i	w (the proof's block)
(I5)	$x \in 2^{-64}\mathbb{Z},\ x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$	μ, a number of $\mathcal{F}_{\mathrm{fx}}$ (Definition I.1); the premise of (L14); (L7)
	$W_x = W_\mu$	The premise of (L14)
	$i \in \{-2^{63}, \dots, 2^{63} - 1\}$	w, an `int32` [L0: `fxp/sign_fxsampler.c:184`] [L0: `fxp/sign_fxsampler.c:213`]
	Its item 2: $j = \lfloor x \rfloor$	
	Its item 1: $z = i$	

(L14) $|\mu| \le T^* \wedge W_\mu = \mu_{\mathrm{fx64}} \bmod 2^{128} \Rightarrow w = \lfloor \mu \rfloor + z$

[(I5); (L12), (L13); the `int32` addition [L0: `fxp/sign_fxsampler.c:184`] [L0: `fxp/sign_fxsampler.c:213`]]

(L15) $|\mu| \le T^* \wedge W_\mu = \mu_{\mathrm{fx64}} \bmod 2^{128} \Rightarrow W_w = w_{\mathrm{fx64}} \bmod 2^{128}$

[(L14): its word [L0: `fxp/sign_fxsampler.c:255-268`]; item 1 of (I5); Definition A.5]

(L16) $|\mu| \le T^* \wedge W_\mu = \mu_{\mathrm{fx64}} \bmod 2^{128} \Rightarrow |w - \mu| \le 39/2$

[(L12), (L14); $\mu - \lfloor \mu \rfloor \in [0, 1)$ (Fact A.41, item 22)]

Proof of the base, $P(h-1)$.

(L17) $\forall \psi : |\widetilde{t}_0(\psi)|, |\widetilde{t}_1(\psi)| \le T_{h-1}$

[$P(h-1)$'s call (the proof's block)]

(L18) $\forall j \in \{0,1\}\ \forall \psi\ \forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\} : W_{\mathfrak{p}(\widetilde{t}_j(\psi))} = \mathfrak{p}(\widetilde{t}_j(\psi))_{\mathrm{fx64}} \bmod 2^{128}$

[$P(h-1)$'s call (the proof's block)]

(L19) $|\mathrm{Re}\, \widetilde{t}_1|, |\mathrm{Im}\, \widetilde{t}_1| \le T^*$

[(L1), (L4), (L17); $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \le |x|$ (Fact A.41, item 1)]

(L20) $|\widetilde{t}_1 - \widetilde{z}_1| \le H_{h-1}$

[(L16), (L19), (L18); $\forall a, b \in \mathbb{R}:\ |a+ib|^2 = a^2 + b^2$ (Fact A.41, item 1); H_{h-1} (the statement)]

Lemma I.48, item 2	This proof
Shared: (f, g, F, G), ν	
ℓ_{child}	ℓ_{h-1} (the statement)
(I6) (f, g, F, G) checked key of degree $n \in \{512, 1024\}$	The statement
ν a node of the tree recursion	The statement
Assumption A2	ν at depth $h - 1 \ge 1$ (the proof's block)
Its conclusion: $\forall \psi:\ \lvert\widetilde{l}_{10}\rvert \le \ell_{\text{child}}$	

(L21) $\forall \psi:\ |\widetilde{l}_{10}| \le \ell_{h-1}$

[(I6)]

(L22) $\forall \psi\ \forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\}:\ W_{\mathfrak{p}(\widetilde{l}_{10}(\psi))} = \mathfrak{p}(\widetilde{l}_{10}(\psi))_{\text{fx64}} \bmod 2^{128}$

[Lemma I.44, item 1, at the checked key (the statement): $\widetilde{l}_{10}$, a word of LDL† (Algorithm 5), line 12, below the root at $m = 2$]

Corollary I.9, item 1	This proof
$\mathcal{F}$	$\mathcal{F}_{\text{fx}}$ (Definition I.1)
u	0
(I7) ζ	2^{-64} (the statement)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\text{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
Its conclusion: $k_B = 3\sqrt{2}$	

(L23) $k_B = 3\sqrt{2}$

[(I7)]

Lemma G.20	This proof
$\mathcal{F}$	$\mathcal{F}_{\text{fx}}$ (Definition I.1)
u	0
ζ	2^{-64} (the statement)
t_0, t_1, z_1	$\widetilde{t}_0, \widetilde{t}_1, \widetilde{z}_1$ (the statement)
(I8) l_{10}	$\widetilde{l}_{10}$ (LDL†, line 12)
$\tilde{tb}_0$	$\widetilde{tb}_0$ (the statement)
e_0, k_I	$0, \sqrt{2}(\lvert\widetilde{l}_{10}\rvert + 4)$ (L23)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\text{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
$t_0, t_1, z_1, l_{10} \in C_{\mathcal{F}}$	(L10), (L20), (L21)
Its conclusion: $\tilde{tb}_0 \,\mathcal{N}\,(u, (1+u)\lvert t_1 - z_1\rvert\lvert l_{10}\rvert e_0 + k_I\zeta)\, tb_0$	

(L24) $\widetilde{tb}_0 \,\mathcal{N}\left(0, \sqrt{2}(|\widetilde{l}_{10}| + 4)2^{-64}\right) \widetilde{t}_0 + (\widetilde{t}_1 - \widetilde{z}_1)\widetilde{l}_{10}$

[(I8)]

(L25) $|\widetilde{tb}_0 - (\widetilde{t}_0 + (\widetilde{t}_1 - \widetilde{z}_1)\widetilde{l}_{10})| \le e_I(\ell_{h-1})$

[(L24), (L21); Definition A.11; e_I (the statement)]

(L26) $|\widetilde{tb}_0| \le T_{\text{leaf}}$

[(L17), (L20), (L21), (L25); $|x+y| \le |x| + |y|$, $|xy| = |x||y|$ (Fact A.41, item 1); Fact A.41, item 8; T_{leaf} (the statement)]

(L27) $|\mathrm{Re}\,\widetilde{tb}_0|, |\mathrm{Im}\,\widetilde{tb}_0| \le T^*$

[(L1), (L26); $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \le |x|$ (Fact A.41, item 1)]

(L28) $\forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\}:\ W_{\mathfrak{p}(\widetilde{tb}_0)} = \mathfrak{p}(\widetilde{tb}_0)_{\text{fx64}} \bmod 2^{128}$

[(L10) along line 9 of deepest (Algorithm 7) from (L18), (L22) and (L15) at $\mu \in \{\mathrm{Re}\,\widetilde{t}_1, \mathrm{Im}\,\widetilde{t}_1\}$, at the bounds of (L17) to (L27), (L1) to (L4)]

(L29) $|\widetilde{tb}_0 - \widetilde{z}_0| \le H_{h-1}$

[(L16), (L27), (L28); $\forall a, b \in \mathbb{R}:\ |a+ib|^2 = a^2+b^2$ (Fact A.41, item 1); H_{h-1} (the statement)]

(L30) $|\widetilde{t}_0 - \widetilde{z}_0| \le D_{h-1}$

[(L20), (L21), (L25), (L29); $|x+y| \le |x|+|y|$, $|xy| = |x||y|$ (Fact A.41, item 1); Fact A.41, item 8; D_{h-1} (the statement)]

(L31) $\forall x \in X_\nu:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[(L10), (L15) along the lines of X_ν from (L18), (L22), (L28), at the bounds of (L17) to (L30), (L1) to (L4)]

(L32) $\forall x \in X_\nu:\ |x| \le 4T^*$

[(L1) to (L4), (L17) to (L30)]

(L33) $\Rightarrow\ P(h-1)$

[(L20), (L26), (L30), (L31), (L32); P (the proof's block)]

Proof of the step, $P(k+1) \Rightarrow\ P(k)$ *at* $k \le h-2$.

(L34) $\forall \psi:\ |\widetilde{t}_0(\psi)|, |\widetilde{t}_1(\psi)| \le T_k$

[$P(k)$'s call (the proof's block)]

(L35) $\forall j \in \{0,1\}\ \forall \psi\ \forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\}:\ W_{\mathfrak{p}(\widetilde{t}_j(\psi))} = \mathfrak{p}(\widetilde{t}_j(\psi))_{\mathrm{fx64}} \bmod 2^{128}$

[$P(k)$'s call (the proof's block)]

(L36) $\forall \psi:\ |\widetilde{t}_1(\psi)|, |\widetilde{t}_1(-\psi)| \le T^*$

[(L1), (L3), (L4), (L34)]

(L37) $\forall a, b \in \mathbb{C}:\ \|((a+b)/2,\ ((a-b)/2)\,\mathrm{conj}\,\psi)\|^2 = (|a|^2+|b|^2)/2$

[Fact A.41, its lead and items 1 and 2; Fact A.42, item 1]

(L38) $\Rightarrow\ \forall \psi:\ \|((\widetilde{t}_1(\psi)+\widetilde{t}_1(-\psi))/2,\ ((\widetilde{t}_1(\psi)-\widetilde{t}_1(-\psi))/2)\,\mathrm{conj}\,\psi)\| \le T^*$

[(L36), (L37); Fact A.41, item 5]

(I9)

Lemma G.14 at every i	This proof
$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
ζ	2^{-64} (the statement)
k	i (the scope)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
$k \in \{1, \dots, 2^{10}-1\}$	i, the scope
Its conclusion: $\tilde{\psi}_k\ \mathcal{I}\left(u^{\pm} + \sqrt{2}\zeta^{\pm}, 0\right)\ \psi_k$	

(L39) $\forall i:\ \widetilde{\psi}_i\ \mathcal{I}\left((\sqrt{2}\,\zeta)^{\pm}, 0\right)\ \psi_i$

[(I9)]

(I10)

Lemma G.17 $\forall \psi$	This proof
$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
ζ	2^{-64} (the statement)
a, b	$\widetilde{t}_1(\psi), \widetilde{t}_1(-\psi)$ (the statement)
ψ	ψ (the scope)
$\tilde{\psi}$	$\widetilde{\psi}$ (Lemma G.14)
$\tilde{f}_0, \tilde{f}_1$	$\widetilde{c}_0, \widetilde{c}_1$ (the proof's block)
(f_0, f_1)	split$(\widetilde{t}_1)$ (split (Algorithm 2))
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
$a, b \in C_{\mathcal{F}}$	(L10), (L36)
$\psi \in \mathbb{C}$	The scope
$\tilde{\psi} \in C_{\mathcal{F}}$	$\widetilde{\psi}$ (Definition A.8)
Assumption A1	Fact A.42, item 1
Assumption A2	(L39)
Its conclusion: $(\tilde{f}_0, \tilde{f}_1)\ \mathcal{N}\left(c_{\mathrm{split}}, \left(\frac{\sqrt{2}}{2} + k_D\right)\zeta\right)\ (f_0, f_1)$	

(L40) $(\widetilde{c}_0, \widetilde{c}_1)\ \mathcal{N}\left(c_{\mathrm{split}}, \left(\frac{\sqrt{2}}{2} + k_D\right) 2^{-64}\right)$ split$(\widetilde{t}_1)$

[(I10)]

(L41) $\|(\widetilde{c}_0, \widetilde{c}_1) - \widetilde{\text{split}}(\widetilde{t}_1)\| \le e_s$

[(L40), (L38); Definition A.11; e_s (the statement)]

(L42) $\forall \psi' : \ |\widetilde{c}_0(\psi')|, |\widetilde{c}_1(\psi')| \le T_{k+1}$

[(L34), (L41); $|\psi| = 1$ (Fact A.42, item 1); $|x+y| \le |x| + |y|$ (Fact A.41, item 1); T_{k+1} (the statement)]

(L43) $\forall j \in \{0,1\}\ \forall \psi'\ \forall \mathfrak{p} \in \{\text{Re}, \text{Im}\} : \ W_{\mathfrak{p}(\widetilde{c}_j(\psi'))} = \mathfrak{p}(\widetilde{c}_j(\psi'))_{\text{fx64}} \bmod 2^{128}$

[(L10) along lines 4 and 6 of $\widetilde{\text{split}}$ (Algorithm 2) on $\widetilde{t}_1$ from (L35) and the stored twiddles' words (Definition I.1, item 5), at the bounds of (L34) to (L42), (L1) to (L4)]

(L44) $\forall \psi' : \ |\widetilde{c}_j(\psi') - \widetilde{z}_{1,j}(\psi')| \le D_{k+1}$

[$P(k+1)$ at (L42), (L43); (L2)]

(L45) $\forall j \in \{0,1\}\ \forall \psi'\ \forall \mathfrak{p} \in \{\text{Re}, \text{Im}\} : \ W_{\mathfrak{p}(\widetilde{z}_{1,j}(\psi'))} = \mathfrak{p}(\widetilde{z}_{1,j}(\psi'))_{\text{fx64}} \bmod 2^{128}$

[$P(k+1)$ at (L42), (L43): item 5 at the call of line 19]

(L46) $\forall \psi' : \ |\widetilde{z}_{1,j}(\psi')| \le 2T^*$

[(L1), (L3), (L4), (L42), (L44); $|x+y| \le |x| + |y|$ (Fact A.41, item 1)]

(L47) $\|(\widetilde{z}_{1,0} + \psi\widetilde{z}_{1,1},\ \widetilde{z}_{1,0} - \psi\widetilde{z}_{1,1})\|^2 = 2(|\widetilde{z}_{1,0}|^2 + |\widetilde{z}_{1,1}|^2)$

[Fact A.41, its lead and item 2, at $(x,y) := (\widetilde{z}_{1,0}, \psi\widetilde{z}_{1,1})$; Fact A.41, item 1; Fact A.42, item 1]

(L48) $\Rightarrow \ \|(\widetilde{z}_{1,0} + \psi\widetilde{z}_{1,1},\ \widetilde{z}_{1,0} - \psi\widetilde{z}_{1,1})\| \le 4T^*$

[(L47), (L46); Fact A.41, item 5]

(I11)

Lemma G.18 $\forall\psi$	This proof
$\mathcal{F}$	$\mathcal{F}_{\text{fx}}$ (Definition I.1)
u	0
ζ	2^{-64} (the statement)
f_0, f_1	$\widetilde{z}_{1,0}, \widetilde{z}_{1,1}$ (the statement)
ψ	ψ (the scope)
$\tilde{\psi}$	$\widetilde{\psi}$ (Lemma G.14)
$\tilde{a}, \tilde{b}$	$\widetilde{z}_1(\psi), \widetilde{z}_1(-\psi)$ ($\widetilde{\text{merge}}$, line 21)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\text{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
$f_0, f_1 \in C_{\mathcal{F}}$	(L10), (L46)
$\psi \in \mathbb{C}$	The scope
$\tilde{\psi} \in C_{\mathcal{F}}$	$\widetilde{\psi}$ (Definition A.8)
Assumption A1	Fact A.42, item 1
Assumption A2	(L39)
Its conclusion: $(\tilde{a}, \tilde{b})\ \mathcal{N}\ (c_{\text{merge}}, k_E\zeta)\ (a, b)$	

(L49) $(\widetilde{z}_1(\psi), \widetilde{z}_1(-\psi))\ \mathcal{N}\ (c_{\text{merge}}, k_E 2^{-64})\ (\widetilde{z}_{1,0} + \psi\widetilde{z}_{1,1}, \widetilde{z}_{1,0} - \psi\widetilde{z}_{1,1})$

[(I11)]

(L50) $\|(\widetilde{z}_1(\psi), \widetilde{z}_1(-\psi)) - (\widetilde{z}_{1,0} + \psi\widetilde{z}_{1,1}, \widetilde{z}_{1,0} - \psi\widetilde{z}_{1,1})\| \le e_m$

[(L49), (L48); Definition A.11; e_m (the statement)]

(L51) $\forall \psi\ \forall \mathfrak{p} \in \{\text{Re}, \text{Im}\} : \ W_{\mathfrak{p}(\widetilde{z}_1(\psi))} = \mathfrak{p}(\widetilde{z}_1(\psi))_{\text{fx64}} \bmod 2^{128}$

[(L10) along line 4 of $\widetilde{\text{merge}}$ (Algorithm 4) and the sum and the difference after it, at line 21, from (L45) and the stored twiddles' words (Definition I.1, item 5), at the bounds of (L44) to (L50), (L1) to (L4)]

(L52) $|\widetilde{t}_1 - \widetilde{z}_1| \le H_k$

[(L41), (L44), (L50); split (Algorithm 2), Post; $|\psi| = 1$ (Fact A.42, item 1); $|x+y| \le |x| + |y|$, $|xy| = |x||y|$ (Fact A.41, item 1); H_k (the statement)]

	Lemma I.48	This proof
	Shared: (f,g,F,G), ν	
	$\ell_{\text{root}}, \ell_{\text{child}}$	ℓ_0, ℓ_k (the statement)
	(f,g,F,G) checked key of degree $n \in \{512, 1024\}$	The statement
(I12)	ν a node of the tree recursion	The statement
	Assumption A1	$k = 0$
	Assumption A2	$k \geq 1$
	Its item 1: $\forall \psi : \ \lvert\widetilde{l}_{10}\rvert \leq \ell_{\text{root}}$	
	Its item 2: $\forall \psi : \ \lvert\widetilde{l}_{10}\rvert \leq \ell_{\text{child}}$	

(L53) $k = 0 \Rightarrow \ \forall \psi : \ \lvert\widetilde{l}_{10}\rvert \leq \ell_0$

[item 1 of (I12)]

(L54) $k \geq 1 \Rightarrow \ \forall \psi : \ \lvert\widetilde{l}_{10}\rvert \leq \ell_k$

[item 2 of (I12)]

(L55) $\lvert\widetilde{l}_{10}\rvert \leq \ell_k$

[(L53), (L54)]

	Lemma I.39, item 1 at $k = 0$	This proof
	$(f,g,F,G), n$	$(f,g,F,G), n$ (the statement)
	W_x	$W_{\mathfrak{p}(\widetilde{l}_{10}(\psi))}$ (LDL†, line 12)
	$n \in \{512, 1024\}$	Definition 5.5, item 1
(I13)	(f,g,F,G) key of degree n	The statement
	W_x a word of the root's step	$\widetilde{l}_{10}$ (LDL† (Algorithm 5), line 12) at the call ν at $k = 0$
	Assumption A1	Definition 5.5, item 2
	Assumption A2	Definition 5.5, item 3
	Its conclusion: $W_x = x_{\text{fx64}} \bmod 2^{128}$	

(L56) $k = 0 \Rightarrow \ \forall \psi \ \forall \mathfrak{p} \in \{\text{Re}, \text{Im}\} : \ W_{\mathfrak{p}(\widetilde{l}_{10}(\psi))} = \mathfrak{p}(\widetilde{l}_{10}(\psi))_{\text{fx64}} \bmod 2^{128}$

[(I13)]

(L57) $k \geq 1 \Rightarrow \ \forall \psi \ \forall \mathfrak{p} \in \{\text{Re}, \text{Im}\} : \ W_{\mathfrak{p}(\widetilde{l}_{10}(\psi))} = \mathfrak{p}(\widetilde{l}_{10}(\psi))_{\text{fx64}} \bmod 2^{128}$

[Lemma I.44, item 1, at the checked key (the statement): $\widetilde{l}_{10}$, a word of LDL† (Algorithm 5), line 12, below the root at $m = 2^{h-k}$]

	Lemma G.20	This proof
	$\mathcal{F}$	$\mathcal{F}_{\text{fx}}$ (Definition I.1)
	u	0
	ζ	2^{-64} (the statement)
	t_0, t_1, z_1	$\widetilde{t}_0, \widetilde{t}_1, \widetilde{z}_1$ (the statement)
(I14)	l_{10}	$\widetilde{l}_{10}$ (LDL†, line 12)
	$\tilde{tb}_0$	$\widetilde{tb}_0$ (the statement)
	e_0, k_I	$0, \sqrt{2}(\lvert\widetilde{l}_{10}\rvert + 4)$ (L23)
	$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\text{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
	$t_0, t_1, z_1, l_{10} \in C_{\mathcal{F}}$	(L10), (L52), (L55)
	Its conclusion: $\tilde{tb}_0 \, \mathcal{N}\,(u, (1+u)\lvert t_1 - z_1\rvert\lvert l_{10}\rvert e_0 + k_I\zeta) \, tb_0$	

(L58) $\widetilde{tb}_0 \, \mathcal{N}\left(0, \sqrt{2}(\lvert\widetilde{l}_{10}\rvert + 4)2^{-64}\right) \widetilde{t}_0 + (\widetilde{t}_1 - \widetilde{z}_1)\widetilde{l}_{10}$

[(I14)]

(L59) $\lvert\widetilde{tb}_0 - (\widetilde{t}_0 + (\widetilde{t}_1 - \widetilde{z}_1)\widetilde{l}_{10})\rvert \leq e_I(\ell_k)$

[(L58), (L55); Definition A.11; e_I (the statement)]

(L60) $\lvert\widetilde{tb}_0\rvert \leq T_k + \ell_k H_k + e_I(\ell_k)$

[(L34), (L52), (L55), (L59); $\lvert x + y\rvert \leq \lvert x\rvert + \lvert y\rvert$, $\lvert xy\rvert = \lvert x\rvert\lvert y\rvert$ (Fact A.41, item 1); Fact A.41, item 8]

(L61) $\forall\psi\ \forall\mathfrak{p}\in\{\mathrm{Re},\mathrm{Im}\}:\ W_{\mathfrak{p}(\widetilde{tb}_0(\psi))}=\mathfrak{p}(\widetilde{tb}_0(\psi))_{\mathrm{fx64}}\bmod 2^{128}$

[(L10) along line 25 of ffsamp (Algorithm 6) from (L35), (L51), (L56), (L57), at the bounds of (L34) to (L60), (L1) to (L4)]

(L62) $\forall\psi:\ |\widetilde{tb}_0(\psi)|,|\widetilde{tb}_0(-\psi)|\le T^*$

[(L60); T_{k+1} (the statement); (L1), (L3), (L4)]

(L63) $\Rightarrow\ \forall\psi:\ \|((\widetilde{tb}_0(\psi)+\widetilde{tb}_0(-\psi))/2,\ ((\widetilde{tb}_0(\psi)-\widetilde{tb}_0(-\psi))/2)\operatorname{conj}\psi)\|\le T^*$

[(L62), (L37); Fact A.41, item 5]

Lemma G.17 $\forall\psi$	This proof
$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
ζ	2^{-64} (the statement)
a,b	$\widetilde{tb}_0(\psi),\widetilde{tb}_0(-\psi)$ (the statement)
ψ	ψ (the scope)
$\tilde{\psi}$	$\widetilde{\psi}$ (Lemma G.14)
$\tilde{f}_0,\tilde{f}_1$	$\widetilde{c}'_0,\widetilde{c}'_1$ (the proof's block)
(I15) (f_0,f_1)	$\widetilde{\mathrm{split}}(\widetilde{tb}_0)$ (split (Algorithm 2))
$\mathcal{F}$ realization at (u,ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0,2^{-64})$ (Definition I.1)
$a,b\in C_{\mathcal{F}}$	(L10), (L62)
$\psi\in\mathbb{C}$	The scope
$\tilde{\psi}\in C_{\mathcal{F}}$	$\widetilde{\psi}$ (Definition A.8)
Assumption A1	Fact A.42, item 1
Assumption A2	(L39)
Its conclusion: $(\tilde{f}_0,\tilde{f}_1)\,\mathcal{N}\left(c_{\mathrm{split}},\left(\frac{\sqrt{2}}{2}+k_D\right)\zeta\right)(f_0,f_1)$	

(L64) $(\widetilde{c}'_0,\widetilde{c}'_1)\,\mathcal{N}\left(c_{\mathrm{split}},\left(\frac{\sqrt{2}}{2}+k_D\right)2^{-64}\right)\widetilde{\mathrm{split}}(\widetilde{tb}_0)$

[(I15)]

(L65) $\|(\widetilde{c}'_0,\widetilde{c}'_1)-\widetilde{\mathrm{split}}(\widetilde{tb}_0)\|\le e_s$

[(L64), (L63); Definition A.11; e_s (the statement)]

(L66) $\forall\psi':\ |\widetilde{c}'_0(\psi')|,|\widetilde{c}'_1(\psi')|\le T_{k+1}$

[(L60), (L65); $|\psi|=1$ (Fact A.42, item 1); $|x+y|\le|x|+|y|$ (Fact A.41, item 1); T_{k+1} (the statement)]

(L67) $\forall j\in\{0,1\}\ \forall\psi'\ \forall\mathfrak{p}\in\{\mathrm{Re},\mathrm{Im}\}:\ W_{\mathfrak{p}(\widetilde{c}'_j(\psi'))}=\mathfrak{p}(\widetilde{c}'_j(\psi'))_{\mathrm{fx64}}\bmod 2^{128}$

[(L10) along lines 4 and 6 of $\widetilde{\mathrm{split}}$ (Algorithm 2) on $\widetilde{tb}_0$ from (L61) and the stored twiddles' words (Definition I.1, item 5), at the bounds of (L60) to (L66), (L1) to (L4)]

(L68) $\forall\psi':\ |\widetilde{c}'_j(\psi')-\widetilde{z}_{0,j}(\psi')|\le D_{k+1}$

[$P(k+1)$ at (L66), (L67); (L2)]

(L69) $\forall j\in\{0,1\}\ \forall\psi'\ \forall\mathfrak{p}\in\{\mathrm{Re},\mathrm{Im}\}:\ W_{\mathfrak{p}(\widetilde{z}_{0,j}(\psi'))}=\mathfrak{p}(\widetilde{z}_{0,j}(\psi'))_{\mathrm{fx64}}\bmod 2^{128}$

[$P(k+1)$ at (L66), (L67): item 5 at the call of line 33]

(L70) $\forall\psi':\ |\widetilde{z}_{0,j}(\psi')|\le 2T^*$

[(L1), (L3), (L4), (L66), (L68); $|x+y|\le|x|+|y|$ (Fact A.41, item 1)]

(L71) $\|(\widetilde{z}_{0,0}+\psi\widetilde{z}_{0,1},\ \widetilde{z}_{0,0}-\psi\widetilde{z}_{0,1})\|^2=2(|\widetilde{z}_{0,0}|^2+|\widetilde{z}_{0,1}|^2)$

[Fact A.41, its lead and item 2, at $(x,y):=(\widetilde{z}_{0,0},\psi\widetilde{z}_{0,1})$; Fact A.41, item 1; Fact A.42, item 1]

(L72) $\Rightarrow\ \|(\widetilde{z}_{0,0}+\psi\widetilde{z}_{0,1},\ \widetilde{z}_{0,0}-\psi\widetilde{z}_{0,1})\|\le 4T^*$

[(L71), (L70); Fact A.41, item 5]

Lemma G.18 $\forall\psi$	This proof
$\mathcal{F}$	$\mathcal{F}_{\text{fx}}$ (Definition I.1)
u	0
ζ	2^{-64} (the statement)
f_0, f_1	$\widetilde{z}_{0,0}, \widetilde{z}_{0,1}$ (the statement)
ψ	ψ (the scope)
$\tilde{\psi}$	$\widetilde{\psi}$ (Lemma G.14)
(I16) $\tilde{a}, \tilde{b}$	$\widetilde{z}_0(\psi), \widetilde{z}_0(-\psi)$ ($\widetilde{\text{merge}}$, line 35)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\text{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
$f_0, f_1 \in C_{\mathcal{F}}$	(L10), (L70)
$\psi \in \mathbb{C}$	The scope
$\tilde{\psi} \in C_{\mathcal{F}}$	$\widetilde{\psi}$ (Definition A.8)
Assumption A1	Fact A.42, item 1
Assumption A2	(L39)
Its conclusion: $(\tilde{a}, \tilde{b})\ \mathcal{N}\ (c_{\text{merge}}, k_E\zeta)\ (a, b)$	

(L73) $(\widetilde{z}_0(\psi), \widetilde{z}_0(-\psi))\ \mathcal{N}\ (c_{\text{merge}}, k_E 2^{-64})\ (\widetilde{z}_{0,0} + \psi\widetilde{z}_{0,1}, \widetilde{z}_{0,0} - \psi\widetilde{z}_{0,1})$

[(I16)]

(L74) $\|(\widetilde{z}_0(\psi), \widetilde{z}_0(-\psi)) - (\widetilde{z}_{0,0} + \psi\widetilde{z}_{0,1}, \widetilde{z}_{0,0} - \psi\widetilde{z}_{0,1})\| \leq e_m$

[(L73), (L72); Definition A.11; e_m (the statement)]

(L75) $|\widetilde{t}b_0 - \widetilde{z}_0| \leq H_k$

[(L65), (L68), (L74); split (Algorithm 2), Post; $|\psi| = 1$ (Fact A.42, item 1); $|x + y| \leq |x| + |y|$, $|xy| = |x||y|$ (Fact A.41, item 1); H_k (the statement)]

(L76) $|\widetilde{t}_0 - \widetilde{z}_0| \leq D_k$

[(L52), (L55), (L59), (L75); $|x + y| \leq |x| + |y|$, $|xy| = |x||y|$ (Fact A.41, item 1); Fact A.41, item 8; D_k (the statement)]

(L77) $\forall x \in X_\nu :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[(L43), (L51), (L61), (L67); (L10) along the lines of X_ν from (L35), (L45), (L56), (L57), (L69) and the stored twiddles' words (Definition I.1, item 5), at the bounds of (L34) to (L76), (L1) to (L4)]

(L78) $\forall x \in X_\nu :\ |x| \leq 4T^*$

[(L1) to (L4), (L34) to (L76)]

(L79) $\Rightarrow\ P(k)$

[(L42), (L43), (L44), (L52), (L66), (L67), (L68), (L76), (L77), (L78); $P(k+1)$ at (L42), (L43) and at (L66), (L67); P (the proof's block)]

Proof of items 1 to 6.

Lemma I.47, items 1 and 2 at $k = 0$	This proof
Shared: $h, n,\ (f, g, F, G),\ \mathsf{h}(\mathsf{m})$ (Definition A.25)	
W_x	W_x (ffSampling$^{\mathcal{F}}$, lines 9, 16 and 18)
$h \in \{3, \ldots, 10\}$	$n \in \{512, 1024\}$ (the statement)
(f, g, F, G) key of degree n	The statement
$\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$	$\mathsf{h}(\mathsf{m})$ (Definition A.25)
(I17) W_x a word of the center's first computation	ffSampling$^{\mathcal{F}}$, lines 9, 16 and 18
Assumption A1	Definition 5.5, item 2; $B_{fg} \leq 127$ (B_{fg}, Definition 5.5)
Assumption A2	Definition 5.5, item 3
Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
Its item 2: $\lvert x_{\text{fx64}}\rvert < 2^{127}$	

Lemma I.46, items 1 and 2 at $k=0$		This proof
Shared: $h, n,\ (f,g,F,G),\ \mathsf{h}(\mathsf{m})$ (Definition A.25)		
(I18)	W_x $h \in \{3,\dots,10\}$ (f,g,F,G) key of degree n $\mathsf{h}(\mathsf{m}) \in \{0,\dots,q-1\}^n$ W_x a word of the center's first computation	W_x (center$_{\text{frac}}$, lines 7 and 12) $n \in \{512, 1024\}$ (the statement) The statement $\mathsf{h}(\mathsf{m})$ (Definition A.25) center$_{\text{frac}}$, lines 7 and 12
Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$		
Its item 2: $\lvert x_{\text{fx64}}\rvert < 2^{127}$		

(L80) $k=0 \Rightarrow\ \forall \psi :\ |\widetilde{t}_0(\psi)|, |\widetilde{t}_1(\psi)| \le T_0$

[item 2 of (I17), item 2 of (I18); [gate: `verify/gates/fx/ranges.py`], each row the bound its lemma proves on a part; $\forall a,b \in \mathbb{R} :\ |a+ib|^2 = a^2+b^2$ (Fact A.41, item 1); T_0 (the statement)]

(L81) $k=0 \Rightarrow\ \forall j \in \{0,1\}\ \forall \psi\ \forall \mathfrak{p} \in \{\mathrm{Re}, \mathrm{Im}\} :\ W_{\mathfrak{p}(\widetilde{t}_j(\psi))} = \mathfrak{p}(\widetilde{t}_j(\psi))_{\text{fx64}} \bmod 2^{128}$

[item 1 of (I17), item 1 of (I18): the words of ffSampling$^{\mathcal{F}}$, lines 16 and 18, and of center$_{\text{frac}}$, line 12, the center the call at $k=0$ receives]

(L82) $P(0)$

[induction on $h-1-k$: (L33), (L79)]

(L83) $\Rightarrow$ item 1

[(L80), (L81), (L82); P (the proof's block)]

(L84) $\Rightarrow$ item 4

[(L80), (L81), (L82); P (the proof's block)]

(L85) $\Rightarrow$ item 5

[(L80), (L81), (L82); P (the proof's block)]

(L86) $\Rightarrow$ item 2

[(L80), (L81), (L82); P (the proof's block); assumption A1]

(L87) $\Rightarrow$ item 3

[(L80), (L81), (L82); P (the proof's block)]

(L88) $\Rightarrow$ item 6

[(L80), (L81), (L82); P (the proof's block)]

□ (items 1 to 6)

I.3.6 No overflow in the base sampler

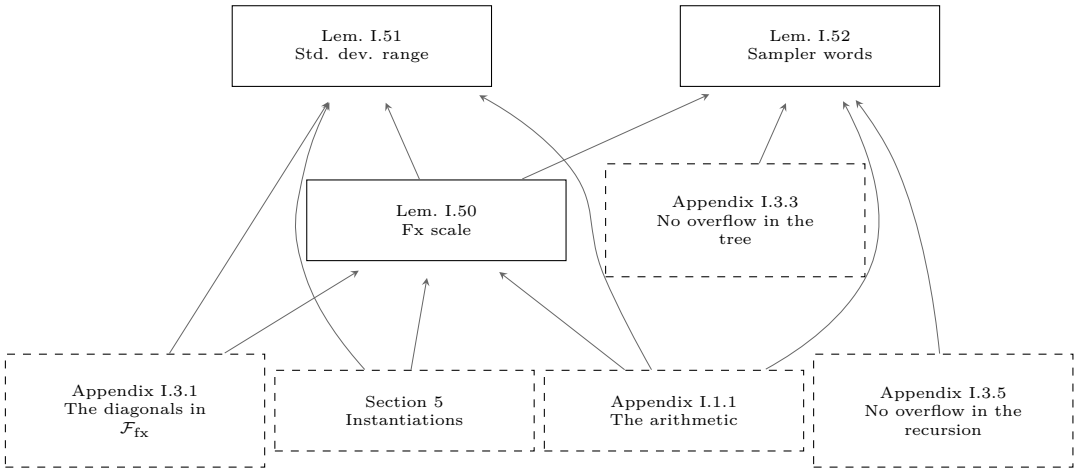


Figure 80: Dependencies, Appendix I.3.6.

Lemma I.50 (The fixed-point signer's scale [to table])**.** *The computed scale of the base sampler is below* 1 *at every leaf. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5), of degree* $n = 2^h \in \{512, 1024\}$*;*
- `isigma` *be an inverse standard deviation that a call of* SamplerZ *(Algorithm 8) by* deepest *(Algorithm 7) takes, in either center's mode.*

Define:

- $\sigma_{\min}$*, the number of the word* `FXP_SIGMA_MIN`$[h]$ *[L0: fxp/fxp_consts.h: 2073-2084];*
- $\widetilde{ccs} := \mathrm{fl}(\texttt{isigma} \cdot \sigma_{\min})$ *(line 6 of* SamplerZ *in* $\mathcal{F}_{\mathrm{fx}}$*).*

Then

$$\widetilde{ccs} < 1.$$

Proof.

COMPUTES $\widetilde{d}$: the diagonal $\widetilde{d}_{00}$ or $\widetilde{d}_{11}$ of deepest (Algorithm 7) on which lines 1 and 3, or their counterparts at $\widetilde{d}_{00}$, compute `isigma`
DEFINES d: the leaf diagonal over $\mathbb{R}$ at the same leaf (Definition A.19)
COMPUTES $\widetilde{r}$: the number line 1 or its counterpart computes on $\widetilde{d}$ in $\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
DEFINES χ_{leaf}, that of Corollary G.36 at the key's tree
DEFINES χ_k, $0 \le k \le h-1$, those of Lemma I.43 at the checked key
DEFINES $(\nu_k)_{0 \le k \le h-1}$: a path of the key's tree to the node of degree 2 above the leaf (Definition I.32)
DEFINES `INV_SIGMA`, the number of the word `FXP_INV_SIGMA`$[h]$ [L0: fxp/fxp_consts.h:2058-2070]
DEFINES $\max_k \chi_k$, the maximum of χ_k over $0 \le k \le h-1$
DEFINES $\bar{c} = ((\sqrt{16822(1 + \max_k \chi_k)} + \zeta_{\mathrm{op}})\,\texttt{INV_SIGMA} + \zeta_{\mathrm{op}})\,\sigma_{\min} + \zeta_{\mathrm{op}}$

(L1) $d \in [q^2/16822,\ 16822]$
[Proposition D.9 at the key, a key of line 3 of keygen (Algorithm 11)]

(L2) $q^2/16822 > 0$
[expand]

(L3) $d > 0$
[(L1), (L2)]

(L4) $|\widetilde{d}/d - 1| \le \chi_{\mathrm{leaf}}$
[χ_{leaf} (Corollary G.36), at the node of degree 2 above the leaf]

(L5) $\widetilde{d} \le d(1 + \chi_{\mathrm{leaf}})$
[(L3), (L4)]

Corollary I.33, item 2 at the checked key	This proof
Shared: $(f, g, F, G), n, h,\ (\nu_k)_{0 \le k \le h-1}, \chi_0, \chi_{h-1}, \chi_{\mathrm{leaf}}$	
(f, g, F, G) checked key of degree $n = 2^h$	The statement
(I1) $(\nu_k)_{0 \le k \le h-1}$ a path of T $\chi_0 \in [0, 1)$	The proof's block Lemma I.43, the first measured row; $\mathcal{A}$ (Definition I.32)
Assumption A1 Assumption A2 Assumption A3	Lemma I.43, (L8) Lemma I.43, (L9) Lemma I.43, the first measured row
Its conclusion: $\chi_{\mathrm{leaf}} \le \chi_{h-1}$	

(L6) $\chi_{\mathrm{leaf}} \le \chi_{h-1}$
[(I1)]

(L7) $\chi_{h-1} \le \max_k \chi_k$
[$\max_k \chi_k$ (the proof's block)]

(L8) $\widetilde{d} \le 16822(1 + \max_k \chi_k)$
[(L1), (L3), (L5), (L6), (L7); $\forall a, a', b, b' \in \mathbb{R},\ 0 \le a \le a',\ 0 \le b \le b' :\ ab \le a'b'$ (Fact A.41, item 8)]

(L9) $\widetilde{d} \geq 0$
[Lemma I.43, item 2, at the checked key (the statement) and the path $(\nu_k)_{0\leq k\leq h-1}$ (the proof's block)]

(L10) $\widetilde{r} \leq \sqrt{\widetilde{d}} + \zeta_{\mathrm{op}}$
[deepest (Algorithm 7), line 1; Definition I.1, item 1, at $\sqrt{\cdot}$; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1); (L9)]

(L11) $\sqrt{\widetilde{d}} \leq \sqrt{16822(1 + \max_k \chi_k)}$
[(L8), (L9); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L12) $\texttt{INV_SIGMA}, \sigma_{\min} \geq 0$
[the stored words $\texttt{FXP_INV_SIGMA}[h]$ and $\texttt{FXP_SIGMA_MIN}[h]$ [L0: `fxp/fxp_consts.h:2058-2070`] [L0: `fxp/fxp_consts.h:2073-2084`]]

(L13) $\widetilde{r}, \texttt{isigma} \geq 0$
[deepest (Algorithm 7), lines 1 and 3; (L9), (L12); $\forall a, b \in \mathbb{R},\ a \leq b :\ \mathrm{fl}(a) \leq \mathrm{fl}(b)$, and $\mathrm{fl}(0) = 0$ (Fact A.6, item 9)]

(L14) $\texttt{isigma} \leq \widetilde{r}\,\texttt{INV_SIGMA} + \zeta_{\mathrm{op}}$
[deepest (Algorithm 7), line 3; Definition I.1, item 1, at $\times$; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1)]

(L15) $\widetilde{ccs} \leq \texttt{isigma} \cdot \sigma_{\min} + \zeta_{\mathrm{op}}$
[$\widetilde{ccs}$ (the statement); Definition I.1, item 1, at $\times$]

(L16) $\widetilde{ccs} \leq \bar{c}$
[(L10) to (L15); $\forall a, a', b, b' \in \mathbb{R},\ 0 \leq a \leq a',\ 0 \leq b \leq b' :\ ab \leq a'b'$ (Fact A.41, item 8); $\bar{c}$ (the proof's block)]

(L17) $\bar{c} < 1$
[[gate: `verify/gates/fx/ccs.py`], on the proved bounds of Proposition 5.8, items 1 to 4, in both modes, at the checked key (the statement)]

(L18) $\Rightarrow$ the statement
[(L16), (L17)]

□

Lemma I.51 (The range of the computed leaf standard deviation [to table])**.** *The computed standard deviation of every leaf lies above $\sigma_{\min}$ and at most σ_0. Let:*

- *(f, g, F, G) be a checked key (Definition 5.5), of degree $n = 2^h \in \{512, 1024\}$;*
- *$\texttt{isigma}$ be an inverse standard deviation that a call of* SamplerZ *(Algorithm 8) by* deepest *(Algorithm 7) takes, in either center's mode.*

Define:

- *$\sigma_{\min}$, the number of the word $\texttt{FXP_SIGMA_MIN}[h]$ [L0: `fxp/fxp_consts.h:2073-2084`];*
- *$\widetilde{\sigma} := 1/\texttt{isigma}$;*
- *$\sigma_0 := 1.8205$ (line 9 of* SamplerZ*).*

Then

1. *$\widetilde{\sigma} > \sigma_{\min}$;*
2. *$\widetilde{\sigma} \leq \sigma_0$.*

Proof.

COMPUTES $\widetilde{d}$: the diagonal $\widetilde{d}_{00}$ or $\widetilde{d}_{11}$ of deepest (Algorithm 7) on which lines 1 and 3, or their counterparts at $\widetilde{d}_{00}$, compute `isigma`

DEFINES d: the leaf diagonal over $\mathbb{R}$ at the same leaf (Definition A.19)

COMPUTES $\widetilde{r}$: the number line 1 or its counterpart computes on $\widetilde{d}$ in $\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)

DEFINES χ_{leaf}, that of Corollary G.36 at the key's tree

DEFINES χ_k, $0 \le k \le h-1$, those of Lemma I.43 at the checked key

DEFINES $(\nu_k)_{0\le k\le h-1}$: a path of the key's tree to the node of degree 2 above the leaf (Definition I.32)

DEFINES `INV_SIGMA`, the number of the word `FXP_INV_SIGMA`$[h]$ [L0: `fxp/fxp_consts.h:2058-2070`]

COMPUTES $\widetilde{c\mathrm{cs}} = \mathrm{fl}(\texttt{isigma} \cdot \sigma_{\min})$, line 6 of SamplerZ (Algorithm 8) in $\mathcal{F}_{\mathrm{fx}}$

DEFINES $\max_k \chi_k$, the maximum of χ_k over $0 \le k \le h-1$

DEFINES $\bar{L} = (\sqrt{(q^2/16822)(1-\max_k \chi_k)} - \zeta_{\mathrm{op}})\,\texttt{INV_SIGMA} - \zeta_{\mathrm{op}}$

(L1) $d \in [q^2/16822,\ 16822]$

[Proposition D.9 at the key, a key of line 3 of keygen (Algorithm 11)]

(L2) $q^2/16822 > 0$

[expand]

(L3) $d > 0$

[(L1), (L2)]

(L4) $|\widetilde{d}/d - 1| \le \chi_{\mathrm{leaf}}$

[χ_{leaf} (Corollary G.36), at the node of degree 2 above the leaf]

(L5) $\widetilde{d} \ge d(1-\chi_{\mathrm{leaf}})$

[(L3), (L4)]

Corollary I.33, item 2 at the checked key	This proof
Shared: $(f,g,F,G), n, h,\ (\nu_k)_{0\le k\le h-1}, \chi_0, \chi_{h-1}, \chi_{\mathrm{leaf}}$	
(f,g,F,G) checked key of degree $n = 2^h$	The statement
(I1) $(\nu_k)_{0\le k\le h-1}$ a path of T	The proof's block
$\chi_0 \in [0,1)$	Lemma I.43, the first measured row; $\mathcal{A}$ (Definition I.32)
Assumption A1	Lemma I.43, (L8)
Assumption A2	Lemma I.43, (L9)
Assumption A3	Lemma I.43, the first measured row
Its conclusion: $\chi_{\mathrm{leaf}} \le \chi_{h-1}$	

(L6) $\chi_{\mathrm{leaf}} \le \chi_{h-1}$

[(I1)]

(L7) $\chi_{h-1} \le \max_k \chi_k$

[$\max_k \chi_k$ (the proof's block)]

(L8) $\max_k \chi_k \le 1/2$

[[gate: `verify/gates/fx/node_chi.py`], on the proved bounds of Proposition 5.8, items 1 to 4, in both modes, at the checked key (the statement)]

(L9) $\widetilde{d} \ge (q^2/16822)(1-\max_k \chi_k)$

[(L1), (L2), (L5), (L6), (L7), (L8); $\forall a, a', b, b' \in \mathbb{R},\ 0 \le a \le a',\ 0 \le b \le b' :\ ab \le a'b'$ (Fact A.41, item 8)]

(L10) $\widetilde{r} \ge \sqrt{\widetilde{d}} - \zeta_{\mathrm{op}}$

[deepest (Algorithm 7), line 1; Definition I.1, item 1, at $\sqrt{\cdot}$; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1); (L2), (L8), (L9)]

(L11) $\sqrt{\widetilde{d}} \ge \sqrt{(q^2/16822)(1-\max_k \chi_k)}$

[(L2), (L8), (L9); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L12) `INV_SIGMA` ≥ 0

[the stored word `FXP_INV_SIGMA`$[h]$ [L0: `fxp/fxp_consts.h:2058-2070`]]

(L13) $\texttt{isigma} \geq \widetilde{r}\,\texttt{INV_SIGMA} - \zeta_{\mathrm{op}}$
[deepest (Algorithm 7), line 3; Definition I.1, item 1, at $\times$; $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1)]

(L14) $\bar{L} > 0$
[[gate: `verify/gates/fx/sigma0.py`], on the proved bounds of Proposition 5.8, items 1 to 4, in both modes, at the checked key (the statement)]

(L15) $1/\bar{L} \leq \sigma_0$
[[gate: `verify/gates/fx/sigma0.py`], on the proved bounds of Proposition 5.8, items 1 to 4, in both modes, at the checked key (the statement)]

(L16) $\widetilde{r} \geq \sqrt{(q^2/16822)(1 - \max_k \chi_k)} - \zeta_{\mathrm{op}}$
[(L10), (L11)]

(L17) $\widetilde{r}\,\texttt{INV_SIGMA} \geq (\sqrt{(q^2/16822)(1 - \max_k \chi_k)} - \zeta_{\mathrm{op}})\,\texttt{INV_SIGMA}$
[(L16), (L12); Fact A.41, item 26, at $c := \texttt{INV_SIGMA}$]

(L18) $\Rightarrow$ $\texttt{isigma} \geq \bar{L}$
[(L13), (L17); $\bar{L}$ (the proof's block)]

(L19) $1/\texttt{isigma} \leq 1/\bar{L}$
[(L14), (L18); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L20) $\texttt{isigma} > 0$
[(L14), (L18)]

Lemma I.50	This proof
(I2) Shared: (f, g, F, G), $\texttt{isigma}$, $\sigma_{\min}$, $\widetilde{ccs}$	
Its conclusion: $\widetilde{ccs} < 1$	

(L21) $\texttt{isigma} \cdot \sigma_{\min} < 1$
[(I2); $\widetilde{ccs}$ (the proof's block); $\forall a, b \in \mathbb{R},\ a \leq b :\ \mathrm{fl}(a) \leq \mathrm{fl}(b)$ (Fact A.6, item 9); $\mathrm{fl}(1) = 1$ (Fact A.6, item 4)]

(L22) $\Rightarrow$ item 1
[(L20), (L21); $\widetilde{\sigma}$ (the statement)]

(L23) $\Rightarrow$ item 2
[(L15), (L19); $\widetilde{\sigma}$ (the statement)]

$\square$ (items 1 and 2)

Lemma I.52 (No overflow in the base sampler [to table])**.** *Every number of the base sampler holds its word within its range, and the clamped split of its exponent and the scale lie in* $[0, 1)$*. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5), of degree* $n = 2^h \in \{512, 1024\}$*;*
- $(\mu, \texttt{isigma})$ *be a pair of inputs that a call of* SamplerZ *(Algorithm 8) by* deepest *(Algorithm 7) takes, in either center's mode;*
- W_x *be a word of* SamplerZ*, lines 2 to 15, or of* BerExp*, lines 2 to 4.*

Define:

- $\widetilde{ccs}$ *and* $\widetilde{x}$*, the values of* SamplerZ*, lines 6 and 15;*
- ϵ_L*,* si*,* $\widetilde{r}'$ *and* r'*, those of* BerExp *(Algorithm 9), lines 1 to 4, on* $(\widetilde{x}, \widetilde{ccs})$*;*
- x*, the number* W_x*'s line computes in* $\mathcal{F}_{\mathrm{fx}}$ *(Definition I.1);*
- $x_{\mathrm{fx64}} := 2^{64}x$ *(Definition A.5);*
- R_x*, the range of* x*'s row of Table 32 at* n*;*
- $W_{r'2^{63}}$ *and* $W_{\widetilde{ccs}2^{63}}$*, the words* `fxp_mul2e` *returns on* $(r', 63)$ *and* $(\widetilde{ccs}, 63)$ *in* `fxp_expm_p63` *[L0: `fxp/sign_fxsampler.c:105`] [L0: `fxp/sign_fxsampler.c:123`].*

Then

1. $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$*;*
2. $|x| \leq R_x$*;*
3. $R_x < 2^{63}$*;*

4. $r' \in [0,1)$;

5. $si \in \{-2^{31}, \ldots, 2^{31}-1\}$;

6. $W_{r'2^{63}} = (r'2^{63})_{\text{fx64}} \bmod 2^{128}$;

7. $W_{\widetilde{ccs}2^{63}} = (\widetilde{ccs}2^{63})_{\text{fx64}} \bmod 2^{128}$;

8. $r'2^{63}, \widetilde{ccs}2^{63} \in [0, 2^{63})$.

Proof.

COMPUTES s, $\widetilde{r}$, z_0 and z: the values of SamplerZ (Algorithm 8), lines 1 to 15

COMPUTES $(\widetilde{t}_0, \widetilde{t}_1)$, the center the call receives (ffsamp (Algorithm 6), line 1)

COMPUTES $\widetilde{tb}_0$, the center of line 9 of deepest (Algorithm 7)

COMPUTES $\widetilde{d}$, the diagonal $\widetilde{d}_{jj}$, $j \in \{0,1\}$, of deepest (Algorithm 7) from which the call's `isigma` $= 1/\widetilde{\sigma}_j$ is computed

COMPUTES $\widetilde{w}$, the square root of $\widetilde{d}$ the call computes, the $\widetilde{r}$ of Lemma I.42

DEFINES X, the range R_x of the row $\widetilde{x}$ of Table 32 at n

DEFINES $\zeta_{\text{op}} := 2^{-65}$ (Definition I.1)

DEFINES $\sigma_{\min}$, the number of the word `FXP_SIGMA_MIN`$[h]$ [LO: `fxp/fxp_consts.h:2073-2084`]

	Lemma I.49, items 1, 2 and 5 at the call of deepest (Algorithm 7) at $k = h-1$ that takes μ, and at its parent call at $k = h-2$	This proof
	Shared: (f, g, F, G), $(\widetilde{t}_0, \widetilde{t}_1)$	
(I1)	(f, g, F, G) checked key of degree $n \in \{512, 1024\}$ ν a call at depth $k \le h-1$	The statement The call of deepest at $k = h-1$ and its parent at $k = h-2$ (the scope)
	Assumption A1	The scope, the depth $h-1$
	Its item 1: $\forall \psi :\ \lvert\widetilde{t}_0(\psi)\rvert, \lvert\widetilde{t}_1(\psi)\rvert \le T_k$	
	Its item 2: $\forall \psi :\ \lvert\widetilde{tb}_0(\psi)\rvert \le T_{\text{leaf}}$	
	Its item 5: $W_x = x_{\text{fx64}} \bmod 2^{128}$	

(L1) $\forall \psi :\ \lvert\widetilde{t}_0(\psi)\rvert, \lvert\widetilde{t}_1(\psi)\rvert \le T_{h-1}$
[item 1 of (I1)]

(L2) $\forall \psi :\ \lvert\widetilde{tb}_0(\psi)\rvert \le T_{\text{leaf}}$
[item 2 of (I1)]

(L3) $T_{h-1} \le T_{\text{leaf}}$
[Lemma I.49, (L4)]

(L4) $T_{\text{leaf}} \le 2^{30}$
[[gate: `verify/gates/fx/samples.py`]]

(L5) $\Rightarrow\ \lvert\mu\rvert \le 2^{30}$
[(L1), (L2), (L3), (L4); μ (the statement); Fact A.41, item 1]

(L6) $W_\mu = \mu_{\text{fx64}} \bmod 2^{128}$
[item 5 of (I1): μ a part of $\widetilde{t}_1$, a word of the parent's splits (ffsamp (Algorithm 6), lines 19 and 33), or of $\widetilde{tb}_0$, a word of line 9 of deepest; μ (the statement)]

Lemma I.43, item 1 at $k = h-1$, at a path (ν_k) of the key's tree to the node of $\widetilde{d}$	This proof

17507 (I2) Shared: (f, g, F, G), $d_{\mathrm{lo}}, d_{\mathrm{hi}}$, χ_k

$\widetilde{d}_{\nu_{h-1}}$	$\widetilde{d}$
Its item 1: $\forall k \in \{0, \dots, h-1\}\ \forall \psi :\ \widetilde{d}^{\nu_k}_{00}(\psi), \widetilde{d}^{\nu_k}_{11}(\psi) \in [d_{\mathrm{lo}}(1 - \max_j \chi_j),\ d_{\mathrm{hi}}(1 + \max_j \chi_j)]$	

17508 (L7) $\widetilde{d} \le d_{\mathrm{hi}}(1 + \max_j \chi_j)$

17509 [(I2)]

17510 (L8) $\widetilde{w} \in [0, \sqrt{\widetilde{d}} + 2^{-65}]$

17511 [deepest (Algorithm 7), line 1; Definition I.1, item 1, at $\sqrt{\cdot}$; $\forall a, b \in \mathbb{R},\ a \le b :\ \mathrm{fl}(a) \le \mathrm{fl}(b)$, and $\mathrm{fl}(0) = 0$
17512 (Fact A.6, item 9)]

17513 (L9) $\texttt{isigma} \in [0, \widetilde{w}\,\texttt{INV_SIGMA} + 2^{-65}]$

17514 [deepest (Algorithm 7), line 3; (L8); $\texttt{INV_SIGMA} \ge 0$ (the stored word $\texttt{FXP_INV_SIGMA}[h]$
17515 [L0: `fxp/fxp_consts.h:2058-2070`]); Definition I.1, item 1, at $\times$; Fact A.6, item 9]

17516 (L10) $\texttt{isigma} \in [0, R_{1/\widetilde{\sigma}}]$

17517 [(L7), (L8), (L9); $\texttt{INV_SIGMA} \ge 0$
17518 (the stored word $\texttt{FXP_INV_SIGMA}[h]$ [L0: `fxp/fxp_consts.h:2058-2070`]); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$
17519 (Fact A.41, item 5); [gate: `verify/gates/fx/node_diag.py`]; [gate: `verify/gates/fx/ranges.py`]: $R_{1/\widetilde{\sigma}}$
17520 the row $1/\widetilde{\sigma}$ of Table 32]

Lemma I.7, item 2 at $x := \mu$	This proof
x	μ (the statement)
(I3) $x \in 2^{-64}\mathbb{Z},\ x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$	μ, a number of $\mathcal{F}_{\mathrm{fx}}$ (Definition I.1); (L5); Definition A.5
$W_x = W_\mu$	(L6)
Its conclusion: $j = \lfloor x \rfloor$	

17521 (I3)

17522 (L11) $s = \lfloor \mu \rfloor$

17523 [(I3); s (SamplerZ, line 1) [L0: `fxp/sign_fxsampler.c:184`]]

17524 (L12) $|s| \le 2^{30} + 1$

17525 [(L5), (L11); $\lfloor \mu \rfloor \in (\mu - 1, \mu]$ (Fact A.41, item 22)]

17526 (L13) $\widetilde{r} = \mu - s$

17527 [(L11); SamplerZ (Algorithm 8), line 2; Definition I.1, item 1, at $-$]

17528 (L14) $\widetilde{r} \in [0, 1)$

17529 [(L11), (L13); $\mu - \lfloor \mu \rfloor \in [0, 1)$ (Fact A.41, item 22)]

17530 (L15) $(z_0, z) \in \{0, \dots, 18\} \times [-18, 19]$

17531 [Lemma I.49, (L11), (L12)]

17532 (L16) $|z - \widetilde{r}| \le 19$

17533 [(L14), (L15)]

17534 (L17) $\forall x$ of lines 2 to 15 and 2 to 3 :\ $|x| \le R_x$

17535 [(L10), (L14), (L15), (L16); Definition I.1, items 1 and 2, at the stored $\sigma_{\min}$, C_0, $\texttt{INV_LOG2}$ and
17536 $\texttt{LOG2}$ [L0: `fxp/fxp_consts.h:2073-2089`]; $|x - y| \le |x| + |y|$ (Fact A.41, item 1); $|\mathrm{trunc}\, y| \le |y|$ (Fact A.6,
17537 item 5); [gate: `verify/gates/fx/ranges.py`]]

17538 (L18) $\forall x :\ R_x < 2^{63}$

17539 [[gate: `verify/gates/fx/ranges.py`]]

	Lemma I.42, item 1 at the diagonal $\widetilde{d}$ of the proof's block	This proof
	Shared: $h, n,\ \widetilde{d}$ (the proof's block)	
	W_x	$W_{\texttt{isigma}}$ (deepest, line 3)
	$n \in \{512, 1024\}$	The statement
(I4)	$\widetilde{d}$ a diagonal of deepest at a node of degree 2	The proof's block
	W_x a word of lines 1 or 3 of deepest	`isigma`, the input of the call (the statement)
	Assumption A1	Lemma I.44, item 1, at the checked key (the statement)
	Assumption A2	Lemma I.43, item 2, at the checked key (the statement)
	Its conclusion: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Lemma I.12, items 1 and 5 at each operation of SamplerZ, lines 2 to 15, and of BerExp, lines 2 to 3, in their order, on its operands' words [L0: `fxp/sign_fxsampler.c:151-162`] [L0: `fxp/sign_fxsampler.c:183-216`]	This proof
	(W_x, W_y)	the words of the operation's operands (the lines)
	o	sub, mul, half (the lines)
	V	the operands' $\cdot_{\text{fx64}}$ (Definition A.5)
	$W_x, W_y \in \{0, \ldots, 2^{128} - 1\}$	Words (Definition A.5)
	$V \in \mathbb{Z}$	Definition A.5
	$o \in \{\text{add}, \text{sub}, \text{neg}, \text{mul}, \text{div}, \text{half}\}$	The scope
(I5)	Assumption A1	μ by (L6); `isigma` by (I4); the stored $\sigma_{\min}$, C_0, `INV_LOG2` and `LOG2` [L0: `fxp/fxp_consts.h:2073-2089`]; the conversions of s, z, z_0^2 and si by Lemma I.7, item 1, s an `int64`, z, z_0^2, si `int32`s [L0: `fxp/sign_fxsampler.c:152`] [L0: `fxp/sign_fxsampler.c:184`]; every other operand by item 5 at the operation that computes it
	Assumption A2	(L5), (L10), (L12), (L15), (L17), (L18)
	Assumption A4	$o \neq \text{div}$ (the scope)
	Assumption A5	(L17), (L18); Definition I.1, items 1 and 2; Definition A.5
	Its item 1: $x_{\text{fx64}} = V$	
	Its item 5: $z_{o,\text{fx64}} = V_o$	

(L19) $\forall x$ of lines 2 to 15 and 2 to 3 : $W_x = x_{\text{fx64}} \bmod 2^{128}$
[(I5); Definition I.1, item 1, and item 2, at each halved operand x, $x_{\text{fx64}} \in [-2^{127}, 2^{127})$ by (L17), (L18) and Definition A.5; the truncation of line 2 by Lemma I.7, item 3, at (L17), (L18)]

Proof of items 4 and 5.

(L20) $\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}) \geq \widetilde{x} \cdot \texttt{INV_LOG2} - \zeta_{\text{op}}$
[(L19); Definition I.1, item 1, at $\times$]

(L21) $si > \text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}) - 1$
[$si = \text{trunc}(\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}))$ (BerExp, line 2); $\text{trunc}\, y = \text{sgn}(y)\lfloor |y| \rfloor$ (Fact A.6, item 5); $\lfloor y \rfloor \in (y - 1, y]$ (Fact A.41, item 22)]

(L22) $\text{fl}(si \cdot \texttt{LOG2}) \geq si \cdot \texttt{LOG2} - \zeta_{\text{op}}$
[(L19); Definition I.1, item 1, at $\times$]

(L23) $\texttt{INV_LOG2} \cdot \texttt{LOG2} = 1 + \epsilon_L$
[ϵ_L (BerExp, line 1)]

(L24) $\widetilde{r}' \leq X|\epsilon_L| + (1 + \zeta_{\text{op}})\texttt{LOG2} + \zeta_{\text{op}}$
[(L17), (L20), (L21), (L22), (L23); $\widetilde{r}' = \widetilde{x} - \text{fl}(si \cdot \texttt{LOG2})$ (BerExp, line 3); $\texttt{LOG2} > 0$ (the stored word

[L0: `fxp/fxp_consts.h:2087`]); X (the proof's block)]

(L25) $X|\epsilon_L| + (1+\zeta_{\text{op}})\texttt{LOG2} + \zeta_{\text{op}} < 1$

[[gate: `verify/gates/fx/ranges.py`]: the row r' of Table 32]

Lemma I.8, item 2 at $(x,y) := (\widetilde{r'}, 0)$	This proof
x, y	$\widetilde{r'}, 0$ (BerExp, line 4)
z	r' (BerExp, line 4)
(I6) $x, y \in 2^{-64}\mathbb{Z},\ x_{\text{fx64}}, y_{\text{fx64}} \in [-2^{127}, 2^{127})$	$\widetilde{r'}$, 0 (the proof's lines); (L17), (L18), (L19)
Assumption A1	(L17), (L18)
Its conclusion: $z = \max(x, y)$	

(L26) $r' \in [0, 1)$

[(L24), (L25); $r' = \max(\widetilde{r'}, 0)$ (BerExp, line 4); (I6)]

(L27) $W_{r'} = r'_{\text{fx64}} \bmod 2^{128}$

[(I6); s_w (Definition A.5) at $w := 128$]

(L28) $|si| \le |\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2})|$

[$|\text{trunc}\, y| \le |y|$ (Fact A.6, item 5)]

(L29) $|\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2})| < 2^{31}$

[(L17); [gate: `verify/gates/fx/ranges.py`]: the row $\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2})$ of Table 32]

(L30) $si \in \{-2^{31}, \ldots, 2^{31} - 1\}$

[(L28), (L29); the cast to `int32` [L0: `fxp/sign_fxsampler.c:152`]]

(L31) $\Rightarrow$ item 5

[(L30)]

(L32) $\Rightarrow$ item 4

[(L26)]

Proof of item 1.

(L33) $\Rightarrow$ item 1

[(L19) at lines 2 to 15 and 2 to 3; (L27) at line 4]

Proof of items 6 to 8.

(L34) $\sigma_{\text{min}} > 0$

[the stored words `FXP_SIGMA_MIN`[9], `FXP_SIGMA_MIN`[10] [L0: `fxp/fxp_consts.h:2073-2084`]]

(L35) $\widetilde{ccs} \ge 0$

[(L10), (L34); $\widetilde{ccs} = \text{fl}(\texttt{isigma} \cdot \sigma_{\text{min}})$ (SamplerZ, line 6); $\forall a, b \in \mathbb{R},\ a \le b:\ \text{fl}(a) \le \text{fl}(b)$, and $\text{fl}(0) = 0$ (Fact A.6, item 9)]

Lemma I.50	This proof
(I7) Shared: (f, g, F, G), `isigma`, $\widetilde{ccs}$	
Its conclusion: $\widetilde{ccs} < 1$	

(L36) $\widetilde{ccs} < 1$

[(I7)]

(L37) $(r'2^{63})_{\text{fx64}}, (\widetilde{ccs}2^{63})_{\text{fx64}} \in [0, 2^{127})$

[(L26), (L35), (L36); $y_{\text{fx64}} = 2^{64}y$ (Definition A.5)]

	Lemma I.6, item 3 at $(x, e) := (r', 63)$ and at $(x, e) := (\widetilde{ccs}, 63)$	This proof
	x	$r', \widetilde{ccs}$ (the statement)
	e	63 (`fxp_expm_p63` [L0: `fxp/sign_fxsampler.c:105`] [L0: `fxp/sign_fxsampler.c:123`])
(I8)	$x \in 2^{-64}\mathbb{Z},\ x_{\text{fx64}} \in [-2^{127}, 2^{127})$	r', $\widetilde{ccs}$, numbers of $\mathcal{F}_{\text{fx}}$ (Definition I.1); (L26); (L35), (L36); Definition A.5
	$W_x = W_{r'}, W_{\widetilde{ccs}}$	(L27); (L19) at line 6
	$e \in \{1, \ldots, 63\}$	63
	Its conclusion: $W_z = W_x 2^e \bmod 2^{128}$	

(L38) $W_{r'2^{63}} = (r'2^{63})_{\text{fx64}} \bmod 2^{128}$

[(I8) at $x := r'$; Definition A.5]

(L39) $\Rightarrow$ item 6

[(L38)]

(L40) $W_{\widetilde{ccs}2^{63}} = (\widetilde{ccs}2^{63})_{\text{fx64}} \bmod 2^{128}$

[(I8) at $x := \widetilde{ccs}$; Definition A.5]

(L41) $\Rightarrow$ item 7

[(L40)]

(L42) $\Rightarrow$ item 8

[(L37); Definition A.5]

Proof of items 2 and 3.

(L43) $\Rightarrow$ item 2

[(L17) at lines 2 to 15 and 2 to 3; (L24), (L26) at line 4, its $R_{r'}$ the bound of (L25)]

(L44) $\Rightarrow$ item 3

[(L18)]

□ (items 1 to 8)

I.3.7 No overflow in the inverse FFT

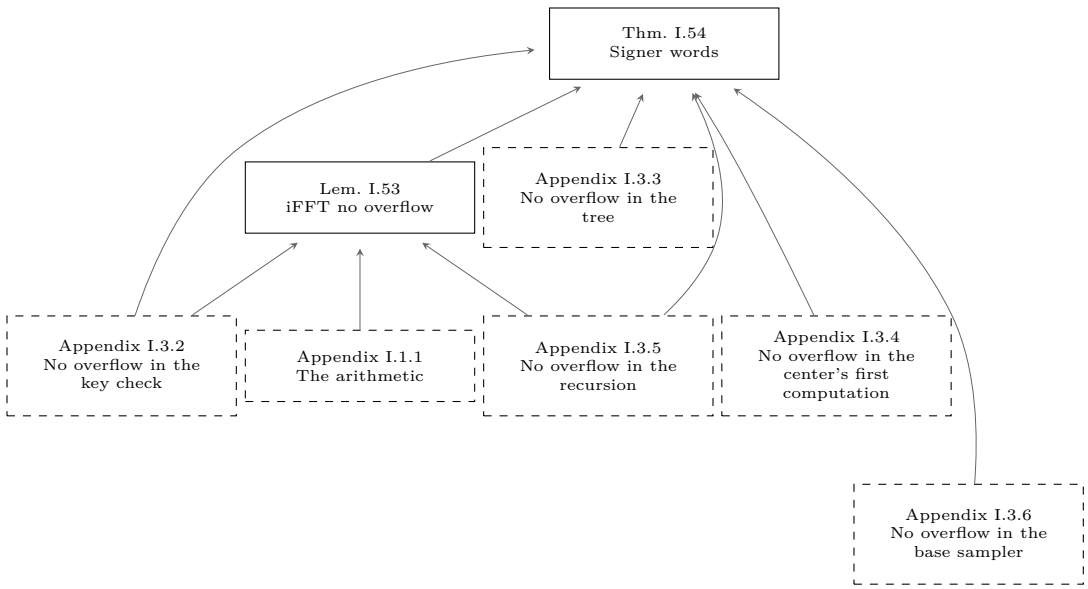


Figure 81: Dependencies, Appendix I.3.7.

Theorem I.54 states the ranges of every word of the signer.

Lemma I.53 (No overflow in the inverse FFT [to table])**.** *The inverse FFT of the root's sample keeps every stage's words within M_j, and the nearest integers of its scaled words are their values.*
Let:

- (f, g, F, G) *be a checked key (Definition 5.5), of degree* $n = 2^h \in \{512, 1024\}$*;*
- $W_x = (W_{x_r}, W_{x_i})$ *be a pair of words* `fxpoly_iFFT` *writes on the sample of line 23 of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10), in either center's mode [LO: fxp/sign_fxcore.c: 203-204]: at its stage* j*,* $1 \le j \le h-1$*, or at its scaling.*

Define:

- *The centers and the samples*
  - R*,* ℓ_0*,* H_0 *and* e_I*, those of Lemma I.49,* H_0 *its* H_k *at* $k = 0$*;*
  - $T_0 := \sqrt{2}\,R$ *and* $D_0 := (1 + \ell_0)H_0 + e_I(\ell_0)$*, the* T_0 *and the* D_k *of Lemma I.49 at* $k = 0$*;*
- *The words*
  - $x := x_r + ix_i$*, the complex number the line of* W_x *computes in* $\mathcal{F}_{\text{fx}}$ *(Definition I.1);*
  - X_0*, the numbers of* $(\widetilde{z}_0(\psi), \widetilde{z}_1(\psi))_\psi$*, the sample of line 23, the input of stage* 1*;*
  - $\forall j \in \{1, \ldots, h-1\}$*:* X_j*, the numbers* x *of the pairs written at stage* j*;*
  - X_{sc}*, the numbers* x *of the pairs written at the scaling;*
- *The word bounds*
  - $M_0 := (T_0 + D_0)2^{64}$*;*
  - $\forall j \le h-2:\ M_{j+1} := 2M_j(2^{64}+1)/2^{64} + \sqrt{2}$*;*
  - $c := 2(1 + 2^{-64})$*.*

Let:

- y_x *be a part of a scaled pair's number* $x \in X_{\text{sc}}$*.*

Define:

- j_x*, the integer* `fxp_rint` *returns on the word of* y_x *[LO: fxp/sign_fxcore.c: 208-209].*

Then

1. $\forall j \le h-1\ \forall x \in X_j:\ W_x = x_{\text{fx64}} \bmod 2^{128}$*, at each part;*
2. $\forall j \le h-1\ \forall x \in X_j:\ |x_{\text{fx64}}| \le M_j$*;*
3. $\forall j \le h-1:\ M_j \le c^{h-1}(M_0 + 2) - 2$*;*
4. $c^{h-1}(M_0 + 2) - 2 < 2^{127}$*;*
5. $\forall x \in X_{\text{sc}}:\ W_x = x_{\text{fx64}} \bmod 2^{128}$*, at each part;*
6. $\forall x \in X_{\text{sc}}:\ |x_{\text{fx64}}| \le M_{h-1}/2^{h-1} + \sqrt{2}/2$*;*
7. $j_x = \operatorname{rint} y_x$*;*
8. $|j_x| < 2^{62}$*.*

Proof.
COMPUTES $(\widetilde{t}_0, \widetilde{t}_1)$, the center the root call receives (ffsamp (Algorithm 6), line 1)

	Lemma I.49 at $k=0$	This proof
	(f,g,F,G)	(f,g,F,G) (the statement)
	ν	the root call (the proof's block)
	W_x	W_x, $x \in X_0$ (ffsamp, lines 21 and 35)
	(f,g,F,G) checked key of degree $n \in \{512,1024\}$	The statement
(I1)	ν a call at depth $k \le h-1$	The root call, $k=0$ (the proof's block)
	W_x a word of ν 's center lines	The merges of ffsamp, lines 21 and 35
	Its item 1: $\forall \psi:\ \lvert\widetilde{t}_0(\psi)\rvert, \lvert\widetilde{t}_1(\psi)\rvert \le T_k$	
	Its item 3: $\forall \psi:\ \lvert\widetilde{t}_1(\psi) - \widetilde{z}_1(\psi)\rvert \le H_k$	
	Its item 4: $\forall \psi:\ \lvert\widetilde{t}_0(\psi) - \widetilde{z}_0(\psi)\rvert \le D_k$	
	Its item 5: $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	

(L1) $\forall \psi:\ \lvert\widetilde{t}_0(\psi)\rvert, \lvert\widetilde{t}_1(\psi)\rvert \le T_0$

[item 1 of (I1)]

(L2) $\forall \psi:\ \lvert\widetilde{t}_1(\psi) - \widetilde{z}_1(\psi)\rvert \le H_0$

[item 3 of (I1)]

(L3) $\forall \psi:\ \lvert\widetilde{t}_0(\psi) - \widetilde{z}_0(\psi)\rvert \le D_0$

[item 4 of (I1)]

(L4) $H_0 \le D_0$

[Lemma I.49, (L2)]

(L5) $\Rightarrow\ \forall x \in X_0:\ \lvert x\rvert \le T_0 + D_0$

[(L1), (L2), (L3), (L4); X_0 (the statement); Fact A.41, item 1]

(L6) $\forall x \in X_0:\ \lvert x_{\mathrm{fx64}}\rvert \le M_0$

[(L5); M_0 (the statement); Definition A.5]

(L7) $\forall x \in X_0:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[item 5 of (I1)]

(L8) $\forall \widetilde{s} \in \{\operatorname{conj} \widetilde{\psi}_k\}_k:\ \lvert\widetilde{s}_{\mathrm{fx64}}\rvert \le 2^{64}+1$

[[gate: `verify/gates/fx/twiddle_pairs.py`], the 1024 stored pairs; $\lvert\operatorname{conj} x\rvert = \lvert x\rvert$ (Fact A.41, item 1)]

(L9) $\forall x,y \in C_{\mathcal{F}_{\mathrm{fx}}}:\ \lvert(x \otimes y)_{\mathrm{fx64}}\rvert \le \lvert x_{\mathrm{fx64}}\rvert\lvert y_{\mathrm{fx64}}\rvert/2^{64} + \sqrt{2}$

[Lemma I.34, item 7]

	Lemma I.10, item 13	This proof
	h	h (the statement)
	$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
	$h \in \{2,\dots,10\}$	$n \in \{512,1024\}$ (the statement)
(I2)	each input array of words	The sample of ffSampling$^{\mathcal{F}}$, line 23 (the statement)
	Assumption A8	$n \in \{512,1024\}$ (the statement)
	Its conclusion: at each of its $h-1$ stages, at each pair (x,y) and its twiddle's conjugate $\widetilde{s}$, the words of $x \oplus y$ and $(x \ominus y) \otimes \widetilde{s}$; then the word of $\mathrm{fl}(x/2^{h-1})$ at each of its 2^h words x	

(L10) $\forall j \le h-2\ \forall x \in X_{j+1}\ \exists a,b \in X_j\ \exists \widetilde{s} \in \{\operatorname{conj}\widetilde{\psi}_k\}_k:\ x \in \{a \oplus b,\ (a \ominus b) \otimes \widetilde{s}\}$

[(I2); X_j (the statement)]

(L11) $\forall j \le h-2:\ M_j \ge 0 \Rightarrow\ M_{j+1} \ge 0$

[M_{j+1} (the statement)]

(L12) $\forall j \le h-1:\ M_j \ge 0$

[induction on j: (L6) at $x \in X_0$, the base; (L11) the step]

(L13) $\forall j \le h-2:\ 2M_j \le M_{j+1}$

[(L12); M_{j+1} (the statement); expand]

(L14) $\forall j \le h-2:\ [\forall x \in X_j:\ \lvert x_{\mathrm{fx64}}\rvert \le M_j] \Rightarrow\ \forall a,b \in X_j:\ \lvert(a \oplus b)_{\mathrm{fx64}}\rvert, \lvert(a \ominus b)_{\mathrm{fx64}}\rvert \le 2M_j$

[$\mathrm{fl}(x \pm y) = x \pm y$ (Definition I.1, item 1); $\lvert x+y\rvert, \lvert x-y\rvert \le \lvert x\rvert + \lvert y\rvert$ (Fact A.41, item 1); Definition A.5]

(L15) $\forall j \le h-2:\ [\forall x \in X_j:\ |x_{\mathrm{fx64}}| \le M_j] \Rightarrow\ \forall a, b \in X_j\ \forall \widetilde{s} \in \{\operatorname{conj} \widetilde{\psi}_k\}_k:\ |((a \ominus b) \otimes \widetilde{s})_{\mathrm{fx64}}| \le 2M_j(2^{64}+1)/2^{64} + \sqrt{2}$

[(L9) at $(x, y) := (a \ominus b, \widetilde{s})$; (L14); (L8)]

(L16) $\forall j \le h-2:\ [\forall x \in X_j:\ |x_{\mathrm{fx64}}| \le M_j] \Rightarrow\ \forall x \in X_{j+1}:\ |x_{\mathrm{fx64}}| \le M_{j+1}$

[(L10), (L13), (L14), (L15); M_{j+1} (the statement)]

Lemma I.12, item 1 at each part of every $x \in X_j$, $j \le h-2$, under $[\forall x \in X_j:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128} \wedge |x_{\mathrm{fx64}}| \le M_j] \wedge M_{j+1} < 2^{127}$	This proof
Shared: W_x (the scope)	
(I3) V $W_x \in \{0, \dots, 2^{128}-1\}$ $V \in \mathbb{Z}$	x_{fx64} (the scope) W_x, a word (Definition A.5) x_{fx64} (Definition A.5)
Assumption A1 Assumption A2	The scope The scope; (L12), (L13); $\lvert\operatorname{Re} x\rvert, \lvert\operatorname{Im} x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
Its conclusion: $x_{\mathrm{fx64}} = V$	

Lemma I.12, item 1 at each part of every twiddle's conjugate $\widetilde{s}$ of (L10)	This proof
(I4) W_x V $W_x \in \{0, \dots, 2^{128}-1\}$ $V \in \mathbb{Z}$	$W_{\widetilde{s}}$ (L10) $\widetilde{s}_{\mathrm{fx64}}$ (Definition A.5) $W_{\widetilde{s}}$, a word (Lemma I.10, item 13) $\widetilde{\psi}_k \in 2^{-64}\mathbb{Z}$ $(\operatorname{roundEven}(2^{64}\operatorname{Re}\psi_k), \operatorname{roundEven}(2^{64}\operatorname{Im}\psi_k) \in \mathbb{Z}$, Definition I.1, item 4); $\widetilde{s} = \operatorname{conj}\widetilde{\psi}_k$ (L10)
Assumption A1 Assumption A2	Definition I.1, item 6; its real part by item 5 (L8); $\lvert\operatorname{Re} x\rvert, \lvert\operatorname{Im} x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
Its conclusion: $x_{\mathrm{fx64}} = V$	

Lemma I.12, item 5 at each part of each operation of (L10), at every $x \in X_{j+1}$, $j \le h-2$, under $[\forall x \in X_j:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128} \wedge |x_{\mathrm{fx64}}| \le M_j] \wedge M_{j+1} < 2^{127}$	This proof
(I5) W_x, W_y o W_{z_o} $W_x, W_y \in \{0, \dots, 2^{128}-1\}$ $o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{neg}, \mathrm{mul}, \mathrm{div}, \mathrm{half}\}$	W_a, W_b at $\oplus, \ominus$; $W_{a \ominus b}, W_{\widetilde{s}}$ at $\otimes$ (Definition A.8; (L10)) add, sub, mul (Definition A.8; (L10)) W_x at $\oplus$ and at $\otimes$; $W_{a \ominus b}$ at $\ominus$ (Definition A.8; (L10)) W_a, W_b, $W_{a \ominus b}$, $W_{\widetilde{s}}$, words (Definition A.5) (L10)
Assumption A4 Assumption A5	$o \in \{\mathrm{add}, \mathrm{sub}, \mathrm{mul}\}$ (L10) The scope; (L13), (L14), (L15), (L16); $\lvert\operatorname{Re} x\rvert, \lvert\operatorname{Im} x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
Its conclusion: $z_{o,\mathrm{fx64}} = V_o$	

(L17) $\forall j \le h-2:\ [\forall x \in X_j:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128} \wedge |x_{\mathrm{fx64}}| \le M_j] \wedge M_{j+1} < 2^{127} \Rightarrow\ \forall x \in X_{j+1}:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128} \wedge |x_{\mathrm{fx64}}| \le M_{j+1}$

[(I2); (I3); (I4); (I5); (L16)]

(L18) $\forall j:\ M_{j+1} = cM_j + \sqrt{2}$

[M_{j+1}, c (the statement)]

(L19) $2c - \sqrt{2} \ge 2$

[c (the statement); expand]

(L20) $M_0 + 2 = c^0(M_0 + 2)$

[expand]

(L21) $\forall j:\ M_{j+1}+2 \le c(M_j+2)$

[(L18), (L19)]

(L22) $\forall j:\ M_j+2 \le c^j(M_0+2)$

[induction on j: (L20) the base, (L21) the step]

(L23) $c \ge 1$

[c (the statement); expand]

(L24) $\forall j \le h-1:\ M_j \le c^{h-1}(M_0+2)-2$

[(L12), (L22), (L23)]

(L25) $c^{h-1}(M_0+2)-2 < 2^{127}$

[[gate: `verify/gates/fx/ranges.py`]: the row of the stages' pairs of Table 32, times 2^{64}]

(L26) $\forall j \le h-1\ \forall x \in X_j:\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[induction on j: (L6), (L7) the base; (L17) the step, its premise $M_{j+1} < 2^{127}$ by (L24), (L25)]

(L27) $\forall j \le h-1\ \forall x \in X_j:\ |x_{\mathrm{fx64}}| \le M_j$

[induction on j: (L6), (L7) the base; (L17) the step, its premise $M_{j+1} < 2^{127}$ by (L24), (L25)]

(L28) $\Rightarrow$ item 1

[(L26)]

(L29) $\Rightarrow$ item 2

[(L27)]

(L30) $\Rightarrow$ item 3

[(L24)]

(L31) $\Rightarrow$ item 4

[(L25)]

Lemma I.6, item 2 at each part of every $x' \in X_{h-1}$	This proof
x	x' (the scope)
W_x	$W_{x'}$ ((L26) at $j = h-1$)
e	$h-1$ (the statement)
(I6) W_z	$W_x,\ x \in X_{\mathrm{sc}}$ (I2)
$x \in 2^{-64}\mathbb{Z}$	x', a number of $\mathcal{F}_{\mathrm{fx}}$ (Definition I.1; the scope)
$x_{\mathrm{fx64}} \in [-2^{127}, 2^{127})$	(L24), (L25); (L27) at $j = h-1$; $\lvert\mathrm{Re}\,x\rvert, \lvert\mathrm{Im}\,x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
$e \in \{1, \dots, 63\}$	$n \in \{512, 1024\}$ (the statement)
Its conclusion: $z_{\mathrm{fx64}} = \mathrm{roundAway}(x_{\mathrm{fx64}}/2^e)$	

(L32) $\forall x \in X_{\mathrm{sc}}\ \exists x' \in X_{h-1}:\ x_{\mathrm{fx64}} = \mathrm{roundAway}(x'_{\mathrm{fx64}}/2^{h-1})$

[(I2); (I6); Definition I.1, item 1, at $y := 2^{h-1}$]

(L33) $\forall v \in \mathbb{R}:\ |\mathrm{roundAway}(v) - v| \le 1/2$

[roundAway (Definition I.1); Fact A.41, item 22]

(L34) $\Rightarrow\ \forall x \in X_{\mathrm{sc}}:\ |x_{\mathrm{fx64}} - x'_{\mathrm{fx64}}/2^{h-1}| \le \sqrt{2}/2$

[(L32), (L33) per part; Fact A.41, item 1]

(L35) $\Rightarrow\ \forall x \in X_{\mathrm{sc}}:\ |x_{\mathrm{fx64}}| \le M_{h-1}/2^{h-1} + \sqrt{2}/2$

[(L27) at $j = h-1$, (L34); Fact A.41, item 1]

	Lemma I.12, item 1 at each part of every $x' \in X_{h-1}$ of (L32)	This proof
(I7)	W_x V $W_x \in \{0, \dots, 2^{128}-1\}$ $V \in \mathbb{Z}$	$W_{x'}$ (L32) x'_{fx64} (L32) $W_{x'}$, a word (Definition A.5) x'_{fx64} (Definition A.5)
	Assumption A1 Assumption A2	(L26) at $j = h-1$ (L24), (L25); (L27) at $j = h-1$; $\lvert\operatorname{Re} x\rvert, \lvert\operatorname{Im} x\rvert \le \lvert x\rvert$ (Fact A.41, item 1)
	Its conclusion: $x_{\text{fx64}} = V$	

(L36) $\forall x \in X_{\text{sc}} :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[(I2); (I6); (I7); (L32); s_w (Definition A.5) at $w := 128$]

(L37) $\Rightarrow$ item 5

[(L36)]

(L38) $\Rightarrow$ item 6

[(L35)]

(L39) $|y_x| + 1/2 < 2^{62}$

[(L24), (L35); $|\operatorname{Re} x|, |\operatorname{Im} x| \le |x|$ (Fact A.41, item 1); [gate: `verify/gates/fx/ranges.py`]: the row of the scaled pairs of Table 32]

	Lemma I.7, item 4 at $x := y_x$	This proof
(I8)	x $x \in 2^{-64}\mathbb{Z},\ x_{\text{fx64}} \in [-2^{127}, 2^{127})$ $W_x = W_{y_x}$	y_x (the statement) y_x, a part of a number of $\mathcal{F}_{\text{fx}}$ (the statement; Definition I.1); (L35), (L39); Definition A.5 (L36) at the part y_x
	Its conclusion: $j \equiv \operatorname{rint} x \pmod{2^{64}}$	

(L40) $j_x \equiv \operatorname{rint} y_x \pmod{2^{64}}$

[(I8); j_x (the statement)]

(L41) $|\operatorname{rint} y_x| \le |y_x| + 1/2$

[rint (Fact A.6, item 5)]

(L42) $j_x = \operatorname{rint} y_x$

[(L39), (L40), (L41); $j_x \in \{-2^{63}, \dots, 2^{63}-1\}$ (an `int64` [L0: `fxp/sign_fxcore.c:208-209`])]

(L43) $\Rightarrow$ item 7

[(L42)]

(L44) $|j_x| < 2^{62}$

[(L39), (L41), (L42)]

(L45) $\Rightarrow$ item 8

[(L44)]

□ (items 1 to 8)

Theorem I.54 (No overflow in the fixed-point signer [to table])**.** *Every word of the signer stores its number. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5), of degree* $n = 2^h \in \{512, 1024\}$*;*
- W_x *be a word of one of:*
  - *The key check (Lemmas I.36, I.37 and I.38);*
  - *The expansion and the Gram of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10), lines 1 and 3;*
  - *The root's step (Lemma I.39);*
  - *Every self-adjoint split at* $m = 2^k$, $2 \le k \le h$, *and every LDL*† *step below the root at* $m = 2^k$, $1 \le k \le h-1$, *of the tree recursion (Lemmas I.43 and I.44);*
  - *The leaves' square roots and inverse standard deviations, lines 1 and 3 of* deepest

(Algorithm 7) and their counterparts (Lemma I.42);

– *The center's first computation in either mode (Lemmas I.46 and I.47);*

– *The center lines of the sampling recursion and the leaves' samples, in either mode (Lemma I.49);*

– *The base sampler,* SamplerZ *(Algorithm 8), lines 2 to 15, and* BerExp *(Algorithm 9), lines 2 to 4 (Lemma I.52);*

– *The inverse FFT of the sample of line 23 and its scaling (Lemma I.53).*

Define:

- x*, the number* W_x*'s line computes in* $\mathcal{F}_{\text{fx}}$ *(Definition I.1);*
- $x_{\text{fx64}} := 2^{64}x$ *(Definition A.5);*
- D*, the numbers of the diagonals' words below the root;*
- $\forall x \in D$*:* r_x*, the floor of* x*'s row of Table 32 at* n*.*

Then

1. $W_x = x_{\text{fx64}} \bmod 2^{128}$*;*
2. $|x| < 2^{63}$*;*
3. $\forall x \in D: \ x \geq r_x$*.*

Proof.

DEFINES $\mathcal{W}_k$, $1 \leq k \leq 9$: the words W_x of the k-th family of the statement's list

DEFINES $\widetilde{p}$: an image of f, g, F or G, ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 1

DEFINES $M_{FG} := M_{h-1}$ (Lemma I.34 at $B := 127$)

DEFINES $M_0 := \sqrt{2}\,127\,2^{64}$ and $\forall j \leq h-2: \ M_{j+1} := M_j(1 + (2^{64}+1)/2^{64}) + \sqrt{2}$ (Lemma I.34)

DEFINES Ψ_n, that of Fact A.43 at $m := n$

(I1)

Lemma I.36 at the checked key and at every $\psi' \in \Psi_n$	This proof
ψ (f, g, F, G) key of degree $n \in \{512, 1024\}$ $\psi \in \Psi_n$	ψ' (the proof's block) The checked key (the statement) ψ' (the scope)
Assumption A1 Assumption A2	Definition 5.5, item 2, at the checked key (the statement) Definition 5.5, item 3, at the checked key (the statement)
Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
Its item 4: $\lvert x_{\text{fx64}} \rvert < 2^{127}$	

(I2)

Lemma I.37 at the checked key and at every $\psi' \in \Psi_n$	This proof
ψ (f, g, F, G) key of degree $n \in \{512, 1024\}$ $\psi \in \Psi_n$	ψ' (the proof's block) The checked key (the statement) ψ' (the scope)
Assumption A1 Assumption A2	Definition 5.5, item 2, at the checked key (the statement) Definition 5.5, item 3, at the checked key (the statement)
Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
Its item 2: $\text{fl}(\widetilde{g}_{00}(\psi)^2) \in (0, 2^{62})$	
Its item 3: $lo > 0$	

Lemma I.38 at the checked key and at every $\psi' \in \Psi_n$	This proof
ψ	ψ' (the proof's block)
(f, g, F, G) key of degree $n \in \{512, 1024\}$	The checked key (the statement)
$\psi \in \Psi_n$	ψ' (the scope)
Assumption A1	Definition 5.5, item 2, at the checked key (the statement)
Assumption A2	Definition 5.5, item 3, at the checked key (the statement)
Its item 1: $W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 2: $\mathrm{fl}(num_\psi / \mathrm{fl}(\widetilde{g}_{00}(\psi)^2)) < 2^{62}$	
Its item 3: $\mathrm{fl}(q/lo),\ \mathrm{fl}(hi/q) < 2^{62}$	

(I3)

(L1) $\forall W_x \in \mathcal{W}_1 :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$

[item 1 of (I1), item 1 of (I2), item 1 of (I3)]

Lemma I.34 at $j := h - 1$	This proof
Shared: h	
p	$p \in \{g, f, G, F\}$ (the statement)
B	127
W_x	$W_{\widetilde{\hat{p}}}$ (the proof's block)
$X_{h-1} \cup X^-$	$\{\widetilde{\hat{p}}\}$ (the proof's block)
M_{h-1}	M_{FG} (the proof's block)
$h \in \{3, \ldots, 10\}$	$n \in \{512, 1024\}$ (the statement)
$p \in \{-128, \ldots, 127\}^{2^h}$	Definition 5.5, items 2 and 3; B_{fg} (Lemma I.37); $B \le 127$ (B, the rows above)
$B \in [0, 127]$	127
W_x a pair of words at stage j	ffSampling$^{\mathcal{F}}$, line 1 (the proof's block)
Assumption A1	Definition 5.5, items 2 and 3; B_{fg} (Lemma I.37)
Its item 1: $\forall j \le h-1\ \forall x \in X_j :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 2: $\forall j \le h-1\ \forall x \in X_j :\ \lvert x_{\mathrm{fx64}} \rvert \le M_j$	
Its item 3: $\forall x \in X^- :\ W_x = x_{\mathrm{fx64}} \bmod 2^{128}$	
Its item 4: $\forall x \in X^- :\ \lvert x_{\mathrm{fx64}} \rvert \le M_{h-1}$	
Its item 5: $\forall j \le h-1 :\ M_j \le c^{h-1}(1.4143\, B 2^{64} + 2) - 2$	
Its item 6: $c^{h-1}(1.4143\, B 2^{64} + 2) - 2 < 2^{81}$	

(I4)

(L2) $\forall \widetilde{\hat{p}} :\ W_{\widetilde{\hat{p}}} = \widetilde{\hat{p}}_{\mathrm{fx64}} \bmod 2^{128}$

[items 1 and 3 of (I4)]

(L3) $\forall \widetilde{\hat{p}} :\ \lvert \widetilde{\hat{p}}_{\mathrm{fx64}} \rvert \le M_{FG}$

[items 2 and 4 of (I4)]

(L4) $M_{FG} < 2^{81}$

[items 5 and 6 of (I4)]

	Lemma I.35	This proof
	b_{jk}	$\widetilde{\hat{p}}$ (the proof's block)
	Y_0, Y_1	$\{\widetilde{\hat{p}}\}, \{\widetilde{\hat{p}}\}$ (the proof's block)
	M_0, M_1	M_{FG}, M_{FG} (the proof's block)
	W_x	$W_x \in \mathcal{W}_2$ (the proof's block)
	b_{jk} arrays of pairs of words of line 1	$\widetilde{\hat{p}}$ (the proof's block)
(I5)	$M_0, M_1 \geq 0$	M_{FG} (the proof's block)
	W_x a word of Gram on the b_{jk}	$\mathcal{W}_2$ (the proof's block)
	Assumption A1	(L2)
	Assumption A2	(L3)
	Assumption A3	(L4)
	Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 6: $\lvert x_{\text{fx64}} \rvert < 2^{127}$	
(L5)	$\forall W_x \in \mathcal{W}_2 :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
		[item 1 of (I5); items 1 and 3 of (I4)]

	Lemma I.39	This proof
	$(f, g, F, G), n$	$(f, g, F, G), n$ (the statement)
	W_x	$W_x \in \mathcal{W}_3$ (the proof's block)
	$n \in \{512, 1024\}$	The statement
	(f, g, F, G) key of degree n	The statement
(I6)	W_x a word of the root's $LDL^\dagger$ step	$\mathcal{W}_3$ (the proof's block)
	Assumption A1	Definition 5.5, item 2
	Assumption A2	Definition 5.5, item 3
	Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 2: $\lvert x_{\text{fx64}} \rvert < 2^{126}$	
(L6)	$\forall W_x \in \mathcal{W}_3 :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
		[item 1 of (I6)]
(L7)	$\forall W_x \in \mathcal{W}_4 :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
		[Lemma I.44, item 1, at the checked key (the statement)]

	Lemma I.42 at every leaf diagonal $\widetilde{d}$	This proof
	Shared: $h, n,\ \widetilde{d}$ (the scope)	
	W_x	$W_x \in \mathcal{W}_5$ (the proof's block)
	$n \in \{512, 1024\}$	The statement
	$\widetilde{d}$ a diagonal of deepest at a node of	The scope
(I7)	degree 2	
	W_x a word of lines 1 or 3 of deepest	$\mathcal{W}_5$ (the proof's block)
	Assumption A1	(L7)
	Assumption A2	Lemma I.43, item 2
	Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 2: $\lvert x_{\text{fx64}} \rvert < 2^{127}$	
(L8)	$\forall W_x \in \mathcal{W}_5 :\ W_x = x_{\text{fx64}} \bmod 2^{128}$	
		[item 1 of (I7)]

	Lemma I.46	This proof
	Shared: $h, n,\ (f, g, F, G),\ \mathsf{h}(\mathsf{m})$ (Definition A.25)	
(I8)	W_x $h \in \{3, \dots, 10\}$ (f, g, F, G) key of degree n $\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ W_x a word of $\text{center}_{\text{frac}}$, lines 7 and 12,	$W_x \in \mathcal{W}_6$ (the proof's block) $n \in \{512, 1024\}$ (the statement) The statement $\mathsf{h}(\mathsf{m})$ (Definition A.25) $\mathcal{W}_6$ (the proof's block)
	Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 2: $\lvert x_{\text{fx64}} \rvert < 2^{127}$	

	Lemma I.47	This proof
	Shared: $h, n,\ (f, g, F, G),\ \mathsf{h}(\mathsf{m})$ (Definition A.25)	
(I9)	W_x $h \in \{3, \dots, 10\}$ (f, g, F, G) key of degree n $\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ W_x a word of $\text{ffSampling}^{\mathcal{F}}$, lines 9, 16 and 18,	$W_x \in \mathcal{W}_6$ (the proof's block) $n \in \{512, 1024\}$ (the statement) The statement $\mathsf{h}(\mathsf{m})$ (Definition A.25) $\mathcal{W}_6$ (the proof's block)
	Assumption A1 Assumption A2	Definition 5.5, item 2; B_{fg} (Lemma I.37) Definition 5.5, item 3
	Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 2: $\lvert x_{\text{fx64}} \rvert < 2^{127}$	

(L9) $\forall W_x \in \mathcal{W}_6 :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[item 1 of (I8), item 1 of (I9)]

(L10) $\forall W_x \in \mathcal{W}_7 :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[Lemma I.49, item 5, at the checked key (the statement)]

(L11) $\forall W_x \in \mathcal{W}_8 :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[Lemma I.52, item 1, at the checked key (the statement)]

(L12) $\forall W_x \in \mathcal{W}_9 :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[Lemma I.53, items 1 and 5, at the checked key (the statement)]

(L13) $\Rightarrow\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[(L1), (L5) to (L12); $\mathcal{W}_1, \dots, \mathcal{W}_9$ (the proof's block)]

(L14) $\forall \psi\ \forall \widetilde{\hat{p}} :\ num_\psi, \widetilde{sq}_{\hat{p}}, \text{fl}(num_\psi / \text{fl}(\widetilde{g}_{00}(\psi)^2)), \text{fl}(q/lo), \text{fl}(hi/q) \geq 0$

[keychecks (Algorithm 12), lines 5, 8, 9, 10 and 11; Definition I.1, item 1; $\forall v \geq 0 :\ \text{roundAway}(v) \geq 0$ (roundAway, Definition I.1); items 2 and 3 of (I2); $hi \geq lo$ (lines 6 and 7)]

(L15) $\forall W_x \in \mathcal{W}_1 :\ \lvert x_{\text{fx64}} \rvert < 2^{127}$

[(L14); item 4 of (I1), item 2 of (I2), items 2 and 3 of (I3); Definition A.5; expand]

(L16) $\forall W_x \in \mathcal{W}_2 :\ \lvert x_{\text{fx64}} \rvert < 2^{127}$

[(L3), (L4) at the images; item 6 of (I5) at the Gram's words]

(L17) $\forall W_x \in \mathcal{W}_3 :\ \lvert x_{\text{fx64}} \rvert < 2^{127}$

[item 2 of (I6)]

(L18) $\forall W_x \in \mathcal{W}_4 :\ \lvert x_{\text{fx64}} \rvert < 2^{127}$

[Lemma I.44, item 2, at the checked key (the statement)]

(L19) $\forall W_x \in \mathcal{W}_5 :\ \lvert x_{\text{fx64}} \rvert < 2^{127}$

[item 2 of (I7)]

(L20) $\forall W_x \in \mathcal{W}_6 :\ \lvert x_{\text{fx64}} \rvert < 2^{127}$

[item 2 of (I8), item 2 of (I9)]

(L21) $\forall W_x \in \mathcal{W}_7 :\ \lvert x_{\text{fx64}} \rvert < 2^{127}$

[Lemma I.49, item 6, at the checked key (the statement); $T^* = 2^{30}$ (Lemma I.49); Definition A.5; expand]

(L22) $\forall W_x \in \mathcal{W}_8 :\ |x_{\mathrm{fx64}}| < 2^{127}$
[Lemma I.52, items 2 and 3, at the checked key (the statement); Definition A.5]

(L23) $\forall W_x \in \mathcal{W}_9 :\ |x_{\mathrm{fx64}}| < 2^{127}$
[Lemma I.53, items 2, 3, 4 and 6, at the checked key (the statement); expand]

(L24) $\Rightarrow\ |x_{\mathrm{fx64}}| < 2^{127}$
[(L15) to (L23); $\mathcal{W}_1, \ldots, \mathcal{W}_9$ (the proof's block)]

(L25) $\Rightarrow\ |x| < 2^{63}$
[(L24); $x_{\mathrm{fx64}} = 2^{64}x$ (the statement)]

(L26) $\forall x \in D :\ x \geq r_x$
[[gate: `verify/gates/fx/ranges.py`]: the floor rows; Lemma I.43, item 1, at the checked key (the statement)]

(L27) $\Rightarrow$ item 1
[(L13)]

(L28) $\Rightarrow$ item 2
[(L25)]

(L29) $\Rightarrow$ item 3
[(L26)]

□ (items 1 to 3)

I.3.8 The sample's integers

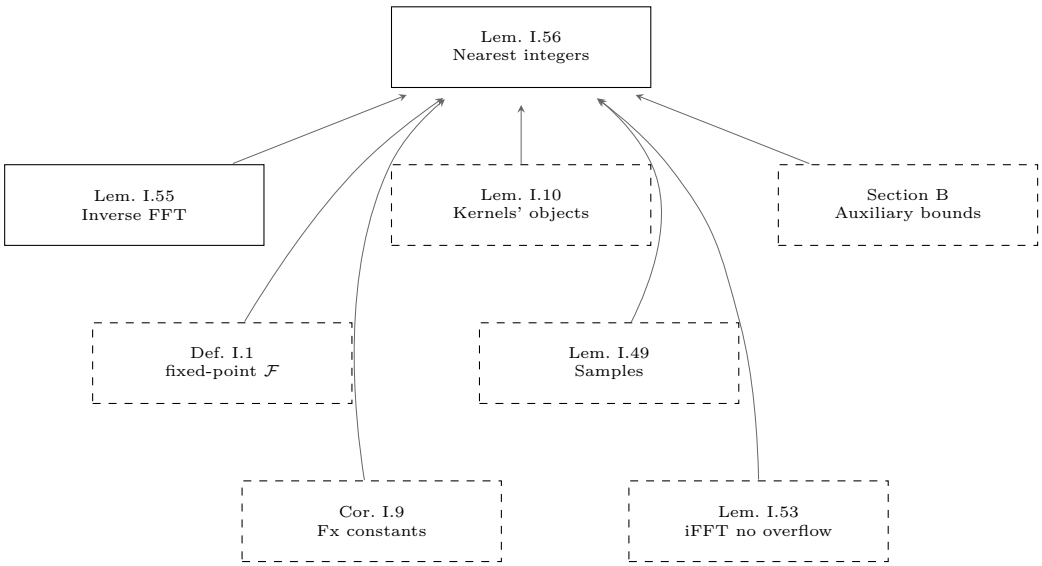


Figure 82: Dependencies, Appendix I.3.8.

Lemma I.55 states the code's inverse FFT over $\mathbb{R}$; Lemma I.56 the nearest integers of the computed inverse FFT.

Lemma I.55 (The code's inverse FFT over $\mathbb{R}$ [to table])**.** *Over $\mathbb{R}$, the stages of `fxpoly_iFFT` undo those of `fxpoly_FFT`, and they do not enlarge a difference. Let:*

- $h \geq 2$ *and* $n = 2^h$*;*
- $f \in \mathbb{R}[x]/(x^n + 1)$*;*
- $v \in \mathbb{C}^{n/2}$*;*
- $w \in \mathbb{C}^{n/2}$*.*

Define:

- $\forall \ell \in \{1, \dots, h-1\}:$ Π_ℓ, *the triples* (j_1, j_2, ψ_k) *of a pair and its root at stage* ℓ *of* `fxpoly_iFFT` *[L0:* `fxp/sign_fxpoly.c:45-81`*];*
- $\forall \ell \in \{1, \dots, h-1\}\ \forall a \in \mathbb{C}^{n/2}\ \forall (j_1, j_2, \psi_k) \in \Pi_\ell:\ (\mathrm{iFFT}_\ell(a)_{j_1}, \mathrm{iFFT}_\ell(a)_{j_2}) := (a_{j_1} + a_{j_2},\ (a_{j_1} - a_{j_2}) \operatorname{conj} \psi_k)$*;*
- $\forall v \in \mathbb{C}^{n/2}:\ \mathrm{iFFT}(v) := 2^{1-h}\mathrm{iFFT}_{h-1}(\cdots \mathrm{iFFT}_1(v))$*;*
- $\hat{f}$*, the output of* FFT *(Algorithm 14), line 26, on* f*;*
- $\mathrm{in}_0 := (f_{[p]} + i\, f_{[p+n/2]})_{p<n/2}$*, that of* FFT*, line 2.*

Then

1. $\mathrm{iFFT}(\hat{f}) = \mathrm{in}_0$*;*
2. $\max_p |\mathrm{iFFT}(v)_p - \mathrm{iFFT}(w)_p| \le \max_\psi |v_\psi - w_\psi|$.

Proof.

DEFINES $\Pi(\Lambda_j)$: the triples (j_1, j_2, ψ) of Λ_j (FFT (Algorithm 14))

(L1) $\forall \ell:\ \Pi_\ell = \Pi(\Lambda_{h-1-\ell})$
[[gate: `verify/gates/tree/ifft_order.py`]: `fxpoly_iFFT` [L0: `fxp/sign_fxpoly.c:45-81`] against `fxpoly_FFT` [L0: `fxp/sign_fxpoly.c:14-40`]; Λ_j (FFT (Algorithm 14))]

(L2) $\forall k:\ |\psi_k| = 1$
[Fact A.42, item 1]

(L3) $\forall x, x', y, y' \in \mathbb{C}:\ (x + y) - (x' + y') = (x - x') + (y - y')$
[expand]

(L4) $\forall x, x', y, y', \psi \in \mathbb{C}:\ (x - y) \operatorname{conj} \psi - (x' - y') \operatorname{conj} \psi = ((x - x') - (y - y')) \operatorname{conj} \psi$
[expand]

(L5) $\forall \ell\ \forall a, a' \in \mathbb{C}^{n/2}:\ \mathrm{iFFT}_\ell(a) - \mathrm{iFFT}_\ell(a') = \mathrm{iFFT}_\ell(a - a')$
[(L3), (L4); iFFT_ℓ (the statement)]

(L6) $\forall a_1, a_2, \psi \in \mathbb{C}:\ (a_1 + a_2\psi) + (a_1 - a_2\psi) = 2a_1$
[expand]

(L7) $\forall a_1, a_2, \psi \in \mathbb{C}:\ ((a_1 + a_2\psi) - (a_1 - a_2\psi)) \operatorname{conj} \psi = 2a_2\psi \operatorname{conj} \psi$
[expand]

(L8) $\Rightarrow\ \forall \ell\ \forall a \in \mathbb{C}^{n/2}:\ \mathrm{iFFT}_\ell(\Lambda_{h-1-\ell}(a)) = 2a$
[(L1), (L2), (L6), (L7); $x \operatorname{conj} x = |x|^2$ (Fact A.41, item 1); $\Lambda_j(a)_{j_1} = a_{j_1} + a_{j_2}\psi$, $\Lambda_j(a)_{j_2} = a_{j_1} - a_{j_2}\psi$ (FFT)]

(L9) $\hat{f} = \Lambda_{h-2}(\cdots \Lambda_0(\mathrm{in}_0))$
[FFT, lines 22 and 26]

(L10) $\mathrm{iFFT}_{h-1}(\cdots \mathrm{iFFT}_1(\hat{f})) = 2^{h-1}\mathrm{in}_0$
[(L5), (L8) at $\ell = 1$ to $h-1$; (L9)]

(L11) $\mathrm{iFFT}(\hat{f}) = \mathrm{in}_0$
[(L10); the division by 2^{h-1} (iFFT, the statement)]

(L12) $\Rightarrow$ item 1
[(L11)]

(L13) $\forall x, x', y, y' \in \mathbb{C}\ \forall k:\ |(x-x')+(y-y')|,\ |((x-x')-(y-y')) \operatorname{conj} \psi_k| \le 2\max(|x-x'|, |y-y'|)$
[(L2); $|x + y| \le |x| + |y|$, $|xy| = |x||y|$ (Fact A.41, item 1)]

(L14) $\forall \ell\ \forall a, a' \in \mathbb{C}^{n/2}:\ \max_p |\mathrm{iFFT}_\ell(a)_p - \mathrm{iFFT}_\ell(a')_p| \le 2\max_p |a_p - a'_p|$
[(L1), (L3), (L4), (L13)]

(L15) $\max_p |\mathrm{iFFT}(v)_p - \mathrm{iFFT}(w)_p| \le 2^{h-1} \max_\psi |v_\psi - w_\psi| / 2^{h-1}$
[(L14) at $\ell = 1$ to $h-1$; the division by 2^{h-1} (iFFT, the statement)]

(L16) $\Rightarrow\ \max_p |\mathrm{iFFT}(v)_p - \mathrm{iFFT}(w)_p| \le \max_\psi |v_\psi - w_\psi|$
[(L15)]

(L17) $\Rightarrow$ item 2
[(L16)]

□ (items 1 and 2)

Lemma I.56 (The nearest integers of the computed inverse FFT [to table])**.** *The integers the signer reads off the sample are those the base sampler returned, arranged by the exact merges. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5), of degree* $n = 2^h \in \{512, 1024\}$.

Define:

- $(\widetilde{z}_0, \widetilde{z}_1)$*, the sample of line 23 of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10), in either center's mode;*
- $(z_0, z_1) \in (\mathbb{Z}[x]/(x^n+1))^2$*, the pair the exact merges of* ffsamp *(Algorithm 6) build from the integers* SamplerZ *(Algorithm 8) returns at deepest's calls (*merge *(Algorithm 4), Postcondition);*
- $w_{j,[p]} \in \mathbb{Z}$*, the integer* `fxp_rint` *returns on the word of the coefficient* p *of* `fxpoly_iFFT`*'s output on* $\widetilde{z}_j$ *[LO:* `fxp/sign_fxcore.c:203-209`*].*

Then

$$\forall j \in \{0,1\}\ \forall p < n: \quad w_{j,[p]} = z_{j,[p]}.$$

Proof.

DEFINES $c_{\text{merge}} := \sqrt{2} \cdot 2^{-64}$ and $k_E := 8\sqrt{2}$ (Lemma G.18 at $(u, \zeta) = (0, 2^{-64})$)
DEFINES $T^* = 2^{30}$ and $e_m = 4c_{\text{merge}}T^* + k_E\zeta$ (Lemma I.49)
DEFINES $\epsilon_{h-1} = 0$
DEFINES $\forall k \le h-2:\ \epsilon_k = 2\epsilon_{k+1} + e_m$
DEFINES M_j, $j \le h-1$, those of Lemma I.53
DEFINES $\forall j \le h-1:\ N_j = M_j/2^{64}$
DEFINES $\delta_0 = 0$
DEFINES $\forall j \le h-2:\ \delta_{j+1} = 2\delta_j + 2\sqrt{2}\,\zeta N_j + 3\sqrt{2}\,\zeta$
DEFINES $\Delta = \epsilon_0 + \delta_{h-1}/2^{h-1} + \sqrt{2}\,\zeta/2$
DEFINES $\hat{z}_{\nu,j}$, at a call ν of the recursion at depth k: the output of FFT (Algorithm 14) on the integer polynomial the exact merges build at ν; $\widetilde{z}_{\nu,j}$, its computed sample
DEFINES u_ℓ and $\widetilde{u}_\ell$, the arrays after ℓ stages of the iFFT of Lemma I.55 and of `fxpoly_iFFT` on $\widetilde{z}_j$
DEFINES y_p, $p < n$: the coefficient p of the scaled output of `fxpoly_iFFT` on $\widetilde{z}_j$
DEFINES $\mathrm{ch}(\nu)$, at a call ν at depth $k \le h-2$: its two children, the calls of lines 19 and 33 of ffsamp (Algorithm 6)
DEFINES μ: a part Re or Im of a center a call of SamplerZ (Algorithm 8) by ν at $k = h-1$ takes

(L1) $\Delta < 1/2$

[[gate: `verify/gates/fx/rint.py`]]

Lemma I.49, items 1, 2, 3, 4 and 5 at every call ν' of the recursion, at its depth k'	This proof
Shared: (f, g, F, G)	
ν, k	ν', k' (the scope)
(f, g, F, G) checked key of degree $n \in \{512, 1024\}$	The statement
ν a call at depth $k \le h - 1$	ν' (the scope)
Assumption A1	$k' = h - 1$ (the scope), at item 2
Its item 1: $\forall \psi : \ \lvert\widetilde{t}_0(\psi)\rvert, \lvert\widetilde{t}_1(\psi)\rvert \le T_k$	
Its item 2: $\forall \psi : \ \lvert\widetilde{tb}_0(\psi)\rvert \le T_{\text{leaf}}$	
Its item 3: $\forall \psi : \ \lvert\widetilde{t}_1(\psi) - \widetilde{z}_1(\psi)\rvert \le H_k$	
Its item 4: $\forall \psi : \ \lvert\widetilde{t}_0(\psi) - \widetilde{z}_0(\psi)\rvert \le D_k$	
Its item 5: $W_x = x_{\text{fx64}} \bmod 2^{128}$	

(I1)

(L2) $k = h - 1 \Rightarrow \ \forall \mu : \ \lvert\mu\rvert \le T^*$
[items 1 and 2 of (I1) at $\nu' := \nu$; Lemma I.49, (L4); [gate: `verify/gates/fx/samples.py`]; $\lvert\mathrm{Re}\, x\rvert, \lvert\mathrm{Im}\, x\rvert \le \lvert x\rvert$ (Fact A.41, item 1); μ, T^* (the proof's block)]

(L3) $k = h - 1 \Rightarrow \ \forall \mu : \ W_\mu = \mu_{\text{fx64}} \bmod 2^{128}$
[item 5 of (I1) at the parent of ν, its splits (ffsamp (Algorithm 6), lines 19 and 33), and at $\nu' := \nu$, line 9 of deepest (Algorithm 7); μ (the proof's block)]

(L4) $k = h - 1 \Rightarrow \ \mathrm{Re}\, \widetilde{z}_{\nu,j}, \ \mathrm{Im}\, \widetilde{z}_{\nu,j} \in \mathbb{Z}$
[Lemma I.49, (L14), (L15), their premises by (L2), (L3)]

(L5) $k = h - 1 \Rightarrow \ \widetilde{z}_{\nu,j} = \hat{z}_{\nu,j}$
[(L4); $\hat{f} = \mathrm{in}_0$ at $h = 1$ (FFT (Algorithm 14), lines 2 and 26)]

(L6) $\lvert\psi\rvert = 1$
[Fact A.42, item 1]

Lemma G.14 at every k	This proof
$\mathcal{F}$	$\mathcal{F}_{\text{fx}}$ (Definition I.1)
u	0
ζ	2^{-64} (the proof's block)
k	k (the scope)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\text{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
$k \in \{1, \ldots, 2^{10} - 1\}$	The scope
Its conclusion: $\tilde{\psi}_k \ \mathcal{I}\left(u^{\pm} + \sqrt{2}\zeta^{\pm}, 0\right) \ \psi_k$	

(I2)

(L7) $\forall k : \ \tilde{\psi}_k \ \mathcal{I}\left((\sqrt{2}\,\zeta)^{\pm}, 0\right) \ \psi_k$
[(I2)]

(L8) $k \le h - 2 \Rightarrow \ \forall \nu' \in \mathrm{ch}(\nu) \ \forall \psi' : \ \lvert\widetilde{z}_{\nu',j}(\psi')\rvert \le 2T^*$
[items 1, 3 and 4 of (I1) at ν'; Lemma I.49, (L1) to (L4); $\lvert x + y\rvert \le \lvert x\rvert + \lvert y\rvert$ (Fact A.41, item 1); T^* (the proof's block)]

Lemma G.18 at every call ν at depth $k \le h-2$, $\forall\psi$, under $\forall\nu' \in \mathrm{ch}(\nu)\ \forall\psi'$: $\lvert\widetilde{z}_{\nu',j}(\psi') - \hat{z}_{\nu',j}(\psi')\rvert \le \epsilon_{k+1}$	This proof
$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
ζ	2^{-64} (the proof's block)
f_0, f_1	$\widetilde{z}_{\nu',j},\ \nu' \in \mathrm{ch}(\nu)$ (the proof's block)
ψ	ψ (the scope)
$\tilde{\psi}$	$\widetilde{\psi}$ (Lemma G.14)
$\tilde{a}, \tilde{b}$	$\widetilde{z}_{\nu,j}(\psi), \widetilde{z}_{\nu,j}(-\psi)$ ($\widetilde{\text{merge}}$ (Algorithm 4))
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
$f_0, f_1 \in C_{\mathcal{F}}$	$\widetilde{\text{merge}}$ (Algorithm 4) and deepest (Algorithm 7), their computed postconditions
$\psi \in \mathbb{C}$	The scope
$\tilde{\psi} \in C_{\mathcal{F}}$	$\widetilde{\psi}$ (Definition A.8)
Assumption A1	(L6)
Assumption A2	(L7)

Its conclusion: $(\tilde{a}, \tilde{b})\ \mathcal{N}\ (c_{\mathrm{merge}}, k_E\zeta)\ (a, b)$

(L9) $k \le h-2 \wedge [\forall\nu' \in \mathrm{ch}(\nu)\ \forall\psi' :\ \lvert\widetilde{z}_{\nu',j}(\psi') - \hat{z}_{\nu',j}(\psi')\rvert \le \epsilon_{k+1}] \Rightarrow\ \lvert\widetilde{z}_{\nu,j}(\pm\psi) - \hat{z}_{\nu,j}(\pm\psi)\rvert \le 2\epsilon_{k+1} + e_m$

[(I3); (L8); Fact A.41, its lead and items 2 and 1; e_m (Lemma I.49); merge (Algorithm 4), Postcondition, at the children's deviations of the premise; $\mathrm{ch}(\nu)$ (the proof's block)]

(L10) $\forall\psi :\ \lvert\widetilde{z}_j(\psi) - \hat{z}_j(\psi)\rvert \le \epsilon_0$

[induction on $h-1-k$: (L5) the base, (L9) the step; ϵ_k (the proof's block)]

Lemma I.55, items 1 and 2 at $f := z_j$ and $(v, w) := (\widetilde{z}_j, \hat{z}_j)$	This proof
Shared: h, n	
f	z_j (the statement)
v, w	$\widetilde{z}_j, \hat{z}_j$ (the proof's block)
$h \ge 2$	$n \in \{512, 1024\}$ (the statement)
$f \in \mathbb{R}[x]/(x^n+1)$	z_j (the statement)
$v, w \in \mathbb{C}^{n/2}$	$\widetilde{z}_j, \hat{z}_j$ at the $n/2$ roots (the proof's block)

Its item 1: $\mathrm{iFFT}(\hat{f}) = \mathrm{in}_0$

Its item 2: $\max_p\lvert\mathrm{iFFT}(v)_p - \mathrm{iFFT}(w)_p\rvert \le \max_\psi\lvert v_\psi - w_\psi\rvert$

(L11) $\mathrm{iFFT}(\hat{z}_j) = (z_{j,[p]} + i\, z_{j,[p+n/2]})_{p<n/2}$

[item 1 of (I4); in_0 (Lemma I.55)]

(L12) $\max_p\lvert\mathrm{iFFT}(\widetilde{z}_j)_p - (z_{j,[p]} + i\, z_{j,[p+n/2]})\rvert \le \epsilon_0$

[(L10), (L11); item 2 of (I4)]

(L13) $\widetilde{u}_0 = u_0$

[$\widetilde{u}_0$, u_0 (the proof's block)]

Corollary I.9, item 1	This proof
$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
ζ	2^{-64} (the proof's block)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0, 2^{-64})$ (Definition I.1)

Its conclusion: $k_B = 3\sqrt{2}$

(L14) $k_B = 3\sqrt{2}$

[(I5)]

(L15) $\forall\ell \le h-1\ \forall p :\ \lvert\widetilde{u}_{\ell,p}\rvert \le N_\ell$

[Lemma I.53, item 2, at the checked key (the statement); Definition A.5; N_ℓ (the proof's block)]

	Lemma I.10, item 13	This proof
(I6)	h	h (the statement)
	$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
	$h \in \{2, \dots, 10\}$	$n \in \{512, 1024\}$ (the statement)
	each input array of words	$\widetilde{z}_j$ (the statement)
	Assumption A8	$n \in \{512, 1024\}$ (the statement)

Its conclusion: at each of its $h-1$ stages, at each pair (x, y) and its twiddle's conjugate $\widetilde{s}$, the words of $x \oplus y$ and $(x \ominus y) \otimes \widetilde{s}$; then the word of $\mathrm{fl}(x/2^{h-1})$ at each of its 2^h words x

	Lemma B.2, item 3 at every stage $\ell \le h-2$, at each pair (x, y) of the stage and its twiddle's conjugate $\widetilde{s}$ of (I6)	This proof
(I7)	$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
	u	0
	ζ	2^{-64} (the proof's block)
	a, b	$x \ominus y, \widetilde{s}$ (I6)
	$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0, 2^{-64})$ (Definition I.1)
	$a, b \in C_{\mathcal{F}}$	$x \ominus y$ (Definition A.8); $\widetilde{s}$, a stored twiddle's conjugate (Definition I.1, item 6)

Its conclusion: $(a \otimes b)\, \mathcal{I}\left(\left(\sqrt{2}u(2+u)\right)^{\pm}, k_B\zeta^{\pm}\right) ab$

(L16) $\forall \ell \le h-2 :\ \max_p |\widetilde{u}_{\ell+1,p} - u_{\ell+1,p}| \le 2 \max_p |\widetilde{u}_{\ell,p} - u_{\ell,p}| + 2\sqrt{2}\,\zeta N_\ell + 3\sqrt{2}\,\zeta$

[(I6); (I7); (L7), (L14), (L15)]

(L17) $\forall \ell \le h-1 :\ \max_p |\widetilde{u}_{\ell,p} - u_{\ell,p}| \le \delta_\ell$

[induction on ℓ: (L13) the base, (L16) the step; δ_ℓ (the proof's block)]

(L18) $\forall p :\ |\mathrm{fl}(\widetilde{u}_{h-1,p}/2^{h-1}) - \widetilde{u}_{h-1,p}/2^{h-1}| \le \sqrt{2}\,\zeta/2$

[Definition I.1, item 1, at /, per part; $\forall a, b \in \mathbb{R} :\ |a + ib|^2 = a^2 + b^2$ (Fact A.41, item 1)]

(L19) $\forall p :\ |\widetilde{u}_{h-1,p}/2^{h-1} - \mathrm{iFFT}(\widetilde{z}_j)_p| \le \delta_{h-1}/2^{h-1}$

[(L17) at $\ell = h-1$; iFFT (Lemma I.55); u_ℓ (the proof's block)]

(L20) $\Rightarrow\ \max_p |\mathrm{fl}(\widetilde{u}_{h-1,p}/2^{h-1}) - \mathrm{iFFT}(\widetilde{z}_j)_p| \le \delta_{h-1}/2^{h-1} + \sqrt{2}\,\zeta/2$

[(L18), (L19); Fact A.41, item 1]

(L21) $\forall p < n :\ |y_p - z_{j,[p]}| \le \Delta$

[(L12), (L20); $|\mathrm{Re}\, x|, |\mathrm{Im}\, x| \le |x|$ (Fact A.41, item 1); Δ (the proof's block)]

(L22) $w_{j,[p]} = \mathrm{rint}\, y_p$

[Lemma I.53, item 7, at the checked key (the statement)]

(L23) $|\mathrm{rint}\, y_p - y_p| \le 1/2$

[rint (Fact A.6, item 5)]

(L24) $|w_{j,[p]} - z_{j,[p]}| < 1$

[(L1), (L21), (L22), (L23); $|x + y| \le |x| + |y|$ (Fact A.41, item 1)]

(L25) $\Rightarrow\ w_{j,[p]} = z_{j,[p]}$

[(L24); $w_{j,[p]}, z_{j,[p]} \in \mathbb{Z}$ (the statement)]

(L26) $\Rightarrow$ the statement

[(L25)]

□

I.3.9 The entry shifts in $\mathcal{F}_{\text{fx}}$

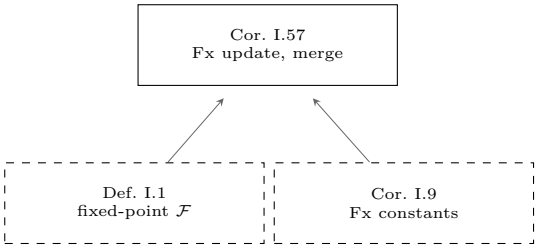


Figure 83: Dependencies, Appendix I.3.9.

Corollary I.57 (The fixed-point update and merge perturbations [to table])**.** *At $u = 0$ the perturbations of each node's center update and of its merged sample are bounded by the factor and merge constants. Let:*

- $h \geq 1$*;*
- $T \in \mathcal{T}_m$ *(Definition A.18) at* $m := 2^h$*.*

Define:

- *The tree*
  - $\forall d \in \mathbb{R}:\ \text{Sub}(d) := \{d\}$ *and* $\text{Sub}(\nu) := \{\nu\} \cup \text{Sub}(L(\nu)) \cup \text{Sub}(R(\nu))$ *(Definition A.18);*
  - $\forall m' \in \{2, 4, \ldots, m\}\ \forall T' \in \text{Sub}(T) \cap \mathcal{T}_{m'}:\ j(T') := \log_2 m' - 1$*;*
  - $k' := j(T_{11}) + 1$*;*
- *The node factor*
  - l_{10}*, that of Lemma G.42;*
  - $\widetilde{l}_{10}$*, that of* LDL† *(Algorithm 5), line 12;*
- *The node bounds*
  - $\ell := \max_\psi |l_{10}|$*;*
  - $E_l := \max_\psi |\widetilde{l}_{10} - l_{10}|$*;*
  - $\widetilde{\ell} := \max_\psi |\widetilde{l}_{10}|$*;*
- *The center shifts*
  - $c_{\text{merge}} := \sqrt{2}\,\zeta$ *and* $k_E := 8\sqrt{2}$ *(Corollary I.9, items 5 and 6, at* $u := 0$*);*
  - $k_I(\widetilde{\ell}) := k_I$ *of Lemma G.20 at* $|l_{10}| := \widetilde{\ell}$*;*
  - $a_0 := 0$*;*
  - $\forall j \geq 0:\ a_{j+1} := \sqrt{2}(1 + c_{\text{merge}})a_j + k_E\zeta$*;*
- *The centers and the samples*
  - $\widetilde{t}_1$*,* X_0*,* $\widetilde{tb}_0$ *and* $\widetilde{z}_1$*, those of* ffsamp *(Algorithm 6);*
  - $\forall \nu \in \text{Sub}(T)$*:* $Z_1(\nu)$*, the outputs* z_1 *of* ffsamp *over* $\mathbb{R}$ *at the subtree* T_{11} *of* ν*.*

Then

1. $\forall k \geq 0\ \forall \nu \in \text{Sub}(T)$ *of degree* $2^{k+2}\ \forall z_1 \in Z_1(\nu)$*:* $\|\widetilde{tb}_0 - X_0\| \leq E_l\|\widetilde{t}_1 - z_1\| + \widetilde{\ell}\|\widetilde{z}_1 - z_1\| + k_I(\widetilde{\ell})\zeta$*;*
2. $\forall \nu \in \text{Sub}(T) \setminus \mathbb{R}\ \forall z_1 \in Z_1(\nu)$*:* $\|\widetilde{z}_1 - z_1\| \leq ((1 + c_{\text{merge}})^{k'} - 1)\|z_1\| + a_{k'}$*;*
3. $\forall j \geq 0:\ a_j \geq 0$*.*

Proof. Proof of item 1.

	Lemma G.51, item 1 at every k, ν and z_1 of item 1	This proof
	Shared: $h, T,\ l_{10}, \widetilde{l}_{10},\ \ell, E_l, \widetilde{\ell},\ k_I(\widetilde{\ell})$	
(I1)	$\mathcal{F}, (u, \zeta)$	$\mathcal{F}_{\mathrm{fx}}, (0, 2^{-64})$ (Definition I.1)
	k, ν, z_1	k, ν, z_1 (the statement)
	$h \geq 1$	The statement
	$\mathcal{F}$ a realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
	$k \geq -1$	$k \geq 0$ (the statement)
	$T \in \mathcal{T}_n$ at $n := 2^h$	$T \in \mathcal{T}_m$ at $m := 2^h$ (the statement)
	$\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_{2^{k+2}}$	$\nu \in \mathrm{Sub}(T)$ of degree 2^{k+2} (the statement)
	$z_1 \in \mathcal{R}_{2^{k+2}}$	$z_1 \in Z_1(\nu)$ (the statement)
	Its item 1: $\|\widetilde{t}\widetilde{b}_0 - X_0\| \leq E_l\|\widetilde{t}_1 - z_1\| + \widetilde{\ell}\|\widetilde{z}_1 - z_1\| + (1+u)(u + (1+u)e_{\mathrm{mul}})\widetilde{\ell}\|\widetilde{t}_1 - \widetilde{z}_1\| + u\|X\| + k_I(\widetilde{\ell})\zeta$	

(L1) $\|\widetilde{t}\widetilde{b}_0 - X_0\| \leq E_l\|\widetilde{t}_1 - z_1\| + \widetilde{\ell}\|\widetilde{z}_1 - z_1\| + (1+u)(u + (1+u)e_{\mathrm{mul}})\widetilde{\ell}\|\widetilde{t}_1 - \widetilde{z}_1\| + u\|X\| + k_I(\widetilde{\ell})\zeta$
[(I1)]

(L2) $e_{\mathrm{mul}} = \sqrt{2}\,u(2+u)$
[e_{mul} (Lemma G.51)]

(L3) $u = 0 \Rightarrow\ e_{\mathrm{mul}} = 0$
[(L2); Definition I.1: $u = 0$; e_{mul} (Corollary I.9, item 7)]

(L4) $u = 0 \Rightarrow\ (1+u)(u + (1+u)e_{\mathrm{mul}})\widetilde{\ell}\|\widetilde{t}_1 - \widetilde{z}_1\| = 0$
[(L3); Definition I.1: $u = 0$]

(L5) $u = 0 \Rightarrow\ u\|X\| = 0$
[Definition I.1: $u = 0$]

(L6) $\Rightarrow$ item 1
[(L1), (L4), (L5)]

□ (item 1)

Proof of item 2.

	Lemma G.52 at every ν of item 2	This proof
	Shared: T	
(I2)	$\mathcal{F}, (u, \zeta)$	$\mathcal{F}_{\mathrm{fx}}, (0, 2^{-64})$ (Definition I.1)
	m, ν	$2^{j(\nu)+1}, \nu$ (the statement)
	$\mathcal{F}$ a realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
	$T \in \mathcal{T}_n$	The statement
	$m \geq 2$	$\nu \in \mathrm{Sub}(T) \setminus \mathbb{R}$ (the statement)
	$\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m$	The statement; j (the statement)
	Its conclusion: $\|\widetilde{z}_1 - z_1\| \leq \left((1 + c_{\mathrm{merge}})^{k'} - 1\right)\|z_1\| + a_{k'}$	

(L7) $\|\widetilde{z}_1 - z_1\| \leq ((1 + c_{\mathrm{merge}})^{j(\nu)} - 1)\|z_1\| + a_{j(\nu)}$
[(I2); $k' := \mathrm{lev}(\nu)$ (Lemma G.52); j (the statement)]

(L8) $j(\nu) \leq k'$
[j, k', Sub (the statement); Definition A.18]

(L9) $\forall j \geq 0 :\ a_j \in [0, a_{j+1}]$
[induction on j: a_0, a_1 (the statement) the base; a_{j+1}, c_{merge}, k_E (the statement), expand, the step]

(L10) $\forall k_1, k_2 \in \mathbb{Z}_{\geq 0},\ k_1 \leq k_2 :\ (1 + c_{\mathrm{merge}})^{k_1} - 1 \leq (1 + c_{\mathrm{merge}})^{k_2} - 1$
[c_{merge} (the statement); expand]

(L11) $\|\widetilde{z}_1 - z_1\| \leq ((1 + c_{\mathrm{merge}})^{k'} - 1)\|z_1\| + a_{k'}$
[(L7), (L8), (L9), (L10); Fact A.41, item 8]

(L12) $c_{\mathrm{merge}} = u + (1+u)\,e$
[c_{merge} (Lemma G.18)]

(L13) $u = 0 \Rightarrow\ e = \sqrt{2}\,\zeta$

[Definition I.1: $u = 0$; e (Corollary I.9, item 4)]

(L14) $u = 0 \Rightarrow\ c_{\text{merge}} = \sqrt{2}\,\zeta$

[(L12), (L13)]

(L15) $u = 0 \Rightarrow\ k_E = 8\sqrt{2}$

[Definition I.1: $u = 0$; k_E (Corollary I.9, item 6)]

(L16) $a_0 = 0$

[a_j (Lemma G.52)]

(L17) $a_{j+1} = \sqrt{2}(1 + c_{\text{merge}})a_j + k_E\zeta$

[a_j (Lemma G.52)]

(L18) $\Rightarrow$ item 2

[(L11), (L14), (L15), (L16), (L17)]

□ (item 2)

Proof of item 3.

(L19) $\Rightarrow$ item 3

[(L9)]

□ (item 3)

I.4 The base sampler's perturbation budget in $\mathcal{F}_{\text{fx}}$

Lemma I.58 states the exponent; Lemma I.59 its split; Lemma I.60 the polynomial; Lemma I.61 the accumulator.

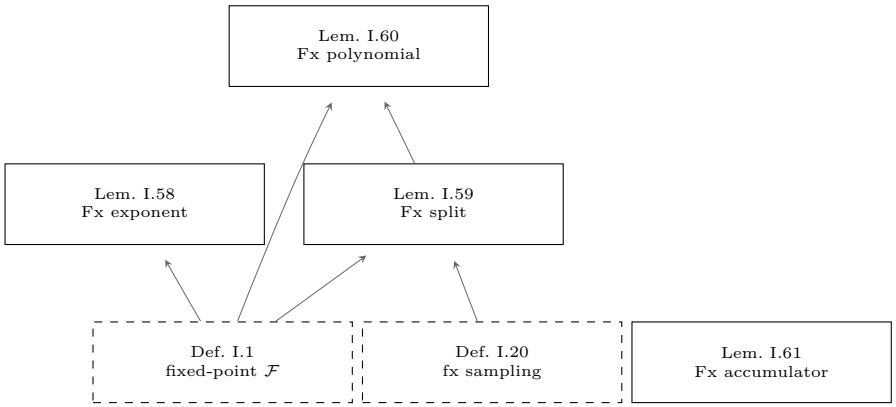


Figure 84: Dependencies, Appendix I.4.

Lemma I.58 (The fixed-point exponent [to table])**.** *In $\mathcal{F}_{\text{fx}}$, the base sampler's exponent lies within $(dss + \frac{3}{2}(z-r)^2 + 2)\zeta_{\text{op}} + \frac{3}{2}\zeta_{\text{op}}^2$ of x. Let:*

- *$z \in \mathbb{Z}$, a value of z of* SamplerZ *(Algorithm 8), line 10;*
- *$r \in \mathbb{R}$, a value of r of line 3;*
- *$\sigma > 0$, a value of $1/\texttt{isigma}$, `isigma` the input of* SamplerZ*.*

Define:

- *dss and x, those of* SamplerZ*, lines 1 to 16, at z, r and σ;*
- *$\zeta_{\text{op}} := 2^{-65}$ (Definition I.1);*
- *$\widetilde{r}$, $\widetilde{dss}$, $\widetilde{a}_x$, $\widetilde{b}_x$ and $\widetilde{x}$, the values* SamplerZ *computes in $\mathcal{F}_{\text{fx}}$ (lines 2 to 15) at z, r and σ.*

Then

$$|\widetilde{x} - x| \le (dss + \tfrac{3}{2}(z-r)^2 + 2)\zeta_{\text{op}} + \tfrac{3}{2}\zeta_{\text{op}}^2.$$

Proof.

DEFINES C_0, z_0, a_x, b_x (SamplerZ (Algorithm 8), its input C_0 and lines 1 to 16)

(L1) $\widetilde{r} = r$

[SamplerZ, line 2; $\mathrm{fl}(x-y) = x - y$ (Fact A.6, item 8)]

(L2) $\exists\, \zeta_a, \zeta_b \in \mathbb{R},\ |\zeta_a|, |\zeta_b| \le \zeta_{\mathrm{op}} :\ \widetilde{dss} = dss + \zeta_a/2 + \zeta_b$

[Definition I.1, item 1, at $\texttt{isigma}^2$, and item 2, at /2]

(L3) $\exists\, \zeta_c, \zeta_e \in \mathbb{R},\ |\zeta_c|, |\zeta_e| \le \zeta_{\mathrm{op}} :\ \widetilde{a}_x = ((z-r)^2 + \zeta_c)\widetilde{dss} + \zeta_e$

[(L1); $\mathrm{fl}(z - \widetilde{r}) = z - \widetilde{r}$ (Fact A.6, items 4 and 8); Definition I.1, item 1, at $(z-\widetilde{r})^2$ and at $\cdot\, \widetilde{dss}$]

(L4) $\exists\, \zeta_f \in \mathbb{R},\ |\zeta_f| \le \zeta_{\mathrm{op}} :\ \widetilde{b}_x = b_x + \zeta_f$

[Definition I.1, item 1, at $z_0^2 C_0$; $\mathrm{fl}(z_0^2) = z_0^2$ (Fact A.6, item 4)]

(L5) $\Rightarrow\ \widetilde{x} - x = \zeta_c\, dss + (z-r)^2(\zeta_a/2 + \zeta_b) + \zeta_c(\zeta_a/2 + \zeta_b) + \zeta_e - \zeta_f$

[(L2), (L3), (L4); $\mathrm{fl}(\widetilde{a}_x - \widetilde{b}_x) = \widetilde{a}_x - \widetilde{b}_x$ (Fact A.6, item 8); $a_x = (z-r)^2 dss$ (SamplerZ, line 12)]

(L6) $\Rightarrow\ |\widetilde{x} - x| \le (dss + \frac{3}{2}(z-r)^2 + 2)\zeta_{\mathrm{op}} + \frac{3}{2}\zeta_{\mathrm{op}}^2$

[(L5); $|x+y| \le |x| + |y|$ (Fact A.41, item 1); $|\zeta_a/2 + \zeta_b| \le \frac{3}{2}\zeta_{\mathrm{op}}$ ((L2); Fact A.41, item 1)]

(L7) $\Rightarrow$ the statement

[(L6)]

□

Lemma I.59 (The fixed-point exponent's split [to table])**.** *In $\mathcal{F}_{\mathrm{fx}}$, the split of the base sampler's exponent lies within $(si+3)\zeta_{\mathrm{op}} + y|\epsilon_L|$ of y, $si \ge 0$, and si is the truncation of y $\texttt{INV_LOG2}$ within ζ_{op}. Let:*

- *$y \in \mathcal{F}_{\mathrm{fx}}$ be the input of* BerExp *(Algorithm 9) in place of $\widetilde{x}$.*

Define:

- $\texttt{LOG2}$ *and* $\texttt{INV_LOG2}$*, the stored* $\ln 2$ *and* $1/\ln 2$ *of* BerExp*;*
- ϵ_L*, that of* BerExp*, line 1;*
- $\zeta_{\mathrm{op}} := 2^{-65}$ *(Definition I.1);*
- $si := \mathrm{trunc}(\mathrm{fl}(y \cdot \texttt{INV_LOG2}))$ *(line 2);*
- $\widetilde{r'} := \mathrm{fl}(y - \mathrm{fl}(si \cdot \texttt{LOG2}))$ *(lines 2 to 4);*
- $r' := \max(\widetilde{r'}, 0)$ *(line 4).*

Assume:

(A1) $y \ge 0$.

Then

1. $|(si \ln 2 + r') - y| \le (si+3)\zeta_{\mathrm{op}} + y|\epsilon_L|$;
2. $si \ge 0$;
3. $\exists\, \zeta_g \in \mathbb{R},\ |\zeta_g| \le \zeta_{\mathrm{op}} :\ si = \mathrm{trunc}(y\, \texttt{INV_LOG2} + \zeta_g)$.

Proof. (L1) $\mathrm{fl}(y\, \texttt{INV_LOG2}) \ge 0$

[$y \ge 0$ (assumption A1); $\texttt{INV_LOG2} > 0$ (Definition I.20); $\forall a, b \in \mathbb{R},\ a \le b :\ \mathrm{fl}(a) \le \mathrm{fl}(b)$, and $\mathrm{fl}(0) = 0$ (Fact A.6, item 9)]

(L2) $\exists\, \zeta_g \in \mathbb{R},\ |\zeta_g| \le \zeta_{\mathrm{op}} :\ si = \mathrm{trunc}(y\, \texttt{INV_LOG2} + \zeta_g)$

[Definition I.1, item 1, at $y \cdot \texttt{INV_LOG2}$]

(L3) $\exists\, \zeta_h \in \mathbb{R},\ |\zeta_h| \le \zeta_{\mathrm{op}} :\ \widetilde{r'} = y - si\, \texttt{LOG2} - \zeta_h$

[Definition I.1, item 1, at $si \cdot \texttt{LOG2}$; $\mathrm{fl}(x-y) = x - y$ (Fact A.6, item 8)]

(L4) $(si \ln 2 + r') - y = si(\ln 2 - \texttt{LOG2}) - \zeta_h + (r' - \widetilde{r'})$

[(L3); expand]

(L5) $\widetilde{r'} \ge y - (y\, \texttt{INV_LOG2} + \zeta_g)\texttt{LOG2} - \zeta_h$

[(L2), (L3), (L1); $\forall v \ge 0 :\ \mathrm{trunc}\, v = \lfloor v \rfloor$ (Fact A.6, item 5); $\lfloor v \rfloor \le v$ (Fact A.41, item 22); $\texttt{LOG2} > 0$ (the stored word [LO: fxp/fxp_consts.h:2087])]

(L6) $y - (y\, \texttt{INV_LOG2} + \zeta_g)\texttt{LOG2} - \zeta_h \ge -y|\epsilon_L| - (\texttt{LOG2} + 1)\zeta_{\mathrm{op}}$

[$\texttt{INV_LOG2} \cdot \texttt{LOG2} = 1 + \epsilon_L$ (BerExp (Algorithm 9), line 1); (L2), (L3); $\texttt{LOG2} > 0$ (the stored word [LO: fxp/fxp_consts.h:2087]); $y \ge 0$ (assumption A1)]

(L7) $\Rightarrow$ $\widetilde{r'} \geq -y|\epsilon_L| - (\texttt{LOG2}+1)\zeta_{\text{op}}$

[(L5), (L6)]

(L8) $\Rightarrow$ $r' - \widetilde{r'} \in [0, y|\epsilon_L| + 2\zeta_{\text{op}}]$

[$r' - \widetilde{r'} = \max(-\widetilde{r'}, 0)$ (the statement); (L7); $\texttt{LOG2} < 1$, the stored $\ln 2$ (Definition I.20)]

(L9) $si \geq 0$

[(L2), (L1); Fact A.6, item 5; Fact A.41, item 22]

(L10) $\Rightarrow$ $|(si \ln 2 + r') - y| \leq (si+3)\zeta_{\text{op}} + y|\epsilon_L|$

[(L4), (L8); $|\ln 2 - \texttt{LOG2}| \leq \zeta_{\text{op}}$ (Definition I.20); $|\zeta_h| \leq \zeta_{\text{op}}$ (L3); $si \geq 0$ (L9)]

(L11) $\Rightarrow$ item 1

[(L10)]

(L12) $\Rightarrow$ item 2

[(L9)]

(L13) $\Rightarrow$ item 3

[(L2)]

□ (items 1 to 3)

Lemma I.60 (The fixed-point polynomial [to table])**.** *In $\mathcal{F}_{\text{fx}}$, the base sampler's polynomial lies within $2^{-51.05}$ of $e^{-r'}\widetilde{ccs}$. Let:*

- `isigma` *be an input of* SamplerZ *(Algorithm 8).*

Define:

- $\sigma := 1/\texttt{isigma}$*;*
- r'*, that of Lemma I.59;*
- $\widetilde{ccs}$*, that of* SamplerZ*, line 6;*
- `expm_p63`*, that of* BerExp *(Algorithm 9), lines 8 to 12;*
- $y := \texttt{fxp_expm_p63}(r', \widetilde{ccs})/2^{63}$ *[L0: fxp/sign_fxsampler.c: 88-135];*
- $L := 0.6931471805599453095 + 2^{-30}$ *(Lemma H.25);*
- $\sigma_{\min}$*, the stored word [L0: fxp/fxp_consts.h: 2073-2089].*

Assume:

(A1) $\sigma \in [\sigma_{\min}, 2\sigma_{\min}]$*;*

(A2) $r' \in [0, L]$*;*

(A3) $\widetilde{ccs} < 1$.

Measured:

- *`fxp_expm_p63` [L0: fxp/sign_fxsampler.c: 88-135] is the plain `expm_p63` [L0: sign_sampler.c: 779-865] statement for statement, with `fpr_trunc`, `fpr_mul2e` read as `fxp_trunc`, `fxp_mul2e`: the same coefficient words, the same integer steps in the same order, the same declared types [gate: verify/gates/sampler/expm_source.py].*

Then

$$|y/(e^{-r'}\widetilde{ccs}) - 1| \leq 2^{-51.05}.$$

Proof. (L1) $\lfloor r' 2^{63} \rfloor = \texttt{fxp_trunc}(\texttt{fxp_mul2e}(r', 63))$

[$\text{fl}(2^e x) = 2^e x$ (Fact A.6, item 3); trunc exact (Fact A.6, item 5; Definition I.1, item 3); assumption A2 [L0: fxp/sign_fxsampler.c:105]]

(L2) $\Rightarrow$ $2^{63} y = \texttt{expm_p63}(r', \widetilde{ccs})$

[y (the statement); (L1) [L0: fxp/sign_fxsampler.c:105]; `fxp_expm_p63`: `expm_p63` at r', $\widetilde{ccs}$ (the measured row)]

(L3) $\sigma_{\min}/\sigma \geq 1/2$

[$\sigma \in [\sigma_{\min}, 2\sigma_{\min}]$ (assumption A1)]

(L4) $\widetilde{ccs} \geq 1/2$

[(L3); $\widetilde{ccs} = \text{fl}(\sigma_{\min}/\sigma)$ (SamplerZ, line 6); $\forall a, b \in \mathbb{R},\ a \leq b:\ \text{fl}(a) \leq \text{fl}(b)$ (Fact A.6, item 9); $\text{fl}(1/2) = 1/2$ ($1/2 \in \mathcal{F}_{\text{fx}}$, Definition I.1)]

(L5) $\widetilde{ccs} \in [1/2, 1)$

[(L4); assumption A3]

Lemma H.25 at $ccs := \widetilde{ccs}$	This proof
Shared: r', L	
(I1) ccs y $r', ccs \in \mathbb{R}$	$\widetilde{ccs}$ (the scope) y (L2) r', $\widetilde{ccs}$
Assumption A1 Assumption A2	Assumption A2 (L5)
Its conclusion: $\lvert y/(e^{-r'} ccs) - 1\rvert \le 2^{-51.05}$	

(L6) $\Rightarrow$ $\lvert y/(e^{-r'} \widetilde{ccs}) - 1\rvert \le 2^{-51.05}$

[(I1)]

(L7) $\Rightarrow$ the statement

[(L6)]

□

Lemma I.61 (The fixed-point accumulator [to table])**.** *In $\mathcal{F}_{\text{fx}}$, the base sampler's accumulator lies within $2 \cdot 2^{-64}$ below its exact value. Let:*

- *$y \in \mathcal{F}_{\text{fx}}$ be the input of* BerExp *(Algorithm 9) in place of $\widetilde{x}$.*

Define:

- `LOG2` *and* `INV_LOG2`*, the stored* $\ln 2$ *and* $1/\ln 2$ *of* BerExp*;*
- $si := \text{trunc}(\text{fl}(y \cdot \texttt{INV_LOG2}))$ *(*BerExp*, line 2);*
- $\widetilde{r'} := \text{fl}(y - \text{fl}(si \cdot \texttt{LOG2}))$ *(*BerExp*, lines 2 to 4);*
- $r' := \max(\widetilde{r'}, 0)$ *(*BerExp*, line 4);*
- $\widetilde{ccs}$*, that of* SamplerZ *(Algorithm 8), line 6;*
- $s_x := \min(si, 63)$ *(Fact G.66);*
- $z_{\text{acc}} := ((\texttt{expm_p63}(r', \widetilde{ccs}) \ll 1) - 1) \gg s_x$ *(Fact G.66 at $ccs := \widetilde{ccs}$);*
- $acc_c := \texttt{expm_p63}(r', \widetilde{ccs})/2^{63+s_x}$ *(Lemma H.26 at the signer's si, r' and $ccs := \widetilde{ccs}$);*
- $\widetilde{acc}_c := z_{\text{acc}}/2^{64}$ *(Lemma H.26).*

Assume:

(A1) $si \in [0, 63]$*;*

(A2) $\texttt{expm_p63}(r', \widetilde{ccs}) \ge 1$.

Then

$$\widetilde{acc}_c/acc_c - 1 \in [-2 \cdot 2^{-64}/acc_c,\ 0].$$

Proof. (L1) $z_{\text{acc}} = ((\texttt{expm_p63}(r', \widetilde{ccs}) \ll 1) - 1) \gg s_x$

[$si \le 63$ (assumption A1); line 15 of BerExp (Algorithm 9) skipped at $si \le 63$ [LO: `fxp/sign_fxsampler.c:164-169`]; Fact G.66 at si, r' and $ccs := \widetilde{ccs}$ (the statement); $si \ge 0$ (assumption A1), assumption A1 of Fact G.66]

Lemma H.26, item 1 at the computed si, r' and $ccs := \widetilde{ccs}$	This proof
Shared: $z_{\text{acc}}, s_x,\ acc_c, \widetilde{acc}_c$	
(I1) si r' ccs	si (the statement; BerExp, line 2) r' (the statement; BerExp, line 4) $\widetilde{ccs}$ (the statement)
Assumption A1 Assumption A2	Assumption A1 Assumption A2
Its conclusion: $\widetilde{acc}_c/acc_c - 1 \in \left[-2 \cdot 2^{-64}/acc_c,\ 0\right]$	

(L2) $\Rightarrow$ $\frac{\widetilde{acc}_c}{acc_c} - 1 \in \left[-\frac{2 \cdot 2^{-64}}{acc_c},\ 0\right]$

[(L1); (I1); $si \leq 63$ (assumption A1)]

(L3) $\Rightarrow$ the statement

[(L2)]

□

I.5 The terms of $\ln R$

Structure. Appendix I.5.1 states the terms and the signer's inputs; Appendix I.5.2 the base sampler's inputs; Appendix I.5.3 the preconditions; Appendix I.5.4 the terms from the derived bounds; Appendix I.5.5 the terms on a sub-event of the tail-cut event; Appendix I.5.6 the leaf sum under a fixed key.

I.5.1 The terms and the signer's inputs

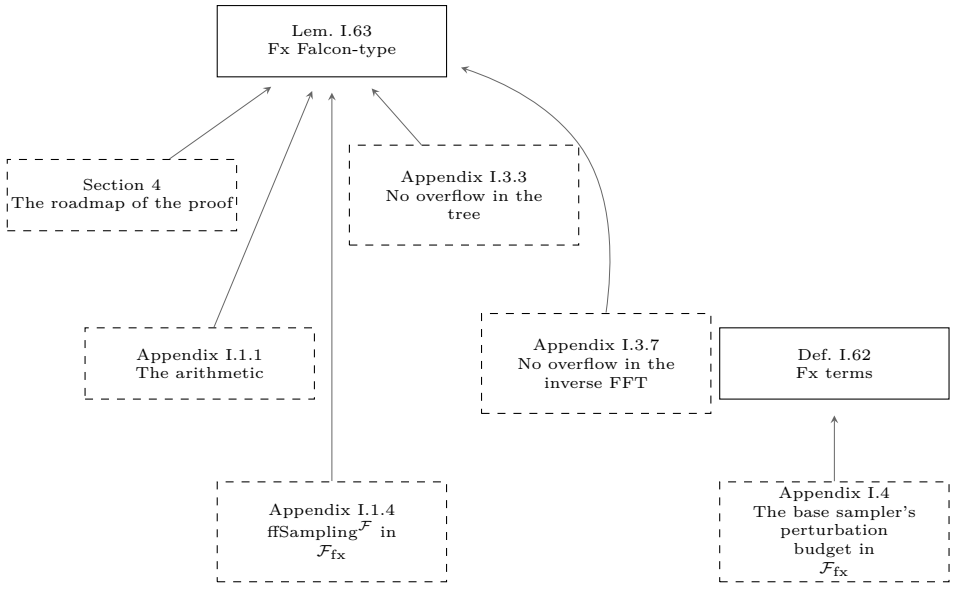


Figure 85: Dependencies, Appendix I.5.1.

Definition I.62 (The fixed-point signer's terms [to table])**.** The chain of the preconditions of Lemmas 4.7, 4.8 and 4.9, Corollary 4.10 and Theorem 4.11, read at $u = 0$ and at this signer's inputs. Let:

- (f, g, F, G) be a checked key (Definition 5.5);
- $\bar{e}, \bar{T}, \bar{Z} \in [0, \infty)$.

Define:

- The signer's words and parameters
  - $h := \log_2 n$;
  - $\zeta_{\text{op}} := 2^{-65}$ (Definition I.1);
  - $\sigma_{\min}$, the stored word [L0: `fxp/fxp_consts.h:2073-2089`];
  - ϵ_L, that of BerExp (Algorithm 9), line 1;
  - $(\lambda, \alpha) := \begin{cases} (128, 257) & n = 512 \\ (256, 513) & n = 1024 \end{cases}$;
- The key bounds
  - m_0, M_0, d_{lo}, d_{hi}, $\bar{\varsigma}$, $\bar{g}_{11}$, $\check{\gamma}_{\text{hyb}}$ and $\check{\gamma}_{\text{root}}$, those of Proposition 5.8;
  - E_{00}, E_{11} and E_{01}, those of Definition A.36, items 5, 6 and 7;

  - $\bar\kappa_{\mathrm{root}} := (\check\gamma_{\mathrm{root}}\, q\check\gamma_{\mathrm{hyb}}^2 + E_{01})^2/q^2$ (Proposition 5.8, item 3);
  - $\forall 1 \le k \le h-1:\ \bar\kappa_k := (\bar\varsigma - 1)^2/(4\bar\varsigma)$ (Proposition 5.8, item 2);
  - $\bar\Xi' := \bar\varsigma^{1/2}$ (Proposition 5.8, item 5);
  - $\bar\Xi'_{\mathrm{root}} := ((M_0 + \bar g_{11})/d_{\mathrm{lo}})^{1/2}$ (Lemma H.21, item 2);
  - $\bar\Xi := \bar\varsigma^{1/2}$ (Proposition 5.8, item 6);
  - $\bar\ell := \max(1,\ \check\gamma_{\mathrm{root}}/(1 - E_{00}\check\gamma_{\mathrm{hyb}}^2/q) + E_{01}/m_0)$ (Proposition 5.8, item 7);
  - $\bar K_n^{\mathrm{fx}} := (\bar\kappa_{\mathrm{root}}, \bar\kappa_k, \bar\Xi', \bar\Xi'_{\mathrm{root}}, \bar\Xi, \bar\ell)$ (Definition 4.6);
- The sampler's bounds
  - $E_x := (1/(2\sigma_{\mathrm{min}}^2) + \frac{3}{2}\cdot 19.5^2 + 2)\zeta_{\mathrm{op}} + \frac{3}{2}\zeta_{\mathrm{op}}^2$ (Lemma I.58 at $dss \le 1/(2\sigma_{\mathrm{min}}^2)$ and $|z-r| \le 19.5$; Lemma H.24, items 1 and 3);
  - $E_s := 66\zeta_{\mathrm{op}} + 45|\epsilon_L|$ (Lemma I.59, item 1, at $si \le 63$ and $y \le 45$);
  - $e_{\mathrm{poly}} := 2^{-51.05}$ (Lemma I.60);
  - $e_+ := e^{E_x+E_s}(1 + e_{\mathrm{poly}}) - 1$;
  - $\forall k \le 18:\ E_{x,k} := (1/(2\sigma_{\mathrm{min}}^2) + \frac{3}{2}(k+1)^2 + 2)\zeta_{\mathrm{op}} + \frac{3}{2}\zeta_{\mathrm{op}}^2$ (Lemma I.58 at $dss \le 1/(2\sigma_{\mathrm{min}}^2)$ and $|z-r| \le k+1$);
  - $\forall k \le 18:\ e_{+,k} := e^{E_{x,k}+E_s}(1 + e_{\mathrm{poly}}) - 1$;
  - $e_{\mathrm{ccs}} := 2\zeta_{\mathrm{op}}$;
- The error chain
  - $e_{00} := E_{00}/m_0$ (Lemma I.25);
  - $\bar G := M_0(1 + e_{00})$;
  - $Z_I := 1 + \zeta\bar G/q^2$ (Lemmas I.26 and I.27 at $\bar G$);
  - $\chi_{\mathrm{root}} := \max(e_{00},\ Z_I/(1 - e_{00}) - 1)$;
  - $\mathcal{U}_\kappa^0$, that of Definition I.28 at d_{lo} and d_{hi};
  - $\forall 1 \le k \le h-1:\ \vartheta_{k-1} := (1 + \chi_{k-1})/(1 - \chi_{k-1})$ (Definition I.32);
  - $\forall 1 \le k \le h-1:\ \hat\kappa_k := \vartheta_{k-1}\bar\kappa_k + (\vartheta_{k-1} - 1)/2$ (Definition I.32 at $\kappa_k := \bar\kappa_k$);
  - $\chi_0 := \chi_{\mathrm{root}}$ (Definition I.32);
  - $\forall 1 \le k \le h-1:\ \chi_k := \mathcal{U}^0_{\hat\kappa_k}(\chi_{k-1})$ (Definition I.32);
  - $\chi_{\mathrm{leaf}} := \chi_{h-1}$;
- The leaf deviations
  - $s := 1.17\sqrt{q}\,\sigma_{\mathrm{min}}$ (Definition A.25);
  - $c_n := 1/s$ (Definition A.25);
  - $\sigma_{\mathrm{max}} := 1.17^2\sigma_{\mathrm{min}}$;
  - $\chi_\sigma := \max\left((1 + \chi_{\mathrm{leaf}})^{1/2} - 1,\ 1 - (1 - \chi_{\mathrm{leaf}})^{1/2}\right)$ (Corollary G.41 at $u = 0$);
  - k_J, that of Corollary G.41 at $\sqrt{\widetilde{d}_{11}} := (d_{\mathrm{hi}}(1 + \chi_{\mathrm{leaf}}))^{1/2}$;
  - $\chi_\sigma^\zeta := \chi_\sigma + k_J\zeta/s_{\mathrm{min}}$ (Corollary G.41 at $s_{\mathrm{min}} := \sqrt{d_{\mathrm{lo}}}\,c_n$);
  - $\bar\delta := \chi_\sigma^\zeta/(1 - \chi_\sigma^\zeta)$;
  - $s_\star := \sigma_{\mathrm{min}}(1 - \bar\delta)\left(\alpha_L + (1 - \alpha_L)(1 - \bar\delta)^2\right)^{-1/2}$;
  - $\epsilon := 2\sum_{k\ge1} e^{-2\pi^2 s_\star^2 k^2}$;
  - ε_0, that of Definition A.38;
  - $\underline{s} := \sigma_{\mathrm{min}}(1 - \bar\delta)\,\theta_{\alpha_L}(-\bar\delta)^{1/2}$ (Definition A.40 at $(\alpha_L, \sigma_{\mathrm{min}}, \bar\delta)$);
  - $\varepsilon_0^\circ := \varepsilon_0(\underline{s})$ (Definition A.40);
- The node bounds
  - $u_0 := (1 + u)(1 + \zeta/(2d_{\mathrm{lo}}(1 - \chi_{\mathrm{leaf}})(1 - u))) - 1$ (Corollary G.43 at $\chi := \chi_{\mathrm{leaf}}$);
  - $\bar\delta_\mu := (1 + u)^2 - 1$ (Corollary G.43);
  - $c_{\mathrm{sa}} := (1 + u)^2(1 + u + \sqrt{2}\,\zeta) - 1$ (Corollary G.43);
  - $k_{\mathrm{sa}} := (1 + u)(1 + u + \sqrt{2}\,\zeta)/2 + \sqrt{2}$ (Corollary G.43);
  - $M_2 := d_{\mathrm{hi}}(1 + \chi_{\mathrm{leaf}})(1 + c_{\mathrm{sa}})/2 + k_{\mathrm{sa}}\zeta$ (Corollary G.43 at $\chi := \chi_{\mathrm{leaf}}$);
  - $\bar e_0 := (1 + \chi_{\mathrm{leaf}})(1 + u_0) - 1$ (Corollary G.43 at $\chi := \chi_{\mathrm{leaf}}$);
  - $\bar a_1 := c_{\mathrm{sa}} + \chi_{\mathrm{leaf}}(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta/d_{\mathrm{lo}}$ (Corollary G.43);

  - $E_l^{\text{child}} := \dfrac{\bar\delta_\mu + \bar e_0}{1-\bar e_0} + \bar a_1 \dfrac{1+\bar\delta_\mu}{1-\bar e_0} + \sqrt{2}\,(M_2(1+u)+1)\,\zeta$ (Corollary G.43 at $u=0$);
  - $E_l^{\text{root}} := \bar\ell\,\dfrac{\bar\delta_\mu + e_{00}}{1-e_{00}} + \dfrac{E_{01}}{m_0}\,\dfrac{1+\bar\delta_\mu}{1-e_{00}} + \sqrt{2}\,((\sqrt{\bar\kappa_{\text{root}}}\,q + E_{01})(1+u)+1)\,\zeta$ (Corollary G.43 at $\ell := \bar\ell$, $\kappa_{\text{root}} := \bar\kappa_{\text{root}}$);
  - $E_l := \max(E_l^{\text{child}}, E_l^{\text{root}})$;
  - $\widetilde{\ell} := \bar\ell + E_l$;
- The center shifts
  - $c_{\text{split}} := (1+u)(1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1$ (Lemma G.16 at $u=0$);
  - $c_{\text{merge}} := u + (1+u)((1+u+\sqrt{2}\,\zeta)(1+\sqrt{2}\,u(2+u)) - 1)$ (Lemma G.18 at $u=0$);
  - $\forall 1 \le k \le h:\ M_k := (1+c_{\text{merge}})^{h-k} - 1$ (Theorem G.59 at $u=0$);
  - $G_X := c_{\text{split}}$;
  - $G_R := (1+c_{\text{split}})E_l$;
  - $G_\gamma := c_{\text{split}} + G_X(1+\bar\ell) + G_R$ (Theorem G.59 at $u=0$, $\ell := \bar\ell$);
  - $G_Z := G_X\bar\ell + G_R + \bar\ell$ (Theorem G.59 at $u=0$, $\ell := \bar\ell$);
  - k_{split} and k_I, those of Theorem G.59 at $u=0$ (Lemma G.53, items 1 and 2);
  - a_j, that of Lemma G.52 at $u=0$;
  - $K_\zeta := (k_{\text{split}} + (1+c_{\text{split}})k_I(\widetilde{\ell}))\zeta$ (Theorem G.59);
  - $\forall 1 \le k \le h:\ \Theta_k := \sqrt{2^{k-1}}(k_{\text{split}}\zeta + K_\zeta + G_Z\,a_{h-k})$ (Theorem G.59);
  - $\forall 1 \le k \le h:\ \Upsilon_k := (c_{\text{split}} + G_X)(k-1)\bar\ell + G_X\bar\ell + G_R$ (Corollary G.62 at $u=0$, $\ell := \bar\ell$);
  - $R^\circ := \sqrt{2}\,\bar\Xi\tau\sigma_{\max}(1+\bar\delta)(n/2)^{1/2}$ (Corollary G.62 at $\Xi := \bar\Xi$, $\sigma_{\max} := 1.17^2\sigma_{\min}$);
  - $c_S := \bar\Xi(n/2)^{1/2}$ (Corollary G.62 at $\Xi := \bar\Xi$);
  - $\gamma := \bar\Xi'(1+2(h-1)\bar\Xi)\,G_\gamma$;
  - $\gamma_S := c_S\bar\Xi'\sum_{k=1}^h \Upsilon_k$;
- The terms
  - $D_0^\circ := \bar\Xi'_{\text{root}}\bar e + \bar\Xi'\sum_{k=1}^h[(c_{\text{split}} + G_X)\bar T + \Upsilon_k R^\circ + \Theta_k]$;
  - $D_Z^\circ := \bar\Xi' G_Z \sum_{k=1}^h M_k$;
  - $D^\circ := D_0^\circ + D_Z^\circ \bar Z$;
  - $D_S := D^\circ/(1-\gamma-\gamma_S)$;
  - $W^\circ := D_S^2/\sigma_{\min}^2$;
  - $M_{2\alpha}$, that of Corollary 4.10, precondition 1, at the row bounds $e_{+,k}$ and e_{ccs}: Lemma G.73 at order 2α, $\sigma_{\min}$, $\sigma_{\max}(1+\bar\delta)$ and τ;
  - ϖ, that of Lemma G.73 at order 2α, $\sigma_{\min}$, $\sigma_{\max}(1+\bar\delta)$, τ, the row bounds $e_{+,k}$ and e_{ccs};
  - $\bar e_{\text{norm}}$, that of Lemma G.73 at order 2α, $\sigma_{\min}$, $\sigma_{\max}(1+\bar\delta)$, τ, the row bounds $e_{+,k}$ and e_{ccs};
  - p_τ, that of Corollary 4.10, precondition 2, at $p_C^D = 0$;
  - $\mathfrak{L}_B$, $\mathfrak{L}_{\bar\delta}$, $\mathfrak{L}_\Delta$, $\mathfrak{L}_\Phi$ and A, those of Theorem 4.11, precondition 1, at $p_C^D = 0$.

Measured:

- $e_+ = 2^{-50.99}$ at $n = 512$ `verify/reports/fx/terms.py`;
- $e_+ = 2^{-50.99}$ at $n = 1024$ `verify/reports/fx/terms.py`;
- χ_{root} to $\mathfrak{L}_B$, every value `verify/reports/fx/terms.py` (Table 33);
- $\sigma_{\max}(1+\bar\delta) \le 1.778$ at $n = 512$ and $n = 1024$ `verify/reports/fx/terms.py`;
- $\varpi \le 2^{-77.22}$ at $n = 512$ and $n = 1024$ `verify/reports/fx/terms.py`;
- $\bar e_{\text{norm}} \le 2^{-51.04}$ at $n = 512$ and $n = 1024$ `verify/reports/fx/terms.py`;
- $\varepsilon_0^\circ < 1$ at $n = 512$ and $n = 1024$ `verify/reports/fx/terms.py`.

Lemma I.63 (The fixed-point signer as a Falcon-type signer [to table])**.** *The fixed-point signer is a Falcon-type signer.* ***Under Hypotheses I.21 and I.22****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Then

the signer is a Falcon-type signer at $(0, \zeta)$ *(Definition 4.5).*

Proof.

DEFINES $h = \log_2 n$, n the degree of the checked key

DEFINES $T = \mathrm{ffLDL}^\dagger(\mathcal{G})$ (Definition A.20), $\mathcal{G}$ the key's Gram matrix

DEFINES $q = 12289$ (Fact A.33)

DEFINES $L = 2^{64} \cdot 2^8$

DEFINES $\mathcal{N} = \bigcup_{2 \le m \le n/2} \mathrm{Sub}(T) \cap \mathcal{T}_m$, the nodes below the root

COMPUTES $\widetilde{g}_{00}$: the Gram's first entry, $\mathrm{ffSampling}^{\mathcal{F}}$ (Algorithm 10), line 3

COMPUTES $\widetilde{f}_{0,\nu}$, $\nu \in \mathcal{N}$: the first entry of the Gram $\mathrm{LDL}^\dagger$ (Algorithm 5) takes at ν, $\widetilde{\mathrm{split}}_{\mathrm{sa}}$ (Algorithm 3), line 4, on the diagonal of ν's parent

DEFINES $X = \{\widetilde{g}_{00}(\psi)\}_\psi \cup \{\widetilde{f}_{0,\nu}(\psi)\}_{\nu \in \mathcal{N}, \psi}$; W_x, $x \in X$, the word of x (Definition I.1)

DEFINES $\mathcal{K}$: the kernels' objects of Lemma I.10, items 1 to 13, and the object of `fxp_ffsamp_fft_inner` of Lemma I.11, item 3, at $\texttt{logn} = h$

DEFINES $\mathcal{C}$: the C functions of **Hypothesis I.21, items 1 and 2**, and of **Hypothesis I.22, item 1**

DEFINES $\mathrm{out}(o)$, $o \in \mathcal{K} \cup \mathcal{C}$: the words o returns on its input words

DEFINES $\mathrm{alg}(o)$, $o \in \mathcal{K} \cup \mathcal{C}$: the words the algorithm lines its item names compute in $\mathcal{F}_{\mathrm{fx}}$ on the same input words

(L1) $h \in \{9, 10\}$

[$n = 2^h$ (the proof's block); $n \in \{512, 1024\}$ (Definition 5.5, item 1) at the checked key]

(L2) $h \in [3, 10]$

[(L1)]

(L3) $\forall \mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n \ \forall k < n : \ \mathsf{h}(\mathsf{m})_{[k]} \in \{0, \ldots, 2^{16} - 1\}$

[Fact I.45, item 1, at every $\mathsf{h}(\mathsf{m})$ and the checked key's f, F (the statement)]

(L4) $\forall \mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n \ \forall j \in \{0, 1\} \ \forall k < n : \ qt_{\mathrm{frac},j,[k]} \in [-2^{15}, 2^{15})$

[Fact I.45, item 2, at every $\mathsf{h}(\mathsf{m})$ and the checked key's f, F (the statement)]

Lemma H.16, item 1 at the checked key and every root ψ	This proof

Shared: n, $\widetilde{g}_{00}$ ($\mathrm{ffSampling}^{\mathcal{F}}$ (Algorithm 10), line 3)

(I1)	
(f, g, F, G) key of degree $n = 2^h$	The checked key (the statement)
$\psi \in \Psi_n$	Every root ψ (the scope)
Assumption A1	Definition 5.5, item 2, at the checked key (the statement)
Assumption A2	Definition 5.5, item 3, at the checked key (the statement)
Its conclusion: $\widetilde{g}_{00} > 2^{-8}$	

(L5) $\forall \psi : \ \widetilde{g}_{00}(\psi) > 2^{-8}$

[(I1)]

(L6) $\Rightarrow \ \forall \psi : \ \widetilde{g}_{00}(\psi) > 0$

[(L5)]

Lemma I.40, (L2) at the diagonal $\widetilde{d}$ of the parent of every $\nu \in \mathcal{N}$	This proof

Shared: a, b, W_a, W_b (Lemma I.40 at $\widetilde{d}$)

(I2)	
$\widetilde{d}$	$\widetilde{d}$ (the scope)
$\widetilde{f}_0$	$\widetilde{f}_{0,\nu}$ (the proof's block)
$h \in \{2, \ldots, 10\}$	2^h the degree of the parent of $\nu \in \mathcal{N}$ (the proof's block)
Assumption A1	Theorem I.54, item 1
Assumption A2	Lemma I.43, item 2, at the checked key
Its conclusion: $\widetilde{f}_{0,\mathrm{fx64}} \ge 2^{64} 2^8 - 1/2$	

(L7) $\forall \nu \in \mathcal{N} \ \forall \psi : \ \widetilde{f}_{0,\nu}(\psi)_{\mathrm{fx64}} \ge L - 1/2$

[(I2)]

(L8) $L - 1/2 > 0$

[L (the proof's block)]

(L9) $\Rightarrow\ \forall \nu \in \mathcal{N}\ \forall \psi :\ \widetilde{f}_{0,\nu}(\psi) > 0$

[(L7), (L8); Definition A.5]

	Theorem I.54	This proof
	Shared: $(f, g, F, G), n, h$	
(I3)	W_x (f, g, F, G) checked key of degree $n \in \{512, 1024\}$ W_x a word of the listed families	$W_x,\ x \in X$ (the proof's block) The statement $\widetilde{g}_{00}$ (ffSampling$^{\mathcal{F}}$, line 3); $\widetilde{f}_{0,\nu}$ ($\widetilde{\text{split}}_{\text{sa}}$, line 4)
	Its item 1: $W_x = x_{\text{fx64}} \bmod 2^{128}$	
	Its item 2: $\lvert x \rvert < 2^{63}$	

(L10) $\forall x \in X :\ W_x = x_{\text{fx64}} \bmod 2^{128}$

[item 1 of (I3)]

(L11) $\forall x \in X :\ \lvert x \rvert < 2^{63}$

[item 2 of (I3)]

(L12) $\forall x \in X :\ \lvert x_{\text{fx64}} \rvert < 2^{127}$

[(L11); Definition A.5]

(L13) $\Rightarrow\ \forall x \in X :\ x_{\text{fx64}} \in (0, 2^{127})$

[(L6), (L9), (L12); Definition A.5]

(L14) $\Rightarrow\ \forall x \in X :\ W_x = x_{\text{fx64}}$

[(L10), (L13); Definition A.5]

(L15) $\Rightarrow\ \forall x \in X :\ W_x \neq 0$

[(L13), (L14)]

(L16) $\forall \psi :\ W_{\widetilde{g}_{00}(\psi)} \neq 0$

[(L15) at $x := \widetilde{g}_{00}(\psi)$]

(L17) $\forall \nu \in \mathcal{N} \setminus \mathcal{T}_2\ \forall \psi :\ W_{\widetilde{f}_{0,\nu}(\psi)} \neq 0$

[(L15) at $x := \widetilde{f}_{0,\nu}(\psi)$]

(L18) $\forall \nu \in \mathcal{N} \cap \mathcal{T}_2\ \forall \psi :\ W_{\widetilde{f}_{0,\nu}(\psi)} \neq 0$

[(L15) at $x := \widetilde{f}_{0,\nu}(\psi)$]

Lemma I.10 at `logn` $= h$	This proof
h	h (the proof's block)
$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
`g00`	$\widetilde{g}_{00}$, $\widetilde{f}_{0,\nu}$ (the proof's block)
$h \in \{2, \ldots, 10\}$	(L2)
each input array of words	The words of $\mathcal{K}$'s inputs (the proof's block; Definition A.5)
Assumption A1	(L2)
Assumption A2	(L16), (L17)
Assumption A3	(L16)

Its item 1: The object of `fxpoly_FFT` in $\mathcal{O}$ returns the words of lines 2 to 25 of $\widetilde{\text{FFT}}$
18374 (I4) (Algorithm 14).

Its item 2: The object of `fxpoly_split_fft` in $\mathcal{O}$ returns the words of lines 4 and 6 of $\widetilde{\text{split}}$ (Algorithm 2).

Its item 3: The object of `fxpoly_split_selfadj_fft` in $\mathcal{O}$ returns the words of lines 4 and 6 of $\widetilde{\text{split}}_{\text{sa}}$ (Algorithm 3).

Its item 4: The object of `fxpoly_merge_fft` in $\mathcal{O}$ returns the words of line 4 of $\widetilde{\text{merge}}$ (Algorithm 4) and of the sum and the difference after it.

Its item 5: The object of `fxpoly_LDL_fft` in $\mathcal{O}$ returns the words of lines 7 to 18 of $\text{LDL}^\dagger$ (Algorithm 5).

Its item 6: The object of `fxpoly_LDL_root_fft` in $\mathcal{O}$ returns the words of lines 7 to 12 of $\text{LDL}^\dagger$ and of line 6 of ffsamp (Algorithm 6).

Lemma I.10 at $\texttt{logn} = h$	This proof
h	h (the proof's block)
f	f, g, F, G (the statement)
$\mathcal{O}$	$\mathcal{O}$ (Lemma I.10)
$\texttt{g00}$	$\widetilde{f}_{0,\nu}$ (the proof's block)
$\texttt{hm}$	$\mathsf{h}(\mathsf{m})$ (L3)
$\texttt{qtfrac0}, \texttt{qtfrac1}$	$qt_{\mathrm{frac},0}, qt_{\mathrm{frac},1}$ ($\mathrm{center}_{\mathrm{frac}}$ (Algorithm 17), line 4)
$h \in \{2, \ldots, 10\}$	(L2)
each input array of words	The words of $\mathcal{K}$'s inputs (the proof's block; Definition A.5)
$f \in \{-128, \ldots, 127\}^{2^h}$	Definition 5.5, items 2 and 3
Assumption A4	(L18)
Assumption A5	(L2)
Assumption A6	(L3)
Assumption A7	(L4)
Assumption A8	(L2)

Its item 7: At a node of degree 2, the object of `fxp_ffsamp_fft` in $\mathcal{O}$ returns the words of lines 7 to 18 of $\mathrm{LDL}^{\dagger}$ and of lines 1 to 18 of deepest (Algorithm 7), each square root $\mathrm{fl}(\sqrt{x})$ of those lines the word $Q(W_x)$ on the word W_x of x, each call of SamplerZ (Algorithm 8) left opaque.

Its item 8: On their input words a and b at each of the 2^{h-1} roots, the objects of `fxpoly_mul_fft`, `fxpoly_add` and `fxpoly_sub` in $\mathcal{O}$ return $a \otimes b$, $a \oplus b$ and $a \ominus b$ (Definition A.8).

(I5)

Its item 9: On f, the object of `fxpoly_set_small` in $\mathcal{O}$ returns the words $W_{f_{[k]}} = f_{[k],\mathrm{fx64}} \bmod 2^{128}$.

Its item 10: On each of its 2^h input words W_a, the object of `fxpoly_neg` in $\mathcal{O}$ returns $-W_a \bmod 2^{128}$.

Its item 11: The object of `fxpoly_gram_fft` in $\mathcal{O}$ returns the words of lines 2 to 18 of Gram (Algorithm 13) at each of the 2^{h-1} roots. Its conjugates' imaginary parts are the words $0 - b_{10,i}$ and $0 - b_{11,i}$ of `fxp_neg`.

Its item 12: The two objects of the center's first computation in $\mathcal{O}$ return their algorithms' words.

- Each coefficient is loaded as the word $(0, \mathsf{h}(\mathsf{m})_{[k]})$.
- The harness's `memmove` copies 8-byte words.
- The object of `fxpoly_apply_basis` in $\mathcal{O}$ returns the words of lines 9, 16 and 18 of $\mathrm{ffSampling}^{\mathcal{F}}$ (Algorithm 10).
- Each residue is loaded as the word $(0, qt_{\mathrm{frac},j,[k]})$, sign-extended.
- The object of `fxpoly_target_fft` in $\mathcal{O}$ returns the words of lines 7 and 12 of $\mathrm{center}_{\mathrm{frac}}$ (Algorithm 17).

Its item 13: The object of `fxpoly_iFFT` in $\mathcal{O}$ writes, at each of its $h - 1$ stages [L0: `fxp/sign_fxpoly.c:52-75`], at each pair (x, y) of the stage and its twiddle's conjugate $\widetilde{s}$, the words of $x \oplus y$ and $(x \ominus y) \otimes \widetilde{s}$; then the word of $\mathrm{fl}(x/2^{h-1})$ at each of its 2^h words x [L0: `fxp/sign_fxpoly.c:76-80`].

	Lemma I.11 at `logn` $= h$	This proof
	h	h (the proof's block)
	`root`	1 (`fxp_ffsamp_fft`)
	`g00`	$\widetilde{g}_{00}$, $\widetilde{f}_{0,\nu}$ (the proof's block)
	$h \in \{2, \ldots, 10\}$	(L2)
	`root` $\in \{0, 1\}$	`root` $= 1$ (the scope)
(I6)	`tmp` an area of words	The words of $\mathcal{K}$'s inputs (the proof's block; Definition A.5)
	Assumption A1	(L16), (L17), (L18)

Its item 3: With each call the object of Lemma I.10, items 2, 3, 4, 5, 6 and 8, or of Lemmas I.3, I.4 and I.5, the object of `fxp_ffsamp_fft_inner` at `logn` $= h$ and `root` returns the words of ffsamp (Algorithm 6) in $\mathcal{F}_{\text{fx}}$ at `INV_SIGMA` $:= W_{\texttt{INV}}$ on every `tmp`, each square root $\text{fl}(\sqrt{x})$ of its lines the word $Q(W_x)$ on the word W_x of x, each call of SamplerZ (Algorithm 8) left opaque.

	Theorem I.54, item 1 at every word W_x the signer writes	This proof
	Shared: $(f, g, F, G), n, h,\ W_x$ (the scope)	
(I7)	(f, g, F, G) checked key of degree $n \in \{512, 1024\}$	The statement
	W_x a word of the listed families	The scope
	Its conclusion: $W_x = x_{\text{fx64}} \bmod 2^{128}$	

(L19) $\forall o \in \mathcal{K} :\ \text{out}(o) = \text{alg}(o)$

[items 1 to 6 of (I4); items 7 to 13 of (I5); item 3 of (I6); (I7); $\mathcal{K}$, out and alg (the proof's block)]

(L20) $\forall o \in \mathcal{C} :\ \text{out}(o) = \text{alg}(o)$

[**Hypothesis I.21, items 1 and 2**; **Hypothesis I.22, item 1**; $\mathcal{C}$, out and alg (the proof's block)]

(L21) $(u, \zeta) = (0, 2^{-64})$

[Definition I.1]

(L22) $u \in [0, 1)$

[(L21)]

(L23) the signer is a Falcon-type signer at $(0, \zeta)$

[Definition 4.5 at the checked key generation (keygen (Algorithm 11)) and ffSampling$^{\mathcal{F}}$ (Algorithm 10) in $\mathcal{F}_{\text{fx}}$; (L19), (L20), (L21), (L22)]

(L24) $\Rightarrow$ the statement

[(L23)]

□

I.5.2 The base sampler's inputs

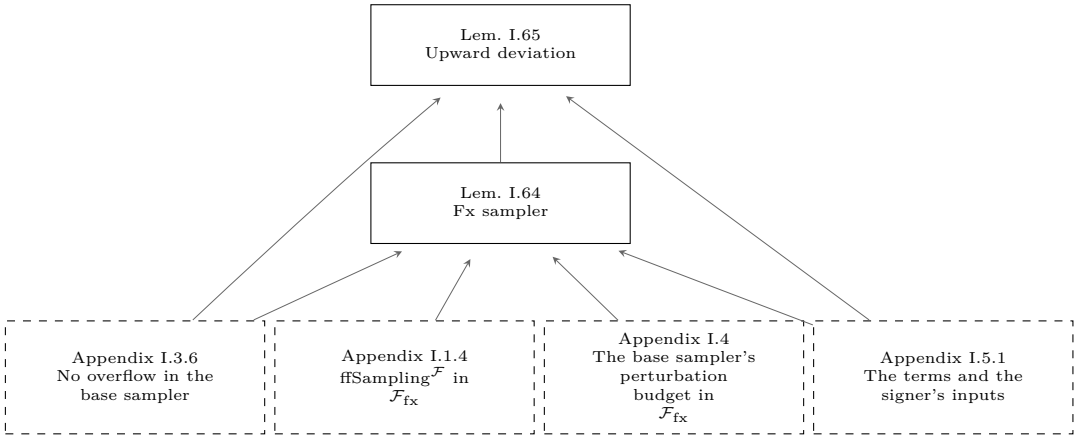


Figure 86: Dependencies, Appendix I.5.2.

Lemma I.64 (The fixed-point signer's base sampler inputs [to table])**.** *The base sampler's computed acceptance is within the row bounds of its exact one, its fringe sets are empty, and its computed scale lies in* $[1/2, 1)$*. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $z \in \mathbb{Z}$*, a value of* z *of* SamplerZ *(Algorithm 8), line 10;*
- $r \in \mathbb{R}$*, a value of* r *of line 3;*
- $\sigma > 0$*, a value of* $1/\texttt{isigma}$*,* `isigma` *the input of* SamplerZ*.*

Define:

- *The signer's words and parameters*
  - ζ_{op}*,* $\sigma_{\min}$ *and* ϵ_L*, those of Definition I.62;*
  - `LOG2` *and* `INV_LOG2`*, the stored* $\ln 2$ *and* $1/\ln 2$ *of* BerExp *(Algorithm 9);*
- *The exponent*
  - x *and* $\widetilde{x}$*, those of Lemma I.58 at a leaf;*
  - $k(z) := \bar{z}_0(z)$*, the row of* z *(Lemma G.64);*
- *The split*
  - $si := \text{trunc}(\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}))$ *(Lemma I.59 at* $y := \widetilde{x}$*);*
  - $\widetilde{r'} := \text{fl}(\widetilde{x} - \text{fl}(si \cdot \texttt{LOG2}))$ *(Lemma I.59 at* $y := \widetilde{x}$*);*
  - $r' := \max(\widetilde{r'}, 0)$ *(Lemma I.59 at* $y := \widetilde{x}$*);*
- *The acceptance*
  - *ccs, that of line 7 of* SamplerZ *(Algorithm 8);*
  - $\widetilde{ccs}$*, that of line 6;*
  - $y := \texttt{expm_p63}(r', \widetilde{ccs})/2^{63}$ *(Lemma H.25 at* $ccs := \widetilde{ccs}$*);*
  - $L := 0.6931471805599453095 + 2^{-30}$ *(Lemma H.25);*
  - $s_x := \min(si, 63)$ *(Fact G.66);*
  - $z_{\text{acc}} := ((\texttt{expm_p63}(r', \widetilde{ccs}) \ll 1) - 1) \gg s_x$ *(Fact G.66 at* $ccs := \widetilde{ccs}$*);*
  - $acc(z) := \widetilde{ccs}\, e^{-x(z)}$*;*
  - $\widetilde{acc}(z) := z_{\text{acc}}/2^{64}$*;*
  - $acc_c := \texttt{expm_p63}(r', \widetilde{ccs})/2^{63+s_x}$ *(Lemma H.26 at the signer's* si*,* r' *and* $ccs := \widetilde{ccs}$*);*
  - $e_{\text{ccs}} := 2\zeta_{\text{op}}$ *(Definition I.62);*
  - $e_{acc}(z) := \widetilde{acc}(z)/acc(z) - 1$*;*
  - $e_{\text{fl}}(z) := 2^{-63}/acc(z)$*;*
- *The row bounds*
  - $E_x := (1/(2\sigma_{\min}^2) + \frac{3}{2} \cdot 19.5^2 + 2)\zeta_{\text{op}} + \frac{3}{2}\zeta_{\text{op}}^2$ *(Definition I.62);*
  - $E_s := 66\zeta_{\text{op}} + 45|\epsilon_L|$ *(Definition I.62);*
  - $e_{\text{poly}} := 2^{-51.05}$ *(Definition I.62);*

– $e_+ := e^{E_x+E_s}(1+e_{\mathrm{poly}})-1$ *(Definition I.62);*

– $\forall k \le 18:\ E_{x,k} := (1/(2\sigma_{\min}^2)+\frac{3}{2}(k+1)^2+2)\zeta_{\mathrm{op}}+\frac{3}{2}\zeta_{\mathrm{op}}^2$ *(Definition I.62);*

– $\forall k \le 18:\ e_{+,k} := e^{E_{x,k}+E_s}(1+e_{\mathrm{poly}})-1$ *(Definition I.62).*

Measured:

- $(64-\zeta_{\mathrm{op}})/\texttt{INV_LOG2} - E_{x,18} - 63\ln 2 \ge 0.693$ *at* $n=512$ *and* $n=1024$*, at the stored words* ***verify/reports/fx/terms.py****;*
- $L - \max_{si\in\{0,63\}}((si+1+\zeta_{\mathrm{op}})/\texttt{INV_LOG2} - si\ln 2) - E_s \ge 2^{-30.01}$ *at the stored words* ***verify/reports/fx/terms.py****.*

Then

1. $\forall z:\ \widetilde{acc}(z)/acc(z) - 1 \le e_+$*;*
2. $C_i = \emptyset$*;*
3. $\bar{U}, \bar{p}_C, \kappa_C = 0$*;*
4. $\forall z:\ e_{acc}(z) \le e_{+,k(z)}$*;*
5. $\forall z:\ |e_{acc}(z)| \le e_{+,k(z)} + e_{\mathrm{fl}}(z)$*;*
6. $\widetilde{ccs} \in [1/2, 1)$*;*
7. $\widetilde{ccs} \ge (1-e_{\mathrm{ccs}})\,ccs$*.*

Proof.

DEFINES $N := 2n$ (Definition A.25)

DEFINES $\widetilde{\sigma}_i := 1/\texttt{isigma}$ at the i-th call of SamplerZ in ffSampling$^{\mathcal{F}}$ (Definition A.25)

DEFINES $\sigma_0 := 1.8205$ (Lemma I.51)

(L1) $\sigma \ge \sigma_{\min}$

[Lemma I.51, item 1, at the checked key (Definition I.62) and the leaf's `isigma`]

(L2) $\sigma \le \sigma_0$

[Lemma I.51, item 2, at the checked key (Definition I.62) and the leaf's `isigma`]

(L3) $\sigma_0 < 2\sigma_{\min}$

[[gate: `verify/gates/sampler/sigma_ccs.py`]]

(L4) $\widetilde{ccs} < 1$

[Lemma I.50 at the checked key (Definition I.62) and the leaf's `isigma`]

Lemma H.24	This proof
Shared: $\sigma,\ z, r,\ \sigma_{\min},\ dss$	
(I1) Assumption A1	(L1)
Its item 3: $dss \le 1/(2\sigma_{\min}^2)$	
Its item 1: $\lvert z-r\rvert \le 19.5$	

(L5) $dss \le 1/(2\sigma_{\min}^2)$

[item 3 of (I1)]

(L6) $|z-r| \le 19.5$

[item 1 of (I1)]

(L7) $|\widetilde{x}-x| \le E_x$

[(L5), (L6); Lemma I.58; E_x (Definition I.62)]

(L8) $\forall w \in \mathbb{R}:\ \mathrm{trunc}\, w > w - 1$

[$\mathrm{trunc}\, w = \mathrm{sgn}(w)\lfloor|w|\rfloor$ (Fact A.6, item 5); $\lfloor v\rfloor \in (v-1, v]$ (Fact A.41, item 22)]

	Lemma I.59, items 1 to 3 at $y := \widetilde{x}$, under the premise $\widetilde{x} \geq 0$ of (L9), (L12) and (L17)	This proof
	Shared: si, r', `INV_LOG2`, ζ_{op}	
	y	$\widetilde{x}$
18464 (I2)	$y \in \mathcal{F}_{\text{fx}}$	$\widetilde{x}$ (Lemma I.58)
	Assumption A1	$\widetilde{x} \geq 0$, the premise of (L9), (L12) and (L17)
	Its item 1: $\lvert(si \ln 2 + r') - y\rvert \leq (si+3)\zeta_{\text{op}} + y\lvert\epsilon_L\rvert$	
	Its item 2: $si \geq 0$	
	Its item 3: $\exists\, \zeta_g \in \mathbb{R},\ \lvert\zeta_g\rvert \leq \zeta_{\text{op}} :\ si = \text{trunc}(y\,\texttt{INV_LOG2} + \zeta_g)$	

18465 (L9) $\widetilde{x} \geq 0 \Rightarrow\ \widetilde{x} \cdot \texttt{INV_LOG2} < si + 1 + \zeta_{\text{op}}$

18466 [item 3 of (I2); (L8)]

18467 (L10) $\widetilde{x} \geq 0 \Rightarrow\ \widetilde{x} < (si + 1 + \zeta_{\text{op}})/\texttt{INV_LOG2}$

18468 [(L9); `INV_LOG2` > 0 (BerExp (Algorithm 9))]

18469 (L11) $si \leq 63 \wedge \widetilde{x} \geq 0 \Rightarrow\ \widetilde{x} \leq 45$

18470 [(L10) at $si \leq 63$; the stored `INV_LOG2` and ζ_{op} [gate: `verify/gates/fx/eplus_y.py`]]

18471 (L12) $si \leq 63 \wedge \widetilde{x} \geq 0 \Rightarrow\ \lvert(si \ln 2 + r') - \widetilde{x}\rvert \leq E_s$

18472 [item 1 of (I2); $si \leq 63$ and $\widetilde{x} \leq 45$ (L11); E_s (Definition I.62)]

18473 (L13) $si \leq 63 \wedge \widetilde{x} \geq 0 \Rightarrow\ r' \leq \widetilde{x} - si \ln 2 + E_s$

18474 [(L12)]

18475 (L14) $si \leq 63 \wedge \widetilde{x} \geq 0 \Rightarrow\ r' < (si + 1 + \zeta_{\text{op}})/\texttt{INV_LOG2} - si \ln 2 + E_s$

18476 [(L13), (L10)]

18477 (L15) $\max_{si \in \{0,63\}}\big((si + 1 + \zeta_{\text{op}})/\texttt{INV_LOG2} - si \ln 2\big) + E_s \leq L$

18478 [the second measured row; $2^{-30.01} > 0$ (Fact A.41, item 12)]

18479 (L16) $si \in [0, 63] \Rightarrow\ (si + 1 + \zeta_{\text{op}})/\texttt{INV_LOG2} - si \ln 2 + E_s \leq L$

18480 [(L15); Fact A.41, item 16, at $s := si$, $[a, b] := [0, 63]$]

18481 (L17) $si \leq 63 \wedge \widetilde{x} \geq 0 \Rightarrow\ r' \leq L$

18482 [(L14), (L16); item 2 of (I2)]

18483 (L18) $x \geq -k(z)^2\big(\widetilde{(1/(2\sigma_0^2))} - 1/(2\sigma_0^2)\big)$

18484 [(L2); $x = (z-r)^2\,\texttt{isigma}^2/2 - z_0^2 C_0$, $z = b + (2b-1)z_0$, $b \in \{0,1\}$, $r \in [0,1)$ (SamplerZ (Algorithm 8), lines 1 to 16); $\bar{z}_0(z) = z_0$ (Lemma G.64, item 1); $k(z) = \bar{z}_0(z)$ (the statement); $C_0 = \widetilde{(1/(2\sigma_0^2))}$ (SamplerZ, its input C_0; Definition I.20)]

18487 (L19) $\widetilde{x} < 0 \Rightarrow\ \lvert\widetilde{x}\rvert \leq E_x + k(z)^2\big(\widetilde{(1/(2\sigma_0^2))} - 1/(2\sigma_0^2)\big)$

18488 [(L7), (L18)]

18489 (L20) $\widetilde{x} < 0 \Rightarrow\ \lvert\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2})\rvert < 1$

18490 [(L19); Definition I.1, item 1; E_x (Definition I.62); $k(z) \leq 18$ (Lemma G.64, item 1; $z_0 \leq 18$, SamplerZ, line 9); Definition I.20: the stored $\widetilde{(1/(2\sigma_0^2))}$ [L0: `fxp/fxp_consts.h:2089`]; expand]

18492 (L21) $\widetilde{x} < 0 \Rightarrow\ si = 0$

18493 [(L20); $\forall v,\ \lvert v\rvert < 1 :\ \text{trunc}\, v = 0$ (Fact A.6, item 5); si (Lemma I.59)]

18494 (L22) $\widetilde{x} < 0 \Rightarrow\ \widetilde{r'} = \widetilde{x}$

18495 [(L21); $\widetilde{r'}$ of Lemma I.59 [L0: `fxp/sign_fxsampler.c:152-162`]; $\text{fl}(0) = 0$ (Fact A.6, item 9);

18496 $\text{fl}(\widetilde{x} - 0) = \widetilde{x} - 0$ (Fact A.6, item 8)]

18497 (L23) $\widetilde{x} < 0 \Rightarrow\ r' = 0$

18498 [(L22); $r' = \max(\widetilde{r'}, 0)$ (Lemma I.59)]

18499 (L24) $si \leq 63 \Rightarrow\ r' \in [0, L]$

18500 [(L17), (L23); $\max(\widetilde{r'}, 0) \geq 0$ (Fact A.41, item 20)]

18501 (L25) $\sigma \in [\sigma_{\min}, 2\sigma_{\min}]$

18502 [(L1), (L2), (L3)]

Lemma I.60 under $si \le 63$	This proof
Shared: $\texttt{isigma}, \sigma,\ r', \widetilde{ccs},\ \texttt{expm_p63},\ L, \sigma_{\min}$	
y	y (Lemma I.60, (L2); y, the statement)
(I3)	
Assumption A1	(L25)
Assumption A2	(L24)
Assumption A3	(L4)
Its conclusion: $\lvert y/(e^{-r'}\widetilde{ccs}) - 1\rvert \le 2^{-51.05}$	

(L26) $si \le 63 \Rightarrow\ y \le \widetilde{ccs}\, e^{-r'}(1 + e_{\text{poly}})$

[(I3); e_{poly} (Definition I.62)]

(L27) $ccs = \sigma_{\min}/\sigma$

[SamplerZ, line 7]

(L28) $ccs > 1/2$

[(L27), (L2), (L3)]

(L29) $\exists\, \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \le \zeta_{\text{op}} :\ \widetilde{ccs} = ccs + \zeta_\circ$

[SamplerZ, line 6; Definition I.1, item 1]

(L30) $\widetilde{ccs} \ge 1/2$

[(L28); SamplerZ, line 6; $\forall a, b \in \mathbb{R},\ a \le b :\ \text{fl}(a) \le \text{fl}(b)$ (Fact A.6, item 9); $\text{fl}(1/2) = 1/2$ ($1/2 \in \mathcal{F}_{\text{fx}}$, Definition I.1)]

(L31) $\widetilde{ccs} \in [1/2, 1)$

[(L30), (L4)]

(L32) $si \le 63 \Rightarrow\ y \ge \widetilde{ccs}\, e^{-r'}(1 - e_{\text{poly}})$

[(I3); e_{poly} (Definition I.62)]

(L33) $si \le 63 \Rightarrow\ y \ge \widetilde{ccs}\, e^{-L}(1 - e_{\text{poly}})$

[(L32); $r' \le L$ (L24); $t \mapsto e^{-t}$ nonincreasing (Fact A.41, item 5); $\widetilde{ccs} \ge 1/2$ (L30); $e_{\text{poly}} < 1$ (e_{poly}, Definition I.62); Fact A.41, item 8]

(L34) $si \le 63 \Rightarrow\ y \ge e^{-L}(1 - e_{\text{poly}})/2$

[(L33); $\widetilde{ccs} \ge 1/2$ (L30); $e^{-L} > 0$ (Fact A.41, item 12); $e_{\text{poly}} < 1$ (e_{poly}, Definition I.62); Fact A.41, item 8]

(L35) $2^{63} e^{-L}(1 - e_{\text{poly}})/2 \ge 1$

[L and e_{poly} (the statement); expand]

(L36) $si \le 63 \Rightarrow\ \texttt{expm_p63}(r', \widetilde{ccs}) \ge 1$

[(L34), (L35); $y = \texttt{expm_p63}(r', \widetilde{ccs})/2^{63}$ (y, the statement); Fact A.41, item 26, at $c := 2^{63}$]

Lemma I.61	This proof
Shared: $si,\ r', \widetilde{ccs},\ acc_c, \widetilde{acc}_c, z_{\text{acc}}$	
y	$\widetilde{x}$ (the statement)
$y \in \mathcal{F}_{\text{fx}}$	$\widetilde{x}$ (Lemma I.58)
(I4)	
Assumption A1	$si \le 63$, the premise of (L37); $si \ge 0$ by item 2 of (I2) at $\widetilde{x} \ge 0$ and by (L21) at $\widetilde{x} < 0$
Assumption A2	(L36) at $si \le 63$, the premise of (L37)
Its conclusion: $\widetilde{acc}_c/acc_c - 1 \in \left[-2 \cdot 2^{-64}/acc_c,\ 0\right]$	

(L37) $si \le 63 \Rightarrow\ \widetilde{acc} \le acc_c$

[(I4); $\widetilde{acc} = \widetilde{acc}_c$ (Lemma H.26)]

		Lemma H.26, item 3 at the computed si, r' and $ccs := \widetilde{ccs}$, under the premise of (L38)	This proof
		Shared: $s_x, z_{\mathrm{acc}},\ acc_c, \widetilde{acc}_c$	
18531	(I5)	si r' ccs	si (the statement) r' (the statement) $\widetilde{ccs}$ (the statement)
		Assumption A1 Assumption A2 Assumption A4	Item 2 of (I2) at $\widetilde{x} \geq 0$; (L21) at $\widetilde{x} < 0$ (L36) at $si \leq 63$, the premise of (L38) The premise of (L38)
		Its conclusion: $acc_c = \texttt{expm_p63}(r', ccs)/2^{63+si}$	
18532	(L38)	$si \leq 63 \Rightarrow\ acc_c = \texttt{expm_p63}(r', \widetilde{ccs})/2^{63+si}$	
18533			[(I5)]
18534	(L39)	$\texttt{expm_p63}(r', \widetilde{ccs})/2^{63} = y$	
18535			[y (the statement)]
18536	(L40)	$si \leq 63 \Rightarrow\ \widetilde{acc} \leq y\, 2^{-si}$	
18537			[(L37), (L38), (L39)]
18538	(L41)	$si \geq 64 \Rightarrow\ \widetilde{acc} = 0$	
18539			[Definition I.20, item 1; $\widetilde{acc} = z_{\mathrm{acc}}/2^{64}$ (the statement)]
18540	(L42)	$\Rightarrow$ item 6	
18541			[(L31)]
18542	(L43)	$\widetilde{ccs} \geq (1 - 2\zeta_{\mathrm{op}})\, ccs$	
18543			[(L28), (L29)]
18544	(L44)	$\Rightarrow$ item 7	
18545			[(L43); e_{ccs} (the statement)]
18546	(L45)	$\forall i \leq N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$	
18547		[Lemma I.51, item 1, at the checked key (Definition I.62) and every leaf's `isigma`; $\widetilde{\sigma}_i$ (the proof's block)]	
18548	(L46)	$\forall i \leq N\ \forall z_{<i} :\ \widetilde{\sigma}_i \leq \sigma_0$	
18549		[Lemma I.51, item 2, at the checked key (Definition I.62) and every leaf's `isigma`; $\widetilde{\sigma}_i$ (the proof's block)]	
18550	(L47)	$\Rightarrow\ \forall i \leq N\ \forall z_{<i} :\ \widetilde{\sigma}_i \in [\sigma_{\min}, \sigma_0]$	
18551			[(L45), (L46)]
		Lemma G.80, items 1 to 4	This proof
		the signer a Falcon-type signer whose BerExp executes line 15	The signer of Definition I.20, item 1
		Assumption A1	(L47)
18552	(I6)	Its item 1: $\forall i \leq N :\ C_i = \emptyset$	
		Its item 2: $\bar{U} = 0$	
		Its item 3: $\bar{p}_C = 0$	
		Its item 4: $\kappa_C = 0$	
18553	(L48)	$C_i = \emptyset$	
18554			[item 1 of (I6)]
18555	(L49)	$\Rightarrow$ item 2	
18556			[(L48)]
18557	(L50)	$\bar{U}, \bar{p}_C, \kappa_C = 0$	
18558			[items 2, 3 and 4 of (I6)]
18559	(L51)	$\Rightarrow$ item 3	
18560			[(L50)]
18561	(L52)	$\lvert z - r \rvert \leq k(z) + 1$	

$[k(z) = \bar{z}_0(z)$ (the statement); $\bar{z}_0(z) := |z - [z > 0]|$ (Lemma G.64); $r \in [0, 1)$ (SamplerZ, line 3)]

(L53) $k(z) \le 18$

[Lemma G.64, item 1; $z_0 \le 18$ (SamplerZ, line 9)]

(L54) $\forall z :\ |\widetilde{x} - x| \le E_{x,k(z)}$

[(L5), (L52), (L53); Lemma I.58; $E_{x,k}$ (Definition I.62)]

(L55) $si \le 63 \Rightarrow\ \widetilde{acc} \ge y\, 2^{-si} - 2 \cdot 2^{-64}$

[(I4); (L38), (L39); $\widetilde{acc} = \widetilde{acc}_c$ (Lemma H.26)]

(L56) $\widetilde{x} < 0 \Rightarrow\ r' + si \ln 2 = 0$

[(L21), (L23)]

(L57) $\widetilde{x} < 0 \Rightarrow\ x < E_{x,k(z)}$

[(L54)]

(L58) $si \le 63 \wedge \widetilde{x} \ge 0 \Rightarrow\ r' + si \ln 2 \ge x - E_{x,k(z)} - E_s$

[(L12), (L54)]

(L59) $si \le 63 \Rightarrow\ r' + si \ln 2 \ge x - E_{x,k(z)} - E_s$

[(L56), (L57), (L58); $E_s \ge 0$ (E_s, Definition I.62)]

(L60) $si \le 63 \wedge \widetilde{x} \ge 0 \Rightarrow\ r' + si \ln 2 \le x + E_{x,k(z)} + E_s$

[(L12), (L54)]

(L61) $si \le 63 \Rightarrow\ r' + si \ln 2 \le x + E_{x,k(z)} + E_s$

[(L60), (L56), (L18); $k(z)^2\big(\widetilde{(1/(2\sigma_0^2))} - 1/(2\sigma_0^2)\big) \le E_{x,k(z)}$ ($E_{x,k}$, Definition I.62; Definition I.20: the stored $\widetilde{(1/(2\sigma_0^2))}$; expand); $E_s \ge 0$ (E_s, Definition I.62)]

(L62) $si \le 63 \Rightarrow\ \widetilde{acc} \le \widetilde{ccs}\, e^{-r'}(1 + e_{\text{poly}})2^{-si}$

[(L26), (L40)]

(L63) $\Rightarrow\ si \le 63 \Rightarrow\ \widetilde{acc} \le \widetilde{ccs}\, e^{-(r' + si \ln 2)}(1 + e_{\text{poly}})$

[(L62); $2^{-si} = e^{-si \ln 2}$ (Fact A.41, item 12)]

(L64) $\Rightarrow\ si \le 63 \Rightarrow\ \widetilde{acc} \le \widetilde{ccs}\, e^{-x} e^{E_{x,k(z)} + E_s}(1 + e_{\text{poly}})$

[(L63), (L59); $t \mapsto e^{-t}$ nonincreasing (Fact A.41, item 5); (L31); $e_{\text{poly}} \ge 0$ (e_{poly}, Definition I.62)]

(L65) $\Rightarrow\ si \le 63 \Rightarrow\ e_{acc} \le e^{E_{x,k(z)} + E_s}(1 + e_{\text{poly}}) - 1$

[(L64); acc and e_{acc} (the statement)]

(L66) $\forall k \le 18 :\ e^{E_{x,k} + E_s}(1 + e_{\text{poly}}) - 1 = e_{+,k}$

[$e_{+,k}$ (Definition I.62)]

(L67) $si \le 63 \Rightarrow\ \widetilde{acc} \ge \widetilde{ccs}\, e^{-r'}(1 - e_{\text{poly}})2^{-si} - 2 \cdot 2^{-64}$

[(L32), (L55); $2^{-si} > 0$ (Fact A.41, item 12)]

(L68) $\Rightarrow\ si \le 63 \Rightarrow\ \widetilde{acc} \ge \widetilde{ccs}\, e^{-(r' + si \ln 2)}(1 - e_{\text{poly}}) - 2 \cdot 2^{-64}$

[(L67); $2^{-si} = e^{-si \ln 2}$ (Fact A.41, item 12)]

(L69) $\Rightarrow\ si \le 63 \Rightarrow\ \widetilde{acc} \ge \widetilde{ccs}\, e^{-x} e^{-(E_{x,k(z)} + E_s)}(1 - e_{\text{poly}}) - 2 \cdot 2^{-64}$

[(L68), (L61); $t \mapsto e^{-t}$ nonincreasing (Fact A.41, item 5); (L31); $e_{\text{poly}} < 1$ (e_{poly}, Definition I.62)]

(L70) $\Rightarrow\ si \le 63 \Rightarrow\ e_{acc} \ge e^{-(E_{x,k(z)} + E_s)}(1 - e_{\text{poly}}) - 1 - e_{\text{fl}}(z)$

[(L69); acc, e_{acc} and e_{fl} (the statement)]

(L71) $\Rightarrow\ si \le 63 \Rightarrow\ e_{acc} \in [e^{-(E_{x,k} + E_s)}(1 - e_{\text{poly}}) - 1 - e_{\text{fl}}, e_{+,k}],\ k := k(z)$

[(L65), (L66) at $k := k(z)$, $k(z) \le 18$ by (L53); (L70)]

(L72) $\Rightarrow\ si \le 63 \Rightarrow\ e_{acc} \in [-e_{+,k} - e_{\text{fl}}, e_{+,k}]$

[(L71); $1 - e^{-E}(1 - p) \le e^E(1 + p) - 1$ at $E, p \ge 0$ (Fact A.41, item 21)]

(L73) $si \ge 64 \Rightarrow\ \text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}) \ge 64$

[$si = \text{trunc}(\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}))$ (Lemma I.59); Fact A.6, item 5; $\lfloor \cdot \rfloor$ (Fact A.41, item 22)]

(L74) $si \ge 64 \Rightarrow\ \widetilde{x} \cdot \texttt{INV_LOG2} \ge 64 - \zeta_{\text{op}}$

[(L73); Definition I.1, item 1]

(L75) $si \ge 64 \Rightarrow\ x \ge 63 \ln 2$

[(L74), (L54), (L53); $E_{x,k} \le E_{x,18}$ (Definition I.62); the first measured row]

(L76) $si \ge 64 \Rightarrow\ e_{\text{fl}} \ge 1$

[(L75), (L4); $acc = \widetilde{ccs}\, e^{-x}$, $e_{\text{fl}} = 2^{-63}/acc$ (the statement)]

(L77) $\Rightarrow\ si \geq 64 \Rightarrow\ e_{acc} = -1$

[(L41)]

(L78) $si \geq 64 \Rightarrow\ -1 \in [-e_{+,k} - e_{\mathrm{fl}},\ e_{+,k}]$

[(L76); $e_{+,k} \geq 0$ ($E_{x,k}, E_s, e_{\mathrm{poly}} \geq 0$, Definition I.62)]

(L79) $\Rightarrow\ si \geq 64 \Rightarrow\ e_{acc} \in [-e_{+,k} - e_{\mathrm{fl}},\ e_{+,k}]$

[(L77), (L78)]

(L80) $\forall k \leq 18 :\ (k+1)^2 \leq 19.5^2$

[expand]

(L81) $\forall k \leq 18 :\ E_{x,k} \leq E_x$

[(L80); $E_{x,k}$, E_x (Definition I.62); Fact A.41, item 26]

(L82) $si \leq 63 \Rightarrow\ e_{acc} \leq e^{E_x+E_s}(1+e_{\mathrm{poly}}) - 1$

[(L65), (L53), (L81); $t \mapsto e^t$ nondecreasing (Fact A.41, item 5); $e_{\mathrm{poly}} \geq 0$ (e_{poly}, Definition I.62)]

(L83) $e^{E_x+E_s}(1+e_{\mathrm{poly}}) - 1 = e_+$

[e_+ (Definition I.62)]

(L84) $e_+ \geq 0$

[e_+, E_x, E_s and e_{poly} (Definition I.62); $e^x \geq 1$ at $x \geq 0$ (Fact A.41, item 27)]

(L85) $si \geq 64 \Rightarrow\ e_{acc} \leq e_+$

[(L77), (L84)]

(L86) $\forall z :\ \widetilde{acc}(z)/acc(z) - 1 \leq e_+$

[(L82), (L83), (L85); e_{acc} (the statement)]

(L87) $\Rightarrow$ item 1

[(L86)]

(L88) $\Rightarrow$ item 4

[(L72), (L79)]

(L89) $\Rightarrow$ item 5

[(L72), (L79)]

□ (items 1 to 7)

Lemma I.65 (The fixed-point base sampler's upward deviation [to table])**.** *At every leaf, the fixed-point base sampler's probability of each integer is at most* $1+\epsilon_{\mathrm{hi}}$ *times the computed Gaussian's. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The signer's words and parameters*
  - $\sigma_{\min}$, $e_{+,k}$ *and* e_{ccs}, *those of Definition I.62;*
  - $\sigma_0 := 1.8205$ *(Lemma G.64);*
  - $N := 2n$ *(Definition A.25);*
- *The leaves*
  - $\widetilde{\sigma}_i$ *and* $\widetilde{t}_i$, *those of Definition A.25 at the key;*
  - $\widetilde{B}_i$ *and* $\widetilde{D}_i$, *those of Definition A.28 at the signer's base sampler;*
- *The table*
  - w_k, ϖ *and* ϵ_k^+, *those of Lemma G.70 at* $\sigma_{\min}$ *and* $\sigma_{\max} := \sigma_0$;
- *The acceptance*
  - $\bar{e}_{\mathrm{norm}}$, *that of Lemma G.72 at* $\sigma_{\min}$, $\sigma_{\max} := \sigma_0$, $e_{+,k}$ *and* e_{ccs};
  - $\epsilon_{\mathrm{hi}} := 4.519 \cdot 10^{-3}$.

Measured [gate: `verify/gates/sampler/eps_hi.py`]:

- $\varpi < 1$ *at* $n \in \{512, 1024\}$;
- $\bar{e}_{\mathrm{norm}} < 1$ *at* $n \in \{512, 1024\}$;
- $\max_{k \leq 18}\big((1+\epsilon_k^+)(1+e_{+,k})/(1-\bar{e}_{\mathrm{norm}}) - 1\big) \leq \epsilon_{\mathrm{hi}}$ *at* $n \in \{512, 1024\}$.

Then

$$\forall i \le N\ \forall z_{<i}\ \forall z_i \in \mathbb{Z}:\ \widetilde{B}_i(z_i) \le (1+\epsilon_{\text{hi}})\,\widetilde{D}_i(z_i).$$

Proof.

DEFINES $\widetilde{D}$, P_0, ϵ, ϵ_{tab} and ϵ_{ar}, those of Lemma G.67 at $(\widetilde{\sigma},\widetilde{t}) := (\widetilde{\sigma}_i,\widetilde{t}_i)$, at each $i \le N$ and $z_{<i}$

$k(y)$ and V_k, those of Lemma G.70 at $(\widetilde{\sigma},\widetilde{t}) := (\widetilde{\sigma}_i,\widetilde{t}_i)$

(L1) $\forall i \le N\ \forall z_{<i}:\ \widetilde{\sigma}_i \in [\sigma_{\min},\sigma_0]$

[Lemma I.51, items 1 and 2, at the checked key and every leaf's `isigma`; $\widetilde{\sigma}_i = 1/$`isigma` (Definition A.25)]

Lemma G.67, item 1 at every $i \le N$ and $z_{<i}$	This proof
Shared: $\sigma_{\min},\ \sigma_0,\ \widetilde{D}, P_0, \epsilon, \epsilon_{\text{tab}}, \epsilon_{\text{ar}}$ (the proof's block)	
$\widetilde{\sigma},\widetilde{t}$	$\widetilde{\sigma}_i,\widetilde{t}_i$ (the statement)
(I1) α	2
$\alpha \ge 2$	$2 \ge 2$
$\sigma_{\min} > 0$	$\sigma_{\min}$, the stored word [L0: `fxp/fxp_consts.h:2073-2084`]
$\widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R}$	(L1); $\widetilde{t}_i$ (Definition A.25)
Assumption A1	(L1)
Its item 1: $\forall y:\ \epsilon = \epsilon_{\text{tab}} + \epsilon_{\text{ar}}(1+\epsilon_{\text{tab}})$	

(L2) $\forall i \le N\ \forall z_{<i}\ \forall y \in \mathbb{Z}:\ 1+\epsilon(y) = (1+\epsilon_{\text{tab}}(y))(1+\epsilon_{\text{ar}}(y))$

[item 1 of (I1); expand]

Lemma G.70 at every $i \le N$ and $z_{<i}$	This proof
Shared: $\sigma_{\min},\ \sigma_0,\ w_k, \varpi, \epsilon_k^+$ (the statement), $\widetilde{D}, P_0, \epsilon_{\text{tab}}, k(y), V_k$ (the proof's block)	
$\sigma_{\max}$	σ_0 (the statement)
$\widetilde{\sigma},\widetilde{t}$	$\widetilde{\sigma}_i,\widetilde{t}_i$ (the statement)
$\sigma_{\min} > 0$	$\sigma_{\min}$, the stored word [L0: `fxp/fxp_consts.h:2073-2084`]
(I2) $\sigma_{\max} \in [\sigma_{\min},\sigma_0]$	(L1)
$\widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R}$	(L1); $\widetilde{t}_i$ (Definition A.25)
Assumption A1	(L1)
Assumption A2	The first measured row
Its item 1: $\forall k \ge 0\ \forall y \in V_k:\ \epsilon_{\text{tab}}(y) \in [\epsilon_k^-,\epsilon_k^+]$	
Its item 4: $\forall y,\ k(y) \ge 19:\ P_0(y) = 0$	

(L3) $\forall i \le N\ \forall z_{<i}\ \forall k \le 18\ \forall y \in V_k:\ 1+\epsilon_{\text{tab}}(y) \le 1+\epsilon_k^+$

[item 1 of (I2)]

(L4) $\forall i \le N\ \forall z_{<i}\ \forall y \in \mathbb{Z}:\ 1+\epsilon_{\text{tab}}(y) \ge 0$

[$1+\epsilon_{\text{tab}} = P_0/\widetilde{D}$ (ϵ_{tab}, the proof's block); P_0, a probability measure (Lemma G.64); $\widetilde{D} > 0$ ($\widetilde{D} = D_{\mathbb{Z},\widetilde{\sigma}_i,\widetilde{t}_i}$, Definition A.2, items 2 and 1; Fact A.41, item 12)]

(L5) $\forall i \le N\ \forall z_{<i}\ \forall y \in \mathbb{Z},\ k(y) \ge 19:\ 1+\epsilon_{\text{tab}}(y) = 0$

[item 4 of (I2); $1+\epsilon_{\text{tab}} = P_0/\widetilde{D}$ (ϵ_{tab}, the proof's block)]

Lemma G.72, item 3 at every $i \le N$ and $z_{<i}$	This proof
Shared: $\sigma_{\min},\ \sigma_0,\ e_{+,k}, e_{\mathrm{ccs}}, \varpi, \bar{e}_{\mathrm{norm}}$ (the statement), $P_0, \epsilon_{\mathrm{ar}}, k(y)$ (the proof's block)	
$\sigma_{\max}$	σ_0 (the statement)
$\widetilde{\sigma}, \widetilde{t}$	$\widetilde{\sigma}_i, \widetilde{t}_i$ (the statement)
$\mathcal{Y}$	$\mathbb{Z}$
$\sigma_{\min} > 0$	$\sigma_{\min}$, the stored word [L0: `fxp/fxp_consts.h:2073-2084`]
$\sigma_{\max} \in [\sigma_{\min}, \sigma_0]$	(L1)
$\widetilde{\sigma} > 0,\ \widetilde{t} \in \mathbb{R}$	(L1); $\widetilde{t}_i$ (Definition A.25)
$\forall k \le 18 :\ e_{+,k} \ge 0$	$e_{+,k}$, $E_{x,k}$, E_s and e_{poly} (Definition I.62); $e^x \ge 1$ at $x \ge 0$ (Fact A.41, item 27)
(I3)	
$e_{\mathrm{ccs}} \in [0, 1)$	$e_{\mathrm{ccs}} := 2\zeta_{\mathrm{op}}$ (Definition I.62)
$\mathcal{Y} \subseteq \mathbb{Z}$	$\mathbb{Z}$
Assumption A1	(L1)
Assumption A2	Lemma I.64, item 7, at the leaf's `isigma`; $ccs = \sigma_{\min}/\widetilde{\sigma}_i$ (SamplerZ (Algorithm 8), line 7)
Assumption A3	The first measured row
Assumption A4	The second measured row
Assumption A5	Lemma I.64, item 5, at the leaf's `isigma`
Assumption A6	Lemma I.64, item 4, at the leaf's `isigma`
Its item 3: $\forall y \in \mathcal{Y} \cap \mathrm{Supp}(P_0) :\ \epsilon_{\mathrm{ar},+}(y) \le (e_{+,k(y)} + \bar{e}_{\mathrm{norm}})/(1 - \bar{e}_{\mathrm{norm}})$	

(L6) $\forall i \le N\ \forall z_{<i}\ \forall y \in \mathrm{Supp}(P_0),\ k(y) \le 18 :\ 1 + \epsilon_{\mathrm{ar}}(y) \le (1 + e_{+,k(y)})/(1 - \bar{e}_{\mathrm{norm}})$

[item 3 of (I3); $x \le \max(x, 0)$ (Fact A.41, item 20); expand]

(L7) $\forall i \le N\ \forall z_{<i}\ \forall y \notin \mathrm{Supp}(P_0) :\ 1 + \epsilon_{\mathrm{ar}}(y) = 1$

[ϵ_{ar} (the proof's block)]

(L8) $\forall k \le 18 :\ (1 + e_{+,k})/(1 - \bar{e}_{\mathrm{norm}}) \ge 1$

[$e_{+,k} \ge 0$ ((I3)); $\bar{e}_{\mathrm{norm}} \ge 0$ ($\bar{e}_{\mathrm{norm}}$, Lemma G.72); the second measured row]

(L9) $\forall i \le N\ \forall z_{<i}\ \forall y \in \mathbb{Z} :\ 1 + \epsilon_{\mathrm{ar}}(y) \ge 0$

[(L7); $1 + \epsilon_{\mathrm{ar}} = \widetilde{B}/P_0$ on $\mathrm{Supp}(P_0)$ (ϵ_{ar}, the proof's block); $\widetilde{B}$, a probability measure (Lemma G.67)]

(L10) $\forall k \le 18 :\ (1 + \epsilon_k^+)(1 + e_{+,k})/(1 - \bar{e}_{\mathrm{norm}}) \le 1 + \epsilon_{\mathrm{hi}}$

[the third measured row]

(L11) $\forall i \le N\ \forall z_{<i}\ \forall y \in \mathbb{Z},\ k(y) \le 18 :\ 1 + \epsilon(y) \le 1 + \epsilon_{\mathrm{hi}}$

[(L2); (L3), (L4) at $k := k(y)$, $y \in V_{k(y)}$ (V_k, the proof's block); (L6), (L7), (L8), (L9); (L10); Fact A.41, item 8]

(L12) $\forall i \le N\ \forall z_{<i}\ \forall y \in \mathbb{Z},\ k(y) \ge 19 :\ 1 + \epsilon(y) = 0$

[(L2), (L5)]

(L13) $\epsilon_{\mathrm{hi}} \ge 0$

[ϵ_{hi} (the statement)]

(L14) $\Rightarrow\ \forall i \le N\ \forall z_{<i}\ \forall y \in \mathbb{Z} :\ 1 + \epsilon(y) \le 1 + \epsilon_{\mathrm{hi}}$

[(L11), (L12), (L13)]

(L15) $\Rightarrow\ \forall i \le N\ \forall z_{<i}\ \forall z_i \in \mathbb{Z} :\ \widetilde{B}_i(z_i) \le (1 + \epsilon_{\mathrm{hi}})\, \widetilde{D}_i(z_i)$

[(L14) at $y := z_i$; $1 + \epsilon = \widetilde{B}/\widetilde{D}$ (ϵ, the proof's block); $\widetilde{D} > 0$ (as at (L4)); $\widetilde{B}_i$ and $\widetilde{D}_i$, the base sampler's and the Gaussian's at $(\widetilde{\sigma}_i, \widetilde{t}_i)$ (Definition A.28)]

(L16) $\Rightarrow$ the statement

[(L15)]

□

I.5.3 The preconditions

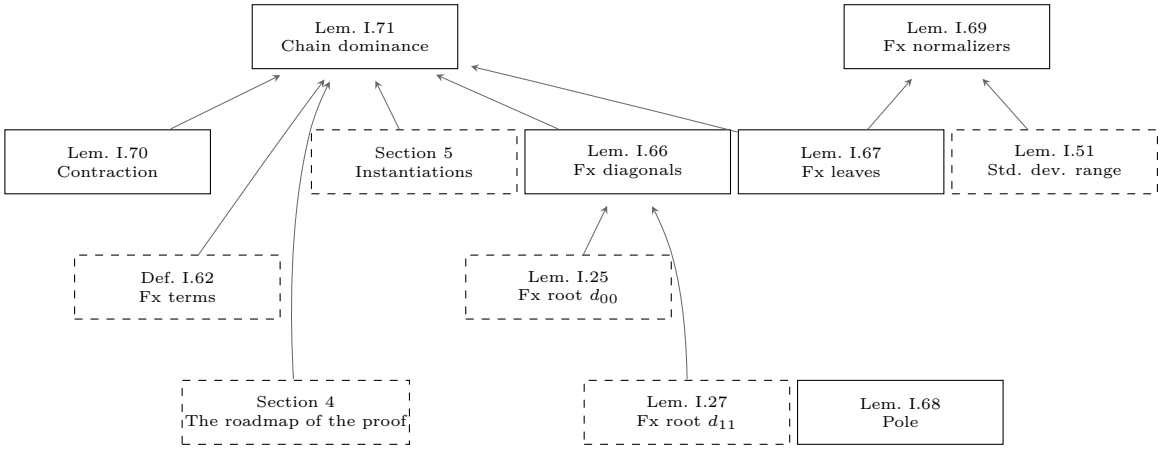


Figure 87: Dependencies, Appendix I.5.3.

Lemma I.66 (The fixed-point signer's diagonal preconditions [to table])**.** *The root's relative bound of Definition I.62 meets the theorem's root diagonal precondition, and the root's first relative bound is below* 1*. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The key bounds*
  - h, d_{lo}, d_{hi}, $\bar{\kappa}_k$ *and* $\bar{G}$*, those of Definition I.62;*
  - m_0 *and* M_0*, those of Proposition 5.8;*
  - E_{00}*, that of Definition A.36, item 5;*
- *The node bounds*
  - $\forall \chi \in [0,1):\ m_1(\chi) := d_{\mathrm{lo}}(1-\chi)$ *(Definition I.28);*
  - $\forall \chi \in [0,1):\ u_0(\chi) := \zeta/(2m_1(\chi))$ *(Definition I.28);*
  - $\mathcal{U}^0_\kappa$*, the node map of Definition I.28 at* d_{lo} *and* d_{hi}*;*
  - $\mathcal{A} := \{\chi : 0 \le \chi < 1,\ u_0(\chi) < 1\}$ *(Definition I.32);*
- *The error chain*
  - $e_{00} := E_{00}/m_0$ *(Lemma I.25);*
  - $Z_I := 1 + \zeta\bar{G}/q^2$ *(Lemmas I.26 and I.27 at* $\bar{G}$*);*
  - $\chi_{\mathrm{root}} := \max(e_{00},\ Z_I/(1-e_{00}) - 1)$ *(Definition I.62);*
  - $\forall 1 \le k \le h-1:\ \vartheta_{k-1} := (1+\chi_{k-1})/(1-\chi_{k-1})$ *(Definition I.32);*
  - $\forall 1 \le k \le h-1:\ \hat{\kappa}_k := \vartheta_{k-1}\bar{\kappa}_k + (\vartheta_{k-1}-1)/2$ *(Definition I.32 at* $\kappa_k := \bar{\kappa}_k$*);*
  - $\chi_0 := \chi_{\mathrm{root}}$ *(Definition I.32);*
  - $\forall 1 \le k \le h-1:\ \chi_k := \mathcal{U}^0_{\hat{\kappa}_k}(\chi_{k-1})$ *(Definition I.32).*

Measured:

- $\forall k \le h-1:\ \chi_k \in \mathcal{A}$ *at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/fx/chain_admissible.py];*
- $e_{00} < 1$ *at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/tree/general_assume.py].*

Then

1. χ_{root} *meets Lemma 4.7, precondition 1;*
2. $\forall k \le h-1:\ \chi_k \in \mathcal{A}$*;*
3. $e_{00} < 1$*.*

Proof.

DEFINES g_{00}, the root node's first diagonal over $\mathbb{R}$ (Lemma I.25)
DEFINES $\widetilde{d}_{00} := \widetilde{g}_{00}$ (Lemma I.25)
DEFINES $d_{11} = q^2/g_{00}$ (Lemma I.27)
DEFINES $\widetilde{d}_{11}$, its computed value, that of Lemma I.26 at each ψ
DEFINES Ψ_n, that of Fact A.43 at $m := n$

Lemma I.25 at the checked key and at every $\psi' \in \Psi_n$	This proof
Shared: $g_{00}, \widetilde{d}_{00}, \Psi_n$ (the proof's block),	E_{00}, m_0, e_{00} (the statement)
ψ	ψ' (the proof's block)
Its conclusion: $\widetilde{d}_{00}(\psi)\ \mathcal{I}\ \left(e_{00}^{\pm}, 0\right)\ g_{00}(\psi)$	

(I1) Shared: $g_{00}, \widetilde{d}_{00}, \Psi_n$ (the proof's block), E_{00}, m_0, e_{00} (the statement)

(L1) $\forall \psi' \in \Psi_n :\ \widetilde{d}_{00}(\psi')\ \mathcal{I}\ \left(e_{00}^{\pm}, 0\right)\ g_{00}(\psi')$
[(I1)]

(L2) $e_{00} < 1$
[the second measured row]

(L3) $m_0 > 0$
[Proposition 5.8, item 8, at the checked key]

Lemma I.27 at the checked key and at every $\psi' \in \Psi_n$	This proof
Shared: $g_{00}, d_{11}, \widetilde{d}_{11}$ (the proof's block),	$E_{00}, m_0, M_0, e_{00}, \bar{G}, Z_I$ (the statement)
ψ	ψ' (the proof's block)
Assumption A1 Assumption A2	(L3) (L2)
Its conclusion: $\widetilde{d}_{11}(\psi)\ \mathcal{I}\ \left((Z_I/(1-e_{00})-1)^{\pm}, 0\right)\ d_{11}(\psi)$	

(I2) ψ | ψ' (the proof's block)

(L4) $\forall \psi' \in \Psi_n :\ \widetilde{d}_{11}(\psi')\ \mathcal{I}\ \left(\left(\frac{Z_I}{1-e_{00}} - 1\right)^{\pm}, 0\right)\ d_{11}(\psi')$
[(I2)]

(L5) $\Rightarrow$ item 1
[(L1), (L4); χ_{root} (Definition I.62)]

(L6) $\forall k \le h-1 :\ \chi_k \in \mathcal{A}$
[the first measured row]

(L7) $\Rightarrow$ item 2
[(L6)]

(L8) $\Rightarrow$ item 3
[(L2)]

□ (items 1 to 3)

Lemma I.67 (The fixed-point signer's leaf preconditions [to table])**.** *The leaves' deviation bounds and the leaf node's first relative bound lie below* 1*. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The key bounds*
  - d_{lo}, χ_{leaf} *and* c_n*, those of Definition I.62;*
- *The node bounds*
  - $u_0 := (1+u)(1+\zeta/(2d_{\text{lo}}(1-\chi_{\text{leaf}})(1-u))) - 1$ *(Corollary G.43 at* $\chi := \chi_{\text{leaf}}$*);*
  - $\bar{e}_0 := (1+\chi_{\text{leaf}})(1+u_0) - 1$ *(Corollary G.43 at* $\chi := \chi_{\text{leaf}}$*);*
- *The leaf deviations*

  - k_J, *that of Definition I.62;*
  - $\chi_\sigma := \max\left((1+\chi_{\text{leaf}})^{1/2}(1+u)^3-1,\ 1-(1-\chi_{\text{leaf}})^{1/2}(1-u)^3\right)$ *(Corollary G.41);*
  - $\chi_\sigma^\zeta := \chi_\sigma + k_J\zeta/s_{\min}$ *(Corollary G.41 at* $s_{\min} := \sqrt{d_{\text{lo}}}\,c_n$*);*
- *The terms*
  - $\bar\delta := \chi_\sigma^\zeta/(1-\chi_\sigma^\zeta)$ *(Definition I.62).*

Measured:

- $\chi_\sigma^\zeta < 1$ *at* $n = 512$ *and* $n = 1024$*, on the proved bounds of Proposition 5.8, items 1 to 4, never the sampled key constants [gate: verify/gates/fx/terms_leaf.py];*
- $\bar e_0 < 1$ *at* $n = 512$ *and* $n = 1024$*, on the proved bounds of Proposition 5.8, items 1 to 4, never the sampled key constants [gate: verify/gates/fx/terms_leaf.py];*
- $\bar\delta < 1$ *at* $n = 512$ *and* $n = 1024$*, on the proved bounds of Proposition 5.8, items 1 to 4, never the sampled key constants [gate: verify/gates/fx/terms_leaf.py].*

Then

1. $\chi_\sigma^\zeta < 1$*;*
2. $\bar e_0 < 1$*;*
3. $\bar\delta < 1$.

Proof. (L1) $\chi_\sigma^\zeta < 1$ [the first measured row]

(L2) $\Rightarrow$ item 1 [(L1)]

(L3) $\bar e_0 < 1$ [the second measured row]

(L4) $\Rightarrow$ item 2 [(L3)]

(L5) $\bar\delta < 1$ [the third measured row]

(L6) $\Rightarrow$ item 3 [(L5)]

□ (items 1 to 3)

Lemma I.68 (The pole on the proved bounds [to table])**.** *The leaves' deviation bound lies below the pole of the one-leaf divergence, on proved bounds. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- α *and* $\bar\delta$*, those of Definition I.62.*

Measured:

- $(1+\bar\delta)^2 < \alpha_L/(\alpha_L-1)$ *at* $n = 512$ *and* $n = 1024$*, on the proved bounds of Proposition 5.8, items 1 to 4, never the sampled key constants [gate: verify/gates/fx/pole.py].*

Then

$$(1+\bar\delta)^2 < \alpha_L/(\alpha_L-1).$$

Proof. (L1) $(1+\bar\delta)^2 < \alpha_L/(\alpha_L-1)$ [the measured row]

(L2) $\Rightarrow$ the statement [(L1)]

□

Lemma I.69 (The fixed-point signer's normalizers [to table])**.** *At every leaf, the normalizer of the computed Gaussian is within a factor* $1 \pm \epsilon$ *of its integral, and* $\epsilon < 1$*. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- $\sigma_{\min}$*,* α*,* χ_σ^ζ*,* $\bar{\delta}$*,* $s_\star$ *and* ϵ*, those of Definition I.62;*
- $\forall s > 0\ \forall c, x \in \mathbb{R}:\ \rho_{s,c}(x) := e^{-(x-c)^2/(2s^2)}$ *(Definition A.2 at* $k := 1$*);*
- $\forall s > 0\ \forall c \in \mathbb{R}:\ \rho_{s,c}(\mathbb{Z}) := \sum_{x\in\mathbb{Z}} \rho_{s,c}(x)$ *(Definition A.2 at* $k := 1$ *and* $A := \mathbb{Z}$*).*

Measured:

- $\epsilon < 1$ *at* $n = 512$ *and* $n = 1024$*, on the proved bounds of Proposition 5.8, items 1 to 4, never the sampled key constants [gate:* `verify/gates/fx/widths.py`*].*

Then

1. $\epsilon \in [0, 1)$*;*
2. $\forall i \le N\ \forall z_{<i}\ \forall c \in \mathbb{R}:\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$*.*

Proof. (L1) $\epsilon \ge 0$

[ϵ (the statement); $e^t > 0$ (Fact A.41, item 12)]

(L2) $\epsilon < 1$

[the measured row]

(L3) $\Rightarrow\ \epsilon \in [0, 1)$

[(L1), (L2)]

(L4) $\Rightarrow$ item 1

[(L3)]

(L5) $\chi_\sigma^\zeta \ge 0$

[χ_σ^ζ, χ_σ and $\chi_{\text{leaf}} = \chi_{h-1}$ (Definition I.62); $\forall k \le h-1:\ \chi_k \in \mathcal{A}$ (Lemma I.66, item 2); $\mathcal{A}$ (Definition I.32); k_J (Corollary G.41); $\sqrt{d_{\text{lo}}}\,c_n > 0$ ($d_{\text{lo}} > 0$, Proposition 5.8, (L13); $c_n = 1/s$, $s = 1.17\sqrt{q}\,\sigma_{\min}$ at the stored word $\sigma_{\min} > 0$, Definition I.62); $\zeta \ge 0$ ($\zeta := 2\zeta_{\text{op}}$, Definition I.1); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5); Fact A.41, items 20 and 8]

(L6) $\chi_\sigma^\zeta \in [0, 1)$

[(L5); Lemma I.67, item 1]

(L7) $\bar{\delta} \ge 0$

[(L6); $\bar{\delta} = \chi_\sigma^\zeta/(1-\chi_\sigma^\zeta)$ (Definition I.62; Corollary G.41)]

(L8) $\bar{\delta} < 1$

[Lemma I.67, item 3]

(L9) $\alpha_L + (1-\alpha_L)(1-\bar{\delta})^2 = 1 + (\alpha_L - 1)(1-(1-\bar{\delta})^2)$

[expand]

(L10) $\alpha_L + (1-\alpha_L)(1-\bar{\delta})^2 \ge 1$

[(L7), (L8), (L9); $\alpha > 1$ (Definition I.62); Fact A.41, item 8]

(L11) $s_\star \le \sigma_{\min}$

[(L7), (L10); $s_\star$ (the statement); $t \mapsto t^{-1/2}$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L12) $s_\star > 0$

[(L8), (L10); $s_\star$ (the statement); the stored word $\sigma_{\min} > 0$ [L0: `fxp/fxp_consts.h:2073-2084`]]

(L13) $\forall i \le N\ \forall z_{<i}:\ \widetilde{\sigma}_i > \sigma_{\min}$

[Lemma I.51, item 1, at the checked key (Definition I.62) and the leaf's `isigma`; $\widetilde{\sigma}_i = 1/$`isigma` (Definition A.25)]

(L14) $\forall s > 0\ \forall c \in \mathbb{R}:\ \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\,s) - 1 = 2\sum_{k\ge1} e^{-2\pi^2 s^2 k^2}\cos(2\pi k c)$

[Lemma E.2, item 1; $d(s,c) = \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\,s) - 1$ (Definition A.29)]

(L15) $\forall s > 0\ \forall c \in \mathbb{R}:\ |\rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\,s) - 1| \le 2\sum_{k\ge1} e^{-2\pi^2 s^2 k^2}$

[(L14); $|\cos| \le 1$ (Fact A.41, item 12); $|x+y| \le |x| + |y|$, $|xy| = |x||y|$ (Fact A.41, item 1)]

(L16) $\forall s \ge s' > 0:\ 2\sum_{k\ge1} e^{-2\pi^2 s^2 k^2} \le 2\sum_{k\ge1} e^{-2\pi^2 s'^2 k^2}$

[exp increasing (Fact A.41, item 5), term by term]

(L17) $\forall i \le N\ \forall z_{<i}\ \forall c \in \mathbb{R}:\ |\rho_{\widetilde{\sigma}_i,c}(\mathbb{Z})/(\sqrt{2\pi}\,\widetilde{\sigma}_i) - 1| \le \epsilon$

[(L15) at $s := \widetilde{\sigma}_i$; (L16) at $(s, s') := (\widetilde{\sigma}_i, s_\star)$ by (L11), (L12), (L13); ϵ (the statement)]

(L18) $\Rightarrow$ item 2

[(L17); $\sqrt{2\pi}\,\widetilde{\sigma}_i > 0$ by (L12), (L13)]

□ (items 1 and 2)

Lemma I.70 (The contraction terms at a checked key [to table])**.** *The two contraction terms of the center shift, read on the bounds every checked key meets, sum below* 1*. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- h*, that of Definition I.62;*
- $\bar{\Xi}'$, $\bar{\Xi}$, G_γ, Υ_k *and* c_S*, those of Definition I.62;*
- $\gamma := \bar{\Xi}'(1 + 2(h-1)\bar{\Xi})\, G_\gamma$ *(Definition I.62);*
- $\gamma_S := c_S \bar{\Xi}' \sum_{k=1}^{h} \Upsilon_k$ *(Definition I.62).*

Measured:

- $\gamma + \gamma_S < 1$ *at* $n = 512$ *and* $n = 1024$*, on the bounds of Proposition 5.8, items 2 to 7, and of Lemma H.21, item 2, never the sampled key constants [gate: verify/gates/fx/gamma.py].*

Then

$$\gamma + \gamma_S < 1.$$

Proof. (L1) $\gamma + \gamma_S < 1$

[the measured row]

(L2) $\Rightarrow$ the statement

[(L1)]

□

Lemma I.71 (Dominance of the bounds' chain [to table])**.** *Every quantity of the chain read at the checked key's own constants is at most the same quantity read at the bounds of Definition I.62, the key's* $\bar{e}_0(\hat{K})$ *is below* 1*, and the row bounds* $e_{+,k}$ *and* e_{ccs} *lie in* $[0, \infty)$ *and* $[0, 1)$*.* ***Under Hypotheses I.21 and I.22****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $\tau \in (1, \infty)$*;*
- $\bar{e}, \bar{T}, \bar{Z} \in [0, \infty)$*.*

Define:

- *The signer's words and parameters*
  - $\zeta_{\mathrm{op}} := 2^{-65}$ *(Definition I.1);*
  - $\sigma_{\min}$*, the stored word [L0: fxp/fxp_consts.h: 2073-2084] (Definition I.62);*
  - $\sigma_{\max} := 1.17^2 \sigma_{\min}$ *(Definition I.62);*
  - ϵ_L*, that of* BerExp *(Algorithm 9), line 1;*
  - $(\lambda, \alpha) := \begin{cases} (128, 257) & n = 512 \\ (256, 513) & n = 1024 \end{cases}$ *(Definition I.62);*
- *The key bounds*
  - h, d_{lo}, d_{hi}, $\bar{\kappa}_{\mathrm{root}}$, $\bar{\kappa}_k$, $\bar{\Xi}'$, $\bar{\Xi}'_{\mathrm{root}}$, $\bar{\Xi}$ *and* $\bar{\ell}$*, those of Definition I.62;*
  - m_0*, that of Proposition 5.8;*
  - E_{01}*, that of Definition A.36, item 7;*
- *The sampler's bounds*
  - $E_s := 66\zeta_{\mathrm{op}} + 45|\epsilon_L|$ *(Definition I.62);*
  - $e_{\mathrm{poly}} := 2^{-51.05}$ *(Definition I.62);*
  - $\forall k \le 18:\ E_{x,k} := (1/(2\sigma_{\min}^2) + \frac{3}{2}(k+1)^2 + 2)\zeta_{\mathrm{op}} + \frac{3}{2}\zeta_{\mathrm{op}}^2$ *(Definition I.62);*
  - $\forall k \le 18:\ e_{+,k} := e^{E_{x,k}+E_s}(1 + e_{\mathrm{poly}}) - 1$ *(Definition I.62);*

- $e_{\mathrm{ccs}} := 2\zeta_{\mathrm{op}}$ *(Definition I.62);*
- $\bar{\varepsilon}_0 := 2e^{-2\pi^2\sigma_{\min}^2}/(1-e^{-2\pi^2\sigma_{\min}^2})$ *(Lemma G.69 at $\sigma_{\min}$);*

- *The chain at the bounds*
  - e_{00}, χ_{root}, χ_k, χ_{leaf}, c_n, χ_σ^ζ, $\bar{\delta}$, E_l^{child}, E_l^{root}, E_l, $\widetilde{\ell}$, c_{split}, M_k, G_X, G_R, G_γ, G_Z, Θ_k, Υ_k, R°, γ, γ_S, D_0°, D_Z°, D°, D_S, W°, p_τ *and* $\mathfrak{L}_B$, *those of Definition I.62 at τ, $\bar{e}$, $\bar{T}$ and $\bar{Z}$;*
  - $u_0 := (1+u)(1+\zeta/(2d_{\mathrm{lo}}(1-\chi_{\mathrm{leaf}})(1-u)))-1$ *(Corollary G.43 at $u := 0$);*
  - $\bar{e}_0 := (1+\chi_{\mathrm{leaf}})(1+u_0)-1$ *(Corollary G.43);*
  - $\mathcal{A}$, *that of Definition I.32;*
  - ϖ, $\bar{e}_{\mathrm{norm}}$ *and* $M_{2\alpha}$, *those of Corollary 4.10, precondition 1, at* $\sigma_{\min}$, $\sigma_{\max}(1+\bar{\delta})$, τ, $e_{+,k}$ *and* e_{ccs};

- *The tree*
  - $\mathcal{G}$, *that of Proposition 5.8;*
  - $T := \mathrm{ffLDL}^\dagger(\mathcal{G})$ *(Definition A.20);*

- *The key constants*
  - $\hat{K}$, *the key's constants (Definition 4.6);*
  - κ_{root}, κ_k, ℓ, $\forall k \in \{1,\dots,h\}:\ \Xi'_k$, $\forall k \in \{1,\dots,h-1\}:\ \Xi_k$, Ξ'_{root} *and* Ξ, *those of Definition 4.6 at the key;*

- *The error chain*
  - $\mathcal{U}_\kappa^0$, *the node map of Definition I.28 at* d_{lo} *and* d_{hi};
  - $\forall 1 \le k \le h-1:\ \vartheta_{k-1}(\hat{K}) := (1+\chi_{k-1}(\hat{K}))/(1-\chi_{k-1}(\hat{K}))$ *(Definition I.32);*
  - $\forall 1 \le k \le h-1:\ \hat{\kappa}_k(\hat{K}) := \vartheta_{k-1}(\hat{K})\kappa_k + (\vartheta_{k-1}(\hat{K})-1)/2$ *(Definition I.32);*
  - $\chi_0(\hat{K}) := \chi_{\mathrm{root}}$ *(Definition I.32);*
  - $\forall 1 \le k \le h-1:\ \chi_k(\hat{K}) := \mathcal{U}^0_{\hat{\kappa}_k(\hat{K})}(\chi_{k-1}(\hat{K}))$ *(Definition I.32);*

- *The leaf deviations*
  - k_J, *that of Corollary G.41 at* $\sqrt{\widetilde{d}_{11}} := (d_{\mathrm{hi}}(1+\chi_{h-1}(\hat{K})))^{1/2}$;
  - $\chi_\sigma(\hat{K}) := \max\left((1+\chi_{h-1}(\hat{K}))^{1/2}-1,\ 1-(1-\chi_{h-1}(\hat{K}))^{1/2}\right)$ *(Corollary G.41 at $u = 0$);*
  - $\chi_\sigma^\zeta(\hat{K}) := \chi_\sigma(\hat{K}) + k_J\zeta/s_{\min}$ *(Corollary G.41 at $s_{\min} := \sqrt{d_{\mathrm{lo}}}\,c_n$);*
  - $\bar{\delta}(\hat{K}) := \chi_\sigma^\zeta(\hat{K})/(1-\chi_\sigma^\zeta(\hat{K}))$;

- *The node bounds*
  - $\bar{e}_0(\hat{K})$, $E_l^{\mathrm{child}}(\hat{K})$ *and* $E_l^{\mathrm{root}}(\hat{K})$, *those of Corollary G.43 at $u = 0$, $\chi := \chi_{h-1}(\hat{K})$,* d_{lo}, d_{hi}, ℓ, m_0, e_{00}, E_{01} *and* κ_{root};
  - $E_l(\hat{K}) := \max(E_l^{\mathrm{child}}(\hat{K}), E_l^{\mathrm{root}}(\hat{K}))$;

- *The center shifts*
  - K_0, k_{split}, K_ζ *and* β_j, *those of Theorem G.59 at $u = 0$ and T;*
  - a_j, *that of Lemma G.52 at $u = 0$;*
  - $G_R(\hat{K}) := K_0 + G_X \max_{\nu,\psi}|\widetilde{l}_{10} - l_{10}|$ *(Theorem G.59 at $E_l := \max_{\nu,\psi}|\widetilde{l}_{10} - l_{10}|$);*
  - $G_\gamma(\hat{K}) := c_{\mathrm{split}} + G_X(1+\ell) + G_R(\hat{K})$ *(Theorem G.59);*
  - $G_Z(\hat{K}) := G_X\ell + G_R(\hat{K}) + \ell$ *(Theorem G.59);*
  - $\forall 1 \le k \le h:\ \Theta_k(\hat{K}) := \sqrt{2^{k-1}}(k_{\mathrm{split}}\zeta + K_\zeta + G_Z(\hat{K})\,a_{h-k})$ *(Theorem G.59);*
  - $\gamma(\hat{K}) := G_\gamma(\hat{K})\sum_{k=1}^h \Xi'_k\beta_{k-1}$ *(Theorem G.59);*
  - $\forall 1 \le k \le h:\ \Upsilon_k(\hat{K}) := (c_{\mathrm{split}}+G_X)(k-1)\ell + G_X\ell + G_R(\hat{K})$ *(Corollary G.62 at $u = 0$ and T);*
  - $c_S := \Xi(n/2)^{1/2}$ *(Corollary G.62);*
  - $\gamma_S(\hat{K}) := c_S\sum_{k=1}^h \Xi'_k\Upsilon_k(\hat{K})$ *(Corollary G.62);*

- *The terms*
  - $\forall R \in [0,\infty):\ D_0^\circ(\hat{K},R) := \Xi'_{\mathrm{root}}\bar{e} + \sum_{k=1}^h \Xi'_k[(c_{\mathrm{split}}+G_X)\bar{T} + \Upsilon_k(\hat{K})R + \Theta_k(\hat{K})]$;
  - $D_Z^\circ(\hat{K}) := G_Z(\hat{K})\sum_{k=1}^h \Xi'_k M_k$;
  - $D_S(\hat{K},\cdot) := (D_0^\circ(\hat{K},\cdot) + D_Z^\circ(\hat{K})\bar{Z})/(1-\gamma(\hat{K})-\gamma_S(\hat{K}))$ *on* $[0,\infty)$;

  - $W^{\circ}(\hat{K},\cdot) := D_S(\hat{K},\cdot)^2/\sigma_{\min}^2$ *on* $[0,\infty)$*;*
  - $\varpi(\hat{K})$*,* $\bar{e}_{\mathrm{norm}}(\hat{K})$ *and* $M_{2\alpha}(\hat{K})$*, the* ϖ*,* $\bar{e}_{\mathrm{norm}}$ *and* $M_{2\alpha}$ *of Corollary 4.10, precondition 1, at* $\sigma_{\min}$*,* $\sigma_{\max}(1+\bar{\delta}(\hat{K}))$*,* τ*,* $e_{+,k}$ *and* e_{ccs}*;*
  - $\mathfrak{L}_B(\hat{K})$*, the* $\mathfrak{L}_B$ *of Theorem 4.11 at* $M_{2\alpha}(\hat{K})$ *and* p_τ*.*

Measured:

- $\bar{\varepsilon}_0 < 1$ *at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/fx/eps0.py].*

Then the key's chain lies below the chain at the bounds, and $\bar{e}_0(\hat{K})$*,* $e_{+,k}$ *and* e_{ccs} *lie in their ranges:*

1. $\forall k \le h-1:\ \chi_k(\hat{K}) \in \mathcal{A}$*;*
2. $\chi_\sigma^\zeta(\hat{K}) \le \chi_\sigma^\zeta$*;*
3. $\bar{\delta}(\hat{K}) \in [0,\bar{\delta}]$*;*
4. $\bar{e}_0(\hat{K}) \le \bar{e}_0$*;*
5. $\gamma(\hat{K}) \le \gamma$*;*
6. $\gamma_S(\hat{K}) \le \gamma_S$*;*
7. $\forall s \in (0,\sigma_{\max}]\ \forall d \in [0,\bar{\delta}]:\ \sqrt{2}\,\Xi\tau s(1+d)(n/2)^{1/2} \le R^{\circ}$*;*
8. $\forall R \in [0,R^{\circ}]:\ D_0^{\circ}(\hat{K},R) \in [0,D_0^{\circ}]$*;*
9. $D_Z^{\circ}(\hat{K}) \in [0,D_Z^{\circ}]$*;*
10. $\forall R \in [0,R^{\circ}]:\ D_S(\hat{K},R) \le D_S$*;*
11. $\forall R \in [0,R^{\circ}]:\ W^{\circ}(\hat{K},R) \le W^{\circ}$*;*
12. $\varpi(\hat{K}) \le \varpi$*;*
13. $\bar{e}_{\mathrm{norm}}(\hat{K}) \le \bar{e}_{\mathrm{norm}}$*;*
14. $\mathfrak{L}_B(\hat{K}) \le \mathfrak{L}_B$*;*
15. $\bar{e}_0(\hat{K}) < 1$*;*
16. $\forall k \le 18:\ e_{+,k} \ge 0$*;*
17. $e_{\mathrm{ccs}} \in [0,1)$*.*

Proof.

DEFINES $\bar{\kappa}_{\mathrm{root}} = (\check{\gamma}_{\mathrm{root}}\, q\check{\gamma}_{\mathrm{hyb}}^2 + E_{01})^2/q^2$ and $\bar{\kappa}_k = (\bar{\varsigma}-1)^2/(4\bar{\varsigma})$ (Definition I.62)

DEFINES $\bar{\Xi}' = \bar{\varsigma}^{1/2}$, $\bar{\Xi} = \bar{\varsigma}^{1/2}$ and $\bar{\Xi}'_{\mathrm{root}} = ((M_0 + \bar{g}_{11})/d_{\mathrm{lo}})^{1/2}$ (Definition I.62)

DEFINES $\bar{\ell} = \max(1,\ \check{\gamma}_{\mathrm{root}}/(1 - E_{00}\check{\gamma}_{\mathrm{hyb}}^2/q) + E_{01}/m_0)$ (Definition I.62)

$\beta_0 = 1/\Xi'_{\mathrm{root}}$ and $\beta_j = 2\Xi_j$, $1 \le j \le h-1$, those of Theorem G.59 at T

$\vartheta_{k-1} = (1+\chi_{k-1})/(1-\chi_{k-1})$ (Definition I.32)

$\hat{\kappa}_k = \vartheta_{k-1}\bar{\kappa}_k + (\vartheta_{k-1}-1)/2$ (Definition I.32 at $\kappa_k := \bar{\kappa}_k$)

$c_{\mathrm{sa}} = \sqrt{2}\,\zeta$ and $k_{\mathrm{sa}} = (1+\sqrt{2}\,\zeta)/2 + \sqrt{2}$ (Corollary G.43 at $u = 0$)

$k_{\mathrm{split}} = \sqrt{2}/2 + k_D$ (Lemma G.53 at $u = 0$)

$k_D = (\sqrt{2}/2)(1+\sqrt{2}\,\zeta) + 3\sqrt{2}$ (Lemma G.16 at $u = 0$)

a_j, $j \ge 0$, those of Corollary I.57

$k_B = 3\sqrt{2}$ (Lemma G.20 at $u = 0$)

$k_I(l) = \sqrt{2}\,l + k_B + \sqrt{2}$, $l \in [0,\infty)$, the k_I of Lemma G.20 at $u = 0$ and $|l_{10}| := l$

COMPUTES $(\widetilde{g}_{00}, \widetilde{g}_{11}, \widetilde{g}_{01})$: the Gram matrix entries ffSampling$^{\mathcal{F}}$ (Algorithm 10) computes in $\mathcal{F}_{\mathrm{fx}}$, line 3

DEFINES (g_{00}, g_{11}, g_{01}): the Gram matrix entries over $\mathbb{R}$

DEFINES $E_{00} := k_H\zeta + 4\gamma'_{fg}\delta_{fg} + 2\delta_{fg}^2$ and $E_{11} := k_H\zeta + 4\gamma'_{FG}\delta_{FG} + 2\delta_{FG}^2$ (Definition A.36)

DEFINES k_H, ζ, γ'_{fg}, γ'_{FG}, δ_{fg} and δ_{FG}, those of Definition A.36

DEFINES $M_0 := q\check{\gamma}_{\mathrm{hyb}}^2 + E_{00}$ (Definition A.37), with $\check{\gamma}_{\mathrm{hyb}}$ that of Definition A.37

DEFINES d_j^ν, $\nu \in \mathrm{Sub}(T)$, $j \in \{00, 11\}$, those of Proposition 5.8

DEFINES $(g_{00}^\nu, g_{01}^\nu, g_{11}^\nu)$, $\nu \in \mathrm{Sub}(T)$, the entries of $\mathcal{G}_\nu(\psi)$, those of Definition 4.6 at the checked key, the (g_{00}, g_{01}, g_{11}) of Corollary G.36 at ν

COMPUTES $(\widetilde{g}_{00}^{\mathrm{K}}, \widetilde{g}_{11}^{\mathrm{K}}, \widetilde{g}_{01}^{\mathrm{K}})$: the Gram matrix entries keychecks (Algorithm 12) computes, line 3, the $\widetilde{g}$ of Lemma H.19

DEFINES Ψ_n, that of Fact A.43 at $m := n$

(L1) $\forall k \in \{1,\dots,h-1\}:\ \kappa_k \le \bar{\kappa}_k$

[Proposition 5.8, item 2, at the checked key (the statement); $\bar{\kappa}_k$ (Definition I.62)]

(L2) $\kappa_{\mathrm{root}} \le \bar{\kappa}_{\mathrm{root}}$

[Proposition 5.8, item 3, at the checked key (the statement); $\bar{\kappa}_{\mathrm{root}}$ (Definition I.62)]

(L3) $\ell \le \bar{\ell}$

[Proposition 5.8, item 7, at the checked key (the statement); $\bar{\ell}$ (Definition I.62)]

(L4) $\forall k \in \{1,\dots,h-1\}:\ \Xi'_k \le \Xi'$

[Ξ' (Definition 4.6, item 12); Fact A.41, item 20]

(L5) $\Xi' \le \bar{\Xi}'$

[Proposition 5.8, item 5, at the checked key (the statement); $\bar{\Xi}'$ (Definition I.62)]

(L6) $\Xi'_h = 1$

[the leaf diagonals d at the depth h (depth, Definition A.18); $\mathcal{L}_d$, the identity ($\mathcal{L}_d$, Definition G.6); Ξ'_k (Definition 4.6, item 8)]

(L7) $1 \le \Xi'$

[Ξ' (Definition 4.6, item 12); Fact A.41, item 20]

(L8) $\Rightarrow\ \forall k \in \{1,\dots,h\}:\ \Xi'_k \in [0, \bar{\Xi}']$

[(L4) to (L7); $\|X\| \ge 0$ (Fact A.41, item 3)]

(L9) $\Xi \le \bar{\Xi}$

[Proposition 5.8, item 6, at the checked key (the statement); $\bar{\Xi}$ (Definition I.62)]

(L10) $\forall j \in \{1,\dots,h-1\}:\ \Xi_j \le \Xi$

[Ξ (Definition 4.6, item 13); Fact A.41, item 20]

(L11) $\Rightarrow\ \forall j \in \{1,\dots,h-1\}:\ \Xi_j \in [0, \bar{\Xi}]$

[(L9), (L10); $\|X\| \ge 0$ (Fact A.41, item 3)]

(L12) $\Xi'_{\mathrm{root}} \in [1, \bar{\Xi}'_{\mathrm{root}}]$

[Lemma H.21, item 2, at the checked key (the statement); $\bar{\Xi}'_{\mathrm{root}}$ (Definition I.62)]

(L13) $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi:\ g^\nu_{00} g^\nu_{11} - |g^\nu_{01}|^2 = g^\nu_{00} d^\nu_{11}$

[$d^\nu_{11}(\psi) = g_{11} - |g_{01}|^2/g_{00}$ (Corollary G.36); $d^\nu_{00}(\psi) = g_{00}$ (Corollary G.36); $(g^\nu_{00}, g^\nu_{01}, g^\nu_{11})$ (the proof's block); Proposition 5.8, item 1, at the checked key; $d_{\mathrm{lo}} > 0$ (Proposition 5.8, (L13)); expand]

(L14) $\forall \nu \in \mathrm{Sub}(T)\ \forall \psi:\ g^\nu_{00} d^\nu_{11} > 0$

[$d^\nu_{00}(\psi) = g_{00}$ (Corollary G.36); $(g^\nu_{00}, g^\nu_{01}, g^\nu_{11})$ (the proof's block); Proposition 5.8, item 1, at the checked key; $d_{\mathrm{lo}} > 0$ (Proposition 5.8, (L13)); Fact A.41, item 26, its strict clause]

(L15) $\Rightarrow\ \forall k \in \{1, \dots, h-1\}:\ \kappa_k \geq 0$

[(L13), (L14); κ_k (Definition 4.6); Fact A.41, items 1 and 20]

(L16) $\forall k \in \{0, \dots, h-1\}:\ \chi_k \in \mathcal{A}$

[Lemma I.66, item 2]

(L17) $\forall \chi, \chi' \in \mathbb{R},\ 0 \leq \chi \leq \chi',\ \chi' \in \mathcal{A}:\ \chi \in \mathcal{A}$

[$\mathcal{A} = \{\chi : 0 \leq \chi < 1,\ u_0(\chi) < 1\}$ (Definition I.32); $u_0 = \zeta/(2m_1)$, $m_1 = d_{\mathrm{lo}}(1-\chi)$ (Definition I.28); $d_{\mathrm{lo}} > 0$ (Proposition 5.8, (L13)); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5); $\zeta \geq 0$ ($\zeta := 2\zeta_{\mathrm{op}}$, Definition I.1); Fact A.41, item 26, at $c := \zeta/2$]

Lemma G.34 at every $\chi \in \mathcal{A}$ and $\kappa \geq 0$ — This proof

Shared: ζ (Definition I.1), $d_{\mathrm{lo}}, d_{\mathrm{hi}}$ (Definition I.62), χ, κ (the scope)

(I1)

u	0
$u \in [0,1)$	$u = 0$ (Definition I.1)
$\zeta \geq 0$	$\zeta := 2\zeta_{\mathrm{op}}$ (Definition I.1)
$d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$	$[d_{\mathrm{lo}}, d_{\mathrm{hi}}] \subseteq (0,\infty)$ (Proposition 5.8, (L14))
$\chi, \kappa \in \mathbb{R}$	The scope
Assumption A1	The scope
Assumption A2	The scope

Its conclusion: $(1+\chi)(1+u_0(\chi)) - 1 \leq \mathcal{U}^\zeta_\kappa(\chi)$

(L18) $\forall \chi \in \mathcal{A}\ \forall \kappa \geq 0:\ (1+\chi)(1+u_0(\chi)) - 1 \leq \mathcal{U}^\zeta_\kappa(\chi)$

[(I1)]

Lemma I.30, item 2 at every $\chi \in [0,1)$, at a node $\nu \in \mathrm{Sub}(T)$ and a root ψ — This proof

Shared: $d_{\mathrm{lo}}, d_{\mathrm{hi}}$ (Definition I.62), $\mathcal{U}^0_\kappa$ (the statement)

(I2)

χ	χ (the scope)
$a, b, \psi, \omega_a, \omega_b$	$d^\nu_{00}(\psi), d^\nu_{00}(\psi), \psi, 0, 0$ (the scope)
$d_{\mathrm{lo}}, d_{\mathrm{hi}} \in (0,\infty)$	$[d_{\mathrm{lo}}, d_{\mathrm{hi}}] \subseteq (0,\infty)$ (Proposition 5.8, (L14))
$a, b \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$	Proposition 5.8, item 1, at the checked key
$\psi \in \mathbb{C},\ \omega_a, \omega_b \in \mathbb{R}$	The scope
$\chi \in [0,1)$	The scope

Its item 2: $\forall \kappa \geq 0:\ \mathcal{U}^\zeta_\kappa(\chi) = \mathcal{U}^0_\kappa(\chi)$

(L19) $\forall \chi \in \mathcal{A}\ \forall \kappa \geq 0:\ \chi \leq \mathcal{U}^0_\kappa(\chi)$

[(L18); (I2); $\mathcal{A}$ (Definition I.32); $(1+\chi)(1+u_0) - 1 \geq \chi$ (Fact A.41, item 8) at $\chi \geq 0$ and $u_0 \geq 0$ (u_0, Definition I.28)]

(L20) $\chi_0(\hat{K}) = \chi_0$

[$\chi_0(\hat{K})$ (the statement); χ_0 (Definition I.62)]

(L21) $\chi_0 \geq 0$

[(L16) at $k = 0$; $\mathcal{A}$ (Definition I.32)]

(L22) $\forall k \in \{1, \dots, h-1\}:\ \chi_{k-1} \in [0,1)$

[(L16) at $k-1$; $\mathcal{A}$ (Definition I.32)]

(L23) $\forall k \in \{1, \dots, h-1\},\ \chi_{k-1}(\hat{K}) \in [0, \chi_{k-1}]:\ 1/(1-\chi_{k-1}(\hat{K})) \leq 1/(1-\chi_{k-1})$

[(L22) and the line's quantifier; $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L24) $\forall k \in \{1, \dots, h-1\},\ \chi_{k-1}(\hat{K}) \in [0, \chi_{k-1}]:\ \vartheta_{k-1}(\hat{K}) \geq 1$

[(L22); $\vartheta_{k-1}(\hat{K})$ (the statement; Definition I.32); expand]

(L25) $\forall k \in \{1,\dots,h-1\},\ \chi_{k-1}(\hat{K}) \in [0,\chi_{k-1}] :\ \vartheta_{k-1}(\hat{K}) \in [1,\vartheta_{k-1}]$
[(L23), (L24) and the line's quantifier; ϑ_{k-1} (the proof's block; Definition I.32); $\vartheta_{k-1}(\hat{K})$ (the statement); Fact A.41, item 8]

(L26) $\forall k \in \{1,\dots,h-1\} :\ \hat{\kappa}_k(\hat{K}) = \vartheta_{k-1}(\hat{K})\kappa_k + (\vartheta_{k-1}(\hat{K}) - 1)/2$
[$\hat{\kappa}_k(\hat{K})$ (the statement); Definition I.32]

(L27) $\forall k \in \{1,\dots,h-1\} :\ \hat{\kappa}_k = \vartheta_{k-1}\bar{\kappa}_k + (\vartheta_{k-1} - 1)/2$
[$\hat{\kappa}_k$ (the proof's block); Definition I.32]

(L28) $\forall k \in \{1,\dots,h-1\},\ \chi_{k-1}(\hat{K}) \in [0,\chi_{k-1}] :\ \hat{\kappa}_k(\hat{K}) \in [0,\hat{\kappa}_k]$
[(L1), (L15), (L25), (L26), (L27); Fact A.41, item 8]

(L29) $\forall \kappa \geq 0 :\ \mathcal{U}^{\zeta}_{\kappa} = \mathcal{U}^{0}_{\kappa}$
[(I2)]

(L30) $\forall k \in \{1,\dots,h-1\} :\ \chi_k(\hat{K}) = \mathcal{U}^{0}_{\hat{\kappa}_k(\hat{K})}(\chi_{k-1}(\hat{K}))$
[$\chi_k(\hat{K})$ (the statement); Definition I.32]

(L31) $\forall k \in \{1,\dots,h-1\} :\ \chi_k = \mathcal{U}^{0}_{\hat{\kappa}_k}(\chi_{k-1})$
[χ_k (Definition I.62); Definition I.32]

Lemma G.33 at every $k \in \{1,\dots,h-1\}$ with $0 \leq \chi_{k-1}(\hat{K}) \leq \chi_{k-1}$	This proof
Shared: ζ (Definition I.1), $d_{\mathrm{lo}}, d_{\mathrm{hi}}$ (Definition I.62)	
u	0
χ, κ	$\chi_{k-1}(\hat{K}), \hat{\kappa}_k(\hat{K})$ (the statement)
χ', κ'	$\chi_{k-1}, \hat{\kappa}_k$ (Definition I.62; the proof's block)
$u \in [0,1)$	$u = 0$ (Definition I.1)
(I3) $\zeta \geq 0$	$\zeta := 2\zeta_{\mathrm{op}}$ (Definition I.1)
$d_{\mathrm{lo}}, d_{\mathrm{hi}} > 0$	$[d_{\mathrm{lo}}, d_{\mathrm{hi}}] \subseteq (0,\infty)$ (Proposition 5.8, (L14))
$\chi, \chi', \kappa, \kappa' \in \mathbb{R}$	The scope; (L28)
Assumption A1	(L16)
Assumption A2	The scope
Assumption A3	The scope
Assumption A4	(L28)
Assumption A5	(L28)
Its conclusion: $\mathcal{U}^{\zeta}_{\kappa}(\chi) \leq \mathcal{U}^{\zeta}_{\kappa'}(\chi')$	

(L32) $\forall k \in \{1,\dots,h-1\},\ \chi_{k-1}(\hat{K}) \in [0,\chi_{k-1}] :\ \mathcal{U}^{\zeta}_{\hat{\kappa}_k(\hat{K})}(\chi_{k-1}(\hat{K})) \leq \mathcal{U}^{\zeta}_{\hat{\kappa}_k}(\chi_{k-1})$
[(I3)]

(L33) $\forall k \in \{1,\dots,h-1\},\ \chi_{k-1}(\hat{K}) \in [0,\chi_{k-1}] :\ \chi_k(\hat{K}) \leq \chi_k$
[(L32), (L29) at $\kappa \in \{\hat{\kappa}_k(\hat{K}), \hat{\kappa}_k\}$ by (L28), (L30), (L31)]

(L34) $\forall k \in \{1,\dots,h-1\},\ \chi_{k-1}(\hat{K}) \in [0,\chi_{k-1}] :\ \chi_{k-1}(\hat{K}) \in \mathcal{A}$
[(L16), (L17)]

(L35) $\forall k \in \{1,\dots,h-1\},\ \chi_{k-1}(\hat{K}) \in [0,\chi_{k-1}] :\ \chi_{k-1}(\hat{K}) \leq \mathcal{U}^{0}_{\hat{\kappa}_k(\hat{K})}(\chi_{k-1}(\hat{K}))$
[(L19) at $\chi := \chi_{k-1}(\hat{K})$ by (L34) and at $\kappa := \hat{\kappa}_k(\hat{K})$ by (L28)]

(L36) $\forall k \in \{1,\dots,h-1\},\ \chi_{k-1}(\hat{K}) \in [0,\chi_{k-1}] :\ \chi_k(\hat{K}) \geq 0$
[(L35), (L30) and the line's quantifier]

(L37) $\Rightarrow\ \forall k \in \{0,\dots,h-1\} :\ \chi_k(\hat{K}) \in [0,\chi_k]$
[induction on k: (L20), (L21) the base; (L33), (L36) the step]

(L38) $\Rightarrow\ \forall k \leq h-1 :\ \chi_k(\hat{K}) \in \mathcal{A}$
[(L16), (L17), (L37)]

(L39) $\Rightarrow$ item 1
[(L38)]

(L40) $\chi_{h-1}(\hat{K}) \in [0,\chi_{\mathrm{leaf}}]$
[(L37) at $k = h-1$; $\chi_{\mathrm{leaf}} = \chi_{h-1}$ (Definition I.62)]

(L41) $\chi_{\text{leaf}} < 1$

[(L16) at $k = h-1$; $\mathcal{A}$ (Definition I.32); $\chi_{\text{leaf}} = \chi_{h-1}$ (Definition I.62)]

(L42) $(1+\chi_{h-1}(\hat{K}))^{1/2} \le (1+\chi_{\text{leaf}})^{1/2}$

[(L40); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L43) $(1-\chi_{\text{leaf}})^{1/2} \le (1-\chi_{h-1}(\hat{K}))^{1/2}$

[(L40), (L41); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L44) $(1+\chi_{h-1}(\hat{K}))^{1/2} \ge 1$

[(L40); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5) at $1 \le 1+\chi_{h-1}(\hat{K})$]

(L45) $\Rightarrow$ $\max((1+\chi_{h-1}(\hat{K}))^{1/2}-1, 1-(1-\chi_{h-1}(\hat{K}))^{1/2}) \in [0, \max((1+\chi_{\text{leaf}})^{1/2}-1, 1-(1-\chi_{\text{leaf}})^{1/2})]$

[(L42), (L43), (L44); Fact A.41, items 20 and 24]

(L46) $d_{\text{hi}}(1+\chi_{h-1}(\hat{K})) \le d_{\text{hi}}(1+\chi_{\text{leaf}})$

[(L40); $[d_{\text{lo}}, d_{\text{hi}}] \subseteq (0,\infty)$ (Proposition 5.8, (L14)); Fact A.41, item 26, at $c := d_{\text{hi}}$]

(L47) $\Rightarrow$ $(d_{\text{hi}}(1+\chi_{h-1}(\hat{K})))^{1/2} \le (d_{\text{hi}}(1+\chi_{\text{leaf}}))^{1/2}$

[(L46); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L48) $\Rightarrow$ $(|c_n| + (d_{\text{hi}}(1+\chi_{h-1}(\hat{K})))^{1/2} + \zeta + 1)\zeta/(\sqrt{d_{\text{lo}}}\, c_n) \in [0, (|c_n| + (d_{\text{hi}}(1+\chi_{\text{leaf}}))^{1/2} + \zeta + 1)\zeta/(\sqrt{d_{\text{lo}}}\, c_n)]$

[(L47); $\zeta \ge 0$ ($\zeta := 2\zeta_{\text{op}}$, Definition I.1); $\sqrt{d_{\text{lo}}}\, c_n > 0$ ($d_{\text{lo}} > 0$, Proposition 5.8, (L13); $c_n = 1/s$, $s = 1.17\sqrt{q}\,\sigma_{\min}$ at the stored word $\sigma_{\min} > 0$, Definition I.62); Fact A.41, item 8]

(L49) $\chi_\sigma^\zeta(\hat{K}) = \max((1+\chi_{h-1}(\hat{K}))^{1/2}-1,\ 1-(1-\chi_{h-1}(\hat{K}))^{1/2}) + (|c_n| + (d_{\text{hi}}(1+\chi_{h-1}(\hat{K})))^{1/2} + \zeta + 1)\zeta/(\sqrt{d_{\text{lo}}}\, c_n)$

[$\chi_\sigma^\zeta(\hat{K})$ (the statement); χ_σ and χ_σ^ζ of Corollary G.41, at $u = 0$ and $s_{\min} := \sqrt{d_{\text{lo}}}\, c_n$; k_J of Corollary G.41, at $u = 0$ and $\sqrt{\widetilde{d}_{11}} := (d_{\text{hi}}(1+\chi_{h-1}(\hat{K})))^{1/2}$]

(L50) $\chi_\sigma^\zeta = \max((1+\chi_{\text{leaf}})^{1/2}-1,\ 1-(1-\chi_{\text{leaf}})^{1/2}) + (|c_n| + (d_{\text{hi}}(1+\chi_{\text{leaf}}))^{1/2} + \zeta + 1)\zeta/(\sqrt{d_{\text{lo}}}\, c_n)$

[χ_σ^ζ (Definition I.62); χ_σ and χ_σ^ζ of Corollary G.41, at $u = 0$ and $s_{\min} := \sqrt{d_{\text{lo}}}\, c_n$; k_J of Corollary G.41, at $u = 0$ and $\sqrt{\widetilde{d}_{11}} := (d_{\text{hi}}(1+\chi_{\text{leaf}}))^{1/2}$]

(L51) $\Rightarrow$ $\chi_\sigma^\zeta(\hat{K}) \le \chi_\sigma^\zeta$

[(L45), (L48), (L49), (L50)]

(L52) $\Rightarrow$ item 2

[(L51)]

(L53) $\chi_\sigma^\zeta(\hat{K}) \ge 0$

[(L45), (L48), (L49)]

(L54) $\chi_\sigma^\zeta < 1$

[Lemma I.67, item 1]

(L55) $\forall t \in (-\infty, 1):\ t/(1-t) = 1/(1-t) - 1$

[expand]

(L56) $1/(1-\chi_\sigma^\zeta(\hat{K})) \le 1/(1-\chi_\sigma^\zeta)$

[(L51), (L54); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L57) $1/(1-\chi_\sigma^\zeta(\hat{K})) \ge 1$

[(L51), (L53), (L54); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5) at $1-\chi_\sigma^\zeta(\hat{K}) \le 1$]

(L58) $\Rightarrow$ $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$

[(L55) at $t := \chi_\sigma^\zeta(\hat{K})$ and at $t := \chi_\sigma^\zeta$; (L56), (L57); $\bar{\delta}(\hat{K}) = \chi_\sigma^\zeta(\hat{K})/(1-\chi_\sigma^\zeta(\hat{K}))$ (the statement); $\bar{\delta} = \chi_\sigma^\zeta/(1-\chi_\sigma^\zeta)$ (Definition I.62)]

(L59) $\Rightarrow$ item 3

[(L58)]

(L60) $2d_{\text{lo}}(1-\chi_{\text{leaf}}) \le 2d_{\text{lo}}(1-\chi_{h-1}(\hat{K}))$

[(L40); $d_{\text{lo}} > 0$ (Proposition 5.8, (L13)); Fact A.41, item 26, at $c := 2d_{\text{lo}}$]

(L61) $\Rightarrow$ $1/(2d_{\text{lo}}(1-\chi_{h-1}(\hat{K}))) \le 1/(2d_{\text{lo}}(1-\chi_{\text{leaf}}))$

[(L41), (L60); $d_{\text{lo}} > 0$ (Proposition 5.8, (L13)); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L62) $\Rightarrow$ $\zeta/(2d_{\text{lo}}(1-\chi_{h-1}(\hat{K}))) \in [0, \zeta/(2d_{\text{lo}}(1-\chi_{\text{leaf}}))]$

[(L61); $\zeta \geq 0$ ($\zeta := 2\zeta_{\mathrm{op}}$, Definition I.1); Fact A.41, item 8]

(L63) $\Rightarrow$ $\bar{e}_0(\hat{K}) \leq \bar{e}_0$

[(L40), (L62); $\bar{e}_0$ and u_0 of Corollary G.43, at $u = 0$; $\bar{e}_0(\hat{K})$ (the statement); $\bar{e}_0$ (Lemma I.67); Fact A.41, item 8]

(L64) $\Rightarrow$ item 4

[(L63)]

(L65) $\bar{e}_0 < 1$

[Lemma I.67, item 2]

(L66) $1/(1 - \bar{e}_0(\hat{K})) \leq 1/(1 - \bar{e}_0)$

[(L63), (L65); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L67) $\bar{e}_0(\hat{K})/(1 - \bar{e}_0(\hat{K})) \leq \bar{e}_0/(1 - \bar{e}_0)$

[(L55) at $t := \bar{e}_0(\hat{K})$ and at $t := \bar{e}_0$, in $(-\infty, 1)$ by (L63), (L65); (L66)]

(L68) $c_{\mathrm{sa}}, k_{\mathrm{sa}} \in [0, \infty)$

[c_{sa} and k_{sa} (the proof's block); $\zeta \geq 0$ ($\zeta := 2\zeta_{\mathrm{op}}$, Definition I.1); expand]

(L69) $c_{\mathrm{sa}} + \chi_{h-1}(\hat{K})(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta/d_{\mathrm{lo}} \in [0, c_{\mathrm{sa}} + \chi_{\mathrm{leaf}}(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta/d_{\mathrm{lo}}]$

[(L40), (L68); $d_{\mathrm{lo}} > 0$ (Proposition 5.8, (L13)); $\zeta \geq 0$ ($\zeta := 2\zeta_{\mathrm{op}}$, Definition I.1); Fact A.41, item 8]

(L70) $\Rightarrow$ $(c_{\mathrm{sa}} + \chi_{h-1}(\hat{K})(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta/d_{\mathrm{lo}})/(1 - \bar{e}_0(\hat{K})) \leq (c_{\mathrm{sa}} + \chi_{\mathrm{leaf}}(1 + c_{\mathrm{sa}}) + k_{\mathrm{sa}}\zeta/d_{\mathrm{lo}})/(1 - \bar{e}_0)$

[(L63), (L65), (L66), (L69); Fact A.41, item 8]

(L71) $d_{\mathrm{hi}}(1 + \chi_{h-1}(\hat{K}))(1 + c_{\mathrm{sa}})/2 + k_{\mathrm{sa}}\zeta \leq d_{\mathrm{hi}}(1 + \chi_{\mathrm{leaf}})(1 + c_{\mathrm{sa}})/2 + k_{\mathrm{sa}}\zeta$

[(L46), (L68); Fact A.41, item 26, at $c := (1 + c_{\mathrm{sa}})/2$]

(L72) $\Rightarrow$ $\sqrt{2}\,(d_{\mathrm{hi}}(1 + \chi_{h-1}(\hat{K}))(1 + c_{\mathrm{sa}})/2 + k_{\mathrm{sa}}\zeta + 1)\zeta \leq \sqrt{2}\,(d_{\mathrm{hi}}(1 + \chi_{\mathrm{leaf}})(1 + c_{\mathrm{sa}})/2 + k_{\mathrm{sa}}\zeta + 1)\zeta$

[(L71); $\zeta \geq 0$ ($\zeta := 2\zeta_{\mathrm{op}}$, Definition I.1); Fact A.41, item 26, at $c := \sqrt{2}\,\zeta$]

(L73) $\Rightarrow$ $E_l^{\mathrm{child}}(\hat{K}) \leq E_l^{\mathrm{child}}$

[(L67), (L70), (L72); E_l^{child}, $\bar{a}_1$, M_2 and $\bar{\delta}_\mu$ of Corollary G.43, at $u = 0$; $E_l^{\mathrm{child}}(\hat{K})$ (the statement); E_l^{child} (Definition I.62)]

(L74) $\ell \geq 0$

[ℓ, a maximum of moduli (Definition 4.6); Fact A.41, item 1]

(L75) $\ell e_{00}/(1 - e_{00}) \leq \bar{\ell} e_{00}/(1 - e_{00})$

[(L3); e_{00} nonnegative (e_{00}, Lemma I.25); $e_{00} < 1$ (Lemma I.66, item 3); Fact A.41, item 26, at $c := e_{00}/(1 - e_{00})$]

(L76) $\kappa_{\mathrm{root}}^{1/2} \leq \bar{\kappa}_{\mathrm{root}}^{1/2}$

[(L2); κ_{root} nonnegative (κ_{root}, Fact A.33, item 6); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L77) $\Rightarrow$ $\sqrt{2}\,((\kappa_{\mathrm{root}}^{1/2} q + E_{01}) + 1)\zeta \leq \sqrt{2}\,((\bar{\kappa}_{\mathrm{root}}^{1/2} q + E_{01}) + 1)\zeta$

[(L76); $q = 12289$ (Definition A.13); $\zeta \geq 0$ ($\zeta := 2\zeta_{\mathrm{op}}$, Definition I.1); Fact A.41, item 26, at $c := q$ and at $c := \sqrt{2}\,\zeta$]

(L78) $\Rightarrow$ $E_l^{\mathrm{root}}(\hat{K}) \leq E_l^{\mathrm{root}}$

[(L75), (L77); E_l^{root} and $\bar{\delta}_\mu$ of Corollary G.43, at $u = 0$; $E_l^{\mathrm{root}}(\hat{K})$ (the statement); E_l^{root} (Definition I.62)]

(L79) $\Rightarrow$ $E_l(\hat{K}) \leq E_l$

[(L73), (L78); Fact A.41, item 24; $E_l = \max(E_l^{\mathrm{child}}, E_l^{\mathrm{root}})$ (Definition I.62); $E_l(\hat{K})$ (the statement)]

(L80) $\forall \psi \in \Psi_n :\ (\widetilde{g}_{00}, \widetilde{g}_{11}, \widetilde{g}_{01}) = (\widetilde{g}_{00}^{\mathrm{K}}, \widetilde{g}_{11}^{\mathrm{K}}, \widetilde{g}_{01}^{\mathrm{K}})$

[ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 1: the images of keychecks (Algorithm 12), line 1, with $\widetilde{f}$ and $\widetilde{F}$ negated [L0: `fxp/kgen_fx.c:71-78`] [L0: `fxp/sign_fxcore.c:24-42`] (Lemma I.10, item 10); Gram (Algorithm 13), lines 2 to 18; $(-x)(-y) = xy$ [L0: `fxp/kgen_fx.c:81`] [L0: `fxp/sign_fxcore.c:184`]]

(L81) $\forall \psi :\ |\widetilde{g}_{00}(\psi) - g_{00}(\psi)| \leq E_{00}$

[(L80); Lemma H.19, item 1, at the checked key]

(L82) $\forall \psi :\ |\widetilde{g}_{11}(\psi) - g_{11}(\psi)| \leq E_{11}$

[(L80); Lemma H.19, item 2, at the checked key]

(L83) $\forall \psi :\ |\widetilde{g}_{01}(\psi) - g_{01}(\psi)| \leq E_{01}$

[(L80); Lemma H.19, item 3, at the checked key]

(L84) $\forall \psi \in \Psi_n :\ g_{00}(\psi) \in [m_0, M_0]$

[Lemma H.19, item 4, at the checked key and at every $\psi \in \Psi_n$ (the proof's block)]

(L85) $\forall \nu \in \mathrm{Sub}(T)\ \forall j \in \{00, 11\}\ \forall \psi :\ d_j^{\nu}(\psi) \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$

[Proposition 5.8, item 1, at the checked key]

(L86) χ_{root} meets Lemma 4.7, precondition 1

[Lemma I.66, item 1]

(L87) $e_{00} < 1$

[Lemma I.66, item 3]

(L88) $\bar{e}_0(\hat{K}) < 1$

[(L63), (L65)]

(I4)

Lemma 4.8	This proof
Shared: ζ (Definition I.1), m_0, E_{01} (the statement), M_0, E_{00}, E_{11} (the proof's block), $d_{\mathrm{lo}}, d_{\mathrm{hi}}$ (Definition I.62)	
the signer	the fixed-point signer (Lemma I.63)
u	0
χ_{00}, χ_{11}	$\chi_{\mathrm{root}}, \chi_{\mathrm{root}}$ (Definition I.62)
χ_k^{ζ}	$\chi_k(\hat{K})$ (L29), (L30)
$E_l, \widetilde{\ell}$	$E_l(\hat{K}), \ell + E_l(\hat{K})$ (the statement)
the signer Falcon-type at (u, ζ)	Lemma I.63
$m_0 > 0$	Proposition 5.8, item 8, at the checked key
$M_0 \geq m_0$	(L84)
$d_{\mathrm{lo}} > 0$	$[d_{\mathrm{lo}}, d_{\mathrm{hi}}] \subseteq (0, \infty)$ (Proposition 5.8, (L14))
$d_{\mathrm{hi}} \geq d_{\mathrm{lo}}$	(L85)
$E_{00}, E_{11}, E_{01} \geq 0$	(L81), (L82), (L83)
$\chi_{00}, \chi_{11} \geq 0$	χ_{root} (Definition I.62); (L21)
Assumption A1	(L81)
Assumption A2	(L82)
Assumption A3	(L83)
Assumption A4	(L87)
Assumption A5	(L84)
Assumption A6	(L84)
Assumption A7	(L86)
Assumption A8	(L86)
Assumption A9	(L85)
Assumption A10	(L38)
Assumption A11	(L88)
Its item 1: $\max_{\psi} \lvert\widetilde{l}_{10} - l_{10}\rvert \leq E_l$	
Its item 2: $\max_{\psi} \lvert\widetilde{l}_{10}\rvert \leq \widetilde{\ell}$	

(L89) $\max_{\nu,\psi} \lvert\widetilde{l}_{10} - l_{10}\rvert \leq E_l(\hat{K})$

[item 1 of (I4); **Hypotheses I.21 and I.22**, named by Lemma I.63]

(L90) $\max_{\nu,\psi} \lvert\widetilde{l}_{10}\rvert \leq \ell + E_l(\hat{K})$

[item 2 of (I4); **Hypotheses I.21 and I.22**, named by Lemma I.63]

(L91) $\Rightarrow\ \max_{\nu,\psi} \lvert\widetilde{l}_{10} - l_{10}\rvert \leq E_l$

[(L79), (L89)]

(L92) $\Rightarrow\ \max_{\nu,\psi} \lvert\widetilde{l}_{10}\rvert \leq \widetilde{\ell}$

[(L3), (L79), (L90); $\widetilde{\ell} = \bar{\ell} + E_l$ (Definition I.62)]

(L93) $c_{\mathrm{split}} \geq 0$

[$c_{\mathrm{split}} = \sqrt{2}\,\zeta$ (Corollary I.9, item 2); $\zeta := 2\zeta_{\mathrm{op}}$, $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1)]

(L94) $G_R(\hat{K}) = (1 + c_{\mathrm{split}}) \max_{\nu,\psi} \lvert\widetilde{l}_{10} - l_{10}\rvert$

[G_R, K_0 and G_X (Theorem G.59) at $u = 0$ and T; $e_{\mathrm{mul}} = 0$ (Corollary I.9, item 7); expand]

(L95) $\max_{\nu,\psi} \lvert\widetilde{l}_{10} - l_{10}\rvert \geq 0$

[Fact A.41, item 1]

(L96) $\Rightarrow\ G_R(\hat{K}) \in [0, G_R]$
[(L91), (L93), (L94), (L95); $G_R = (1 + c_{\text{split}})E_l$ (Definition I.62); Fact A.41, item 8]

(L97) $c_{\text{split}}(1 + \ell) \le c_{\text{split}}(1 + \bar{\ell})$
[(L3), (L93); Fact A.41, item 26, at $c := c_{\text{split}}$]

(L98) $\Rightarrow\ G_\gamma(\hat{K}) \in [0, G_\gamma]$
[(L74), (L93), (L96), (L97); G_γ and G_X of Theorem G.59, at $u = 0$; G_γ (Definition I.62)]

(L99) $c_{\text{split}}\ell \le c_{\text{split}}\bar{\ell}$
[(L3), (L93); Fact A.41, item 26, at $c := c_{\text{split}}$]

(L100) $\Rightarrow\ G_Z(\hat{K}) \in [0, G_Z]$
[(L3), (L74), (L93), (L96), (L99); G_Z and G_X of Theorem G.59, at $u = 0$; G_Z (Definition I.62)]

(L101) $k_I(\max_{\nu,\psi}|\widetilde{l}_{10}|) \le k_I(\widetilde{\ell})$
[(L92); $\max_{\nu,\psi}|\widetilde{l}_{10}| \ge 0$ (Fact A.41, item 1); k_I (the proof's block); Fact A.41, item 26, at $c := \sqrt{2}$]

(L102) $\Rightarrow\ (k_{\text{split}} + (1 + c_{\text{split}})k_I(\max_{\nu,\psi}|\widetilde{l}_{10}|))\zeta \in [0, (k_{\text{split}} + (1 + c_{\text{split}})k_I(\widetilde{\ell}))\zeta]$
[(L93), (L101); k_{split} and k_I nonnegative (Corollary I.9, items 1 and 3); $\zeta \ge 0$ ($\zeta := 2\zeta_{\text{op}}$, Definition I.1); Fact A.41, item 8]

(L103) $\forall k \in \{1, \dots, h\}:\ G_Z(\hat{K})a_{h-k} \in [0, G_Z a_{h-k}]$
[(L100); Corollary I.57, item 3; Fact A.41, item 8]

(L104) $\Rightarrow\ \forall k \in \{1, \dots, h\}:\ \Theta_k(\hat{K}) \in [0, \Theta_k]$
[(L102), (L103); Θ_k and K_ζ of Theorem G.59, at $u = 0$; k_{split} nonnegative (Corollary I.9, item 3); Θ_k (Definition I.62); Fact A.41, item 8]

(L105) $\forall k \in \{1, \dots, h\}:\ (c_{\text{split}} + G_X)(k-1)\ell + G_X\ell \le (c_{\text{split}} + G_X)(k-1)\bar{\ell} + G_X\bar{\ell}$
[(L3), (L93); $G_X = c_{\text{split}}$ (Definition I.62); Fact A.41, item 26, at $c := (c_{\text{split}} + G_X)(k-1)$ and at $c := G_X$]

(L106) $\Rightarrow\ \forall k \in \{1, \dots, h\}:\ \Upsilon_k(\hat{K}) \in [0, \Upsilon_k]$
[(L74), (L93), (L96), (L105); Υ_k of Corollary G.62, at $u = 0$; Υ_k (Definition I.62)]

(L107) $\gamma(\hat{K}) = G_\gamma(\hat{K}) \sum_{k=1}^{h} \Xi'_k \beta_{k-1}$
[γ (Theorem G.59) at T; β_j (the proof's block)]

(L108) $\beta_0 \in (0, 1]$
[(L12); $\beta_0 = 1/\Xi'_{\text{root}}$ (the proof's block); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L109) $\Xi'_1\beta_0 \in [0, \bar{\Xi}']$
[(L8), (L108); Fact A.41, item 8]

(L110) $\forall k \in \{2, \dots, h\}:\ \Xi'_k\beta_{k-1} \in [0, 2\bar{\Xi}'\bar{\Xi}]$
[(L8), (L11); $\beta_j = 2\Xi_j$ (the proof's block); Fact A.41, item 8]

(L111) $\Rightarrow\ \sum_{k=1}^{h} \Xi'_k\beta_{k-1} \in [0, \bar{\Xi}'(1 + 2(h-1)\bar{\Xi})]$
[(L109), (L110); collect]

(L112) $\Rightarrow\ \gamma(\hat{K}) \le \gamma$
[(L98), (L107), (L111); $\gamma := \bar{\Xi}'(1 + 2(h-1)\bar{\Xi})\, G_\gamma$ (Definition I.62); Fact A.41, item 8]

(L113) $\Rightarrow$ item 5
[(L112)]

(L114) $\Xi \ge 1$
[Ξ (Definition 4.6, item 13); Fact A.41, item 20]

(L115) $\Xi(n/2)^{1/2} \in [0, \bar{\Xi}(n/2)^{1/2}]$
[(L9), (L114); Fact A.41, item 8]

(L116) $\forall k \in \{1, \dots, h\}:\ \Xi'_k\Upsilon_k(\hat{K}) \in [0, \bar{\Xi}'\Upsilon_k]$
[(L8), (L106); Fact A.41, item 8]

(L117) $\Rightarrow\ \gamma_S(\hat{K}) \le \gamma_S$
[(L115), (L116); γ_S and c_S of Corollary G.62, at T; $\gamma_S = c_S\bar{\Xi}' \sum_{k=1}^{h} \Upsilon_k$ and $c_S = \bar{\Xi}(n/2)^{1/2}$ (Definition I.62, its c_S); Fact A.41, item 8]

(L118) $\Rightarrow$ item 6
[(L117)]

(L119) $\forall s \in (0, \sigma_{\max}]\ \forall d \in [0, \bar{\delta}]:\ s(1 + d) \in [0, \sigma_{\max}(1 + \bar{\delta})]$

[Fact A.41, item 8]

(L120) $\Rightarrow$ $\forall s \in (0, \sigma_{\max}]\ \forall d \in [0, \bar{\delta}]:\ \sqrt{2}\,\Xi\tau s(1+d)(n/2)^{1/2} \le R^\circ$
[(L115), (L119); $\tau > 1$ (the statement); R° of Corollary G.62, at $\Xi := \bar{\Xi}$, $\sigma_{\max}$ and $\bar{\delta}$ (Definition I.62); Fact A.41, item 8]

(L121) $\Rightarrow$ item 7
[(L120)]

(L122) $\Xi'_{\text{root}}\bar{e} \in [0, \bar{\Xi}'_{\text{root}}\bar{e}]$
[(L12); $\bar{e} \in [0, \infty)$ (the statement); Fact A.41, item 8]

(L123) $\forall R \in [0, R^\circ]\ \forall k \in \{1, \dots, h\}:\ (c_{\text{split}} + G_X)\bar{T} + \Upsilon_k(\hat{K})R + \Theta_k(\hat{K}) \in [0, (c_{\text{split}} + G_X)\bar{T} + \Upsilon_k R^\circ + \Theta_k]$
[(L93), (L104), (L106); $G_X = c_{\text{split}}$ (Definition I.62); $\bar{T} \in [0, \infty)$ (the statement); Fact A.41, item 8]

(L124) $\forall R \in [0, R^\circ]\ \forall k \in \{1, \dots, h\}:\ \Xi'_k[(c_{\text{split}} + G_X)\bar{T} + \Upsilon_k(\hat{K})R + \Theta_k(\hat{K})] \in [0, \bar{\Xi}'[(c_{\text{split}} + G_X)\bar{T} + \Upsilon_k R^\circ + \Theta_k]]$
[(L8), (L123); Fact A.41, item 8]

(L125) $\Rightarrow$ $\forall R \in [0, R^\circ]:\ D_0^\circ(\hat{K}, R) \in [0, D_0^\circ]$
[(L122), (L124); $D_0^\circ(\hat{K}, R)$ (the statement); D_0° (Definition I.62); collect]

(L126) $\Rightarrow$ item 8
[(L125)]

(L127) $\forall k \in \{1, \dots, h\}:\ M_k \ge 0$
[M_k of Theorem G.59; $c_{\text{merge}} = \sqrt{2}\,\zeta$ (Corollary I.9, item 5); Fact A.41, item 23]

(L128) $\forall k \in \{1, \dots, h\}:\ \Xi'_k M_k \in [0, \bar{\Xi}' M_k]$
[(L8), (L127); Fact A.41, item 8]

(L129) $\Rightarrow$ $D_Z^\circ(\hat{K}) \in [0, D_Z^\circ]$
[(L100), (L128); $D_Z^\circ(\hat{K})$ (the statement); D_Z° (Definition I.62); Fact A.41, item 8]

(L130) $\Rightarrow$ item 9
[(L129)]

(L131) $1 - \gamma - \gamma_S > 0$
[Lemma I.70]

(L132) $1 - \gamma(\hat{K}) - \gamma_S(\hat{K}) \ge 1 - \gamma - \gamma_S$
[(L112), (L117)]

(L133) $\forall R \in [0, R^\circ]:\ D_0^\circ(\hat{K}, R) + D_Z^\circ(\hat{K})\bar{Z} \ge 0$
[(L125), (L129); $\bar{Z} \in [0, \infty)$ (the statement); Fact A.41, item 8]

(L134) $\forall R \in [0, R^\circ]:\ D_0^\circ(\hat{K}, R) + D_Z^\circ(\hat{K})\bar{Z} \le D_0^\circ + D_Z^\circ\bar{Z}$
[(L125), (L129); $\bar{Z} \in [0, \infty)$ (the statement); Fact A.41, item 8]

(L135) $1/(1 - \gamma(\hat{K}) - \gamma_S(\hat{K})) \le 1/(1 - \gamma - \gamma_S)$
[(L131), (L132); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5)]

(L136) $\Rightarrow$ $\forall R \in [0, R^\circ]:\ D_S(\hat{K}, R) \le D_S$
[(L131), (L132), (L133), (L134), (L135); D_S and D° (Definition I.62); $D_S(\hat{K}, R)$ (the statement); Fact A.41, item 8]

(L137) $\Rightarrow$ item 10
[(L136)]

(L138) $\forall R \in [0, R^\circ]:\ D_S(\hat{K}, R) \ge 0$
[(L131), (L132), (L133); $D_S(\hat{K}, R)$ (the statement); Fact A.41, item 8]

(L139) $\Rightarrow$ $\forall R \in [0, R^\circ]:\ D_S(\hat{K}, R)^2 \le D_S^2$
[(L136), (L138); $t \mapsto t^2$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L140) $\Rightarrow$ $\forall R \in [0, R^\circ]:\ W^\circ(\hat{K}, R) \le W^\circ$
[(L139); $\sigma_{\min} > 0$ (the stored word [L0: `fxp/fxp_consts.h:2073-2084`]); W° (Definition I.62); $W^\circ(\hat{K}, R)$ (the statement); Fact A.41, item 8]

(L141) $\Rightarrow$ item 11
[(L140)]

(L142) $\sigma_{\max} \geq \sigma_{\min}$

[$\sigma_{\max} = 1.17^2 \sigma_{\min}$ (Definition I.62); $\sigma_{\min} > 0$ (the stored word [L0: fxp/fxp_consts.h:2073-2084])]

(L143) $\Rightarrow$ $\sigma_{\max}(1 + \bar{\delta}(\hat{K})) \in [\sigma_{\min}, \sigma_{\max}(1 + \bar{\delta})]$

[(L58), (L142); Fact A.41, item 8]

(L144) $\sigma_{\max}(1 + \bar{\delta}) \leq 1.778$

[Definition I.62, its measured row]

(L145) $1.778 < \sigma_0$

[σ_0 (Lemma G.64)]

(L146) $\varpi < 1$

[$\varpi \leq 2^{-77.22}$ (Definition I.62, its measured row)]

(L147) $\bar{e}_{\text{norm}} < 1$

[$\bar{e}_{\text{norm}} \leq 2^{-51.04}$ (Definition I.62, its measured row)]

(L148) $\bar{\varepsilon}_0 < 1$

[the measured row]

(L149) $\sigma_{\max}(1 + \bar{\delta}(\hat{K})), \sigma_{\max}(1 + \bar{\delta}) \in [\sigma_{\min}, \sigma_0]$

[(L143), (L144), (L145)]

(L150) $2\alpha \geq 2$

[α (Definition I.62)]

(L151) $\sigma_{\min} > 0$

[the stored word [L0: fxp/fxp_consts.h:2073-2084]]

(L152) $\forall k \leq 18 : \; e_{+,k} \geq 0$

[$e_{+,k}$, $E_{x,k}$, E_s and e_{poly} (Definition I.62) at $\zeta_{\text{op}} = 2^{-65}$ (Definition I.1); $e^x \geq 1$ at $x \geq 0$ (Fact A.41, item 27); Fact A.41, item 8]

(L153) $e_{\text{ccs}} \in [0, 1)$

[e_{ccs} (Definition I.62)]

Lemma G.74 at order 2α	This proof
Shared: $\tau, \sigma_{\min}, e_{+,k}, e_{\text{ccs}}$ (the statement)	
α	2α (Definition I.62)
s, s'	$\sigma_{\max}(1 + \bar{\delta}(\hat{K})), \sigma_{\max}(1 + \bar{\delta})$ (the statement)
$\varpi(s), \varpi(s')$	$\varpi(\hat{K}), \varpi$ (the statement)
$\bar{e}_{\text{norm}}(s), \bar{e}_{\text{norm}}(s')$	$\bar{e}_{\text{norm}}(\hat{K}), \bar{e}_{\text{norm}}$ (the statement)
$\big(\sqrt{\bar{M}_{\text{tab}}(s)} + \sqrt{\bar{M}_{\text{ar}}(s)}\big)^2, \big(\sqrt{\bar{M}_{\text{tab}}(s')} + \sqrt{\bar{M}_{\text{ar}}(s')}\big)^2$	$M_{2\alpha}(\hat{K}), M_{2\alpha}$ (the statement; Definition I.62)
$\alpha \geq 2$	(L150)
$\tau > 1$	The statement
(I5) $\sigma_{\min} > 0$	(L151)
$e_{+,k} \geq 0$	(L152)
$e_{\text{ccs}} \in [0, 1)$	(L153)
$s, s' \in [\sigma_{\min}, \sigma_0]$	(L149)
Assumption A1	(L143)
Assumption A2	(L148)
Assumption A3	(L146)
Assumption A4	(L147)
Its item 1: $\varpi(s) \leq \varpi(s')$	
Its item 2: $\bar{e}_{\text{norm}}(s) \leq \bar{e}_{\text{norm}}(s')$	
Its item 3: $\big(\sqrt{\bar{M}_{\text{tab}}(s)} + \sqrt{\bar{M}_{\text{ar}}(s)}\big)^2 \leq \big(\sqrt{\bar{M}_{\text{tab}}(s')} + \sqrt{\bar{M}_{\text{ar}}(s')}\big)^2$	

(L154) $\varpi(\hat{K}) \leq \varpi$

[item 1 of (I5)]

(L155) $\Rightarrow$ item 12

[(L154)]

(L156) $\bar{e}_{\mathrm{norm}}(\hat{K}) \le \bar{e}_{\mathrm{norm}}$

[item 2 of (I5)]

(L157) $\Rightarrow$ item 13

[(L156)]

(L158) $M_{2\alpha}(\hat{K}) \le M_{2\alpha}$

[item 3 of (I5)]

(L159) $\alpha M_{2\alpha}(\hat{K}) + 2p_\tau \le \alpha M_{2\alpha} + 2p_\tau$

[(L158); $(\lambda, \alpha) = (128, 257)$ at $n = 512$ (Definition I.62); $(\lambda, \alpha) = (256, 513)$ at $n = 1024$ (Definition I.62); Fact A.41, item 26, at $c := \alpha$]

(L160) $\mathfrak{L}_B(\hat{K}) = N\alpha_L(\alpha M_{2\alpha}(\hat{K}) + 2p_\tau)/(2(\alpha - 1))$

[$\mathfrak{L}_B$ of Theorem 4.11, at $M_{2\alpha}(\hat{K})$; $\mathfrak{L}_B(\hat{K})$ (the statement)]

(L161) $\mathfrak{L}_B = N\alpha_L(\alpha M_{2\alpha} + 2p_\tau)/(2(\alpha - 1))$

[$\mathfrak{L}_B$ of Theorem 4.11, at $M_{2\alpha}$; $\mathfrak{L}_B$ (Definition I.62)]

(L162) $N\alpha_L/(2(\alpha - 1)) > 0$

[N (Definition A.25); α (Definition I.62)]

(L163) $\Rightarrow$ $\mathfrak{L}_B(\hat{K}) \le \mathfrak{L}_B$

[(L159), (L160), (L161), (L162); Fact A.41, item 26, at $c := N\alpha_L/(2(\alpha - 1))$]

(L164) $\Rightarrow$ item 14

[(L163)]

(L165) $\Rightarrow$ item 15

[(L88)]

(L166) $\Rightarrow$ item 16

[(L152)]

(L167) $\Rightarrow$ item 17

[(L153)]

□ (items 1 to 17)

I.5.4 The terms from the derived bounds

Proposition 5.9 (*Inputs of the phase statements at the fixed-point signer [to table]*) [to statement].

At a computed center within the bounds below, the fixed-point signer meets the inputs of Lemmas 4.7, 4.8 and 4.9, Corollary 4.10 and Theorem 4.11 at its key's constants, with the terms of Definition I.62, and those statements' bounds hold there. ***Under Hypotheses I.21 and I.22****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $c \in \{t, t_{\mathrm{frac}}\}$ *be a center,* t *and* t_{frac} *those of Definition 4.5 at the key and* $\mathsf{h}(\mathsf{m})$*;*
- $\bar{e}, \bar{T}, \bar{Z} \in [0, \infty)$.

Define:

- *The signer's words and parameters*
  - $\sigma_{\min}$*, that of Definition I.62;*
  - σ_0*, that of Lemma G.64;*
- *The coefficient norm*
  - $\|\cdot\|$*, the coefficient norm (Appendix G.5);*
- *The center and the samples*
  - $\widetilde{t}_T$*, the computed value of* c *in* $\mathcal{F}_{\mathrm{fx}}$ *(*ffSampling$^{\mathcal{F}}$ *(Algorithm 10) at* $\mathsf{h}(\mathsf{m})$*, lines 9 to 20 at* $c = t$*,* center$_{\mathrm{frac}}$ *(Algorithm 17) at* $c = t_{\mathrm{frac}}$*);*
  - $z' := (z_0, z_1)$*, the sample* ffsamp *(Algorithm 6) returns at* c *(*ffSampling$^{\mathcal{F}}$*, line 24);*
- *The terms*
  - α*,* $e_{+,k}$ *and* e_{ccs}*, those of Definition I.62;*

- c_n, $\sigma_{\max}$, $\bar{\delta}$, ϵ *and* ε_0°, *those of Definition I.62;*
- R°, W°, p_τ *and* $\mathfrak{L}_B$, *those of Definition I.62;*
- p'_τ, *that of Corollary 4.10, precondition 3;*

- *The key constants*
  - $\hat{K}$, *the key's constants (Definition 4.6);*
  - $\bar{\delta}(\hat{K})$, $\chi^\zeta_\sigma(\hat{K})$, $\gamma(\hat{K})$, $\gamma_S(\hat{K})$, $\varpi(\hat{K})$, $\bar{e}_{\mathrm{norm}}(\hat{K})$, $M_{2\alpha}(\hat{K})$ *and* $\mathfrak{L}_B(\hat{K})$, *those of Lemma I.71 at* τ, $\bar{e}$, $\bar{T}$ *and* $\bar{Z}$;
- *The leaves*
  - $\forall z \in \mathbb{Z}^N :\ W(z) := \sum_{i \le N} \Delta_i(z_{<i})^2 / \sigma_i(z_{<i})^2$;
  - $\widetilde{B}_i$, $\bar{\rho}_B$ *and* $\bar{p}_C$, *those of Definition A.28 at the signer's base sampler;*
  - C_i, *the fringe sets of Definition A.26 at the signer's base sampler;*
  - $\forall s > 0\ \forall c, x \in \mathbb{R} :\ \rho_{s,c}(x) := e^{-(x-c)^2/(2s^2)}$ *(Definition A.2 at* $k := 1$*);*
  - $\forall s > 0\ \forall c \in \mathbb{R} :\ \rho_{s,c}(\mathbb{Z}) := \sum_{x \in \mathbb{Z}} \rho_{s,c}(x)$ *(Definition A.2 at* $k := 1$ *and* $A := \mathbb{Z}$*).*

Assume:

(A1) $\|\widetilde{t}_T - c\| \le \bar{e}$;

(A2) $\|c\| \le \bar{T}$;

(A3) $\forall z \in S :\ \|z'\| \le \bar{Z}$;

(A4) $p'_\tau < 1$.

Then the signer meets the inputs of the tree, the centers, the base sampler and the summary at its key's constants, and their bounds hold there:

1. *The signer is a Falcon-type signer at* $(0, \zeta)$;
2. $\forall k \le 18 :\ e_{+,k} \ge 0$;
3. $e_{\mathrm{ccs}} \in [0, 1)$;
4. $\chi^\zeta_\sigma(\hat{K}) < 1$;
5. $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$;
6. $\forall z \in S\ \forall i \le N :\ |\delta_i| \le \bar{\delta}(\hat{K})$;
7. $\gamma(\hat{K}) + \gamma_S(\hat{K}) < 1$;
8. $\forall z \in S :\ W(z) \le W^\circ$;
9. $\bar{\delta}(\hat{K}) < 1$;
10. $\sigma_{\max}(1 + \bar{\delta}(\hat{K})) \le \sigma_0$;
11. $\varpi(\hat{K}) < 1$;
12. $\bar{e}_{\mathrm{norm}}(\hat{K}) < 1$;
13. $\forall i \le N\ \forall z_{<i}\ \forall c \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$;
14. $\mathfrak{L}_B(\hat{K}) \le \mathfrak{L}_B$;
15. $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}(\hat{K})$;
16. $p_\tau \ge 0$;
17. $\forall i \le N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$;
18. $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$;
19. $\forall S' \subseteq S\ \forall I \subseteq \{1, \ldots, N\} :\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$;

19419 *20.* $\sigma_{\min} > 0$*;*

19420 *21.* $\forall i \le N :\ \sigma_i \in (\sigma_{\min}, \sigma_{\max})$*;*

19421 *22.* $\forall i \le N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$*;*

19422 *23.* $(1+\bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$*;*

19423 *24.* $\varepsilon_0^\circ < 1$*;*

19424 *25.* $p'_\tau + \bar{p}_C < 1$*;*

19425 *26.* $\bar{\delta} \in [0, 1)$*;*

19426 *27.* $W^\circ \ge 0$.

19427 *Proof.*

DEFINES $R^\circ(\hat{K}) := \sqrt{2}\,\Xi\tau\sigma_{\max}(1+\bar{\delta}(\hat{K}))(n/2)^{1/2}$, Ξ that of Definition 4.6 at the key and $\bar{\delta}(\hat{K})$ that of Lemma I.71: the R° of Lemma 4.9, precondition 1, at the key

19428 DEFINES $W^\circ(\hat{K}, \cdot) = D_S(\hat{K}, \cdot)^2/\sigma_{\min}^2$ on $[0, \infty)$ (Lemma I.71)

DEFINES $D_S(\hat{K}, \cdot)$, that of Lemma I.71 at τ, $\bar{e}$, $\bar{T}$ and $\bar{Z}$

19429 *Proof of items 1 to 27.*

19430 (L1) $C_i = \emptyset$

19431 [Lemma I.64, item 2]

19432 (L2) $\bar{p}_C = 0$

19433 [Lemma I.64, item 3]

19434 (L3) $\bar{\delta} \in [0, 1)$

19435 [Lemma I.69, (L7); Lemma I.67, item 3]

19436 (L4) $W^\circ \ge 0$

19437 [$W^\circ = D_S^2/\sigma_{\min}^2$ (Definition I.62)]

19438 (L5) the signer is a Falcon-type signer at $(0, \zeta)$

19439 [Lemma I.63; **Hypotheses I.21 and I.22**, named by Lemma I.63]

Lemma I.71	This proof
Shared: (f, g, F, G), $\tau, \bar{e}, \bar{T}, \bar{Z}$ Shared: $\tau > 1$	
$\bar{e}, \bar{T}, \bar{Z} \in [0, \infty)$	The statement; Definition I.62
Its item 2: $\chi_\sigma^\zeta(\hat{K}) \le \chi_\sigma^\zeta$	
Its item 3: $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$	
Its item 5: $\gamma(\hat{K}) \le \gamma$	
(I1) Its item 6: $\gamma_S(\hat{K}) \le \gamma_S$	
Its item 7: $\forall s \in (0, \sigma_{\max}]\ \forall d \in [0, \bar{\delta}] :\ \sqrt{2}\,\Xi\tau s(1+d)(n/2)^{1/2} \le R^\circ$	
Its item 11: $\forall R \in [0, R^\circ] :\ W^\circ(\hat{K}, R) \le W^\circ$	
Its item 12: $\varpi(\hat{K}) \le \varpi$	
Its item 13: $\bar{e}_{\text{norm}}(\hat{K}) \le \bar{e}_{\text{norm}}$	
Its item 14: $\mathfrak{L}_B(\hat{K}) \le \mathfrak{L}_B$	
Its item 16: $\forall k \le 18 :\ e_{+,k} \ge 0$	
Its item 17: $e_{\text{ccs}} \in [0, 1)$	

19440

19441 (L6) $\chi_\sigma^\zeta(\hat{K}) < 1$

19442 [item 2 of (I1); Lemma I.67, item 1; **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L7) $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$

[item 3 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L8) $\bar{\delta}(\hat{K}) < 1$

[(L7); Lemma I.67, item 3]

(L9) $\sigma_{\max}(1 + \bar{\delta}(\hat{K})) \le \sigma_0$

[Lemma I.71, (L143), (L145); $\sigma_{\max}(1 + \bar{\delta}) \le 1.778$ (Definition I.62, its measured row); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L10) $\varpi(\hat{K}) < 1$

[item 12 of (I1); Lemma I.71, (L146); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L11) $\bar{e}_{\mathrm{norm}}(\hat{K}) < 1$

[item 13 of (I1); Lemma I.71, (L147); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L12) $\gamma(\hat{K}) + \gamma_S(\hat{K}) < 1$

[Lemma I.70; items 5 and 6 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L13) $p'_\tau + \bar{p}_C < 1$

[assumption A4; (L2)]

(L14) $\sigma_{\min} > 0$

[the stored word [L0: `fxp/fxp_consts.h:2073-2084`]]

(L15) $\forall i \le N : \ \sigma_i \in (\sigma_{\min}, \sigma_{\max})$

[Lemma D.11, items 1 and 2, at the fixed-point signer; $\sigma_{\max}$ (Definition I.62); σ_i (Definition A.25)]

Lemma I.51, item 1 at every $i \le N$ and $z_{<i}$	This proof
Shared: (f, g, F, G), $\sigma_{\min}$	
(I2) `isigma`	$1/\widetilde{\sigma}_i$ (Definition A.25)
$n \in \{512, 1024\}$	Definition 5.5, item 1
`isigma` taken by a call of SamplerZ by deepest	The i-th call of $\mathrm{ffSampling}^{\mathcal{F}}$ (Definition A.25), at deepest (Algorithm 7)
Its conclusion: $\widetilde{\sigma} > \sigma_{\min}$	

(L16) $\forall i \le N \ \forall z_{<i} : \ \widetilde{\sigma}_i > \sigma_{\min}$

[(I2)]

(L17) $\texttt{INV_SIGMA}[\log_2 n] \ \mathcal{I}\,(u^{\pm}, \zeta^{\pm})\ c_n$

[Lemma D.10 at the fixed-point signer; c_n (Definition I.62)]

(L18) $\varepsilon_0^\circ < 1$

[the ε_0° row of Definition I.62]

(L19) $(1 + \bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$

[Lemma I.68]

(L20) $\epsilon \in [0, 1)$

[Lemma I.69, item 1]

(L21) $\forall i \le N \ \forall z_{<i} \ \forall c \in \mathbb{R} : \ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1 - \epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1 + \epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$

[Lemma I.69, item 2]

(L22) $\forall s \in (0, \sigma_{\max}] \ \forall d \in [0, \bar{\delta}] : \ \sqrt{2}\,\Xi\tau s(1 + d)(n/2)^{1/2} \le R^\circ$

[item 7 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L23) $R^\circ(\hat{K}) \ge 0$

[(L7), (L14); $R^\circ(\hat{K})$ (the proof's block); $\Xi \ge 0$ (Ξ, Definition 4.6, item 13); $\tau > 1$ (τ, Definition A.26); $\sigma_{\max} = 1.17^2\sigma_{\min}$ (Definition I.62); Fact A.41, item 8]

(L24) $R^\circ(\hat{K}) \in [0, R^\circ]$

[(L23); (L22) at $s := \sigma_{\max}$, in $(0, \sigma_{\max}]$ by (L14), and $d := \bar{\delta}(\hat{K})$ by (L7); $R^\circ(\hat{K})$ (the proof's block)]

(L25) $W^\circ(\hat{K}, R^\circ(\hat{K})) \le W^\circ$

[(L24); item 11 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

	Lemma 4.7	This proof
	Shared: $m_0, M_0, d_{\mathrm{lo}}, d_{\mathrm{hi}}, E_{00}, E_{11}, E_{01}$ (Definition I.62)	
	the signer, u, ζ	the fixed-point signer, $0, \zeta$ (L5)
	χ_{00}, χ_{11}	$\chi_{\mathrm{root}}, \chi_{\mathrm{root}}$ (Definition I.62)
	χ_k^ζ	$\chi_k(\hat{K})$ (Lemma I.71, (L29), (L30))
	k_J, χ_σ^ζ	$k_J, \chi_\sigma^\zeta(\hat{K})$ (Lemma I.71)
	$\bar{\delta}$	$\bar{\delta}(\hat{K})$ (the statement)
	the signer Falcon-type at (u, ζ)	(L5)
	$m_0 > 0$	Proposition 5.8, item 8, at the checked key
	$M_0 \geq m_0$	Lemma I.71, (L84)
(I3)	$d_{\mathrm{lo}} > 0$	$[d_{\mathrm{lo}}, d_{\mathrm{hi}}] \subseteq (0, \infty)$ (Proposition 5.8, (L14))
	$d_{\mathrm{hi}} \geq d_{\mathrm{lo}}$	Proposition 5.8, item 1
	$E_{00}, E_{11}, E_{01} \geq 0$	Lemma I.71, (L81), (L82), (L83)
	$\chi_{00}, \chi_{11} \geq 0$	χ_{root} (Definition I.62)
	Assumption A1	Lemma I.66, item 1
	Assumption A2	Lemma I.66, item 1
	Assumption A3	Proposition 5.8, item 1
	Assumption A4	Lemma I.71, item 1
	Assumption A5	(L6)
	Assumption A6	(L17)
	Its conclusion: $\forall i \leq N\ \forall z_{<i} :\ \lvert\delta_i\rvert \leq \bar{\delta}$	

(L26) $\forall i \leq N\ \forall z_{<i} :\ \lvert\delta_i\rvert \leq \bar{\delta}(\hat{K})$

[(I3); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L27) $\forall z \in S\ \forall i \leq N :\ \lvert\delta_i\rvert \leq \bar{\delta}(\hat{K})$

[(L26) at $z_{<i}$ of $z \in S$]

	Lemma 4.9, item 2 at the key's constants $\hat{K}$	This proof
	Shared: $\bar{T}, \bar{Z}$	
	the signer, u, ζ	the fixed-point signer, $0, \zeta$ (L5)
	$t, \widetilde{t}_T, z'$	$c, \widetilde{t}_T, z'$ (the statement)
	$\lVert e_{\mathrm{root}} \rVert$	$\bar{e}$ (the statement)
	$\bar{\delta}$	$\bar{\delta}(\hat{K})$ (L7), (L27)
	$E_l, \widetilde{\ell}$	$E_l(\hat{K}), \ell + E_l(\hat{K})$ (Lemma I.71, (L89), (L90))
	D_S, W°	$D_S(\hat{K}, R^\circ(\hat{K})), W^\circ(\hat{K}, R^\circ(\hat{K}))$ (the proof's block; Lemma I.71)
	the signer Falcon-type at (u, ζ)	(L5)
	$t \in \mathcal{R}_n \times \mathcal{R}_n$	$c \in \{t, t_{\mathrm{frac}}\}$ (the statement; Definition A.25)
(I4)	$e_{\mathrm{root}} \in \mathcal{R}_n \times \mathcal{R}_n$	$\bar{e} \in [0, \infty)$ (the statement)
	$\bar{T}, \bar{Z} \geq 0$	The statement
	$\bar{\delta} \in [0, 1)$	(L7), (L8)
	$\forall z \in S\ \forall i \leq N :\ \lvert\delta_i\rvert \leq \bar{\delta}$	(L27)
	$\max_\psi \lvert\widetilde{l}_{10} - l_{10}\rvert \leq E_l$	Lemma I.71, (L89)
	$\max_\psi \lvert\widetilde{l}_{10}\rvert \leq \widetilde{\ell}$	Lemma I.71, (L90)
	Assumption A1	Assumption A1
	Assumption A2	Assumption A2
	Assumption A3	Assumption A3
	Assumption A4	(L12)
	Assumption A5	(L14)
	Assumption A6	(L15)
	Its conclusion: $\forall z \in S :\ W(z) \leq W^\circ$	

(L28) $\forall z \in S :\ W(z) \leq W^\circ(\hat{K}, R^\circ(\hat{K}))$

[(I4); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L29) $\forall z \in S:\ W(z) \le W^\circ$

[(L28), (L25)]

(L30) $\forall k \le 18:\ e_{+,k} \ge 0$

[item 16 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L31) $e_{\mathrm{ccs}} \in [0,1)$

[item 17 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

Corollary 4.10 at the key's constants $\hat{K}$	This proof
Shared: $\sigma_0, \sigma_{\max}, p_\tau, p'_\tau$	
$\mathcal{F}, u, \zeta$	$\mathcal{F}_{\mathrm{fx}}, 0, \zeta$ (L5)
$e_{+,k}, e_{\mathrm{ccs}}, \epsilon$	$e_{+,k}, e_{\mathrm{ccs}}, \epsilon$ (Definition I.62; (L20))
$\bar{\delta}$	$\bar{\delta}(\hat{K})$ (L7), (L27)
p_C^D	0 (L1); Definition I.62
$M_{2\alpha}, \varpi, \bar{e}_{\mathrm{norm}}$	$M_{2\alpha}(\hat{K}), \varpi(\hat{K}), \bar{e}_{\mathrm{norm}}(\hat{K})$ (Lemma I.71)
$\mathcal{F}$ the realization of a Falcon-type signer at (u,ζ)	(L5)
$e_{+,k} \ge 0,\ e_{\mathrm{ccs}} \in [0,1)$	(L30), (L31)
$\epsilon \in [0,1)$	(L20)
$\bar{\delta} \ge 0$	(L7)
$\forall z \in S\ \forall i \le N:\ \lvert\delta_i\rvert \le \bar{\delta}$	(L27)
Assumption A1	Lemma I.64, items 4 to 7
(I5) Assumption A2	(L14)
Assumption A3	(L15)
Assumption A4	(L16)
Assumption A5	(L9)
Assumption A6	(L8)
Assumption A7	(L21)
Assumption A8	(L10)
Assumption A9	(L11)
Assumption A10	(L13)
Its item 7: $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}$	
Its item 8: $p_\tau \ge 0$	
Its item 4: $\forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$	
Its item 2: $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$	
Its item 6: $\forall S' \subseteq S\ \forall I \subseteq \{1,\dots,N\}:\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{\lvert I\rvert}$	

(L32) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}(\hat{K})$

[item 7 of (I5); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L33) $\forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$

[item 4 of (I5); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L34) $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$

[item 2 of (I5); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L35) $\forall S' \subseteq S\ \forall I \subseteq \{1,\dots,N\}:\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{\lvert I\rvert}$

[item 6 of (I5); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L36) $\mathfrak{L}_B(\hat{K}) \le \mathfrak{L}_B$

[item 14 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L37) $\Rightarrow$ item 1

[(L5)]

(L38) $\Rightarrow$ item 2

[(L30)]

(L39) $\Rightarrow$ item 3

[(L31)]

(L40) $\Rightarrow$ item 4

[(L6)]

(L41) $\Rightarrow$ item 5

[(L7)]

(L42) $\Rightarrow$ item 6

[(L27)]

(L43) $\Rightarrow$ item 7

[(L12)]

(L44) $\Rightarrow$ item 8

[(L29)]

(L45) $\Rightarrow$ item 9

[(L8)]

(L46) $\Rightarrow$ item 10

[(L9)]

(L47) $\Rightarrow$ item 11

[(L10)]

(L48) $\Rightarrow$ item 12

[(L11)]

(L49) $\Rightarrow$ item 13

[(L21)]

(L50) $\Rightarrow$ item 14

[(L36)]

(L51) $\Rightarrow$ item 15

[(L32)]

(L52) $\Rightarrow$ item 17

[(L33)]

(L53) $\Rightarrow$ item 18

[(L34)]

(L54) $\Rightarrow$ item 19

[(L35)]

(L55) $\Rightarrow$ item 20

[(L14)]

(L56) $\Rightarrow$ item 21

[(L15)]

(L57) $\Rightarrow$ item 22

[(L16)]

(L58) $\Rightarrow$ item 23

[(L19)]

(L59) $\Rightarrow$ item 24

[(L18)]

(L60) $\Rightarrow$ item 25

[(L13)]

(L61) $\Rightarrow$ item 26

[(L3)]

(L62) $\Rightarrow$ item 27

[(L4)]

(L63) $p_\tau \geq 0$

[item 8 of (I5); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L64) $\Rightarrow$ item 16

[(L63)]

19565 □ (items 1 to 27)

19566

n	χ_{root}	χ_{leaf}	$\bar{\delta}$	E_l **at a child**
512	$2^{-47.3}$	$2^{-35.4}$	$2^{-36.4}$	$2^{-34.4}$
1024	$2^{-45.9}$	$2^{-33.6}$	$2^{-34.6}$	$2^{-32.6}$

Table 33: The terms of Definition I.62, at both centers t and t_{frac}. Gate: `verify/reports/fx/terms.py`, at the bounds every checked key meets.

19567 **Corollary 5.10** (*The fixed-point signer's divergence and bit security [to table]*) [to statement].

19568 *At a computed center within the bounds below, the fixed-point signer's* $\ln R$ *is at most* A*, its*
19569 *fringe classes and its divergence conditioned on* S_0 *are bounded, and its signatures keep the bit*
19570 *security* $\lambda_{\mathcal{F}}$*.* ***Under Hypotheses I.21 and I.22****, let:*

19571 - (f, g, F, G) *be a checked key (Definition 5.5);*
19572 - $c \in \{t, t_{\text{frac}}\}$ *be a center,* t *and* t_{frac} *those of Definition 4.5 at the key and* $\mathsf{h}(\mathsf{m})$*;*
19573 - $\bar{e}, \bar{T}, \bar{Z} \in [0, \infty)$*;*
19574 - $Q_s \in \mathbb{Z}_{>0}$*;*
19575 - $M_C \in \mathbb{Z}_{\geq 0}$*.*

19576 *Define:*

19577 - *The coefficient norm*
19578 - $\|\cdot\|$*, the coefficient norm (Appendix G.5);*
19579 - *The center and the samples*
19580 - $\widetilde{t}_T$*, the computed value of* c *in* $\mathcal{F}_{\text{fx}}$ (ffSampling$^{\mathcal{F}}$ *(Algorithm 10) at* $\mathsf{h}(\mathsf{m})$*, lines 9 to 20 at* $c = t$*,* center$_{\text{frac}}$ *(Algorithm 17) at* $c = t_{\text{frac}}$*);*
19581 - $z' := (z_0, z_1)$*, the sample* ffsamp *(Algorithm 6) returns at* c *(*ffSampling$^{\mathcal{F}}$*, line 24);*
19582 - *The terms*
19583 - λ *and* α*, those of Definition I.62;*
19584 - $\sigma_{\max}$*,* $\bar{\delta}$ *and* ε_0°*, those of Definition I.62;*
19585 - W°*,* p_τ*,* $\mathfrak{L}_B$*,* $\mathfrak{L}_{\bar{\delta}}$*,* $\mathfrak{L}_\Delta$*,* $\mathfrak{L}_\Phi$ *and* A*, those of Definition I.62;*
19586 - p'_τ*, that of Corollary 4.10, precondition 3;*
19587 - *The classes and the measures*
19588 - S_k*,* S_0*,* P_{S_0} *and* Q_{S_0}*, those of Theorem 4.11 at* $S' := S$*;*
19589 - $R_\alpha^{S_k}(P \,\|\, Q)$*, that of Definition A.28 at* $\mathcal{Y} := S_k$*;*
19590 - κ_C *and* $\bar{p}_C$*, those of Definition A.28 at the signer's base sampler;*
19591 - R*, that of Definition A.30 at* S*,* $\bar{\delta}$ *and the signer's* $\bar{\rho}_B$*;*
19592 - $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$*, the probability measures of* Q_s *independent signatures on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1);*
19593 - *The bit security*
19594 - $\lambda_{\mathcal{F}}$*, that of Definition 5.3 at* A*,* κ_C*,* $\bar{p}_C$ *and* M_C*.*

19595 *Assume:*

19596 *(A1)* $\|\widetilde{t}_T - c\| \leq \bar{e}$*;*
19597 *(A2)* $\|c\| \leq \bar{T}$*;*
19598 *(A3)* $\forall z \in S : \ \|z'\| \leq \bar{Z}$*;*
19599 *(A4)* $p'_\tau < 1$*.*

19600 *Then* $\ln R$ *is at most* A*, the fringe classes and the conditional divergence are bounded, and the bit*
19601 *security holds:*

19602 1. $\ln R \leq A$*;*
19603 2. $\forall k \leq N : \ R_\alpha^{S_k}(P \,\|\, Q)^{\alpha-1} \leq \binom{N}{k} \kappa_C^k \, R^{\alpha-1}$*;*
19604 3. $R_\alpha(P_{S_0} \,\|\, Q_{S_0}) \leq R\,(1 - P(S_0^c))^{-\alpha/(\alpha-1)}$*;*

19607 *4.* $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$.

19608 *Proof.*

DEFINES $A(\hat{K}) := \mathfrak{L}_B(\hat{K}) + \mathfrak{L}_{\bar{\delta}} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$, $\mathfrak{L}_B(\hat{K})$ that of Lemma I.71: the A of Theorem 4.11, precondition 1, at $M_{2\alpha}(\hat{K})$ of Lemma I.71

$\lambda_{\mathcal{F}}(\hat{K})$, the $\lambda_{\mathcal{F}}$ of Definition 5.3 at $A(\hat{K})$, κ_C, $\bar{p}_C$ and M_C

DEFINES $y(\hat{K}) := (2^{-\lambda} e^{Q_s A(\hat{K})})^{(\alpha-1)/\alpha}$ and $y := (2^{-\lambda} e^{Q_s A})^{(\alpha-1)/\alpha}$ (Definition 5.3)

19609 DEFINES $\bar{\delta}(\hat{K})$, $M_{2\alpha}(\hat{K})$ and $\mathfrak{L}_B(\hat{K})$, those of Lemma I.71 at τ, $\bar{e}$, $\bar{T}$ and $\bar{Z}$

DEFINES $W(z) := \sum_{i \le N} \Delta_i(z_{<i})^2/\sigma_i(z_{<i})^2$, Δ_i that of Definition A.27 and σ_i that of Definition A.25

DEFINES $\widetilde{B}_i$ and $\bar{\rho}_B$, those of Definition A.28 at the signer's base sampler, and C_i, the fringe sets of Definition A.26

19610 *Proof of items 1 to 4.*

Proposition 5.9	This proof
Shared: (f, g, F, G), $\tau, \bar{e}, \bar{T}, \bar{Z}$, $\hat{K}$ (Definition 4.6), $\bar{\delta}, W^\circ$ Shared: assumptions A1, A2, A3, A4	
$c, \widetilde{t}_T, z'$	$c, \widetilde{t}_T, z'$ (the statement)
$c \in \{t, t_{\text{frac}}\}$	The statement

Its item 1: the signer is a Falcon-type signer at $(0, \zeta)$
Its item 5: $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$
Its item 6: $\forall z \in S\ \forall i \le N :\ \lvert\delta_i\rvert \le \bar{\delta}(\hat{K})$
Its item 8: $\forall z \in S :\ W(z) \le W^\circ$
Its item 14: $\mathfrak{L}_B(\hat{K}) \le \mathfrak{L}_B$
Its item 15: $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}(\hat{K})$
(I1) Its item 16: $p_\tau \ge 0$
Its item 17: $\forall i \le N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$
Its item 18: $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$
Its item 19: $\forall S' \subseteq S\ \forall I \subseteq \{1, \dots, N\} :\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{\lvert I\rvert}$
Its item 20: $\sigma_{\min} > 0$
Its item 21: $\forall i \le N :\ \sigma_i \in (\sigma_{\min}, \sigma_{\max})$
Its item 22: $\forall i \le N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$
Its item 23: $(1 + \bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$
Its item 24: $\varepsilon_0^\circ < 1$
Its item 25: $p'_\tau + \bar{p}_C < 1$
Its item 26: $\bar{\delta} \in [0, 1)$
Its item 27: $W^\circ \ge 0$

19612 (L1) the signer is a Falcon-type signer at $(0, \zeta)$

19613 [item 1 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

19614 (L2) $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$

19615 [item 5 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

19616 (L3) $\forall z \in S\ \forall i \le N :\ \lvert\delta_i\rvert \le \bar{\delta}(\hat{K})$

19617 [item 6 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

19618 (L4) $\forall z \in S\ \forall i \le N :\ \lvert\delta_i\rvert \le \bar{\delta}$

19619 [(L2), (L3)]

(L5) $\forall z \in S:\ W(z) \le W^\circ$

[item 8 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L6) $\forall i \le N\ \forall z_{<i} \in S_{<i}:\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}(\hat{K})$

[item 15 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L7) $\forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$

[item 17 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L8) $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$

[item 18 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L9) $\sigma_{\min} > 0$

[item 20 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L10) $\forall i \le N:\ \sigma_i \in (\sigma_{\min}, \sigma_{\max})$

[item 21 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L11) $\forall i \le N\ \forall z_{<i}:\ \widetilde{\sigma}_i > \sigma_{\min}$

[item 22 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L12) $(1 + \bar{\delta})^2 < \alpha_L/(\alpha_L - 1)$

[item 23 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L13) $\varepsilon_0^\circ < 1$

[item 24 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L14) $p'_\tau + \bar{p}_C < 1$

[item 25 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L15) $\bar{\delta} \in [0, 1)$

[item 26 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L16) $W^\circ \ge 0$

[item 27 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

Theorem 4.11 at the key's constants $\hat{K}$ and $S' := S$	This proof
the signer, u, ζ	the fixed-point signer, $0, \zeta$ (L1)
$S', \bar{\delta}_{S'}, W^\circ_{S'}$	$S, \bar{\delta}, W^\circ$ (L15), (L16)
$M_{2\alpha}, p_\tau, p'_\tau$	$M_{2\alpha}(\hat{K}), p_\tau, p'_\tau$ (the proof's block; the statement)
A, R	$A(\hat{K}), R$ (precondition 1; the proof's block; Definition A.30)
the signer Falcon-type at (u, ζ)	(L1)
$\bar{\delta}_{S'} \in [0, 1),\ W^\circ_{S'} \ge 0$	(L15), (L16)
$p_\tau \ge 0$	Item 16 of (I1)
$\forall i \le N\ \forall z_{<i} \in S_{<i}:$ $R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le$ $1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}$	(L6)
(I2) $\forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$	(L7)
$\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$	(L8)
precondition 1	$A(\hat{K})$ (the proof's block)
Assumption A1	(L9)
Assumption A2	(L10)
Assumption A3	(L11)
Assumption A4	(L12)
Assumption A5	(L14)
Assumption A6	(L13)
Assumption A7	(L4)
Assumption A8	(L5)

Its item 1: $\ln R \le A$

Its item 2: $\forall k \le N:\ R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k\, R^{\alpha-1}$

Its item 3: $R_\alpha(P_{S_0} \,\|\, Q_{S_0}) \le R\,(1 - P(S_0^c))^{-\alpha/(\alpha-1)}$

(L17) $\forall S' \subseteq S\ \forall I \subseteq \{1,\dots,N\}:\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$

[item 19 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L18) $\forall I \subseteq \{1,\dots,N\}:\ P(\{z \in S : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{|I|}$

[(L17) at $S' := S$]

(L19) $\ln R \le A(\hat{K})$

[item 1 of (I2)]

(L20) $\forall k \le N:\ R_\alpha^{S_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k R^{\alpha-1}$

[item 2 of (I2)]

(L21) $R_\alpha(P_{S_0} \,\|\, Q_{S_0}) \le R\,(1 - P(S_0^c))^{-\alpha/(\alpha-1)}$

[item 3 of (I2)]

(L22) $\mathfrak{L}_B(\hat{K}) \le \mathfrak{L}_B$

[item 14 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L23) $A(\hat{K}) \le A$

[(L22); $A(\hat{K})$ (the proof's block); A (Definition I.62; Theorem 4.11, precondition 1)]

(L24) $\ln R \le A$

[(L19), (L23)]

(L25) $\Rightarrow$ item 1

[(L24)]

(L26) $\Rightarrow$ item 2

[(L20)]

(L27) $\Rightarrow$ item 3

[(L21)]

(L28) $M_{2\alpha}(\hat{K}) \ge 0$

[$M_{2\alpha}(\hat{K})$, the $M_{2\alpha} := (\sqrt{\bar{M}_{\text{tab}}} + \sqrt{\bar{M}_{\text{ar}}})^2$ of Corollary 4.10, precondition 1 (the proof's block; Lemma I.71); $\forall t \in \mathbb{R}:\ t^2 \ge 0$ (Fact A.41, item 13, at $j := 1$)]

Lemma G.79 at $M_{2\alpha}(\hat{K})$ and $S' := S$	This proof
Shared: $\sigma_{\min}, p_\tau,\ \bar{\theta}_{\alpha_L}, \bar{W}_{\alpha_L}$ (Definition I.62)	
$M_{2\alpha}$	$M_{2\alpha}(\hat{K})$ (the proof's block)
$\bar{\delta}_{S'}, W^\circ_{S'}$	$\bar{\delta}, W^\circ$ (L15), (L16)
$p_\tau \ge 0$	Item 16 of (I1)
$\bar{\delta}_{S'} \in [0,1)$	(L15)
$W^\circ_{S'} \ge 0$	(L16)
(I3) $\bar{\theta}_{\alpha_L} \ge 0,\ \forall \delta > -1,\ \lvert\delta\rvert \le \bar{\delta}_{S'}:$ $\theta_{\alpha_L}(\delta) \le \bar{\theta}_{\alpha_L}$	Definition A.30 at $\bar{\delta}$ (Definition I.62)
$\bar{W}_{\alpha_L} > 0,\ \forall \delta > -1,\ \lvert\delta\rvert \le \bar{\delta}_{S'}:$ $\theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \le \bar{W}_{\alpha_L}$	Definition A.30 at $\bar{\delta}$ (Definition I.62)
Assumption A1	(L9)
Assumption A2	(L28)
Assumption A3	(L12)
Assumption A4	(L13)
Its conclusion: $A \ge 0$	

(L29) $A(\hat{K}) \ge 0$

[(I3); $A(\hat{K})$ (the proof's block)]

Theorem 1.2 at every adversary's event A_{adv}	This proof
Shared: R (Definition A.30), A_{adv} (Definition 5.1)	
Shared: $\tau > 1$	
$\lambda, \alpha, Q_s, \tau, M_C$	$\lambda, \alpha, Q_s, \tau, M_C$ (Definition I.62; the statement)
A	$A(\hat{K})$ (the proof's block)
S'	S
$\lambda_{\mathcal{F}}$	$\lambda_{\mathcal{F}}(\hat{K})$ (the proof's block)
$\alpha > 1$	α (Definition I.62)
(I4) $\lambda \in \mathbb{R}$	λ (Definition I.62)
$Q_s \in \mathbb{Z}_{>0}$	Q_s (the statement)
$A \geq 0$	(L29)
$M_C \in \mathbb{Z}_{\geq 0}$	M_C (the statement)
$R > 0$	Theorem 4.11, (L18), (L21), (L22)
A_{adv} an adversary's event at (λ, Q_s)	Definition 5.1
Assumption A1	(L19)
Assumption A2	(L20)
Assumption A3	(L18)
Its conclusion: $P^{\otimes Q_s}(A_{\mathrm{adv}}) \leq 2^{-\lambda_{\mathcal{F}}}$	

(L30) $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \leq 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\mathrm{adv}}) \leq 2^{-\lambda_{\mathcal{F}}(\hat{K})}$

[(I4)]

(L31) $e^{Q_s A(\hat{K})} \leq e^{Q_s A}$

[(L23); $Q_s \in \mathbb{Z}_{>0}$ (the statement); Fact A.41, item 26, at $c := Q_s$; exp increasing (Fact A.41, item 5)]

(L32) $y(\hat{K}) \leq y$

[(L31); $y(\hat{K})$ and y (the proof's block); $t \mapsto t^p$ nondecreasing on $[0, \infty)$ at $p := (\alpha - 1)/\alpha \geq 0$ (Fact A.41, item 5), $\alpha > 1$ (α, Definition I.62); $2^{-\lambda} e^{Q_s A(\hat{K})} > 0$ (Fact A.41, item 12); Fact A.41, item 8]

(L33) $\forall m \leq M_C :\ \min\big(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} y(\hat{K}),\ \binom{Q_s N}{m} \bar{p}_C^m\big) \leq \min\big(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} y,\ \binom{Q_s N}{m} \bar{p}_C^m\big)$

[(L32); Lemma I.64, item 3; Fact A.41, items 8, 40 and 25]

(L34) $\sum_{m=1}^{M_C} \min\big(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} y(\hat{K}),\ \binom{Q_s N}{m} \bar{p}_C^m\big) \leq \sum_{m=1}^{M_C} \min\big(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} y,\ \binom{Q_s N}{m} \bar{p}_C^m\big)$

[(L33) summed over m]

(L35) $\Pi_C(y(\hat{K})) \leq \Pi_C(y)$

[(L34); Π_C (Definition 5.2)]

(L36) $2^{-\lambda_{\mathcal{F}}(\hat{K})} \leq 2^{-\lambda_{\mathcal{F}}}$

[(L32); (L35); Definition 5.3 at $A(\hat{K})$ and at A, the same S, κ_C, $\bar{p}_C$ and M_C; $\lambda_{\mathcal{F}}(\hat{K})$ (the proof's block); $\lambda_{\mathcal{F}}$ (the statement)]

(L37) $\Rightarrow$ item 4

[(L30), (L36)]

□ (items 1 to 4)

I.5.5 The terms on a sub-event of the tail-cut event

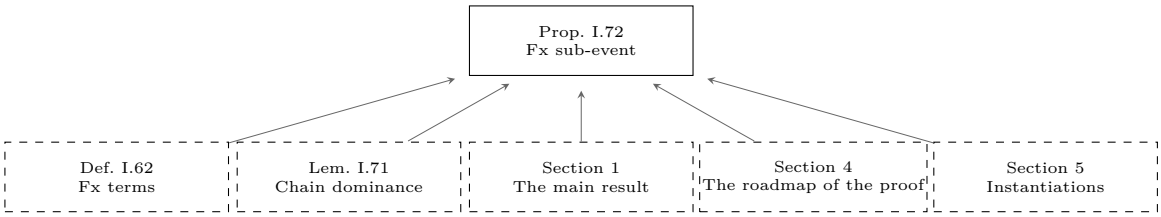


Figure 88: Dependencies, Appendix I.5.5.

Proposition I.72 (The fixed-point signer's bit security on a sub-event [to table])**.** *On a sub-event of the tail-cut event where the leaf sum is at most W° and every leaf's standard deviation perturbation at most $\bar\delta$, the fixed-point signer's signatures keep the bit security those bounds imply, less the event's tail.* ***Under Hypotheses I.21 and I.22****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $c \in \{t, t_{\text{frac}}\}$ *be a center, t and t_{frac} those of Definition 4.5 at the key and* $\mathsf{h}(\mathsf{m})$*;*
- $\bar e, \bar T, \bar Z \in [0, \infty)$*;*
- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$*;*
- $W^\circ \geq 0$*;*
- $\bar\delta \in [0, 1)$*;*
- $E \subseteq \mathbb{Z}^N$*, an event;*
- $\eta_E \geq 0$*;*
- $M_C \in \mathbb{Z}_{\geq 0}$*.*

Define:

- *The signer's words and parameters*
  - $(\lambda, \alpha) := \begin{cases} (128, 257) & n = 512 \\ (256, 513) & n = 1024 \end{cases}$ *(Definition I.62);*
  - $\sigma_{\min}$*, the stored word [L0: fxp/fxp_consts.h: 2073-2084] (Definition I.62);*
- *The coefficient norm*
  - $\|\cdot\|$*, the coefficient norm (Appendix G.5);*
- *The center and the samples*
  - $\widetilde{t}_T$*, the computed value of c in $\mathcal{F}_{\text{fx}}$ (ffSampling$^{\mathcal{F}}$ (Algorithm 10) at* $\mathsf{h}(\mathsf{m})$*, lines 9 to 20 at $c = t$,* center$_{\text{frac}}$ *(Algorithm 17) at $c = t_{\text{frac}}$);*
  - $z' := (z_0, z_1)$*, the sample* ffsamp *(Algorithm 6) returns at c (ffSampling$^{\mathcal{F}}$, line 24);*
- *The probability measures*
  - $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$*, the probability measures of Q_s independent outputs $(z^{(1)}, \ldots, z^{(Q_s)})$ of P and of Q on $(\mathbb{Z}^N)^{Q_s}$ (Fact A.45, item 1);*
- *The leaf perturbations*
  - $\forall z \in \mathbb{Z}^N :\ W(z) := \sum_{i \leq N} \Delta_i(z_{<i})^2 / \sigma_i(z_{<i})^2$*;*
- *The leaf deviations*
  - ε_0*, that of Definition A.38;*
  - $\underline{s} := \sigma_{\min}(1 - \bar\delta)\, \theta_{\alpha_L}(-\bar\delta)^{1/2}$ *and* $\varepsilon_0^\circ := \varepsilon_0(\underline{s})$ *(Definition A.40 at $(\alpha_L, \sigma_{\min}, \bar\delta)$);*
- *The terms*
  - $\mathfrak{L}_B$*, that of Definition I.62;*
  - p'_τ*, that of Corollary 4.10, precondition 3;*
  - $\mathfrak{L}_{\bar\delta}$*, $\mathfrak{L}_\Delta$ and $\mathfrak{L}_\Phi$, those of Theorem 4.11, precondition 1, at $W^\circ_{S'} := W^\circ$ and $\bar\delta_{S'} := \bar\delta$;*
  - $A := \mathfrak{L}_B + \mathfrak{L}_{\bar\delta} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$*;*
  - $\lambda'_{\mathcal{F}}$*, that of Definition 5.3 at A, κ_C, $\bar p_C$, M_C and $S' := S$;*
  - $\lambda_{\mathcal{F}} := -\log_2(2^{-\lambda'_{\mathcal{F}}} + \eta_E)$*.*

Assume:

(A1) $\|\widetilde{t}_T - c\| \leq \bar e$*;*
(A2) $\|c\| \leq \bar T$*;*
(A3) $\forall z \in S :\ \|z'\| \leq \bar Z$*;*
(A4) $p'_\tau < 1$*;*
(A5) $\forall z \in S \cap E :\ W(z) \leq W^\circ$*;*
(A6) $\forall z \in S \cap E\ \forall i \leq N :\ |\delta_i(z_{<i})| \leq \bar\delta$*;*
(A7) $(1 + \bar\delta)^2 < \alpha_L / (\alpha_L - 1)$*;*
(A8) $\varepsilon_0^\circ < 1$*;*
(A9) $Q_s P(S \cap E^c) \leq \eta_E$*.*

Then

$$\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \leq 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \leq 2^{-\lambda_{\mathcal{F}}}.$$

19745 *Proof.*

DEFINES $\lambda''_{\mathcal{F}}$, that of Definition 5.3 at A, κ_C, $\bar{p}_C$, M_C and $S' := S \cap E$

DEFINES $A(\hat{K}) := \mathfrak{L}_B(\hat{K}) + \mathfrak{L}_{\bar{\delta}} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$, $\mathfrak{L}_B(\hat{K})$ that of Lemma I.71: the A of Theorem 4.11, precondition 1, at the key

DEFINES $\lambda''_{\mathcal{F}}(\hat{K})$, that of Definition 5.3 at $A(\hat{K})$, κ_C, $\bar{p}_C$, M_C and $S' := S \cap E$

19746 DEFINES $y(\hat{K}) := (2^{-\lambda} e^{Q_s A(\hat{K})})^{(\alpha-1)/\alpha}$ and $y := (2^{-\lambda} e^{Q_s A})^{(\alpha-1)/\alpha}$ (Definition 5.3)

DEFINES $M_{2\alpha}(\hat{K})$, that of Lemma I.71 at τ, $\bar{e}$, $\bar{T}$ and $\bar{Z}$

DEFINES p_τ, that of Definition I.62

DEFINES $S' := S \cap E$

19747 (L1) $S \cap E \subseteq S$

19748 [Fact A.41, item 17]

19749 (L2) $p'_\tau + \bar{p}_C < 1$

19750 [assumption A4; Lemma I.64, item 3]

Proposition 5.9	This proof
Shared: (f, g, F, G), $\tau, \bar{e}, \bar{T}, \bar{Z}$, $\hat{K}$ (Definition 4.6)	
Shared: assumptions A3, A4	
$c, \widetilde{t}_T, z'$	$c, \widetilde{t}_T, z'$ (the statement)
$c \in \{t, t_{\text{frac}}\}$	The statement
Assumption A1	Assumption A1
Assumption A2	Assumption A2
Its item 15: $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}(\hat{K})$	
19751 (I1) Its item 16: $p_\tau \ge 0$	
Its item 17: $\forall i \le N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$	
Its item 18: $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$	
Its item 19: $\forall S' \subseteq S\ \forall I \subseteq \{1, \dots, N\} :\ P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \le \bar{p}_C^{\lvert I \rvert}$	
Its item 20: $\sigma_{\min} > 0$	
Its item 21: $\forall i \le N :\ \sigma_i \in (\sigma_{\min}, \sigma_{\max})$	
Its item 22: $\forall i \le N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$	
Its item 14: $\mathfrak{L}_B(\hat{K}) \le \mathfrak{L}_B$	

19752 (L3) $\forall i \le N\ \forall z_{<i} \in S_{<i} :\ R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \le 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}(\hat{K})$

19753 [item 15 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

19754 (L4) $\forall i \le N\ \forall z_{<i} :\ \widetilde{B}_i(\mathcal{Z}_i^c) \le p'_\tau$

19755 [item 17 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

19756 (L5) $\bar{\rho}_B \ge (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$

19757 [item 18 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

Theorem 4.11 at the key's constants $\hat{K}$	This proof
the signer, u, ζ	the fixed-point signer, $0, \zeta$ (the statement)
$S', \bar{\delta}_{S'}, W^{\circ}_{S'}$	$S \cap E, \bar{\delta}, W^{\circ}$ (L1); the statement
$M_{2\alpha}, p_\tau, p'_\tau$	$M_{2\alpha}(\hat{K}), p_\tau, p'_\tau$ (the proof's block; the statement)
A, R	$A(\hat{K}), R$ (precondition 1; the proof's block; Definition A.30)
the signer Falcon-type at (u, ζ)	Lemma I.63
$\bar{\delta}_{S'} \in [0, 1),\ W^{\circ}_{S'} \geq 0$	The statement
$p_\tau \geq 0$	Item 16 of (I1)
$\forall i \leq N\ \forall z_{<i} \in S_{<i}$: $R_{2\alpha}^{\mathcal{Z}_i \setminus C_i}(\widetilde{B}_i \,\|\, \widetilde{D}_i)^{\alpha_L} \leq 1 + 2\alpha\, p_\tau + \alpha\, \alpha_L M_{2\alpha}$	(L3)
(I2) $\forall i \leq N\ \forall z_{<i}$: $\widetilde{B}_i(\mathcal{Z}_i^c) \leq p'_\tau$	(L4)
$\bar{\rho}_B \geq (1 - p'_\tau - \bar{p}_C)^{2\alpha/\alpha_L}$	(L5)
precondition 1	$A(\hat{K})$ (the proof's block)
Assumption A1	Item 20 of (I1)
Assumption A2	Item 21 of (I1)
Assumption A3	Item 22 of (I1)
Assumption A4	Assumption A7
Assumption A5	(L2)
Assumption A6	Assumption A8
Assumption A7	Assumption A6
Assumption A8	Assumption A5
Its item 1: $\ln R \leq A$	
Its item 2: $\forall k \leq N$: $R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \leq \binom{N}{k} \kappa_C^k\, R^{\alpha-1}$	

(L6) $\ln R \leq A(\hat{K})$

[item 1 of (I2); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L7) $\forall k \leq N$: $R_\alpha^{S'_k}(P \,\|\, Q)^{\alpha-1} \leq \binom{N}{k} \kappa_C^k\, R^{\alpha-1}$

[item 2 of (I2); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L8) $\forall I \subseteq \{1, \ldots, N\}$: $P(\{z \in S' : \forall i \in I\ z_i \in C_i(z_{<i})\}) \leq \bar{p}_C^{|I|}$

[item 19 of (I1) at S' (the proof's block) by (L1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L9) $M_{2\alpha}(\hat{K}) \geq 0$

[$M_{2\alpha}(\hat{K})$, the $M_{2\alpha} := (\sqrt{\bar{M}_{\text{tab}}} + \sqrt{\bar{M}_{\text{ar}}})^2$ of Corollary 4.10, precondition 1 (the proof's block; Lemma I.71); $\forall t \in \mathbb{R}$: $t^2 \geq 0$ (Fact A.41, item 13, at $j := 1$)]

Lemma G.79 at $M_{2\alpha}(\hat{K})$ and $S' := S \cap E$	This proof
Shared: $\sigma_{\min}$ (the statement), p_τ (the proof's block), $\bar{\theta}_{\alpha_L}, \bar{W}_{\alpha_L}$ (the statement)	
$M_{2\alpha}$	$M_{2\alpha}(\hat{K})$ (the proof's block)
$\bar{\delta}_{S'}, W^{\circ}_{S'}$	$\bar{\delta}, W^{\circ}$ (the statement)
$p_\tau \geq 0$	Item 16 of (I1)
$\bar{\delta}_{S'} \in [0, 1)$	$\bar{\delta} \in [0, 1)$ (the statement)
$W^{\circ}_{S'} \geq 0$	$W^{\circ} \geq 0$ (the statement)
(I3) $\bar{\theta}_{\alpha_L} \geq 0,\ \forall \delta > -1,\ \lvert\delta\rvert \leq \bar{\delta}_{S'}$: $\theta_{\alpha_L}(\delta) \leq \bar{\theta}_{\alpha_L}$	Definition A.30 at $\bar{\delta}$ (the statement)
$\bar{W}_{\alpha_L} > 0,\ \forall \delta > -1,\ \lvert\delta\rvert \leq \bar{\delta}_{S'}$: $\theta_{\alpha_L}(\delta)^{1/2}(1+\delta)^{1-\alpha_L} \leq \bar{W}_{\alpha_L}$	Definition A.30 at $\bar{\delta}$ (the statement)
Assumption A1	Item 20 of (I1)
Assumption A2	(L9)
Assumption A3	Assumption A7
Assumption A4	Assumption A8
Its conclusion: $A \geq 0$	

(L10) $A(\hat{K}) \geq 0$

[(I3); $A(\hat{K})$ (the proof's block)]

Theorem 1.2 at every adversary's event A_{adv}	This proof
Shared: R (Definition A.30), A_{adv} (Definition 5.1)	
Shared: $\tau > 1$	
$\lambda, \alpha, Q_s, \tau, M_C$	$\lambda, \alpha, Q_s, \tau, M_C$ (the statement; Definition I.62)
A	$A(\hat{K})$ (the proof's block)
S'	$S \cap E$ (L1)
$\lambda_{\mathcal{F}}$	$\lambda''_{\mathcal{F}}(\hat{K})$ (the proof's block)
$\alpha > 1$	α (Definition I.62)
(I4) $\lambda \in \mathbb{R}$	λ (Definition I.62)
$Q_s \in \mathbb{Z}_{>0}$	Q_s (the statement)
$A \geq 0$	(L10)
$M_C \in \mathbb{Z}_{\geq 0}$	M_C (the statement)
$R > 0$	Theorem 4.11, (L18), (L21), (L22)
A_{adv} an adversary's event at (λ, Q_s)	Definition 5.1
Assumption A1	(L6)
Assumption A2	(L7)
Assumption A3	(L8)
Its conclusion: $P^{\otimes Q_s}(A_{\mathrm{adv}}) \leq 2^{-\lambda_{\mathcal{F}}}$	

(L11) $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \leq 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\mathrm{adv}}) \leq 2^{-\lambda''_{\mathcal{F}}(\hat{K})}$

[(I4); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L12) $\mathfrak{L}_B(\hat{K}) \leq \mathfrak{L}_B$

[item 14 of (I1); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L13) $A(\hat{K}) \leq A$

[(L12); $A(\hat{K})$ (the proof's block); A (the statement)]

(L14) $e^{Q_s A(\hat{K})} \leq e^{Q_s A}$

[(L13); $Q_s \geq 1$ (Q_s, the statement); Fact A.41, item 26, at $c := Q_s$; exp increasing (Fact A.41, item 5)]

(L15) $y(\hat{K}) \leq y$

[(L14); $y(\hat{K})$ and y (the proof's block); $t \mapsto t^p$ nondecreasing on $[0, \infty)$ at $p := (\alpha - 1)/\alpha \geq 0$ (Fact A.41, item 5), $\alpha > 1$ (α, Definition I.62); $2^{-\lambda} e^{Q_s A(\hat{K})} > 0$ (Fact A.41, item 12); Fact A.41, item 8]

(L16) $\forall m \leq M_C :\ \min\big(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} y(\hat{K}),\ \binom{Q_s N}{m} \bar{p}_C^m\big) \leq \min\big(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} y,\ \binom{Q_s N}{m} \bar{p}_C^m\big)$

[(L15); Lemma I.64, item 3; Fact A.41, items 8, 40 and 25]

(L17) $\sum_{m=1}^{M_C} \min\big(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} y(\hat{K}),\ \binom{Q_s N}{m} \bar{p}_C^m\big) \leq \sum_{m=1}^{M_C} \min\big(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha} y,\ \binom{Q_s N}{m} \bar{p}_C^m\big)$

[(L16) summed over m]

(L18) $\Pi_C(y(\hat{K})) \leq \Pi_C(y)$

[(L17); Π_C (Definition 5.2)]

(L19) $2^{-\lambda''_{\mathcal{F}}(\hat{K})} \leq 2^{-\lambda''_{\mathcal{F}}}$

[(L15); (L18); Definition 5.3 at $A(\hat{K})$ and at A, the same $S' := S \cap E$, κ_C, $\bar{p}_C$ and M_C; $\lambda''_{\mathcal{F}}(\hat{K})$ and $\lambda''_{\mathcal{F}}$ (the proof's block)]

(L20) $2^{-\lambda''_{\mathcal{F}}} = 2^{-\lambda'_{\mathcal{F}}} + Q_s P((S \cap E)^c) - Q_s P(S^c)$

[$\lambda''_{\mathcal{F}}$ (the proof's block) and $\lambda'_{\mathcal{F}}$ (the statement), Definition 5.3 at the same A, κ_C, $\bar{p}_C$ and M_C]

(L21) $(S \cap E)^c = S^c \cup E^c$

[Fact A.41, item 17, at $(A, B) := (S, E^c)$; $S \setminus E^c = S \cap E$ (expand)]

(L22) $E^c \subseteq (E^c \cap S) \cup S^c$

[Fact A.41, item 17, at $(A, B) := (E^c, S)$]

(L23) $\Rightarrow\ (S \cap E)^c \subseteq S^c \cup (S \cap E^c)$

[(L21), (L22)]

(L24) $\Rightarrow\ P((S \cap E)^c) \leq P(S^c) + P(S \cap E^c)$

[(L23); Fact A.45, items 12 and 5]

(L25) $\Rightarrow$ $Q_s P((S \cap E)^c) - Q_s P(S^c) \le \eta_E$

[(L24) times Q_s (the statement); assumption A9]

(L26) $\Rightarrow$ $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda'_{\mathcal{F}}} + \eta_E$

[(L11), (L19), (L20), (L25)]

(L27) $\Rightarrow$ $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$

[(L26); $2^{-\lambda_{\mathcal{F}}} = 2^{-\lambda'_{\mathcal{F}}} + \eta_E$ ($\lambda_{\mathcal{F}}$, the statement; $\log_2 = \ln / \ln 2$; Fact A.41, item 28, at $y := 2^{-\lambda'_{\mathcal{F}}} + \eta_E$); $2^{-\lambda'_{\mathcal{F}}} > 0$ (Fact A.41, item 12); $\eta_E \ge 0$ (the statement)]

(L28) $\Rightarrow$ the statement

[(L27)]

□

I.5.6 The leaf sum under a fixed key

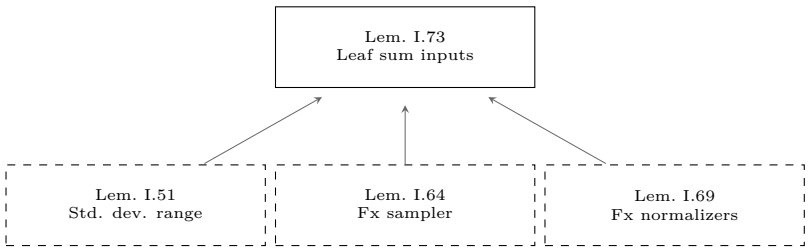


Figure 89: Dependencies, Appendix I.5.6.

Statistics I.23, items 10 and 11, states that every key of the sample meets each center's thresholds.

Lemma I.73 (The fixed-point signer's leaf sum inputs [to table])**.** *At a checked key and either center, the fixed-point signer meets the realization, the key, the normalizer deviation, the fringe sets and the range of the leaf standard deviations that Lemmas 4.13 and 4.14 take. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5) of degree* n*;*
- $t_{\text{c}} \in \{t, t_{\text{frac}}\}$ *be a center,* t *and* t_{frac} *those of Definition 4.5 at the key and* $\mathsf{h}(\mathsf{m})$*.*

Define:

- $\sigma_{\min}$ *and* ϵ*, those of Definition I.62 at the key;*
- $\forall s > 0\ \forall c, x \in \mathbb{R} :\ \rho_{s,c}(x) := e^{-(x-c)^2/(2s^2)}$ *(Definition A.2 at* $k := 1$*);*
- $\forall s > 0\ \forall c \in \mathbb{R} :\ \rho_{s,c}(\mathbb{Z}) := \sum_{x \in \mathbb{Z}} \rho_{s,c}(x)$ *(Definition A.2 at* $k := 1$ *and* $A := \mathbb{Z}$*);*
- $\forall i \le N :\ \widetilde{\sigma}_i$*, that of Definition A.25 at* $\mathcal{F}_{\text{fx}}$*, the key,* $\mathsf{h}(\mathsf{m})$ *and* t_{c}*;*
- $\forall i \le N :\ C_i(z_{<i})$*, the fringe sets of the fixed-point signer's base sampler (Definition A.26).*

Then $\mathcal{F}_{\text{fx}}$ *is the realization of a Falcon-type signer, the key is a key of that signer, and the normalizer deviation, the fringe sets and the leaf standard deviations meet the leaf sum's assumptions:*

1. $\mathcal{F}_{\text{fx}}$ *is the realization of a Falcon-type signer at* $(u, \zeta) = (0, 2^{-64})$ *(Definition 4.5);*
2. (f, g, F, G) *is a key of degree* n *of that signer (Definition 4.6);*
3. $\epsilon \in [0, 1)$*;*
4. $\forall i \le N\ \forall z_{<i}\ \forall c \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$*;*
5. $\forall i \le N\ \forall z_{<i} :\ C_i(z_{<i}) = \emptyset$*;*
6. $\sigma_{\min} > 0$*;*
7. $\forall i \le N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$*.*

Proof. Proof of items 1 to 7.

(L1) $(u, \zeta) = (0, 2^{-64})$
[Definition I.1]

(L2) $u \in [0, 1)$
[(L1)]

(L3) $\mathcal{F}_{\text{fx}}$ is the realization of a Falcon-type signer at $(0, 2^{-64})$
[Definition 4.5 at $\mathcal{F} := \mathcal{F}_{\text{fx}}$ (Definition A.4, item 8), keygen (Algorithm 11) and SamplerZ (Algorithm 8) with BerExp (Algorithm 9); (L1), (L2)]

(L4) $\Rightarrow$ item 1
[(L3)]

(L5) (f, g, F, G) is a key of degree n of that signer
[Definition 5.5, item 1; keygen (Algorithm 11), line 8; Definition 4.6]

(L6) $\Rightarrow$ item 2
[(L5)]

(L7) $\epsilon \in [0, 1)$
[Lemma I.69, item 1, at the checked key]

(L8) $\Rightarrow$ item 3
[(L7)]

(L9) $\forall i \leq N\ \forall z_{<i}\ \forall c \in \mathbb{R}:\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$
[Lemma I.69, item 2, at the checked key and the center t_{c}]

(L10) $\Rightarrow$ item 4
[(L9)]

(L11) $\forall i \leq N\ \forall z_{<i}:\ C_i(z_{<i}) = \emptyset$
[Lemma I.64, item 2, at the checked key]

(L12) $\Rightarrow$ item 5
[(L11)]

(L13) $\sigma_{\min} > 0$
[the stored word `FXP_SIGMA_MIN` [L0: `fxp/fxp_consts.h:2073-2084`]; $\sigma_{\min}$ (Definition I.62)]

(L14) $\Rightarrow$ item 6
[(L13)]

Lemma I.51, item 1 at every $i \leq N$ and $z_{<i}$	This proof
Shared: (f, g, F, G), $\sigma_{\min}$	
(I1) `isigma`	$1/\widetilde{\sigma}_i$ (the statement; Definition A.25)
$n \in \{512, 1024\}$	Definition 5.5, item 1
`isigma` taken by a call of SamplerZ by deepest	The i-th call of ffSampling$^{\mathcal{F}}$ at t_{c} (Definition A.25), at deepest (Algorithm 7)
Its conclusion: $\widetilde{\sigma} > \sigma_{\min}$	

(L15) $\forall i \leq N\ \forall z_{<i}:\ \widetilde{\sigma}_i > \sigma_{\min}$
[(I1)]

(L16) $\Rightarrow$ item 7
[(L15)]

□ (items 1 to 7)

I.6 ffSampling$^{\mathcal{F}}(B, s, t)$

The bit security of this version. Its level under **Hypotheses I.21 and I.22**, at a key within three thresholds, is Theorem 1.3's at the center t, read at the tail of Lemma 4.14 (Table 34).

Structure. Appendix I.6.1 states the shift at the root node's entry; Appendix I.6.2 the loss.

I.6.1 The shift at the root node's entry

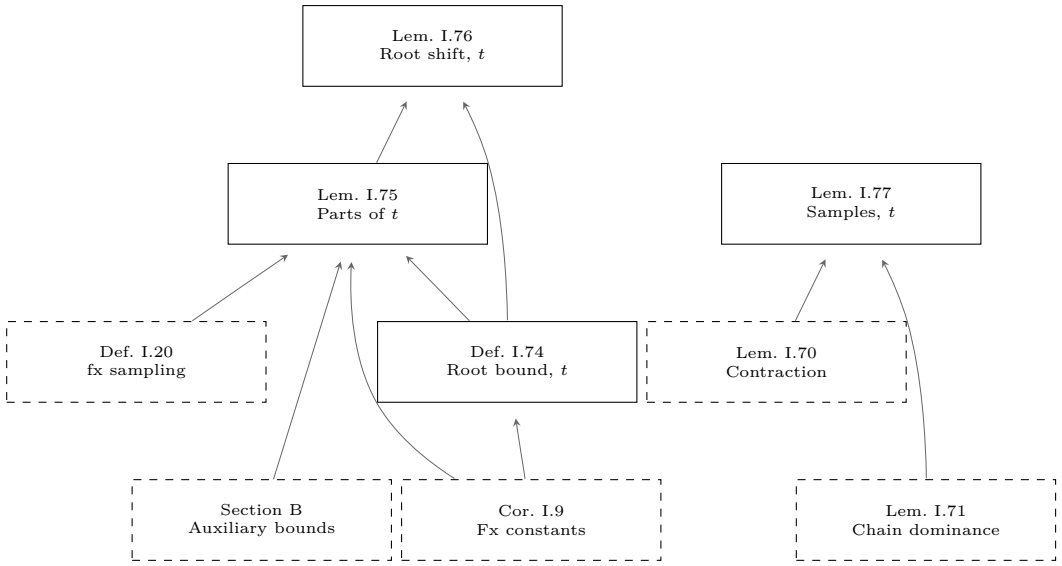


Figure 90: Dependencies, Appendix I.6.1.

Definition I.74 (The root node's entry bound at the center t [to table])**.** Let:

- $\gamma', \delta \in [0, \infty)$.

Define:

- The signer's words and parameters
  - h and $n := 2^h$, those of FFT, Precondition;
  - $\zeta_{\mathrm{op}} := 2^{-65}$ (Definition I.1);
  - P, that of FFT (Algorithm 14), line 1;
  - H, that of ffSampling$^{\mathcal{F}}$ (Algorithm 10), lines 9 to 19;
- The center shifts
  - $c_{\mathrm{merge}} := \sqrt{2}\,\zeta$ and $k_E := 8\sqrt{2}$ (Corollary I.9, items 5 and 6, at $u := 0$);
  - $R_{h-1} := (1 + c_{\mathrm{merge}})^{h-1} - 1$;
  - $A_0 := 0$;
  - $\forall j < h - 1 :\ A_{j+1} := \sqrt{2}(1 + c_{\mathrm{merge}})A_j + k_E\,\zeta\sqrt{P}$;
  - $\delta_{\mathsf{h}(\mathsf{m})} := R_{h-1}\,nq/\sqrt{2} + A_{h-1}$;
- The entry shifts
  - $e_p(\gamma', \delta) := H\delta + \gamma'\delta_{\mathsf{h}(\mathsf{m})} + \delta_{\mathsf{h}(\mathsf{m})}\delta + 3\sqrt{2}\,\zeta$;
  - $e_t(\gamma', \delta) := e_p(\gamma', \delta)(1/q + \zeta_{\mathrm{op}}) + H\gamma'\zeta_{\mathrm{op}} + \sqrt{2}\,\zeta_{\mathrm{op}}$.

Lemma I.75 (The center t's parts at the root node's entry [to table])**.** *The computed center's parts lie within e_t of their values over $\mathbb{R}$. Define:*

- *h and $n := 2^h$, those of FFT (Algorithm 14), Precondition;*
- *$\Psi_n := \{\psi_k : k < n/2\}$, that of Fact A.43 at $m := n$.*

Let:

- *(f, g, F, G) be a checked key (Definition 5.5);*
- *$\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$ be a hashed message (Definition A.25);*
- *$\psi \in \Psi_n$.*

Define:

- *The signer's words and parameters*
  - *H, c_{merge}, k_E, P and ζ_{op}, those of Definition I.74;*

- *The center shifts*
  - $A_0 := 0$ *and* $\forall j < h-1 :\ A_{j+1} := \sqrt{2}(1+c_{\text{merge}})A_j + k_E\,\zeta\sqrt{P}$ *(Definition I.74);*
  - $R_{h-1} := (1+c_{\text{merge}})^{h-1} - 1$ *and* $\delta_{\mathsf{h}(\mathsf{m})} := R_{h-1}\,nq/\sqrt{2} + A_{h-1}$ *(Definition I.74);*
- *The Gram deltas*
  - $\check{\gamma}_{fg}$ *and* $\check{\gamma}_{FG}$*, those of Definition A.36;*
  - $\delta_{fg} := R_{h-1}(\check{\gamma}_{fg}\sqrt{n/2} + A_{h-1})/(1-R_{h-1}) + A_{h-1}$ *(Definition A.36);*
  - $\delta_{FG} := R_{h-1}(\check{\gamma}_{FG}\sqrt{n/2} + A_{h-1})/(1-R_{h-1}) + A_{h-1}$ *(Definition A.36);*
  - $\gamma'_{fg} := \check{\gamma}_{fg} + \delta_{fg}$ *and* $\gamma'_{FG} := \check{\gamma}_{FG} + \delta_{FG}$ *(Definition A.36);*
- *The center*
  - $\hat{h}$, $\hat{f}$, $\hat{F}$, b *and* t*, those of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10) at* $\mathsf{h}(\mathsf{m})$*, lines 9 to 19;*
  - $\widetilde{\hat{h}}$, $\widetilde{b}$, $\widetilde{(1/q)}$ *and* $\widetilde{t}$*, the values* ffSampling$^{\mathcal{F}}$ *computes in* $\mathcal{F}_{\text{fx}}$ *(lines 9 to 20)* `[LO: sign_fpoly.c: 2663-2712]`*;*
- *The entry shifts*
  - $e_p(\gamma', \delta) := H\delta + \gamma'\delta_{\mathsf{h}(\mathsf{m})} + \delta_{\mathsf{h}(\mathsf{m})}\delta + 3\sqrt{2}\,\zeta$ *(Definition I.74);*
  - $e_t(\gamma', \delta) := e_p(\gamma', \delta)(1/q + \zeta_{\text{op}}) + H\gamma'\zeta_{\text{op}} + \sqrt{2}\,\zeta_{\text{op}}$ *(Definition I.74).*

Then

1. $|\widetilde{t}_0(\psi) - t_0(\psi)| \le e_t(\gamma'_{FG}, \delta_{FG})$*;*
2. $|\widetilde{t}_1(\psi) - t_1(\psi)| \le e_t(\gamma'_{fg}, \delta_{fg})$*.*

Proof.

DEFINES $(b_0, \gamma'_0, \delta_0, c_0) := (b_{11}, \gamma'_{FG}, \delta_{FG}, 1/q)$ and $(b_1, \gamma'_1, \delta_1, c_1) := (b_{01}, \gamma'_{fg}, \delta_{fg}, -1/q)$, b_{01} and b_{11} the entries of b (the statement)

$(\widetilde{b}_0, \widetilde{c}_0) := (\widetilde{b}_{11}, \widetilde{(1/q)})$ and $(\widetilde{b}_1, \widetilde{c}_1) := (\widetilde{b}_{01}, \widetilde{(-1/q)})$, the values ffSampling$^{\mathcal{F}}$ (Algorithm 10) computes, lines 16 and 18

$\forall j \in \{0,1\} :\ t_j = \hat{h}b_jc_j$ (ffSampling$^{\mathcal{F}}$, lines 17 and 19)

DEFINES $\widetilde{\hat{f}}$ and $\widetilde{\hat{F}}$, the images keychecks (Algorithm 12) computes in $\mathcal{F}_{\text{fx}}$, line 1

(I1)

Lemma H.12 at ψ	This proof
Shared: $\zeta,\ h, n,\ P,\ R_{h-1}, A_{h-1}$ (Definition I.74)	
$\mathcal{F}$	$\mathcal{F}_{\text{fx}}$ (Definition I.1)
u	0
f	$\mathsf{h}(\mathsf{m})$ (the statement)
$\hat{f}_k, \widetilde{\hat{f}}_k$	$\hat{h}(\psi), \widetilde{\hat{h}}(\psi)$ (FFT (Algorithm 14), Post; the statement)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\text{fx}}$ at $(0, \zeta)$ (Definition I.1)
$f_{[a]} \in \mathcal{F},\ a < n$	$\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ (the statement); Definition A.4, item 8
$k < n/2$	The position of ψ (FFT, Post)
Its conclusion: $\forall k < n/2 :\ \lvert\widetilde{\hat{f}}_k - \hat{f}_k\rvert \le R_{h-1}\lVert\hat{f}\rVert + A_{h-1}$	

(L1) $|\widetilde{\hat{h}}(\psi) - \hat{h}(\psi)| \le R_{h-1}\left(\sum_{\psi' \in \Psi_n} |\hat{h}(\psi')|^2\right)^{1/2} + A_{h-1}$

[(I1); the array's indexing a bijection of its $n/2$ entries onto the roots [gate: `verify/gates/tree/tower_index.py`], the fixed-point twiddles indexed by the same k (Definition I.1, item 4)]

(I2)

Proposition G.15 at $f := \mathsf{h}(\mathsf{m})$	This proof
Shared: n, h	
f	$\mathsf{h}(\mathsf{m})$ (the statement)
$h \ge 1$	$h \in \{1, \dots, 10\}$ (FFT (Algorithm 14), Precondition)
$f \in \mathbb{R}[x]/(x^n+1)$	$\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ (the statement)
Its conclusion: $\sum_{p<n} f_{[p]}^2 = \frac{2}{n}\sum_{k<n/2} \lvert f(\psi_k)\rvert^2$	

(L2) $\sum_{\psi' \in \Psi_n} |\hat{h}(\psi')|^2 = (n/2)\|\mathsf{h}(\mathsf{m})\|^2$
[(I2); Ψ_n (the statement); $\hat{h} = \mathrm{FFT}(\mathsf{h}(\mathsf{m}))$ (ffSampling$^{\mathcal{F}}$, line 10); $\|\mathsf{h}(\mathsf{m})\|$, the coefficient norm (Definition A.1)]

(L3) $\|\mathsf{h}(\mathsf{m})\|^2 < nq^2$
[$\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$ (the statement)]

(L4) $\sum_{\psi' \in \Psi_n} |\hat{h}(\psi')|^2 < (n/2)nq^2$
[(L2), (L3)]

(L5) $R_{h-1} \geq 0$
[$R_{h-1} = (1 + c_{\mathrm{merge}})^{h-1} - 1$ and $c_{\mathrm{merge}} = \sqrt{2}\zeta$ (Definition I.74); $\zeta \geq 0$ ($\zeta := 2\zeta_{\mathrm{op}}$, Definition I.1); $h \geq 1$ (FFT (Algorithm 14), Precondition); $t \mapsto t^p$ nondecreasing on $[0, \infty)$ at $p := h - 1$ (Fact A.41, item 5)]

(L6) $\Rightarrow \ |\widetilde{\hat{h}}(\psi) - \hat{h}(\psi)| \leq \delta_{\mathsf{h}(\mathsf{m})}$
[(L1), (L4), (L5); $\delta_{\mathsf{h}(\mathsf{m})}$ (Definition I.74); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5); Fact A.41, item 26]

(L7) $|\hat{h}(\psi)| \leq \|\mathsf{h}(\mathsf{m})\|_1$
[Fact A.42, item 3, at $f := \mathsf{h}(\mathsf{m})$; $\hat{h} = \mathrm{FFT}(\mathsf{h}(\mathsf{m}))$ (ffSampling$^{\mathcal{F}}$, line 10)]

(L8) $\|\mathsf{h}(\mathsf{m})\|_1 < nq$
[$\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$ (the statement)]

(L9) $|\hat{h}(\psi)| \leq H$
[(L7), (L8); H (ffSampling$^{\mathcal{F}}$, line 11)]

(L10) $k_E\, \zeta \sqrt{P} = 4\sqrt{2}\, \zeta \sqrt{n}$
[$k_E = 8\sqrt{2}$ (Definition I.74); $P = n/4$ (FFT (Algorithm 14), line 1); expand]

(L11) $\forall j: \ |b_j(\psi)| \leq \gamma'_j$
[(the proof's block); $(b_{01}, b_{11}) = (-\hat{f}, -\hat{F})$ (b, the statement); Lemma H.18, items 1 and 2, at ψ (the statement), its R_{h-1} and A_{h-1} (Definition A.36) the statement's by $c_{\mathrm{merge}} = \sqrt{2}\zeta$ (Definition I.74) and (L10); $|-x| = |x|$ (Fact A.41, item 1)]

(L12) $\forall \psi \in \Psi_n: \ (\widetilde{b}_{01}(\psi), \widetilde{b}_{11}(\psi)) = (-\widetilde{\hat{f}}(\psi), -\widetilde{\hat{F}}(\psi))$
[ffSampling$^{\mathcal{F}}$ (Algorithm 10), the line after line 11: the images of keychecks (Algorithm 12), line 1, negated [L0: `fxp/kgen_fx.c:71-78`] [L0: `fxp/sign_fxcore.c:24-42`] (Lemma I.10, item 10); $\widetilde{\hat{f}}$, $\widetilde{\hat{F}}$ (the proof's block)]

(L13) $\forall j: \ |\widetilde{b}_j(\psi) - b_j(\psi)| \leq \delta_j$
[(the proof's block); (L12); $(b_{01}, b_{11}) = (-\hat{f}, -\hat{F})$ (b, the statement); Lemma H.18, item 3, at ψ (the statement), its R_{h-1} and A_{h-1} the statement's by $c_{\mathrm{merge}} = \sqrt{2}\zeta$ (Definition I.74) and (L10); $|-x| = |x|$ (Fact A.41, item 1)]

Corollary I.9, item 1	This proof
Shared: ζ	
(I3) $\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0, \zeta)$ (Definition I.1)
Its conclusion: $k_B = 3\sqrt{2}$	

Lemma B.2, item 3 at every $j \in \{0, 1\}$	This proof
Shared: ζ	
$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
(I4) a, b	$\widetilde{\hat{h}}, \widetilde{b}_j$ (the statement; the proof's block)
k_B	$3\sqrt{2}$ (I3)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0, \zeta)$ (Definition I.1)
$a, b \in C_{\mathcal{F}}$	$\widetilde{\hat{h}}$, $\widetilde{b}_j$, computed in $\mathcal{F}_{\mathrm{fx}}$ (the statement)
Its item 3: $(a \otimes b)\, \mathcal{I}\left(\left(\sqrt{2}u(2+u)\right)^{\pm}, k_B \zeta^{\pm}\right) ab$	

(L14) $\forall j\ \exists e_B \in \mathbb{C},\ |e_B| \le 3\sqrt{2}\,\zeta :\ \widetilde{\hat{h}} \otimes \widetilde{b}_j = \widetilde{\hat{h}}\widetilde{b}_j + e_B$

[(I4)]

(L15) $\forall x, \widetilde{x}, y, \widetilde{y} \in \mathbb{C} :\ \widetilde{x}\widetilde{y} - xy = x(\widetilde{y} - y) + y(\widetilde{x} - x) + (\widetilde{x} - x)(\widetilde{y} - y)$

[expand]

(L16) $\forall j :\ |\widetilde{\hat{h}} \otimes \widetilde{b}_j - \hat{h}b_j| \le H\delta_j + \gamma'_j\delta_{\mathsf{h}(\mathsf{m})} + \delta_{\mathsf{h}(\mathsf{m})}\delta_j + 3\sqrt{2}\,\zeta$

[(L15); (L6), (L9), (L11), (L13), (L14); $|x+y| \le |x| + |y|$ (Fact A.41, item 1); Fact A.41, item 8]

(L17) $\Rightarrow\ \forall j :\ |\widetilde{\hat{h}} \otimes \widetilde{b}_j - \hat{h}b_j| \le e_p(\gamma'_j, \delta_j)$

[(L16); e_p (Definition I.74)]

(L18) $\forall j\ \exists \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \le \zeta_{\mathrm{op}} :\ \widetilde{c}_j = c_j + \zeta_\circ$

[Definition I.20; $\widetilde{(-1/q)} = -\widetilde{(1/q)}$ [L0: `fxp/fxp_consts.h:2090-2091`]; $(\widetilde{c}_j, c_j)$ (the proof's block)]

(L19) $\forall j\ \exists \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \le \zeta_{\mathrm{op}},\ \exists e_c \in \mathbb{C},\ |e_c| \le \sqrt{2}\,\zeta_{\mathrm{op}} :\ \widetilde{t}_j = (\widetilde{\hat{h}} \otimes \widetilde{b}_j)\,(c_j + \zeta_\circ) + e_c$

[(L18); ffSampling$^{\mathcal{F}}$, lines 16 and 18; $c \otimes a$ (Definition A.8); Definition I.1, item 1]

(L20) $\forall j :\ |\hat{h}(\psi)b_j(\psi)| \le H\gamma'_j$

[(L9), (L11); $|xy| = |x||y|$ (Fact A.41, item 1); Fact A.41, item 8]

(L21) $\forall j :\ |\widetilde{t}_j - t_j| \le e_p(\gamma'_j, \delta_j)(1/q + \zeta_{\mathrm{op}}) + H\gamma'_j\zeta_{\mathrm{op}} + \sqrt{2}\,\zeta_{\mathrm{op}}$

[(L17), (L19), (L20); $t_j = \hat{h}b_jc_j$ and $|c_j| = 1/q$ (the proof's block)]

(L22) $\Rightarrow\ \forall j :\ |\widetilde{t}_j - t_j| \le e_t(\gamma'_j, \delta_j)$

[(L21); e_t (Definition I.74); (γ'_j, δ_j) (the proof's block)]

(L23) $\Rightarrow$ item 1

[(L22)]

(L24) $\Rightarrow$ item 2

[(L22)]

□ (items 1 and 2)

Lemma I.76 (The root entry shift at the center t [to table])**.** *The shift at the root node's entry is at most* $(e_t(\gamma'_{FG}, \delta_{FG})^2 + e_t(\gamma'_{fg}, \delta_{fg})^2)^{1/2}$*. Let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The signer's words and parameters*
  - h *and* $n := 2^h$*, those of* FFT *(Algorithm 14), Precondition;*
  - H, c_{merge}, k_E, P *and* ζ_{op}*, those of Definition I.74;*
- *The center shifts*
  - $A_0 := 0$ *and* $\forall j < h-1 :\ A_{j+1} := \sqrt{2}(1 + c_{\mathrm{merge}})A_j + k_E\,\zeta\sqrt{P}$ *(Definition I.74);*
  - $R_{h-1} := (1 + c_{\mathrm{merge}})^{h-1} - 1$ *and* $\delta_{\mathsf{h}(\mathsf{m})} := R_{h-1}\,nq/\sqrt{2} + A_{h-1}$ *(Definition I.74);*
- *The Gram deltas*
  - $\check{\gamma}_{fg}$ *and* $\check{\gamma}_{FG}$*, those of Definition A.36;*
  - $\delta_{fg} := R_{h-1}(\check{\gamma}_{fg}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$ *(Definition A.36);*
  - $\delta_{FG} := R_{h-1}(\check{\gamma}_{FG}\sqrt{n/2} + A_{h-1})/(1 - R_{h-1}) + A_{h-1}$ *(Definition A.36);*
  - $\gamma'_{fg} := \check{\gamma}_{fg} + \delta_{fg}$ *and* $\gamma'_{FG} := \check{\gamma}_{FG} + \delta_{FG}$ *(Definition A.36);*
- *The center*
  - t*, that of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10) at* $\mathsf{h}(\mathsf{m})$*, lines 9 to 19;*
  - $\widetilde{t}$*, its computed value in* $\mathcal{F}_{\mathrm{fx}}$ *(lines 9 to 20);*
  - e_{root}*, that of* ffSampling$^{\mathcal{F}}$*, line 20;*
- *The entry shifts*
  - $e_p(\gamma', \delta) := H\delta + \gamma'\delta_{\mathsf{h}(\mathsf{m})} + \delta_{\mathsf{h}(\mathsf{m})}\delta + 3\sqrt{2}\,\zeta$ *(Definition I.74);*
  - $e_t(\gamma', \delta) := e_p(\gamma', \delta)(1/q + \zeta_{\mathrm{op}}) + H\gamma'\zeta_{\mathrm{op}} + \sqrt{2}\,\zeta_{\mathrm{op}}$ *(Definition I.74);*
- *The terms*
  - $\bar{e} := (e_t(\gamma'_{FG}, \delta_{FG})^2 + e_t(\gamma'_{fg}, \delta_{fg})^2)^{1/2}$.

Then

$$\|e_{\mathrm{root}}\| \le \bar{e}.$$

Proof.

DEFINES Ψ_n, that of Fact A.43 at $m := n$

Proposition G.15 at $f := \widetilde{t}_0 - t_0$ and at $f := \widetilde{t}_1 - t_1$	This proof
Shared: n, h	
(I1) f	$\widetilde{t}_0 - t_0, \widetilde{t}_1 - t_1$ (the statement)
$h \ge 1$	$h \in \{1, \dots, 10\}$ (FFT (Algorithm 14), Precondition)
$f \in \mathbb{R}[x]/(x^n + 1)$	$\widetilde{t}, t$ (the statement); $\mathcal{R}_n := \mathbb{R}[x]/(x^n + 1)$ (Definition A.1)
Its conclusion: $\sum_{p<n} f_{[p]}^2 = \frac{2}{n} \sum_{k<n/2} \lvert f(\psi_k)\rvert^2$	

(L1) $\|(\widetilde{t}_0, \widetilde{t}_1) - (t_0, t_1)\|^2 = \frac{2}{n} \sum_{\psi \in \Psi_n} (|\widetilde{t}_0(\psi) - t_0(\psi)|^2 + |\widetilde{t}_1(\psi) - t_1(\psi)|^2)$
[(I1); Ψ_n (the proof's block); $\|(X, Y)\|^2 := \|X\|^2 + \|Y\|^2$ (Fact A.41, its lead); $\|\cdot\|$, the coefficient norm (Appendix G.5)]

(L2) $\frac{2}{n} \sum_{\psi \in \Psi_n} (|\widetilde{t}_0(\psi) - t_0(\psi)|^2 + |\widetilde{t}_1(\psi) - t_1(\psi)|^2) \le e_t(\gamma'_{FG}, \delta_{FG})^2 + e_t(\gamma'_{fg}, \delta_{fg})^2$
[Lemma I.75, items 1 and 2, at the checked key and at every $\psi \in \Psi_n$ (the proof's block); Fact A.41, item 5, at $p := 2$]

(L3) $\Rightarrow$ $\|e_{\mathrm{root}}\| \le (e_t(\gamma'_{FG}, \delta_{FG})^2 + e_t(\gamma'_{fg}, \delta_{fg})^2)^{1/2}$
[(L1), (L2); $e_{\mathrm{root}} = (\widetilde{t}_0, \widetilde{t}_1) - (t_0, t_1)$ (ffSampling$^{\mathcal{F}}$, line 20); Fact A.41, item 5, at $p := 1/2$]

(L4) $\Rightarrow$ the statement
[(L3); $\bar{e}$ (the statement)]

□

Lemma I.77 (Sample norms at the center t [to table])**.** *At the center t, the fixed-point signer's samples on the tail-cut event have norm at most $\bar{Z}$. **Under Hypotheses I.21 and I.22**, let:*

- *(f, g, F, G) be a checked key (Definition 5.5);*
- *$\tau \in (1, \infty)$.*

Define:

- *The signer's words and parameters*
  - *h and $n := 2^h$, those of FFT (Algorithm 14), Precondition;*
- *The key bounds*
  - *d_{hi}, M_0 and $\bar{g}_{11}$, those of Proposition 5.8;*
  - *$\bar{\Xi}_0 := (d_{\mathrm{hi}}(M_0 + \bar{g}_{11}))^{1/2}/q$ (Lemma H.21);*
- *The leaf deviations*
  - *$\sigma_{\min}$ and χ_σ^ζ, those of Definition I.62;*
  - *$\sigma_{\max} := 1.17^2 \sigma_{\min}$ and $\bar{\delta} := \chi_\sigma^\zeta/(1 - \chi_\sigma^\zeta)$ (Definition I.62);*
- *The center and the samples*
  - *t, that of ffSampling$^{\mathcal{F}}$ (Algorithm 10) at $\mathsf{h}(\mathsf{m})$, lines 9 to 19;*
  - *$\widetilde{t}_T$, its computed value in $\mathcal{F}_{\mathrm{fx}}$ (lines 9 to 20);*
  - *$z' := (z_0, z_1)$, the sample ffsamp (Algorithm 6) returns at t (ffSampling$^{\mathcal{F}}$, line 24);*
- *The center shifts*
  - *$\bar{\Xi}'$, $\bar{\Xi}$, $\bar{\Xi}'_{\mathrm{root}}$, G_γ, c_S, Υ_k, c_{split}, G_X, R°, Θ_k, G_Z and M_k, those of Definition I.62;*
  - *$\gamma := \bar{\Xi}'(1 + 2(h-1)\bar{\Xi})\, G_\gamma$ and $\gamma_S := c_S \bar{\Xi}' \sum_{k=1}^h \Upsilon_k$ (Definition I.62);*
- *The terms*
  - *γ'_{fg} and γ'_{FG}, those of Definition A.36;*
  - *$\bar{T} := (n(\gamma'^2_{FG} + \gamma'^2_{fg}))^{1/2}$ (Lemma H.22);*
  - *$\bar{e}$, the bound of Lemma I.76;*

– $D_0^\circ := \bar{\Xi}'_{\mathrm{root}}\bar{e} + \bar{\Xi}' \sum_{k=1}^{h}[(c_{\mathrm{split}} + G_X)\bar{T} + \Upsilon_k R^\circ + \Theta_k]$ *(Definition I.62 at $\bar{e}$);*

– $D_Z^\circ := \bar{\Xi}' G_Z \sum_{k=1}^{h} M_k$ *(Definition I.62);*

– $$\bar{Z} := \frac{\bar{T} + \bar{\Xi}_0\left(\tau\sigma_{\max}(1+\bar{\delta})\sqrt{N} + D_0^\circ/(1-\gamma-\gamma_S)\right)}{1 - \bar{\Xi}_0 D_Z^\circ/(1-\gamma-\gamma_S)}.$$

Measured:

- $\bar{\Xi}_0 D_Z^\circ < 1-\gamma-\gamma_S$ *at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/fx/sample_norm.py].*

Then

$$\forall z \in S:\ \|z'\| \le \bar{Z}.$$

Proof.

DEFINES $T = \mathrm{ffLDL}^\dagger(\mathcal{G})$ (Definition A.20), $\mathcal{G}$ the key's Gram matrix

$\bar{Z}(\hat{K})$, the $\bar{Z}$ of Lemma H.23 at $u = 0$, ζ of Definition I.1, T, $\bar{T}$, $\bar{e}$, $\bar{\sigma} := \sigma_{\max}$, $\bar{\Xi}_0$ and $\bar{\delta}$

$R^\circ(\hat{K}) := \sqrt{2}\,\Xi\tau\sigma_{\max}(1+\bar{\delta})(n/2)^{1/2}$, that of Lemma H.23 at the key, $\bar{\sigma} := \sigma_{\max}$ and $\bar{\delta}$: Ξ that of Definition 4.6 at the key

DEFINES $\bar{\delta}(\hat{K}) = \chi_\sigma^\zeta(\hat{K})/(1-\chi_\sigma^\zeta(\hat{K}))$ (Lemma I.71)

DEFINES $D_Z^\circ(\hat{K}) = G_Z(\hat{K})\sum_{k=1}^{h}\Xi'_k M_k$ (Lemma I.71)

DEFINES $\gamma(\hat{K})$, $\gamma_S(\hat{K})$ and $D_0^\circ(\hat{K},\cdot)$, those of Lemma I.71 at τ, $\bar{e}$ and $\bar{T}$

(L1) $\|t\| \le \bar{T}$

[Lemma H.22 at the checked key (the statement) and $\mathsf{h}(\mathsf{m})$]

(L2) $\|\widetilde{t}_T - t\| \le \bar{e}$

[Lemma I.76 at the key and $\mathsf{h}(\mathsf{m})$; $e_{\mathrm{root}} = \widetilde{t}_T - t$ (ffSampling$^{\mathcal{F}}$, line 20)]

(L3) $\forall i \le N\ \forall z_{<i}:\ |\delta_i| \le \bar{\delta}(\hat{K})$

[Proposition 5.9, (L26); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L4) $\forall i \le N\ \exists\,\delta_i \in \mathbb{R},\ |\delta_i| \le \bar{\delta}(\hat{K}):\ \widetilde{\sigma}_i = \sigma_i(1+\delta_i)$

[(L3); δ_i (Definition A.27); $\bar{\delta}(\hat{K})$ (Lemma I.71)]

(L5) $\Rightarrow\ \forall i \le N\ \exists\,\delta_i \in \mathbb{R},\ |\delta_i| \le \bar{\delta}:\ \widetilde{\sigma}_i = \sigma_i(1+\delta_i)$

[(L4); $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$ (Lemma I.71, item 3)]

(L6) $\forall i \le N:\ \sigma_i \le \sigma_{\max}$

[Lemma D.11, item 2, at the fixed-point signer; $\sigma_{\max} = 1.17^2\sigma_{\min}$ (Definition I.62)]

(L7) $\|\mathcal{L}_T^{-1}\| \le \bar{\Xi}_0$

[Lemma H.21, item 1, at the key (the statement)]

(L8) $1-\gamma-\gamma_S > 0$

[Lemma I.70]

(L9) $1-\gamma(\hat{K})-\gamma_S(\hat{K}) \ge 1-\gamma-\gamma_S$

[$\gamma(\hat{K}) \le \gamma$ and $\gamma_S(\hat{K}) \le \gamma_S$ (Lemma I.71, items 5 and 6)]

(L10) $\sigma_{\min} > 0$

[the stored word `FXP_SIGMA_MIN` [L0: `fxp/fxp_consts.h:2073-2084`]]

(L11) $\sigma_{\max} > 0$

[(L10); $\sigma_{\max}$ (the statement; Definition I.62)]

(L12) $\bar{\delta} \ge 0$

[Lemma I.69, (L7)]

(L13) $R^\circ(\hat{K}) \ge 0$

[(L11), (L12); $R^\circ(\hat{K})$ (the proof's block); $\Xi \ge 0$ (Ξ, Definition 4.6, item 13); $\tau > 1$ (τ, the statement); Fact A.41, item 8]

Lemma I.71	This proof
Shared: (f, g, F, G), τ, $\bar{e}$, $\bar{T}$	
Shared: $\tau > 1$	
$\bar{Z}$	0
(I1) $\bar{e}, \bar{T} \in [0, \infty)$	(L2), (L1)
$\bar{Z} \in [0, \infty)$	$0 \in [0, \infty)$
Its item 7: $\forall s \in (0, \sigma_{\max}]\ \forall d \in [0, \bar{\delta}] :\ \sqrt{2}\,\Xi\tau s(1+d)(n/2)^{1/2} \le R^\circ$	
Its item 8: $\forall R \in [0, R^\circ] :\ D_0^\circ(\hat{K}, R) \in [0, D_0^\circ]$	
Its item 9: $D_Z^\circ(\hat{K}) \in [0, D_Z^\circ]$	

(L14) $\forall s \in (0, \sigma_{\max}]\ \forall d \in [0, \bar{\delta}] :\ \sqrt{2}\,\Xi\tau s(1+d)(n/2)^{1/2} \le R^\circ$
[item 7 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L15) $R^\circ(\hat{K}) \in [0, R^\circ]$
[(L13); (L14) at $s := \sigma_{\max}$ by (L11) and $d := \bar{\delta}$ by (L12); $R^\circ(\hat{K})$ (the proof's block); R° (Definition I.62)]

(L16) $\forall R \in [0, R^\circ] :\ D_0^\circ(\hat{K}, R) \in [0, D_0^\circ]$
[item 8 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L17) $D_0^\circ(\hat{K}, R^\circ(\hat{K})) \in [0, D_0^\circ]$
[(L15), (L16)]

(L18) $D_Z^\circ(\hat{K}) \in [0, D_Z^\circ]$
[item 9 of (I1); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L19) $\bar{\Xi}_0 D_Z^\circ(\hat{K}) < 1 - \gamma(\hat{K}) - \gamma_S(\hat{K})$
[(L9), (L18); the measured row; $\bar{\Xi}_0$ nonnegative ($\bar{\Xi}_0$, Lemma H.21)]

(L20) $\gamma(\hat{K}) + \gamma_S(\hat{K}) < 1$
[(L8), (L9)]

(L21) $n \in \{512, 1024\}$
[Definition 5.5, item 1]

Lemma H.23	This proof
Shared: ζ (Definition I.1), h, T, t, $\widetilde{t}_T$, z', τ, S, $\bar{T}$, $\bar{e}$, $\bar{\Xi}_0$, $\bar{\delta}$	
Shared: $\tau > 1$	
$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
$\bar{\sigma}$	$\sigma_{\max}$ (the statement)
γ, γ_S	$\gamma(\hat{K}), \gamma_S(\hat{K})$ (the proof's block)
D_0°, D_Z°	$D_0^\circ(\hat{K}, R^\circ(\hat{K})), D_Z^\circ(\hat{K})$ (the proof's block)
$\bar{Z}$	$\bar{Z}(\hat{K})$ (the proof's block)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0, \zeta)$ (Definition I.1)
$h \ge 1$	(L21)
$T \in \mathcal{T}_n$	T (the proof's block; Proposition 5.8)
(I2) $t \in \mathcal{R}_n \times \mathcal{R}_n$	t (the statement)
$\bar{T}, \bar{e} \in [0, \infty)$	(L1), (L2)
$\bar{\sigma} \in [0, \infty)$	(L11)
$\bar{\Xi}_0 \in [0, \infty)$	$\bar{\Xi}_0$ (Lemma H.21)
$\bar{\delta} \in [0, \infty)$	(L12)
Assumption A1	(L1)
Assumption A2	(L2)
Assumption A3	(L5)
Assumption A4	(L6)
Assumption A5	(L7)
Assumption A6	(L20)
Assumption A7	(L19)
Its conclusion: $\forall z \in S :\ \|z'\| \le \bar{Z}$	

(L22) $\forall z \in S:\ \|z'\| \le \bar{Z}(\hat{K})$

[(I2); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L23) $1 - \bar{\Xi}_0 D_Z^\circ(\hat{K})/(1-\gamma(\hat{K})-\gamma_S(\hat{K})) \ge 1 - \bar{\Xi}_0 D_Z^\circ/(1-\gamma-\gamma_S)$

[(L8), (L9), (L18); $\bar{\Xi}_0$ nonnegative ($\bar{\Xi}_0$, Lemma H.21); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5); Fact A.41, item 8]

(L24) $1 - \bar{\Xi}_0 D_Z^\circ/(1-\gamma-\gamma_S) > 0$

[(L8); the measured row]

(L25) $$\bar{Z}(\hat{K}) = \frac{\bar{T} + \bar{\Xi}_0\left(\tau\sigma_{\max}(1+\bar{\delta})\sqrt{N} + D_0^\circ(\hat{K}, R^\circ(\hat{K}))/(1-\gamma(\hat{K})-\gamma_S(\hat{K}))\right)}{1 - \bar{\Xi}_0 D_Z^\circ(\hat{K})/(1-\gamma(\hat{K})-\gamma_S(\hat{K}))}$$

[$\bar{Z}(\hat{K})$ (the proof's block); $\bar{Z}$ (Lemma H.23)]

(L26) $D_0^\circ(\hat{K}, R^\circ(\hat{K}))/(1-\gamma(\hat{K})-\gamma_S(\hat{K})) \in [0, D_0^\circ/(1-\gamma-\gamma_S)]$

[(L8), (L9), (L17); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5); Fact A.41, item 8]

(L27) $$\bar{T} + \bar{\Xi}_0\left(\tau\sigma_{\max}(1+\bar{\delta})\sqrt{N} + D_0^\circ(\hat{K}, R^\circ(\hat{K}))/(1-\gamma(\hat{K})-\gamma_S(\hat{K}))\right) \in \left[0, \bar{T} + \bar{\Xi}_0\left(\tau\sigma_{\max}(1+\bar{\delta})\sqrt{N} + D_0^\circ/(1-\gamma-\gamma_S)\right)\right]$$

[(L26); $\bar{T}$, $\bar{\Xi}_0$, τ and $\sigma_{\max}$ nonnegative ($\bar{T}$, $\bar{\Xi}_0$, τ, $\sigma_{\max}$, the statement); $\bar{\delta} \ge 0$ ((L12)); Fact A.41, item 8]

(L28) $1/(1 - \bar{\Xi}_0 D_Z^\circ(\hat{K})/(1-\gamma(\hat{K})-\gamma_S(\hat{K}))) \in \left(0, 1/(1 - \bar{\Xi}_0 D_Z^\circ/(1-\gamma-\gamma_S))\right]$

[(L23), (L24); $t \mapsto 1/t$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L29) $\bar{Z}(\hat{K}) \le \bar{Z}$

[(L25), (L27), (L28); $\bar{Z}$ (the statement); Fact A.41, item 8]

(L30) $\Rightarrow\ \forall z \in S:\ \|z'\| \le \bar{Z}$

[(L22), (L29)]

(L31) $\Rightarrow$ the statement

[(L30)]

□

I.6.2 The loss

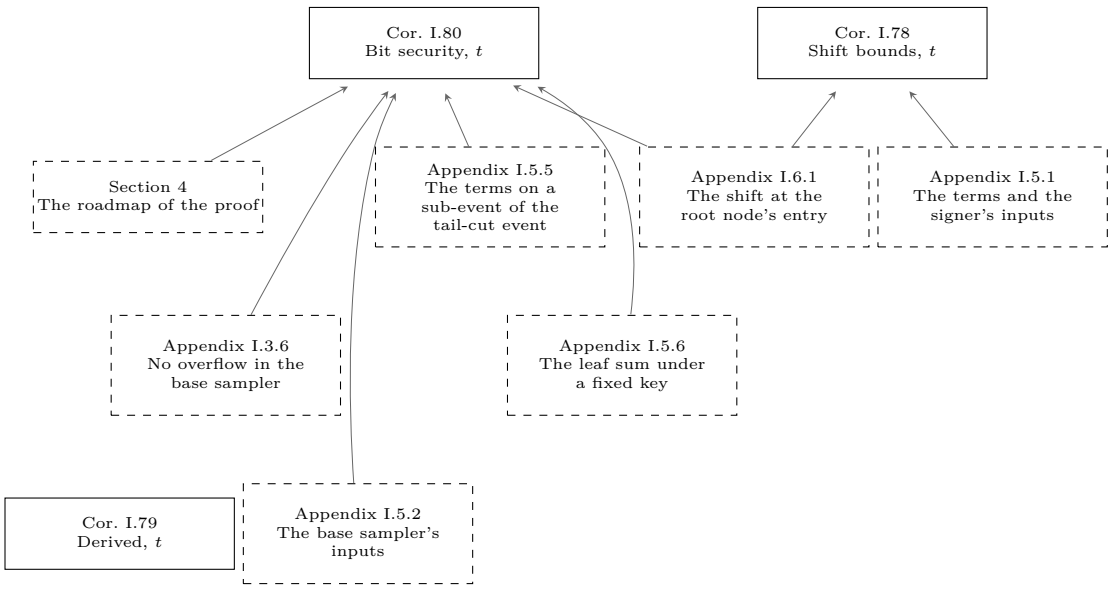


Figure 91: Dependencies, Appendix I.6.2.

Corollary I.78 (Root shift and center-shift bound at the center t [to table])**.** *At the center t and $n = 1024$, the bound on the shift at the root node's entry and the center-shift bound take the values below, at the tail-cut rate the bit security at the tail reads at $Q_s = 2^{64}$. Define:*

- n, *that of* FFT *(Algorithm 14), Precondition;*
- $\tau := 21.91$*;*
- $\bar{e}$*, the bound of Lemma I.76;*
- γ'_{fg} *and* γ'_{FG}*, those of Definition A.36;*
- $\bar{T} := (n(\gamma'^2_{FG} + \gamma'^2_{fg}))^{1/2}$ *(Lemma H.22);*
- $\bar{Z}$*, that of Lemma I.77 at* τ*;*
- D°_0*,* D°_Z*,* γ *and* γ_S*, those of Definition I.62 at* $\bar{e}$*,* $\bar{T}$ *and* τ*;*
- $D^\circ := D^\circ_0 + D^\circ_Z \bar{Z}$ *(Definition I.62);*
- $D_S := D^\circ/(1 - \gamma - \gamma_S)$ *(Definition I.62).*

Assume:

(A1) $n = 1024$.

Measured [gate: `verify/reports/fx/terms.py`*]:*

- $\bar{e}$ *at* $n = 1024$*;*
- D_S *at* $n = 1024$.

Then

1. $\bar{e} = 2^{-28.6}$*;*
2. $D_S = 2^{-8.9}$.

Proof. (L1) $\bar{e} = 2^{-28.6}$ [the first measured row at $n = 1024$; assumption A1]

(L2) $\Rightarrow$ item 1 [(L1)]

(L3) $D_S = 2^{-8.9}$ [the second measured row at $n = 1024$; assumption A1]

(L4) $\Rightarrow$ item 2 [(L3)]

□ (items 1 and 2)

Corollary I.79 (No bit from the derived bounds at the center t [to table])**.** *On the derived bounds, our proof keeps no bit at the center* t *at the searched tail-cut rate; the bit security it keeps is that at the tail (Table 34). Let:*

- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$.

Define:

- n*, that of* FFT *(Algorithm 14), Precondition;*
- $\bar{e}$*, the bound of Lemma I.76;*
- γ'_{fg} *and* γ'_{FG}*, those of Definition A.36;*
- $\bar{T} := (n(\gamma'^2_{FG} + \gamma'^2_{fg}))^{1/2}$ *(Lemma H.22);*
- λ*, that of Definition I.62;*
- $\forall \tau' > 1 :\ \lambda_{\mathcal{F}}(\tau')$*, that of Corollary 5.10 at* $c := t$*,* $\bar{e}$*,* $\bar{T}$*, the* $\bar{Z}$ *of Lemma I.77 at* τ'*,* $\tau := \tau'$ *and* $M_C := 0$.

Measured [gate: `verify/reports/fx/terms.py`*]:*

- τ*, the value a golden-section search of* $\lambda - \lambda_{\mathcal{F}}(\tau')$ *over* $\tau' \in [1.5, 60]$ *returns, at each* (n, λ, Q_s) *(*`verify/lib/renyi_terms.py`*);*
- $\lambda - \lambda_{\mathcal{F}}(\tau)$ *at every* (n, λ, Q_s).

Then

1. $\forall (n, \lambda, Q_s) :\ \lambda - \lambda_{\mathcal{F}}(\tau) \geq \lambda$*;*
2. *Assume:*

   (A1) $(n, \lambda, Q_s) = (512, 128, 2^{32})$.

Then $\lambda - \lambda_{\mathcal{F}}(\tau) = 3.48e+03$.

Proof. (L1) $\forall (n, \lambda, Q_s) :\ \lambda - \lambda_{\mathcal{F}}(\tau) \geq \lambda$ [the second measured row at every (n, λ, Q_s)]

(L2) $\Rightarrow$ item 1 [(L1)]

(L3) $\lambda - \lambda_{\mathcal{F}}(\tau) = 3.48e+03$ [the second measured row at $(512, 128, 2^{32})$; assumption A1]

(L4) $\Rightarrow$ item 2 [(L3)]

□ (items 1 and 2)

Corollary I.80 (Under **Hypotheses I.21 and I.22**, the bit security at the center t [to table])**.** *At a key whose matrix K, leaf standard deviations and remainder lie within three thresholds, the fixed-point signer at the center t keeps the bit security below, the leaf sum read at the tail of Lemma 4.14 with one failure probability η, and the center shift's term exceeds the base sampler's; every term is read at one tail-cut rate, the least multiple of* 0.01 *whose tail costs at most* $2^{-\lambda-10}$*.*

***Under Hypotheses I.21 and I.22**, let:*

- (f, g, F, G) *be a checked key of degree n (Definition 5.5) passing the tail checks at t (Definition 5.6);*
- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$.

Define:

- *The signer's words and parameters*
  - $(\lambda, \alpha) := \begin{cases} (128, 257) & n = 512 \\ (256, 513) & n = 1024 \end{cases}$ *(Definition I.62);*
  - $\eta := 2^{-\lambda}$*;*
- *The stored words*
  - M_n*,* D_n *and* B_n*, those of Definition I.14 at n and the center t;*
  - τ_K*, that of Definition I.14 at n and the center t;*
- *The leaf deviations*
  - ϵ_{hi}*, that of Lemma I.65;*
  - $s_\star := \sigma_{\min}(1 - D_n)\left(\alpha_L + (1 - \alpha_L)(1 - D_n)^2\right)^{-1/2}$ *(Definition I.62 at $\bar{\delta} := D_n$);*
  - $\epsilon_D := 2\sum_{k \geq 1} e^{-2\pi^2 s_\star^2 k^2}$ *(Definition I.62 at $\bar{\delta} := D_n$);*
- *The tail-cut event*
  - $\tau := \min\{\, \tau' \in 0.01\mathbb{Z} : \tau' > 1,\ Q_s N(1 + \epsilon_{\mathrm{hi}})(1 + \epsilon_D)(1 - \epsilon_D)^{-1} \tau' e^{(1-\tau'^2)/2} \leq 2^{-\lambda-10} \,\}$ *at each (n, λ, Q_s);*
  - $S_\tau := \{\, z \in \mathbb{Z}^N : \forall i \leq N\ |z_i - \widetilde{t}_i(z_{<i})| \leq \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$ *(Definition A.26);*
  - $S_{\tau_K} := \{\, z \in \mathbb{Z}^N : \forall i \leq N\ |z_i - \widetilde{t}_i(z_{<i})| \leq \tau_K\, \widetilde{\sigma}_i(z_{<i}) \,\}$ *(Definition A.26 at $\tau := \tau_K$, the key, $\mathsf{h}(\mathsf{m})$ and the center t);*
- *The leaf perturbations*
  - I_N*,* $\widetilde{\sigma}_i$*,* K*,* r*,* δ_i *and* μ_{key}*, those of Definition 4.12 at $\mathcal{F}_{\mathrm{fx}}$, the key, $\mathsf{h}(\mathsf{m})$ and $t_{\mathrm{c}} := t$;*
  - W *and* W^{tail}*, those of Lemma 4.14 at $\mathcal{F}_{\mathrm{fx}}$, the key, $\mathsf{h}(\mathsf{m})$, $t_{\mathrm{c}} := t$, τ, $M := M_n$, $D := D_n$, $B := B_n$, $\eta_1 := \eta/Q_s$ and the inputs of Lemma I.73;*
- *The sub-event*
  - $E := \{\, z \in \mathbb{Z}^N : W(z) \leq W^{\mathrm{tail}} \,\}$*;*
- *The probability measures*
  - P*,* $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$*, those of Proposition I.72 at the key and $c := t$;*
- *The terms*
  - $\mathfrak{L}_\Delta$*,* $\lambda_{\mathcal{F}}$*,* p'_τ*,* ε_0° *and* A*, those of Proposition I.72 at $c := t$, at Q_s, τ, $W^\circ := W^{\mathrm{tail}}$, $\bar{\delta} := D_n$, E, $\eta_E := \eta$ and $M_C := 0$, and at the $\bar{e}$, $\bar{T}$ and $\bar{Z}$ of Lemma I.77 at τ;*
  - $y := (2^{-\lambda} e^{Q_s A})^{(\alpha-1)/\alpha}$ *(Definition 5.3 at A);*

– $\lambda_n^{64} := \begin{cases} 126.28 & n = 512 \\ 248.78 & n = 1024 \end{cases}$ *(Table 34 at $Q_s = 2^{64}$);*

– $\mathfrak{L}_B$*, that of Definition I.62 at the center* t *and* τ*, and at the* $\bar{e}$*,* $\bar{T}$ *and* $\bar{Z}$ *of Lemma I.77 at* τ*.*

Assume:

(A1) $\mu_{\mathrm{key}} \le M_n$*;*

(A2) $\forall i \le N\ \forall z_{<i} :\ |\delta_i(z_{<i})| \le D_n$*;*

(A3) $\forall z \in S_{\tau_K} :\ \sum_{i \le N} (r(I_N + K))_i^2 / \tilde{\sigma}_i^2 \le B_n$*.*

Measured:

- $\tau_K = \tau$ *at* $(n, \lambda, 2^{64})$ *[gate: verify/gates/fx/tail_copy_tau.py];*
- $-\log_2(Q_s N\, p'_\tau + y + \eta)$ *at least the cell of Table 34 at every* (n, λ, Q_s) *[gate: verify/gates/fx/tail_level_cells.py--centert];*
- $(1 + D_n)^2 < \alpha_L/(\alpha_L - 1)$ *at* $n \in \{512, 1024\}$ *[gate: verify/gates/fx/tail_conditions.py];*
- $\varepsilon_0^\circ < 1$ *at every* (n, λ, Q_s) *[gate: verify/gates/fx/tail_conditions.py];*
- W^{tail} *at* $(n, Q_s) = (1024, 2^{64})$ *[gate: verify/gates/fx/tail_w.py];*
- $p'_\tau < 1$ *at every* (n, λ, Q_s) *[gate: verify/gates/fx/tail_conditions.py];*
- $\mathfrak{L}_\Delta$ *at* $(n, Q_s) = (1024, 2^{64})$ `verify/reports/fx/tail_levels.py`*;*
- $\mathfrak{L}_B$ *at* $(n, Q_s) = (1024, 2^{64})$ `verify/reports/fx/tail_levels.py`*.*

Then

1. $Q_s P(S_\tau \cap E^c) \le \eta$*;*
2. $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$*;*
3. *Assume:*
   (A4) $(n, \lambda, Q_s) = (512, 128, 2^{60})$*.*
   Then $\lambda_{\mathcal{F}} \ge 126.70$*;*
4. *Assume:*
   (A5) $(n, \lambda, Q_s) = (1024, 256, 2^{60})$*.*
   Then $\lambda_{\mathcal{F}} \ge 254.46$*;*
5. *Assume:*
   (A6) $(n, Q_s) = (1024, 2^{64})$*.*
   Then $W^{\mathrm{tail}} = 2^{-71.2}$*;*
6. *Assume:*
   (A7) $(n, Q_s) = (1024, 2^{64})$*.*
   Then $\mathfrak{L}_\Delta = 2^{-62.2}$*;*
7. *Assume:*
   (A8) $(n, Q_s) = (1024, 2^{64})$*.*
   Then $\mathfrak{L}_B = 2^{-63.8}$*;*
8. *Assume:*
   (A9) $(n, Q_s) = (1024, 2^{64})$*.*
   Then $\mathfrak{L}_\Delta > \mathfrak{L}_B$*;*
9. $\lambda_{\mathcal{F}} \ge \lambda_n^{64}$*.*

Proof. Proof of item 1.

(L1) $Q_s \le 2^{64}$

[Q_s (the statement)]

(L2) $\epsilon_D = \varepsilon_0^\circ$

[ϵ_D, $s_\star$ (Definition I.62 at $\bar\delta := D_n$); ε_0°, r_-, $\underline{s}$ (Definition A.40 at $\alpha := \alpha_L$, $s_{\rm lo} := \sigma_{\min}$, $\bar\delta := D_n$, as Proposition I.72 instantiates it); θ_{α_L} (Definition A.29); ε_0 (Definition A.38)]

(L3) $\epsilon_D < 1$

[(L2); the fourth measured row]

(L4) $N(1+\epsilon_{\rm hi})(1+\epsilon_D)(1-\epsilon_D)^{-1}\tau_K e^{(1-\tau_K^2)/2} \ge 0$

[$N := 2n$ (Definition A.25); $n \in \{512, 1024\}$ (Definition 5.5, item 1); $\epsilon_{\rm hi}$ (the statement); ϵ_D, a sum of exponentials (Definition I.62); (L3); τ_K (the statement); Fact A.41, items 28, 12 and 8]

(L5) $Q_s N(1+\epsilon_{\rm hi})(1+\epsilon_D)(1-\epsilon_D)^{-1}\tau_K e^{(1-\tau_K^2)/2} \le 2^{64} N(1+\epsilon_{\rm hi})(1+\epsilon_D)(1-\epsilon_D)^{-1}\tau_K e^{(1-\tau_K^2)/2}$

[(L1), (L4); Fact A.41, item 26]

(L6) $2^{64} N(1+\epsilon_{\rm hi})(1+\epsilon_D)(1-\epsilon_D)^{-1}\tau_K e^{(1-\tau_K^2)/2} \le 2^{-\lambda-10}$

[$\tau_K = \tau$ at $(n, \lambda, 2^{64})$ (the statement, the measured row); τ (the statement)]

(L7) $\Rightarrow\ \tau \le \tau_K$

[(L5), (L6); τ and τ_K (the statement)]

Lemma I.51, item 1 at every $i \le N$ and $z_{<i}$	This proof
Shared: (f, g, F, G), $\sigma_{\min}$ (Definition I.62)	
(I1) `isigma`	$1/\widetilde{\sigma}_i$ (Definition A.25)
$n \in \{512, 1024\}$	Definition 5.5, item 1
`isigma` taken by a call of SamplerZ by deepest	The i-th call of ffSampling$^{\mathcal{F}}$ at t (Definition A.25), at deepest (Algorithm 7)
Its conclusion: $\widetilde{\sigma} > \sigma_{\min}$	

(L8) $\forall i \le N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$

[(I1)]

(L9) $\sigma_{\min} > 0$

[the stored word `FXP_SIGMA_MIN` [L0: `fxp/fxp_consts.h:2073-2084`]]

(L10) $\Rightarrow\ \forall z \in S_\tau\ \forall i \le N :\ |z_i - \widetilde{t}_i(z_{<i})| \le \tau_K \widetilde{\sigma}_i$

[(L7), (L8), (L9); S_τ (the statement); Fact A.41, item 26]

(L11) $\Rightarrow\ S_\tau \subseteq S_{\tau_K}$

[(L10); S_{τ_K} (the statement)]

(L12) $\Rightarrow\ \forall z \in S_\tau :\ \sum_{i \le N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2 \le B_n$

[(L11); assumption A3]

(L13) $D_n \in [0, 1)$

[D_n (Definition I.14)]

(L14) $\eta/Q_s \in (0, 1)$

[$\eta := 2^{-\lambda}$ and Q_s (the statement)]

	Lemma 4.14	This proof
	Shared: (f, g, F, G), $\mathsf{h}(\mathsf{m})$, τ, ϵ_{hi} (the statement)	
	$\mathcal{F}, u, \zeta$	$\mathcal{F}_{\mathrm{fx}}, 0, 2^{-64}$ (Definition I.1)
	t_{c}	t (the statement)
	M	M_n (the statement)
	D	D_n (the statement)
	B	B_n (the statement)
	η_1	η/Q_s (the statement)
	S	S_τ (the statement)
	ϵ	ϵ (Definition I.62)
	$\mathcal{F}$ the realization of a Falcon-type signer at (u, ζ)	Lemma I.73, item 1
	(f, g, F, G) a key of degree n of the signer	Lemma I.73, item 2; the statement
(I2)	$t_{\mathrm{c}} \in \{t, t_{\mathrm{frac}}\}$	t (Definition A.13)
	$M \geq 0$	M_n (Definition I.14)
	$D \in [0, 1)$	(L13)
	$B \geq 0$	B_n (Definition I.14)
	$\eta_1 \in (0, 1)$	(L14)
	$\epsilon \in [0, 1)$	Lemma I.73, item 3
	$\epsilon_{\mathrm{hi}} \geq 0$, $\forall i \leq N\ \forall z_{<i}\ \forall z_i \notin C_i$: $\widetilde{B}_i(z_i) \leq (1 + \epsilon_{\mathrm{hi}})\, \widetilde{D}_i(z_i)$	Lemma I.65 at the checked key; $\epsilon_{\mathrm{hi}} \geq 0$ (ϵ_{hi}, Lemma I.65)
	Assumption A1	Assumption A2; $\bar{\delta}_K$ (Definition 4.12, item 1)
	Assumption A2	Assumption A1
	Assumption A3	(L12); $\bar{B}_K$ (Definition 4.12, item 3, at $\tau_K := \tau$)
	Assumption A4	Lemma I.73, item 4, at $t_{\mathrm{c}} := t$
	Assumption A5	Lemma I.73, item 5
	Assumption A6	Lemma I.73, item 6
	Assumption A7	Lemma I.73, item 7, at $t_{\mathrm{c}} := t$
	Its conclusion: $P(S \cap \{z \in \mathbb{Z}^N : W(z) > W^{\mathrm{tail}}\}) \leq \eta_1$	

(L15) $P(S_\tau \cap \{z \in \mathbb{Z}^N : W(z) > W^{\mathrm{tail}}\}) \leq \eta/Q_s$

[(I2)]

(L16) $S_\tau \cap E^c = S_\tau \cap \{z \in \mathbb{Z}^N : W(z) > W^{\mathrm{tail}}\}$

[E (the statement)]

(L17) $\Rightarrow\ Q_s P(S_\tau \cap E^c) \leq \eta$

[(L15), (L16); $Q_s > 0$ (Q_s, the statement); Fact A.41, item 26]

(L18) $\Rightarrow$ item 1

[(L17)]

□ (item 1)

Proof of items 2 to 9.

(L19) $W^{\mathrm{tail}} \geq 0$

[W^{tail} (Lemma 4.14); $t^2 \geq 0$ (Fact A.41, item 13); Fact A.41, item 8]

(L20) $\|\widetilde{t}_T - t\| \leq \bar{e}$

[Lemma I.76 at the checked key and the hashed message; $e_{\mathrm{root}} = \widetilde{t}_T - t$ (ffSampling$^{\mathcal{F}}$, line 20)]

(L21) $\|t\| \leq \bar{T}$

[Lemma H.22 at the checked key and the hashed message]

(L22) $\forall z \in S_\tau :\ \|z'\| \leq \bar{Z}$

[Lemma I.77 at the checked key and the hashed message; **Hypotheses I.21 and I.22**, named by Lemma I.77]

(L23) $p'_\tau < 1$

[[gate: `verify/gates/fx/tail_conditions.py`] at every (n, λ, Q_s)]

(L24) $\forall z \in S_\tau \cap E :\ W(z) \leq W^{\mathrm{tail}}$

[E (the statement)]

(L25) $(1+D_n)^2 < \alpha_L/(\alpha_L-1)$

[the third measured row]

(L26) $\varepsilon_0^\circ < 1$

[the fourth measured row]

(L27) $\bar{e}, \bar{T}, \bar{Z} \geq 0$

[(L20), (L21); $\|\cdot\| \geq 0$ (Fact A.41, item 3); $\bar{Z}$ (Lemma I.77) and Lemma I.77, (L24), (L27); Fact A.41, item 8]

Proposition I.72	This proof
Shared: (f, g, F, G), Q_s, τ, E, $\bar{e}, \bar{T}, \bar{Z}$ (Lemma I.77)	
c	t (the statement)
W°	W^{tail} (the statement)
$\bar{\delta}$	D_n (the statement)
η_E	η (the statement)
M_C	0
S	S_τ (the statement)
$c \in \{t, t_{\text{frac}}\}$	t (Definition 4.5)
$\bar{e}, \bar{T}, \bar{Z} \in [0, \infty)$	(L27)
$M_C \in \mathbb{Z}_{\geq 0}$	$0 \in \mathbb{Z}_{\geq 0}$
$W^\circ \geq 0$	(L19)
(I3) $\bar{\delta} \in [0, 1)$	(L13)
$E \subseteq \mathbb{Z}^N$	E (the statement)
$\eta_E \geq 0$	η (the statement)
Assumption A1	(L20)
Assumption A2	(L21)
Assumption A3	(L22)
Assumption A4	(L23)
Assumption A5	(L24)
Assumption A6	Assumption A2
Assumption A7	(L25)
Assumption A8	(L26)
Assumption A9	(L17)
Its conclusion: $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \leq 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \leq 2^{-\lambda_{\mathcal{F}}}$	

(L28) $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \leq 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \leq 2^{-\lambda_{\mathcal{F}}}$

[(I3); **Hypotheses I.21 and I.22**, named by Proposition I.72]

(L29) $\Rightarrow$ item 2

[(L28)]

Corollary E.21 at τ	This proof
Shared: τ, ϵ_{hi} (the statement)	
Shared: $N := 2n$, $\tau > 1$	
ϵ	ϵ (Definition I.62)
S	S_τ (the statement)
(I4) $\epsilon \in [0, 1)$	Lemma I.73, item 3
$\epsilon_{\text{hi}} \geq 0$, $\forall i \leq N\ \forall z_{<i}\ \forall z_i \notin C_i :$ $\widetilde{B}_i(z_i) \leq (1+\epsilon_{\text{hi}})\, \widetilde{D}_i(z_i)$	Lemma I.65 at the checked key; $\epsilon_{\text{hi}} \geq 0$ (ϵ_{hi}, Lemma I.65)
Assumption A1	(L8), (L9)
Assumption A2	Lemma I.73, item 4, at $t_c := t$
Its conclusion: $P(S_\tau^c) \leq N\,(1+\epsilon_{\text{hi}})\,\frac{1+\epsilon}{1-\epsilon}\,\tau\, e^{(1-\tau^2)/2}$	

(L30) $P(S_\tau^c) \leq N\, p'_\tau$

[(I4); p'_τ (Corollary 4.10, precondition 3)]

(L31) $2^{-\lambda_{\mathcal{F}}} \leq Q_s N\, p'_\tau + y + \eta$

[(L30); $\lambda_{\mathcal{F}}$ and $\lambda'_{\mathcal{F}}$ (Proposition I.72; Definition 5.3 at A, κ_C, $\bar{p}_C$, $M_C := 0$ and $S' := S_\tau$); Π_C (Definition 5.2 at $M_C := 0$); Lemma I.64, item 3]

(L32) $\Rightarrow\ \lambda_{\mathcal{F}} \geq -\log_2(Q_s N\, p'_\tau + y + \eta)$
[(L31); $t \mapsto -\log_2 t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5); $-\log_2 2^{-x} = x$ (Fact A.41, item 28)]

(L33) $\lambda_{\mathcal{F}} \geq 126.70$
[(L32); the second measured row at $(512, 128, 2^{60})$; assumption A4]

(L34) $\Rightarrow$ item 3
[(L33)]

(L35) $\lambda_{\mathcal{F}} \geq 254.46$
[(L32); the second measured row at $(1024, 256, 2^{60})$; assumption A5]

(L36) $\Rightarrow$ item 4
[(L35)]

(L37) $W^{\text{tail}} = 2^{-71.2}$
[the fifth measured row; assumption A6]

(L38) $\Rightarrow$ item 5
[(L37)]

(L39) $\mathfrak{L}_\Delta = 2^{-62.2}$
[`verify/reports/fx/tail_levels.py` at $(n, Q_s) = (1024, 2^{64})$; assumption A7]

(L40) $\Rightarrow$ item 6
[(L39)]

(L41) $\mathfrak{L}_B = 2^{-63.8}$
[`verify/reports/fx/tail_levels.py` at $(n, Q_s) = (1024, 2^{64})$; assumption A8]

(L42) $\Rightarrow$ item 7
[(L41)]

(L43) $\mathfrak{L}_\Delta > \mathfrak{L}_B$
[(L39), (L41); expand; assumption A9]

(L44) $\Rightarrow$ item 8
[(L43)]

(L45) $n = 512 \Rightarrow\ \lambda_{\mathcal{F}} \geq 126.28$
[(L32); the second measured row at $(512, 128, Q_s)$; Table 34 at $n = 512$; expand]

(L46) $n = 1024 \Rightarrow\ \lambda_{\mathcal{F}} \geq 248.78$
[(L32); the second measured row at $(1024, 256, Q_s)$; Table 34 at $n = 1024$; expand]

(L47) $\Rightarrow$ item 9
[(L45), (L46); λ_n^{64} (the statement); $n \in \{512, 1024\}$ (Definition 5.5, item 1)]

□ (items 2 to 9)

The end-to-end gate of ffSampling$^{\mathcal{F}}(B, s, t)$**.** The gate of ffSampling$^{\mathcal{F}}(B, s, t)$ end to end: every signature of 16 checked keys times 16 messages per degree verifies under the reference's `fndsa_verify`, a tampered copy is rejected, and the mean of $\|s_1\|^2 + \|s_2\|^2$ is within 2% of $2n\sigma^2$ (Statistics I.23, items 7 to 9). The words reach 2^{33} at $n = 1024$ (Theorem I.54): the products $\widetilde{\hat{h}} \otimes \widetilde{b}$ before the scaling by $1/q$.

I.7 ffSampling$^{\mathcal{F}}(B, s, t_{\text{frac}})$

Algorithm 17 describes the center split over the integers.

The split is this version's one change. The split is this version's one change from ffSampling$^{\mathcal{F}}(B, s, t)$: both versions compute the root node's second diagonal by the NTRU

identity (Lemma I.27). The split keeps the words small (Theorem I.54) and removes the products of Lemma I.75 (Remark I.90).

The bit security of this version. Its level under **Hypotheses I.21 and I.22**, at a key within three thresholds, is Theorem 1.3's at the center t_{frac}, read at the tail of Lemma 4.14 (Table 34).

Algorithm 17 $\text{center}_{\text{frac}}(\mathsf{h}(\mathsf{m}), f, F)$, the center split over the integers, over $\mathbb{R}$ and in $\mathcal{F}_{\text{fx}}$ [L2: BFLP26, Alg. 7] [L0: `fxp/sign_fxcore.c:60-81`] [L0: `fxp/sign_fxpoly.c:292-304`]

Input: $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$; f, F (keygen (Algorithm 11))
Output (code): $(\widetilde{t}_{\text{frac}}, t_{\text{int}})$, $\widetilde{t}_{\text{frac}} \in \mathcal{F}_{\text{fx}}$, $t_{\text{int}} \in \mathbb{Z}^{2n}$
Output (idealized): $(t_{\text{frac}}, t_{\text{int}})$, $t_{\text{frac}} = \text{FFT}(qt_{\text{frac}})/q \in \mathcal{R}_n \times \mathcal{R}_n$, $qt_{\text{frac}} = qt \bmod q$, $qt = (-\mathsf{h}(\mathsf{m})\, F, \mathsf{h}(\mathsf{m})\, f)$
Postcondition: $(\mathsf{h}(\mathsf{m}), 0)B^{-1} = t_{\text{int}} + qt_{\text{frac}}/q$ (Lemma I.81)
In the proofs: qt, qt_{frac}, $\widetilde{h}_j$, $\hat{h}_j$, v, δ_T, $\widetilde{(1/q)}$, e_{root}

$qt_0 \leftarrow -\mathsf{h}(\mathsf{m})\, F$ ▷ in $\mathbb{Z}[x]/(x^n+1)$, exact; $\forall i < 2n : \ |qt_{[i]}| < 2^{31}$ [L0: `fxp/sign_fxcore.c:65-73`]
$qt_1 \leftarrow \mathsf{h}(\mathsf{m})\, f$
for all $j \in \{0,1\}$, $i < n$ **do**
    $qt_{\text{frac},j,i} \leftarrow qt_{j,i} \bmod q \in [-q/2, q/2)$ ▷ [L0: `fxp/sign_fxcore.c:75-78`]
    $t_{\text{int},j,i} \leftarrow (qt_{j,i} - qt_{\text{frac},j,i})/q$ ▷ [L0: `fxp/sign_fxcore.c:79`]
end for
$\forall j : \ \widetilde{h}_j \leftarrow \widetilde{\text{FFT}}(qt_{\text{frac},j})$ ▷ $\|\widetilde{h}_j - \hat{h}_j\| \le \delta_T$ [L0: `fxp/sign_fxpoly.c:296-303`]
$\forall j \in \{0,1\} : \ \hat{h}_j \leftarrow \text{FFT}(qt_{\text{frac},j})$
$v \leftarrow \sqrt{n}\, q/2$ ▷ $\|\hat{h}_j\| = \|qt_{\text{frac},j}\| \le v$, the coefficient norm (Proposition G.15)
$\delta_T \leftarrow R_{h-1} v + A_{h-1}/\sqrt{n/2}$ ▷ Lemma H.11 at $(0, \zeta)$, in the coefficient norm
$\widetilde{(1/q)} \leftarrow \text{fl}(1/q)$ ▷ $= 1/q + \zeta_\circ$, $|\zeta_\circ| \le \zeta_{\text{op}}$ (Definition I.20)
$\forall j : \ \widetilde{t}_{\text{frac},j} \leftarrow \widetilde{h}_j \otimes \widetilde{(1/q)}$
$\forall j : \ t_{\text{frac},j} \leftarrow \hat{h}_j\, (1/q)$
$e_{\text{root}} \leftarrow \widetilde{t}_{\text{frac}} - t_{\text{frac}}$
return $(\widetilde{t}_{\text{frac}}, t_{\text{int}})$
return $(t_{\text{frac}}, t_{\text{int}})$

Structure. Appendix I.7.1 states the shift at the root node's entry; Appendix I.7.2 the loss.

I.7.1 The shift at the root node's entry

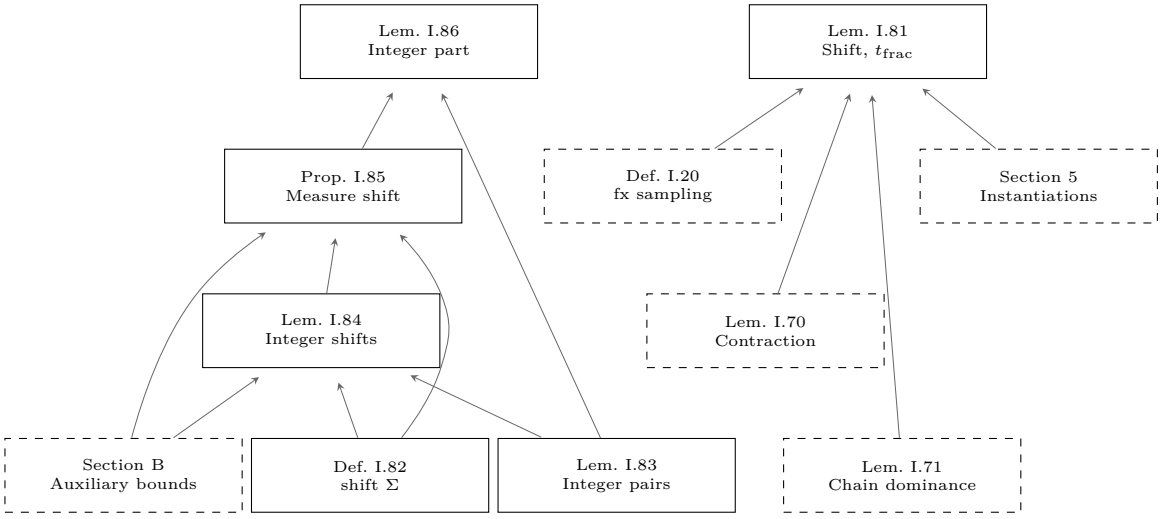


Figure 92: Dependencies, Appendix I.7.1.

Lemma I.81 (Shift and norms at the center t_{frac} [to table])**.** *The fractional center's root shift is at most $\bar{e}$, its norm at most $\bar{T}$, and every sample on S at most $\bar{Z}$.* ***Under Hypotheses I.21 and I.22****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The signer's words and parameters*
  - h *and* $n := 2^h$*, those of* FFT *(Algorithm 14), Precondition;*
  - $\zeta_{\mathrm{op}} := 2^{-65}$ *(Definition I.1);*
  - P*, that of* FFT*, line 1;*
- *The key bounds*
  - d_{hi}*,* M_0 *and* $\bar{g}_{11}$*, those of Proposition 5.8;*
  - $\bar{\Xi}_0 := (d_{\mathrm{hi}}(M_0 + \bar{g}_{11}))^{1/2}/q$ *(Lemma H.21);*
- *The leaf deviations*
  - $\sigma_{\min}$ *and* χ^{ζ}_{σ}*, those of Definition I.62;*
  - $\sigma_{\max} := 1.17^2\sigma_{\min}$ *(Definition I.62);*
  - $\bar{\delta} := \chi^{\zeta}_{\sigma}/(1 - \chi^{\zeta}_{\sigma})$ *(Definition I.62);*
- *The tree*
  - $\mathcal{G}$*, that of Proposition 5.8;*
  - $T :=$ ffLDL$^{\dagger}(\mathcal{G})$ *(Definition A.20);*
- *The centers and the samples*
  - qt_{frac}*,* $\hat{h}_j$*,* v*,* t_{frac} *and* δ_T*, those of* center$_{\mathrm{frac}}$ *(Algorithm 17), lines 4 to 14;*
  - $\widetilde{h}_j$*,* $\widetilde{(1/q)}$*,* $\widetilde{t}_{\mathrm{frac}}$ *and* e_{root}*, the values* center$_{\mathrm{frac}}$ *computes in* $\mathcal{F}_{\mathrm{fx}}$ *(lines 7 to 14);*
  - $z' := (z_0, z_1)$*, the sample* ffsamp *(Algorithm 6) returns at* t_{frac} *(*ffSampling$^{\mathcal{F}}$ *(Algorithm 10), line 24), the sample before line 29;*
  - $c := (c_i)_{i \le N}$*, the leaf centers of Proposition G.48 at* T*, the center* t_{frac} *and the sample* z'*;*
  - $\widetilde{t} := (\widetilde{t}_i)_{i \le N}$*, the centers* ffSampling$^{\mathcal{F}}(B, s, t_{\mathrm{frac}})$ *passes to the base sampler (Definition A.25);*
- *The center shifts*
  - $c_{\mathrm{merge}} := \sqrt{2}\,\zeta$ *(Corollary I.9, item 5, at* $u := 0$*);*
  - $k_E := 8\sqrt{2}$ *(Corollary I.9, item 6, at* $u := 0$*);*
  - $R_{h-1} := (1 + c_{\mathrm{merge}})^{h-1} - 1$*;*

  - $A_0 := 0$;
  - $\forall j < h-1:\ A_{j+1} := \sqrt{2}(1+c_{\mathrm{merge}})A_j + k_E\,\zeta\sqrt{P}$;
  - $\bar{\Xi}'$, $\bar{\Xi}$, $\bar{\Xi}'_{\mathrm{root}}$, G_γ, c_S, Υ_k, c_{split}, G_X, R°, Θ_k, G_Z *and* M_k, *those of Definition I.62*;
  - $\gamma := \bar{\Xi}'(1+2(h-1)\bar{\Xi})\,G_\gamma$ *(Definition I.62)*;
  - $\gamma_S := c_S\bar{\Xi}'\sum_{k=1}^{h}\Upsilon_k$ *(Definition I.62)*;
- *The terms*
  - $\bar{e} := \sqrt{2}(\delta_T/q + v\zeta_{\mathrm{op}} + \delta_T\zeta_{\mathrm{op}} + \sqrt{2}\,\zeta_{\mathrm{op}})$;
  - $\bar{T} := \sqrt{n/2}$;
  - $D_0^\circ := \bar{\Xi}'_{\mathrm{root}}\bar{e} + \bar{\Xi}'\sum_{k=1}^{h}[(c_{\mathrm{split}}+G_X)\bar{T} + \Upsilon_k R^\circ + \Theta_k]$ *(Definition I.62 at* $\bar{e}$*)*;
  - $D_Z^\circ := \bar{\Xi}'G_Z\sum_{k=1}^{h}M_k$ *(Definition I.62)*;
  - $\bar{Z} := \dfrac{\bar{T} + \bar{\Xi}_0\left(\tau\sigma_{\max}(1+\bar{\delta})\sqrt{N} + D_0^\circ/(1-\gamma-\gamma_S)\right)}{1-\bar{\Xi}_0 D_Z^\circ/(1-\gamma-\gamma_S)}$.

Measured:

- $\bar{\Xi}_0 D_Z^\circ < 1-\gamma-\gamma_S$ *at* $n=512$ *and* $n=1024$ *[gate: verify/gates/fx/sample_norm.py].*

Then

1. $\|e_{\mathrm{root}}\| \le \bar{e}$;
2. $\|t_{\mathrm{frac}}\| \le \bar{T}$;
3. $\forall z \in S:\ \|z'\| \le \bar{Z}$.

Proof. Proof of item 1.

(L1) $\|\hat{h}_j\| = \|qt_{\mathrm{frac},j}\|$
[$\hat{h}_j = \mathrm{FFT}(qt_{\mathrm{frac},j})$ (the statement); Proposition G.15; $\|\cdot\|$, the coefficient norm (Appendix G.5)]

(L2) $\|qt_{\mathrm{frac},j}\| \le \sqrt{n}\,q/2$
[$\forall i < n:\ |qt_{\mathrm{frac},j,[i]}| \le q/2$ ($\mathrm{center}_{\mathrm{frac}}$, line 4); $\|\cdot\|$, the coefficient norm (Definition A.1); Fact A.41, item 5]

(L3) $\Rightarrow\ \|\hat{h}_j\| \le v$
[(L1), (L2); v ($\mathrm{center}_{\mathrm{frac}}$ (Algorithm 17))]

(L4) $\forall x:\ \sum_\psi |x(\psi)|^2 = (n/2)\|x\|^2$
[Proposition G.15; $\|x\|$, the coefficient norm (Definition A.1)]

Lemma H.11	This proof
Shared: ζ (Definition I.1), h, n	
$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
f	$qt_{\mathrm{frac},j}$ (the statement)
$\hat{f}$	$\hat{h}_j$ (the statement)
$\widetilde{f}$	$\widetilde{h}_j$ (the statement)
$\mathcal{F}$ realization at (u,ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0,\zeta)$ (Definition I.1)
$\forall i < n:\ f_{[i]} \in \mathcal{F}$	$qt_{\mathrm{frac},j,i} \in \mathbb{Z}$ ($\mathrm{center}_{\mathrm{frac}}$, line 4); $\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
Its conclusion: $\|\widetilde{f} - \hat{f}\| \le R_{h-1}\|\hat{f}\| + A_{h-1}$	

(I1)

(L5) $\left(\sum_\psi |\widetilde{h}_j(\psi) - \hat{h}_j(\psi)|^2\right)^{1/2} \le R_{h-1}\left(\sum_\psi |\hat{h}_j(\psi)|^2\right)^{1/2} + A_{h-1}$
[(I1); $\|X\|^2 := \sum_i |X_i|^2$ (Fact A.41, its lead) over the $n/2$ roots]

(L6) $R_{h-1} \ge 0$
[R_{h-1} (the statement); $c_{\mathrm{merge}} = \sqrt{2}\,\zeta$ (the statement); $\zeta \ge 0$ ($\zeta := 2\zeta_{\mathrm{op}}$, Definition I.1); $h \ge 1$ (FFT (Algorithm 14), Precondition); $t \mapsto t^p$ nondecreasing on $[0,\infty)$ at $p := h-1$ (Fact A.41, item 5)]

(L7) $\|\widetilde{h}_j - \hat{h}_j\| \le R_{h-1}v + A_{h-1}/\sqrt{n/2}$
[(L5), (L6), (L4), (L3); the array $(\hat{h}_j(\psi))_\psi$ indexed by [gate: verify/gates/tree/tower_index.py]; Fact A.41, item 26]

(L8) $\Rightarrow\ \|\widetilde{h}_j - \hat{h}_j\| \le \delta_T$
[(L7); δ_T ($\mathrm{center}_{\mathrm{frac}}$ (Algorithm 17))]

(L9) $\exists\, \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \le \zeta_{\mathrm{op}} :\ \widetilde{(1/q)} = 1/q + \zeta_\circ$

[Definition I.20]

(L10) $\forall \psi :\ |(\widetilde{h}_j \otimes \widetilde{(1/q)})(\psi) - \widetilde{h}_j(\psi)\,\widetilde{(1/q)}| \le \sqrt{2}\,\zeta_{\mathrm{op}}$

[$c \otimes a$ (Definition A.8); Definition I.1, item 1, at its two products; $\forall a, b \in \mathbb{R} :\ |a+ib|^2 = a^2 + b^2$ (Fact A.41, item 1)]

(L11) $\forall x \in \mathbb{C}^{n/2} :\ \|x\| \le \max_\psi |x(\psi)|$

[Proposition G.15; Fact A.41, items 20 and 5]

(L12) $\exists\, \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \le \zeta_{\mathrm{op}},\ \exists\, e_c,\ \|e_c\| \le \sqrt{2}\,\zeta_{\mathrm{op}} :\ \widetilde{t}_{\mathrm{frac},j} = \widetilde{h}_j(1/q + \zeta_\circ) + e_c$

[(L9), (L10), (L11); $\mathrm{center}_{\mathrm{frac}}$, line 12]

(L13) $\|\widetilde{h}_j\| \le v + \delta_T$

[(L3), (L8); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3)]

(L14) $\Rightarrow\ \|\widetilde{t}_{\mathrm{frac},j} - t_{\mathrm{frac},j}\| \le \delta_T/q + v\zeta_{\mathrm{op}} + \delta_T\zeta_{\mathrm{op}} + \sqrt{2}\,\zeta_{\mathrm{op}}$

[(L8), (L12), (L13); $t_{\mathrm{frac},j} = \hat{h}_j/q$ ($\mathrm{center}_{\mathrm{frac}}$, EnsureI); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3); Fact A.41, items 1 and 8]

(L15) $\Rightarrow$ item 1

[(L14) for $j = 0, 1$; $e_{\mathrm{root}} = \widetilde{t}_{\mathrm{frac}} - t_{\mathrm{frac}}$ ($\mathrm{center}_{\mathrm{frac}}$, line 14); $\|(X,Y)\| \le \sqrt{2}\max(\|X\|, \|Y\|)$ (Fact A.41, item 3); $\bar{e}$ (the statement)]

□ (item 1)

Proof of items 2 and 3.

DEFINES D° and $R^\circ(\hat{K})$, the D° and R° of Corollary G.62 at $u = 0$, T, $\bar{\delta}$, the center t_{frac}, e_{root}, $\bar{T}$ and $Z := \|z'\|$

DEFINES $\bar{\delta}(\hat{K}) = \chi^\zeta_\sigma(\hat{K})/(1 - \chi^\zeta_\sigma(\hat{K}))$ (Lemma I.71)

DEFINES $D^\circ_Z(\hat{K}) = G_Z(\hat{K}) \sum_{k=1}^h \Xi'_k M_k$ (Lemma I.71)

DEFINES $\gamma(\hat{K})$, $\gamma_S(\hat{K})$ and $D^\circ_0(\hat{K}, \cdot)$, those of Lemma I.71 at τ, $\bar{e}$ and $\bar{T}$

(L16) $\|t_{\mathrm{frac}}\| \le \sqrt{2}\,v/q$

[(L3); $t_{\mathrm{frac},j} = \hat{h}_j/q$ ($\mathrm{center}_{\mathrm{frac}}$, EnsureI); $\|(X,Y)\| \le \sqrt{2}\max(\|X\|, \|Y\|)$ (Fact A.41, item 3); Fact A.41, item 1]

(L17) $\sqrt{2}\,v/q = \sqrt{n/2}$

[v ($\mathrm{center}_{\mathrm{frac}}$ (Algorithm 17))]

(L18) $\Rightarrow\ \|t_{\mathrm{frac}}\| \le \bar{T}$

[(L16), (L17); $\bar{T}$ (the statement)]

(L19) $\Rightarrow$ item 2

[(L18)]

(I2)

Proposition G.48, item 2	This proof
T	T (the statement)
t	t_{frac} (the statement)
z	z' (the statement)
$T \in \mathcal{T}_n$	T (the statement; Proposition 5.8)
$t \in \mathcal{R}_n \times \mathcal{R}_n$	t_{frac} (the statement)
$z \in \mathbb{Z}^N$	z', a sample of ffSampling(t, T) (the statement)
Its conclusion: $t - z = (c - z)\mathcal{L}_T^{-1}$	

(L20) $t_{\mathrm{frac}} - z' = (c - z')\mathcal{L}_T^{-1}$

[(I2)]

(L21) $\|\mathcal{L}_T^{-1}\| \le \bar{\Xi}_0$

[Lemma H.21, item 1, at the key (the statement)]

(L22) $\forall z \in S :\ \|z'\| \le \|t_{\mathrm{frac}}\| + \bar{\Xi}_0\|c - z'\|$

[(L20), (L21); $\|x+y\| \le \|x\| + \|y\|$ (Fact A.41, item 3); $\|\mathcal{L}_T^{-1}\|$ (Definition 4.6, item 7); Fact A.41, item 26]

(L23) $\forall z \in S\ \forall i \le N :\ |z'_i - \widetilde{t}_i| \le \tau\widetilde{\sigma}_i$

[Definition A.26]

(L24) $\forall i \le N\ \forall z_{<i}:\ |\delta_i| \le \bar{\delta}(\hat{K})$

[Proposition 5.9, (L26); **Hypotheses I.21 and I.22**, named by Proposition 5.9]

(L25) $\forall i \le N:\ \widetilde{\sigma}_i \le \sigma_i(1+\bar{\delta}(\hat{K}))$

[(L24); δ_i (Definition A.27); $\bar{\delta}(\hat{K})$ (Lemma I.71); $\sigma_i > \sigma_{\min}$ (Lemma D.11, item 1, at the fixed-point signer); $\sigma_{\min} > 0$ (the stored word [L0: `fxp/fxp_consts.h:2073-2084`]); Fact A.41, item 26]

Lemma I.71	This proof
Shared: (f, g, F, G), τ, $\bar{e}$, $\bar{T}$	
Shared: $\tau > 1$	
$\bar{Z}$	0
$\bar{e}, \bar{T} \in [0, \infty)$	(L15), (L18); $\|\cdot\| \ge 0$ (Fact A.41, item 3)
$\bar{Z} \in [0, \infty)$	$0 \in [0, \infty)$
(I3) Its item 3: $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$	
Its item 5: $\gamma(\hat{K}) \le \gamma$	
Its item 6: $\gamma_S(\hat{K}) \le \gamma_S$	
Its item 7: $\forall s \in (0, \sigma_{\max}]\ \forall d \in [0, \bar{\delta}]:\ \sqrt{2}\,\Xi\tau s(1+d)(n/2)^{1/2} \le R^\circ$	
Its item 8: $\forall R \in [0, R^\circ]:\ D_0^\circ(\hat{K}, R) \in [0, D_0^\circ]$	
Its item 9: $D_Z^\circ(\hat{K}) \in [0, D_Z^\circ]$	

(L26) $\bar{\delta}(\hat{K}) \in [0, \bar{\delta}]$

[item 3 of (I3); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L27) $\gamma(\hat{K}) \le \gamma$

[item 5 of (I3); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L28) $\gamma_S(\hat{K}) \le \gamma_S$

[item 6 of (I3); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L29) $\forall s \in (0, \sigma_{\max}]\ \forall d \in [0, \bar{\delta}]:\ \sqrt{2}\,\Xi\tau s(1+d)(n/2)^{1/2} \le R^\circ$

[item 7 of (I3); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L30) $\forall R \in [0, R^\circ]:\ D_0^\circ(\hat{K}, R) \in [0, D_0^\circ]$

[item 8 of (I3); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L31) $D_Z^\circ(\hat{K}) \in [0, D_Z^\circ]$

[item 9 of (I3); **Hypotheses I.21 and I.22**, named by Lemma I.71]

(L32) $\Rightarrow\ \forall i \le N:\ \widetilde{\sigma}_i \le \sigma_i(1+\bar{\delta})$

[(L25), (L26); $\sigma_i > \sigma_{\min}$ (Lemma D.11, item 1, at the fixed-point signer); $\sigma_{\min} > 0$ (the stored word [L0: `fxp/fxp_consts.h:2073-2084`])]

(L33) $\forall i \le N:\ \sigma_i < \sigma_{\max}$

[Lemma D.11, item 2, at the fixed-point signer; $\sigma_{\max} = 1.17^2\sigma_{\min}$ (Definition I.62)]

(L34) $\forall z \in S\ \forall i \le N:\ |\widetilde{t}_i - z'_i| \le \tau\sigma_{\max}(1+\bar{\delta})$

[(L23), (L32), (L33); $\bar{\delta} \ge 0$ (Lemma I.69, (L7)); Fact A.41, items 1 and 8]

(L35) $\forall z \in S:\ \|\widetilde{t} - z'\| \le \tau\sigma_{\max}(1+\bar{\delta})\sqrt{N}$

[(L34) over the N leaves; $\widetilde{t}$ (the statement); Fact A.41, item 5]

(L36) $1 - \gamma - \gamma_S > 0$

[Lemma I.70]

(L37) $1 - \gamma(\hat{K}) - \gamma_S(\hat{K}) \ge 1 - \gamma - \gamma_S$

[(L27), (L28)]

(L38) $\forall i \le N\ \exists \delta_i \in \mathbb{R},\ |\delta_i| \le \bar{\delta}:\ \widetilde{\sigma}_i = \sigma_i(1+\delta_i)$

[(L24), (L26); δ_i (Definition A.27)]

(L39) $\|\widetilde{t}_{\text{frac}} - t_{\text{frac}}\| = \|e_{\text{root}}\|$

[$\text{center}_{\text{frac}}$, line 14]

Corollary G.62 at every $z \in S$	This proof
Shared: ζ (Definition I.1), h, n, T, $\bar{T}$, e_{root}, $S, \tau, \bar{\delta}$, D°	
$\mathcal{F}$	$\mathcal{F}_{\mathrm{fx}}$ (Definition I.1)
u	0
t	t_{frac} (the statement)
$\widetilde{t}_T$	$\widetilde{t}_{\mathrm{frac}}$ (center$_{\mathrm{frac}}$, Return; ffSampling$^{\mathcal{F}}$, line 23)
z	z' (the statement)
Z	$\|z'\|$ (the proof's block)
Δ	$\widetilde{t} - c$ (Proposition G.48)
γ, γ_S	$\gamma(\hat{K}), \gamma_S(\hat{K})$ (Lemma I.71)
$\mathcal{F}$ realization at (u, ζ)	$\mathcal{F}_{\mathrm{fx}}$ at $(0, \zeta)$ (Definition I.1)
$h \geq 1$	$n \in \{512, 1024\}$ (Definition 5.5, item 1)
(I4) $T \in \mathcal{T}_n$	T (the statement; Proposition 5.8)
$t \in \mathcal{R}_n \times \mathcal{R}_n$	t_{frac} (the statement)
$z \in \mathbb{Z}^N$	z' (the statement)
$Z \geq 0$	$\|z'\| \geq 0$ (Fact A.41, item 3)
$\bar{T} \in \mathbb{R}$	$\bar{T}$ (the statement)
$e_{\mathrm{root}} \in \mathcal{R}_n \times \mathcal{R}_n$	e_{root} (the statement)
$\bar{\delta} \in \mathbb{R}$	$\bar{\delta}$ (the statement)
Assumption A1	The scope
Assumption A2	$Z := \|z'\|$ (the proof's block)
Assumption A3	(L18)
Assumption A4	(L39)
Assumption A5	(L38)
Its conclusion: $(1 - \gamma - \gamma_S)\|\Delta\| \leq D^\circ$	

(L40) $\forall z \in S:\ (1 - \gamma(\hat{K}) - \gamma_S(\hat{K}))\|\widetilde{t} - c\| \leq D^\circ$

[(I4)]

(L41) $\max_i \sigma_i \in (0, \sigma_{\max}]$

[(L33); Lemma D.11, item 1, at the fixed-point signer; $\sigma_{\min} > 0$ (the stored word [L0: `fxp/fxp_consts.h:2073-2084`]); Fact A.41, item 20]

(L42) $\bar{\delta} \geq 0$

[Lemma I.69, (L7)]

(L43) $R^\circ(\hat{K}) \in [0, R^\circ]$

[(L29) at $s := \max_i \sigma_i$ by (L41) and $d := \bar{\delta}$ by (L42); $R^\circ(\hat{K})$ (the proof's block); R° (Definition I.62); $\Xi \geq 1$ (Ξ, Definition 4.6, item 13); Fact A.41, item 8]

(L44) $\Xi'_{\mathrm{root}} \geq 0$

[$\Xi'_{\mathrm{root}} = \|\mathcal{L}_T\|$ (Definition 4.6, item 10); Fact A.41, item 3]

(L45) $\Xi'_{\mathrm{root}}\|e_{\mathrm{root}}\| \leq \Xi'_{\mathrm{root}}\bar{e}$

[(L15), (L44); Fact A.41, item 8]

(L46) $\forall z \in S:\ D^\circ \leq D_0^\circ(\hat{K}, R^\circ(\hat{K})) + D_Z^\circ(\hat{K})\|z'\|$

[(L45); D° (the proof's block); (I3)]

(L47) $D_0^\circ(\hat{K}, R^\circ(\hat{K})) \in [0, D_0^\circ]$

[(L43), (L30)]

(L48) $\Rightarrow\ \forall z \in S:\ \|\widetilde{t} - c\| \leq \frac{D_0^\circ + D_Z^\circ\|z'\|}{1 - \gamma - \gamma_S}$

[(L36), (L37), (L40), (L46), (L47), (L31); $\|z'\| \geq 0$ (Fact A.41, item 3); $t \mapsto 1/t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5); Fact A.41, item 8]

(L49) $\Rightarrow\ \forall z \in S:\ \|c - z'\| \leq \tau\sigma_{\max}(1 + \bar{\delta})\sqrt{N} + \frac{D_0^\circ + D_Z^\circ\|z'\|}{1 - \gamma - \gamma_S}$

[(L35), (L48); $\|x + y\| \leq \|x\| + \|y\|$ (Fact A.41, item 3)]

(L50) $\Rightarrow\ \forall z \in S:\ \|z'\| \leq \bar{T} + \bar{\Xi}_0 \left(\tau\sigma_{\max}(1 + \bar{\delta})\sqrt{N} + \frac{D_0^\circ}{1 - \gamma - \gamma_S}\right) + \frac{\bar{\Xi}_0 D_Z^\circ}{1 - \gamma - \gamma_S}\|z'\|$

[(L18), (L22), (L49); $\bar{\Xi}_0 \geq 0$ ($\bar{\Xi}_0$, the statement); Fact A.41, item 26; expand]

(L51) $1 - \bar{\Xi}_0 D_Z^\circ/(1 - \gamma - \gamma_S) > 0$

[the measured row; (L36)]

(L52) $\Rightarrow$ $\forall z \in S : \ \|z'\| \le \bar{Z}$

[(L50), (L36), (L51); $\bar{Z}$ (the statement); Fact A.41, item 26]

(L53) $\Rightarrow$ item 3

[(L52)]

□ (items 2 and 3)

Definition I.82 (The shift of the output measure at a subtree [to table])**.** The merged samples, the section of a set and the two calls' centers write the output measure at a node; the shift property says a shifted center shifts it. Let:

- $h \ge 1$;
- $T \in \mathcal{T}_n$ (Definition A.18) at $n := 2^h$;
- $m' \in \{2, 4, \dots, n\}$;
- $T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}$;
- $d \in \mathrm{Sub}(T) \cap \mathbb{R}$, a leaf diagonal;
- $a \in \mathbb{Z}^{I(T')}$;
- $y \in \mathbb{Z}^{I(d)}$;
- $m \in \{2, 4, \dots, n\}$;
- $\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m$;
- $A \subseteq \mathbb{Z}^{I(\nu)}$;
- $t' = (t'_0, t'_1) \in \mathcal{R}_m \times \mathcal{R}_m$;
- $v' \in \mathcal{R}_{m'} \times \mathcal{R}_{m'}$;
- $c \in \mathbb{Z} + i\mathbb{Z}$.

Define:

- The coordinates
  - $x^{(a)}$, the element of $\mathcal{R}^2_{m'}$ with the coordinates a (Definition G.6);
  - v'_i, the coordinates of v' (Definition G.6);
  - $\forall a \in \mathbb{Z}^{I(T_{11})} : \ A(a) := \{b \in \mathbb{Z}^{I(T_{00})} : (a, b) \in A\}$, the section of A;
- The centers and the samples
  - $\mu_{T'}(a) := \mathrm{merge}(x^{(a)})$ (merge (Algorithm 4)), the merged samples;
  - $\mu_d(y) := y_1 + iy_2$ at $y = (y_1, y_2)$, the leaf's sample;
  - $t'_{T_{11}} := \begin{cases} \mathrm{split}(t'_1) & m \ge 4 \\ t'_1 & m = 2 \end{cases}$, the first of the two calls' centers at t' (Definition A.21, items 13 and 7);
  - $\forall a \in \mathbb{Z}^{I(T_{11})} : \ t'_{T_{00}}(a) := \begin{cases} \mathrm{split}\,(t'_0 + (t'_1 - \mu_{T_{11}}(a))\, l_{10}) & m \ge 4 \\ t'_0 + (t'_1 - \mu_{T_{11}}(a))\, l_{10} & m = 2 \end{cases}$, the second of the two calls' centers at t' (Definition A.21, items 17 and 10);
  - $t_{T'}$, the center of the call at T' (Definition A.21);
- The probability measures
  - $\forall t'' \in \mathcal{R}_{m'} \times \mathcal{R}_{m'}\ \forall B \subseteq \mathbb{Z}^{I(T')} : \ Q_{T',t''}(B) := \Pr[z_{T'} \in B]$ at $t_{T'} = t''$, the output measure (Definition G.9);
- The shift property
  - $\Sigma(T', v') :\Leftrightarrow \ \forall t' \in \mathcal{R}_{m'} \times \mathcal{R}_{m'}\ \forall B \subseteq \mathbb{Z}^{I(T')} : \ Q_{T',t'+v'}(B) = Q_{T',t'}(B - (v'_i)_{i \in I(T')})$, the shift property;
  - $\Sigma(d, c) :\Leftrightarrow \ \forall t' \in \mathbb{C}\ \forall B \subseteq \mathbb{Z}^{I(d)} : \ Q_{d,t'+c}(B) = Q_{d,t'}(B - (\mathrm{Re}\, c, \mathrm{Im}\, c))$, the shift property at a leaf diagonal.

Lemma I.83 (Integer pairs on every subtree [to table])**.** *An integer pair has integer coordinates on every subtree. Let:*

- $h \ge 1$*;*
- $T \in \mathcal{T}_n$ *(Definition A.18) at* $n := 2^h$*.*

Define:

- $\forall m' \in \{2, 4, \dots, n\}\ \forall v' \in (\mathbb{Z}[x]/(x^{m'}+1))^2$*:* v'_i*, the coordinates of Definition G.6 at* $x := v'$*;*
- $I(T')$*, that of Definition A.19;*
- $\forall d \in \mathbb{R}:\ \mathrm{Sub}(d) := \{d\}$ *and* $\forall m' \in \{2, 4, \dots, n\}\ \forall \nu \in \mathcal{T}_{m'}:\ \mathrm{Sub}(\nu) := \{\nu\} \cup \mathrm{Sub}(L(\nu)) \cup \mathrm{Sub}(R(\nu))$ *(Definition A.18).*

Then

$$\forall m' \in \{2, 4, \dots, n\}\ \forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}\ \forall v' \in (\mathbb{Z}[x]/(x^{m'}+1))^2 : \quad (v'_i)_{i \in I(T')} \in \mathbb{Z}^{I(T')}.$$

Proof. (L1) $\forall i \in I(T'):\ v'_i = (v'_{c_{i,1}})_{[p_i]}$

[$c_{i,1}$, p_i (Definition G.6); Definition G.6, the coordinates at T', $x := v'$]

(L2) $\Rightarrow$ the statement

[(L1); $v'_0, v'_1 \in \mathbb{Z}[x]/(x^{m'}+1)$ (the statement)]

□

Lemma I.84 (Integer shifts at a leaf and a node [to table])**.** *A leaf diagonal passes an integer shift, and so does a node whose two children pass the shift's two halves. Let:*

- $h \geq 1$*;*
- $T \in \mathcal{T}_n$ *(Definition A.18) at* $n := 2^h$*.*

Define:

- Σ*, that of Definition I.82;*
- $Q_{d,c}(A) := \Pr[z_d \in A]$ *at* $t_d = c$*, the output measure (Definition G.9 at* $T' := d$*);*
- $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\}:\ (\sigma_j, \sigma_{j+1}) := (s/\sqrt{d_j},\ s/\sqrt{d_{j+1}})$ *(Definition A.21, item 1;* $I(d)$*,* d_j *of Definition A.19).*

Then

1. $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R}\ \forall v' \in \mathbb{Z} + i\mathbb{Z}:\quad \Sigma(d, v')$*;*
2. *Let:*
   - $m \in \{2, 4, \dots, n\}$*;*
   - $\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11}) \in \mathrm{Sub}(T) \cap \mathcal{T}_m$*;*
   - $v' = (v_0, v_1) \in (\mathbb{Z}[x]/(x^m+1))^2$*.*

   Define:
   - $w_1 := \begin{cases} \mathrm{split}(v_1) & m \geq 4 \\ v_1 & m = 2 \end{cases}$*;*
   - $w_0 := \begin{cases} \mathrm{split}(v_0) & m \geq 4 \\ v_0 & m = 2 \end{cases}$*.*

   Then $[\Sigma(T_{11}, w_1),\ \Sigma(T_{00}, w_0)] \Rightarrow\ \Sigma(\nu, v')$*.*

Proof. Proof of item 1.

(L1) $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R},\ I(d) = \{j, j+1\}\ \forall c \in \mathbb{C}\ \forall z_j, z_{j+1} \in \mathbb{Z}:\ Q_{d,c}(\{(z_j, z_{j+1})\}) = D_{\mathbb{Z},\sigma_j,\mathrm{Re}\,c}(z_j)\, D_{\mathbb{Z},\sigma_{j+1},\mathrm{Im}\,c}(z_{j+1})$

[$Q_{d,c}$ (the statement; Definition G.9); Definition A.21, items 1, 2 and 3]

(L2) $\forall \sigma > 0\ \forall c \in \mathbb{R}\ \forall k \in \mathbb{Z}:\ \rho_{\sigma,c+k}(\mathbb{Z}) = \rho_{\sigma,c}(\mathbb{Z})$

[Definition A.2, item 1; the sum over $\mathbb{Z}$ reindexed at $x := x' + k$]

(L3) $\forall \sigma > 0\ \forall c \in \mathbb{R}\ \forall k \in \mathbb{Z}\ \forall z \in \mathbb{Z}:\ D_{\mathbb{Z},\sigma,c+k}(z+k) = D_{\mathbb{Z},\sigma,c}(z)$

[(L2); Definition A.2, items 1 and 2]

(L4) $\forall \sigma > 0\ \forall c \in \mathbb{R}\ \forall k \in \mathbb{Z}\ \forall A \subseteq \mathbb{Z}:\ D_{\mathbb{Z},\sigma,c+k}(A) = D_{\mathbb{Z},\sigma,c}(A-k)$

[(L3) summed over A]

(L5) $I(d) = \{j, j+1\}$

[Definition A.19]

(L6) $\forall x \in \mathcal{R}_2 :\ (x_j, x_{j+1}) = (x_{[0]}, x_{[1]})$

[Definition G.6, the coordinates at d]

(L7) $\forall v' \in \mathbb{Z} + i\mathbb{Z} :\ v' = \operatorname{Re} v' + x \operatorname{Im} v'$

[$\mathcal{R}_2 = \mathbb{C}$, $x \mapsto i$ (Definition A.21)]

(L8) $\forall v' \in \mathbb{Z} + i\mathbb{Z} :\ (v'_j, v'_{j+1}) = (\operatorname{Re} v',\ \operatorname{Im} v')$

[(L5), (L6), (L7)]

(L9) $\forall v' \in \mathbb{Z} + i\mathbb{Z} :\ (\operatorname{Re} v',\ \operatorname{Im} v') \in \mathbb{Z}^2$

[$v' \in \mathbb{Z} + i\mathbb{Z}$]

(L10) $\Rightarrow\ \forall v' \in \mathbb{Z} + i\mathbb{Z} :\ (v'_j, v'_{j+1}) \in \mathbb{Z}^2$

[(L8), (L9)]

(L11) $\Rightarrow\ \forall d \in \operatorname{Sub}(T) \cap \mathbb{R}\ \forall v' \in \mathbb{Z} + i\mathbb{Z} :\ \Sigma(d, v')$

[(L1), (L9); (L4) at $k := \operatorname{Re} v'$ on the first factor and at $k := \operatorname{Im} v'$ on the second; Σ (Definition I.82)]

(L12) $\Rightarrow$ item 1

[(L11)]

□ (item 1)

Proof of item 2.

(L13) $\forall \nu \in \operatorname{Sub}(T) \cap \mathcal{T}_m\ \forall t'\ \forall a \in \mathbb{Z}^{I(T_{11})}\ \forall b \in \mathbb{Z}^{I(T_{00})}$:

$$Q_{\nu,t'}(\{(a,b)\}) = Q_{T_{11},t'_{T_{11}}}(\{a\})\, Q_{T_{00},t'_{T_{00}}(a)}(\{b\})$$

[Fact A.45, item 1, over the samples $z_{T_{11}}$ then $z_{T_{00}}$ (Definition A.21, items 13 to 17); $t'_{T'}$ (Definition I.82, the two calls' centers)]

(L14) $\forall A \subseteq \mathbb{Z}^{I(\nu)} :\ A = \bigcup_{a \in \mathbb{Z}^{I(T_{11})}} \{a\} \times A(a)$

[$A(a)$ (Definition I.82, the section)]

(L15) $\forall \nu \in \operatorname{Sub}(T) \cap \mathcal{T}_m\ \forall t'\ \forall A \subseteq \mathbb{Z}^{I(\nu)}$:

$$Q_{\nu,t'}(A) = \sum_{a \in \mathbb{Z}^{I(T_{11})}} Q_{T_{11},t'_{T_{11}}}(\{a\})\, Q_{T_{00},t'_{T_{00}}(a)}(A(a))$$

[(L13), (L14); Fact A.45, item 9]

(L16) $m \geq 4 \Rightarrow\ (t' + v')_{T_{11}} = t'_{T_{11}} + w_1$

[$t'_{T_{11}}$ (Definition I.82) at t' and at $t' + v'$; split linear (Lemma B.3); w_1 (the statement)]

(L17) $m = 2 \Rightarrow\ (t' + v')_{T_{11}} = t'_{T_{11}} + w_1$

[$t'_{T_{11}}$ (Definition I.82) at $m = 2$, at t' and at $t' + v'$; w_1 (the statement)]

(L18) $\forall \nu\ \forall t'\ \forall v' = (v_0, v_1) \in (\mathbb{Z}[x]/(x^m + 1))^2\ \forall A$:

$$Q_{\nu,t'+v'}(A) = \sum_a Q_{T_{11},t'_{T_{11}}+w_1}(\{a\})\, Q_{T_{00},(t'+v')_{T_{00}}(a)}(A(a))$$

[(L15) at $t' + v'$; (L16), (L17)]

(L19) $\Sigma(T_{11}, w_1) \Rightarrow\ \forall a :\ Q_{T_{11},t'_{T_{11}}+w_1}(\{a\}) = Q_{T_{11},t'_{T_{11}}}(\{a - ((w_1)_i)_{i \in I(T_{11})}\})$

[Σ (Definition I.82) at T_{11}, its center $t' := t'_{T_{11}}$ and $B := \{a\}$]

Lemma I.83 at $m \geq 4$	This proof
Shared: h, n, T, $\operatorname{Sub}(T)$ (Definition A.18)	
Shared: $h \geq 1$, $T \in \mathcal{T}_n$	
m'	$m/2$ (the statement)
T'	T_{11} (the statement)
v'	w_1 (the statement)
$m' \in \{2, 4, \ldots, n\}$	The scope; m (the statement)
$T' \in \operatorname{Sub}(T) \cap \mathcal{T}_{m'}$	ν, T_{11} (the statement); $\operatorname{Sub}(T)$, $\mathcal{T}_m$ (Definition A.18)
$v' \in (\mathbb{Z}[x]/(x^{m'} + 1))^2$	w_1 (the statement); split (Lemma B.3)
Its conclusion: $(v'_i)_{i \in I(T')} \in \mathbb{Z}^{I(T')}$	

(I1)

(L20) $((w_1)_i)_{i \in I(T_{11})} \in \mathbb{Z}^{I(T_{11})}$

[(I1) at $m \geq 4$; (L10) at $m = 2$, $v' := w_1$; w_1 (the statement); $\mathcal{R}_2 = \mathbb{C}$, $x \mapsto i$ (Definition A.21)]

(L21) $\{a' + ((w_1)_i)_{i \in I(T_{11})} : a' \in \mathbb{Z}^{I(T_{11})}\} = \mathbb{Z}^{I(T_{11})}$

[(L20)]

(L22) $\Rightarrow\ \Sigma(T_{11}, w_1) \Rightarrow\ \forall A \subseteq \mathbb{Z}^{I(\nu)}$:

$$Q_{\nu,t'+v'}(A) = \sum_{a'} Q_{T_{11},t'_{T_{11}}}(\{a'\})\, Q_{T_{00},(t'+v')_{T_{00}}(a'+((w_1)_i)_{i\in I(T_{11})})}(A(a' + ((w_1)_i)_{i\in I(T_{11})}))$$

[(L18), (L19), (L21)]

(L23) $x^{(a'+((w_1)_i)_{i\in I(T_{11})})} = x^{(a')} + w_1$

[Fact G.7, item 4]

(L24) $\mathrm{merge}(\mathrm{split}(v_1)) = v_1$

[Postconditions of split (Algorithm 2) and merge (Algorithm 4)]

(L25) $m \geq 4 \Rightarrow\ \forall a' :\ \mu_{T_{11}}(a' + ((w_1)_i)_{i\in I(T_{11})}) = \mu_{T_{11}}(a') + v_1$

[(L23), (L24); $\mu_{T_{11}}$ (Definition I.82); merge linear (Lemma G.18)]

(L26) $m = 2 \Rightarrow\ \forall a' :\ \mu_d(a' + (\mathrm{Re}\, v_1, \mathrm{Im}\, v_1)) = \mu_d(a') + v_1$

[$\mu_d(a_1, a_2) = a_1 + ia_2$ (Definition I.82, the merged samples); $w_1 = v_1$ at $m = 2$ (the statement)]

(L27) $\forall v_0, v_1 :\ tb_0(t_0 + v_0, t_1 + v_1, z_1 + v_1) = tb_0(t_0, t_1, z_1) + v_0$

[$tb_0 = t_0 + (t_1 - z_1)l_{10}$ (Definition A.21, item 16)]

(L28) $\forall a' :\ t'_0 + v_0 + (t'_1 + v_1 - \mu_{T_{11}}(a') - v_1)\, l_{10} = (t'_0 + (t'_1 - \mu_{T_{11}}(a'))\, l_{10}) + v_0$

[(L27) at $(t_0, t_1) := (t'_0, t'_1)$ and $z_1 := \mu_{T_{11}}(a')$]

(L29) $\Rightarrow\ \forall a' :\ (t' + v')_{T_{00}}(a' + ((w_1)_i)_{i\in I(T_{11})}) = t'_{T_{00}}(a') + w_0$

[w_0 (the statement); $t'_{T_{00}}(a)$ (Definition I.82) at t' and at $t' + v'$; (L25), (L26), (L28); split linear (Lemma B.3)]

(L30) $\Sigma(T_{00}, w_0) \Rightarrow\ \forall a'\ \forall B \subseteq \mathbb{Z}^{I(T_{00})} :\ Q_{T_{00},t'_{T_{00}}(a')+w_0}(B) = Q_{T_{00},t'_{T_{00}}(a')}(B - ((w_0)_i)_{i\in I(T_{00})})$

[Σ (Definition I.82) at T_{00}, its center $t' := t'_{T_{00}}(a')$ and $B := A(a' + ((w_1)_i)_{i\in I(T_{11})})$]

(L31) $(v'_i)_{i\in I(T_{11})} = ((w_1)_i)_{i\in I(T_{11})}$

[Fact G.7, items 1 and 2, at ν; w_1 (the statement)]

(L32) $(v'_i)_{i\in I(T_{00})} = ((w_0)_i)_{i\in I(T_{00})}$

[Fact G.7, items 1 and 3, at ν; w_0 (the statement)]

(L33) $\forall A \subseteq \mathbb{Z}^{I(\nu)} :\ (a', b') \in A - (v'_i)_{i\in I(\nu)} \iff (a' + ((w_1)_i)_{i\in I(T_{11})},\ b' + ((w_0)_i)_{i\in I(T_{00})}) \in A$

[(L31), (L32)]

(L34) $\forall A \subseteq \mathbb{Z}^{I(\nu)}\ \forall a' :\ A(a' + ((w_1)_i)_{i\in I(T_{11})}) - ((w_0)_i)_{i\in I(T_{00})} = (A - (v'_i)_{i\in I(\nu)})(a')$

[$A(a)$ (Definition I.82); (L33)]

(L35) $\Rightarrow\ [\Sigma(T_{11}, w_1),\ \Sigma(T_{00}, w_0)] \Rightarrow\ \forall A \subseteq \mathbb{Z}^{I(\nu)}$:

$$Q_{\nu,t'+v'}(A) = \sum_{a'} Q_{T_{11},t'_{T_{11}}}(\{a'\})\, Q_{T_{00},t'_{T_{00}}(a')}((A - (v'_i)_{i\in I(\nu)})(a'))$$

[(L22), (L29), (L30) at $B := A(a' + ((w_1)_i)_{i\in I(T_{11})})$, (L34)]

(L36) $\Rightarrow\ [\Sigma(T_{11}, w_1),\ \Sigma(T_{00}, w_0)] \Rightarrow\ \forall t'\ \forall A \subseteq \mathbb{Z}^{I(\nu)} :\ Q_{\nu,t'+v'}(A) = Q_{\nu,t'}(A - (v'_i)_{i\in I(\nu)})$

[(L35); (L15) at $A := A - (v'_i)_{i\in I(\nu)}$]

(L37) $\Rightarrow$ item 2

[(L36); Σ (Definition I.82)]

□ (item 2)

Proposition I.85 (Shift of the output measure by an integer center [to table])**.** *An integer shift of the center shifts the output measure by the shift's coordinates. Let:*

- $h \geq 1$;
- $T \in \mathcal{T}_n$ *(Definition A.18) at* $n := 2^h$;
- $t \in \mathcal{R}_n \times \mathcal{R}_n$.

Define:

- $Q_{T,t}(A) := \Pr[z_T \in A]$ *at* $t_T = t$, *the output measure (Definition G.9);*
- $\forall v \in (\mathbb{Z}[x]/(x^n + 1))^2$*:* v_i*, the coordinates of Definition G.6 at* $x := v$;

- $N := 2n$;
- Σ, *that of Definition I.82.*

Then

$$\forall v \in (\mathbb{Z}[x]/(x^n+1))^2\ \forall A \subseteq \mathbb{Z}^N : \quad Q_{T,\,t+v}(A) = Q_{T,\,t}(A - (v_i)_{i\le N}).$$

Proof.

DEFINES w_0 and w_1, those of Lemma I.84

(L1) $\forall v' = (v_0, v_1) \in (\mathbb{Z}[x]/(x^m+1))^2,\ m \ge 4 :\ w_1, w_0 \in (\mathbb{Z}[x]/(x^{m/2}+1))^2$

[split$(\mathbb{Z}[x]/(x^m+1)) \subseteq (\mathbb{Z}[x]/(x^{m/2}+1))^2$ (Lemma B.3)]

(L2) $\forall v' = (v_0, v_1) \in (\mathbb{Z}[x]/(x^2+1))^2 :\ w_1, w_0 \in \mathbb{Z} + i\mathbb{Z}$

[$\mathcal{R}_2 = \mathbb{C}$, $x \mapsto i$ (Definition A.21); w_1, w_0 at $m = 2$ (Lemma I.84, item 2)]

Lemma I.84, item 1 at (T_{11}, w_1) and at (T_{00}, w_0), $m = 2$	This proof
Shared: h, n, T, Σ (Definition I.82)	
Shared: $h \ge 1$, $T \in \mathcal{T}_n$	
(I1) d	T_{11}, T_{00} (Definition A.18)
v'	w_1, w_0 (the statement)
$d \in \mathrm{Sub}(T) \cap \mathbb{R}$	T_{11}, T_{00} at $m = 2$ (Definition A.18)
$v' \in \mathbb{Z} + i\mathbb{Z}$	(L2)
Its item 1: $\Sigma(d, v')$	

Lemma I.84, item 2 at $m = 2$ and at every $m \in \{4, \dots, n\}$, $\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m$ and $v' \in (\mathbb{Z}[x]/(x^m+1))^2$	This proof
(I2) Shared: h, n, T, Σ (Definition I.82), m, ν, v', w_0, w_1	
Shared: $h \ge 1$, $T \in \mathcal{T}_n$, $m \in \{2, 4, \dots, n\}$, $\nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m$, $v' \in (\mathbb{Z}[x]/(x^m+1))^2$	
$\nu = \mathrm{node}(l_{10};\ T_{00}, T_{11})$	$\mathcal{T}_m$ (Definition A.18)
Its item 2: $[\Sigma(T_{11}, w_1),\ \Sigma(T_{00}, w_0)] \Rightarrow\ \Sigma(\nu, v')$	

(L3) $\forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_2\ \forall v' \in (\mathbb{Z}[x]/(x^2+1))^2 :\ \Sigma(\nu, v')$

[(I2) at $m = 2$; (I1)]

(L4) $\forall m \in \{4, \dots, n\} :\ [\forall \nu' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m/2}\ \forall v'' \in (\mathbb{Z}[x]/(x^{m/2}+1))^2 :\ \Sigma(\nu', v'')]$

$\Rightarrow\ \forall \nu \in \mathrm{Sub}(T) \cap \mathcal{T}_m\ \forall v' \in (\mathbb{Z}[x]/(x^m+1))^2 :\ \Sigma(\nu, v')$

[(I2) at m; $T_{00}, T_{11} \in \mathrm{Sub}(T) \cap \mathcal{T}_{m/2}$ (Definition A.18); $w_1, w_0 \in (\mathbb{Z}[x]/(x^{m/2}+1))^2$ by (L1)]

(L5) $\Rightarrow\ \forall m' \in \{2, 4, \dots, n\}\ \forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}\ \forall v' \in (\mathbb{Z}[x]/(x^{m'}+1))^2 :\ \Sigma(T', v')$

[induction on m: (L3) the base, (L4) the step]

(L6) $\Rightarrow\ \forall v \in (\mathbb{Z}[x]/(x^n+1))^2\ \forall A \subseteq \mathbb{Z}^N :\ Q_{T,t+v}(A) = Q_{T,t}(A - (v_i)_{i\le N})$

[(L5) at $T' = T$; Σ (Definition I.82) at $t' := t$; $I(T) = \{1, \dots, N\}$ (Definition A.19)]

(L7) $\Rightarrow$ the statement

[(L6)]

□

Lemma I.86 (The output measure's shift by the integer part [to table])**.** *The center's integer part shifts the output measure at its fractional part by integer coordinates. Define:*

- n, *that of* FFT *(Algorithm 14), Precondition;*
- T, *the tree* ffSampling$^{\mathcal{F}}$ *(Algorithm 10) samples on at the key, line 24;*
- $Q_{T,t}(A) := \Pr[z_T \in A]$ *at* $t_T = t$, *the output measure (Definition G.9);*
- t_{int} *and* t_{frac}, *those of* center$_{\mathrm{frac}}$ *(Algorithm 17) at the key and* $\mathsf{h}(\mathsf{m})$;
- $(t_{\mathrm{int}})_i$, *those of Definition G.6 at* $x := t_{\mathrm{int}}$.

Then

1. $\forall A \subseteq \mathbb{Z}^N :\ Q_{T,\, t_{\text{int}}+t_{\text{frac}}}(A) = Q_{T,\, t_{\text{frac}}}(A - ((t_{\text{int}})_i)_{i\le N})$;

2. $((t_{\text{int}})_i)_{i\le N} \in \mathbb{Z}^N$.

Proof. (L1) $t_{\text{int}} \in (\mathbb{Z}[x]/(x^n+1))^2$

$[t_{\text{int}} = (qt - qt_{\text{frac}})/q$ (center$_{\text{frac}}$ (Algorithm 17), line 5); $qt - qt_{\text{frac}} \in q\,(\mathbb{Z}[x]/(x^n+1))^2$ (line 4)]

Lemma I.83	This proof
Shared: $n,\ T$	
m'	n
T'	T
v'	t_{int}
(I1) $h \ge 1$	$n = 2^h,\ h \ge 1$ (FFT (Algorithm 14), Precondition)
$T \in \mathcal{T}_n$	T (ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 24)
$m' \in \{2, 4, \ldots, n\}$	$n = 2^h,\ h \ge 1$ (FFT (Algorithm 14), Precondition)
$T' \in \text{Sub}(T) \cap \mathcal{T}_{m'}$	Sub(T) (Definition A.18)
$v' \in (\mathbb{Z}[x]/(x^{m'}+1))^2$	(L1)
Its conclusion: $(v'_i)_{i\in I(T')} \in \mathbb{Z}^{I(T')}$	

(L2) $((t_{\text{int}})_i)_{i\le N} \in \mathbb{Z}^N$

$[$(I1); $I(T) = \{1, \ldots, N\}$ (Definition A.19)$]$

(L3) $\Rightarrow$ item 2

[(L2)]

Proposition I.85	This proof
Shared: $n,\ T,\ Q_{T,t}$ (Definition G.9), N	
t	t_{frac} (center$_{\text{frac}}$ (Algorithm 17))
v	t_{int}
(I2) $h \ge 1$	$n = 2^h,\ h \ge 1$ (FFT (Algorithm 14), Precondition)
$T \in \mathcal{T}_n$	T (ffSampling$^{\mathcal{F}}$ (Algorithm 10), line 24)
$t \in \mathcal{R}_n \times \mathcal{R}_n$	$t_{\text{frac}} \in \mathcal{R}_n \times \mathcal{R}_n$ (center$_{\text{frac}}$ (Algorithm 17))
$v \in (\mathbb{Z}[x]/(x^n+1))^2$	(L1)
Its conclusion: $\forall v \in (\mathbb{Z}[x]/(x^n+1))^2\ \forall A \subseteq \mathbb{Z}^N :\ Q_{T,\,t+v}(A) = Q_{T,\,t}(A - (v_i)_{i\le N})$	

(L4) $\Rightarrow\ \forall A \subseteq \mathbb{Z}^N :\ Q_{T,\, t_{\text{int}}+t_{\text{frac}}}(A) = Q_{T,\, t_{\text{frac}}}(A - ((t_{\text{int}})_i)_{i\le N})$

[(I2)]

(L5) $\Rightarrow$ item 1

[(L4)]

□ (items 1 and 2)

I.7.2 The loss

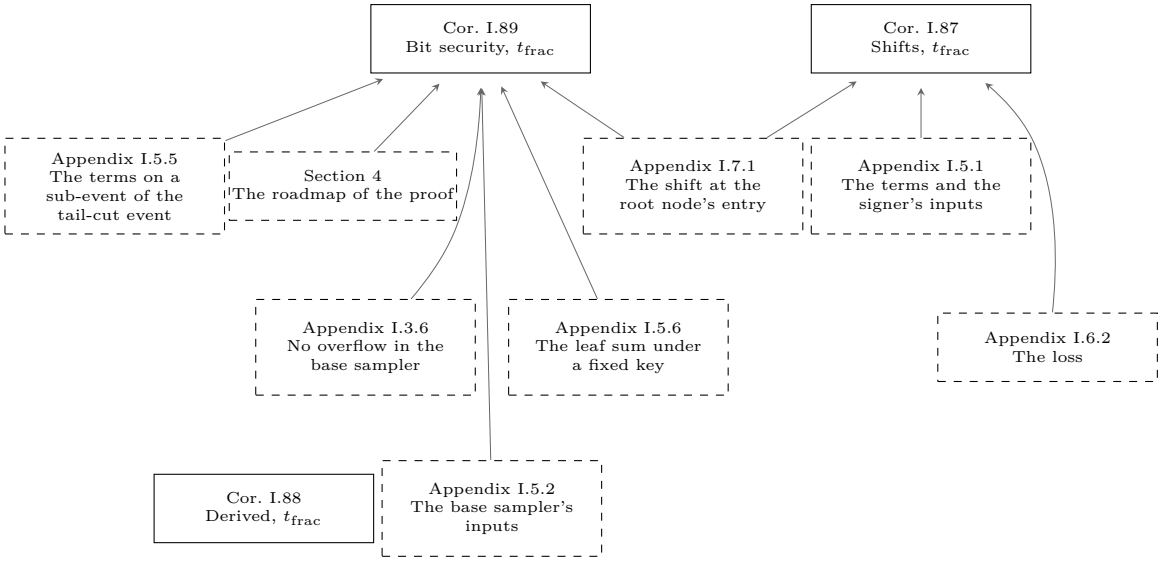


Figure 93: Dependencies, Appendix I.7.2.

Corollary I.87 (Root shift and center-shift bound at the center t_{frac} [to table])**.** *At $n = 1024$, the center t_{frac}'s bound on the shift at the root node's entry is below that of the center t, and its center-shift bound takes the value below. Define:*

- *n, that of* FFT *(Algorithm 14), Precondition;*
- *$\bar{e}$, the bound of Lemma I.81, item 1;*
- *$\tau := 21.91$ (Corollary I.78);*
- *$\bar{T} := \sqrt{n/2}$ (Lemma I.81);*
- *$\bar{Z}$, that of Lemma I.81 at τ;*
- *D_0°, D_Z°, γ and γ_S, those of Definition I.62 at $\bar{e}$, $\bar{T}$ and τ;*
- *$D^\circ := D_0^\circ + D_Z^\circ \bar{Z}$ (Definition I.62);*
- *$D_S := D^\circ/(1 - \gamma - \gamma_S)$ (Definition I.62);*
- *$\bar{e}'$, the bound of Lemma I.76.*

Assume:

(A1) $n = 1024$.

Measured [gate: `verify/reports/fx/terms.py`]:

- *$\bar{e}$ at $n = 1024$;*
- *D_S at $n = 1024$.*

Then

1. *$\bar{e} = 2^{-46.9}$;*
2. *$\bar{e} < \bar{e}'$;*
3. *$D_S = 2^{-8.9}$.*

Proof. (I1)

Corollary I.78, item 1	This proof
Shared: n, τ Shared: assumption A1	
$\bar{e}$	$\bar{e}'$ (the statement)
Its conclusion: $\bar{e} = 2^{-28.6}$	
$\bar{e}' = 2^{-28.6}$	

[(I1)]

(L2) $\bar{e} = 2^{-46.9}$
[the first measured row at $n = 1024$; assumption A1]

(L3) $\Rightarrow$ item 1
[(L2)]

(L4) $\bar{e} < \bar{e}'$
[(L1), (L2); expand]

(L5) $\Rightarrow$ item 2
[(L4)]

(L6) $D_S = 2^{-8.9}$
[the second measured row at $n = 1024$; assumption A1]

(L7) $\Rightarrow$ item 3
[(L6)]
□ (items 1 to 3)

Corollary I.88 (No bit from the derived bounds at the center t_{frac} [to table])**.** *On the derived bounds, our proof keeps no bit at the center t_{frac} at the searched tail-cut rate; the bit security it keeps is that at the tail (Table 34). Let:*

- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$.

Define:

- *n, that of* FFT *(Algorithm 14), Precondition;*
- *$\bar{e}$, the bound of Lemma I.81, item 1;*
- *$\bar{T} := \sqrt{n/2}$ (Lemma I.81);*
- *λ, that of Definition I.62;*
- *$\forall \tau' > 1 :\ \lambda_{\mathcal{F}}(\tau')$, that of Corollary 5.10 at $c := t_{\text{frac}}$, $\bar{e}$, $\bar{T}$, the $\bar{Z}$ of Lemma I.81 at τ', $\tau := \tau'$ and $M_C := 0$.*

Measured [gate: `verify/reports/fx/terms.py`]:

- *τ, the value a golden-section search of $\lambda - \lambda_{\mathcal{F}}(\tau')$ over $\tau' \in [1.5, 60]$ returns, at each (n, λ, Q_s) (`verify/lib/renyi_terms.py`);*
- *$\lambda - \lambda_{\mathcal{F}}(\tau)$ at every (n, λ, Q_s).*

Then

1. *$\forall (n, \lambda, Q_s) :\ \lambda - \lambda_{\mathcal{F}}(\tau) \geq \lambda$;*
2. *Assume:*

   (A1) $(n, \lambda, Q_s) = (512, 128, 2^{32})$.

   Then $\lambda - \lambda_{\mathcal{F}}(\tau) = 3.46e + 03$.

Proof. (L1) $\forall (n, \lambda, Q_s) :\ \lambda - \lambda_{\mathcal{F}}(\tau) \geq \lambda$
[the second measured row at every (n, λ, Q_s)]

(L2) $\Rightarrow$ item 1
[(L1)]

(L3) $\lambda - \lambda_{\mathcal{F}}(\tau) = 3.46e + 03$
[the second measured row at $(512, 128, 2^{32})$; assumption A1]

(L4) $\Rightarrow$ item 2
[(L3)]
□ (items 1 and 2)

Corollary I.89 (Under **Hypotheses I.21 and I.22**, the bit security at the center t_{frac} [to table])**.** *At a key whose matrix K, leaf standard deviations and remainder lie within three thresholds, the fixed-point signer at the center t_{frac} keeps the bit security below, the leaf sum read at the tail of*

Lemma 4.14 with one failure probability η; every term is read at one tail-cut rate, the least multiple of 0.01 whose tail costs at most $2^{-\lambda-10}$. ***Under Hypotheses I.21 and I.22****, let:*

- (f, g, F, G) *be a checked key of degree* n *(Definition 5.5) passing the tail checks at* t_{frac} *(Definition 5.6);*
- $Q_s \in \{2^{32}, 2^{36}, \dots, 2^{64}\}$.

Define:

- *The signer's words and parameters*
  - $(\lambda, \alpha) := \begin{cases} (128, 257) & n = 512 \\ (256, 513) & n = 1024 \end{cases}$ *(Definition I.62);*
  - $\eta := 2^{-\lambda}$;
- *The stored words*
  - M_n, D_n *and* B_n, *those of Definition I.14 at* n *and the center* t_{frac};
  - τ_K, *that of Definition I.14 at* n *and the center* t_{frac};
- *The leaf deviations*
  - ϵ_{hi}, *that of Lemma I.65;*
  - $s_\star := \sigma_{\min}(1 - D_n)\,(\alpha_L + (1-\alpha_L)(1-D_n)^2)^{-1/2}$ *(Definition I.62 at* $\bar\delta := D_n$*);*
  - $\epsilon_D := 2\sum_{k\ge 1} e^{-2\pi^2 s_\star^2 k^2}$ *(Definition I.62 at* $\bar\delta := D_n$*);*
- *The tail-cut event*
  - $\tau := \min\{\, \tau' \in 0.01\mathbb{Z} : \tau' > 1,\ Q_s N(1+\epsilon_{\mathrm{hi}})(1+\epsilon_D)(1-\epsilon_D)^{-1}\tau' e^{(1-\tau'^2)/2} \le 2^{-\lambda-10} \,\}$ *at each* (n, λ, Q_s);
  - $S_\tau := \{\, z \in \mathbb{Z}^N : \forall i \le N\ |z_i - \widetilde{t}_i(z_{<i})| \le \tau\, \widetilde{\sigma}_i(z_{<i}) \,\}$ *(Definition A.26);*
  - $S_{\tau_K} := \{\, z \in \mathbb{Z}^N : \forall i \le N\ |z_i - \widetilde{t}_i(z_{<i})| \le \tau_K\, \widetilde{\sigma}_i(z_{<i}) \,\}$ *(Definition A.26 at* $\tau := \tau_K$*, the key,* $\mathsf{h}(\mathsf{m})$ *and the center* t_{frac}*);*
- *The leaf perturbations*
  - I_N, $\widetilde{\sigma}_i$, K, r, δ_i *and* μ_{key}, *those of Definition 4.12 at* $\mathcal{F}_{\mathrm{fx}}$, *the key,* $\mathsf{h}(\mathsf{m})$ *and* $t_{\mathrm{c}} := t_{\mathrm{frac}}$;
  - W *and* W^{tail}, *those of Lemma 4.14 at* $\mathcal{F}_{\mathrm{fx}}$, *the key,* $\mathsf{h}(\mathsf{m})$, $t_{\mathrm{c}} := t_{\mathrm{frac}}$, τ, $M := M_n$, $D := D_n$, $B := B_n$, $\eta_1 := \eta/Q_s$ *and the inputs of Lemma I.73;*
- *The sub-event*
  - $E := \{\, z \in \mathbb{Z}^N : W(z) \le W^{\mathrm{tail}} \,\}$;
- *The probability measures*
  - P, $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$, *those of Proposition I.72 at the key and* $c := t_{\mathrm{frac}}$;
- *The terms*
  - $\lambda_{\mathcal{F}}$, p'_τ, ε_0° *and* A, *those of Proposition I.72 at* $c := t_{\mathrm{frac}}$, *at* Q_s, τ, $W^\circ := W^{\mathrm{tail}}$, $\bar\delta := D_n$, E, $\eta_E := \eta$ *and* $M_C := 0$, *and at the* $\bar e$, $\bar T$ *and* $\bar Z$ *of Lemma I.81 at* τ;
  - $y := (2^{-\lambda} e^{Q_s A})^{(\alpha-1)/\alpha}$ *(Definition 5.3 at* A*);*
  - $\lambda_n^{64} := \begin{cases} 126.70 & n = 512 \\ 253.53 & n = 1024 \end{cases}$ *(Table 34 at* $Q_s = 2^{64}$*).*

Assume:

(A1) $\mu_{\mathrm{key}} \le M_n$;

(A2) $\forall i \le N\ \forall z_{<i} :\ |\delta_i(z_{<i})| \le D_n$;

(A3) $\forall z \in S_{\tau_K} :\ \sum_{i\le N} (r(I_N + K))_i^2/\widetilde{\sigma}_i^2 \le B_n$.

Measured:

- $\tau_K = \tau$ *at* $(n, \lambda, 2^{64})$ *[gate: verify/gates/fx/tail_copy_tau.py];*
- $-\log_2(Q_s N\, p'_\tau + y + \eta)$ *at least the cell of Table 34 at every* (n, λ, Q_s) *[gate: verify/gates/fx/tail_level_cells.py];*
- $(1+D_n)^2 < \alpha_L/(\alpha_L - 1)$ *at* $n \in \{512, 1024\}$ *[gate: verify/gates/fx/tail_conditions.py];*
- $\varepsilon_0^\circ < 1$ *at every* (n, λ, Q_s) *[gate: verify/gates/fx/tail_conditions.py];*
- W^{tail} *at* $(n, Q_s) = (1024, 2^{64})$ *[gate: verify/gates/fx/tail_w.py];*
- $p'_\tau < 1$ *at every* (n, λ, Q_s) *[gate: verify/gates/fx/tail_conditions.py].*

Then

1. $Q_s P(S_\tau \cap E^c) \le \eta$;

2. $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$;

3. *Assume:*

   (A4) $(n, \lambda, Q_s) = (512, 128, 2^{60})$.

   Then $\lambda_{\mathcal{F}} \ge 126.72$;

4. *Assume:*

   (A5) $(n, \lambda, Q_s) = (1024, 256, 2^{60})$.

   Then $\lambda_{\mathcal{F}} \ge 254.66$;

5. *Assume:*

   (A6) $(n, Q_s) = (1024, 2^{64})$.

   Then $W^{\mathrm{tail}} = 2^{-79.2}$;

6. $\lambda_{\mathcal{F}} \ge \lambda_n^{64}$.

Proof. Proof of item 1.

(L1) $Q_s \le 2^{64}$

[Q_s (the statement)]

(L2) $\epsilon_D = \varepsilon_0^{\circ}$

[ϵ_D, $s_\star$ (Definition I.62 at $\bar{\delta} := D_n$); ε_0°, r_-, $\underline{s}$ (Definition A.40 at $\alpha := \alpha_L$, $s_{\mathrm{lo}} := \sigma_{\min}$, $\bar{\delta} := D_n$, as Proposition I.72 instantiates it); θ_{α_L} (Definition A.29); ε_0 (Definition A.38)]

(L3) $\epsilon_D < 1$

[(L2); the fourth measured row]

(L4) $N(1+\epsilon_{\mathrm{hi}})(1+\epsilon_D)(1-\epsilon_D)^{-1}\tau_K e^{(1-\tau_K^2)/2} \ge 0$

[$N := 2n$ (Definition A.25); $n \in \{512, 1024\}$ (Definition 5.5, item 1); ϵ_{hi} (the statement); ϵ_D, a sum of exponentials (Definition I.62); (L3); τ_K (the statement); Fact A.41, items 28, 12 and 8]

(L5) $Q_s N(1+\epsilon_{\mathrm{hi}})(1+\epsilon_D)(1-\epsilon_D)^{-1}\tau_K e^{(1-\tau_K^2)/2} \le 2^{64} N(1+\epsilon_{\mathrm{hi}})(1+\epsilon_D)(1-\epsilon_D)^{-1}\tau_K e^{(1-\tau_K^2)/2}$

[(L1), (L4); Fact A.41, item 26]

(L6) $2^{64} N(1+\epsilon_{\mathrm{hi}})(1+\epsilon_D)(1-\epsilon_D)^{-1}\tau_K e^{(1-\tau_K^2)/2} \le 2^{-\lambda-10}$

[$\tau_K = \tau$ at $(n, \lambda, 2^{64})$ (the statement, the measured row); τ (the statement)]

(L7) $\Rightarrow\ \tau \le \tau_K$

[(L5), (L6); τ and τ_K (the statement)]

Lemma I.51, item 1 at every $i \le N$ and $z_{<i}$	This proof
Shared: (f, g, F, G), $\sigma_{\min}$ (Definition I.62)	
(I1) `isigma`	$1/\widetilde{\sigma}_i$ (Definition A.25)
$n \in \{512, 1024\}$	Definition 5.5, item 1
`isigma` taken by a call of SamplerZ by deepest	The i-th call of ffSampling$^{\mathcal{F}}$ at t_{frac} (Definition A.25), at deepest (Algorithm 7)
Its conclusion: $\widetilde{\sigma} > \sigma_{\min}$	

(L8) $\forall i \le N\ \forall z_{<i} :\ \widetilde{\sigma}_i > \sigma_{\min}$

[(I1)]

(L9) $\sigma_{\min} > 0$

[the stored word `FXP_SIGMA_MIN` [L0: `fxp/fxp_consts.h:2073-2084`]]

(L10) $\Rightarrow\ \forall z \in S_\tau\ \forall i \le N :\ |z_i - \widetilde{t}_i(z_{<i})| \le \tau_K \widetilde{\sigma}_i$

[(L7), (L8), (L9); S_τ (the statement); Fact A.41, item 26]

(L11) $\Rightarrow\ S_\tau \subseteq S_{\tau_K}$

[(L10); S_{τ_K} (the statement)]

(L12) $\Rightarrow\ \forall z \in S_\tau :\ \sum_{i\le N}(r(I_N+K))_i^2/\widetilde{\sigma}_i^2 \le B_n$

[(L11); assumption A3]

(L13) $D_n \in [0,1)$

[D_n (Definition I.14)]

(L14) $\eta/Q_s \in (0,1)$

[$\eta := 2^{-\lambda}$ and Q_s (the statement)]

Lemma 4.14	This proof
Shared: (f,g,F,G), $\mathsf{h}(\mathsf{m})$, τ, ϵ_{hi} (the statement)	
$\mathcal{F}, u, \zeta$	$\mathcal{F}_{\mathrm{fx}}, 0, 2^{-64}$ (Definition I.1)
t_{c}	t_{frac} (the statement)
M	M_n (the statement)
D	D_n (the statement)
B	B_n (the statement)
η_1	η/Q_s (the statement)
S	S_τ (the statement)
ϵ	ϵ (Definition I.62)
$\mathcal{F}$ the realization of a Falcon-type signer at (u,ζ)	Lemma I.73, item 1
(f,g,F,G) a key of degree n of the signer	Lemma I.73, item 2; the statement
(I2) $t_{\mathrm{c}} \in \{t, t_{\mathrm{frac}}\}$	t_{frac} (Definition A.13)
$M \ge 0$	M_n (Definition I.14)
$D \in [0,1)$	(L13)
$B \ge 0$	B_n (Definition I.14)
$\eta_1 \in (0,1)$	(L14)
$\epsilon \in [0,1)$	Lemma I.73, item 3
$\epsilon_{\mathrm{hi}} \ge 0,\ \forall i \le N\ \forall z_{\le i}\ \forall z_i \notin C_i :$ $\widetilde{B}_i(z_i) \le (1+\epsilon_{\mathrm{hi}})\,\widetilde{D}_i(z_i)$	Lemma I.65 at the checked key; $\epsilon_{\mathrm{hi}} \ge 0$ (ϵ_{hi}, Lemma I.65)
Assumption A1	Assumption A2; $\bar{\delta}_K$ (Definition 4.12, item 1)
Assumption A2	Assumption A1
Assumption A3	(L12); $\bar{B}_K$ (Definition 4.12, item 3, at $\tau_K := \tau$)
Assumption A4	Lemma I.73, item 4, at $t_{\mathrm{c}} := t_{\mathrm{frac}}$
Assumption A5	Lemma I.73, item 5
Assumption A6	Lemma I.73, item 6
Assumption A7	Lemma I.73, item 7, at $t_{\mathrm{c}} := t_{\mathrm{frac}}$
Its conclusion: $P(S \cap \{z \in \mathbb{Z}^N : W(z) > W^{\mathrm{tail}}\}) \le \eta_1$	

(L15) $P(S_\tau \cap \{z \in \mathbb{Z}^N : W(z) > W^{\mathrm{tail}}\}) \le \eta/Q_s$

[(I2)]

(L16) $S_\tau \cap E^c = S_\tau \cap \{z \in \mathbb{Z}^N : W(z) > W^{\mathrm{tail}}\}$

[E (the statement)]

(L17) $\Rightarrow\ Q_s P(S_\tau \cap E^c) \le \eta$

[(L15), (L16); $Q_s > 0$ (Q_s, the statement); Fact A.41, item 26]

(L18) $\Rightarrow$ item 1

[(L17)]

□ (item 1)

Proof of items 2 to 6.

(L19) $W^{\mathrm{tail}} \ge 0$

[W^{tail} (Lemma 4.14); $t^2 \ge 0$ (Fact A.41, item 13); Fact A.41, item 8]

(L20) $\|e_{\mathrm{root}}\| \le \bar{e}$

[Lemma I.81, item 1, at the checked key and the hashed message; **Hypotheses I.21 and I.22**, named by Lemma I.81]

(L21) $\|t_{\mathrm{frac}}\| \le \bar{T}$

[Lemma I.81, item 2, at the checked key and the hashed message; **Hypotheses I.21 and I.22**, named by Lemma I.81]

(L22) $\forall z \in S_\tau : \ \|z'\| \le \bar{Z}$

[Lemma I.81, item 3, at the checked key and the hashed message; **Hypotheses I.21 and I.22**, named by Lemma I.81]

(L23) $p'_\tau < 1$

[the last measured row]

(L24) $\forall z \in S_\tau \cap E : \ W(z) \le W^{\mathrm{tail}}$

[E (the statement)]

(L25) $(1 + D_n)^2 < \alpha_L/(\alpha_L - 1)$

[the third measured row]

(L26) $\varepsilon_0^\circ < 1$

[the fourth measured row]

(L27) $\bar{e}, \bar{T}, \bar{Z} \ge 0$

[(L20), (L21); $\|\cdot\| \ge 0$ (Fact A.41, item 3); $\bar{Z}$ (Lemma I.81) and Lemma I.81, (L18), (L36), (L42), (L47), (L51); $\bar{\Xi}_0$, $\sigma_{\max}$ nonnegative (Lemma I.81); $\tau > 1$ (τ, the statement); Fact A.41, item 8]

Proposition I.72	This proof
Shared: (f, g, F, G), Q_s, τ, E, $\bar{e}, \bar{T}, \bar{Z}$ (Lemma I.81)	
c	t_{frac}
W°	W^{tail} (the statement)
$\bar{\delta}$	D_n (the statement)
η_E	η (the statement)
M_C	0
S	S_τ (the statement)
$c \in \{t, t_{\mathrm{frac}}\}$	t_{frac} (Definition 4.5)
$\bar{e}, \bar{T}, \bar{Z} \in [0, \infty)$	(L27)
$M_C \in \mathbb{Z}_{\ge 0}$	$0 \in \mathbb{Z}_{\ge 0}$
$W^\circ \ge 0$	(L19)
(I3) $\bar{\delta} \in [0, 1)$	(L13)
$E \subseteq \mathbb{Z}^N$	E (the statement)
$\eta_E \ge 0$	η (the statement)
Assumption A1	(L20)
Assumption A2	(L21)
Assumption A3	(L22)
Assumption A4	(L23)
Assumption A5	(L24)
Assumption A6	Assumption A2
Assumption A7	(L25)
Assumption A8	(L26)
Assumption A9	(L17)
Its conclusion: $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s}, \ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda} : \ P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$	

(L28) $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s}, \ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda} : \ P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$

[(I3); **Hypotheses I.21 and I.22**, named by Proposition I.72]

(L29) $\Rightarrow$ item 2

[(L28)]

	Corollary E.21 at τ	This proof
	Shared: τ, ϵ_{hi} (the statement)	
	Shared: $N := 2n$, $\tau > 1$	
	ϵ	ϵ (Definition I.62)
	S	S_τ (the statement)
(I4)	$\epsilon \in [0, 1)$	Lemma I.73, item 3
	$\epsilon_{\text{hi}} \geq 0$, $\forall i \leq N\ \forall z_{<i}\ \forall z_i \notin C_i$: $\widetilde{B}_i(z_i) \leq (1 + \epsilon_{\text{hi}})\, \widetilde{D}_i(z_i)$	Lemma I.65 at the checked key; $\epsilon_{\text{hi}} \geq 0$ (ϵ_{hi}, Lemma I.65)
	Assumption A1	(L8), (L9)
	Assumption A2	Lemma I.73, item 4, at $t_{\text{c}} := t_{\text{frac}}$
	Its conclusion: $P(S_\tau^c) \leq N\,(1 + \epsilon_{\text{hi}})\, \frac{1+\epsilon}{1-\epsilon}\, \tau\, e^{(1-\tau^2)/2}$	

(L30) $P(S_\tau^c) \leq N\, p'_\tau$

[(I4); p'_τ (Corollary 4.10, precondition 3)]

(L31) $2^{-\lambda_{\mathcal{F}}} \leq Q_s N\, p'_\tau + y + \eta$

[(L30); $\lambda_{\mathcal{F}}$ and $\lambda'_{\mathcal{F}}$ (Proposition I.72; Definition 5.3 at A, κ_C, $\bar{p}_C$, $M_C := 0$ and $S' := S_\tau$); Π_C (Definition 5.2 at $M_C := 0$); Lemma I.64, item 3]

(L32) $\Rightarrow\ \lambda_{\mathcal{F}} \geq -\log_2(Q_s N\, p'_\tau + y + \eta)$

[(L31); $t \mapsto -\log_2 t$ nonincreasing on $(0, \infty)$ (Fact A.41, item 5); $-\log_2 2^{-x} = x$ (Fact A.41, item 28)]

(L33) $\lambda_{\mathcal{F}} \geq 126.72$

[(L32); the second measured row at $(512, 128, 2^{60})$; assumption A4]

(L34) $\Rightarrow$ item 3

[(L33)]

(L35) $\lambda_{\mathcal{F}} \geq 254.66$

[(L32); the second measured row at $(1024, 256, 2^{60})$; assumption A5]

(L36) $\Rightarrow$ item 4

[(L35)]

(L37) $W^{\text{tail}} = 2^{-79.2}$

[the fifth measured row; assumption A6]

(L38) $\Rightarrow$ item 5

[(L37)]

(L39) $n = 512 \Rightarrow\ \lambda_{\mathcal{F}} \geq 126.70$

[(L32); the second measured row at $(512, 128, Q_s)$; Table 34 at $n = 512$; expand]

(L40) $n = 1024 \Rightarrow\ \lambda_{\mathcal{F}} \geq 253.53$

[(L32); the second measured row at $(1024, 256, Q_s)$; Table 34 at $n = 1024$; expand]

(L41) $\Rightarrow$ item 6

[(L39), (L40); λ_n^{64} (the statement); $n \in \{512, 1024\}$ (Definition 5.5, item 1)]

□ (items 2 to 6)

Center	n	λ	2^{32}	2^{36}	2^{40}	2^{44}	2^{48}	2^{52}	2^{56}	2^{60}	2^{64}
t	512	128	126.72	126.72	126.72	126.72	126.72	126.72	126.72	126.70	126.28
t	1024	256	254.72	254.72	254.72	254.72	254.72	254.72	254.71	254.46	248.78
t_{frac}	512	128	126.72	126.72	126.72	126.72	126.72	126.72	126.72	126.72	126.70
t_{frac}	1024	256	254.72	254.72	254.72	254.72	254.72	254.72	254.72	254.66	253.53

Table 34: Fixed-point signer, both centers: a lower bound of the bit security $\lambda_{\mathcal{F}}$ in bits at the tail W^{tail} of Lemma 4.14 at each center's thresholds M_n, D_n and B_n (Corollaries I.80 and I.89), with $\eta = 2^{-\lambda}$ and $\alpha = 2\lambda + 1$, by Q_s. Report: `verify/reports/fx/tail_levels.py`; gates: `verify/gates/fx/tail_conditions.py`, `verify/gates/fx/level_leading.py`, `verify/gates/fx/tail_level_cells.py`.

Table 35 lists the four terms of $\ln R$ at the tail's W^{tail} and, beside them, the terms of Corollary F.5 at its $\bar{W}_{\alpha_L}(\bar{\delta})$ and $\bar{\theta}_{\alpha_L}(\bar{\delta})$.

Center	n	α	T_B	$T_{\bar{\delta}}$	T_Δ	T_Φ	A	$\bar{T}_{\bar{\delta}}$	$\bar{T}_\Delta$	$\bar{A}$
t	512	257	-69.1	-96.9	-65.2	-81.0	-65.1	-96.9	-65.2	-65.1
t	1024	513	-63.8	-93.8	-62.2	-83.0	-61.8	-93.8	-62.2	-61.8
t_{frac}	512	257	-69.1	-96.9	-74.2	-81.0	-69.0	-96.9	-74.2	-69.0
t_{frac}	1024	513	-63.8	-93.8	-70.2	-83.0	-63.8	-93.8	-70.2	-63.8

Table 35: Fixed-point signer, both centers: the four terms of $\ln R$ per signature at the tail W^{tail} of Lemma 4.14 at $Q_s = 2^{64}$ and the threshold D_n as $\bar{\delta}$, all $\log_2$ (Corollaries I.80 and I.89), and the terms of Corollary F.5 at its $\bar{W}_{\alpha_L}(\bar{\delta})$ and $\bar{\theta}_{\alpha_L}(\bar{\delta})$ with their sum $\bar{A}$, which bound $T_{\bar{\delta}}$, T_Δ and A. Report: `verify/reports/fx/tail_levels.py`; gate: `verify/gates/fx/lnr_leading_tail.py`.

The end-to-end gate of ffSampling$^{\mathcal{F}}(B, s, t_{\text{frac}})$**.** The gate of ffSampling$^{\mathcal{F}}(B, s, t_{\text{frac}})$ end to end: every signature of 16 checked keys times 16 messages per degree verifies under the reference's `fndsa_verify`, a tampered copy is rejected, and the mean of $\|s_1\|^2 + \|s_2\|^2$ is within 2% of $2n\sigma^2$ (Statistics I.23, items 7, 8 and 9). The words reach 2^{25} at $n = 1024$ (Theorem I.54).

Remark I.90 (The gain of the center's split)**.** Two things, unequal in size, and a third it does not buy.

1. The words stay small. In ffSampling$^{\mathcal{F}}(B, s, t)$ the FFT image of the center has coordinates up to $nq\gamma'_{FG}$ and the words reach 2^{31} at $n = 512$ and 2^{33} at $n = 1024$ (Theorem I.54); in ffSampling$^{\mathcal{F}}(B, s, t_{\text{frac}})$ every coordinate of t_{frac} is a residue in $[-q/2, q/2)$ divided by q, below $1/2$ in magnitude, and the words reach 2^{24} and 2^{25}: the headroom of the 64.64 type, the reason for [L2: BFLP26, Alg. 7]. The integer part t_{int} is added back exactly, and over $\mathbb{R}$ the output measure is the same (Lemma I.86).

2. The computed center is more accurate. ffSampling$^{\mathcal{F}}(B, s, t)$ multiplies $\widetilde{\hat{h}}$ by the key's images and then by the stored $1/q$, rounded at 2^{-65} on products near $nq\gamma'_{FG}$: $\bar{e} = 2^{-30.2}$ at $n = 512$ (Lemma I.75); ffSampling$^{\mathcal{F}}(B, s, t_{\text{frac}})$ computes $(-\mathsf{h}(\mathsf{m})\,F, \mathsf{h}(\mathsf{m})\,f)$ and the residues exactly in integers and rounds only the FFT of residues below $q/2$ and one $1/q$: $\bar{e} = 2^{-47.4}$ (Lemma I.81).

3. What it does not buy under the derived bounds. The derived loss is set by the node recursion, $E_l R_k$ in D_S (Definition I.62), not by the center: the center's part of D_S falls from $2^{-22.1}$ to $2^{-39.3}$ at $n = 512$ and was the smaller part in both, so on the derived bounds our proof keeps no bit at either center (Corollaries I.79 and I.88). At the tail of Lemma 4.14 the remainder's threshold sets W^{tail} at both centers, and the stored constants' part of the remainder sets the threshold: B_n is $2^{-71.19}$ rounded up to $2^{-160}\mathbb{Z}$ at t against $2^{-79.17}$ at t_{frac} at $n = 1024$ (Definition I.14), the rounding of the center's products near $nq\gamma'_{FG}$ read at the leaves `verify/reports/fx/leafsum_key.py`; the bit security of both centers at that tail is Table 34's.

I.8 The tail checks' hypothesis

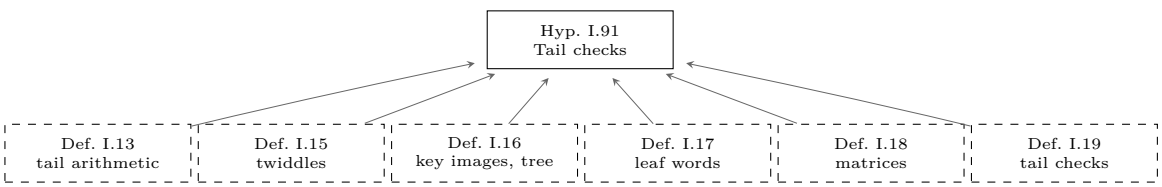


Figure 94: Dependencies, Appendix I.8.

Hypothesis I.91 states the tail checks' upper bounds; Lemma 5.7 the quantities within the thresholds.

Hypothesis I.91 (Code alignment of the C tail checks [to table])**.** A code-alignment hypothesis: on every key the key generation produces, the C tail checks compute the upper bounds of Definition I.19 along tailcheck (Algorithm 15) and tailbounds (Algorithm 16) at the center the key generation checks, and those bounds lie at or above the three quantities of Definition 4.12 at that center. Items 1, 2 and 3 are the alignment of the C tail checks and of their primitives. The gate of the arithmetic, `verify/gates/fx/interval_ops.py`, drives every operation of Definition I.13 against exact rationals on seeded operands, with cases built to leave a length or a precondition, `fxi_twiddles` against cos and sin at 60 digits, and the message rounding sites' bounds $m_i^{\uparrow}$ of Definition I.17, item 2, against their exact recursion on 16 checked keys per degree at both centers. A test of the bounds on a sample of keys is Statistics I.23, item 12. Define:

- $q := 12289$ (Definition A.13).

Let:

- $c \in \{t, t_{\text{frac}}\}$ be a center (Definition A.25);
- (f, g, F, G) be a checked key of degree n (Definition 5.5) passing the tail checks at c (Definition 5.6);
- $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$ be a hashed message (Definition A.25).

Define:

- e, that of Definition I.13, item 22;
- τ_K, that of Definition I.14 at n and c;
- $\bar{\delta}_K$, μ_{key} and $\bar{B}_K$, those of Definition 4.12 at $\mathcal{F}_{\text{fx}}$, the key, $\mathsf{h}(\mathsf{m})$, $t_{\text{c}} := c$ and τ_K;
- $\delta^{\uparrow}$, that of Definition I.19, item 1, at the key and c;
- $\mu^{\uparrow}$ and $B^{\uparrow}$, those of Definition I.19, item 2, at the key and c.

We assume:

1. `fxp_key_tail_pass` computes the lines of tailcheck (Algorithm 15) at the center its argument `which` names, t or t_{frac}, the quantities of Definitions I.15, I.16, I.17, I.18 and I.19 **[hypothesis, sampled gate: `verify/gates/fx/tail_bounds.py`]**;
2. Each C function of Definition I.13, items 2 to 21, at operands within its item's precondition and with $e = 0$, returns an interval that holds the exact result at any points of its operands, or an upper bound at or above that result **[hypothesis, sampled gate: `verify/gates/fx/interval_ops.py`]**;
3. $\forall k < 1024$: the two intervals Ψ_k (Definition I.15, item 1) that `fxi_twiddles` returns hold $\cos(\pi \operatorname{rev}_{10}(k)/1024)$ and $\sin(\pi \operatorname{rev}_{10}(k)/1024)$, rev_{10} that of Definition I.15 [gate: `verify/gates/fx/interval_twiddles.py`];
4. $\mu_{\text{key}} \leq \mu^{\uparrow}$;
5. $\bar{\delta}_K \leq \delta^{\uparrow}$;
6. $\bar{B}_K \leq B^{\uparrow}$.

[L3: code alignment] Not discharged.

Lemma 5.7 (*Under **Hypothesis I.91**, the three quantities' bounds [to table]*) [to statement]**.**
The items bound the three quantities of a key passing the tail checks at a center by the center's thresholds. ***Under Hypothesis I.91**, let:*

- $c \in \{t, t_{\text{frac}}\}$ *be a center (Definition A.25);*
- (f, g, F, G) *be a checked key of degree n (Definition 5.5) passing the tail checks at c (Definition 5.6);*
- $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$ *be a hashed message (Definition A.25).*

Define:

- M_n, D_n, B_n *and* τ_K, *those of Definition I.14 at* n *and* c;
- N, S_{τ_K}, I_N, $\widetilde{\sigma}_i$, K, r, δ_i *and* μ_{key}, *those of Definition 4.12 at* $\mathcal{F}_{\mathrm{fx}}$, *the key,* $\mathsf{h}(\mathsf{m})$, $t_{\mathrm{c}} := c$ *and* τ_K.

Then

1. $\mu_{\mathrm{key}} \leq M_n$;
2. $\forall i \leq N\ \forall z_{<i} :\ |\delta_i(z_{<i})| \leq D_n$;
3. $\forall z \in S_{\tau_K} :\ \sum_{i \leq N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2 \leq B_n$.

Proof.

DEFINES $\delta^{\uparrow}$, $\mu^{\uparrow}$ and $B^{\uparrow}$, those of Definition I.19 at the key and c

(L1) $\mu^{\uparrow} \leq M_n$
[Definition 5.6, item 2]

(L2) $\mu_{\mathrm{key}} \leq \mu^{\uparrow}$
[**Hypothesis I.91, item 4**]

(L3) $\Rightarrow$ $\mu_{\mathrm{key}} \leq M_n$
[(L1), (L2)]

(L4) $\Rightarrow$ item 1
[(L3)]

(L5) $\delta^{\uparrow} \leq D_n$
[Definition 5.6, item 1]

(L6) $\forall i \leq N\ \forall z_{<i} :\ |\delta_i(z_{<i})| \leq \delta^{\uparrow}$
[**Hypothesis I.91, item 5**; $\bar{\delta}_K$ (Definition 4.12, item 1)]

(L7) $\Rightarrow$ $\forall i \leq N\ \forall z_{<i} :\ |\delta_i(z_{<i})| \leq D_n$
[(L5), (L6)]

(L8) $\Rightarrow$ item 2
[(L7)]

(L9) $B^{\uparrow} \leq B_n$
[Definition 5.6, item 3]

(L10) $\forall z \in S_{\tau_K} :\ \sum_{i \leq N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2 \leq B^{\uparrow}$
[**Hypothesis I.91, item 6**; $\bar{B}_K$ (Definition 4.12, item 3)]

(L11) $\Rightarrow$ $\forall z \in S_{\tau_K} :\ \sum_{i \leq N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2 \leq B_n$
[(L9), (L10)]

(L12) $\Rightarrow$ item 3
[(L11)]

□ (items 1 to 3)

I.9 The result

Theorem 1.3 (*Under* ***Hypotheses I.21, I.22 and I.91****, the fixed-point signer's bit security at both centers [to table]*) [to statement].

The items bound the fixed-point signer's bit security from below at both centers and at every number of signatures of the sweep: the bound, its least value over the sweep, and the probability that the tail bound fails. ***Under Hypotheses I.21, I.22 and I.91****, define:*

- q, *the modulus of Definition A.13.*

Let:

- $c \in \{t, t_{\mathrm{frac}}\}$ *be a center (Definition A.25);*

- (f, g, F, G) *be a checked key of degree* n *(Definition 5.5) passing the tail checks at* c *(Definition 5.6);*
- $\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ *be a hashed message (Definition A.25);*
- $Q_s \in \{2^{32}, 2^{36}, \dots, 2^{64}\}$.

Define:

- *The signer's words and parameters*
  - $\lambda := 128$ *at* $n = 512$ *and* $\lambda := 256$ *at* $n = 1024$ *(Definition I.62);*
  - $N := 2n$ *(Definition A.25);*
  - $\eta := 2^{-\lambda}$;
- *The stored words*
  - M_n, D_n *and* B_n, *those of Corollary I.80 at* $c = t$ *and those of Corollary I.89 at* $c = t_{\mathrm{frac}}$, *at the key,* $\mathsf{h}(\mathsf{m})$ *and* Q_s;
- *The tail-cut events*
  - S_τ *and* S_{τ_K}, *those of Corollary I.80 at* $c = t$ *and those of Corollary I.89 at* $c = t_{\mathrm{frac}}$, *at the key,* $\mathsf{h}(\mathsf{m})$ *and* Q_s;
- *The three quantities*
  - μ_{key}, *that of Corollary I.80 at* $c = t$ *and that of Corollary I.89 at* $c = t_{\mathrm{frac}}$, *at the key,* $\mathsf{h}(\mathsf{m})$ *and* Q_s;
- *The sub-event*
  - E, *that of Corollary I.80 at* $c = t$ *and that of Corollary I.89 at* $c = t_{\mathrm{frac}}$, *at the key,* $\mathsf{h}(\mathsf{m})$ *and* Q_s;
- *The probability measures*
  - P *and* Q, *the output measures of* $\mathrm{ffSampling}^{\mathcal{F}}$ *and* $\mathrm{ffSampling}^{\mathbb{R}}$ *(Definition A.25 at the key,* $\mathsf{h}(\mathsf{m})$ *and* c*);*
  - $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$, *the probability measures of* Q_s *independent outputs* $(z^{(1)}, \dots, z^{(Q_s)})$ *of* P *and of* Q *on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1);*
- *The leaf perturbations*
  - I_N, $\widetilde{\sigma}_i$, K, r *and* δ_i, *those of Definition 4.12 at* $\mathcal{F}_{\mathrm{fx}}$, *the key,* $\mathsf{h}(\mathsf{m})$ *and* $t_{\mathrm{c}} := c$;
- *The terms*
  - $\lambda_{\mathcal{F}}$, *that of Corollary I.80 at* $c = t$ *and that of Corollary I.89 at* $c = t_{\mathrm{frac}}$, *at* (n, λ, Q_s).

Then

1. *At* $c = t$ *or* $c = t_{\mathrm{frac}}$: $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$;

	$c = t$	$c = t_{\mathrm{frac}}$
$n = 512$	2. $\lambda_{\mathcal{F}} \ge 126.28$	3. $\lambda_{\mathcal{F}} \ge 126.70$
$n = 1024$	4. $\lambda_{\mathcal{F}} \ge 248.78$	5. $\lambda_{\mathcal{F}} \ge 253.53$

6. *At* $c = t$ *or* $c = t_{\mathrm{frac}}$: $Q_s P(S_\tau \cap E^c) \le 2^{-\lambda}$.

Proof. (I1)

Lemma 5.7	This proof
Shared: (f, g, F, G), $\mathsf{h}(\mathsf{m})$ Shared: $c \in \{t, t_{\mathrm{frac}}\}$	
c (f, g, F, G) key of degree n passing the tail checks at c	t (the premise of (L1)) The statement; the premise of (L1)
Its item 1: $\mu_{\mathrm{key}} \le M_n$	
Its item 2: $\forall i \le N\ \forall z_{<i} :\ \lvert\delta_i(z_{<i})\rvert \le D_n$	
Its item 3: $\forall z \in S_{\tau_K} :\ \sum_{i \le N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2 \le B_n$	
$c = t \Rightarrow\ \mu_{\mathrm{key}} \le M_n$	

[item 1 of (I1); **Hypothesis I.91**, named by Lemma 5.7]

(L2) $c = t \Rightarrow\ \forall i \le N\ \forall z_{<i} :\ |\delta_i(z_{<i})| \le D_n$

[item 2 of (I1); **Hypothesis I.91**, named by Lemma 5.7]

(L3) $c = t \Rightarrow\ \forall z \in S_{\tau_K} :\ \sum_{i \le N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2 \le B_n$

[item 3 of (I1); **Hypothesis I.91**, named by Lemma 5.7]

Corollary I.80, items 2 and 9	This proof
Shared: (f, g, F, G), $\mathsf{h}(\mathsf{m})$, Q_s, $\lambda_{\mathcal{F}}$	
t	c (the premise of (L4))
(f, g, F, G) key of degree n passing the tail checks at t	The statement; the premise of (L4)
(I2) $Q_s \in \{2^{32}, 2^{36}, \dots, 2^{64}\}$	The statement
Assumption A1	(L1)
Assumption A2	(L2)
Assumption A3	(L3)
Its item 2: $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$	
Its item 9: $\lambda_{\mathcal{F}} \ge \lambda_n^{64}$	

(L4) $c = t \Rightarrow\ \forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$

[item 2 of (I2); **Hypotheses I.21 and I.22**, named by Corollary I.80]

Lemma 5.7	This proof
Shared: (f, g, F, G), $\mathsf{h}(\mathsf{m})$	
Shared: $c \in \{t, t_{\text{frac}}\}$	
c	t_{frac} (the premise of (L5))
(I3) (f, g, F, G) key of degree n passing the tail checks at c	The statement; the premise of (L5)
Its item 1: $\mu_{\text{key}} \le M_n$	
Its item 2: $\forall i \le N\ \forall z_{<i} :\ \lvert\delta_i(z_{<i})\rvert \le D_n$	
Its item 3: $\forall z \in S_{\tau_K} :\ \sum_{i \le N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2 \le B_n$	

(L5) $c = t_{\text{frac}} \Rightarrow\ \mu_{\text{key}} \le M_n$

[item 1 of (I3); **Hypothesis I.91**, named by Lemma 5.7]

(L6) $c = t_{\text{frac}} \Rightarrow\ \forall i \le N\ \forall z_{<i} :\ |\delta_i(z_{<i})| \le D_n$

[item 2 of (I3); **Hypothesis I.91**, named by Lemma 5.7]

(L7) $c = t_{\text{frac}} \Rightarrow\ \forall z \in S_{\tau_K} :\ \sum_{i \le N} (r(I_N + K))_i^2 / \widetilde{\sigma}_i^2 \le B_n$

[item 3 of (I3); **Hypothesis I.91**, named by Lemma 5.7]

Corollary I.89, items 2 and 6	This proof
Shared: (f, g, F, G), $\mathsf{h}(\mathsf{m})$, Q_s, $\lambda_{\mathcal{F}}$	
t_{frac}	c (the premise of (L8))
(f, g, F, G) key of degree n passing the tail checks at t_{frac}	The statement; the premise of (L8)
(I4) $Q_s \in \{2^{32}, 2^{36}, \dots, 2^{64}\}$	The statement
Assumption A1	(L5)
Assumption A2	(L6)
Assumption A3	(L7)
Its item 2: $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$	
Its item 6: $\lambda_{\mathcal{F}} \ge \lambda_n^{64}$	

(L8) $c = t_{\text{frac}} \Rightarrow\ \forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$

[item 2 of (I4); **Hypotheses I.21 and I.22**, named by Corollary I.89]

(L9) $\Rightarrow$ item 1

[(L4), (L8); $c \in \{t, t_{\text{frac}}\}$ (the statement)]

(L10) $(n, c) = (512, t) \Rightarrow\ \lambda_{\mathcal{F}} \geq 126.28$
[item 9 of (I2); λ_n^{64} (Corollary I.80) at $n = 512$, the premise; **Hypotheses I.21 and I.22**, named by Corollary I.80; [gate: `verify/gates/fx/tail_level_cells.py--centert`] at $(512, 128, 2^{64})$]

(L11) $\Rightarrow$ item 2
[(L10)]

(L12) $(n, c) = (512, t_{\text{frac}}) \Rightarrow\ \lambda_{\mathcal{F}} \geq 126.70$
[item 6 of (I4); λ_n^{64} (Corollary I.89) at $n = 512$, the premise; **Hypotheses I.21 and I.22**, named by Corollary I.89; [gate: `verify/gates/fx/tail_level_cells.py`] at $(512, 128, 2^{64})$]

(L13) $\Rightarrow$ item 3
[(L12)]

(L14) $(n, c) = (1024, t) \Rightarrow\ \lambda_{\mathcal{F}} \geq 248.78$
[item 9 of (I2); λ_n^{64} (Corollary I.80) at $n = 1024$, the premise; **Hypotheses I.21 and I.22**, named by Corollary I.80; [gate: `verify/gates/fx/tail_level_cells.py--centert`] at $(1024, 256, 2^{64})$]

(L15) $\Rightarrow$ item 4
[(L14)]

(L16) $(n, c) = (1024, t_{\text{frac}}) \Rightarrow\ \lambda_{\mathcal{F}} \geq 253.53$
[item 6 of (I4); λ_n^{64} (Corollary I.89) at $n = 1024$, the premise; **Hypotheses I.21 and I.22**, named by Corollary I.89; [gate: `verify/gates/fx/tail_level_cells.py`] at $(1024, 256, 2^{64})$]

(L17) $\Rightarrow$ item 5
[(L16)]

(I5)

Corollary I.80, item 1	This proof
Shared: (f, g, F, G), $\mathsf{h}(\mathsf{m})$, Q_s	
t	c (the premise of (L18))
(f, g, F, G) key of degree n passing the tail checks at t	The statement; the premise of (L18)
$Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$	The statement
Assumption A1	(L1)
Assumption A2	(L2)
Assumption A3	(L3)
Its conclusion: $Q_s P(S_\tau \cap E^c) \leq \eta$	

(L18) $c = t \Rightarrow\ Q_s P(S_\tau \cap E^c) \leq \eta$
[(I5); **Hypotheses I.21 and I.22**, named by Corollary I.80]

(L19) $c = t \Rightarrow\ Q_s P(S_\tau \cap E^c) \leq 2^{-\lambda}$
[(L18); $\eta := 2^{-\lambda}$ (the statement)]

(I6)

Corollary I.89, item 1	This proof
Shared: (f, g, F, G), $\mathsf{h}(\mathsf{m})$, Q_s	
t_{frac}	c (the premise of (L20))
(f, g, F, G) key of degree n passing the tail checks at t_{frac}	The statement; the premise of (L20)
$Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$	The statement
Assumption A1	(L5)
Assumption A2	(L6)
Assumption A3	(L7)
Its conclusion: $Q_s P(S_\tau \cap E^c) \leq \eta$	

(L20) $c = t_{\text{frac}} \Rightarrow\ Q_s P(S_\tau \cap E^c) \leq \eta$
[(I6); **Hypotheses I.21 and I.22**, named by Corollary I.89]

(L21) $c = t_{\text{frac}} \Rightarrow\ Q_s P(S_\tau \cap E^c) \leq 2^{-\lambda}$
[(L20); $\eta := 2^{-\lambda}$ (the statement)]

(L22) $\Rightarrow$ item 6

[(L19), (L21); $c \in \{t, t_{\mathrm{frac}}\}$ (the statement)]
□ (items 1 to 6)

Theorem 5.12 (*Under **Hypotheses I.21, I.22 and I.91**, the checks' impact [to table]*) [to statement].

*The items single out what the tail checks of Definition 5.6 change in the fixed-point signer's bit security: the bit security our proof keeps without them is that of Corollaries I.79, item 1, and I.88, item 1, the bit security with them that of Theorem 1.3. The bit security of item 4 consists of these terms: $Q_s P(S_\tau^c)$, η, y and $\Pi_C(y)$. **Under Hypotheses I.21, I.22 and I.91**, define:*

- $q := 12289$ *(Definition A.13).*

Let:

- $c \in \{t, t_{\mathrm{frac}}\}$ *be a center (Definition A.25);*
- (f, g, F, G) *be a checked key of degree n (Definition 5.5) passing the tail checks at c (Definition 5.6);*
- $\mathsf{h}(\mathsf{m}) \in \{0, \ldots, q-1\}^n$ *be a hashed message (Definition A.25);*
- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$*;*
- $M_C \in \mathbb{Z}_{\geq 0}$.

Define:

- *The signer's words and parameters*
  - $(\lambda, \alpha) := \begin{cases} (128, 257) & n = 512 \\ (256, 513) & n = 1024 \end{cases}$ *(Definition I.62);*
  - $N := 2n$ *(Definition A.25);*
  - $\eta := 2^{-\lambda}$*;*
- *The stored words*
  - M_n, D_n *and* B_n*, those of Definition I.14 at n and c;*
- *The probability measures*
  - P*, the output measure of* $\mathrm{ffSampling}^{\mathcal{F}}$ *(Definition A.25 at the key,* $\mathsf{h}(\mathsf{m})$ *and c);*
- *The tail-cut event*
  - τ, S_τ *and* E*, those of Corollary I.80 at $c = t$ and those of Corollary I.89 at $c = t_{\mathrm{frac}}$, at the key,* $\mathsf{h}(\mathsf{m})$ *and* Q_s*;*
- *The leaf perturbations*
  - δ_i, W *and* W^{tail}*, those of Lemma 4.14 at* $\mathcal{F}_{\mathrm{fx}}$*, the key,* $\mathsf{h}(\mathsf{m})$*,* $t_{\mathrm{c}} := c$*,* τ*,* $M := M_n$*,* $D := D_n$*,* $B := B_n$*,* $\eta_1 := \eta / Q_s$ *and the inputs of Lemma I.73;*
- *The terms*
  - $\mathfrak{L}_B$*, that of Definition I.62 at c and τ, and at the $\bar{e}$,* $\bar{T}$ *and* $\bar{Z}$ *of Lemma I.77 at $c = t$ and of Lemma I.81 at $c = t_{\mathrm{frac}}$, at τ;*
  - $\mathfrak{L}_{\bar{\delta}}$, $\mathfrak{L}_\Delta$ *and* $\mathfrak{L}_\Phi$*, those of Proposition I.72 at c, Q_s, τ,* $W^\circ := W^{\mathrm{tail}}$*,* $\bar{\delta} := D_n$*,* E *and* $\eta_E := \eta$*, and at the $\bar{e}$,* $\bar{T}$ *and* $\bar{Z}$ *of Lemma I.77 at $c = t$ and of Lemma I.81 at $c = t_{\mathrm{frac}}$, at τ;*
  - $A := \mathfrak{L}_B + \mathfrak{L}_{\bar{\delta}} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$ *(Proposition I.72);*
  - $y := (2^{-\lambda} e^{Q_s A})^{(\alpha-1)/\alpha}$ *(Definition 5.3);*
  - $\Pi_C(y)$*, that of Definition 5.2 at* (Q_s, M_C)*;*
  - $\lambda_{\mathcal{F}}$*, that of Corollary I.80 at $c = t$ and that of Corollary I.89 at $c = t_{\mathrm{frac}}$, at the key,* $\mathsf{h}(\mathsf{m})$ *and* Q_s.

Then the thresholds bound $|\delta_i|$ and the leaf sum, the event E costs η, and $2^{-\lambda_{\mathcal{F}}}$ is the sum of four terms, the last zero:

1. $\forall i \leq N \ \forall z_{<i} : \ |\delta_i(z_{<i})| \leq D_n$*;*
2. $\forall z \in S_\tau \cap E : \ W(z) \leq W^{\mathrm{tail}}$*;*
3. $Q_s P(S_\tau \cap E^c) \leq \eta$*;*

4. $2^{-\lambda_{\mathcal{F}}} = Q_s\, P(S_\tau^c) + \eta + y + \Pi_C(y)$;

5. $\Pi_C(y) = 0$.

Proof.

DEFINES $\lambda'_{\mathcal{F}}$, that of Proposition I.72 at c, Q_s, τ, $W^\circ := W^{\text{tail}}$, $\bar\delta := D_n$, E and $\eta_E := \eta$, and at the $\bar e$, $\bar T$ and $\bar Z$ of Lemma I.77 at $c = t$ and of Lemma I.81 at $c = t_{\text{frac}}$, at τ

Proof of item 1.

	Lemma 5.7, item 2	This proof
(I1)	Shared: c, (f,g,F,G), $\mathsf{h}(\mathsf{m})$, N, D_n, δ_i Shared: $c \in \{t, t_{\text{frac}}\}$	
	(f,g,F,G) key of degree n passing the tail checks at c	The statement
	Its conclusion: $\forall i \le N\ \forall z_{<i} :\ \lvert\delta_i(z_{<i})\rvert \le D_n$	

(L1) $\forall i \le N\ \forall z_{<i} :\ \lvert\delta_i(z_{<i})\rvert \le D_n$

[(I1); **Hypothesis I.91**, named by Lemma 5.7]

(L2) $\Rightarrow$ item 1

[(L1)]

□ (item 1)

Proof of item 2.

(L3) $\forall z \in S_\tau \cap E :\ W(z) \le W^{\text{tail}}$

[$E := \{\, z \in \mathbb{Z}^N : W(z) \le W^{\text{tail}} \,\}$ (Corollary I.80 at $c = t$, Corollary I.89 at $c = t_{\text{frac}}$; the statement)]

(L4) $\Rightarrow$ item 2

[(L3)]

□ (item 2)

Proof of item 3.

	Theorem 1.3	This proof
(I2)	Shared: c, (f,g,F,G), $\mathsf{h}(\mathsf{m})$, Q_s, λ, N, S_τ, E Shared: $c \in \{t, t_{\text{frac}}\}$, $Q_s \in \{2^{32}, 2^{36}, \dots, 2^{64}\}$	
	(f,g,F,G) key of degree n passing the tail checks at c	The statement
	Its item 6: $Q_s P(S_\tau \cap E^c) \le 2^{-\lambda}$	

(L5) $Q_s P(S_\tau \cap E^c) \le 2^{-\lambda}$

[item 6 of (I2); **Hypotheses I.21, I.22 and I.91**, named by Theorem 1.3]

(L6) $\Rightarrow$ $Q_s P(S_\tau \cap E^c) \le \eta$

[(L5); $\eta := 2^{-\lambda}$ (the statement)]

(L7) $\Rightarrow$ item 3

[(L6)]

□ (item 3)

Proof of items 4 and 5.

(L8) $2^{-\lambda_{\mathcal{F}}} = 2^{-\lambda'_{\mathcal{F}}} + \eta$

[$\lambda_{\mathcal{F}}$ (the statement; Proposition I.72); Fact A.41, item 28; $\eta := 2^{-\lambda}$ (the statement); $\lambda'_{\mathcal{F}}$ (the proof's block)]

(L9) $2^{-\lambda'_{\mathcal{F}}} = Q_s\, P(S_\tau^c) + y + \Pi_C(y)$

[$\lambda'_{\mathcal{F}}$ (the proof's block), the $\lambda'_{\mathcal{F}}$ of Proposition I.72 at $S := S_\tau$, Definition 5.3 at A, κ_C, $\bar p_C$, M_C and $S' := S_\tau$; A, y and $\Pi_C(y)$ (the statement)]

(L10) $\Rightarrow$ $2^{-\lambda_{\mathcal{F}}} = Q_s\, P(S_\tau^c) + \eta + y + \Pi_C(y)$

[(L8), (L9)]

(L11) $\Rightarrow$ item 4

[(L10)]

(L12) $\kappa_C = 0$

[Lemma I.64, item 3]

(L13) $\bar{p}_C = 0$

[Lemma I.64, item 3]

(L14) $\forall m \in \{1, \ldots, M_C\} : \binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha}\, y = 0$

[(L12); $0^a = 0$ at $a > 0$ (Fact A.41, item 44) at $a := m/\alpha$; $\alpha > 1$ (α, the statement)]

(L15) $\forall m \in \{1, \ldots, M_C + 1\} : \binom{Q_s N}{m} \bar{p}_C^m = 0$

[(L13); $0^a = 0$ at $a > 0$ (Fact A.41, item 44) at $a := m$]

(L16) $\forall m \in \{1, \ldots, M_C\} : \min\left(\binom{Q_s N}{m}^{1/\alpha} \kappa_C^{m/\alpha}\, y,\ \binom{Q_s N}{m} \bar{p}_C^m \right) = 0$

[(L14), (L15); $\min(0,0) \le 0$ (Fact A.41, item 20); $0 \le \min(0,0)$ (Fact A.41, item 47, at $c := 0$)]

(L17) $\Pi_C(y) = 0$

[(L15) at $m := M_C + 1$, (L16); $\Pi_C(y)$ (Definition 5.2)]

(L18) $\Rightarrow$ item 5

[(L17)]

$\square$ (items 4 and 5)

J The floating-point signer: `c-fn-dsa`

Table 36 lists this section's definitions, facts and hypotheses, Table 37 how each lemma, proposition and corollary of this section is verified.

Table 36: Appendix J: its definitions, facts and hypotheses.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Def. J.1	✓				
Fact J.2					
Fact J.3					
Def. J.5	✓				
Def. J.28					
Hyp. J.31				mathematical	
Def. J.32					
Def. J.33					
Fact J.34	✓				
Def. J.40	✓				
Def. J.41	✓				
Hyp. J.47				mathematical	
Hyp. J.48				mathematical	
Hyp. J.54	✓			mathematical	
Def. J.55	✓				
Hyp. J.61				mathematical	
Hyp. J.62				mathematical	
Hyp. J.63				sampled	
Hyp. J.64				sampled	L2: BFLP26, (33), (34)
Def. J.66				**J.63**	
Hyp. J.75				mathematical	

Table 37: Appendix J: how each lemma, proposition and corollary is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source	Eyes
Lemma J.4			✓			
Lemma J.6	✓					
Lemma J.7	✓					
Lemma J.8	✓					
Lemma J.9	✓					
Lemma J.10	✓					
Lemma J.11	✓	✓				
Lemma J.12	✓	✓				
Lemma J.13	✓	✓				
Lemma J.14	✓	✓				
Lemma J.15	✓					
Lemma J.16	✓					
Lemma J.17	✓					
Lemma J.18	✓					
Lemma J.19	✓					
Lemma J.20	✓	✓				
Lemma J.21	✓	✓				
Lemma J.22	✓	✓				
Lemma J.23	✓					
Lemma J.24	✓					
Lemma J.25	✓					
Lemma J.26			✓			
Cor. J.27	✓					
Lemma J.29			✓			
Lemma J.30			✓			
Lemma J.35	✓			**J.31**		
Lemma J.36	✓					
Lemma J.37	✓			**J.31**		
Lemma J.38	✓			**J.31**		
Lemma J.39	✓			**J.31**		
Cor. J.42	✓					
Cor. J.43	✓			**J.31**		
Cor. J.44	✓			**J.31**		
Cor. J.45	✓					
Cor. J.46	✓		✓			
Lemma J.49	✓			**J.31**		
Lemma J.50	✓			**J.31**		
Lemma J.51	✓		✓	**J.31**		
Lemma J.52	✓		✓	**J.31**, **J.47**, **J.48**		
Lemma J.53	✓			**J.31**		
Lemma J.56	✓		✓	**J.31**, **J.47**, **J.48**		
Lemma J.57	✓			**J.48**		
Lemma J.58	✓			**J.31**, **J.47**, **J.48**, **J.54**		
Lemma J.59	✓			**J.31**, **J.47**, **J.48**, **J.54**		
Lemma J.60	✓		✓	**J.31**, **J.47**, **J.48**, **J.54**		
Lemma J.65	✓			**J.64**		
Lemma J.67	✓			**J.31**, **J.61**		
Lemma J.68	✓			**J.31**, **J.61**		
Lemma J.69	✓		✓	**J.31**, **J.61**		
Lemma J.70	✓		✓	**J.31**, **J.61**		
Lemma J.71			✓	**J.31**, **J.48**, **J.61**		
Lemma J.72	✓			**J.31**, **J.47**, **J.48**, **J.54**, **J.61**		
Prop. J.73	✓			**J.31**, **J.47**, **J.48**, **J.54**, **J.61**, **J.62**		
Prop. J.74	✓		✓	**J.31**, **J.47**, **J.48**, **J.54**, **J.61**, **J.64**		
Prop. J.76				**J.31**, **J.47**, **J.48**, **J.54**, **J.61**, **J.62**, **J.75**		✓

Statement	Lean	CryptoLine	Gate	Hypotheses	Source	Eyes
Prop. J.77						✓
Prop. J.78				**J.31**, **J.47**, **J.48**, **J.54**, **J.61**, **J.64**		✓

Structure. This appendix proves the floating-point signer's bit security. Appendix J.1 states the realization; Appendix J.2 the key; Appendix J.3 the tree and the centers at $\zeta = 0$; Appendix J.4 the base sampler's perturbation budget; Appendix J.5 the loss; Appendix J.6 lists this signer's gates.

The floating-point signer. The floating-point signer, the realization of Definition J.1, is ffSampling$^{\mathcal{F}}$ (Algorithm 10) executed in the emulated binary64 type `fpr` on the keys the checked key generation accepts (Definition 5.5): the plain C build of `c-fn-dsa` at commit `a5f1589`, its plain `fpoly_*` kernels and its plain `sampler_next`, the signing code untouched and the key generation the one of keygen (Algorithm 11). It is the Falcon-type signer of Definition 4.5 at $(u, \zeta) = (2^{-53}, 0)$ under **Hypothesis J.31** (Corollary J.27). Its realization meets the preconditions the shared algorithms take, Definition A.4, items 3 to 7, by Fact J.3, items 1, 2, 3, 4 and 5. This appendix instantiates Theorem 4.11 at it: it collects every statement that holds for this signer only, its realization, its hypotheses, and the statements of Appendix G.3 to Appendix G.6 at $\zeta = 0$, each derived from the general form. Table 38 lists its routines by their code names, the algorithm each one is, its lines and the operations each performs per ψ.

The hypotheses of the floating-point signer. Its hypotheses are stated in the subsections whose statements use them: no underflow in ffSampling$^{\mathcal{F}}$ (**Hypothesis J.31**, Appendix J.1.2); the computed leaf standard deviations at most σ_0 and $\widetilde{ccs} < 1$ (**Hypotheses J.47 and J.48**, Appendix J.4.1); the normalizer bounds at the leaves (**Hypothesis J.54**, Appendix J.4.2); the two interfaces of an instantiation, the pole, the key constants at the sample maxima and the Gaussian model of the leaf perturbations (**Hypotheses J.61, J.62, J.63 and J.64**, Appendix J.5.1); the exponential at $p = 64$ and $p = 113$ (**Hypothesis J.75**, Appendix J.5.4). Theorems F.4 and 4.11 take the pole and the normalizer bound as assumptions: the fixed-point signer proves both (Lemmas I.68 and I.69), the floating-point signer assumes the pole (**Hypothesis J.62**) and proves the normalizer bound at its computed leaves (Lemma J.71). It meets the two interfaces of **Hypothesis J.61** (Section 4.5.1) under **Hypothesis J.31** (Lemma J.52).

Object	Routine	Algorithm	`c-fn-dsa`	Operations per ψ
B in FFT form	`basis_to_FFT`	FFT, line 2 of ffSampling$^{\mathcal{F}}$	[LO: `sign_core.c:11-30`]	$(h-1)$ levels of Lemma G.18
$\mathcal{G} = BB^\dagger$	`fpoly_gram_fft`	Gram	[LO: `sign_fpoly.c:2625-2652`]	$\lvert b\rvert^2$, $b \operatorname{conj} b'$, $\oplus$
$LDL^\dagger$ of one node	`fpoly_LDL_fft`	$\mathrm{LDL}^\dagger$	[LO: `sign_fpoly.c:2136-2149`]	$1/x$, $4\times$, $+$, $-$
$d \to (d_0, d_1)$	`fpoly_split_selfadj_fft`	$\mathrm{split}_{\mathrm{sa}}$	[LO: `sign_fpoly.c:2351-2362`]	Lemma B.3, real
$t \to (t_0, t_1)$	`fpoly_split_fft`	split	[LO: `sign_fpoly.c:2258-2272`]	Lemma B.3
$(z_0, z_1) \to z$	`fpoly_merge_fft`	merge	[LO: `sign_fpoly.c:2452-2463`]	Lemma G.18
$t_0 + (t_1 - z_1)\, l_{10}$	`fpoly_mul_fft` and adds	ffsamp, line 26	[LO: `sign_sampler.c:1315-1319`]	$\otimes$ (Lemma B.2, item 5), $\oplus$, $\ominus$
Leaf (t_i, σ_i)	`ffsamp_fft_deepest`	deepest, lines 1 to 18	[LO: `sign_sampler.c:1185-1234`]	$\sqrt{d} \cdot$ `INV_SIGMA`
Base sampler	`sampler_next`	SamplerZ	[LO: `sign_sampler.c:916-968`]	Appendix G.6

Table 38: The floating-point signer's routines, the algorithm each one is, its lines, and the lemma that bounds it.

J.1 The realization

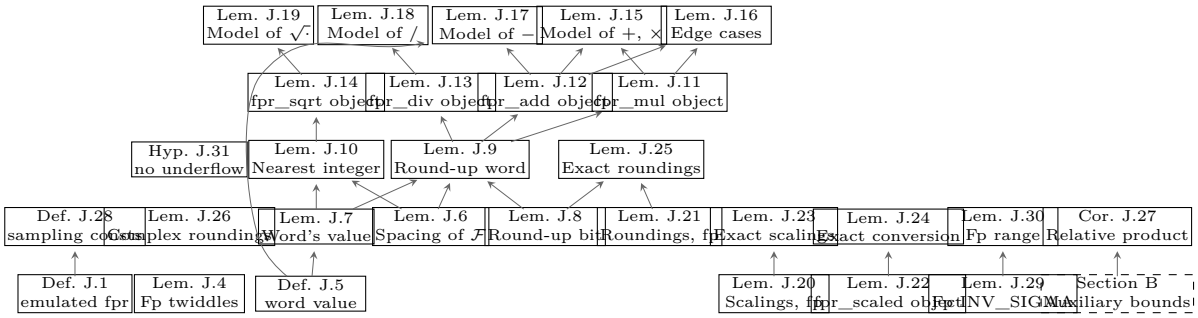


Figure 95: Dependencies, Appendix J.1.

Structure. Appendix J.1.1 states the arithmetic; Appendix J.1.2 ffSampling$^{\mathcal{F}}$ in $\mathcal{F}$.

J.1.1 The arithmetic

The floating-point realization (Definition J.1, Fact J.3).

- In `c-fn-dsa`, $\mathrm{fl}(x)$ is the binary64 nearest to x, a tie to even, through a sticky bit.
- In `c-fn-dsa`, `fpr_inv`$(x) =$ `fpr_div`$(1, x)$.
- Under **Hypothesis J.31**, the floating-point signer has $(u, \zeta) = (2^{-53}, 0)$, by Definition J.1 and Corollary J.27.
- Its realization meets the preconditions the shared algorithms take on $\mathcal{F}$, Definition A.4, items 3 to 7, by Fact J.3.

The exact operations (Fact J.2). In the floating-point signer, let $x, y \in \mathcal{F}$ be values, and $e, i \in \mathbb{Z}$ integers. Let $\mathrm{trunc}\, x := \mathrm{sgn}(x)\lfloor |x| \rfloor$ be the truncation of x, and $\mathrm{rint}\, x$ the integer nearest to x, a tie to even.

- $\mathrm{fl}(-x) = -x$ and $\mathrm{fl}(\mathrm{conj}\, x) = \mathrm{conj}\, x$.
- $\mathrm{fl}(x/2) = x/2$.
- Absent underflow and overflow, $\mathrm{fl}(2^e x) = 2^e x$.
- For $|i| < 2^{53}$, $\mathrm{fl}(i) = i$.
- $\lfloor x \rfloor, \mathrm{trunc}\, x, \mathrm{rint}\, x \in \mathbb{Z}$, exact.
- $\mathrm{fl}(x + 0) = x$ and $\mathrm{fl}(x \times 1) = x$.
- $\mathrm{fl}(x \circ y) = \mathrm{fl}(y \circ x)$ for $\circ \in \{+, \times\}$.
- $\forall a, b \in \mathbb{R},\ a \le b :\ \mathrm{fl}(a) \le \mathrm{fl}(b)$, and $\mathrm{fl}(x) = x$.

Definition J.1 (The emulated `fpr` [to table])**.** The floating-point signer computes in binary64 without subnormals, each operation rounded to nearest, a tie to even. Define:

- $\mathcal{F} := \{\pm m 2^e : m, e \in \mathbb{Z},\ 2^{52} \le m < 2^{53},\ -1074 \le e \le 971\} \cup \{0\}$, the floating-point signer's realization;
- $u := 2^{-53}$;
- $\zeta := 0$.

Let:

- $x \in \mathcal{F}$;
- $y \in \mathcal{F}$;
- $e \in \mathbb{Z}$.

The code:

- Represents $\mathcal{F}$ as binary64 without subnormals, infinities and NaN, W_x and W_y the binary64 words that store x and y [L0: `sign_inner.h:21-38`];
- Computes $\mathrm{fl}(x \circ y)$ for $\circ \in \{+, -, \times, /\}$ as the element of $\mathcal{F}$ nearest to $x \circ y$, and $\mathrm{fl}(\sqrt{x})$ as the element of $\mathcal{F}$ nearest to $\sqrt{x}$, a tie to even, through a sticky bit [L0: `sign_fpr.c:20`];

- Computes $\texttt{fpr_inv}(x) = \texttt{fpr_div}(1, x)$ [L0: `sign_inner.h:292`];
- Computes $\mathrm{fl}(x/2) = x/2$ and $\mathrm{fl}(2^e x) = 2^e x$ [L0: `sign_inner.h:248-325`];
- Computes $\mathrm{fl}(i) = i$ for $i \in \mathbb{Z}$ with $|i| < 2^{53}$, and $\lfloor \cdot \rfloor$, trunc and rint exactly [L0: `sign_inner.h:105-190`];
- Stores each twiddle as $\widetilde{\psi}_k = \mathrm{fl}(\psi_k)$ [L0: `sign_fpoly.c:13-1038`];
- Computes the FFT form of Definition A.8 [L0: `sign_fpoly.c:2156-2180`], and its $\oplus$ and $\otimes$ [L0: `sign_inner.h:327`].

```
def InF (w : Real) : Prop :=
  w = 0 \/ exists s e m : Int, (s = 0 \/ s = 1) /\ 1 <= e /\ e <= 2046 /\ 2 ^ 52 <= m /\ m < 2
      ^ 53 /\ w = fprVal s e m
```

Figure 96: The Lean declarations carrying Definition J.1: `InF` (`FprRound.lean`); with `fprVal` of Figure 97; Lean's symbols in ASCII.

Fact J.2 (Exact operations of the floating-point signer [to table])**.** The sign, the conjugate, the scalings by powers of two, the small integers and the roundings to integers are exact. Let:

- $x \in \mathcal{F}$;
- $y \in \mathcal{F}$;
- $e \in \mathbb{Z}$;
- $i \in \mathbb{Z}$.

In the floating-point signer, we have

1. $\mathrm{fl}(-x) = -x$, $\mathrm{fl}(\mathrm{conj}\, x) = \mathrm{conj}\, x$ [L0: `sign_inner.h:241`]
2. $\mathrm{fl}(x/2) = x/2$ [L0: `sign_inner.h:248-325`] (Lemma J.23, item 1)
3. $\mathrm{fl}(2^e x) = 2^e x$, absent underflow and overflow [L0: `sign_inner.h:248-325`] (Lemma J.23, items 2 to 4)
4. $\mathrm{fl}(i) = i$ for $|i| < 2^{53}$ [L0: `sign_inner.h:105-190`]
5. $\lfloor x \rfloor$, $\mathrm{trunc}\, x$, $\mathrm{rint}\, x \in \mathbb{Z}$, exact, where $\mathrm{trunc}\, x = \mathrm{sgn}(x)\lfloor |x| \rfloor$ and $\mathrm{rint}\, x$ is the integer nearest to x, a tie to even [L0: `sign_inner.h:105-190`]
6. $\mathrm{fl}(x + 0) = x$, $\mathrm{fl}(x \times 1) = x$ [derived]
7. $\mathrm{fl}(x \circ y) = \mathrm{fl}(y \circ x)$, $\circ \in \{+, \times\}$ [derived]
8. $\forall a, b \in \mathbb{R},\ a \le b$: $\mathrm{fl}(a) \le \mathrm{fl}(b)$, and $\mathrm{fl}(x) = x$: the rounding to nearest is nondecreasing and fixes $\mathcal{F}$ [derived]

Fact J.3 (Halvings and exact operations of the floating-point signer [to table])**.** In the floating-point signer, the halving rounds by at most $\zeta/2$, the halved sum or difference of two values is one rounding of the model followed by the halving, and an integer of modulus below 2^{53}, a negation and a conjugate are exact: the signer meets Definition A.4, items 3 to 7. Let:

- $\mathcal{F}$ be the realization of the floating-point signer, that of Definition J.1, at $(u, \zeta) = (2^{-53}, 0)$;
- $x, y \in \mathcal{F}$;
- $i \in \mathbb{Z}$.

We have

1. $\exists\, \zeta_\circ \in \mathbb{R},\ |\zeta_\circ| \le \zeta/2 :\ \mathrm{fl}(x/2) = x/2 + \zeta_\circ$ [L0: `sign_inner.h:248-325`] (Fact J.2);
2. $\forall \circ \in \{+, -\}\ \exists\, u_\circ, \zeta_\circ \in \mathbb{R},\ |u_\circ| \le u,\ |\zeta_\circ| \le \zeta :\ \mathrm{fl}(\mathrm{fl}(x \circ y)/2) = ((x \circ y)(1 + u_\circ) + \zeta_\circ)/2$ [L0: `sign_inner.h:248-325`] (Definition A.4, item 1; Fact J.2);

3. $|i| < 2^{53} \Rightarrow \mathrm{fl}(i) = i$ [L0: `sign_inner.h:105-190`] (Fact J.2, item 4);

4. $\mathrm{fl}(-x) = -x$ [L0: `sign_inner.h:241`] (Fact J.2, item 1);

5. $\mathrm{fl}(\mathrm{conj}\, x) = \mathrm{conj}\, x$ [L0: `sign_inner.h:241`] (Fact J.2, item 1).

Lemma J.4 (The floating-point signer's stored twiddles [to table])**.** *In the floating-point signer, each stored root of unity is the root rounded once per component, so it lies within the realization's rounding of the root: the signer meets Definition A.8, item 1. Let:*

- $k \in \{1, \dots, 2^{10} - 1\}$.

Define:

- $\mathcal{F}$, $u := 2^{-53}$ *and* $\zeta := 0$, *those of Definition J.1;*
- $k_j \in \{0, 1\}$, $j < 10$, *by* $k = \sum_{j<10} k_j 2^j$;
- $\mathrm{rev}_{10}(k) := \sum_{j<10} k_j 2^{9-j}$;
- $\psi_k := \exp(i\pi\, \mathrm{rev}_{10}(k)/1024)$;
- $\tilde{\psi}_k :=$ `GM`$[k]$, *the stored root [L0: `sign_fpoly.c:13`].*

Measured:

- $\tilde{\psi}_k$ *in* `c-fft-dsa`*: each component is the value of* $\mathcal{F}$ *nearest to the component of* ψ_k, *bit for bit up to the sign of a zero, at 0 exceptions [gate: `verify/gates/fp/twiddle.py`].*

Then

$$\tilde{\psi}_k \; \mathcal{I}\left(u^{\pm} + \sqrt{2}\zeta^{\pm}, 0\right) \psi_k.$$

Proof.

DEFINES $c_k := \cos(\pi\, \mathrm{rev}_{10}(k)/1024)$
DEFINES $s_k := \sin(\pi\, \mathrm{rev}_{10}(k)/1024)$
COMPUTES $\widetilde{c}_k := \mathrm{Re}\, \widetilde{\psi}_k$
COMPUTES $\widetilde{s}_k := \mathrm{Im}\, \widetilde{\psi}_k$

(L1) $\psi_k = c_k + i s_k$
[ψ_k (the statement); Fact A.41, item 12: $e^{i\theta} = \cos\theta + i \sin\theta$]

(L2) $\widetilde{c}_k = \mathrm{RN}(c_k)$
[the statement's measured row [L0: `sign_fpoly.c:8-12`]]

(L3) $\widetilde{s}_k = \mathrm{RN}(s_k)$
[the statement's measured row [L0: `sign_fpoly.c:8-12`]]

(L4) $\Rightarrow \exists\, u_c, \zeta_c \in \mathbb{R},\ |u_c| \le u,\ |\zeta_c| \le \zeta :\ \widetilde{c}_k = c_k(1 + u_c) + \zeta_c$
[(L2); Definition A.4: $\mathrm{fl}(c) = c(1 + u_\circ) + \zeta_\circ$ for a stored constant c]

(L5) $\Rightarrow \exists\, u_s, \zeta_s \in \mathbb{R},\ |u_s| \le u,\ |\zeta_s| \le \zeta :\ \widetilde{s}_k = s_k(1 + u_s) + \zeta_s$
[(L3); Definition A.4: $\mathrm{fl}(c) = c(1 + u_\circ) + \zeta_\circ$ for a stored constant c]

(L6) $|\psi_k| = 1$
[(L1); Fact A.41, item 12: $\cos^2\theta + \sin^2\theta = 1$; Fact A.41, item 1: $|a + ib|^2 = a^2 + b^2$]

Lemma B.2, item 4	This proof
Shared: u, ζ	
a	ψ_k
$\tilde{a}$	$\widetilde{\psi}_k$
(I1) $a \in \mathbb{C}$	(L1)
$\lvert a\rvert = 1$	(L6)
$\tilde{a} \in C_{\mathcal{F}}$	(L2), (L3); $\widetilde{c}_k$, $\widetilde{s}_k$ (the proof's block)
$\tilde{a}_r \; \mathcal{I}\,(u^{\pm}, \zeta^{\pm})\; a_r$	(L1), (L4); $\widetilde{c}_k$ (the proof's block)
$\tilde{a}_i \; \mathcal{I}\,(u^{\pm}, \zeta^{\pm})\; a_i$	(L1), (L5); $\widetilde{s}_k$ (the proof's block)
Its item 4: $\tilde{a}\; \mathcal{I}\left(u^{\pm} + \sqrt{2}\,\zeta^{\pm}, 0\right)\; a$	

(L7) $\Rightarrow \widetilde{\psi}_k \; \mathcal{I}\left(u^{\pm} + \sqrt{2}\,\zeta^{\pm}, 0\right) \psi_k$
[(I1)]

(L8) $\Rightarrow$ the statement

[(L7)]

□

Definition J.5 (The value of a word [to table])**.** A 64-bit word has three fields, and its value is read from them. Let:

- $W \in \{0, \dots, 2^{64} - 1\}$;
- $s \in \{0, 1\}$;
- $e \in \mathbb{Z}$;
- $M \in \mathbb{Z}$.

Define:

- $s_W := \lfloor W/2^{63} \rfloor$, the sign;
- $e_W := \lfloor W/2^{52} \rfloor \bmod 2^{11}$, the biased exponent;
- $m_W := W \bmod 2^{52}$, the significand field;
- $\mathrm{val}(s, e, M) := (1 - 2s)M2^{e-1075}$;
- $\mathrm{val}(W)$, the value of W,

$$\mathrm{val}(W) := \begin{cases} \mathrm{val}(s_W, e_W, 2^{52} + m_W) & \text{at } e_W \geq 1, \\ 0 & \text{at } W \in \{0, 2^{63}\}. \end{cases}$$

```
noncomputable def wordVal (W : Int) : Real :=
  if W / 2 ^ 52 % 2 ^ 11 = 0 then (1 - 2 * (W / 2 ^ 63 : Int)) * (W % 2 ^ 52 : Int) * (2 :
      Real) ^ (-1074 : Int)
  else fprVal (W / 2 ^ 63) (W / 2 ^ 52 % 2 ^ 11) (W % 2 ^ 52 + 2 ^ 52)

noncomputable def fprVal (s e M : Int) : Real := (1 - 2 * s) * M * (2 : Real) ^ (e - 1075)
```

Figure 97: The Lean declarations carrying Definition J.5: `wordVal`, `fprVal` (`FprRound.lean`, `MachineWords.lean`); Lean's symbols in ASCII.

Lemma J.6 (The spacing of the elements of $\mathcal{F}$ [to table])**.** *Every element of $\mathcal{F}$ is an integer multiple of a given power of two, or smaller than 2^{52} times it in modulus. Let:*

- $f \in \mathbb{Z}$.

Define:

- *$\mathcal{F}$, that of Definition J.1;*
- $g = 2^{f-1075}$.

Then

$$\forall w \in \mathcal{F}: \quad w \in g\mathbb{Z} \vee |w| < 2^{52}g.$$

Proof. (L1) $\forall w \in \mathcal{F} \setminus \{0\}\ \exists m, e \in \mathbb{Z},\ 2^{52} \leq m < 2^{53}:\ |w| = m2^e$

[Definition J.1]

(L2) $\forall w \in \mathcal{F} \setminus \{0\},\ |w| = m2^e,\ e \geq f - 1075:\ |w| = m2^{e-f+1075}g$

[(L1); g (the statement)]

(L3) $\Rightarrow$ $\forall w \in \mathcal{F} \setminus \{0\},\ |w| = m2^e,\ e \geq f - 1075:\ w \in g\mathbb{Z}$

[(L2); $m \in \mathbb{Z}$, $e - f + 1075 \geq 0$]

(L4) $\forall w \in \mathcal{F} \setminus \{0\},\ |w| = m2^e,\ e < f - 1075:\ |w| < 2^{53}2^e$

[$m < 2^{53}$ ((L1))]

(L5) $\forall e \in \mathbb{Z},\ e < f - 1075:\ 2^{53}2^e \leq 2^{52}g$

[$e \leq f - 1076$ ($e, f \in \mathbb{Z}$, $e < f - 1075$, the line's quantifier); g (the statement)]

(L6) $\Rightarrow$ $\forall w \in \mathcal{F} \setminus \{0\},\ |w| = m2^e,\ e < f - 1075:\ |w| < 2^{52}g$

[(L4), (L5)]

(L7) $0 \in g\mathbb{Z}$

[$0 = 0 \cdot g$]

(L8) $\Rightarrow\ \forall w \in \mathcal{F}:\ w \in g\mathbb{Z} \vee |w| < 2^{52}g$

[(L3), (L6), (L7)]

(L9) $\Rightarrow$ the statement

[(L8)]

□

Lemma J.7 (A word's value at a normalized significand [to table])**.** *A word whose significand lies in* $[2^{52}, 2^{53}]$ *holds an element of* $\mathcal{F}$*: its sign times its significand times the power of two its exponent field sets. Let:*

- $s \in \{0, 1\}$*;*
- $f \in \{1, \ldots, 2045\}$*;*
- $Q \in \mathbb{Z}$*.*

Define:

- $\mathcal{F}$*, that of Definition J.1;*
- val*, that of Definition J.5;*
- $W = s2^{63} + (f-1)2^{52} + Q$*;*
- $g = 2^{f-1075}$*.*

Assume:

(A1) $2^{52} \le Q \le 2^{53}$*.*

Then

1. $\mathrm{val}(W) = (1-2s)Qg$*;*
2. $\mathrm{val}(W) \in \mathcal{F}$*.*

Proof. Proof of item 1.

(L1) $Q < 2^{53} \Rightarrow\ (s_W, e_W, m_W) = (s, f, Q - 2^{52})$

[W (the statement); $2^{52} \le Q$ (assumption A1); Definition J.5]

(L2) $Q = 2^{53} \Rightarrow\ (s_W, e_W, m_W) = (s, f+1, 0)$

[W (the statement); Definition J.5]

(L3) $Q < 2^{53} \Rightarrow\ \mathrm{val}(W) = (1-2s)Q2^{f-1075}$

[(L1); Definition J.5]

(L4) $Q = 2^{53} \Rightarrow\ \mathrm{val}(W) = (1-2s)2^{52}2^{f+1-1075}$

[(L2); Definition J.5]

(L5) $(1-2s)2^{52}2^{f+1-1075} = (1-2s)2^{53}g$

[g (the statement)]

(L6) $\Rightarrow\ \mathrm{val}(W) = (1-2s)Qg$

[(L3), (L4), (L5); g (the statement)]

(L7) $\Rightarrow$ item 1

[(L6)]

□ (item 1)

Proof of item 2.

(L8) $f - 1075 \in \{-1074, \ldots, 970\}$

[$f \in \{1, \ldots, 2045\}$ (the statement)]

(L9) $Q < 2^{53} \Rightarrow\ \mathrm{val}(W) \in \mathcal{F}$

[(L3), (L8); $2^{52} \le Q$ (assumption A1); Definition J.1]

(L10) $Q = 2^{53} \Rightarrow\ \mathrm{val}(W) \in \mathcal{F}$

[(L4), (L8); Definition J.1]

(L11) $\Rightarrow$ $\mathrm{val}(W) \in \mathcal{F}$

[(L9), (L10)]

(L12) $\Rightarrow$ item 2

[(L11)]

□ (item 2)

Lemma J.8 (The round-up bit [to table])**.** *A quotient plus its round-up bit counts the multiple of the divisor nearest to the dividend, even at a tie, within half the divisor. Let:*

- $d \in \mathbb{Z}_{>0}$ *(Definition A.1);*
- $M, Q, R \in \mathbb{Z}$.

Define:

- $[C] = 1$ *for a condition* C *that holds,* $[C] = 0$ *otherwise;*
- $b = [2R > d] + [2R = d]\,[Q \equiv 1 \pmod 2]$.

Assume:

(A1) $M = Qd + R$;

(A2) $0 \le R < d$.

Then

1. $\forall q \in \mathbb{Z} :\ |(Q+b)d - M| \le |qd - M|$;
2. $\forall q \in \mathbb{Z},\ q \ne Q+b,\ |qd - M| = |(Q+b)d - M| :\ Q + b \equiv 0 \pmod 2$;
3. $2|(Q+b)d - M| \le d$.

Proof.

DEFINES $Q' = Q + b$

Proof of item 1.

(L1) $\forall q \in \mathbb{Z} :\ |qd - M| = |(q-Q)d - R|$

[$M = Qd + R$ (assumption A1)]

(L2) $\forall q \in \mathbb{Z},\ q \le Q - 1 :\ |qd - M| \ge d + R$

[(L1); $R \ge 0$ (assumption A2)]

(L3) $\forall q \in \mathbb{Z},\ q \ge Q + 2 :\ |qd - M| \ge 2d - R$

[(L1); $R < d$ (assumption A2)]

(L4) $|Qd - M| = R$

[(L1); $R \ge 0$ (assumption A2)]

(L5) $|(Q+1)d - M| = d - R$

[(L1); $R < d$ (assumption A2)]

(L6) $\forall q \in \mathbb{Z} :\ \min(R, d-R) \le |qd - M|$

[(L2) to (L5); $R \in [0, d)$ (assumption A2)]

(L7) $b = 0 \Rightarrow\ 2R \le d$

[b (the statement)]

(L8) $b = 1 \Rightarrow\ 2R \ge d$

[b (the statement)]

(L9) $|Q'd - M| = \min(R, d-R)$

[(L4), (L5), (L7), (L8); $Q' = Q + b$ (the block)]

(L10) $\Rightarrow\ \forall q \in \mathbb{Z} :\ |Q'd - M| \le |qd - M|$

[(L6), (L9)]

(L11) $\Rightarrow$ item 1

[(L10)]

□ (item 1)

Proof of item 2.

(L12) $\forall q \in \mathbb{Z},\ q \notin \{Q, Q+1\} :\ |qd - M| > \min(R, d-R)$

[(L2), (L3); $R \in [0, d)$ (assumption A2)]

(L13) $\forall q \in \mathbb{Z},\ q \neq Q',\ |qd - M| = |Q'd - M| :\ 2R = d$

[(L4), (L5), (L9), (L12)]

(L14) $2R = d \Rightarrow\ Q' = Q + [Q \equiv 1 \pmod 2]$

[b (the statement); $Q' = Q + b$ (the block)]

(L15) $[Q \equiv 1 \pmod 2] \equiv Q \pmod 2$

[[·] (the statement)]

(L16) $Q + [Q \equiv 1 \pmod 2] \equiv 0 \pmod 2$

[(L15)]

(L17) $\Rightarrow\ \forall q \in \mathbb{Z},\ q \neq Q',\ |qd - M| = |Q'd - M| :\ Q' \equiv 0 \pmod 2$

[(L13), (L14), (L16)]

(L18) $\Rightarrow$ item 2

[(L17)]

□ (item 2)

Proof of item 3.

(L19) $\forall a, a' \in \mathbb{R} :\ 2\min(a, a') \leq a + a'$

[$\min(a, a') \leq a$, $\min(a, a') \leq a'$ (Fact A.41, item 20)]

(L20) $\Rightarrow\ 2|Q'd - M| \leq d$

[(L9); (L19) at $(a, a') = (R, d-R)$]

(L21) $\Rightarrow$ item 3

[(L20)]

□ (item 3)

Lemma J.9 (The word with the round-up bit [to table])**.** *The word built from a quotient and its round-up bit holds the element of $\mathcal{F}$ nearest to the scaled quotient, even at a tie, within a relative 2^{-53} of it. Let:*

- $s \in \{0, 1\}$;
- $f \in \{1, \ldots, 2045\}$;
- $d \in \mathbb{Z}_{>0}$;
- $M, Q, R \in \mathbb{Z}$.

Define:

- $\mathcal{F}$, *that of Definition J.1;*
- val, *that of Definition J.5;*
- $b = [2R > d] + [2R = d]\,[Q \equiv 1 \pmod 2]$;
- $W = s2^{63} + (f-1)2^{52} + Q + b$;
- $v = (1 - 2s)(M/d)2^{f-1075}$.

Assume:

(A1) $M = Qd + R$;
(A2) $0 \leq R < d$;
(A3) $2^{52} \leq Q < 2^{53}$.

Then

1. $\mathrm{val}(W) \in \mathcal{F}$;
2. $\forall w \in \mathcal{F} :\ |\mathrm{val}(W) - v| \leq |w - v|$;
3. $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w - v| = |\mathrm{val}(W) - v| :\ W \equiv 0 \pmod 2$;
4. $\mathrm{val}(W)\ \mathcal{I}\left((2^{-53})^{\pm}, 0\right)\ v$.

Proof.

DEFINES $Q' = Q + b$

DEFINES $g = 2^{f-1075}$

DEFINES $V = (M/d)g$

Proof of item 1.

(L1) $Q' \in [2^{52}, 2^{53}]$

[$Q \in [2^{52}, 2^{53})$ (assumption A3); $b \in \{0, 1\}$ (the statement's b)]

(L2) $\mathrm{val}(W) = (1 - 2s)Q'g$

[Lemma J.7, item 1, at $Q := Q'$; (L1)]

(L3) $\mathrm{val}(W) \in \mathcal{F}$

[Lemma J.7, item 2, at $Q := Q'$; (L1)]

(L4) $\Rightarrow$ item 1

[(L3)]

□ (item 1)

Proof of item 2.

(L5) $\forall q \in \mathbb{Z} : \ |Q'd - M| \le |qd - M|$

[Lemma J.8, item 1; $Q' = Q + b$ (the block); its assumptions by assumptions A1, A2]

(L6) $\forall q \in \mathbb{Z} : \ |qg - V| = |qd - M|g/d$

[g, V (the block)]

(L7) $M \ge 2^{52}d$

[$M = Qd + R$, $R \ge 0$, $Q \ge 2^{52}$ (assumptions A1, A2, A3)]

(L8) $V \ge 2^{52}g$

[(L7); V (the block)]

(L9) $\forall w \in \mathcal{F} : \ (1 - 2s)w \in \mathcal{F}$

[Definition J.1]

(L10) $\forall w \in \mathbb{R} : \ |w - v| = |(1 - 2s)w - V|$

[$v = (1 - 2s)V$ (v, the statement; V, the block); $s \in \{0, 1\}$ (the statement)]

(L11) $|\mathrm{val}(W) - v| = |Q'g - V|$

[(L2), (L10)]

(L12) $\forall q \in \mathbb{Z} : \ |Q'g - V| \le |qg - V|$

[(L5), (L6)]

(L13) $\forall w' \in \mathcal{F}, \ |w'| < 2^{52}g : \ |w' - V| > V - 2^{52}g$

[(L8); $|w' - V| \ge V - |w'|$ (Fact A.41, item 1)]

(L14) $V - 2^{52}g = |2^{52}g - V|$

[(L8)]

(L15) $|2^{52}g - V| \ge |Q'g - V|$

[(L12) at $q = 2^{52}$]

(L16) $\Rightarrow \ \forall w' \in \mathcal{F}, \ |w'| < 2^{52}g : \ |w' - V| > |Q'g - V|$

[(L13), (L14), (L15)]

(L17) $\Rightarrow \ \forall w \in \mathcal{F} : \ |\mathrm{val}(W) - v| \le |w - v|$

[Lemma J.6 at f, on $(1 - 2s)w$; (L9) to (L12), (L16)]

(L18) $\Rightarrow$ item 2

[(L17)]

□ (item 2)

Proof of item 3.

(L19) $W \equiv Q' \pmod 2$

[W (the statement); $s2^{63} + (f - 1)2^{52} \equiv 0 \pmod 2$ ($s, f \in \mathbb{Z}$, the statement)]

(L20) $\forall w \in \mathcal{F}, \ w \ne \mathrm{val}(W), \ |w - v| = |\mathrm{val}(W) - v| \ \exists q \in \mathbb{Z}, \ q \ne Q' : \ (1 - 2s)w = qg$

[Lemma J.6 at f, on $(1 - 2s)w$; (L2), (L9), (L10), (L11), (L16)]

(L21) $\Rightarrow$ $|qd - M| = |Q'd - M|$

[(L6), (L10), (L11), (L20)]

(L22) $\Rightarrow$ $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w - v| = |\mathrm{val}(W) - v| :\ W \equiv 0 \pmod 2$

[Lemma J.8, item 2; (L19), (L21); its assumptions by assumptions A1, A2]

(L23) $\Rightarrow$ item 3

[(L22)]

□ (item 3)

Proof of item 4.

(L24) $2|Q'd - M| \leq d$

[Lemma J.8, item 3; its assumptions by assumptions A1, A2]

(L25) $|\mathrm{val}(W) - v| = |Q'd - M|g/d$

[(L6) at $q = Q'$, (L11)]

(L26) $|\mathrm{val}(W) - v| \leq g/2$

[(L24), (L25)]

(L27) $g/2 \leq 2^{-53}V$

[(L8)]

(L28) $|v| = V$

[(L10) at $w = 0$; $V > 0$ ((L8))]

(L29) $\Rightarrow$ $|\mathrm{val}(W) - v| \leq 2^{-53}|v|$

[(L26), (L27), (L28)]

(L30) $v \neq 0$

[(L8), (L28)]

(L31) $\Rightarrow$ $\exists u_\circ \in \mathbb{R},\ |u_\circ| \leq 2^{-53} :\ \mathrm{val}(W) = v(1 + u_\circ)$

[(L29), (L30); $u_\circ := (\mathrm{val}(W) - v)/v$]

(L32) $\Rightarrow$ item 4

[(L31); Definition A.10]

□ (item 4)

Lemma J.10 (The word of a nearest integer significand [to table])**.** *The word built from the integer nearest to a real value, even at a tie, holds the element of $\mathcal{F}$ nearest to the scaled value, even at a tie, within a relative 2^{-53} of it. Let:*

- $s \in \{0, 1\}$;
- $f \in \{1, \ldots, 2045\}$;
- $Q \in \mathbb{Z}$;
- $b \in \{0, 1\}$;
- $t \in \mathbb{R}$.

Define:

- $\mathcal{F}$, *that of Definition J.1*;
- val, *that of Definition J.5*;
- $W = s2^{63} + (f - 1)2^{52} + Q + b$;
- $v = (1 - 2s)t2^{f-1075}$.

Assume:

(A1) $2^{52} \leq Q < 2^{53}$;

(A2) $Q \leq t < Q + 1$;

(A3) $\forall q \in \mathbb{Z} :\ |Q + b - t| \leq |q - t|$;

(A4) $\forall q \in \mathbb{Z},\ q \neq Q + b,\ |q - t| = |Q + b - t| :\ Q + b \equiv 0 \pmod 2$.

Then

1. $\mathrm{val}(W) \in \mathcal{F}$;

2. $\forall w \in \mathcal{F}:\ |\mathrm{val}(W) - v| \le |w - v|$;

3. $\forall w \in \mathcal{F},\ w \ne \mathrm{val}(W),\ |w - v| = |\mathrm{val}(W) - v|:\ W \equiv 0 \pmod 2$;

4. $\mathrm{val}(W)\ \mathcal{I}\left((2^{-53})^{\pm}, 0\right)\ v$.

Proof.

DEFINES $Q' = Q + b$

DEFINES $g = 2^{f-1075}$

DEFINES $V = tg$

Proof of item 1.

(L1) $Q' \in [2^{52}, 2^{53}]$

[$Q \in [2^{52}, 2^{53})$ (assumption A1); $b \in \{0, 1\}$ (the statement)]

(L2) $\mathrm{val}(W) = (1 - 2s)Q'g$

[Lemma J.7, item 1, at $Q := Q'$; (L1)]

(L3) $\mathrm{val}(W) \in \mathcal{F}$

[Lemma J.7, item 2, at $Q := Q'$; (L1)]

(L4) $\Rightarrow$ item 1

[(L3)]

□ (item 1)

Proof of item 2.

(L5) $\forall q \in \mathbb{Z}:\ |qg - V| = |q - t|g$

[g, V (the block)]

(L6) $V \ge 2^{52}g$

[$t \ge Q$, $Q \ge 2^{52}$ (assumptions A1, A2); V (the block)]

(L7) $\forall w \in \mathcal{F}:\ (1 - 2s)w \in \mathcal{F}$

[Definition J.1]

(L8) $\forall w \in \mathbb{R}:\ |w - v| = |(1 - 2s)w - V|$

[$v = (1 - 2s)V$ (v, the statement; V, the block); $s \in \{0, 1\}$ (the statement)]

(L9) $|\mathrm{val}(W) - v| = |Q'g - V|$

[(L2), (L8)]

(L10) $\forall q \in \mathbb{Z}:\ |Q'g - V| \le |qg - V|$

[(L5); $|Q' - t| \le |q - t|$ (assumption A3)]

(L11) $\forall w' \in \mathcal{F},\ |w'| < 2^{52}g:\ |w' - V| > V - 2^{52}g$

[(L6); $|w' - V| \ge V - |w'|$ (Fact A.41, item 1)]

(L12) $V - 2^{52}g = |2^{52}g - V|$

[(L6)]

(L13) $|2^{52}g - V| \ge |Q'g - V|$

[(L10) at $q = 2^{52}$]

(L14) $\Rightarrow\ \forall w' \in \mathcal{F},\ |w'| < 2^{52}g:\ |w' - V| > |Q'g - V|$

[(L11), (L12), (L13)]

(L15) $\Rightarrow\ \forall w \in \mathcal{F}:\ |\mathrm{val}(W) - v| \le |w - v|$

[Lemma J.6 at f, on $(1 - 2s)w$; (L7) to (L10), (L14)]

(L16) $\Rightarrow$ item 2

[(L15)]

□ (item 2)

Proof of item 3.

(L17) $W \equiv Q' \pmod 2$

[W (the statement); $s2^{63} + (f - 1)2^{52} \equiv 0 \pmod 2$ ($s, f \in \mathbb{Z}$, the statement)]

(L18) $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w-v| = |\mathrm{val}(W)-v|\ \exists q \in \mathbb{Z},\ q \neq Q' :\ (1-2s)w = qg$
[Lemma J.6 at f, on $(1-2s)w$; (L2), (L7), (L8), (L9), (L14)]

(L19) $\Rightarrow\ |q-t| = |Q'-t|$
[(L5), (L8), (L9), (L18)]

(L20) $\Rightarrow\ \forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w-v| = |\mathrm{val}(W)-v| :\ W \equiv 0 \pmod 2$
[(L17), (L19); $Q' \equiv 0 \pmod 2$ at a tie (assumption A4)]

(L21) $\Rightarrow$ item 3
[(L20)]

□ (item 3)

Proof of item 4.

(L22) $|Q'-t| \leq t-Q$
[$|Q'-t| \leq |q-t|$ at $q=Q$ (assumption A3); $Q \leq t$ (assumption A2)]

(L23) $|Q'-t| \leq Q+1-t$
[$|Q'-t| \leq |q-t|$ at $q=Q+1$ (assumption A3); $t < Q+1$ (assumption A2)]

(L24) $\Rightarrow\ 2|Q'-t| \leq 1$
[(L22), (L23)]

(L25) $|\mathrm{val}(W)-v| = |Q'-t|g$
[(L5) at $q=Q'$, (L9)]

(L26) $|\mathrm{val}(W)-v| \leq g/2$
[(L24), (L25)]

(L27) $g/2 \leq 2^{-53}V$
[(L6)]

(L28) $|v| = V$
[(L8) at $w=0$; $V>0$ ((L6))]

(L29) $\Rightarrow\ |\mathrm{val}(W)-v| \leq 2^{-53}|v|$
[(L26), (L27), (L28)]

(L30) $v \neq 0$
[(L6), (L28)]

(L31) $\Rightarrow\ \exists u_\circ \in \mathbb{R},\ |u_\circ| \leq 2^{-53} :\ \mathrm{val}(W) = v(1+u_\circ)$
[(L29), (L30); $u_\circ := (\mathrm{val}(W)-v)/v$]

(L32) $\Rightarrow$ item 4
[(L31); Definition A.10]

□ (item 4)

The operations proved on a compiled object. The code's operations proved on a compiled object by CryptoLine (Section 2.2) are the following four lemmas and Lemmas J.20, J.21 and J.22.

Lemma J.11 (The object of `fpr_mul` [to table])**.** *The Cortex-M4 object of* `fpr_mul` *returns the word of the element of $\mathcal{F}$ nearest to the product, even at a tie, within a relative 2^{-53} of it, and a signed zero at a zero operand. Define:*

- *$\mathcal{F}$, that of Definition J.1.*

Let:

- *$x, y \in \mathcal{F}$.*

Define:

- val*, that of Definition J.5;*
- *W_x and W_y, the binary64 words that store x and y (Definition J.1);*
- *$(x_s, e_x, x_m) = (s_{W_x}, e_{W_x}, m_{W_x})$, the fields of W_x (Definition J.5);*
- *$(y_s, e_y, y_m) = (s_{W_y}, e_{W_y}, m_{W_y})$, the fields of W_y;*

- W, *the word the Cortex-M4* `arm-none-eabi-gcc -O2` *object of* `fpr_mul` *returns on* (W_x, W_y).

Then

1. *Assume:*

   (A1) $e_x, e_y \geq 1$;
   (A2) $2^{-1022} \leq |xy| < 2^{1023}$.

   Then $\mathrm{val}(W) = \mathrm{fl}(xy)$.

2. *Assume:*

   (A3) $e_x, e_y \geq 1$;
   (A4) $2^{-1022} \leq |xy| < 2^{1023}$.

   Then $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w - xy| = |\mathrm{val}(W) - xy| :\ W \equiv 0 \pmod 2$.

3. *Assume:*

   (A5) $e_x, e_y \geq 1$;
   (A6) $2^{-1022} \leq |xy| < 2^{1023}$.

   Then $\mathrm{fl}(xy)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ xy$.

4. *Assume:*

   (A7) $W_x \in \{0, 2^{63}\}$ *or* $W_y \in \{0, 2^{63}\}$.

   Then $W = ((x_s + y_s) \bmod 2)2^{63}$.

[CryptoLine: `lemmas/fpr_cfndsa/mul/lem_mul.cl`*]*

Proof.

DEFINES $X = 2^{52} + x_m$
DEFINES $Y = 2^{52} + y_m$
DEFINES $P = XY$
DEFINES $E = [P \geq 2^{105}]$
DEFINES $Q = \lfloor P/2^{52+E} \rfloor$
DEFINES $R = P - Q2^{52+E}$
DEFINES $b = [2R > 2^{52+E}] + [2R = 2^{52+E}]\,[Q \equiv 1 \pmod 2]$
DEFINES $f = e_x + e_y + E - 1023$
MEASURED the object: 85 instructions, no branch [CryptoLine: `lemmas/fpr_cfndsa/mul/lem_mul.cl`]

Proof of items 1 to 3.

(L1) $X \in [2^{52}, 2^{53})$
[$e_x \geq 1$ (assumptions A1, A3, A5); X (the block)]

(L2) $Y \in [2^{52}, 2^{53})$
[$e_y \geq 1$ (assumptions A1, A3, A5); Y (the block)]

(L3) $P \in [2^{104+E}, 2^{105+E})$
[(L1), (L2); P, E (the block)]

(L4) $Q \in [2^{52}, 2^{53})$
[(L3); Q (the block)]

(L5) $R \in [0, 2^{52+E})$
[Q, R (the block)]

(L6) $|xy| = P2^{e_x+e_y-2150}$
[Definition J.5; X, Y, P (the block)]

(L7) $e_x + e_y + E \in [1024, 3068]$
[(L3), (L6); $|xy| \in [2^{-1022}, 2^{1023})$ (assumptions A2, A4, A6)]

(L8) $f \in [1, 2045]$

[(L7); f (the block)]

(L9) $W \equiv ((x_s + y_s) \bmod 2)2^{63} + (f-1)2^{52} + Q + b \pmod{2^{64}}$

[[CryptoLine: `lemmas/fpr_cfndsa/mul/lem_mul.cl`], `lem_mul.cl` at (P, E, Q, R), its precondition by (L3), (L7); b, f (the block)]

(L10) $((x_s + y_s) \bmod 2)2^{63} + (f-1)2^{52} + Q + b < 2^{64}$

[(L4), (L8); b (the block)]

(L11) $W = ((x_s + y_s) \bmod 2)2^{63} + (f-1)2^{52} + Q + b$

[(L9), (L10); $W \in \{0, \ldots, 2^{64} - 1\}$ (Definition J.5)]

(L12) $xy = (1 - 2((x_s + y_s) \bmod 2))(P/2^{52+E})2^{f-1075}$

[Definition J.5; X, Y, P, f (the block)]

(L13) $\mathrm{val}(W) = \mathrm{fl}(xy)$

[Lemma J.9, items 1 and 2, at $s = (x_s + y_s) \bmod 2$, f, $d = 2^{52+E}$, $M = P$; (L4), (L5), (L8), (L11), (L12); fl (Definition J.1)]

(L14) $\Rightarrow$ item 1

[(L13)]

(L15) $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w - xy| = |\mathrm{val}(W) - xy| :\ W \equiv 0 \pmod 2$

[Lemma J.9, item 3, at the same values; (L4), (L5), (L8), (L11), (L12)]

(L16) $\Rightarrow$ item 2

[(L15)]

(L17) $\mathrm{fl}(xy)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ xy$

[Lemma J.9, item 4, at the same values; (L12), (L13)]

(L18) $\Rightarrow$ item 3

[(L17)]

□ (items 1 to 3)

Proof of item 4.

(L19) $W = ((x_s + y_s) \bmod 2)2^{63}$

[[CryptoLine: `lemmas/fpr_cfndsa/mul/lem_mul_zero.cl`], `lem_mul_zero.cl`; $W_x \in \{0, 2^{63}\}$ or $W_y \in \{0, 2^{63}\}$ (assumption A7)]

(L20) $\Rightarrow$ item 4

[(L19)]

□ (item 4)

Lemma J.12 (The object of `fpr_add` [to table])**.** *The Cortex-M4 object of* `fpr_add` *returns the word of the element of $\mathcal{F}$ nearest to the sum, even at a tie, within a relative 2^{-53} of it; operands more than 63 binades apart return the larger, a cancelling pair returns $+0$, and a zero operand returns the other. Define:*

- *$\mathcal{F}$, that of Definition J.1.*

Let:

- *$x, y \in \mathcal{F}$.*

Define:

- val, *that of Definition J.5;*
- *W_x and W_y, the binary64 words that store x and y (Definition J.1);*
- *$(x_s, e_x, x_m) = (s_{W_x}, e_{W_x}, m_{W_x})$, the fields of W_x (Definition J.5);*
- *$(y_s, e_y, y_m) = (s_{W_y}, e_{W_y}, m_{W_y})$, the fields of W_y;*
- *W, the word the Cortex-M4* `arm-none-eabi-gcc -O2` *object of* `fpr_add` *returns on (W_x, W_y).*

Then

1. *Assume:*

(A1) $e_x, e_y \geq 1$*;*
(A2) $|e_x - e_y| \leq 63$*;*
(A3) $2^{-1022} \leq |x + y| < 2^{1023}$.

Then $\mathrm{val}(W) = \mathrm{fl}(x + y)$.

2. *Assume:*

(A4) $e_x, e_y \geq 1$*;*
(A5) $|e_x - e_y| \leq 63$*;*
(A6) $2^{-1022} \leq |x + y| < 2^{1023}$.

Then $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w - (x + y)| = |\mathrm{val}(W) - (x + y)| :\ W \equiv 0 \pmod 2$.

3. *Assume:*

(A7) $e_x, e_y \geq 1$*;*
(A8) $|e_x - e_y| \leq 63$*;*
(A9) $2^{-1022} \leq |x + y| < 2^{1023}$.

Then $\mathrm{fl}(x + y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x + y)$.

4. *Assume:*

(A10) $e_x, e_y \geq 1$*;*
(A11) $e_x - e_y > 63$.

Then $W = W_x$.

5. *Assume:*

(A12) $e_x, e_y \geq 1$*;*
(A13) $e_y - e_x > 63$.

Then $W = W_y$.

6. *Assume:*

(A14) $e_x \geq 1$*;*
(A15) $y = -x$.

Then $W = 0$.

7. *Assume:*

(A16) $W_x \in \{0, 2^{63}\}$*;*
(A17) $W_y \notin \{0, 2^{63}\}$.

Then $W = W_y$.

8. *Assume:*

(A18) $W_y \in \{0, 2^{63}\}$*;*
(A19) $W_x \notin \{0, 2^{63}\}$.

Then $W = W_x$.

9. *Assume:*

(A20) $W_x, W_y \in \{0, 2^{63}\}$.

Then $W = x_s y_s 2^{63}$.

[CryptoLine: `lemmas/fpr_cfndsa/add/lem_add.cl` *]*

Proof.

DEFINES $X = 2^{52} + x_m$

DEFINES $Y = 2^{52} + y_m$

DEFINES $e_0 = \min(e_x, e_y)$

DEFINES $S_X = X2^{e_x - e_0}$

DEFINES $S_Y = Y2^{e_y - e_0}$

DEFINES $M = |(1 - 2x_s)S_X + (1 - 2y_s)S_Y|$

DEFINES $s_g = x_s$ at $x_s = y_s$ or $S_Y \le S_X$, and $s_g = y_s$ otherwise

DEFINES $L \in \mathbb{Z}$ with $2^L \le M < 2^{L+1}$

DEFINES $D = 2^{\max(L-52,0)}$

DEFINES $M' = M2^{\max(52-L,0)}$

DEFINES $Q = \lfloor M'/D \rfloor$

DEFINES $R = M' - QD$

DEFINES $b = [2R > D] + [2R = D]\,[Q \equiv 1 \pmod 2]$

DEFINES $f = e_0 + L - 52$

MEASURED the object: 156 instructions, no branch [CryptoLine: `lemmas/fpr_cfndsa/add/lem_add.cl`]

Proof of items 1 to 3.

(L1) $x + y = (1 - 2s_g)M2^{e_0 - 1075}$

[Definition J.5; X, Y, e_0, S_X, S_Y, M, s_g (the block); $e_x, e_y \ge 1$ (assumptions A1, A4, A7)]

(L2) $M > 0$

[(L1); $|x + y| \ge 2^{-1022}$ (assumptions A3, A6, A9)]

(L3) $S_X < 2^{116}$

[X (the block); $|e_x - e_y| \le 63$ (assumptions A2, A5, A8)]

(L4) $S_Y < 2^{116}$

[Y (the block); $|e_x - e_y| \le 63$ (assumptions A2, A5, A8)]

(L5) $L \le 116$

[$M < 2^{117}$ ((L3), (L4)); L (the block)]

(L6) $|x + y| \in [2^{e_0+L-1075}, 2^{e_0+L+1-1075})$

[(L1), (L2); L (the block)]

(L7) $e_0 + L \in [53, 2097]$

[(L6); $|x + y| \in [2^{-1022}, 2^{1023})$ (assumptions A3, A6, A9)]

(L8) $f \in [1, 2045]$

[(L7); f (the block)]

(L9) $M'/D = M2^{52-L}$

[D, M' (the block)]

(L10) $M'/D \in [2^{52}, 2^{53})$

[(L9); L (the block)]

(L11) $Q \in [2^{52}, 2^{53})$

[(L10); Q (the block)]

(L12) $M' = QD + R$

[R (the block)]

(L13) $R \in [0, D)$

[Q, R (the block)]

(L14) $W \equiv s_g 2^{63} + (f - 1)2^{52} + Q + b \pmod{2^{64}}$

[[CryptoLine: `lemmas/fpr_cfndsa/add/lem_add.cl`], `lem_add.cl` at $(e_0, S_X, S_Y, M, s_g, L, Q, R)$, its precondition by (L5), (L7), (L11), (L12); b, f (the block)]

(L15) $s_g 2^{63} + (f - 1)2^{52} + Q + b < 2^{64}$

[(L8), (L11); b (the block)]

(L16) $W = s_g 2^{63} + (f - 1)2^{52} + Q + b$

[(L14), (L15); $W \in \{0, \ldots, 2^{64} - 1\}$ (Definition J.5)]

(L17) $x + y = (1 - 2s_g)(M'/D)2^{f-1075}$

[(L1), (L9); f (the block)]

(L18) $\mathrm{val}(W) = \mathrm{fl}(x + y)$

[Lemma J.9, items 1 and 2, at $s = s_g$, f, $d = D$, $M := M'$; (L8), (L11) to (L13), (L16), (L17); fl (Definition J.1)]

(L19) $\Rightarrow$ item 1

[(L18)]

(L20) $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w - (x + y)| = |\mathrm{val}(W) - (x + y)| :\ W \equiv 0 \pmod 2$

[Lemma J.9, item 3, at the same values; (L8), (L11) to (L13), (L16), (L17)]

(L21) $\Rightarrow$ item 2

[(L20)]

(L22) $\mathrm{fl}(x + y)\ \mathcal{I}\ \left((2^{-53})^{\pm}, 0\right)\ (x + y)$

[Lemma J.9, item 4, at the same values; (L17), (L18)]

(L23) $\Rightarrow$ item 3

[(L22)]

□ (items 1 to 3)

Proof of items 4 to 9.

(L24) $W = W_x$

[[CryptoLine: `lemmas/fpr_cfndsa/add/lem_add_far.cl`], `lem_add_far.cl`; $e_x - e_y > 63$ (assumption A11); $e_x, e_y \geq 1$ (assumption A10)]

(L25) $\Rightarrow$ item 4

[(L24)]

(L26) $W = W_y$

[[CryptoLine: `lemmas/fpr_cfndsa/add/lem_add_far.cl`], `lem_add_far.cl`; $e_y - e_x > 63$ (assumption A13); $e_x, e_y \geq 1$ (assumption A12)]

(L27) $\Rightarrow$ item 5

[(L26)]

(L28) $W = 0$

[[CryptoLine: `lemmas/fpr_cfndsa/add/lem_add_cancel.cl`], `lem_add_cancel.cl`; $y = -x$ (assumption A15); $e_x \geq 1$ (assumption A14)]

(L29) $\Rightarrow$ item 6

[(L28)]

(L30) $W = W_y$

[[CryptoLine: `lemmas/fpr_cfndsa/add/lem_add_zero.cl`], `lem_add_zero.cl`; assumptions A16, A17]

(L31) $\Rightarrow$ item 7

[(L30)]

(L32) $W = W_x$

[[CryptoLine: `lemmas/fpr_cfndsa/add/lem_add_zero.cl`], `lem_add_zero.cl`; assumptions A18, A19]

(L33) $\Rightarrow$ item 8

[(L32)]

(L34) $W = x_s y_s 2^{63}$

[[CryptoLine: `lemmas/fpr_cfndsa/add/lem_add_zero.cl`], `lem_add_zero.cl`; assumption A20]

(L35) $\Rightarrow$ item 9

[(L34)]

□ (items 4 to 9)

Lemma J.13 (The object of `fpr_div` [to table])**.** *The Cortex-M4 object of* `fpr_div` *returns the word of the element of $\mathcal{F}$ nearest to the quotient, even at a tie, within a relative 2^{-53} of it. Define:*

- *$\mathcal{F}$, that of Definition J.1.*

Let:

- $x, y \in \mathcal{F}$.

Define:

- val, *that of Definition J.5;*
- W_x *and* W_y*, the binary64 words that store* x *and* y *(Definition J.1);*
- $(x_s, e_x, x_m) = (s_{W_x}, e_{W_x}, m_{W_x})$*, the fields of* W_x *(Definition J.5);*
- $(y_s, e_y, y_m) = (s_{W_y}, e_{W_y}, m_{W_y})$*, the fields of* W_y*;*
- W*, the word the Cortex-M4* `arm-none-eabi-gcc -O2` *object of* `fpr_div` *returns on* (W_x, W_y).

Assume:

(A1) $e_x, e_y \geq 1$*;*

(A2) $2^{-1022} \leq |x/y| < 2^{1023}$.

Then

1. $\mathrm{val}(W) = \mathrm{fl}(x/y)$*;*
2. $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w - x/y| = |\mathrm{val}(W) - x/y| :\ W \equiv 0 \pmod 2$*;*
3. $\mathrm{fl}(x/y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x/y)$.

[CryptoLine: `lemmas/fpr_cfndsa/div/lem_div.cl`*]*

Proof.

DEFINES	$X = 2^{52} + x_m$
DEFINES	$Y = 2^{52} + y_m$
COMPUTES	N_{it}: the number of loop iterations the object runs
COMPUTES	xu_j: the loop's remainder word after j iterations, $j \leq 55$ (`lem_divbody.cl`'s xu)
COMPUTES	q_j: the loop's quotient word after j iterations (`lem_divbody.cl`'s q)
COMPUTES	t_j: the quotient bit of iteration $j+1$ (`lem_divbody.cl`'s t)
DEFINES	$X_W = xu_{55}$
DEFINES	$Q_W = q_{55}$
DEFINES	$q = Q_W/2$
DEFINES	$r = X_W/2$
DEFINES	$E = [q \geq 2^{54}]$
DEFINES	$T = 2^{1+E}$
DEFINES	$Q = \lfloor q/T \rfloor$
DEFINES	$R = (q - QT)Y + r$
DEFINES	$f = e_x - e_y + 1022 + E$
DEFINES	$b = [2R > TY] + [2R = TY]\,[Q \equiv 1 \pmod 2]$
MEASURED	the object: a loop of 55 iterations on a counter [CryptoLine: `lemmas/fpr_cfndsa/div/lem_div.cl`]

(L1) $N_{\mathrm{it}} = 55$
[[CryptoLine: `lemmas/fpr_cfndsa/div/lem_div_path.cl`], `lem_div_path.cl`: the counter's 55 branches asserted]

(L2) $\forall j < 55 :\ xu_{j+1} = 2xu_j - 2t_jY$
[[CryptoLine: `lemmas/fpr_cfndsa/div/lem_divbody.cl`], `lem_divbody.cl`: the body as a contract from $xu_j < 2Y$]

(L3) $\forall j < 55 :\ q_{j+1} = 2q_j + 2t_j$
[[CryptoLine: `lemmas/fpr_cfndsa/div/lem_divbody.cl`], `lem_divbody.cl`]

(L4) $\forall j < 55 :\ xu_{j+1} < 2Y$
[[CryptoLine: `lemmas/fpr_cfndsa/div/lem_divbody.cl`], `lem_divbody.cl`]

(L5) $X_W + Q_WY = 2^{55}X$
[[CryptoLine: `lemmas/fpr_cfndsa/div/lem_div.cl`], `lem_div.cl`: (L2) to (L4) at the 55 iterations of (L1)]

(L6) $X_W \equiv 0 \pmod 2$

[[CryptoLine: `lemmas/fpr_cfndsa/div/lem_div.cl`], `lem_div.cl`]

(L7) $Q_W \equiv 0 \pmod 2$

[[CryptoLine: `lemmas/fpr_cfndsa/div/lem_div.cl`], `lem_div.cl`]

(L8) $r \in [0, Y)$

[[CryptoLine: `lemmas/fpr_cfndsa/div/lem_div.cl`], `lem_div.cl`; r (the block)]

(L9) $qY + r = 2^{54}X$

[(L5) to (L7); q, r (the block)]

(L10) $q \in [2^{53}, 2^{55})$

[(L8), (L9); $2^{52} \le X, Y < 2^{53}$ ($e_x, e_y \ge 1$, assumption A1)]

(L11) $Q \in [2^{52}, 2^{53})$

[(L10); E, T, Q (the block)]

(L12) $E = [X \ge Y]$

[(L8), (L9); E (the block)]

(L13) $|x/y| = (X/Y)2^{e_x - e_y}$

[Definition J.5; X, Y (the block)]

(L14) $f \in [1, 2045]$

[(L12), (L13); $|x/y| \in [2^{-1022}, 2^{1023})$ (assumption A2); f (the block)]

(L15) $2^{54}X = Q(TY) + R$

[(L9); Q, R (the block)]

(L16) $R \in [0, TY)$

[(L8); $q - QT \in [0, T)$ (Q, the block); R (the block)]

(L17) $W \equiv ((x_s + y_s) \bmod 2)2^{63} + (f - 1)2^{52} + Q + b \pmod{2^{64}}$

[[CryptoLine: `lemmas/fpr_cfndsa/div/lem_div.cl`], `lem_div.cl`: its round-up test on $(q - QT, r)$; b, R, f (the block)]

(L18) $((x_s + y_s) \bmod 2)2^{63} + (f - 1)2^{52} + Q + b < 2^{64}$

[(L11), (L14); b (the block)]

(L19) $W = ((x_s + y_s) \bmod 2)2^{63} + (f - 1)2^{52} + Q + b$

[(L17), (L18); $W \in \{0, \ldots, 2^{64} - 1\}$ (Definition J.5)]

(L20) $x/y = (1 - 2((x_s + y_s) \bmod 2))(2^{54}X/(TY))2^{f - 1075}$

[(L13); f, T (the block)]

(L21) $\mathrm{val}(W) = \mathrm{fl}(x/y)$

[Lemma J.9, items 1 and 2, at $s = (x_s + y_s) \bmod 2$, f, $d = TY$, $M = 2^{54}X$; (L11), (L14) to (L16), (L19), (L20); fl (Definition J.1)]

(L22) $\Rightarrow$ item 1

[(L21)]

(L23) $\forall w \in \mathcal{F},\ w \ne \mathrm{val}(W),\ |w - x/y| = |\mathrm{val}(W) - x/y| :\ W \equiv 0 \pmod 2$

[Lemma J.9, item 3, at the same values; (L11), (L14) to (L16), (L19), (L20)]

(L24) $\Rightarrow$ item 2

[(L23)]

(L25) $\mathrm{fl}(x/y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x/y)$

[Lemma J.9, item 4, at the same values; (L20), (L21)]

(L26) $\Rightarrow$ item 3

[(L25)]

□ (items 1 to 3)

Lemma J.14 (The object of `fpr_sqrt` [to table]). *The Cortex-M4 object of `fpr_sqrt` returns the word of the element of $\mathcal{F}$ nearest to the square root, even at a tie, within a relative 2^{-53} of it. Define:*

- *$\mathcal{F}$, that of Definition J.1.*

Let:

- $x \in \mathcal{F}$.

Define:

- val, *that of Definition J.5;*
- W_x, *the binary64 word that stores* x *(Definition J.1);*
- $(x_s, e_x, x_m) = (s_{W_x}, e_{W_x}, m_{W_x})$, *the fields of* W_x *(Definition J.5);*
- W, *the word the Cortex-M4* `arm-none-eabi-gcc -O2` *object of* `fpr_sqrt` *returns on* W_x.

Assume:

(A1) $e_x \geq 1$;

(A2) $x_s = 0$.

Then

1. $\mathrm{val}(W) = \mathrm{fl}(\sqrt{x})$;
2. $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w - \sqrt{x}| = |\mathrm{val}(W) - \sqrt{x}| :\ W \equiv 0 \pmod 2$;
3. $\mathrm{fl}(\sqrt{x})\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ \sqrt{x}$.

[CryptoLine: `lemmas/fpr_cfndsa/sqrt/lem_sqrt.cl`*]*

Proof.

DEFINES	$X = 2^{52} + x_m$
DEFINES	$p = (e_x + 1) \bmod 2$
DEFINES	$X' = 2(1 + p)X$
DEFINES	$N = 2^{53}X'$
COMPUTES	N_{it}: the number of loop iterations the object runs
COMPUTES	xu_j, q_j, r_j: the loop's remainder, root and bit words after j iterations, $j \leq 54$ (`lem_sqrtbody.cl`'s xu, q, r)
DEFINES	$X_W = xu_{54}$
DEFINES	$Q_W = q_{54}$
DEFINES	$Q = \lfloor Q_W/2 \rfloor$
DEFINES	$\rho = Q_W - 2Q$
DEFINES	$b = \rho\,[X_W > 0 \vee Q \equiv 1 \pmod 2]$
DEFINES	$t = \sqrt{N}/2$
DEFINES	$f = \lfloor (e_x + 1021)/2 \rfloor + 1$
MEASURED	the object: a loop of 54 iterations on a counter [CryptoLine: `lemmas/fpr_cfndsa/sqrt/lem_sqrt.cl`]

(L1) $N_{\mathrm{it}} = 54$
[[CryptoLine: `lemmas/fpr_cfndsa/sqrt/lem_sqrt_path.cl`], `lem_sqrt_path.cl`: the counter's 54 branches asserted]

(L2) $\forall j < 53 :\ 2^{53}X' - q_j^2 = xu_j r_j$
[[CryptoLine: `lemmas/fpr_cfndsa/sqrt/lem_sqrtbody.cl`], `lem_sqrtbody.cl`: the body as a contract carrying the invariant]

(L3) $2(N - Q_W^2) = X_W$
[[CryptoLine: `lemmas/fpr_cfndsa/sqrt/lem_sqrt.cl`], `lem_sqrt.cl`: (L2) at iterations 0 to 52 of (L1), the last inline]

(L4) $X_W \in [0, 4Q_W]$
[[CryptoLine: `lemmas/fpr_cfndsa/sqrt/lem_sqrt.cl`], `lem_sqrt.cl`]

(L5) $N \in [2^{106}, 2^{108})$
[$X \in [2^{52}, 2^{53})$ ($e_x \geq 1$, assumption A1); $p \in \{0, 1\}$; X', N (the block)]

(L6) $Q_W^2 \leq N$
[$X_W \geq 0$ ((L3), (L4))]

(L7) $N \le Q_W^2 + 2Q_W$

[$X_W \le 4Q_W$ ((L3), (L4))]

(L8) $Q_W^2 + 2Q_W < (Q_W + 1)^2$

[$(Q_W + 1)^2 = Q_W^2 + 2Q_W + 1$]

(L9) $Q_W = \lfloor \sqrt{N} \rfloor$

[(L6), (L7), (L8)]

(L10) $Q_W \in [2^{53}, 2^{54})$

[(L5), (L9)]

(L11) $Q \in [2^{52}, 2^{53})$

[(L10); Q (the block)]

(L12) $W \equiv (f-1)2^{52} + Q + b \pmod{2^{64}}$

[[CryptoLine: `lemmas/fpr_cfndsa/sqrt/lem_sqrt.cl`], `lem_sqrt.cl`, at (L10)'s binade; b, f (the block)]

(L13) $f \in [511, 1534]$

[$e_x \in [1, 2046]$ (assumption A1; Definition J.5); f (the block)]

(L14) $(f-1)2^{52} + Q + b < 2^{64}$

[(L11), (L13); b (the block)]

(L15) $W = (f-1)2^{52} + Q + b$

[(L12), (L14); $W \in \{0, \ldots, 2^{64} - 1\}$ (Definition J.5)]

(L16) $\rho \in \{0, 1\}$

[Q, ρ (the block)]

(L17) $t - Q = (\rho + (\sqrt{N} - Q_W))/2$

[t, ρ (the block)]

(L18) $\sqrt{N} - Q_W \in [0, 1)$

[(L9)]

(L19) $t \in [Q, Q + 1)$

[(L16), (L17), (L18)]

(L20) $\rho = 0 \Rightarrow\ t - Q < 1/2$

[(L17), (L18)]

(L21) $\rho = 1 \Rightarrow\ t - Q \ge 1/2$

[(L17), (L18)]

(L22) $\sqrt{N} = Q_W \iff N = Q_W^2$

[$Q_W \ge 0$]

(L23) $\rho = 1 \Rightarrow\ (t - Q = 1/2 \iff X_W = 0)$

[(L3), (L17), (L22)]

(L24) $\forall q \in \mathbb{Z} :\ |Q + b - t| \le |q - t|$

[(L19), (L20), (L21), (L23); b (the block)]

(L25) $\forall q \in \mathbb{Z},\ q \ne Q + b,\ |q - t| = |Q + b - t| :\ Q + b \equiv 0 \pmod{2}$

[(L19), (L20), (L21), (L23); b (the block)]

(L26) $e_x - 1075 = 2(f - 1049) + p$

[f, p (the block)]

(L27) $2^p = 1 + p$

[$p \in \{0, 1\}$]

(L28) $x = X 2^{e_x - 1075}$

[Definition J.5; $x_s = 0$ (assumption A2)]

(L29) $\sqrt{x} = t 2^{f - 1075}$

[(L26), (L27), (L28); X', N, t (the block)]

(L30) $\mathrm{val}(W) = \mathrm{fl}(\sqrt{x})$

[Lemma J.10, items 1 and 2, at $s = 0$, f, Q, b, t; (L11), (L13), (L15), (L19), (L24), (L25), (L29); fl (Definition J.1)]

(L31) $\Rightarrow$ item 1

[(L30)]

(L32) $\forall w \in \mathcal{F},\ w \neq \mathrm{val}(W),\ |w - \sqrt{x}| = |\mathrm{val}(W) - \sqrt{x}| :\ W \equiv 0 \pmod 2$

[Lemma J.10, item 3, at the same values; (L11), (L13), (L15), (L19), (L24), (L25), (L29)]

(L33) $\Rightarrow$ item 2

[(L32)]

(L34) $\mathrm{fl}(\sqrt{x})\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ \sqrt{x}$

[Lemma J.10, item 4, at the same values; (L29), (L30)]

(L35) $\Rightarrow$ item 3

[(L34)]

□ (items 1 to 3)

Lemma J.15 (The rounding model of addition and multiplication [to table])**.** *The word the code returns for a sum or a product holds its rounding to the nearest element of $\mathcal{F}$, within a relative 2^{-53} of it. Define:*

- *$\mathcal{F}$, fl, $u = 2^{-53}$ and $\zeta = 0$, those of Definition J.1.*

Let:

- *$\circ \in \{+, \times\}$;*
- *$x, y \in \mathcal{F}$.*

Define:

- val, *that of Definition J.5;*
- *W_x and W_y, the binary64 words that store x and y (Definition J.1);*
- *$e_x = e_{W_x}$, the exponent field of W_x (Definition J.5);*
- *$e_y = e_{W_y}$, the exponent field of W_y;*
- *W, the word the Cortex-M4 `-O2` object of `fpr_add` at $\circ = +$, of `fpr_mul` at $\circ = \times$, returns on (W_x, W_y).*

Assume:

(A1) $e_x, e_y \geq 1$;

(A2) $2^{-1022} \leq |x \circ y| < 2^{1023}$;

(A3) $\circ = \times$ *or* $|e_x - e_y| \leq 63$.

Then

1. $\mathrm{val}(W) = \mathrm{fl}(x \circ y)$;
2. $\mathrm{fl}(x \circ y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x \circ y)$.

Proof. (L1) $\mathrm{val}(W) = \mathrm{fl}(xy)$

[at $\circ = \times$: Lemma J.11, item 1; its assumptions by assumptions A1, A2]

(L2) $\mathrm{val}(W) = \mathrm{fl}(x + y)$

[at $\circ = +$: Lemma J.12, item 1; $|e_x - e_y| \leq 63$ (assumption A3); its assumptions by assumptions A1, A2]

(L3) $\mathrm{val}(W) = \mathrm{fl}(x \circ y)$

[(L1), (L2)]

(L4) $\Rightarrow$ item 1

[(L3)]

(L5) $\mathrm{fl}(xy)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ xy$

[at $\circ = \times$: Lemma J.11, item 3; its assumptions by assumptions A1, A2]

(L6) $\mathrm{fl}(x + y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x + y)$

[at $\circ = +$: Lemma J.12, item 3; $|e_x - e_y| \leq 63$ (assumption A3); its assumptions by assumptions A1, A2]

(L7) $\mathrm{fl}(x \circ y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x \circ y)$

[(L5), (L6)]

(L8) $\Rightarrow$ item 2

[(L7)]

□ (items 1 and 2)

Lemma J.16 (The edge cases of addition [to table])**.** *At a zero operand and at a cancelling pair, the words of the product and the sum hold the exact result; at operands more than* 63 *binades apart, the word of the sum holds the larger operand, within a relative* 2^{-62} *of the sum. Define:*

- $\mathcal{F}$, fl, $u = 2^{-53}$ *and* $\zeta = 0$, *those of Definition J.1.*

Let:

- $x, y \in \mathcal{F}$.

Define:

- val, *that of Definition J.5;*
- W_x *and* W_y, *the binary64 words that store* x *and* y *(Definition J.1);*
- $(x_s, e_x) = (s_{W_x}, e_{W_x})$, *the sign and exponent fields of* W_x *(Definition J.5);*
- $(y_s, e_y) = (s_{W_y}, e_{W_y})$, *those of* W_y;
- $W_\times$, *the word the Cortex-M4* `-O2` *object of* `fpr_mul` *returns on* (W_x, W_y);
- W_+, *the word the Cortex-M4* `-O2` *object of* `fpr_add` *returns on* (W_x, W_y).

Then

1. *Assume:*

   (A1) $W_x \in \{0, 2^{63}\}$ *or* $W_y \in \{0, 2^{63}\}$.

   Then $\mathrm{val}(W_\times) = xy$.

2. *Assume:*

   (A2) $W_x \in \{0, 2^{63}\}$ *or* $W_y \in \{0, 2^{63}\}$.

   Then $\mathrm{val}(W_+) = x + y$.

3. *Assume:*

   (A3) $e_x \geq 1$;
   (A4) $y = -x$.

   Then $\mathrm{val}(W_+) = x + y$.

4. *Assume:*

   (A5) $e_x, e_y \geq 1$;
   (A6) $e_x - e_y > 63$.

   Then $\mathrm{val}(W_+) = x$.

5. *Assume:*

   (A7) $e_x, e_y \geq 1$;
   (A8) $e_x - e_y > 63$.

   Then $x \mathrel{\mathcal{I}} \left((2^{-62})^{\pm}, 0\right) (x + y)$.

Proof. (L1) $W_x \in \{0, 2^{63}\} \Rightarrow\ x = 0$
[Definition J.5]

(L2) $W_y \in \{0, 2^{63}\} \Rightarrow\ y = 0$
[Definition J.5]

(L3) $W_\times = ((x_s + y_s) \bmod 2)2^{63}$
[Lemma J.11, item 4; assumption A1]

(L4) $\mathrm{val}(W_\times) = 0$
[(L3); Definition J.5]

(L5) $\mathrm{val}(W_\times) = xy$
[(L1), (L2), (L4); assumption A1]

(L6) $\Rightarrow$ item 1

[(L5)]

(L7) $W_x \in \{0, 2^{63}\} \wedge W_y \notin \{0, 2^{63}\} \Rightarrow\ W_+ = W_y$

[Lemma J.12, item 7]

(L8) $W_y \in \{0, 2^{63}\} \wedge W_x \notin \{0, 2^{63}\} \Rightarrow\ W_+ = W_x$

[Lemma J.12, item 8]

(L9) $W_x, W_y \in \{0, 2^{63}\} \Rightarrow\ W_+ \in \{0, 2^{63}\}$

[Lemma J.12, item 9]

(L10) $\mathrm{val}(W_+) = x + y$

[(L1), (L2), (L7), (L8), (L9); Definition J.5; assumption A2]

(L11) $\Rightarrow$ item 2

[(L10)]

(L12) $W_+ = 0$

[Lemma J.12, item 6; assumptions A3, A4]

(L13) $\mathrm{val}(W_+) = x + y$

[(L12); Definition J.5; $y = -x$ (assumption A4)]

(L14) $\Rightarrow$ item 3

[(L13)]

(L15) $W_+ = W_x$

[Lemma J.12, item 4; assumptions A5, A6]

(L16) $\mathrm{val}(W_+) = x$

[(L15); Definition J.5]

(L17) $\Rightarrow$ item 4

[(L16)]

(L18) $|y| < 2^{53} 2^{e_y - 1075}$

[Definition J.5; $e_y \geq 1$ (assumption A7)]

(L19) $|x| \geq 2^{52} 2^{e_x - 1075}$

[Definition J.5; $e_x \geq 1$ (assumption A7)]

(L20) $|y| < 2^{-63}|x|$

[(L18), (L19); $e_x - e_y \geq 64$ (assumption A8)]

(L21) $|x + y| \geq (1 - 2^{-63})|x|$

[(L20); $|x + y| \geq |x| - |y|$ (Fact A.41, item 1)]

(L22) $x - (x + y) = -y$

[expand]

(L23) $|x - (x + y)| < 2^{-63}|x|$

[(L20), (L22)]

(L24) $2^{-63}|x| \leq \frac{2^{-63}}{1-2^{-63}}|x + y|$

[(L21)]

(L25) $\frac{2^{-63}}{1-2^{-63}} \leq 2^{-62}$

[$1 - 2^{-63} \geq 1/2$]

(L26) $|x - (x + y)| \leq 2^{-62}|x + y|$

[(L23), (L24), (L25)]

(L27) $x + y \neq 0$

[(L19), (L21)]

(L28) $\exists\, u_\circ \in \mathbb{R},\ |u_\circ| \leq 2^{-62} :\ x = (x + y)(1 + u_\circ)$

[(L26), (L27); $u_\circ := (x - (x + y))/(x + y)$]

(L29) $\Rightarrow$ item 5

[(L28); Definition A.10]

□ (items 1 to 5)

Lemma J.17 (The rounding model of subtraction [to table])**.** *The word the code returns for a difference holds its rounding to the nearest element of $\mathcal{F}$, within a relative 2^{-53} of it. Define:*

- *$\mathcal{F}$,* fl*, $u = 2^{-53}$ and $\zeta = 0$, those of Definition J.1.*

Let:

- *$x, y \in \mathcal{F}$.*

Define:

- val*, that of Definition J.5;*
- *W_x and W_y, the binary64 words that store x and y (Definition J.1);*
- *$e_x = e_{W_x}$, the exponent field of W_x (Definition J.5);*
- *$e_y = e_{W_y}$, the exponent field of W_y;*
- *W_-, the word `fpr_sub` returns on (W_x, W_y).*

Assume:

(A1) $e_x, e_y \geq 1$;

(A2) $2^{-1022} \leq |x - y| < 2^{1023}$;

(A3) $|e_x - e_y| \leq 63$.

Then

1. $\mathrm{val}(W_-) = \mathrm{fl}(x - y)$;
2. $\mathrm{fl}(x - y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x - y)$.

Proof.

DEFINES $W'_y = (W_y + 2^{63}) \bmod 2^{64}$

(L1) W_- = the word of `fpr_add` on (W_x, W'_y)
[`fpr_sub`'s code [L0: `sign_inner.h:194-199`]]

(L2) $(s_{W'_y}, e_{W'_y}, m_{W'_y}) = (1 - s_{W_y}, e_y, m_{W_y})$
[W'_y (the block); Definition J.5]

(L3) $\mathrm{val}(W'_y) = -y$
[(L2); Definition J.5]

(L4) $\mathrm{val}(W_-) = \mathrm{fl}(x - y)$
[Lemma J.12, item 1, at $(x, -y)$; (L1), (L2), (L3); assumptions A1, A2, A3]

(L5) $\Rightarrow$ item 1
[(L4)]

(L6) $\mathrm{fl}(x - y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x - y)$
[Lemma J.12, item 3, at $(x, -y)$; (L1), (L2), (L3); its assumptions by assumptions A1, A2, A3]

(L7) $\Rightarrow$ item 2
[(L6)]

□ (items 1 and 2)

Lemma J.18 (The rounding model of division [to table])**.** *The word the code returns for a quotient holds its rounding to the nearest element of $\mathcal{F}$, within a relative 2^{-53} of it. Define:*

- *$\mathcal{F}$,* fl*, $u = 2^{-53}$ and $\zeta = 0$, those of Definition J.1.*

Let:

- *$x, y \in \mathcal{F}$.*

Define:

- val*, that of Definition J.5;*
- *W_x and W_y, the binary64 words that store x and y (Definition J.1);*
- *$e_x = e_{W_x}$, the exponent field of W_x (Definition J.5);*
- *$e_y = e_{W_y}$, the exponent field of W_y;*
- *W, the word the Cortex-M4 `-O2` object of `fpr_div` returns on (W_x, W_y).*

Assume:

(A1) $e_x, e_y \geq 1$;
(A2) $2^{-1022} \leq |x/y| < 2^{1023}$.
Then

1. $\mathrm{val}(W) = \mathrm{fl}(x/y)$;
2. $\mathrm{fl}(x/y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x/y)$.

Proof. (L1) $\mathrm{val}(W) = \mathrm{fl}(x/y)$
[Lemma J.13, item 1; its assumptions by assumptions A1, A2]
(L2) $\Rightarrow$ item 1
[(L1)]
(L3) $\mathrm{fl}(x/y)\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ (x/y)$
[Lemma J.13, item 3; its assumptions by assumptions A1, A2]
(L4) $\Rightarrow$ item 2
[(L3)]
□ (items 1 and 2)

Lemma J.19 (The rounding model of the square root [to table])**.** *The word the code returns for a square root holds its rounding to the nearest element of* $\mathcal{F}$*, within a relative* 2^{-53} *of it. Define:*

- $\mathcal{F}$, fl, $u = 2^{-53}$ *and* $\zeta = 0$, *those of Definition J.1.*

Let:

- $x \in \mathcal{F}$.

Define:

- val, *that of Definition J.5;*
- W_x, *the binary64 word that stores* x *(Definition J.1);*
- $(x_s, e_x) = (s_{W_x}, e_{W_x})$, *its sign and exponent fields (Definition J.5);*
- W, *the word the Cortex-M4* `-O2` *object of* `fpr_sqrt` *returns on* W_x.

Assume:
(A1) $e_x \geq 1$;
(A2) $x_s = 0$.
Then

1. $\mathrm{val}(W) = \mathrm{fl}(\sqrt{x})$;
2. $\mathrm{fl}(\sqrt{x})\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ \sqrt{x}$.

Proof. (L1) $\mathrm{val}(W) = \mathrm{fl}(\sqrt{x})$
[Lemma J.14, item 1; its assumptions by assumptions A1, A2]
(L2) $\Rightarrow$ item 1
[(L1)]
(L3) $\mathrm{fl}(\sqrt{x})\ \mathcal{I}\ ((2^{-53})^{\pm}, 0)\ \sqrt{x}$
[Lemma J.14, item 3; its assumptions by assumptions A1, A2]
(L4) $\Rightarrow$ item 2
[(L3)]
□ (items 1 and 2)

Lemma J.20 (The objects of the scalings [to table])**.** *The Cortex-M4 objects of the four scalings add a multiple of* 2^{52} *to the word or subtract it, and return a zero word unchanged. Let:*

- $W \in \{0, \ldots, 2^{64} - 1\}$;
- $k \in \{0, \ldots, 2^{11} - 1\}$.

Define:

- z_{half}, *the word the Cortex-M4* `arm-none-eabi-gcc -O2` *object of a wrapper of* `fpr_half` *returns on* W*;*
- z_{double}, *the word that object of* `fpr_double` *returns on* W*;*
- z_{div2e}, *the word that object of* `fpr_div2e` *returns on* (W, k)*;*
- z_{mul2e}, *the word that object of* `fpr_mul2e` *returns on* (W, k)*;*
- s_W, e_W *and* m_W, *its fields (Definition J.5).*

Then

1. *Assume:*

   (A1) $e_W \geq 1$.

   Then $z_{\text{half}} = W - 2^{52}$. *[CryptoLine:* `lemmas/fpr_cfndsa/inline/lem_half.cl`*]*

2. *Assume:*

   (A2) $e_W \geq 1$.

   Then $z_{\text{double}} = (W + 2^{52}) \bmod 2^{64}$. *[CryptoLine:* `lemmas/fpr_cfndsa/inline/lem_double.cl`*]*

3. *Assume:*

   (A3) $k < e_W$.

   Then $z_{\text{div2e}} = W - k2^{52}$. *[CryptoLine:* `lemmas/fpr_cfndsa/inline/lem_div2e.cl`*]*

4. *Assume:*

   (A4) $e_W \geq 1$;
   (A5) $e_W + k < 2047$.

   Then $z_{\text{mul2e}} = W + k2^{52}$. *[CryptoLine:* `lemmas/fpr_cfndsa/inline/lem_mul2e.cl`*]*

5. *Assume:*

   (A6) $e_W = 0$;
   (A7) $m_W = 0$.

   Then $z_{\text{half}}, z_{\text{double}}, z_{\text{div2e}}, z_{\text{mul2e}} = W$. *[CryptoLine:* `lemmas/fpr_cfndsa/inline/lem_half_zero.cl`*], [CryptoLine:* `lemmas/fpr_cfndsa/inline/lem_double_zero.cl`*], [CryptoLine:* `lemmas/fpr_cfndsa/inline/lem_div2e_zero.cl`*], [CryptoLine:* `lemmas/fpr_cfndsa/inline/lem_mul2e_zero.cl`*]*

Proof. (L1) $z_{\text{half}} \equiv W - 2^{52} \pmod{2^{64}}$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_half.cl`]; $e_W \geq 1$ (assumption A1)]

(L2) $W \geq e_W 2^{52}$
[$e_W \leq \lfloor W/2^{52} \rfloor$ (Definition J.5)]

(L3) $z_{\text{half}} = W - 2^{52}$
[(L1), (L2); $e_W \geq 1$ (assumption A1); $z_{\text{half}} \in \{0, \ldots, 2^{64} - 1\}$]

(L4) $\Rightarrow$ item 1
[(L3)]

(L5) $z_{\text{double}} \equiv W + 2^{52} \pmod{2^{64}}$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_double.cl`]; $e_W \geq 1$ (assumption A2)]

(L6) $z_{\text{double}} = (W + 2^{52}) \bmod 2^{64}$
[(L5); $z_{\text{double}} \in \{0, \ldots, 2^{64} - 1\}$]

(L7) $\Rightarrow$ item 2
[(L6)]

(L8) $z_{\text{div2e}} \equiv W - k2^{52} \pmod{2^{64}}$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_div2e.cl`]; $k < e_W$ (assumption A3)]

(L9) $z_{\text{div2e}} = W - k2^{52}$
[(L2), (L8); $k < e_W$ (assumption A3); $z_{\text{div2e}} \in \{0, \ldots, 2^{64} - 1\}$]

(L10) $\Rightarrow$ item 3

[(L9)]

(L11) $z_{\text{mul2e}} \equiv W + k2^{52} \pmod{2^{64}}$

[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_mul2e.cl`]; assumption A4]

(L12) $W < s_W 2^{63} + (e_W + 1)2^{52}$

[Definition J.5]

(L13) $W + k2^{52} < 2^{64}$

[(L12); $e_W + k < 2047$ (assumption A5)]

(L14) $z_{\text{mul2e}} = W + k2^{52}$

[(L11), (L13); $z_{\text{mul2e}} \in \{0, \ldots, 2^{64} - 1\}$]

(L15) $\Rightarrow$ item 4

[(L14)]

(L16) $z_{\text{half}}, z_{\text{double}}, z_{\text{div2e}}, z_{\text{mul2e}} = W$

[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_half_zero.cl`], [CryptoLine: `lemmas/fpr_cfndsa/inline/lem_double_zero.cl`], [CryptoLine: `lemmas/fpr_cfndsa/inline/lem_div2e_zero.cl`], [CryptoLine: `lemmas/fpr_cfndsa/inline/lem_mul2e_zero.cl`], the four `lem_*_zero.cl`; assumptions A6, A7]

(L17) $\Rightarrow$ item 5

[(L16)]

$\square$ (items 1 to 5)

Lemma J.21 (The objects of the integer roundings [to table]). *The Cortex-M4 objects of* `fpr_trunc`, `fpr_floor` *and* `fpr_rint` *return, modulo* 2^{64}*, the significand shifted to the integer point, its ceiling for a negative* `fpr_floor`*, and its round bit added for* `fpr_rint`*. Let:*

- $W \in \{0, \ldots, 2^{64} - 1\}$.

Define:

- z_{trunc}, z_{floor} *and* z_{rint}*, the words the Cortex-M4* `arm-none-eabi-gcc -O2` *objects of a wrapper of* `fpr_trunc`, `fpr_floor` *and* `fpr_rint` *return on* W*;*
- s_W, e_W *and* m_W*, its fields (Definition J.5);*
- $\hat{m}_W = (2^{52} + m_W)2^{10}$*;*
- $\text{sh}_W = 63$ *at* $e_W \leq 1021$*, and* $\text{sh}_W = 1085 - e_W$ *at* $e_W \geq 1022$*;*
- $q_W = \lfloor \hat{m}_W / 2^{\text{sh}_W} \rfloor$*;*
- $r_W = \hat{m}_W - q_W 2^{\text{sh}_W}$*;*
- $b_W = [2r_W > 2^{\text{sh}_W}] + [2r_W = 2^{\text{sh}_W}]\,[q_W \equiv 1 \pmod 2]$.

Assume:

(A1) $e_W \leq 1085$.

Then

1. $z_{\text{trunc}} = (1 - 2s_W)q_W \bmod 2^{64}$. *[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_trunc.cl`]*
2. *Assume:*

   (A2) $s_W = 0$.

   Then $z_{\text{floor}} = q_W$. *[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_floor.cl`]*
3. *Assume:*

   (A3) $s_W = 1$.

   Then $z_{\text{floor}} = -\lceil \hat{m}_W / 2^{\text{sh}_W} \rceil \bmod 2^{64}$. *[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_floor.cl`]*
4. *Assume:*

   (A4) $e_W \leq 1021$.

Then $z_{\text{rint}} = 0$. *[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_rint.cl`]*

5. *Assume:*

   (A5) $e_W \geq 1022$.

   Then $z_{\text{rint}} = (1 - 2s_W)(q_W + b_W) \bmod 2^{64}$. *[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_rint.cl`]*

Proof. (L1) $\hat{m}_W \gg \text{sh}_W = q_W$
[q_W (the statement); $a \gg s = \lfloor a/2^s \rfloor$ (Definition A.5)]

(L2) $z_{\text{trunc}} \equiv (1 - 2s_W)(\hat{m}_W \gg \text{sh}_W) \pmod{2^{64}}$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_trunc.cl`], the object's word at $s_W = 0$ and at $s_W = 1$; assumption A1]

(L3) $z_{\text{trunc}} = (1 - 2s_W)q_W \bmod 2^{64}$
[(L1), (L2); $z_{\text{trunc}} \in \{0, \ldots, 2^{64} - 1\}$]

(L4) $\Rightarrow$ item 1
[(L3)]

(L5) $z_{\text{floor}} \equiv \hat{m}_W \gg \text{sh}_W \pmod{2^{64}}$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_floor.cl`]; $s_W = 0$ (assumption A2)]

(L6) $\hat{m}_W < 2^{63}$
[$\hat{m}_W$ (the statement); $m_W < 2^{52}$ (m_W a field of Definition J.5)]

(L7) $z_{\text{floor}} = q_W$
[(L1), (L5), (L6); $z_{\text{floor}} \in \{0, \ldots, 2^{64} - 1\}$]

(L8) $\Rightarrow$ item 2
[(L7)]

(L9) $z_{\text{floor}} \equiv -((\hat{m}_W + 2^{\text{sh}_W} - 1) \gg \text{sh}_W) \pmod{2^{64}}$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_floor.cl`]; $s_W = 1$ (assumption A3)]

(L10) $\hat{m}_W + 2^{\text{sh}_W} - 1 < 2^{64}$
[(L6); $\text{sh}_W \leq 63$ (sh_W, the statement)]

(L11) $\forall a' \in \mathbb{Z}\ \forall d \geq 1 :\ \lfloor (a' + d - 1)/d \rfloor = \lceil a'/d \rceil$
[Fact A.41, item 22, at $a := a'$]

(L12) $(\hat{m}_W + 2^{\text{sh}_W} - 1) \gg \text{sh}_W = \lceil \hat{m}_W / 2^{\text{sh}_W} \rceil$
[(L10); (L11) at $(a', d) = (\hat{m}_W, 2^{\text{sh}_W})$; $a \gg s = \lfloor a/2^s \rfloor$ (Definition A.5)]

(L13) $z_{\text{floor}} = -\lceil \hat{m}_W / 2^{\text{sh}_W} \rceil \bmod 2^{64}$
[(L9), (L12); $z_{\text{floor}} \in \{0, \ldots, 2^{64} - 1\}$]

(L14) $\Rightarrow$ item 3
[(L13)]

(L15) $z_{\text{rint}} = 0$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_rint.cl`]; $e_W \leq 1021$ (assumption A4)]

(L16) $\Rightarrow$ item 4
[(L15)]

(L17) $z_{\text{rint}} \equiv (1 - 2s_W)((\hat{m}_W \gg \text{sh}_W) + b_W) \pmod{2^{64}}$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_rint.cl`], b_W its round bit; $e_W \geq 1022$ (assumption A5)]

(L18) $z_{\text{rint}} = (1 - 2s_W)(q_W + b_W) \bmod 2^{64}$
[(L1), (L17); $z_{\text{rint}} \in \{0, \ldots, 2^{64} - 1\}$]

(L19) $\Rightarrow$ item 5
[(L18)]

□ (items 1 to 5)

Lemma J.22 (The object of `fpr_scaled` at scale 0 [to table])**.** *The Cortex-M4 object of* `fpr_scaled` *at the scale* 0 *returns, for an integer below* 2^{53} *in modulus, the zero word at zero, and otherwise the word with the integer's sign and its modulus shifted to the top of the significand. Let:*

- $i \in \mathbb{Z}$.

Define:

- W, *the word* `fpr_scaled` *returns at* $(i \bmod 2^{64}, 0)$ *on the Cortex-M4* `arm-none-eabi-gcc -O2` *object of* `sign_fpr.c` *[L0: sign_fpr.c : 60-78];*
- s_W, e_W *and* m_W, *its fields (Definition J.5);*
- $A_W = 2^{52} + m_W$;
- $k_W = 1075 - e_W$.

Assume:

(A1) $|i| < 2^{53}$.

Then

1. *Assume:*

   (A2) $i = 0$.

   Then $W = 0$.

2. *Assume:*

   (A3) $i \neq 0$.

   Then $s_W = [i < 0]$.

3. *Assume:*

   (A4) $i \neq 0$.

   Then $e_W \in [1023, 1075]$.

4. *Assume:*

   (A5) $i \neq 0$.

   Then $\lfloor A_W / 2^{k_W} \rfloor = |i|$.

5. *Assume:*

   (A6) $i \neq 0$.

   Then $|i| 2^{k_W} \bmod 2^{64} = A_W$.

[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_scaled.cl`]

Proof.

DEFINES $X = i \bmod 2^{64}$

DEFINES $a = X$ at $X < 2^{63}$, and $a = 2^{64} - X$ at $X \geq 2^{63}$

(L1) $i \geq 0 \Rightarrow\ X = i$

[X (the block); $|i| < 2^{53}$ (assumption A1)]

(L2) $i < 0 \Rightarrow\ X = 2^{64} + i$

[X (the block); $|i| < 2^{53}$ (assumption A1)]

(L3) $X < 2^{63} \iff i \geq 0$

[(L1), (L2); $|i| < 2^{53}$ (assumption A1)]

(L4) $a = |i|$

[(L1), (L2), (L3); a (the block)]

(L5) $W = 0$

[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_scaled.cl`] at $sc = 0$; $X = 0$ by (L1) at $i = 0$ (assumption A2)]

(L6) $\Rightarrow$ item 1

[(L5)]

(L7) $s_W = [X \geq 2^{63}]$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_scaled.cl`] at $sc = 0$; $X \neq 0$ ($i \neq 0$, assumptions A3, A4, A5, A6)]

(L8) $s_W = [i < 0]$
[(L3), (L7)]

(L9) $\Rightarrow$ item 2
[(L8)]

(L10) $e_W \in [1023, 1075]$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_scaled.cl`] at $sc = 0$; $X \neq 0$ ($i \neq 0$, assumption A4; (L1), (L2))]

(L11) $\Rightarrow$ item 3
[(L10)]

(L12) $\lfloor A_W / 2^{k_W} \rfloor = a$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_scaled.cl`] at $sc = 0$, its right shift; $X \neq 0$ ($i \neq 0$, assumption A5; (L1), (L2))]

(L13) $a 2^{k_W} \bmod 2^{64} = A_W$
[[CryptoLine: `lemmas/fpr_cfndsa/inline/lem_scaled.cl`] at $sc = 0$, its left shift; $X \neq 0$ ($i \neq 0$, assumption A6; (L1), (L2))]

(L14) $\lfloor A_W / 2^{k_W} \rfloor = |i|$
[(L4), (L12)]

(L15) $\Rightarrow$ item 4
[(L14)]

(L16) $|i| 2^{k_W} \bmod 2^{64} = A_W$
[(L4), (L13)]

(L17) $\Rightarrow$ item 5
[(L16)]

□ (items 1 to 5)

Lemma J.23 (Exactness of the scalings [to table]). *Within the exponent range, the four scalings return the word of the value times a power of two, with no rounding. Let:*

- $W \in \{0, \ldots, 2^{64} - 1\}$;
- $k \in \{0, \ldots, 2^{11} - 1\}$.

Define:

- s_W, e_W, m_W *and* val, *those of Definition J.5;*
- z_{half}, z_{double}, z_{div2e} *and* z_{mul2e}, *those of Lemma J.20, the words the code returns [LO: `sign_inner.h: 247-319`].*

Then

1. *Assume:*
   (A1) $e_W \in [2, 2046]$.
   Then $\text{val}(z_{\text{half}}) = \text{val}(W)/2$.
2. *Assume:*
   (A2) $e_W \in [1, 2045]$.
   Then $\text{val}(z_{\text{double}}) = 2\,\text{val}(W)$.
3. *Assume:*
   (A3) $e_W \in [k + 1, 2046]$.
   Then $\text{val}(z_{\text{div2e}}) = 2^{-k}\text{val}(W)$.

4. Assume:

(A4) $e_W \in [1, 2046 - k]$.

Then $\mathrm{val}(z_{\mathrm{mul2e}}) = 2^k \mathrm{val}(W)$.

Proof. (L1) $\forall j \in \mathbb{Z},\ 0 \le e_W + j < 2^{11} :\ (s_{W+j2^{52}}, e_{W+j2^{52}}, m_{W+j2^{52}}) = (s_W, e_W + j, m_W)$ [Definition J.5]

(L2) $\forall j \in \mathbb{Z},\ e_W \ge 1,\ 1 \le e_W + j \le 2046 :\ \mathrm{val}(W + j2^{52}) = 2^j\,\mathrm{val}(W)$ [(L1); val (Definition J.5)]

(L3) $\mathrm{val}(z_{\mathrm{half}}) = \mathrm{val}(W)/2$ [Lemma J.20, item 1; (L2) at $j = -1$; $e_W \in [2, 2046]$ (assumption A1)]

(L4) $\Rightarrow$ item 1 [(L3)]

(L5) $W + 2^{52} < 2^{64}$ [$W < s_W 2^{63} + (e_W + 1)2^{52}$ (Definition J.5); $e_W \le 2045$ (assumption A2)]

(L6) $\mathrm{val}(z_{\mathrm{double}}) = 2\,\mathrm{val}(W)$ [Lemma J.20, item 2; (L5); (L2) at $j = 1$]

(L7) $\Rightarrow$ item 2 [(L6)]

(L8) $\mathrm{val}(z_{\mathrm{div2e}}) = 2^{-k}\mathrm{val}(W)$ [Lemma J.20, item 3; (L2) at $j = -k$; assumption A3]

(L9) $\Rightarrow$ item 3 [(L8)]

(L10) $\mathrm{val}(z_{\mathrm{mul2e}}) = 2^k \mathrm{val}(W)$ [Lemma J.20, item 4; (L2) at $j = k$; assumption A4]

(L11) $\Rightarrow$ item 4 [(L10)]

□ (items 1 to 4)

Lemma J.24 (Exact conversion of small integers [to table])**.** *The code converts an integer below* 2^{53} *in modulus to its own value. Let:*

- $i \in \mathbb{Z}$.

Define:

- $\texttt{fpr_of}(i) = \texttt{fpr_scaled}(i \bmod 2^{64}, 0)$*, the word the code returns [L0: sign_inner.h: 105-114];*
- $\mathcal{F}$*,* $u = 2^{-53}$ *and* $\zeta = 0$*, those of Definition J.1;*
- val*, that of Definition J.5;*
- $\mathrm{fl}(i) = \mathrm{val}(\texttt{fpr_of}(i))$*;*
- $W = \texttt{fpr_of}(i)$*;*
- s_W *and* e_W*, those of Definition J.5 at* W*;*
- A_W *and* k_W*, those of Lemma J.22.*

Assume:

(A1) $|i| < 2^{53}$.

Then

$$\mathrm{fl}(i) = i.$$

Proof.

DEFINES $W = \texttt{fpr_of}(i)$

DEFINES s_W, e_W, A_W, k_W: those of Lemma J.22 at i

(L1) $W = 0$ [at $i = 0$: Lemma J.22, item 1; its assumptions by assumption A1]

(L2) $\mathrm{val}(W) = 0$

[at $i = 0$: (L1); Definition J.5]

(L3) $|i|2^{k_W} \le A_W$

[at $i \neq 0$: Lemma J.22, item 4; its assumptions by assumption A1]

(L4) $A_W < 2^{64}$

[A_W (Lemma J.22); $m_W < 2^{52}$ (Definition J.5)]

(L5) $A_W = |i|2^{k_W}$

[at $i \neq 0$: Lemma J.22, item 5; (L3), (L4); its assumptions by assumption A1]

(L6) $\mathrm{val}(W) = (1 - 2s_W)A_W 2^{e_W - 1075}$

[at $i \neq 0$: Definition J.5; $e_W \ge 1023$ (Lemma J.22, item 3)]

(L7) $(1 - 2s_W)A_W 2^{e_W - 1075} = (1 - 2s_W)|i|$

[(L5); $k_W = 1075 - e_W$ (Lemma J.22)]

(L8) $(1 - 2s_W)|i| = i$

[Lemma J.22, item 2; its assumptions by assumption A1]

(L9) $\mathrm{fl}(i) = i$

[(L2), (L6), (L7), (L8); fl(i) (the statement)]

(L10) $\Rightarrow$ the statement

[(L9)]

□

Lemma J.25 (Exactness of the integer roundings [to table])**.** *Within the exponent range of the integer roundings,* `fpr_trunc`*,* `fpr_floor` *and* `fpr_rint` *return the truncation, the floor and the nearest integer, even at a tie, of the word's value. Let:*

- $W \in \{0, \ldots, 2^{64} - 1\}$.

Define:

- s_W, e_W *and* val*, those of Definition J.5;*
- $\hat{m}_W$, sh_W, q_W, r_W, b_W, z_{trunc}, z_{floor} *and* z_{rint}*, those of Lemma J.21;*
- t_{trunc}, t_{floor} *and* t_{rint}*, the integers in* $[-2^{63}, 2^{63})$ *congruent to* z_{trunc}, z_{floor} *and* z_{rint} *modulo* 2^{64}*, the signed words the code returns* `[L0: sign_inner.h: 116-189]`*.*

Assume:

(A1) $1 \le e_W \le 1085$.

Then

1. $t_{\mathrm{trunc}} = (1 - 2s_W)\lfloor|\mathrm{val}(W)|\rfloor$;
2. $t_{\mathrm{floor}} = \lfloor \mathrm{val}(W) \rfloor$;
3. $\forall k \in \mathbb{Z} : \ |t_{\mathrm{rint}} - \mathrm{val}(W)| \le |k - \mathrm{val}(W)|$;
4. $\forall k \in \mathbb{Z},\ k \neq t_{\mathrm{rint}},\ |k - \mathrm{val}(W)| = |t_{\mathrm{rint}} - \mathrm{val}(W)| : \ t_{\mathrm{rint}} \equiv 0 \pmod 2$.

Proof. (L1) $|\mathrm{val}(W)| = \hat{m}_W / 2^{1085 - e_W}$

[Definition J.5 at $e_W \ge 1$ (assumption A1); $\hat{m}_W$ (Lemma J.21)]

(L2) $\mathrm{val}(W) = (1 - 2s_W)|\mathrm{val}(W)|$

[Definition J.5]

(L3) $\hat{m}_W < 2^{63}$

[$\hat{m}_W$ (Lemma J.21); $m_W < 2^{52}$ (m_W a field of Definition J.5)]

(L4) $q_W < 2^{62}$

[at $\mathrm{sh}_W \ge 1$: (L3); q_W (Lemma J.21)]

(L5) $b_W = 0$

[at $\mathrm{sh}_W = 0$: $r_W = 0$ and b_W (Lemma J.21)]

(L6) $q_W + b_W < 2^{63}$

[(L3), (L4), (L5); q_W at $\mathrm{sh}_W = 0$ (Lemma J.21)]

(L7) $|\mathrm{val}(W)| < 1/2$

[at $e_W \le 1021$: (L1), (L3)]

(L8) $\hat{m}_W / 2^{\mathrm{sh}_W} = |\mathrm{val}(W)|$

[at $e_W \ge 1022$: (L1); $\mathrm{sh}_W = 1085 - e_W$ (Lemma J.21)]

(L9) $q_W = 0$

[at $e_W \le 1021$: $\mathrm{sh}_W = 63$ (Lemma J.21); (L3)]

(L10) $\lfloor |\mathrm{val}(W)| \rfloor = 0$

[at $e_W \le 1021$: (L7)]

(L11) $q_W = \lfloor |\mathrm{val}(W)| \rfloor$

[(L8), (L9), (L10); q_W (Lemma J.21)]

(L12) $t_{\mathrm{trunc}} = (1 - 2s_W) q_W$

[Lemma J.21, item 1; (L6); t_{trunc} (the statement); its assumption by assumption A1]

(L13) $t_{\mathrm{trunc}} = (1 - 2s_W) \lfloor |\mathrm{val}(W)| \rfloor$

[(L11), (L12)]

(L14) $\Rightarrow$ item 1

[(L13)]

(L15) $\lceil \hat{m}_W / 2^{\mathrm{sh}_W} \rceil = 1$

[at $e_W \le 1021$: $\hat{m}_W \in (0, 2^{63})$ ((L3)), $\mathrm{sh}_W = 63$ (Lemma J.21)]

(L16) $\lceil |\mathrm{val}(W)| \rceil = 1$

[at $e_W \le 1021$: (L7); $\mathrm{val}(W) \neq 0$ ($e_W \ge 1$, assumption A1; Definition J.5)]

(L17) $\lceil \hat{m}_W / 2^{\mathrm{sh}_W} \rceil = \lceil |\mathrm{val}(W)| \rceil$

[(L8) at $e_W \ge 1022$; (L15), (L16) at $e_W \le 1021$]

(L18) $\forall y \in \mathbb{R} : \ -\lceil y \rceil = \lfloor -y \rfloor$

[Fact A.41, item 22]

(L19) $t_{\mathrm{floor}} = \lfloor |\mathrm{val}(W)| \rfloor$

[at $s_W = 0$: Lemma J.21, item 2; (L11); t_{floor} (the statement)]

(L20) $t_{\mathrm{floor}} = \lfloor -|\mathrm{val}(W)| \rfloor$

[at $s_W = 1$: Lemma J.21, item 3; (L3), (L17), (L18); t_{floor} (the statement)]

(L21) $t_{\mathrm{floor}} = \lfloor \mathrm{val}(W) \rfloor$

[(L2), (L19), (L20)]

(L22) $\Rightarrow$ item 2

[(L21)]

(L23) $t_{\mathrm{rint}} = 0$

[at $e_W \le 1021$: Lemma J.21, item 4]

(L24) $\forall k \in \mathbb{Z},\ k \neq 0 : \ |k - \mathrm{val}(W)| > 1/2$

[at $e_W \le 1021$: (L7)]

(L25) $t_{\mathrm{rint}} = (1 - 2s_W)(q_W + b_W)$

[at $e_W \ge 1022$: Lemma J.21, item 5; (L6); t_{rint} (the statement)]

(L26) $\forall k \in \mathbb{Z} : \ |(q_W + b_W) 2^{\mathrm{sh}_W} - \hat{m}_W| \le |k 2^{\mathrm{sh}_W} - \hat{m}_W|$

[at $e_W \ge 1022$: Lemma J.8, item 1, at $d = 2^{\mathrm{sh}_W}$, $M = \hat{m}_W$, $Q = q_W$, $R = r_W$]

(L27) $\forall k \in \mathbb{Z},\ k \neq q_W + b_W,\ |k 2^{\mathrm{sh}_W} - \hat{m}_W| = |(q_W + b_W) 2^{\mathrm{sh}_W} - \hat{m}_W| : \ q_W + b_W \equiv 0 \pmod 2$

[at $e_W \ge 1022$: Lemma J.8, item 2, at the same values]

(L28) $\forall k \in \mathbb{Z} : \ |(1 - 2s_W) k - \mathrm{val}(W)| = |k - \hat{m}_W / 2^{\mathrm{sh}_W}|$

[at $e_W \ge 1022$: (L2), (L8); $s_W \in \{0, 1\}$ (Definition J.5)]

(L29) $\forall k \in \mathbb{Z} : \ |t_{\mathrm{rint}} - \mathrm{val}(W)| \le |k - \mathrm{val}(W)|$

[(L7), (L23), (L24) at $e_W \le 1021$; (L25), (L26), (L28) at $e_W \ge 1022$]

(L30) $\Rightarrow$ item 3

[(L29)]

(L31) $\forall k \in \mathbb{Z},\ k \neq t_{\text{rint}},\ |k - \text{val}(W)| = |t_{\text{rint}} - \text{val}(W)| :\ t_{\text{rint}} \equiv 0 \pmod 2$
[(L7), (L24) at $e_W \leq 1021$, where no such k exists; (L25), (L27), (L28) at $e_W \geq 1022$]

(L32) $\Rightarrow$ item 4
[(L31)]

□ (items 1 to 4)

Lemma J.26 (Roundings of the complex operations [to table]). *The code forms each complex result of $\oplus$, $\ominus$, $\otimes$ and $c \otimes a$ with 2, 2, 6 and 2 calls of `fpr_add`, `fpr_sub` and `fpr_mul`, one rounding each. Define:*

- *$\oplus$, $\ominus$, $\otimes$ and $c \otimes a$, the complex operations of Definition A.8;*
- *$\mathcal{F}$, fl, $u = 2^{-53}$ and $\zeta = 0$, those of Definition J.1;*
- *$N_\circ$, at $\circ \in \{\oplus, \ominus, \otimes, c \otimes a\}$, the number of calls of `fpr_add`, `fpr_sub` and `fpr_mul` the code makes per complex result of $\circ$.*

Then

1. $N_\oplus = 2$;
2. $N_\ominus = 2$;
3. $N_\otimes = 6$;
4. $N_{c\otimes a} = 2$.

[gate: verify/gates/fp/complex_roundings.py]

Proof. (L1) $N_\oplus = 2$
[[gate: `verify/gates/fp/complex_roundings.py`] on the plain branch of `fpoly_add` [L0: `sign_fpoly.c:1625-2032`]]

(L2) $\Rightarrow$ item 1
[(L1)]

(L3) $N_\ominus = 2$
[[gate: `verify/gates/fp/complex_roundings.py`] on the plain branch of `fpoly_sub` [L0: `sign_fpoly.c:1625-2032`]]

(L4) $\Rightarrow$ item 2
[(L3)]

(L5) $N_\otimes = 6$
[[gate: `verify/gates/fp/complex_roundings.py`] on the body of `FPC_MUL` [L0: `sign_inner.h:327-338`]]

(L6) $\Rightarrow$ item 3
[(L5)]

(L7) $N_{c\otimes a} = 2$
[[gate: `verify/gates/fp/complex_roundings.py`] on the plain branch of `fpoly_mulconst` [L0: `sign_fpoly.c:1625-2032`]]

(L8) $\Rightarrow$ item 4
[(L7)]

□ (items 1 to 4)

Corollary J.27 (The complex product's relative bound [to table]). *At $\zeta = 0$ the absolute part of the bound on the complex product is 0, and its relative constant is the one below. Let:*

- *$\mathcal{F}$ be a realization of Definition A.4 at $\zeta = 0$.*

Define:

- *u, its relative bound (Definition A.4).*

Then

1. $\forall a, b \in C_{\mathcal{F}}:\ (a \otimes b)\ \mathcal{I}\left((\sqrt{2}\,u(2+u))^{\pm}, 0\right)\ ab.$

Proof. (L1) $k_B\zeta = 0$

[$\zeta = 0$ (the statement); k_B (Lemma B.2)]

(L2) $\forall a, b \in C_{\mathcal{F}}:\ (a \otimes b)\ \mathcal{I}\left((\sqrt{2}\,u(2+u))^{\pm}, 0\right)\ ab$

[Lemma B.2, item 3; (L1)]

(L3) $\Rightarrow$ item 1

[(L2)]

□ (item 1)

J.1.2 ffSampling$^{\mathcal{F}}$ in $\mathcal{F}$

Definition J.28 (The stored sampling constants of `c-fn-dsa` [to table])**.** The code of `c-fn-dsa` stores its sampling constants rounded once. Define:

- $\mathcal{F}$, that of Definition J.1;
- fl, that of Definition J.1;
- σ, that of SamplerZ (Algorithm 8), Require;
- $\sigma_{\min}$, that of SamplerZ, Require, and of Definition A.25 in this signer: the number of the stored word `SIGMA_MIN` of `c-fn-dsa` at $\log_2 n$ [L0: `sign_sampler.c:44-56`];
- σ_0, that of line 9 of SamplerZ.

The code stores $\widetilde{c} = \mathrm{fl}(c)$ for

- $c = 1/\sigma$ and $c = \sigma_{\min}$ at each $\log_2 n \in \{1, \ldots, 10\}$ [L0: `sign_sampler.c:31-56`];
- $c = \ln 2$ and $c = 1/\ln 2$ [L0: `sign_sampler.c:59-62`];
- $c = 1/(2\sigma_0^2)$ [L0: `sign_sampler.c:19`];
- $c = 1/q$ and $c = -1/q$ [L0: `sign_fpoly.c:2657-2658`].

Lemma J.29 (The floating-point signer's stored word `INV_SIGMA` [to table])**.** *For the floating-point signer, the stored inverse standard deviation is $1/s$ within one rounding of its realization. Let:*

- *The signer be the floating-point signer at $(u, \zeta) = (2^{-53}, 0)$ (Definition J.1).*

Define:

- `INV_SIGMA`*, the number of the signer's stored word at $\log_2 n$:* `INV_SIGMA` *of* `c-fn-dsa` *[L0: `sign_sampler.c:31-43`];*
- $c_n = 1/s$.

Measured:

- $(\texttt{INV_SIGMA} - \zeta)\ s \le 1 + u$ *for the floating-point signer at its (u, ζ), at $n = 512$ and $n = 1024$ [gate: `verify/gates/sampler/invsigma_fp.py`];*
- $(\texttt{INV_SIGMA} + \zeta)\ s \ge 1 - u$ *for the floating-point signer at its (u, ζ), at $n = 512$ and $n = 1024$ [gate: `verify/gates/sampler/invsigma_fp.py`].*

Then

$$\texttt{INV_SIGMA}\ \mathcal{I}\left(u^{\pm}, \zeta^{\pm}\right)\ c_n.$$

Proof. (L1) $s > 0$

[$s = 1.17\sqrt{q}\,\sigma_{\min}$ (Definition A.25); the stored word $\sigma_{\min} > 0$ [L0: `sign_sampler.c:44-56`]]

(L2) $\texttt{INV_SIGMA} - c_n \le uc_n + \zeta$

[the first measured row, divided by $s > 0$ ((L1)); $c_n = 1/s$ (the statement)]

(L3) $c_n - \texttt{INV_SIGMA} \le uc_n + \zeta$

[the second measured row, divided by $s > 0$ ((L1)); $c_n = 1/s$ (the statement)]

(L4) $\Rightarrow\ \exists\, u_\circ, \zeta_\circ \in \mathbb{R},\ |u_\circ| \le u,\ |\zeta_\circ| \le \zeta:\ \texttt{INV_SIGMA} = c_n(1 + u_\circ) + \zeta_\circ$

[(L2), (L3) at $u_\circ := \max(-u, \min(u, (\texttt{INV_SIGMA} - c_n)/c_n))$, $\zeta_\circ := \texttt{INV_SIGMA} - c_n(1 + u_\circ)$, $c_n > 0$ by (L1)]

(L5) $\Rightarrow$ the statement

[(L4); Definition A.10]

□

Lemma J.30 (The range of the floating-point signer's leaf standard deviations [to table])**.** *On a key the key generation accepts, every leaf standard deviation over $\mathbb{R}$ lies strictly between $\sigma_{\min}$ and $1.17^2\sigma_{\min}$, for the floating-point signer's stored constants. Let:*

- *The signer be the floating-point signer at $(u, \zeta) = (2^{-53}, 0)$ (Definition J.1).*

Define:

- `INV_SIGMA`*, the number of the signer's stored word at $\log_2 n$:* `INV_SIGMA` *of* `c-fn-dsa` *[LO: sign_sampler.c: 31-43];*
- $c_n = 1/s$*;*
- d_i*, $i \le N$, the leaf diagonals of T (Definition A.19);*
- $\sigma_i := 1/(\sqrt{d_i}\, c_n)$*, the standard deviation of the leaf i over $\mathbb{R}$: lines 1 and 3 of* deepest *(Algorithm 7) over $\mathbb{R}$, at* `INV_SIGMA` $= c_n$*.*

Measured:

- $\sqrt{16822}\,\sigma_{\min}(\texttt{INV_SIGMA}+\zeta)/(1-u) < 1$ *for the floating-point signer at its (u, ζ), at $n = 512$ and $n = 1024$ [gate: verify/gates/sampler/leafsigma_fp.py];*
- $\sqrt{q^2/16822}\cdot 1.17^2\sigma_{\min}(\texttt{INV_SIGMA} - \zeta)/(1+u) > 1$ *for the floating-point signer at its (u, ζ), at $n = 512$ and $n = 1024$ [gate: verify/gates/sampler/leafsigma_fp.py].*

We have

1. $\forall i \le N:\ \sigma_i > \sigma_{\min}$*;*
2. $\forall i \le N:\ \sigma_i < 1.17^2\sigma_{\min}$*.*

Proof. (L1) $\forall i \le N:\ d_i \in [q^2/16822,\ 16822]$

[Proposition D.9]

(L2) $q^2/16822 > 0$

[expand]

(L3) `INV_SIGMA` $\mathcal{I}\,(u^{\pm}, \zeta^{\pm})\ c_n$

[Lemma J.29 at n]

(L4) $c_n, \sigma_{\min} > 0$

[$c_n = 1/s$ (the statement); $s = 1.17\sqrt{q}\,\sigma_{\min}$ (Definition A.25); the stored word $\sigma_{\min} > 0$ [LO: `sign_sampler.c:44-56`]]

(L5) $c_n \le (\texttt{INV_SIGMA} + \zeta)/(1-u)$

[(L3), (L4); $u = 2^{-53}$ (Definition J.1)]

(L6) $c_n \ge (\texttt{INV_SIGMA} - \zeta)/(1+u)$

[(L3), (L4)]

(L7) $\forall i \le N:\ \sqrt{d_i} \le \sqrt{16822}$

[(L1); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L8) $\forall i \le N:\ \sqrt{d_i} \ge \sqrt{q^2/16822}$

[(L1), (L2); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5)]

(L9) $\forall i \le N:\ \sqrt{d_i}\, c_n \sigma_{\min} < 1$

[(L4), (L5), (L7); the first measured row; $\forall a, a', b, b' \in \mathbb{R},\ 0 \le a \le a',\ 0 \le b \le b':\ ab \le a'b'$ (Fact A.41, item 8)]

(L10) $\forall i \le N:\ \sigma_i > \sigma_{\min}$

[(L4), (L9); σ_i (the statement)]

(L11) $\forall i \le N:\ \sqrt{d_i}\, c_n \cdot 1.17^2\sigma_{\min} > 1$

[(L2), (L4), (L6), (L8); the second measured row; $\forall a, a', b, b' \in \mathbb{R},\ 0 \le a \le a',\ 0 \le b \le b':\ ab \le a'b'$ (Fact A.41, item 8)]

(L12) $\forall i \le N:\ \sigma_i < 1.17^2\sigma_{\min}$

[(L4), (L11); σ_i (the statement)]

(L13) $\Rightarrow$ item 1

[(L10)]

(L14) $\Rightarrow$ item 2

[(L12)]

□ (items 1 and 2)

Hypothesis J.31 (No underflow [to table])**.** A mathematical hypothesis: no value the floating-point signer computes in $\mathcal{F}$ underflows. Define:

- $\mathcal{V} = \{w_1, \ldots, w_M\} \subset \mathcal{F}$, the results of the M operations ffSampling$^{\mathcal{F}}$ (Algorithm 10) performs in $\mathcal{F}$, its base sampler's included: the images, the Gram, the $LDL^\dagger$ steps, the operations of ffsamp (Algorithm 6) on the center, the exponent and its split; the $\mathcal{V}$(ffSampling$^{\mathcal{F}}$) of ν_2-walk (Algorithm 19);
- $r_i = \widetilde{t}_i - \lfloor \widetilde{t}_i \rfloor$, the fractional part line 3 of SamplerZ (Algorithm 8) computes and line 16 squares.

We assume

(1) $\forall w \in \mathcal{V},\ w \neq 0:\ |w| \ge 2^{-1022}$;

(2) $\forall i,\ r_i \neq 0:\ r_i \ge 2^{-511}$.

[L3: mathematical] Not discharged.

The underflow of `make`. A deficit is not detected where it occurs. Measured on `make` [L0: `sign_fpr.c:20-25`] at a nonzero result k binades below 2^{-1022} [gate: `verify/gates/fp/make.py`]: at $k = 1$ the exponent field is 0 and the mantissa kept, read as 0 by `fpr_mul` [L0: `sign_fpr.c:220`] and as a value below 2^{-1023} by `fpr_add` [L0: `sign_fpr.c:118-126`]; at $k \ge 2$ the sign is flipped, the exponent field is $2049 - k$ and the magnitude near 2^{1026-k}.

The first site of an underflow. Item (2) is the site ffSampling$^{\mathcal{F}}$ reaches first: at $z = 0$ at leaf i the base sampler squares r_i [L0: `sign_sampler.c:962`], so $r_i \in (0, 2^{-511})$ underflows there, the acceptance probability of $z = 0$ at that leaf is then unrelated to e^{-x}, and no later step of ffSampling$^{\mathcal{F}}$ tests it.

Definition J.32 (The 2-adic valuation [to table])**.** The 2-adic valuation of a nonzero element is the largest power of two dividing it. Let:

- $w \in \mathcal{F}$, $w \neq 0$.

Define:

- $\nu_2(w) := \max\{j \in \mathbb{Z} : w \in 2^j\mathbb{Z}\}$.

Definition J.33 (The valuation walk $\underline{\nu_2}$ [to table])**.** The valuation walk assigns a lower bound on the valuation to each value of a program, one rule per operation. Let:

- P, a straight-line program over $\mathcal{F}$ whose operations are those of ν_2 (Algorithm 18).

Define:

- $\mathcal{V}(P)$, the values of P (ν_2-walk (Algorithm 19));
- $\underline{\nu_2} : \mathcal{V}(P) \to \mathbb{Z}$, the valuation walk: the values ν_2-walk (Algorithm 19) assigns along P, one rule of ν_2 (Algorithm 18) per operation.

Fact J.34 (The valuation's floor on the magnitude [to table])**.** A nonzero element of $\mathcal{F}$ is at least every power of two up to its valuation in modulus. Define:

- ν_2, that of Definition J.32.

Then

$$\forall w \in \mathcal{F},\ w \neq 0\ \forall k \in \mathbb{Z},\ k \le \nu_2(w):\quad |w| \ge 2^k. \qquad \text{[derived]}$$

Proof. (L1) $\forall w \in \mathcal{F},\ w \neq 0\ \exists m \in \mathbb{Z} \setminus \{0\} :\ w = m2^{\nu_2(w)}$
[Definition J.32]

(L2) $|w| \geq 2^{\nu_2(w)}$
[$|m| \geq 1$ ((L1))]

(L3) $\forall k \in \mathbb{Z},\ k \leq \nu_2(w) :\ 2^k \leq 2^{\nu_2(w)}$
[$t \mapsto 2^t$ increasing (Fact A.41, item 5)]

(L4) $\forall k \in \mathbb{Z},\ k \leq \nu_2(w) :\ |w| \geq 2^k$
[(L2), (L3)]

(L5) $\Rightarrow$ the statement
[(L4)]
□

The valuation walk and item (1). At $P :=$ ffSampling$^{\mathcal{F}}$ (Algorithm 10) on integer inputs, the valuation walk (Definition J.33) with its postcondition, $\underline{\nu_2} \leq \nu_2$ (ν_2-walk (Algorithm 19)), and Fact J.34 is item (1).

Algorithm 18 $\underline{\nu_2}$: a lower bound on ν_2, one rule per operation of Definition A.4 `verify/reports/fp/grids.py`

Input: $x, y \in \mathcal{F}$, $\underline{\nu_2}(x) \leq \nu_2(x)$, $\underline{\nu_2}(y) \leq \nu_2(y)$
Output: $\underline{\nu_2}(z)$ for z the result of one operation of Definition A.4 on x, y
Postcondition: $\underline{\nu_2}(z) \leq \nu_2(z)$

1: $x = m2^e,\ m \in \mathbb{Z} \Rightarrow\ \underline{\nu_2}(x) \leftarrow e$ ▷ an input
2: $\underline{\nu_2}(\mathrm{fl}(x)) \leftarrow \underline{\nu_2}(x)$ ▷ $\nu_2(\mathrm{fl}(x)) \geq \nu_2(x)$: a multiple of $2^{\underline{\nu_2}(x)}$ rounds to one
3: $\underline{\nu_2}(x \pm y) \leftarrow \min(\underline{\nu_2}(x), \underline{\nu_2}(y))$
4: $\underline{\nu_2}(xy) \leftarrow \underline{\nu_2}(x) + \underline{\nu_2}(y)$
5: $\underline{\nu_2}(x/2) \leftarrow \underline{\nu_2}(x) - 1$
6: $\underline{\nu_2}(x/y) \leftarrow \lfloor \log_2 |x/y| \rfloor - 52$ ▷ a quotient keeps no valuation of its operands

Algorithm 19 $\underline{\nu_2}$-walk: $\underline{\nu_2}$ along a straight-line program over $\mathcal{F}$ `verify/reports/fp/grids.py`

Input: $P = (o_1, \ldots, o_M)$, o_i an operation of Definition A.4 on the inputs of P and on $w_1, \ldots, w_{i-1}$; $\underline{\nu_2}$ on the inputs
Output: $\underline{\nu_2}(w_i)$, $i \leq M$; $\mathcal{V}(P) := \{w_1, \ldots, w_M\}$
Postcondition: $\forall w \in \mathcal{V}(P) :\ \underline{\nu_2}(w) \leq \nu_2(w)$

1: **for** $i = 1$ to M **do**
2: $\quad \underline{\nu_2}(w_i) \leftarrow \nu_2(o_i)$ ▷ ν_2 (Algorithm 18) at the operands of o_i
3: **end for**

The valuations the walk measures. ν_2-walk at $P =$ ffSampling$^{\mathcal{F}}$ (Algorithm 10) on integer inputs, at $n = 512$ and $n = 1024$, measures $\underline{\nu_2}(\hat{b}) = -452, -513$ (line 2, $h-1$ twiddle levels by line 4) [L0: `sign_fpoly.c:1244-1266`], $\underline{\nu_2}(\mathcal{G}) = -904, -1026$ (line 4) [L0: `sign_core.c:11`], $\underline{\nu_2}(t) = -969, -1091$ (line 17), below -511 at both degrees [L0: `sign_fpoly.c:2663`], $\underline{\nu_2}(\widetilde{l}_{10}) = -979, -1102$ (line 4 of ffsamp (Algorithm 6) at the root node, by line 6) [L0: `sign_fpoly.c:2135-2150`], and $\underline{\nu_2}((\widetilde{t}_1 \ominus \widetilde{z}_1) \otimes \widetilde{l}_{10}) = \underline{\nu_2}(\widetilde{t}_1) + \underline{\nu_2}(\widetilde{l}_{10})$ (line 26), admitted below -1022 at both degrees `verify/reports/fp/grids.py`.

Why the root node's product stays open. No range argument passes the root node's product $(\widetilde{t}_1 \ominus \widetilde{z}_1) \otimes \widetilde{l}_{10}$. The calculus is realizable value by value: two values of equal valuation may cancel to the last bit, and whether a hash output, a key and a seed reach such values is a statement about ffSampling$^{\mathcal{F}}$, whose probability this report does not model.

A floor on the key's values moves neither threshold. A floor on the key's own values moves neither threshold into the calculus. A floor 2^{-F} on the nonzero components of the key's FFT images and of $\widetilde{l}_{10}$, measured per key, implies $\nu_2 \geq -F - 52$ for them instead, and the gate's options `--keyfloor`, `--l10floor` run ν_2-walk with it. Measured on 16 key generation keys per degree, the reference's own routines on the key-only values of the recursion, at $n = 512$, 1024 (`verify/reports/fp/keyfloor.py`): the key's FFT images are $\geq 2^{-7}$, 2^{-10} and $\widetilde{l}_{10}$ at any depth $\geq 2^{-19}$, 2^{-21}; the Gram matrix entries are $\geq 2^3$ and the diagonals $\geq 2^9$; no value is zero; with those floors $\underline{\nu_2}(t) = -576$, -640, still below -511; and the recursion's worst value is admitted below 2^{-1022} from depth 3, 3.

The measured values of ffSampling$^{\mathcal{F}}$. ffSampling$^{\mathcal{F}}$ itself is measured on 256 signatures per degree under 4 key generation keys, an instrumented copy of the reference's sampler, at $n = 512$, 1024 (`verify/reports/fp/runfloor.py`): no value of the recursion is zero and the smallest are 2^{-18}, 2^{-18} ($\widetilde{l}_{10}$); the computed centers are $\geq 2^{-17}$, 2^{-15}; of 262144, 524288 leaf fractional parts none is zero and the smallest are 2^{-16}, 2^{-20}; $\Pr[r < 2^{-8}]$ is 1009 against 1024 expected and 1983 against 2048; and $\Pr[r < 2^{-12}]$ is 50 against 64 and 112 against 128.

The measurements are evidence, not a proof. The measurements are evidence for item (2), not a proof. Under the uniform model $\Pr[r < 2^{-k}] = 2^{-k}$ the counts above follow, and a leaf center within 2^{-511} of an integer has probability 2^{-511}.

The hypothesis is void for the fixed-point signer. For the fixed-point signer the hypothesis is void: Theorem I.54 takes its place (Appendix I).

J.2 The key

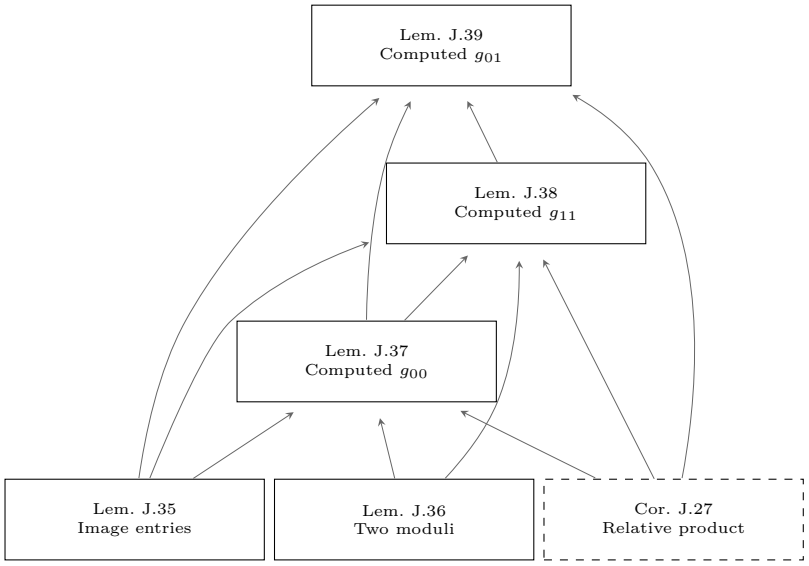


Figure 98: Dependencies, Appendix J.2.

Lemmas J.37, J.38 and J.39 state the computed Gram's three entries. The key generation is the checked key generation.

Lemma J.35 (The computed images' entries [to table])**.** *On a checked key, every entry of the computed images of the basis lies within the FFT's relative bound times the images' bound of the exact entry.* ***Under Hypothesis J.31****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- $u = 2^{-53}$ *and* $\zeta = 0$*, those of Definition J.1;*
- γ'_{fg} *and* γ'_{FG}*, those of Proposition 5.8;*
- h *and* $n = 2^h$*, those of* FFT *(Algorithm 14), Precondition;*
- $\hat{b}_{ij} = (b_{ij}(\psi_k))_{k<n/2}$*, the images of* $b = \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}$*;*
- $\widetilde{\hat{b}}_{ij} = \widetilde{\mathrm{FFT}}(b_{ij})$*, the computed images (line 2 of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10) in* $\mathcal{F}$*);*
- R_{h-1} *and* A_{h-1}*, those of Lemma H.12 at* $(u, 0)$*;*
- $\delta^{\mathrm{fp}}_{fg} = R_{h-1}\sqrt{n/2}\,\gamma'_{fg} \in [0, \infty)$*;*
- $\delta^{\mathrm{fp}}_{FG} = R_{h-1}\sqrt{n/2}\,\gamma'_{FG} \in [0, \infty)$.

Then

1. $\forall k < n/2 :\ |\widetilde{\hat{b}}_{00,k} - \hat{b}_{00,k}| \le \delta^{\mathrm{fp}}_{fg}$ *and* $|\widetilde{\hat{b}}_{01,k} - \hat{b}_{01,k}| \le \delta^{\mathrm{fp}}_{fg}$*;*
2. $\forall k < n/2 :\ |\widetilde{\hat{b}}_{10,k} - \hat{b}_{10,k}| \le \delta^{\mathrm{fp}}_{FG}$ *and* $|\widetilde{\hat{b}}_{11,k} - \hat{b}_{11,k}| \le \delta^{\mathrm{fp}}_{FG}$.

Proof. (L1) $A_0 = 0$

[Lemma H.12]

(L2) $\forall j < h-1 :\ A_{j+1} = \sqrt{2}(1 + c_{\mathrm{merge}})A_j$

[Lemma H.12: $A_{j+1} = \sqrt{2}(1 + c_{\mathrm{merge}})A_j + k_E\zeta\sqrt{P}$; $\zeta = 0$ (the statement)]

(L3) $\forall j < h-1 :\ A_j = 0 \Rightarrow\ A_{j+1} = 0$

[(L2)]

(L4) $\forall j \le h-1 :\ A_j = 0$

[induction on j: (L1) the base, (L3) the step]

(L5) $\forall i, j\ \forall k < n/2 :\ |\widetilde{\hat{b}}_{ij,k} - \hat{b}_{ij,k}| \le R_{h-1}\|\hat{b}_{ij}\|$

[Lemma H.12 at $f := b_{ij}$; (L4) at $j = h-1$; **Hypothesis J.31, item (1)**]

(L6) $\forall i, j :\ \|\hat{b}_{ij}\|^2 = \sum_{k<n/2}|\hat{b}_{ij,k}|^2$

[$\|X\|^2 = \sum_k |X_k|^2$ (Fact A.41)]

(L7) $\forall i, j :\ \sum_{k<n/2}|\hat{b}_{ij,k}|^2 \le (n/2)\max_\psi|\hat{b}_{ij}|^2$

[$\forall k < n/2 :\ |\hat{b}_{ij,k}| \le \max_\psi|\hat{b}_{ij}|$ (Fact A.41, item 20)]

(L8) $|\hat{b}_{00}|, |\hat{b}_{01}| \le \gamma'_{fg}$

[Lemma H.18, item 1, at $b_{00} = g$, $b_{01} = -f$]

(L9) $|\hat{b}_{10}|, |\hat{b}_{11}| \le \gamma'_{FG}$

[Lemma H.18, item 2, at $b_{10} = G$, $b_{11} = -F$]

(L10) $\forall k < n/2 :\ |\widetilde{\hat{b}}_{00,k} - \hat{b}_{00,k}|, |\widetilde{\hat{b}}_{01,k} - \hat{b}_{01,k}| \le \delta^{\mathrm{fp}}_{fg}$

[(L5) to (L8); $\delta^{\mathrm{fp}}_{fg}$ (the statement)]

(L11) $\Rightarrow$ item 1

[(L10)]

(L12) $\forall k < n/2 :\ |\widetilde{\hat{b}}_{10,k} - \hat{b}_{10,k}|, |\widetilde{\hat{b}}_{11,k} - \hat{b}_{11,k}| \le \delta^{\mathrm{fp}}_{FG}$

[(L5), (L6), (L7), (L9); $\delta^{\mathrm{fp}}_{FG}$ (the statement)]

(L13) $\Rightarrow$ item 2

[(L12)]

□ (items 1 and 2)

Lemma J.36 (A sum of two squared moduli [to table])**.** *When each of two complex values moves by a bounded amount and their squared moduli sum to at least a floor, the sum moves by a relative amount the bound and the floor determine. Let:*

- $x_0, x_1, \widetilde{x}_0, \widetilde{x}_1 \in \mathbb{C}$*;*
- $\delta \in \mathbb{R}$*;*
- $m \in (0, \infty)$.

Define:

- $S = |x_0|^2 + |x_1|^2$;
- $\widetilde{S} = |\widetilde{x}_0|^2 + |\widetilde{x}_1|^2$;
- $c = 2\sqrt{2}\,\delta/\sqrt{m} + 2\delta^2/m$.

Assume:

(A1) $|\widetilde{x}_0 - x_0| \le \delta$;

(A2) $|\widetilde{x}_1 - x_1| \le \delta$;

(A3) $|x_0|^2 + |x_1|^2 \ge m$.

Then

$$|\widetilde{S} - S| \le cS.$$

Proof. (L1) $\forall x, e \in \mathbb{C}:\ |x+e|^2 = |x|^2 + 2\,\mathrm{Re}(\mathrm{conj}\,x e) + |e|^2$

[expand $(x+e)\,\mathrm{conj}\,(x+e)$]

(L2) $\forall x, e \in \mathbb{C}:\ ||x+e|^2 - |x|^2| \le 2|x||e| + |e|^2$

[(L1); $|\mathrm{Re}\,w| \le |w|$, $|ww'| = |w||w'|$, $|w+w'| \le |w| + |w'|$ (Fact A.41, item 1)]

(L3) $|\widetilde{S} - S| \le 2\delta(|x_0| + |x_1|) + 2\delta^2$

[(L2) at $(x, e) := (x_0, \widetilde{x}_0 - x_0)$ and at $(x_1, \widetilde{x}_1 - x_1)$; assumptions A1, A2]

(L4) $|x_0| + |x_1| \le \sqrt{2}\,\sqrt{S}$

[Fact A.41, item 4, at $X := (x_0, x_1)$, $Y := (1,1)$; S (the statement)]

(L5) $\sqrt{S} \le S/\sqrt{m}$

[$S \ge m$, $m > 0$ (assumption A3; the statement)]

(L6) $1 \le S/m$

[$S \ge m$, $m > 0$ (assumption A3; the statement)]

(L7) $|\widetilde{S} - S| \le cS$

[(L3) to (L6); c (the statement)]

(L8) $\Rightarrow$ the statement

[(L7)]

□

Lemma J.37 (The computed g_{00} [to table])**.** *On a checked key, the first diagonal entry the code computes from the computed images is within a relative bound of the exact one at each root.* ***Under Hypothesis J.31****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The signer's words and parameters*
  - $u = 2^{-53}$ *and* $\zeta = 0$*, those of Definition J.1;*
  - h *and* $n = 2^h$*, those of* FFT *(Algorithm 14), Precondition;*
- *The key bounds*
  - m_0*, that of Proposition 5.8;*
- *The images*
  - $\hat{b}_{ij}$ *and* $\widetilde{\hat{b}}_{ij}$*, those of Lemma J.35;*
- *The Gram deltas*
  - $\delta_{fg}^{\mathrm{fp}}$*, that of Lemma J.35;*
- *The Gram matrix entries*
  - g_{00}*, at each* ψ*, the entry of Lemma G.22 at* $b := \hat{b}$*;*
  - $\widetilde{g}_{00}$*, at each* ψ*, the entry of Lemma G.22 at* $b := \widetilde{\hat{b}}$*, the value line 3 of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10) computes in* $\mathcal{F}$*;*
  - $g_{00}^{\circ} = |\widetilde{\hat{b}}_{00}|^2 + |\widetilde{\hat{b}}_{01}|^2$*, at each* ψ*;*
- *The error chain*
  - $p_3 = (1+u)^3 - 1 \in [0, \infty)$*;*

- $c_{00} = 2\sqrt{2}\,\delta_{fg}^{\mathrm{fp}}/\sqrt{m_0} + 2(\delta_{fg}^{\mathrm{fp}})^2/m_0 \in [0,\infty)$;
- $\bar{e}_{00} = (1+c_{00})(1+p_3) - 1 \in [0,\infty)$.

Then

1. $\forall\psi\ \exists\, e_{00}^{\circ} \in \mathbb{R},\ |e_{00}^{\circ}| \le c_{00} :\ g_{00}^{\circ} = g_{00}(1+e_{00}^{\circ})$;
2. $\forall\psi :\ \widetilde{g}_{00}\ \mathcal{I}\left(\bar{e}_{00}^{\pm}, 0\right)\ g_{00}$.

Proof. (L1) $\forall\psi :\ g_{00} = |\hat{b}_{00}|^2 + |\hat{b}_{01}|^2$
[Lemma G.22 at $b := \hat{b}$, assumption A1 by Definition J.1]

(L2) $\forall\psi :\ m_0 \in (0, g_{00}]$
[Lemma H.19, item 4]

(L3) $\forall\psi :\ |g_{00}^{\circ} - g_{00}| \le c_{00}\, g_{00}$
[Lemma J.36 at $(x_0,x_1) := (\hat{b}_{00},\hat{b}_{01})$, $(\widetilde{x}_0,\widetilde{x}_1) := (\widetilde{\hat{b}}_{00},\widetilde{\hat{b}}_{01})$, $\delta := \delta_{fg}^{\mathrm{fp}}$, $m := m_0$; Lemma J.35, item 1; (L1), (L2); **Hypothesis J.31, item (1)**]

(L4) $\forall\psi\ \exists\, e_{00}^{\circ} \in \mathbb{R},\ |e_{00}^{\circ}| \le c_{00} :\ g_{00}^{\circ} = g_{00}(1+e_{00}^{\circ})$
[(L2), (L3); Lemma G.1, items 1 and 2, at $c := c_{00}$]

(L5) $\Rightarrow$ item 1
[(L4)]

(L6) $\forall\psi\ \exists\, t_{00} \in \mathbb{R},\ |t_{00}| \le p_3 :\ \widetilde{g}_{00} = g_{00}^{\circ}(1+t_{00})$
[Lemma G.22, item 1, at $b := \widetilde{\hat{b}}$, $\zeta = 0$ (Corollary J.27), assumption A1 by Definition J.1; p_3 (the statement); **Hypothesis J.31, item (1)**]

(L7) $\forall\psi :\ \widetilde{g}_{00} = g_{00}(1+e_{00}^{\circ})(1+t_{00})$
[(L4), (L6)]

(L8) $|(1+e_{00}^{\circ})(1+t_{00}) - 1| \le (1+c_{00})(1+p_3) - 1$
[Lemma G.4 at $k = 2$; (L4), (L6)]

(L9) $\forall\psi :\ \widetilde{g}_{00}\ \mathcal{I}\left(\bar{e}_{00}^{\pm}, 0\right)\ g_{00}$
[(L7), (L8); $\bar{e}_{00}$ (the statement)]

(L10) $\Rightarrow$ item 2
[(L9)]

□ (items 1 and 2)

Lemma J.38 (The computed g_{11} [to table])**.** *On a checked key, the second diagonal entry the code computes from the computed images is within a relative bound of the exact one at each root.* ***Under Hypothesis J.31****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The signer's words and parameters*
  - $u = 2^{-53}$ *and* $\zeta = 0$*, those of Definition J.1;*
  - h *and* $n = 2^h$*, those of* FFT *(Algorithm 14), Precondition;*
- *The key bounds*
  - M_0*, that of Proposition 5.8;*
  - $m_{11} = q^2/M_0 \in [0,\infty)$*;*
- *The images*
  - $\hat{b}_{ij}$ *and* $\widetilde{\hat{b}}_{ij}$*, those of Lemma J.35;*
- *The Gram deltas*
  - $\delta_{FG}^{\mathrm{fp}}$*, that of Lemma J.35;*
- *The Gram matrix entries*
  - g_{00}*,* g_{01} *and* g_{11}*, at each* ψ*, the entries of Lemmas G.22 and G.23 at* $b := \hat{b}$*;*
  - $\widetilde{g}_{11}$*, at each* ψ*, the entry of Lemma G.22 at* $b := \widetilde{\hat{b}}$*, the value line 3 of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10) computes in* $\mathcal{F}$*;*

- $g^{\circ}_{11} = |\widetilde{\hat{b}}_{10}|^2 + |\widetilde{\hat{b}}_{11}|^2$, *at each* ψ;

- *The error chain*
  - p_3, *that of Lemma J.37;*
  - $c_{11} = 2\sqrt{2}\,\delta^{\mathrm{fp}}_{FG}/\sqrt{m_{11}} + 2(\delta^{\mathrm{fp}}_{FG})^2/m_{11} \in [0,\infty)$;
  - $\bar{e}_{11} = (1+c_{11})(1+p_3) - 1 \in [0,\infty)$.

Then

1. $\forall\psi\ \exists\, e^{\circ}_{11} \in \mathbb{R},\ |e^{\circ}_{11}| \le c_{11} :\ g^{\circ}_{11} = g_{11}(1+e^{\circ}_{11})$;

2. $\forall\psi :\ \widetilde{g}_{11}\ \mathcal{I}\left(\bar{e}^{\pm}_{11}, 0\right)\ g_{11}$.

Proof. (L1) $\forall\psi :\ g_{11} = |\hat{b}_{10}|^2 + |\hat{b}_{11}|^2$
[Lemma G.22 at $b := \hat{b}$, assumption A1 by Definition J.1]

(L2) $\forall\psi :\ g_{00}g_{11} - |g_{01}|^2 = q^2$
[Fact A.33, item 2]

(L3) $\forall\psi :\ g_{00} \in (0, M_0]$
[Lemma H.19, item 4]

(L4) $\forall\psi :\ g_{11} = (q^2 + |g_{01}|^2)/g_{00}$
[(L2), (L3)]

(L5) $\forall\psi :\ (q^2 + |g_{01}|^2)/g_{00} \ge q^2/M_0$
[(L3)]

(L6) $\forall\psi :\ g_{11} \ge m_{11}$
[(L4), (L5); m_{11} (the statement)]

(L7) $m_{11} > 0$
[m_{11} (the statement)]

(L8) $\forall\psi :\ |g^{\circ}_{11} - g_{11}| \le c_{11}\, g_{11}$
[Lemma J.36 at $(x_0,x_1) := (\hat{b}_{10},\hat{b}_{11})$, $(\widetilde{x}_0,\widetilde{x}_1) := (\widetilde{\hat{b}}_{10},\widetilde{\hat{b}}_{11})$, $\delta := \delta^{\mathrm{fp}}_{FG}$, $m := m_{11}$; Lemma J.35, item 2; (L1), (L6), (L7); **Hypothesis J.31, item (1)**]

(L9) $\forall\psi\ \exists\, e^{\circ}_{11} \in \mathbb{R},\ |e^{\circ}_{11}| \le c_{11} :\ g^{\circ}_{11} = g_{11}(1+e^{\circ}_{11})$
[(L6), (L7), (L8); Lemma G.1, items 1 and 2, at $c := c_{11}$]

(L10) $\Rightarrow$ item 1
[(L9)]

(L11) $\forall\psi\ \exists\, t_{11} \in \mathbb{R},\ |t_{11}| \le p_3 :\ \widetilde{g}_{11} = g^{\circ}_{11}(1+t_{11})$
[Lemma G.22, item 2, at $b := \widetilde{\hat{b}}$, $\zeta = 0$ (Corollary J.27), assumption A1 by Definition J.1; p_3 (Lemma J.37); **Hypothesis J.31, item (1)**]

(L12) $\forall\psi :\ \widetilde{g}_{11} = g_{11}(1+e^{\circ}_{11})(1+t_{11})$
[(L9), (L11)]

(L13) $|(1+e^{\circ}_{11})(1+t_{11}) - 1| \le (1+c_{11})(1+p_3) - 1$
[Lemma G.4 at $k = 2$; (L9), (L11)]

(L14) $\forall\psi :\ \widetilde{g}_{11}\ \mathcal{I}\left(\bar{e}^{\pm}_{11}, 0\right)\ g_{11}$
[(L12), (L13); $\bar{e}_{11}$ (the statement)]

(L15) $\Rightarrow$ item 2
[(L14)]

□ (items 1 and 2)

Lemma J.39 (The computed g_{01} [to table])**.** *On a checked key, the off-diagonal entry the code computes from the computed images is within an absolute bound of the exact one at each root.* ***Under Hypothesis J.31****, let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The signer's words and parameters*
  - $u = 2^{-53}$ *and* $\zeta = 0$*, those of Definition J.1;*
  - h *and* $n = 2^h$*, those of* FFT *(Algorithm 14), Precondition;*
- *The key bounds*
  - γ'_{fg} *and* γ'_{FG}*, those of Proposition 5.8;*
- *The images*
  - $\hat{b}_{ij}$, $\widetilde{\hat{b}}_{ij}$, $\delta^{\mathrm{fp}}_{fg}$ *and* $\delta^{\mathrm{fp}}_{FG}$*, those of Lemma J.35;*
- *The Gram matrix entries*
  - g_{00}, g_{01} *and* g_{11}*, at each* ψ*, the entries of Lemmas G.22 and G.23 at* $b := \hat{b}$*;*
  - $\widetilde{g}_{01}$*, at each* ψ*, the entry of Lemma G.23 at* $b := \widetilde{\hat{b}}$*, the value line 3 of* ffSampling$^{\mathcal{F}}$ *(Algorithm 10) computes in* $\mathcal{F}$*;*
  - $g^{\circ}_{01} = \widetilde{\hat{b}}_{00} \operatorname{conj} \widetilde{\hat{b}}_{10} + \widetilde{\hat{b}}_{01} \operatorname{conj} \widetilde{\hat{b}}_{11}$*, at each* ψ*;*
- *The error chain*
  - g°_{00}, c_{00} *and* $\bar{e}_{00}$*, those of Lemma J.37;*
  - g°_{11}, c_{11} *and* $\bar{e}_{11}$*, those of Lemma J.38;*
- *The Gram deltas*
  - $E_\gamma = 2(\delta^{\mathrm{fp}}_{fg}\gamma'_{FG} + \delta^{\mathrm{fp}}_{FG}\gamma'_{fg} + \delta^{\mathrm{fp}}_{fg}\delta^{\mathrm{fp}}_{FG}) \in [0, \infty)$*;*
  - $\bar{E}_a = E_\gamma(1+u)^2 + u|g_{01}| + (1+u)\sqrt{2}\,u(2+u)\sqrt{g_{00}g_{11}(1+\bar{e}_{00})(1+\bar{e}_{11})} \in [0, \infty)$*, at each* ψ*.*

Then

$$\forall \psi : \quad \widetilde{g}_{01} \, \mathcal{N}\left(0, \bar{E}_a\right) \, g_{01}.$$

Proof. (L1) $\forall x, y, e, e' \in \mathbb{C} : \; (x+e)\operatorname{conj}(y+e') - x \operatorname{conj} y = x \operatorname{conj} e' + e \operatorname{conj} y + e \operatorname{conj} e'$
[expand]

(L2) $\forall x, y, e, e' \in \mathbb{C} : \; |(x+e)\operatorname{conj}(y+e') - x \operatorname{conj} y| \le |x||e'| + |y||e| + |e||e'|$
[(L1); $|w+w'| \le |w| + |w'|$, $|ww'| = |w||w'|$, $|\operatorname{conj} w| = |w|$ (Fact A.41, item 1)]

(L3) $\forall \psi : \; g_{01} = \hat{b}_{00} \operatorname{conj} \hat{b}_{10} + \hat{b}_{01} \operatorname{conj} \hat{b}_{11}$
[Lemma G.23 at $b := \hat{b}$]

(L4) $\forall \psi : \; |\hat{b}_{00}|, |\hat{b}_{01}| \le \gamma'_{fg}$
[Lemma H.18, item 1]

(L5) $\forall \psi : \; |\hat{b}_{10}|, |\hat{b}_{11}| \le \gamma'_{FG}$
[Lemma H.18, item 2]

(L6) $\forall \psi : \; |\widetilde{\hat{b}}_{00} \operatorname{conj} \widetilde{\hat{b}}_{10} - \hat{b}_{00} \operatorname{conj} \hat{b}_{10}| \le \delta^{\mathrm{fp}}_{FG}\gamma'_{fg} + \delta^{\mathrm{fp}}_{fg}\gamma'_{FG} + \delta^{\mathrm{fp}}_{fg}\delta^{\mathrm{fp}}_{FG}$
[(L2) at $(x, y) := (\hat{b}_{00}, \hat{b}_{10})$; Lemma J.35, items 1 and 2; (L4), (L5); **Hypothesis J.31, item (1)**]

(L7) $\forall \psi : \; |\widetilde{\hat{b}}_{01} \operatorname{conj} \widetilde{\hat{b}}_{11} - \hat{b}_{01} \operatorname{conj} \hat{b}_{11}| \le \delta^{\mathrm{fp}}_{FG}\gamma'_{fg} + \delta^{\mathrm{fp}}_{fg}\gamma'_{FG} + \delta^{\mathrm{fp}}_{fg}\delta^{\mathrm{fp}}_{FG}$
[(L2) at $(x, y) := (\hat{b}_{01}, \hat{b}_{11})$; Lemma J.35, items 1 and 2; (L4), (L5); **Hypothesis J.31, item (1)**]

(L8) $\forall \psi : \; |g^{\circ}_{01} - g_{01}| \le E_\gamma$
[(L3), (L6), (L7); g°_{01}, E_γ (the statement); Fact A.41, item 1]

(L9) $\forall \psi \, \exists \, t_{01} \in \mathbb{C}, \; |t_{01}| \le u \, \exists \, e_{01} \in \mathbb{C}, \; |e_{01}| \le (1+u)\sqrt{2}\,u(2+u)\sqrt{g^{\circ}_{00}g^{\circ}_{11}} : \; \widetilde{g}_{01} = g^{\circ}_{01}(1+t_{01}) + e_{01}$
[Lemma G.23 at $b := \widetilde{\hat{b}}$, $\zeta = 0$ (Corollary J.27); **Hypothesis J.31, item (1)**]

(L10) $c_{00} \le \bar{e}_{00}$
[$\bar{e}_{00} = (1+c_{00})(1+p_3) - 1$, $p_3 \ge 0$ (Lemma J.37)]

(L11) $c_{11} \le \bar{e}_{11}$
[$\bar{e}_{11} = (1+c_{11})(1+p_3) - 1$, $p_3 \ge 0$ (Lemma J.38)]

(L12) $\forall \psi : \; g^{\circ}_{00} \le g_{00}(1+\bar{e}_{00})$
[Lemma J.37, item 1; (L10); **Hypothesis J.31, item (1)**]

(L13) $\forall \psi : \; g^{\circ}_{11} \le g_{11}(1+\bar{e}_{11})$
[Lemma J.38, item 1; (L11); **Hypothesis J.31, item (1)**]

(L14) $\forall \psi : \; g^{\circ}_{00}g^{\circ}_{11} \le g_{00}g_{11}(1+\bar{e}_{00})(1+\bar{e}_{11})$
[(L12), (L13); Fact A.41, item 8]

(L15) $\forall \psi:\ |e_{01}| \le (1+u)\sqrt{2}\,u(2+u)\sqrt{g_{00}g_{11}(1+\bar{e}_{00})(1+\bar{e}_{11})}$

[(L9), (L14); $t \mapsto \sqrt{t}$ nondecreasing on $[0,\infty)$ (Fact A.41, item 5)]

(L16) $\forall \psi:\ \widetilde{g}_{01} - g_{01} = (g^{\circ}_{01} - g_{01})(1+t_{01}) + g_{01}t_{01} + e_{01}$

[(L9)]

(L17) $\forall \psi:\ |\widetilde{g}_{01} - g_{01}| \le |g^{\circ}_{01} - g_{01}|(1+|t_{01}|) + |g_{01}||t_{01}| + |e_{01}|$

[(L16); Fact A.41, item 1]

(L18) $\forall \psi:\ |\widetilde{g}_{01} - g_{01}| \le E_{\gamma}(1+u) + u|g_{01}| + |e_{01}|$

[(L8), (L9), (L17)]

(L19) $E_{\gamma}(1+u) \le E_{\gamma}(1+u)^2$

[$u, E_{\gamma} \ge 0$ (the statement)]

(L20) $\forall \psi:\ |\widetilde{g}_{01} - g_{01}| \le \bar{E}_a$

[(L15), (L18), (L19); $\bar{E}_a$ (the statement)]

(L21) $\forall \psi:\ \widetilde{g}_{01}\ \mathcal{N}\left(0, \bar{E}_a\right)\ g_{01}$

[(L20); Definition A.10]

(L22) $\Rightarrow$ the statement

[(L21)]

□

The fixed-point counterpart of the three bounds. The three bounds are the floating-point counterpart of Lemma H.19, items 1 to 3: there the key's checks are read in $\mathcal{F}_{\mathrm{fx}}$ and the deviations stay absolute, here they are read in $\mathcal{F}$ and the two diagonals keep a relative form, which the floors m_0 and $m_{11} = q^2/M_0$ of the checked key supply. The key generation of `c-fn-dsa` alone bounds no image from below at one root (Fact A.34 checks norms), and without such a floor Lemma H.12's bound is a bound in norm only.

The perturbation admitted at one root. What Lemma H.11 admits at one root is measured, with R_{h-1} at $(u,0)$, $r_{ij,k} = R_{h-1}\|\hat{b}_{ij}\|/|\hat{b}_{ij,k}|$ (Lemma H.12) and $d_{11}(b) = g_{11}(b) - |g_{01}(b)|^2/g_{00}(b)$, on 16 keys of the checked key generation per degree at $n = 512, 1024$ (`verify/reports/fp/basisimage.py`): $R_{h-1} = 2^{-48.0}$, $2^{-47.8}$ and $\max_{ij,k} r_{ij,k} = 2^{-36.0}$, $2^{-35.6}$, and $|d_{11}(\widetilde{\hat{b}})/d_{11}(\hat{b}) - 1|$ is admitted up to $2^{-30.5}$, $2^{-28.1}$ to first order in the $r_{ij,k}$, against $2^{-22.3}$, $2^{-18.8}$, the bound of Corollary J.44.

The three bounds cost the derived level at binary64. Carrying the three bounds is what costs the derived level at binary64: χ_{root} carries $\bar{e}_{00}$ (Lemma J.37), $\bar{e}_{11}$ (Lemma J.38) and $\bar{E}_a$ (Lemma J.39) through Corollary J.44, and Table 42 reads them at each precision. **Hypothesis J.64** needs none of them: its sample replays ffSampling$^{\mathbb{R}}$ from the exact images (Appendix J.5).

J.3 The tree and the centers at $\zeta = 0$

Structure. Appendix J.3.1 states the recursion of the leaf diagonals; Appendix J.3.2 the root node's diagonals; Appendix J.3.3 the leaf standard deviation; Appendix J.3.4 the center shift. Every statement of this subsection holds at $\zeta = 0$.

J.3.1 The recursion of the leaf diagonals at $\zeta = 0$

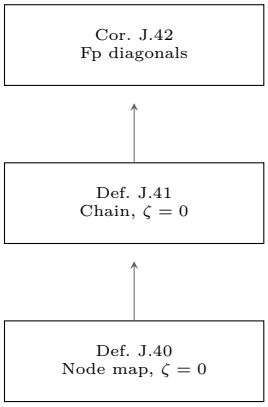


Figure 99: Dependencies, Appendix J.3.1.

Definition J.40 (The node map at $\zeta = 0$ [to table])**.** Let:

- $u \in [0, 1)$;
- $\kappa \in [0, \infty)$;
- $\chi \in [0, 1)$.

Define:

- $\Phi_\kappa(\chi) = \left(1 + \dfrac{\chi + \chi^2}{1 - \chi}\right)\left(1 + (1 + \kappa)((1 + u)^2 - 1) + \kappa((1 + u)^{10} - 1)\right)\dfrac{1 + u}{1 - u} - 1.$

```
noncomputable def Phi (u kappa eps : Real) : Real :=
  (1 + (eps + eps ^ 2) / (1 - eps)) * (1 + (1 + kappa) * ((1 + u) ^ 2 - 1) + kappa * ((1 + u) ^
      10 - 1))
    * ((1 + u) / (1 - u)) - 1
```

Figure 100: The Lean declarations carrying Definition J.40: `Phi` (`Depth.lean`); Lean's symbols in ASCII.

Definition J.41 (The chain of the leaf diagonals' bounds at $\zeta = 0$ [to table])**.** Let:

- $u \in [0, 1)$;
- $h \in \mathbb{Z}_{>0}$;
- $\chi_0 \in [0, 1)$.

Define:

- κ_k, $k \in \{1, \dots, h - 1\}$, those of Corollary G.36;
- Φ_κ, that of Definition J.40;
- $\forall k \in \{1, \dots, h - 1\},\ \chi_{k-1} < 1 :\ \vartheta_{k-1} = (1 + \chi_{k-1})/(1 - \chi_{k-1})$;
- $\forall k \in \{1, \dots, h - 1\},\ \chi_{k-1} < 1 :\ \hat{\kappa}_k = \vartheta_{k-1}\kappa_k + (\vartheta_{k-1} - 1)/2$;
- $\forall k \in \{1, \dots, h - 1\},\ \chi_{k-1} < 1 :\ \chi_k = \Phi_{\hat{\kappa}_k}(\chi_{k-1})$, the three defined together by induction on k.

```
noncomputable def PhiIter (u : Real) (kappa : Nat -> Real) (eps0 : Real) : Nat -> Real
  | 0 => eps0
  | k + 1 => Phi u (kappa (k + 1)) (PhiIter u kappa eps0 k)
```

Figure 101: The Lean declarations carrying Definition J.41: `PhiIter` (`Depth.lean`); with `Phi` of Figure 100; Lean's symbols in ASCII.

Corollary J.42 (The computed diagonals of the floating-point signer [to table])**.** *At $\zeta = 0$, every diagonal on a path of the tree is within the chain's relative bound at its depth of its exact value, and the leaf diagonals within the chain's last bound. Let:*

- $\zeta = 0$*;*
- $u \in [0, 1)$*;*
- $h \geq 1$*;*
- $T \in \mathcal{T}_n$ *with* $n = 2^h$*;*
- $(\nu_k)_{0 \leq k \leq h-1}$ *be a path:* $\nu_0 = T$ *and* $\forall k \in \{1, \ldots, h-1\} : \ \nu_k \in \{L(\nu_{k-1}), R(\nu_{k-1})\}$ *(Definition A.18);*
- $\chi_0 \in [0, 1)$.

Define:

- χ_k, $k \in \{1, \ldots, h-1\}$, *those of Definition J.41;*
- d_j^ν, $\widetilde{d}_j^\nu$, κ_k *and* χ_{leaf}, *those of Corollary G.36;*
- d_ν *and* $\widetilde{d}_\nu$, *each diagonal* d_j^ν, $j \in \{00, 11\}$, *of the node* ν *and its computed* $\widetilde{d}_j^\nu$*;*
- d_{00}, $\widetilde{d}_{00}$, d_{11} *and* $\widetilde{d}_{11}$, *the root node's* d_{00}^T, $\widetilde{d}_{00}^T$, d_{11}^T *and* $\widetilde{d}_{11}^T$.

Assume:

(A1) $\forall \psi$ *of the root node:* $\widetilde{d}_{00} \ \mathcal{I}\left(\chi_0^\pm, 0\right) d_{00}$*;*

(A2) $\forall \psi$ *of the root node:* $\widetilde{d}_{11} \ \mathcal{I}\left(\chi_0^\pm, 0\right) d_{11}$*;*

(A3) $\forall k \leq h-1 : \ \chi_k < 1$.

Then

1. $\forall k \leq h-1 \ \forall \psi : \ \widetilde{d}_{\nu_k} \ \mathcal{I}\left(\chi_k^\pm, 0\right) d_{\nu_k}$*;*
2. $\chi_{\text{leaf}} \leq \chi_{h-1}$.

Proof.

DEFINES $\mathcal{U}_\kappa^\zeta$, $\mathcal{A}$, χ_k^ζ: those of Corollary G.36

DEFINES $\hat{\kappa}_k^\zeta$: the $\hat{\kappa}_k$ of Corollary G.36

(L1) $\mathcal{U}_\kappa^0 = \Phi_\kappa$

[Lemma G.33; $\zeta = 0$ (the statement)]

(L2) $\chi_0^0 = \chi_0$

[χ_0^ζ (Corollary G.36)]

(L3) $\forall k \in \{1, \ldots, h-1\} : \ \chi_{k-1}^0 = \chi_{k-1} \Rightarrow \ \hat{\kappa}_k^0 = \hat{\kappa}_k$

[$\hat{\kappa}_k^\zeta$ (Corollary G.36); $\hat{\kappa}_k$ (Definition J.41)]

(L4) $\forall k \in \{1, \ldots, h-1\} : \ \chi_{k-1}^0 = \chi_{k-1} \Rightarrow \ \chi_k^0 = \chi_k$

[(L1), (L3); χ_k^ζ (Corollary G.36); χ_k (Definition J.41)]

(L5) $\forall k \leq h-1 : \ \chi_k^0 = \chi_k$

[induction on k: (L2) the base, (L4) the step]

(L6) $\mathcal{A} = [0, 1)$

[$\zeta = 0$ (the statement): $u_0 = u$, $u < 1$ (Lemma G.32, item 1); $\mathcal{A}$ (Corollary G.36)]

(L7) $\forall k \leq h-1 : \ \chi_k \geq 0$

[$\chi_0 \geq 0$ (the statement); $\Phi_\kappa(\chi) \geq 0$ at $\chi, \kappa \geq 0$ (Definition J.40)]

(L8) $\forall k \leq h-1 : \ \chi_k^0 \in \mathcal{A}$

[(L5), (L6), (L7); $\chi_k < 1$ (assumption A3)]

(L9) $\forall k \leq h-1 \ \forall \psi : \ \widetilde{d}_{\nu_k} \ \mathcal{I}\left(\chi_k^\pm, 0\right) d_{\nu_k}$

[Corollary G.36, item 1, at $\zeta = 0$; (L5), (L8); assumptions A1, A2]

(L10) $\Rightarrow$ item 1

[(L9)]

(L11) $\chi_{\text{leaf}} \leq \chi_{h-1}$

[Corollary G.36, item 2, at $\zeta = 0$; (L5), (L8); assumptions A1, A2]

(L12) $\Rightarrow$ item 2

[(L11)]

□ (items 1 and 2)

J.3.2 The root node's diagonals at $\zeta = 0$

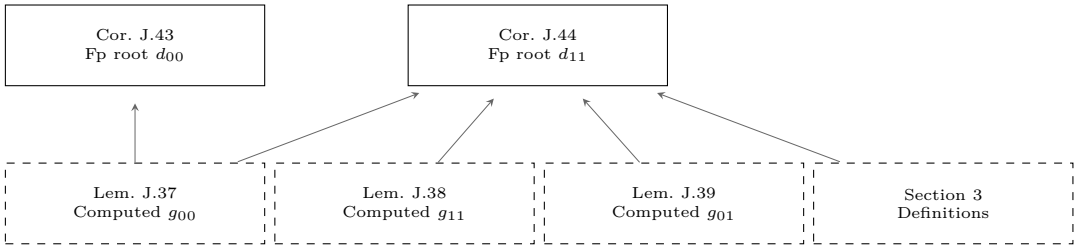


Figure 102: Dependencies, Appendix J.3.2.

Corollary J.43 (The floating-point root's first diagonal [to table])**.** *On a checked key, the root node's computed first diagonal is within a relative bound of the exact one at each root.* ***Under Hypothesis J.31****, define:*

- $u = 2^{-53}$ *and* $\zeta = 0$*, those of Definition J.1;*
- g_{00}*,* $\widetilde{g}_{00}$ *and* $\bar{e}_{00}$*, those of Lemma J.37;*
- $\bar{e}_{11}$*, that of Lemma J.38;*
- $\widetilde{d}_{00} = \widetilde{g}_{00}$*, the root node's computed first diagonal (*LDL† *(Algorithm 5));*
- $\bar{e} = \max(\bar{e}_{00}, \bar{e}_{11})$.

Then

$$\forall \psi : \quad \widetilde{d}_{00}\, \mathcal{I}\left(\bar{e}^{\pm}, 0\right)\, g_{00}.$$

Proof. (L1) $\forall \psi : \ \widetilde{g}_{00}\, \mathcal{I}\left(\bar{e}_{00}^{\pm}, 0\right)\, g_{00}$

[Lemma J.37, item 2; **Hypothesis J.31, item (1)**]

(L2) $\bar{e}_{00} \leq \bar{e}$

[$\bar{e}$ (the statement)]

(L3) $\forall \psi : \ \widetilde{g}_{00}\, \mathcal{I}\left(\bar{e}^{\pm}, 0\right)\, g_{00}$

[(L1), (L2); Definition A.10]

(L4) $\forall \psi : \ \widetilde{d}_{00}\, \mathcal{I}\left(\bar{e}^{\pm}, 0\right)\, g_{00}$

[(L3); $\widetilde{d}_{00} = \widetilde{g}_{00}$ (the statement)]

(L5) $\Rightarrow$ the statement

[(L4)]

□

Corollary J.44 (The floating-point root's second diagonal [to table])**.** *On a checked key, the root node's computed second diagonal is within a relative bound of the exact one at each root.* ***Under Hypothesis J.31****, define:*

- *The signer's words and parameters*
  - $u = 2^{-53}$ *and* $\zeta = 0$*, those of Definition J.1;*
- *The Gram matrix entries*
  - g_{00}*,* $\widetilde{g}_{00}$ *and* $\bar{e}_{00}$*, those of Lemma J.37;*
  - g_{11}*,* $\widetilde{g}_{11}$ *and* $\bar{e}_{11}$*, those of Lemma J.38;*
  - g_{01}*,* $\widetilde{g}_{01}$ *and* $\bar{E}_a$*, those of Lemma J.39;*
- *The diagonals*
  - $d_{11} = q^2/g_{00}$*, at each* ψ*;*

  - $\widetilde{d}_{11}$, *the value* LDL† *(Algorithm 5) computes at* $(\widetilde{g}_{00}, \widetilde{g}_{01}, \widetilde{g}_{11})$ *(line 18), at each* ψ*;*
- *The key constants*
  - $\kappa_{\mathrm{root}} = |g_{01}|^2/q^2$*, at each* ψ*;*
- *The error chain*
  - $\bar{e} = \max(\bar{e}_{00}, \bar{e}_{11})$*;*
  - $\chi_{11} = \Big(1 + (1+\kappa_{\mathrm{root}})\left((1+\bar{e})^2 - 1\right) + \kappa_{\mathrm{root}}\left((1+u)^4 - 1\right) + \Big(2\sqrt{\kappa_{\mathrm{root}}}\,\frac{\bar{E}_a}{q} + \frac{\bar{E}_a^2}{q^2}\Big)(1+u)^4\Big)\frac{1+u}{1-\bar{e}} - 1$*, at each* ψ*.*

Assume:

(A1) $\bar{e} < 1$*.*

Then

$$\forall \psi: \quad \widetilde{d}_{11}\ \mathcal{I}\left(\chi_{11}^{\pm}, 0\right) d_{11}.$$

Proof.

DEFINES $\kappa = \kappa_{\mathrm{root}}$

DEFINES $e = \bar{e}$

COMPUTES $\widetilde{zo}$: the value LDL† (Algorithm 5) computes at line 15 from $(\widetilde{g}_{00}, \widetilde{g}_{01})$

(L1) $\forall \psi\ \exists\, e_{00} \in \mathbb{R},\ |e_{00}| \le \bar{e}_{00}:\ \widetilde{g}_{00} = g_{00}(1+e_{00})$
[Lemma J.37, item 2; Definition A.10; **Hypothesis J.31, item (1)**]

(L2) $\forall \psi\ \exists\, e_{11} \in \mathbb{R},\ |e_{11}| \le \bar{e}_{11}:\ \widetilde{g}_{11} = g_{11}(1+e_{11})$
[Lemma J.38, item 2; Definition A.10; **Hypothesis J.31, item (1)**]

(L3) $\forall \psi\ \exists\, a \in \mathbb{C},\ |a| \le \bar{E}_a:\ \widetilde{g}_{01} = g_{01} + a$
[Lemma J.39; Definition A.10; **Hypothesis J.31, item (1)**]

(L4) $\exists\, e_{zo} \in \mathbb{R},\ |e_{zo}| \le (1+u)^4 - 1:\ \widetilde{zo} = (|\widetilde{g}_{01}|^2/\widetilde{g}_{00})(1+e_{zo})$
[Lemma G.24, item 3; **Hypothesis J.31, item (1)**]

(L5) $\exists\, t \in \mathbb{R},\ |t| \le u:\ \widetilde{d}_{11} = (\widetilde{g}_{11} - \widetilde{zo})(1+t)$
[Definition A.4 for $-$; **Hypothesis J.31, item (1)**]

(L6) $\widetilde{d}_{11} = \frac{\widetilde{g}_{00}\widetilde{g}_{11} - |\widetilde{g}_{01}|^2(1+e_{zo})}{\widetilde{g}_{00}}(1+t)$
[(L4), (L5)]

(L7) $|g_{01}|^2 = q^2\kappa$
[κ, κ_{root} (the statement)]

(L8) $g_{00}g_{11} = q^2(1+\kappa)$
[(L7); $g_{00}g_{11} - |g_{01}|^2 = q^2$ (Fact A.33, item 2)]

(L9) $|\widetilde{g}_{01}|^2 = |g_{01}|^2 + 2\,\mathrm{Re}(\mathrm{conj}\, g_{01}a) + |a|^2$
[(L3); expand $(g_{01}+a)\,\mathrm{conj}\,(g_{01}+a)$]

(L10) $\frac{\widetilde{g}_{00}\widetilde{g}_{11} - |\widetilde{g}_{01}|^2(1+e_{zo})}{q^2} - 1 = (1+\kappa)((1+e_{00})(1+e_{11}) - 1) - \kappa e_{zo} - \frac{2\,\mathrm{Re}(\mathrm{conj}\, g_{01}a) + |a|^2}{q^2}(1+e_{zo})$
[(L1), (L2), (L7), (L8), (L9)]

(L11) $|\mathrm{Re}(\mathrm{conj}\, g_{01}a)| \le q\sqrt{\kappa}|a|$
[Fact A.41, item 1; (L7)]

(L12) $|(1+e_{00})(1+e_{11}) - 1| \le (1+e)^2 - 1$
[(L1), (L2); Lemma G.4 at $k=2$; e (the block)]

(L13) $\left|\frac{\widetilde{g}_{00}\widetilde{g}_{11} - |\widetilde{g}_{01}|^2(1+e_{zo})}{q^2} - 1\right| \le (1+\kappa)((1+e)^2-1) + \kappa((1+u)^4-1) + \Big(2\sqrt{\kappa}\,\frac{|a|}{q} + \frac{|a|^2}{q^2}\Big)(1+u)^4$
[(L4), (L10), (L11), (L12); Fact A.41, item 1]

(L14) $d_{11} > 0$
[d_{11} (the statement); $g_{00} > 0$ (Lemma H.19, item 4)]

(L15) $\frac{\widetilde{d}_{11}}{d_{11}} = \frac{\widetilde{g}_{00}\widetilde{g}_{11} - |\widetilde{g}_{01}|^2(1+e_{zo})}{q^2} \cdot \frac{1+t}{1+e_{00}}$
[(L1), (L6), (L14); d_{11} (the statement)]

(L16) $\left|\frac{\widetilde{d}_{11}}{d_{11}} - 1\right| \le \left(1 + \left|\frac{\widetilde{g}_{00}\widetilde{g}_{11} - |\widetilde{g}_{01}|^2(1+e_{zo})}{q^2} - 1\right|\right)\frac{1+u}{1-e} - 1$
[(L15); $|t| \le u$ (L5); $|e_{00}| \le e$, $e < 1$ ((L1); assumption A1)]

(L17) $\left|\frac{\widetilde{d}_{11}}{d_{11}} - 1\right| \leq \chi_{11}$

[(L3), (L13), (L16); χ_{11} (the statement)]

(L18) $\forall \psi :\ \widetilde{d}_{11}\ \mathcal{I}\left(\chi_{11}^{\pm}, 0\right)\ d_{11}$

[(L17); Definition A.10]

(L19) $\Rightarrow$ the statement

[(L18)]

□

J.3.3 The leaf standard deviation at $\zeta = 0$

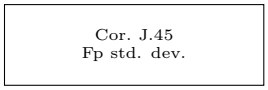


Figure 103: Dependencies, Appendix J.3.3.

Corollary J.45 (The floating-point leaf standard deviation [to table])**.** *At $\zeta = 0$, a leaf diagonal within a relative bound of its exact value bounds the computed standard deviation within a relative bound of its exact one. Let:*

- $\zeta = 0$;
- $u \in [0, 1]$;
- $d_{11} \in (0, \infty)$;
- $\chi_{\text{leaf}} \in [0, 1)$;
- $\delta_d \in \mathbb{R}$;
- $c_n \in \mathbb{R}$.

Define:

- `isigma` *and* $\widetilde{\texttt{isigma}}$, *those of Lemma G.21 at* $(n, d_{11}, \delta_d, c_n)$, $\widetilde{d}_{11} = d_{11}(1 + \delta_d)$;
- χ_σ, *that of Corollary G.41;*
- $\sigma = 1/\texttt{isigma}$;
- $\widetilde{\sigma} = 1/\widetilde{\texttt{isigma}}$.

Assume:

(A1) $d_{11}(1 + \delta_d) \in \mathcal{F}$;

(A2) $|\delta_d| \leq \chi_{\text{leaf}}$;

(A3) $\texttt{INV_SIGMA}[\log_2 n]\ \mathcal{I}\left(u^{\pm}, 0\right)\ c_n$;

(A4) $\chi_\sigma < 1$.

Then

$$\widetilde{\sigma}\ \mathcal{I}\left((\chi_\sigma/(1 - \chi_\sigma))^{\pm}, 0\right)\ \sigma.$$

Proof.

DEFINES k_J: that of Lemma G.21

DEFINES χ_σ^ζ: that of Corollary G.41 at $s_{\min} := \texttt{isigma}$

(L1) $\texttt{isigma} > 0$

[Lemma G.21; $d_{11} > 0$ (the statement)]

(L2) $\chi_\sigma^\zeta = \chi_\sigma + k_J \zeta / \texttt{isigma}$

[Corollary G.41 at $s_{\min} := \texttt{isigma}$; (L1); its assumptions by assumptions A1, A2 and A3 at $\zeta = 0$]

(L3) $\chi_\sigma^\zeta = \chi_\sigma$

[(L2); $\zeta = 0$ (the statement)]

(L4) $\chi_\sigma^\zeta < 1$

[(L3); $\chi_\sigma < 1$ (assumption A4)]

(L5) $\widetilde{\sigma}\ \mathcal{I}\left((\chi_\sigma/(1-\chi_\sigma))^{\pm}, 0\right)\ \sigma$
[Corollary G.41 at $s_{\min} :=$ `isigma`, δ_d, χ_{leaf}; $|\delta_d| \le \chi_{\text{leaf}}$ (assumption A2); its assumption A2 by assumption A3 at $\zeta = 0$; (L1), (L3), (L4)]

(L6) $\Rightarrow$ the statement

[(L5)]

□

J.3.4 The center shift at $\zeta = 0$

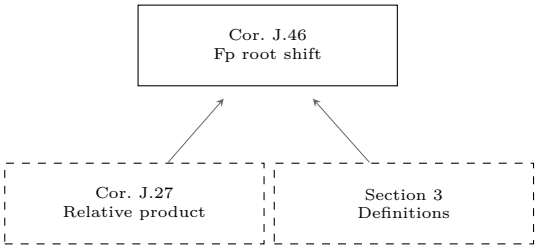


Figure 104: Dependencies, Appendix J.3.4.

Corollary J.46 states the root entry shift e_{root}.

Corollary J.46 (The floating-point root entry shift [to table])**.** *At $\zeta = 0$, the computed center's two parts lie, at every root, within e_t of their values over $\mathbb{R}$, and the shift at the root node's entry is at most $\bar{e}_{\text{root}}$. Let:*

- *(f, g, F, G) be a checked key (Definition 5.5) of degree n;*
- *h with $n = 2^h$, as FFT (Algorithm 14) takes them (Precondition);*
- *$\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ be the hashed message.*

Define:

- *The signer's words and parameters*
  - *$u = 2^{-53}$ and $\zeta = 0$, those of Definition J.1;*
  - *$e_{\text{mul}} = \sqrt{2}\,u(2+u)$, the relative bound of Lemma B.2, item 3;*
  - *P, that of FFT (Algorithm 14), line 1;*
- *The center shifts*
  - *c_{merge} and k_E, those of Lemma G.18;*
  - *$R_{h-1} = (1 + c_{\text{merge}})^{h-1} - 1$;*
  - *$A_0 = 0$;*
  - *$A_{j+1} = \sqrt{2}(1 + c_{\text{merge}})A_j + k_E\,\zeta\sqrt{P}$, $j < h - 1$;*
  - *$\delta_{\mathsf{h}(\mathsf{m})} = R_{h-1}\,nq/\sqrt{2} + A_{h-1}$;*
- *The Gram deltas*
  - *γ'_{fg} and γ'_{FG}, those of Lemma H.18;*
  - *$\delta_{FG} = R_{h-1}(n/2)^{1/2}\gamma'_{FG} + A_{h-1}$;*
  - *$\delta_{fg} = R_{h-1}(n/2)^{1/2}\gamma'_{fg} + A_{h-1}$;*
- *The center*
  - *$\hat{h}$, H, b_{01}, b_{11} and $t = (t_0, t_1)$, the values ffSampling$^{\mathcal{F}}$ (Algorithm 10) names over $\mathbb{R}$ at $\mathsf{h}(\mathsf{m})$ (lines 9 to 19);*
  - *$\widetilde{\hat{h}}$, $\widetilde{b}_{01}$, $\widetilde{b}_{11}$, $\widetilde{(1/q)}$, $\widetilde{(-1/q)}$, $\widetilde{t} = (\widetilde{t}_0, \widetilde{t}_1)$ and e_{root}, the values it computes in $\mathcal{F}$ (lines 9 to 20);*
- *The entry shifts*
  - *$e_p(\gamma', \delta) = H\delta + \gamma'\delta_{\mathsf{h}(\mathsf{m})} + \delta_{\mathsf{h}(\mathsf{m})}\delta + e_{\text{mul}}(H + \delta_{\mathsf{h}(\mathsf{m})})(\gamma' + \delta)$, at $\gamma', \delta \in [0, \infty)$;*
  - *$e_t(\gamma', \delta) = e_p(\gamma', \delta)(1+u)^2/q + H\gamma'((1+u)^2 - 1)/q$, at $\gamma', \delta \in [0, \infty)$;*
  - *$\bar{e}_{\text{root}} = (e_t(\gamma'_{FG}, \delta_{FG})^2 + e_t(\gamma'_{fg}, \delta_{fg})^2)^{1/2}$.*

Then

1. $\forall \psi :\ |\widetilde{t}_0(\psi) - t_0(\psi)| \le e_t(\gamma'_{FG}, \delta_{FG})$;
2. $\forall \psi :\ |\widetilde{t}_1(\psi) - t_1(\psi)| \le e_t(\gamma'_{fg}, \delta_{fg})$;
3. $\|e_{\mathrm{root}}\| \le \bar{e}_{\mathrm{root}}$.

Proof.

DEFINES $(b_0, s_0, \gamma'_0, \delta_0) := (b_{11}, 1/q, \gamma'_{FG}, \delta_{FG})$, $(b_1, s_1, \gamma'_1, \delta_1) := (b_{01}, -1/q, \gamma'_{fg}, \delta_{fg})$
$\widetilde{b}_0 := \widetilde{b}_{11}$, $\widetilde{b}_1 := \widetilde{b}_{01}$, $\widetilde{s}_0 := \widetilde{(1/q)}$, $\widetilde{s}_1 := \widetilde{(-1/q)}$

Proof of items 1 and 2.

(L1) $\forall j :\ t_j = \hat{h}\, b_j\, s_j$
[lines 9 to 19 of ffSampling$^{\mathcal{F}}$ (Algorithm 10); the proof's block]

(L2) $\forall j :\ \widetilde{t}_j = (\widetilde{\hat{h}} \otimes \widetilde{b}_j) \otimes \widetilde{s}_j$
[lines 16 and 18 of ffSampling$^{\mathcal{F}}$; the proof's block]

(L3) $\forall \psi :\ |\widetilde{\hat{h}}(\psi) - \hat{h}(\psi)| \le R_{h-1} \left(\sum_{\psi'} |\hat{h}(\psi')|^2\right)^{1/2} + A_{h-1}$
[Lemma H.12 on the array $(\hat{h}(\psi))_\psi$; the array's indexing a bijection of its $n/2$ entries onto the roots [gate: `verify/gates/tree/tower_index.py`]]

(L4) $\sum_{\psi'} |\hat{h}(\psi')|^2 = (n/2)\|\mathsf{h}(\mathsf{m})\|^2$
[Proposition G.15; $\|\mathsf{h}(\mathsf{m})\|$, the coefficient norm (Section 3.1)]

(L5) $\|\mathsf{h}(\mathsf{m})\|^2 \le nq^2$
[$\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ (the statement)]

(L6) $\Rightarrow\ \forall \psi :\ |\widetilde{\hat{h}}(\psi) - \hat{h}(\psi)| \le \delta_{\mathsf{h}(\mathsf{m})}$
[(L3), (L4), (L5); $\delta_{\mathsf{h}(\mathsf{m})}$ (the statement)]

(L7) $\|\mathsf{h}(\mathsf{m})\|_1 < nq$
[$\mathsf{h}(\mathsf{m}) \in \{0, \dots, q-1\}^n$ (the statement)]

(L8) $\forall \psi :\ |\hat{h}(\psi)| \le H$
[Fact A.42, item 3, at $f := \mathsf{h}(\mathsf{m})$; (L7); H (ffSampling$^{\mathcal{F}}$, line 11)]

(L9) $\forall j\ \forall \psi :\ |b_j(\psi)| \le \gamma'_j$
[$b_{11} = -\hat{F}$, $b_{01} = -\hat{f}$ (ffSampling$^{\mathcal{F}}$, lines 9 to 19); Lemma H.18, items 1 and 2, at the checked key (the statement)]

(L10) $\forall j\ \forall \psi :\ |\widetilde{b}_j(\psi) - b_j(\psi)| \le R_{h-1} \left(\sum_{\psi'} |b_j(\psi')|^2\right)^{1/2} + A_{h-1}$
[Lemma H.12 on the arrays $(b_j(\psi))_\psi$; $\mathrm{fl}(-x) = -x$ (Fact J.2, item 1)]

(L11) $\forall j :\ \sum_{\psi'} |b_j(\psi')|^2 \le (n/2)\gamma'^2_j$
[(L9) over the $n/2$ roots]

(L12) $\Rightarrow\ \forall j\ \forall \psi :\ |\widetilde{b}_j(\psi) - b_j(\psi)| \le \delta_j$
[(L10), (L11); δ_{FG}, δ_{fg} (the statement); the proof's block]

(L13) $\forall j\ \forall \psi\ \exists \delta_p \in \mathbb{C},\ |\delta_p| \le e_{\mathrm{mul}} :\ \widetilde{\hat{h}} \otimes \widetilde{b}_j = \widetilde{\hat{h}}\, \widetilde{b}_j (1 + \delta_p)$
[Corollary J.27, item 1]

(L14) $\forall x, \widetilde{x}, y, \widetilde{y} \in \mathbb{C} :\ \widetilde{x}\widetilde{y} - xy = x(\widetilde{y} - y) + y(\widetilde{x} - x) + (\widetilde{x} - x)(\widetilde{y} - y)$
[expand]

(L15) $\forall j\ \forall \psi :\ |\widetilde{\hat{h}}\widetilde{b}_j - \hat{h} b_j| \le H\delta_j + \gamma'_j \delta_{\mathsf{h}(\mathsf{m})} + \delta_{\mathsf{h}(\mathsf{m})}\delta_j$
[(L14); (L6), (L8), (L9), (L12); $|x+y| \le |x| + |y|$, $|xy| = |x||y|$ (Fact A.41, item 1)]

(L16) $\forall j\ \forall \psi :\ |\widetilde{\hat{h}}\widetilde{b}_j| \le (H + \delta_{\mathsf{h}(\mathsf{m})})(\gamma'_j + \delta_j)$
[(L6), (L8), (L9), (L12); Fact A.41, item 1]

(L17) $\Rightarrow\ \forall j\ \forall \psi :\ |\widetilde{\hat{h}} \otimes \widetilde{b}_j - \hat{h} b_j| \le e_p(\gamma'_j, \delta_j)$
[(L13), (L15), (L16); Fact A.41, item 1; e_p (the statement)]

(L18) $\forall j\ \exists t_q \in \mathbb{R},\ |t_q| \le u :\ \widetilde{s}_j = s_j(1 + t_q)$
[Definition J.28: $\widetilde{s}_j = \mathrm{fl}(s_j)$; Definition A.4, item 1]

(L19) $\forall p \in C_{\mathcal{F}}\ \forall x \in \mathcal{F}\ \exists\, \delta_s \in \mathbb{C},\ |\delta_s| \le u :\ p \otimes x = xp(1+\delta_s)$
[Definition A.8, $a \otimes c$ and $c \otimes a$ at $(c, a) := (x, p)$; Definition A.4, item 1; Lemma G.13 at $c := u$]

(L20) $\forall j\ \forall \psi :\ \widetilde{t}_j - t_j = s_j(\widetilde{\hat{h}} \otimes \widetilde{b}_j - \hat{h}b_j)(1+t_q)(1+\delta_s) + s_j\hat{h}b_j((1+t_q)(1+\delta_s) - 1)$
[(L1), (L2), (L18), (L19); expand]

(L21) $|(1+t_q)(1+\delta_s) - 1| \le (1+u)^2 - 1$
[Lemma G.4 at $k = 2$, $c_1 = c_2 := u$; (L18), (L19)]

(L22) $|(1+t_q)(1+\delta_s)| \le (1+u)^2$
[(L21); Fact A.41, item 1]

(L23) $\forall j\ \forall \psi :\ |\widetilde{t}_j - t_j| \le e_p(\gamma'_j, \delta_j)(1+u)^2/q + H\gamma'_j((1+u)^2 - 1)/q$
[(L8), (L9), (L17), (L20), (L21), (L22); $|s_j| = 1/q$ (the proof's block); Fact A.41, item 1]

(L24) $\forall \psi :\ |\widetilde{t}_0(\psi) - t_0(\psi)| \le e_t(\gamma'_{FG}, \delta_{FG})$
[(L23) at $j = 0$; e_t (the statement); the proof's block]

(L25) $\Rightarrow$ item 1
[(L24)]

(L26) $\forall \psi :\ |\widetilde{t}_1(\psi) - t_1(\psi)| \le e_t(\gamma'_{fg}, \delta_{fg})$
[(L23) at $j = 1$; e_t (the statement); the proof's block]

(L27) $\Rightarrow$ item 2
[(L26)]

□ (items 1 and 2)

Proof of item 3.

(L28) $\|e_{\text{root}}\|^2 = \frac{2}{n}\sum_{\psi}(|\widetilde{t}_0(\psi) - t_0(\psi)|^2 + |\widetilde{t}_1(\psi) - t_1(\psi)|^2)$
[$e_{\text{root}} = \widetilde{t} - t$ (line 20); the coefficient norm over the $n/2$ roots (Proposition G.15; Appendix G.5)]

(L29) $\frac{2}{n}\sum_{\psi}(|\widetilde{t}_0(\psi) - t_0(\psi)|^2 + |\widetilde{t}_1(\psi) - t_1(\psi)|^2) \le e_t(\gamma'_{FG}, \delta_{FG})^2 + e_t(\gamma'_{fg}, \delta_{fg})^2$
[items 1 and 2 over the $n/2$ roots]

(L30) $\Rightarrow$ $\|e_{\text{root}}\| \le \bar{e}_{\text{root}}$
[(L28), (L29); $t \mapsto \sqrt{t}$ nondecreasing on $[0, \infty)$ (Fact A.41, item 5); $\bar{e}_{\text{root}}$ (the statement)]

(L31) $\Rightarrow$ item 3
[(L30)]

□ (item 3)

J.4 The base sampler's perturbation budget

Structure. Appendix J.4.1 states the exponent and the acceptance; Appendix J.4.2 the fringe set of a leaf.

J.4.1 The exponent and the acceptance

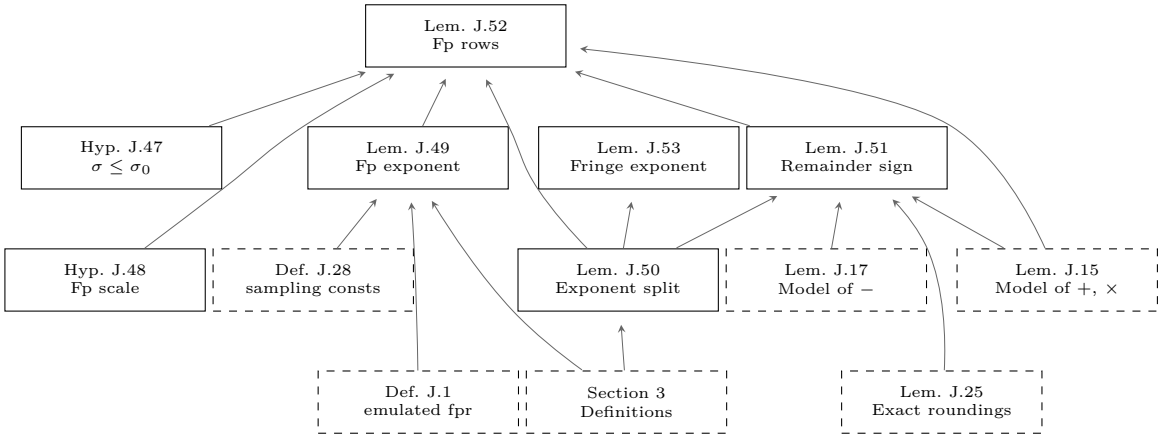


Figure 105: Dependencies, Appendix J.4.1.

Structure. **Hypothesis J.47** states the leaf standard deviations below σ_0; **Hypothesis J.48** the computed scale below 1; Lemma J.49 the exponent's argument; Lemmas J.50 and J.51 its split; Lemma J.52 the acceptance on each row; Lemma J.53 the points at which the shift saturates.

Hypothesis J.47 (Leaf standard deviations below σ_0 [to table])**.** A mathematical hypothesis: no computed leaf standard deviation exceeds the base sampler's σ_0. Define:

- $\sigma_0 := 1.8205$, line 9 of SamplerZ (Algorithm 8).

We assume

$$\forall i \le N \ \forall z_{<i} : \quad \widetilde{\sigma}_i(z_{<i}) \le \sigma_0.$$

[L3: mathematical]

Hypothesis J.48 (The floating-point signer's scale [to table])**.** A mathematical hypothesis: the base sampler's computed scale $\widetilde{ccs}$ stays below 1. Define:

- $\widetilde{\texttt{isigma}} := 1/\sigma_1$, that of line 1 of deepest (Algorithm 7) in $\mathcal{F}$;
- $\sigma_{\min} := \texttt{SIGMA_MIN}[\log_2 n]$ [L0: `sign_sampler.c:21-30`] [L0: `fxp/fxp_consts.h:2073`];
- $\widetilde{ccs} := \mathrm{fl}(\widetilde{\texttt{isigma}} \cdot \sigma_{\min})$, line 6 of SamplerZ (Algorithm 8), the value the code passes to BerExp (Algorithm 9).

We assume

1. $\widetilde{ccs} < 1$.

[L3: mathematical]

Lemma J.49 (The floating-point exponent [to table])**.** *The argument of the exponent that SamplerZ computes in $\mathcal{F}$ lies within one rounding of the argument over $\mathbb{R}$ plus the propagated perturbations of its two terms.* ***Under Hypothesis J.31****, let:*

- $\sigma = 1/\texttt{isigma}$*, the input of SamplerZ (Algorithm 8).*

Define:

- $u = 2^{-53}$*, that of Definition J.1;*
- $z \in [-18, 19]$*, that of line 10 of SamplerZ (Algorithm 8);*
- $r \in [0, 1)$*, that of line 3;*
- s*, that of line 1;*
- dss*,* a_x*,* b_x *and* x*, the values SamplerZ (Algorithm 8) names over $\mathbb{R}$, lines 1 to 16;*
- σ_0 *and* C_0*, those of SamplerZ (Algorithm 8), Require;*
- z_0*, that of line 9;*
- $\widetilde{r}$*,* $\widetilde{dss}$*,* $\widetilde{a}_x$*,* $\widetilde{b}_x$ *and* $\widetilde{x}$*, the values SamplerZ computes in $\mathcal{F}$ at lines 2 to 15.*

Then

$$|\widetilde{x}-x| \le u|x| + (1+u)\big[(2|z-r|\,r\,u+r^2u^2)(1+u)^5\,dss + ((1+u)^5-1)a_x + ((1+u)^2-1)b_x\big]. \qquad \textit{[derived]}$$

Proof.

DEFINES $P = (1+t_1)^2(1+t_2)(1+t_3)(1+t_4)$, with $t_1,\dots,t_4$ of (L2) to (L5)

(L1) $\exists\, t_0 \in \mathbb{R},\ |t_0| \le u:\ \widetilde{r} = r(1+t_0)$
[Definition A.4, item 1, at line 2; **Hypothesis J.31, item (1)**]

(L2) $\exists\, t_1 \in \mathbb{R},\ |t_1| \le u:\ \mathrm{fl}(z-\widetilde{r}) = (z-\widetilde{r})(1+t_1)$
[Definition A.4, item 1; **Hypothesis J.31, item (1)**]

(L3) $\exists\, t_2 \in \mathbb{R},\ |t_2| \le u:\ \mathrm{fl}(\mathrm{fl}(z-\widetilde{r})^2) = \mathrm{fl}(z-\widetilde{r})^2(1+t_2)$
[Definition A.4, item 1; **Hypothesis J.31, item (1)**]

(L4) $\exists\, t_3 \in \mathbb{R},\ |t_3| \le u:\ \widetilde{dss} = dss(1+t_3)$
[Definition A.4, item 1, at $\mathrm{fl}(\texttt{isigma}^2)$; $\mathrm{fl}(x/2) = x/2$ (Definition J.1); **Hypothesis J.31, item (1)**]

(L5) $\exists\, t_4 \in \mathbb{R},\ |t_4| \le u:\ \widetilde{a}_x = \mathrm{fl}(\mathrm{fl}(z-\widetilde{r})^2)\,\widetilde{dss}(1+t_4)$
[Definition A.4, item 1; **Hypothesis J.31, item (1)**]

(L6) $\widetilde{a}_x = (z-\widetilde{r})^2 P\,dss$
[(L2) to (L5); P (the block)]

(L7) $\exists\, t_6, t_7 \in \mathbb{R},\ |t_6|, |t_7| \le u:\ \widetilde{b}_x = b_x(1+t_6)(1+t_7)$
[Definition A.4, item 1, at the stored $C_0 = \mathrm{fl}(1/(2\sigma_0^2))$ (Definition J.28) and at the product; $\mathrm{fl}(z_0^2) = z_0^2$ (Definition J.1); **Hypothesis J.31, item (1)**]

(L8) $\exists\, t_8 \in \mathbb{R},\ |t_8| \le u:\ \widetilde{x} = (\widetilde{a}_x - \widetilde{b}_x)(1+t_8)$
[Definition A.4, item 1, at line 15; **Hypothesis J.31, item (1)**]

(L9) $(z-\widetilde{r})^2 - (z-r)^2 = -2(z-r)\,r\,t_0 + r^2t_0^2$
[(L1)]

(L10) $|(z-\widetilde{r})^2 - (z-r)^2| \le 2|z-r|\,r\,u + r^2u^2$
[(L9); $|t_0| \le u$ (L1); $r \ge 0$ (the statement)]

(L11) $\widetilde{a}_x - a_x = ((z-\widetilde{r})^2 - (z-r)^2)P\,dss + a_x(P-1)$
[(L6); $a_x = (z-r)^2 dss$ (line 16)]

(L12) $P \in (0, (1+u)^5]$
[Lemma G.2 at $k=5$; $u < 1$ (the statement)]

(L13) $|P-1| \le (1+u)^5 - 1$
[Lemma G.2 at $k=5$]

(L14) $a_x, b_x, dss \ge 0$
[$dss = 1/(2\sigma^2)$, $a_x = (z-r)^2 dss$, $b_x = z_0^2 C_0$ (SamplerZ (Algorithm 8), lines 1 to 16); $C_0 > 0$ (SamplerZ, Require); Fact A.41, items 13 and 8]

(L15) $|\widetilde{a}_x - a_x| \le (2|z-r|\,r\,u + r^2u^2)(1+u)^5\,dss + ((1+u)^5-1)\,a_x$
[(L10) to (L13); (L14)]

(L16) $|\widetilde{b}_x - b_x| \le ((1+u)^2-1)\,b_x$
[(L7); Lemma G.2 at $k=2$; (L14)]

(L17) $\widetilde{x} - x = (a_x - b_x)t_8 + ((\widetilde{a}_x - a_x) - (\widetilde{b}_x - b_x))(1+t_8)$
[(L8); $x = a_x - b_x$ (line 16)]

(L18) $|\widetilde{x} - x| \le u|x| + (1+u)(|\widetilde{a}_x - a_x| + |\widetilde{b}_x - b_x|)$
[(L17); $|t_8| \le u$ (L8); Fact A.41, item 1]

(L19) $|\widetilde{x}-x| \le u|x| + (1+u)\big[(2|z-r|\,r\,u+r^2u^2)(1+u)^5\,dss + ((1+u)^5-1)a_x + ((1+u)^2-1)b_x\big]$
[(L15), (L16), (L18)]

(L20) $\Rightarrow$ the statement
[(L19)]

□

Lemma J.50 (The floating-point exponent's split [to table])**.** *The split of* BerExp *returns a non-negative quotient at most the argument times the stored* $1/\ln 2$*, rounded up, and its reconstruction lies within a bound of the argument.* ***Under Hypothesis J.31****, let:*

- $x \in \mathcal{F}$.

Define:

- $u = 2^{-53}$*, that of Definition J.1;*
- si *and* $r' = \widetilde{r}'$*, the values* BerExp *(Algorithm 9) computes in* $\mathcal{F}$ *on the input* x*, lines 2 and 3; the floating-point signer has no clamp at line 4;*
- `LOG2` *and* `INV_LOG2`*, those of* BerExp *(Algorithm 9), Require.*

Assume:

(A1) $x \geq 0$.

Measured `verify/reports/sampler/glitch.py`*:*

- $\texttt{INV_LOG2} \cdot \texttt{LOG2}\,(1+u) = 1 + 0.572\,u$.

Then

1. $0 \leq si \leq x\,\texttt{INV_LOG2}\,(1+u)$;
2. $|(si \ln 2 + r') - x| \leq u|x| + (1+u)\,si\,(|\texttt{LOG2} - \ln 2| + u\,\texttt{LOG2})$. *[derived]*

Proof. (L1) $\exists\, t_9 \in \mathbb{R},\ |t_9| \leq u:\ \mathrm{fl}(x \cdot \texttt{INV_LOG2}) = x \cdot \texttt{INV_LOG2}\,(1+t_9)$
[Definition A.4, item 1; **Hypothesis J.31, item (1)**]

(L2) $si = \mathrm{trunc}(\mathrm{fl}(x \cdot \texttt{INV_LOG2}))$
[line 2 of BerExp (Algorithm 9)]

(L3) $si \in [0, x \cdot \texttt{INV_LOG2}\,(1+t_9)]$
[(L1), (L2); $\mathrm{trunc}\, w \in [0, w]$ at $w \geq 0$ ($\mathrm{trunc}\, w = \mathrm{sgn}(w)\lfloor |w| \rfloor$, Fact J.2, item 5; Fact A.41, item 22); $x \geq 0$ (assumption A1); $\texttt{INV_LOG2} > 0$]

(L4) $si \in [0, x\,\texttt{INV_LOG2}\,(1+u)]$
[(L3); $|t_9| \leq u$ ((L1))]

(L5) $\Rightarrow$ item 1
[(L4)]

(L6) $\exists\, t_{10}, t_{11} \in \mathbb{R},\ |t_{10}|, |t_{11}| \leq u:\ r' = (x - si \cdot \texttt{LOG2}\,(1+t_{10}))(1+t_{11})$
[Definition A.4, item 1, at the product and the subtraction of line 3; **Hypothesis J.31, item (1)**]

(L7) $(si \ln 2 + r') - x = (x - si\,\texttt{LOG2})t_{11} - si\,\texttt{LOG2}\,t_{10}(1+t_{11}) + si(\ln 2 - \texttt{LOG2})$
[(L6)]

(L8) $\texttt{INV_LOG2} \cdot \texttt{LOG2}\,(1+u) < 2$
[the measured row]

(L9) $0 \leq si\,\texttt{LOG2}$
[(L4); $\texttt{LOG2} > 0$]

(L10) $si\,\texttt{LOG2} \leq 2x$
[(L4), (L8)]

(L11) $|x - si\,\texttt{LOG2}| \leq x$
[(L9), (L10)]

(L12) $|(x - si\,\texttt{LOG2})t_{11}| \leq ux$
[(L11); $|t_{11}| \leq u$ (L6)]

(L13) $|si\,\texttt{LOG2}\,t_{10}(1+t_{11})| \leq u(1+u)\,si\,\texttt{LOG2}$
[$|t_{10}|, |t_{11}| \leq u$ (L6); $si \geq 0$ (L4)]

(L14) $si|\ln 2 - \texttt{LOG2}| \leq (1+u)\,si|\texttt{LOG2} - \ln 2|$
[$u \geq 0$ (the statement); $si \geq 0$ (L4)]

(L15) $|(si \ln 2 + r') - x| \leq u|x| + (1+u)\,si(|\texttt{LOG2} - \ln 2| + u\,\texttt{LOG2})$
[(L7), (L12), (L13), (L14); Fact A.41, item 1; $x = |x|$ (assumption A1)]

(L16) $\Rightarrow$ item 2

[(L15)]

□ (items 1 and 2)

Lemma J.51 (Nonnegativity of the split's remainder [to table])**.** *Below the largest argument a candidate reaches, the remainder of the split is nonnegative.* ***Under Hypothesis J.31****, let:*

- $x \in \mathcal{F}$.

Define:

- u, LOG2 *and* INV_LOG2*, those of Lemma J.50;*
- $\sigma_{\min}$ *and* C_0*, those of* SamplerZ *(Algorithm 8), Require, at either degree;*
- si *and* r'*, those of Lemma J.50 on the input* x*;*
- $x_c = 19^2/(2\sigma_{\min}^2) - 18^2 C_0$.

Assume:

(A1) $0 \le x \le x_c$.

Measured [gate: verify/gates/sampler/rpos.py]:

- *The windows: every binary64* x *within relative* 2^{-44} *of* $\mathrm{fl}(k\,\mathtt{LOG2})$, $k = 1, \ldots, 240$*;*
- *The inputs run in the windows: 174596;*
- *The inputs in the windows with* $r' < 0$*: 0;*
- $x_c\,\mathtt{INV_LOG2}\,(1+u) < 240$ *at both degrees.*

Then

$$r' \ge 0.$$

Proof. (L1) $r' = \mathrm{fl}(x - \mathrm{fl}(si\,\mathtt{LOG2}))$

[line 3 of BerExp (Algorithm 9); no clamp (Lemma J.50); **Hypothesis J.31**, named by Lemma J.50]

(L2) $\mathrm{fl}(si\,\mathtt{LOG2}) \le x \Rightarrow\ r' \ge 0$

[(L1); fl nondecreasing with $\mathrm{fl}(0) = 0$ (Fact J.2, item 8)]

(L3) $si\,\mathtt{LOG2} \le x(1 + 0.572\,u)$

[Lemma J.50, item 1; the measured row of Lemma J.50; its $x \ge 0$ by assumption A1; **Hypothesis J.31**, named by Lemma J.50]

(L4) $si\,\mathtt{LOG2} \ge 0$

[$si \ge 0$ (Lemma J.50, item 1); $\mathtt{LOG2} > 0$; Fact A.41, item 8]

(L5) $\mathrm{fl}(si\,\mathtt{LOG2}) \le si\,\mathtt{LOG2}\,(1+u)$

[Definition A.4, item 1; **Hypothesis J.31, item (1)**; (L4)]

(L6) $\mathrm{fl}(si\,\mathtt{LOG2}) > x \Rightarrow\ x - si\,\mathtt{LOG2} < u\,si\,\mathtt{LOG2}$

[(L5)]

(L7) $si\,\mathtt{LOG2} - x \le 0.572\,u\,x$

[(L3)]

(L8) $\mathrm{fl}(si\,\mathtt{LOG2}) > x \Rightarrow\ si\,\mathtt{LOG2} - x \le 0.572\,u(1+u)\,si\,\mathtt{LOG2}$

[(L5), (L7)]

(L9) $\mathrm{fl}(si\,\mathtt{LOG2}) > x \Rightarrow\ |x - si\,\mathtt{LOG2}| \le 2^{-45}\,si\,\mathtt{LOG2}$

[(L6), (L8); $0.572\,u(1+u) \le 2^{-45}$ and $u \le 2^{-45}$ at $u = 2^{-53}$]

(L10) $si < 240$

[Lemma J.50, item 1; $x \le x_c$ (assumption A1); the last measured row; **Hypothesis J.31**, named by Lemma J.50]

(L11) $\forall k \ge 1:\ |x - k\,\mathtt{LOG2}| \le 2^{-45} k\,\mathtt{LOG2} \Rightarrow\ |x - \mathrm{fl}(k\,\mathtt{LOG2})| \le 2^{-44}\,\mathrm{fl}(k\,\mathtt{LOG2})$

[$|\mathrm{fl}(k\,\mathtt{LOG2}) - k\,\mathtt{LOG2}| \le u\,k\,\mathtt{LOG2}$ (Definition A.4, item 1); $u \le 2^{-46}$]

(L12) $\mathrm{fl}(si\,\mathtt{LOG2}) > x \Rightarrow\ r' \ge 0$

[(L9), (L10), (L11); no input in the windows with $r' < 0$ (the third measured row); the gate's binary64 $\times$ and $-$: the code's (Lemma J.15, item 1; Lemma J.17, item 1), its truncation exact (Lemma J.25, item 1)]

(L13) $r' \ge 0$

[(L2), (L12)]

(L14) $\Rightarrow$ the statement

[(L13)]

□

Lemma J.52 (The floating-point acceptance per row [to table])**.** *On a candidate of a given row, the computed acceptance is within the row's relative bound of the exact one below the saturation; at the saturation the row is one that can hold a fringe candidate, and the acceptance is below* 2^{-64} *in both.* ***Under Hypotheses J.31****,* *J.48* *and* *J.47****,*** *define:*

- *The signer's words and parameters*
  - $\sigma_{\min}$ *and* σ_0*, those of* SamplerZ *(Algorithm 8), Require;*
  - `LOG2` *and* `INV_LOG2`*, those of Lemma J.50;*
  - $\bar{\delta}$*, that of Lemma 4.7, precondition 4;*
- *The exponent*
  - u*,* z*,* r*,* σ*,* dss*,* z_0*,* a_x*,* b_x*,* x *and* $\widetilde{x}$*, those of Lemma J.49;*
  - $k := z_0$*;*
- *The split*
  - si *and* r'*, those of Lemma J.50 on the input* $\widetilde{x}$*;*
  - x_c*, that of Lemma J.51;*
- *The acceptance*
  - ccs *and* $\widetilde{ccs}$*, those of lines 7 and 6 of* SamplerZ *(Algorithm 8);*
  - y *and* L*, those of Lemma H.25 at* $(r', \widetilde{ccs})$*;*
  - z_{acc}*, that of Fact G.66;*
  - $acc := \widetilde{ccs}\, e^{-x}$*;*
  - $\widetilde{acc} := z_{\text{acc}}/2^{64}$*;*
  - $e_{acc} := \widetilde{acc}/acc - 1$*;*
  - $e_{\text{fl}} := 2^{-63}/acc$*;*
- *The row bounds*
  - $e_{\text{poly}} := 2^{-51.05}$*;*
  - $\forall k \le 18:\ a_k := (k+1)^2/(2\sigma_{\min}^2)$*;*
  - $\forall k \le 18:\ b_k := k^2/(2\sigma_0^2)$*;*
  - $\forall k \le 18:\ x_k := \max(a_k, b_k)$*;*
  - $\forall k \le 18:\ E^{\text{fp}}_{x,k} := u\,x_k + (1+u)\big[(2(k+1)u+u^2)(1+u)^5/(2\sigma_{\min}^2) + ((1+u)^5-1)a_k + ((1+u)^2-1)b_k\big]$*;*
  - $\forall k \le 18:\ si_k := \min(63, \lfloor (x_k + E^{\text{fp}}_{x,k})\,\texttt{INV_LOG2}\,(1+u)\rfloor)$*;*
  - $\forall k \le 18:\ E^{\text{fp}}_{s,k} := u(x_k + E^{\text{fp}}_{x,k}) + (1+u)\,si_k\,(|\texttt{LOG2} - \ln 2| + u\,\texttt{LOG2})$*;*
  - $\forall k \le 18:\ e_{+,k} := e^{E^{\text{fp}}_{x,k} + E^{\text{fp}}_{s,k}}(1+e_{\text{poly}}) - 1$*;*
  - $\mathcal{K}_C := \{\, k \le 18 : a_k - b_k + E^{\text{fp}}_{x,k} \ge 64/(\texttt{INV_LOG2}\,(1+u)) \,\}$.

Assume:

(A1) $\sigma \in [\sigma_{\min}, \sigma_0]$*;*

(A2) $\sigma \le 1.17^2\sigma_{\min}(1+\bar{\delta})$.

Measured at the stored words, at $n = 512$ *and* $n = 1024$ *`verify/reports/fp/terms.py`:*

- $1/(2(1.17^2\sigma_{\min}(1+\bar{\delta}))^2) - 1/(2\sigma_0^2) - E^{\text{fp}}_{x,18} \ge 0.007$*;*
- $x_c - 64/(\texttt{INV_LOG2}\,(1-u)) \ge 13.846$*;*
- $64/(\texttt{INV_LOG2}\,(1+u)) - E^{\text{fp}}_{x,18} - 63\ln 2 \ge 0.693$*;*
- $L - \max_{si\in\{0,63\}}((si+1)/(\texttt{INV_LOG2}\,(1-u)) - si\ln 2) - \max_k E^{\text{fp}}_{s,k} \ge 2^{-30.01}$*;*
- $\min \mathcal{K}_C$*: 15 at* $n = 512$*, 16 at* $n = 1024$.

Measured [gate: `verify/gates/sampler/sigma_ccs.py`]:

- $\sigma_0 < 2\sigma_{\min}$.

Then

1. *Assume:*

(A3) $si \le 63$.

Then $e_{acc} \in [-e_{+,k} - e_{\mathrm{fl}}, e_{+,k}]$.

2. *Assume:*

(A4) $si \ge 64$.

Then $k \in \mathcal{K}_C$.

3. *Assume:*

(A5) $si \ge 64$.

Then $e_{\mathrm{fl}} \ge 1$.

4. *Assume:*

(A6) $si \ge 64$.

Then $|e_{acc}| \le e_{\mathrm{fl}}$.

5. $\widetilde{ccs} \in [1/2, 1)$.

6. $\widetilde{ccs} \ge (1-u)\, ccs$.

Proof. (L1) $k \le 18$

[$k = z_0$ (the statement); $z_0 \in \{0, \dots, 18\}$ (Lemma G.64)]

(L2) $|z - r| \le k + 1$

[$z \in \{-k, k+1\}$ (line 10); $r \in [0, 1)$]

(L3) $a_x \le a_k$

[(L2); $dss \le 1/(2\sigma_{\min}^2)$ (Lemma H.24, item 3); $a_x = (z-r)^2 dss$ (the statement); its $\sigma \ge \sigma_{\min}$ by assumption A1]

(L4) $b_x = b_k$

[$b_x = z_0^2/(2\sigma_0^2)$ (the statement); $k = z_0$ (the statement)]

(L5) $|x| \le x_k$

[$x = a_x - b_x$ (the statement), $a_x, b_x \ge 0$ (Lemma J.49, (L14)); (L3), (L4); **Hypothesis J.31**, named by Lemma J.49]

(L6) $|\widetilde{x} - x| \le E_{x,k}^{\mathrm{fp}}$

[Lemma J.49; (L2) to (L5); $r < 1$ (Lemma J.49); $E_{x,k}^{\mathrm{fp}}$ (the statement); **Hypothesis J.31, item (1)**]

(L7) $\widetilde{x} \ge 0$

[at $k = 0$: $\widetilde{b}_x = \mathrm{fl}(0)$, $\mathrm{fl}(0) = 0$ and $\widetilde{x} = \mathrm{fl}(\widetilde{a}_x)$, $\mathrm{fl}(\widetilde{a}_x) \ge 0$ (Definition J.1)]

(L8) $x \ge k^2(dss - 1/(2\sigma_0^2))$

[at $k \ge 1$: $|z - r| \ge k$ ((L2)'s $z \in \{-k, k+1\}$, $r \in [0, 1)$); $x = (z-r)^2 dss - k^2/(2\sigma_0^2)$ (the statement)]

(L9) $dss - 1/(2\sigma_0^2) \ge 1/(2(1.17^2 \sigma_{\min}(1+\bar{\delta}))^2) - 1/(2\sigma_0^2)$

[$dss = 1/(2\sigma^2)$ (the statement); $\sigma \le 1.17^2 \sigma_{\min}(1+\bar{\delta})$ (assumption A2)]

(L10) $\forall k \le 18 : \; E_{x,k}^{\mathrm{fp}} \le E_{x,18}^{\mathrm{fp}}$

[$E_{x,k}^{\mathrm{fp}}$ (the statement); $a_k \le a_{k+1}$, $b_k \le b_{k+1}$, $x_k \le x_{k+1}$ (a_k, b_k, x_k, the statement; Fact A.41, item 5; Fact A.41, item 20)]

(L11) $x > E_{x,18}^{\mathrm{fp}}$

[at $k \ge 1$: (L8), (L9); the first measured row]

(L12) $\Rightarrow \; x > E_{x,k}^{\mathrm{fp}}$

[(L11), (L10)]

(L13) $\widetilde{x} \ge 0$

[at $k \ge 1$: (L6), (L12)]

(L14) $\mathrm{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}) \ge \widetilde{x} \cdot \texttt{INV_LOG2}\,(1-u)$

[(L7), (L13); Lemma J.15, item 2, at $\circ = \times$, or $\mathrm{fl}(0) = 0$ (Fact J.2, item 4); **Hypothesis J.31, item (1)**]

(L15) $si \le 63 \Rightarrow\ \widetilde{x} < 64/(\texttt{INV_LOG2}\,(1-u))$

[(L14); $si = \mathrm{trunc}(\mathrm{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}))$ (line 2)]

(L16) $64/(\texttt{INV_LOG2}\,(1-u)) < x_c$

[the second measured row]

(L17) $si \le 63 \Rightarrow\ r' \ge 0$

[(L7), (L13), (L15), (L16); Lemma J.51 at $x := \widetilde{x} \in [0, x_c]$; **Hypothesis J.31, item (1)**]

(L18) $si \le 63 \Rightarrow\ si \le si_k$

[Lemma J.50, item 1, at $x := \widetilde{x}$; $\widetilde{x} \le x_k + E^{\mathrm{fp}}_{x,k}$ ((L5), (L6)); si_k (the statement); **Hypothesis J.31, item (1)**]

(L19) $si \le 63 \Rightarrow\ |(si \ln 2 + r') - \widetilde{x}| \le E^{\mathrm{fp}}_{s,k}$

[Lemma J.50, item 2, at $x := \widetilde{x}$; (L5), (L6), (L18); $E^{\mathrm{fp}}_{s,k}$ (the statement); **Hypothesis J.31, item (1)**]

(L20) $si \le 63 \Rightarrow\ \mathrm{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}) < si + 1$

[$si = \mathrm{trunc}(\mathrm{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}))$ (BerExp (Algorithm 9), line 2)]

(L21) $si \le 63 \Rightarrow\ \widetilde{x} < (si+1)/(\texttt{INV_LOG2}\,(1-u))$

[(L14), (L20)]

(L22) $si \le 63 \Rightarrow\ r' \le \widetilde{x} - si \ln 2 + E^{\mathrm{fp}}_{s,k}$

[(L19)]

(L23) $si \le 63 \Rightarrow\ r' < (si+1)/(\texttt{INV_LOG2}\,(1-u)) - si \ln 2 + \max_k E^{\mathrm{fp}}_{s,k}$

[(L21), (L22)]

(L24) $\max_{0 \le si \le 63}\big((si+1)/(\texttt{INV_LOG2}\,(1-u)) - si \ln 2\big) = \max_{si \in \{0,63\}}\big((si+1)/(\texttt{INV_LOG2}\,(1-u)) - si \ln 2\big)$

[Fact A.41, item 16, in si over $[0, 63]$, both ends among the si]

(L25) $si \le 63 \Rightarrow\ r' \le L$

[(L23), (L24); the fourth measured row]

(L26) $\widetilde{ccs}\ \mathcal{I}\,(u^{\pm}, 0)\ ccs$

[Lemma J.15, item 2, at $\circ = \times$ (line 6); **Hypothesis J.31, item (1)**]

(L27) $ccs = \sigma_{\min}/\sigma$

[$ccs = \texttt{isigma} \cdot \sigma_{\min}$ (line 7)]

(L28) $ccs \ge \sigma_{\min}/\sigma_0$

[(L27); $\sigma \le \sigma_0$ (assumption A1; **Hypothesis J.47**)]

(L29) $\sigma_{\min}/\sigma_0 > 1/2$

[$\sigma_0 < 2\sigma_{\min}$ (the statement's measured row)]

(L30) $\Rightarrow\ ccs > 1/2$

[(L28), (L29)]

(L31) $\widetilde{ccs} \ge 1/2$

[(L30); fl nondecreasing with $\mathrm{fl}(1/2) = 1/2$ (Fact J.2, item 8)]

(L32) $\widetilde{ccs} < 1$

[**Hypothesis J.48, item 1**]

(L33) $\widetilde{ccs} \in [1/2, 1)$

[(L31), (L32)]

(L34) $\Rightarrow$ item 5

[(L33)]

(L35) $\widetilde{ccs} \ge (1-u)\,ccs$

[(L26)]

(L36) $\Rightarrow$ item 6

[(L35)]

(L37) $si \le 63 \Rightarrow\ y/(\widetilde{ccs}\,e^{-r'}) \in [1 - e_{\mathrm{poly}},\ 1 + e_{\mathrm{poly}}]$

[(L17), (L25), (L33); Lemma H.25 at $(r', \widetilde{ccs})$; e_{poly} (the statement)]

(L38) $si \le 63 \Rightarrow\ acc_c = y\,2^{-si}$

[Lemma H.26, item 3; y (Lemma H.25); its assumptions by assumption A3; $si \ge 0$ (Lemma J.50, item 1,

at $x := \widetilde{x}$, its assumption A1 by (L7) and (L13)), assumption A1 of Lemma H.26; $2^{63}y \geq 1$ ((L25), (L33), (L37)), assumption A2 of Lemma H.26; **Hypothesis J.31**, named by Lemma J.50]

(L39) $\widetilde{acc} \in [acc_c - 2 \cdot 2^{-64}, acc_c]$

[Lemma H.26, item 1; $\widetilde{acc}$ (the statement); its assumptions by assumption A3; $si \geq 0$ (Lemma J.50, item 1, at $x := \widetilde{x}$, its assumption A1 by (L7) and (L13)), assumption A1 of Lemma H.26; $2^{63}y \geq 1$ ((L25), (L33), (L37)), assumption A2 of Lemma H.26; **Hypothesis J.31**, named by Lemma J.50]

(L40) $2^{-si} = e^{-si \ln 2}$

[$e^{\ln 2} = 2$; Fact A.41, item 12]

(L41) $2 \cdot 2^{-64}/acc = e_{\text{fl}}$

[e_{fl} (the statement)]

(L42) $si \leq 63 \Rightarrow \; e_{acc} \in [e^{-(E^{\text{fp}}_{x,k}+E^{\text{fp}}_{s,k})}(1 - e_{\text{poly}}) - 1 - e_{\text{fl}}, e_{+,k}]$

[(L6), (L19), (L37) to (L41); $acc = \widetilde{ccs}\, e^{-x}$, e_{acc}, $e_{+,k}$ (the statement)]

(L43) $\forall E, p \geq 0 : \; p(e^E - e^{-E}) \geq 0$

[$e^{-E} \leq e^E$ at $E \geq 0$ (Fact A.41, item 5); Fact A.41, item 8]

(L44) $\forall E, p \geq 0 : \; 1 - e^{-E}(1 - p) \leq e^E(1 + p) - 1$

[$e^E + e^{-E} \geq 2$ (Fact A.41, item 21); (L43)]

(L45) $si \leq 63 \Rightarrow \; e_{acc} \in [-e_{+,k} - e_{\text{fl}}, e_{+,k}]$

[(L42), (L44) at $E := E^{\text{fp}}_{x,k} + E^{\text{fp}}_{s,k}$, $p := e_{\text{poly}}$]

(L46) $\Rightarrow$ item 1

[(L45)]

(L47) $\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}) \leq \widetilde{x} \cdot \texttt{INV_LOG2}\,(1 + u)$

[(L7), (L13); Lemma J.15, item 2, at $\circ = \times$; **Hypothesis J.31, item (1)**]

(L48) $si \geq 64 \Rightarrow \; \widetilde{x} \geq 64/(\texttt{INV_LOG2}\,(1 + u))$

[(L47); $\text{fl}(\widetilde{x} \cdot \texttt{INV_LOG2}) \geq si$ (line 2)]

(L49) $x \in [\widetilde{x} - E^{\text{fp}}_{x,k}, a_k - b_k]$

[(L3), (L4), (L6)]

(L50) $si \geq 64 \Rightarrow \; a_k - b_k + E^{\text{fp}}_{x,k} \geq 64/(\texttt{INV_LOG2}\,(1 + u))$

[(L48), (L49)]

(L51) $si \geq 64 \Rightarrow \; k \in \mathcal{K}_C$

[(L1), (L50); $\mathcal{K}_C$ (the statement); assumption A4]

(L52) $\Rightarrow$ item 2

[(L51)]

(L53) $si \geq 64 \Rightarrow \; x \geq 63 \ln 2$

[(L10), (L48), (L49); the third measured row]

(L54) $acc \leq e^{-x}$

[$acc = \widetilde{ccs}\, e^{-x}$ (the statement); (L32)]

(L55) $si \geq 64 \Rightarrow \; e_{\text{fl}} \geq 1$

[$acc \leq 2^{-63}$ ((L53), (L54)); e_{fl} (the statement); assumption A5]

(L56) $\Rightarrow$ item 3

[(L55)]

(L57) $si \geq 64 \Rightarrow \; z_{\text{acc}} \leq 1$

[Fact G.66: $s_x = 63$ and $z_{\text{acc}} = ((P \ll 1) - 1) \gg 63$ with $P < 2^{63}$; assumption A1 of Fact G.66 at $si \geq 64$]

(L58) $si \geq 64 \Rightarrow \; e_{acc} \in [-1, e_{\text{fl}}/2 - 1]$

[$\widetilde{acc} \in [0, 2^{-64}]$ ((L57)); e_{acc}, e_{fl} (the statement)]

(L59) $si \geq 64 \Rightarrow \; |e_{acc}| \leq e_{\text{fl}}$

[(L55), (L58); assumption A6]

(L60) $\Rightarrow$ item 4

[(L59)]

□ (items 1 to 6)

Lemma J.53 (A fringe candidate's exponent [to table])**.** *At the saturation, the argument of the exponent is at least* $64 \ln 2\,(1-3u)$*.* ***Under Hypothesis J.31****, let:*

- $\sigma = 1/\texttt{isigma}$*, the input of* SamplerZ *(Algorithm 8).*

Define:

- $z \in [-18, 19]$*, that of line 10 of* SamplerZ *(Algorithm 8);*
- $r \in [0, 1)$*, that of line 3;*
- x*,* z_0 *and* u*, those of Lemma J.49;*
- C_0*, that of* SamplerZ *(Algorithm 8), Require;*
- si*,* LOG2 *and* INV_LOG2*, those of Lemma J.50 on the input* x*.*

Assume:

(A1) $x \geq 0$*;*

(A2) $si \geq 64$*.*

Measured `verify/reports/sampler/glitch.py`*:*

- $\texttt{LOG2} - \ln 2 = -2.319e-17$*.*

Then

1. $x \geq 64 \ln 2\,(1-3u)$*.*

Proof. (L1) $si \leq x\,\texttt{INV_LOG2}\,(1+u)$
[Lemma J.50, item 1; **Hypothesis J.31, item (1)**; its assumptions by assumption A1]

(L2) $x \geq \frac{si\,\texttt{LOG2}}{1+0.572\,u}$
[(L1); $\texttt{INV_LOG2} \cdot \texttt{LOG2}\,(1+u) = 1 + 0.572\,u$ (Lemma J.50, the measured row); $\texttt{LOG2} > 0$]

(L3) $|\texttt{LOG2} - \ln 2| \leq u \ln 2$
[the measured row; $u = 2^{-53}$ (the statement)]

(L4) $\texttt{LOG2} \geq (1-u) \ln 2$
[(L3)]

(L5) $1 + 0.572\,u \leq 1 + 2u$
[the measured row of Lemma J.50: $0.572 \leq 2$]

(L6) $(1-u)/(1+2u) - (1-3u) = 6u^2/(1+2u)$
[expand]

(L7) $(1-u)/(1+2u) \geq 1 - 3u$
[(L6); $6u^2/(1+2u) \geq 0$ ($u \geq 0$, Definition A.4)]

(L8) $x \geq 64 \ln 2\,(1-3u)$
[(L2), (L4), (L5), (L7); $si \geq 64$ (assumption A2)]

(L9) $\Rightarrow$ item 1
[(L8)]

□ (item 1)

J.4.2 The fringe set of a leaf

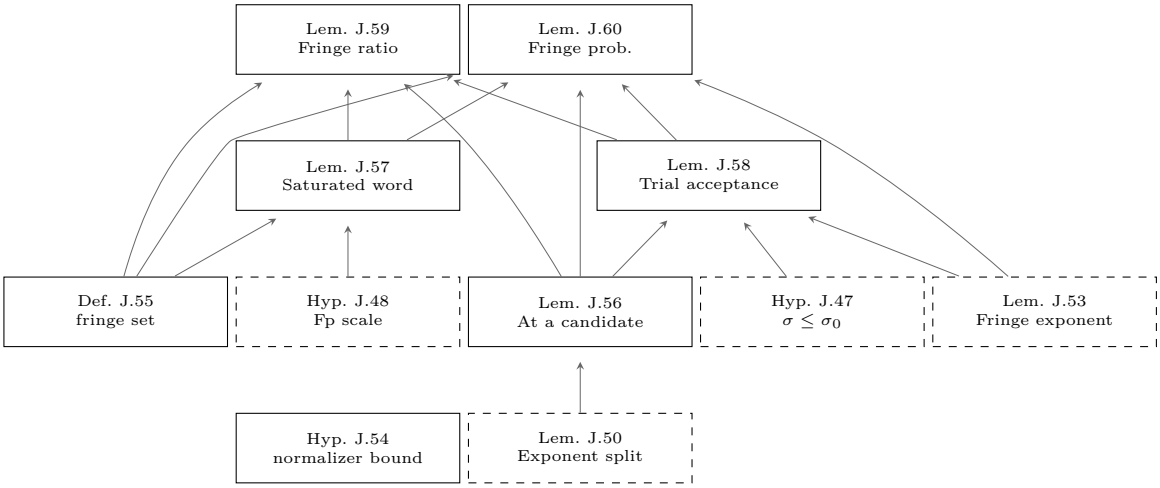


Figure 106: Dependencies, Appendix J.4.2.

Structure. **Hypothesis J.54** states the normalizer bounds at the leaves; Definition J.55 the fringe set C_i at a leaf; Lemmas J.56, J.57 and J.58 the acceptances on it; Lemma J.59 the ratio $\bar{U}$; Lemma J.60 the probability $\bar{p}_C$.

Hypothesis J.54 (The normalizer bounds at the leaves [to table])**.** A mathematical hypothesis: the normalizer of every Gaussian a leaf meets is within a factor $1 \pm \epsilon$ of its integral. Let:

- $\epsilon \in [0, 1)$.

Define:

- $\rho_{s,c}(\mathbb{Z}) := \sum_{z \in \mathbb{Z}} e^{-(z-c)^2/(2s^2)}$ (Section 3.1);
- s_i'', the s'' of Lemma 4.1 at the order α_L of Theorem F.4, $s_1 = \widetilde{\sigma}_i$ and $s_2 = \sigma_i$, at every $i \le N$ where its assumption A1 holds.

We assume

1. $\forall i \le N\ \forall s \in \{\sigma_i, \widetilde{\sigma}_i, s_i''\}\ \forall c \in \mathbb{R}:\ \rho_{s,c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\, s, (1+\epsilon)\sqrt{2\pi}\, s]$.

[L3: mathematical]

Definition J.55 (The fringe set of a leaf [to table])**.** Define:

- $\sigma_{\min}$ and σ_0, those of SamplerZ (Algorithm 8), Require.

Let:

- $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$, a leaf's computed standard deviation;
- $\widetilde{t} \in \mathbb{R}$, its computed center.

Define:

- The leaf parameters
  - $\sigma_{\max} := \sigma_0$;
  - $r := \widetilde{t} - \lfloor \widetilde{t} \rceil$;
- The probability measures
  - $\widetilde{B}$ and $\widetilde{D}$, those of Lemma G.68 at $(\widetilde{\sigma}, \widetilde{t})$, read on the candidates: at a candidate z, $\widetilde{B}(z)$ and $\widetilde{D}(z)$ are their values at its sample $\lfloor \widetilde{t} \rceil + z$ (SamplerZ (Algorithm 8), lines 1 and 18);
- The exponent
  - $x(z)$, that of Lemma J.49 at $(\widetilde{\sigma}, \widetilde{t})$, at each candidate z;
- The split
  - $si(z)$, that of Lemma J.50 on the input $x(z)$, at each candidate z;
- The fringe set

- $\mathcal{Z} := \{\, z \in \mathbb{Z} : |z - r| \le \tau\,\widetilde{\sigma} \,\}$;
- $C := \{\, z \in \mathcal{Z} \cap \mathrm{Supp}(\widetilde{B}) : si(z) \ge 64 \,\}$;
- $\bar{U}(\tau) := \max_{\widetilde{\sigma},\, \widetilde{t},\, z \in C} \widetilde{B}(z)/\widetilde{D}(z)$;
- $\bar{p}_C(\tau) := \max_{\widetilde{\sigma},\, \widetilde{t}} \widetilde{B}(C)$.

```
abbrev capSet (Z : Set Int) (B : Int -> Real) (si : Int -> Int) : Set Int :=
  {z | z in Z /\ B z != 0 /\ 64 <= si z}
```

Figure 107: The Lean declarations carrying Definition J.55: `capSet` (`Falcon.lean`); Lean's symbols in ASCII.

Lemma J.56 (The acceptance at a candidate [to table])**.** *At every candidate of a leaf, the argument and the shift are bounded, and the exact acceptance is within an exponential factor of the form the split defines.* ***Under Hypotheses J.31****, J.47 and J.48, define:*

- $\sigma_{\min}$ *and* σ_0*, those of Definition J.55.*

Let:

- $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$*, a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$*, its computed center.*

Define:

- *The signer's words and parameters*
  - $\sigma_{\max}$ *and* r*, those of Definition J.55;*
  - C_0*, that of* SamplerZ *(Algorithm 8), Require;*
- *The candidates*
  - $z \in [-18, 19]$*, those of Lemma G.64;*
  - $\bar{z}_0$*, that of Lemma G.64;*
- *The exponent*
  - u*,* z_0 *and* x*, those of Lemma J.49 at* $(\widetilde{\sigma}, \widetilde{t})$*;*
  - $g(z_0) := (z_0 + 1)^2/(2\sigma_{\min}^2) - z_0^2 C_0$*;*
  - x_c*, that of Lemma J.51;*
- *The split*
  - si*,* r'*,* `LOG2` *and* `INV_LOG2`*, those of Lemma J.50 on the input* x*;*
  - L*, that of Lemma H.25;*
  - $s_c := \lfloor x_c \,\mathtt{INV_LOG2}\,(1 + u) \rfloor$*;*
  - $E_s := u\,x_c + (1 + u)\,s_c\,(|\mathtt{LOG2} - \ln 2| + u\,\mathtt{LOG2})$*;*
- *The acceptance*
  - $ccs := \sigma_{\min}/\widetilde{\sigma}$ *(line 7 of* SamplerZ *(Algorithm 8));*
  - $acc := ccs\, e^{-x}$*.*

Measured at the stored words, at $n = 512$ *and* $n = 1024$ *[gate: verify/gates/sampler/cap_margin.py]:*

- $L - \max_{si \in \{0, s_c\}}((si + 1)/(\mathtt{INV_LOG2}\,(1 - u)) - si \ln 2) - E_s > 0$.

Measured [gate: verify/gates/sampler/sigma_ccs.py]:

- $\sigma_0 < 2\sigma_{\min}$.

Then

1. $\forall z_0, z_0' \in \{0, \ldots, 18\},\ z_0 \le z_0' :\ g(z_0) \le g(z_0')$*;*
2. $\forall z :\ x(z) \le g(\bar{z}_0(z))$*;*
3. $\forall z :\ x(z) \in [0, x_c]$*;*
4. $\forall z :\ si(z) \le s_c$*;*
5. $\forall z :\ ccs\, e^{-r'}\, 2^{-si}\, e^{-E_s} \le acc(z) \le ccs\, e^{-r'}\, 2^{-si}\, e^{E_s}$*;*

6. $\forall z:\ r'(z) \in [0, L]$;

7. $ccs \in [1/2, 1)$.

Proof. (L1) $\sigma_{\min} \le \sigma_0$

[$\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$ (the statement)]

(L2) $\forall z_0 \le 17:\ g(z_0+1) - g(z_0) = \frac{2z_0+3}{2\sigma_{\min}^2} - (2z_0+1)C_0$

[g (the statement)]

(L3) $\forall z_0 \le 17:\ g(z_0+1) - g(z_0) \ge 0$

[(L1), (L2); $C_0 = 1/(2\sigma_0^2)$ (SamplerZ (Algorithm 8), Require)]

(L4) $\forall z_0, z_0' \in \{0, \dots, 18\},\ z_0 \le z_0':\ g(z_0) \le g(z_0')$

[(L3)]

(L5) $\Rightarrow$ item 1

[(L4)]

(L6) $\forall z:\ |z - r| \in [z_0, z_0+1]$

[$z = b + (2b-1)z_0$, $b \in \{0,1\}$ (line 10); $r \in [0,1)$]

(L7) $\forall z:\ x(z) = \frac{(z-r)^2}{2\widetilde{\sigma}^2} - z_0^2 C_0$

[line 16 at $\sigma = \widetilde{\sigma}$]

(L8) $\forall z:\ x(z) \le g(\bar{z}_0(z))$

[(L6), (L7); $\widetilde{\sigma} \ge \sigma_{\min}$ (the statement); g (the statement)]

(L9) $\Rightarrow$ item 2

[(L8)]

(L10) $\forall z:\ x(z) \ge z_0^2 \left(\frac{1}{2\widetilde{\sigma}^2} - \frac{1}{2\sigma_0^2}\right)$

[(L6), (L7)]

(L11) $\forall z:\ z_0^2 \left(\frac{1}{2\widetilde{\sigma}^2} - \frac{1}{2\sigma_0^2}\right) \ge 0$

[$\widetilde{\sigma} \le \sigma_0$ (the statement; **Hypothesis J.47**)]

(L12) $\Rightarrow\ \forall z:\ x(z) \ge 0$

[(L10), (L11)]

(L13) $\forall z:\ z_0 \le 18$

[Lemma G.64]

(L14) $\forall z:\ x(z) \le g(18)$

[(L4), (L8), (L13)]

(L15) $g(18) = x_c$

[x_c (Lemma J.51); g (the statement)]

(L16) $\Rightarrow\ \forall z:\ x(z) \le x_c$

[(L14), (L15)]

(L17) $\forall z:\ x(z) \in [0, x_c]$

[(L12), (L16)]

(L18) $\Rightarrow$ item 3

[(L17)]

(L19) $\forall z:\ si(z) \le s_c$

[Lemma J.50, item 1, on the input $x(z) \ge 0$ by (L12); (L17); $si \in \mathbb{Z}_{\ge 0}$ (Lemma J.50); $\mathbb{Z}_{\ge 0}$ (Definition A.1); s_c (the statement); **Hypothesis J.31, item (1)**]

(L20) $\Rightarrow$ item 4

[(L19)]

(L21) $\forall z:\ |(si \ln 2 + r') - x| \le E_s$

[Lemma J.50, item 2, on the input $x(z) \ge 0$ by (L12); (L17), (L19); E_s (the statement); **Hypothesis J.31, item (1)**]

(L22) $e^{-(si \ln 2 + r')} = 2^{-si} e^{-r'}$

[$e^{\ln 2} = 2$]

(L23) $ccs > 0$

[$ccs = \sigma_{\min}/\widetilde{\sigma}$ (the statement)]

(L24) $\forall z:\ acc(z) \in [ccs\, e^{-r'}\, 2^{-si}\, e^{-E_s}, ccs\, e^{-r'}\, 2^{-si}\, e^{E_s}]$

[$acc = ccs\, e^{-x}$ (the statement); (L21), (L22), (L23); exp increasing (Fact A.41, item 5)]

(L25) $\Rightarrow$ item 5

[(L24)]

(L26) $\forall z:\ \mathrm{fl}(x \cdot \texttt{INV_LOG2}) \geq x \cdot \texttt{INV_LOG2}\,(1-u)$

[(L17); Lemma J.15, item 2, at $\circ = \times$, or $\mathrm{fl}(0) = 0$ (Fact J.2, item 4); **Hypothesis J.31, item (1)**]

(L27) $\forall z:\ \mathrm{fl}(x \cdot \texttt{INV_LOG2}) < si + 1$

[$si = \mathrm{trunc}(\mathrm{fl}(x \cdot \texttt{INV_LOG2}))$ (line 2)]

(L28) $\forall z:\ x < (si+1)/(\texttt{INV_LOG2}\,(1-u))$

[(L26), (L27)]

(L29) $\forall z:\ r' \leq x - si \ln 2 + E_s$

[(L21)]

(L30) $\forall z:\ r' < (si+1)/(\texttt{INV_LOG2}\,(1-u)) - si \ln 2 + E_s$

[(L28), (L29)]

(L31) $\max_{0 \leq si \leq s_c}\big((si+1)/(\texttt{INV_LOG2}\,(1-u)) - si \ln 2\big) = \max_{si \in \{0, s_c\}}\big((si+1)/(\texttt{INV_LOG2}\,(1-u)) - si \ln 2\big)$

[Fact A.41, item 16, in si over $[0, s_c]$, both ends among the si]

(L32) $\forall z:\ r' \leq L$

[(L19), (L30), (L31); the first measured row]

(L33) $\forall z:\ r' \geq 0$

[(L17); Lemma J.51 at $x := x(z) \in [0, x_c]$; **Hypothesis J.31, item (1)**]

(L34) $\forall z:\ r'(z) \in [0, L]$

[(L32), (L33)]

(L35) $\Rightarrow$ item 6

[(L34)]

(L36) $ccs \geq \sigma_{\min}/\sigma_0$

[$ccs = \sigma_{\min}/\widetilde{\sigma}$ (the statement); $\widetilde{\sigma} \leq \sigma_0$ (the statement)]

(L37) $\sigma_{\min}/\sigma_0 > 1/2$

[the second measured row]

(L38) $\widetilde{ccs} < 1$

[**Hypothesis J.48, item 1**]

(L39) $ccs < 1$

[(L38); $\widetilde{ccs} = \mathrm{fl}(ccs)$ (**Hypothesis J.48**); $\forall a, b \in \mathbb{R},\ a \leq b:\ \mathrm{fl}(a) \leq \mathrm{fl}(b)$ (Fact J.2, item 8); $\mathrm{fl}(1) = 1$ (Fact J.2, item 4)]

(L40) $ccs \in [1/2, 1)$

[(L36), (L37), (L39)]

(L41) $\Rightarrow$ item 7

[(L40)]

□ (items 1 to 5)

Lemma J.57 (The saturated word and acceptance [to table]). *At every point of the fringe set, the shift saturates at* 63*, the acceptance word is* 1 *and the computed acceptance is* 2^{-64}*.* ***Under Hypothesis J.48****, define:*

- $\sigma_{\min}$ *and* σ_0*, those of Definition J.55.*

Let:

- $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$*, a leaf's computed standard deviation.*

Define:

- C*,* si *and* $\widetilde{B}$*, those of Definition J.55;*

- r', *that of Lemma J.50 on the input x of Definition J.55;*
- ccs, *that of Lemma J.56;*
- y, *that of Lemma H.25 at (r', ccs);*
- z_{acc} *and* s_x, *those of Fact G.66;*
- $\widetilde{acc}_c$, *that of Lemma H.26.*

Then

1. $\forall z \in C:\ s_x = 63$;
2. $\forall z \in C:\ z_{\mathrm{acc}} = 1$;
3. $\forall z \in C:\ \widetilde{acc}_c(z) = 2^{-64}$.

Proof. (L1) $\forall z \in C:\ si(z) \geq 64$

[C (Definition J.55)]

(L2) $\forall z \in C:\ s_x = 63$

[(L1); $s_x = \min(si, 63)$ (Fact G.66)]

(L3) $\Rightarrow$ item 1

[(L2)]

(L4) $2^{63} y \leq 2^{63}$

[line 12 of BerExp (Algorithm 9); $ccs \leq 1$ (**Hypothesis J.48**)]

(L5) $\forall z \in C:\ z_{\mathrm{acc}} \leq 1$

[$z_{\mathrm{acc}} = ((2^{63} y \ll 1) - 1) \gg s_x$ (Fact G.66; line 13); (L2), (L4)]

(L6) $\forall z \in C:\ \widetilde{B}(z) > 0$

[$C \subseteq \mathrm{Supp}(\widetilde{B})$ (Definition J.55)]

(L7) $\forall z:\ \widetilde{B}(z) > 0 \Rightarrow\ \widetilde{acc}_c(z) > 0$

[Fact A.45, item 4: $\widetilde{B}(z) = q(z)\,\widetilde{acc}_c(z) / \sum_{z'} q(z')\,\widetilde{acc}_c(z')$, q the proposal of Lemma G.64]

(L8) $\forall z \in C:\ z_{\mathrm{acc}} \geq 1$

[(L6), (L7); $\widetilde{acc}_c = z_{\mathrm{acc}}/2^{64}$ (Lemma H.26); $z_{\mathrm{acc}} \in \mathbb{Z}$]

(L9) $\forall z \in C:\ z_{\mathrm{acc}} = 1$

[(L5), (L8)]

(L10) $\Rightarrow$ item 2

[(L9)]

(L11) $\forall z \in C:\ \widetilde{acc}_c(z) = 2^{-64}$

[(L9); $\widetilde{acc}_c = z_{\mathrm{acc}}/2^{64}$ (Lemma H.26)]

(L12) $\Rightarrow$ item 3

[(L11)]

□ (items 1 to 3)

Lemma J.58 (The trial and computed acceptances [to table])**.** *At a leaf, the mean acceptance of a trial lies between two constants of the table, and the computed one lies above a floor.* ***Under Hypotheses J.48****, J.31, J.47 and J.54, define:*

- $\sigma_{\min}$ *and* σ_0, *those of Definition J.55.*

Let:

- $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$, *a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$, *its computed center.*

Define:

- *The signer's words and parameters*
  - $\sigma_{\max}$ *and* r, *those of Definition J.55;*
  - C_0, *that of* SamplerZ *(Algorithm 8), Require;*
  - ϵ, *that of* ***Hypothesis J.54****;*
- *The table*

  - $m(z_0)$, $w(z_0)$, P_0, $\rho_{\widetilde{\sigma}}$, ρ_{σ_0} *and* $z \in [-18, 19]$, *those of Lemma G.64,* $\rho_{\widetilde{\sigma}}$ *its* ρ_σ *at* $\sigma := \widetilde{\sigma}$;
  - $w_{\mathrm{lo}} := \min_{z_0 \le 18} w(z_0)$;
  - $w_{\mathrm{hi}} := \max_{z_0 \le 18} w(z_0)$;
  - $q(z) := m(\bar{z}_0(z))/2$;
- *The exponent*
  - u, z_0 *and* x, *those of Lemma J.49 at* $(\widetilde{\sigma}, \widetilde{t})$;
- *The split*
  - si *and* r', *those of Lemma J.50 on the input* x;
  - $\hat{C} := \{\, z \in [-18, 19] : si(z) \ge 64 \,\}$;
- *The acceptance*
  - ccs, acc *and* E_s, *those of Lemma J.56;*
  - acc_c *and* $\widetilde{acc}_c$, *those of Lemma H.26;*
  - y, *that of Lemma H.25 at* (r', ccs);
  - $e_{\mathrm{poly}} := 2^{-51.05}$ *(Lemma H.25);*
- *The trial acceptance*
  - $\Sigma_w := \sum_{z' \in [-18,19]} w(\bar{z}_0(z'))\, \rho_{\widetilde{\sigma}}(z' - r)$;
  - $T := \sum_{z' \in [-18,19]} q(z')\, acc(z')$;
  - $\widetilde{T} := \sum_{z' \in [-18,19]} q(z')\, \widetilde{acc}_c(z')$ *(line 18 of* BerExp *(Algorithm 9));*
  - $t_{18} := \dfrac{1+\epsilon}{1-\epsilon} \cdot \dfrac{18}{\sigma_{\max}}\, e^{(1-(18/\sigma_{\max})^2)/2}$;
  - $acc_{\mathrm{lo}} := \dfrac{w_{\mathrm{lo}}\,(1-\epsilon)\sqrt{2\pi}\,\sigma_{\min}\,(1-t_{18})}{2\,\rho_{\sigma_0}(\mathbb{Z}_{\ge 0})}$;
  - $acc_{\mathrm{hi}} := \dfrac{w_{\mathrm{hi}}\,(1+\epsilon)\sqrt{2\pi}\,\sigma_{\min}}{2\,\rho_{\sigma_0}(\mathbb{Z}_{\ge 0})}$;
  - $acc_{\min} := (1 - e_{\mathrm{poly}})\, e^{-E_s}\, acc_{\mathrm{lo}} - 2^{-63} - 2^{-64(1-3u)}$.

Measured `verify/reports/sampler/cap.py`*:*

- $acc_{\min} \ge 2^{-0.7965}$ *at both degrees.*

Then

1. $T \in [acc_{\mathrm{lo}}, acc_{\mathrm{hi}}]$;
2. $\widetilde{T} \ge acc_{\min}$;
3. $w_{\mathrm{lo}}\,(1 - t_{18})\, \rho_{\widetilde{\sigma},r}(\mathbb{Z}) \le \Sigma_w$;
4. $acc_{\min} > 0$.

Proof. (L1) $\forall z \notin \hat{C} :\ si(z) \le 63$

[$\hat{C}$ (the statement)]

(L2) $\forall z \notin \hat{C} :\ acc_c = y\, 2^{-si}$

[(L1); Lemma H.26, item 3; $si \ge 0$ (Lemma J.50, item 1, at x, its assumption A1 by Lemma J.56, item 3), assumption A1 of Lemma H.26; **Hypothesis J.31**, named by Lemmas J.50 and J.56; assumption A2 of Lemma H.26 by Lemma H.25 at (r', ccs), its assumptions A1 and A2 by Lemma J.56, items 6 and 7; y (Lemma H.25)]

(L3) $\forall z :\ y \ge ccs\, e^{-r'}(1 - e_{\mathrm{poly}})$

[Lemma H.25 at (r', ccs); its assumptions by Lemma J.56, items 6 and 7; e_{poly} (the statement); **Hypotheses J.48, J.47 and J.31**, named by Lemma J.56]

(L4) $\forall z \notin \hat{C} :\ acc_c(z) \ge (1 - e_{\mathrm{poly}})\, e^{-E_s}\, acc(z)$

[(L2), (L3); Lemma J.56, item 5, its upper half; **Hypothesis J.31, item (1)**; **Hypotheses J.48 and J.47**, named by Lemma J.56]

(L5) $\forall z :\ \widetilde{acc}_c(z) \ge acc_c(z) - 2 \cdot 2^{-64}$

[Lemma H.26, item 1; $si \ge 0$ (Lemma J.50, item 1, at x, its assumption A1 by Lemma J.56, item 3), assumption A1 of Lemma H.26; **Hypothesis J.31**, named by Lemmas J.50 and J.56; $2^{63} y \ge 1$ ((L3); Lemma J.56, items 6 and 7), assumption A2 of Lemma H.26]

(L6) $\forall z \notin \hat{C}:\ \widetilde{acc}_c(z) \geq (1 - e_{\text{poly}})\, e^{-E_s}\, acc(z) - 2^{-63}$

[(L4), (L5)]

(L7) $\forall z \in \hat{C}:\ x(z) \geq 64 \ln 2\,(1 - 3u)$

[Lemma J.53, item 1; $si \geq 64$ on $\hat{C}$ (the statement); $x \geq 0$ (Lemma J.56, item 3); **Hypothesis J.31, item (1)**]

(L8) $ccs \leq 1$

[$ccs = \sigma_{\min}/\widetilde{\sigma}$ (Lemma J.56), $\widetilde{\sigma} \geq \sigma_{\min}$ (the statement)]

(L9) $\forall z \in \hat{C}:\ acc(z) \leq 2^{-64(1-3u)}$

[(L7), (L8); $acc = ccs\, e^{-x}$ (the statement); $e^{-64 \ln 2\,(1-3u)} = 2^{-64(1-3u)}$ (Fact A.41, item 12)]

(L10) $\forall z:\ e^{-x(z)} = \rho_{\widetilde{\sigma}}(z - r)/\rho_{\sigma_0}(z_0)$

[$x = (z-r)^2/(2\widetilde{\sigma}^2) - z_0^2 C_0$ (line 16); $C_0 = 1/(2\sigma_0^2)$ (SamplerZ (Algorithm 8), Require)]

(L11) $\forall z_0:\ m(z_0) = w(z_0)\rho_{\sigma_0}(z_0)/\rho_{\sigma_0}(\mathbb{Z}_{\geq 0})$

[w (Lemma G.64)]

(L12) $\forall z:\ q(z) = w(z_0)\rho_{\sigma_0}(z_0)/(2\rho_{\sigma_0}(\mathbb{Z}_{\geq 0}))$

[(L11); q (the statement)]

(L13) $T = \frac{ccs}{2\,\rho_{\sigma_0}(\mathbb{Z}_{\geq 0})}\,\Sigma_w$

[T, Σ_w, acc (the statement; Lemma J.56); (L10), (L12)]

(L14) $\sum_{z' \in [-18,19]} \rho_{\widetilde{\sigma}}(z' - r) = \rho_{\widetilde{\sigma},r}(\mathbb{Z}) - \rho_{\widetilde{\sigma},r}(\mathbb{Z} \setminus [-18, 19])$

[$\rho_{\widetilde{\sigma},r}(\mathbb{Z}) = \sum_{z \in \mathbb{Z}} \rho_{\widetilde{\sigma}}(z - r)$ (Section 3.1)]

(L15) $\mathbb{Z} \setminus [-18, 19] \subseteq \{\, z' : |z' - r| > 18 \,\}$

[$r \in [0, 1)$]

(L16) $\forall \tau' > 1:\ \frac{d}{d\tau'}\left(\tau' e^{(1-\tau'^2)/2}\right) = (1 - \tau'^2) e^{(1-\tau'^2)/2}$

[differentiate]

(L17) $\forall \tau' > 1:\ (1 - \tau'^2) e^{(1-\tau'^2)/2} < 0$

[$1 - \tau'^2 < 0$ ($\tau' > 1$, the line's quantifier); $e^t > 0$ (Fact A.41, item 12)]

(L18) $\Rightarrow\ \forall \tau' > 1:\ \frac{d}{d\tau'}\left(\tau' e^{(1-\tau'^2)/2}\right) < 0$

[(L16), (L17)]

(L19) $\rho_{\widetilde{\sigma},r}(\mathbb{Z} \setminus [-18, 19]) \leq t_{18}\, \rho_{\widetilde{\sigma},r}(\mathbb{Z})$

[(L15); Lemma E.18, item 2, at $s := \widetilde{\sigma}$, $t := r$, $\tau' := 18/\widetilde{\sigma} > 1$, ϵ; (L18) at $18/\widetilde{\sigma} \geq 18/\sigma_{\max}$; t_{18} (the statement)]

(L20) $w_{\text{lo}}\,(1 - t_{18})\,\rho_{\widetilde{\sigma},r}(\mathbb{Z}) \leq \Sigma_w$

[$w \geq w_{\text{lo}}$ (the statement); (L14), (L19)]

(L21) $\Rightarrow$ item 3

[(L20)]

(L22) $\Sigma_w \leq w_{\text{hi}}\, \rho_{\widetilde{\sigma},r}(\mathbb{Z})$

[$w \leq w_{\text{hi}}$ (the statement); (L14)]

(L23) $ccs\, \rho_{\widetilde{\sigma},r}(\mathbb{Z}) \in [(1 - \epsilon)\sqrt{2\pi}\,\sigma_{\min}, (1 + \epsilon)\sqrt{2\pi}\,\sigma_{\min}]$

[$ccs = \sigma_{\min}/\widetilde{\sigma}$ (the statement); **Hypothesis J.54, item 1**, at $s := \widetilde{\sigma}$, $c := r$]

(L24) $T \in [acc_{\text{lo}}, acc_{\text{hi}}]$

[(L13), (L20), (L22), (L23); acc_{lo}, acc_{hi} (the statement)]

(L25) $\Rightarrow$ item 1

[(L24)]

(L26) $acc_{\min} > 0$

[the measured row]

(L27) $\Rightarrow$ item 4

[(L26)]

(L28) $\sum_{z'} q(z') = 1$

[two candidates per z_0 and $\sum_{z_0 \leq 18} m(z_0) = 1$ (Lemma G.64)]

(L29) $e_{\text{poly}} < 1$

[$e_{\text{poly}} = 2^{-51.05}$ (the statement)]

(L30) $\widetilde{T} \geq \sum_{z' \notin \hat{C}} q(z')\, \widetilde{acc}_c(z')$

[$\widetilde{acc}_c \geq 0$; $\widetilde{T}$ (the statement)]

(L31) $\sum_{z' \notin \hat{C}} q(z')\, \widetilde{acc}_c(z') \geq (1 - e_{\text{poly}}) e^{-E_s} \sum_{z' \notin \hat{C}} q(z')\, acc(z') - 2^{-63}$

[(L6), (L28)]

(L32) $\sum_{z' \notin \hat{C}} q(z')\, acc(z') = T - \sum_{z' \in \hat{C}} q(z')\, acc(z')$

[T (the statement)]

(L33) $(1 - e_{\text{poly}}) e^{-E_s} \sum_{z' \in \hat{C}} q(z')\, acc(z') \leq 2^{-64(1-3u)}$

[(L9); (L28); $(1 - e_{\text{poly}})e^{-E_s} \in [0,1]$ (L29)]

(L34) $\widetilde{T} \geq (1 - e_{\text{poly}}) e^{-E_s} T - 2^{-63} - 2^{-64(1-3u)}$

[(L30) to (L33)]

(L35) $\widetilde{T} \geq acc_{\min}$

[(L24), (L29), (L34); $acc_{\min}$ (the statement)]

(L36) $\Rightarrow$ item 2

[(L35)]

$\square$ (items 1 to 4)

Lemma J.59 (The fringe set's ratio [to table])**.** *On the fringe set, the computed leaf probability exceeds the exact one by at most a ratio the shift's ceiling bounds.* ***Under Hypotheses J.48****, J.31, J.47 and J.54, define:*

- $\sigma_{\min}$ *and* σ_0*, those of Definition J.55.*

Let:

- $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$*, a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$*, its computed center.*

Define:

- $\sigma_{\max}$*,* r*,* $\widetilde{B}$*,* $\widetilde{D}$*,* C*,* τ *and* $\bar{U}(\tau)$*, those of Definition J.55;*
- *ccs, acc,* s_c *and* E_s*, those of Lemma J.56;*
- r' *and si, those of Lemma J.50 on the input* x *of Lemma J.49;*
- y*, that of Lemma H.25 at* (r', ccs)*;*
- $\widetilde{acc}_c$*, that of Lemma H.26;*
- e_{poly}*,* w_{lo}*,* w_{hi}*,* q*,* T*,* $\widetilde{T}$*,* Σ_w*,* t_{18}*,* acc_{hi} *and* $acc_{\min}$*, those of Lemma J.58;*
- $w(z_0)$*,* P_0 *and* $\rho_{\widetilde{\sigma}}$*, those of Lemma G.64,* $\rho_{\widetilde{\sigma}}$ *its* ρ_σ *at* $\sigma := \widetilde{\sigma}$*,* P_0 *read on the candidates as* $\widetilde{B}$ *is (Definition J.55);*
- $\epsilon_C = \dfrac{acc_{\text{hi}}}{acc_{\min}} \cdot \dfrac{w_{\text{hi}}}{w_{\text{lo}}\,(1 - t_{18})} \cdot (1 + e_{\text{poly}})\, e^{E_s} - 1.$

Then

1. $\forall z \in C:\ \widetilde{B}(z) \leq \bar{U}(\tau)\, \widetilde{D}(z)$*;*
2. $\bar{U}(\tau) \leq 2^{s_c - 63}\,(1 + \epsilon_C)$*.*

Proof. (L1) $\forall z \in C:\ \widetilde{B}(z) \leq \bar{U}(\tau)\, \widetilde{D}(z)$

[$\bar{U}(\tau)$ (Definition J.55)]

(L2) $\Rightarrow$ item 1

[(L1)]

(L3) $\forall z \in C:\ ((2^{63} y \ll 1) - 1) \gg 63 = 1$

[Lemma J.57, items 1 and 2; **Hypothesis J.48**, named by Lemma J.57]

(L4) $\forall z \in C:\ 2 \cdot 2^{63} y - 1 \geq 2^{63}$

[(L3); $a \gg 63 \geq 1 \iff a \geq 2^{63}$ ($a \in [0, 2^{64})$; $\gg$, Definition A.5)]

(L5) $\forall z \in C:\ y \geq 1/2$

[(L4); $2^{63} y \in \mathbb{Z}$]

(L6) $\forall z \in C:\ y \leq ccs\, e^{-r'}(1 + e_{\text{poly}})$

[Lemma H.25 at (r', ccs); its assumptions by Lemma J.56, items 6 and 7; e_{poly} (Lemma J.58); **Hypotheses J.48, J.47 and J.31**, named by Lemma J.56]

(L7) $\forall z \in C:\ ccs\, e^{-r'} \geq \frac{1}{2(1+e_{\text{poly}})}$

[(L5), (L6)]

(L8) $\forall z \in C:\ acc(z) \geq ccs\, e^{-r'}\, 2^{-si}\, e^{-E_s}$

[Lemma J.56, item 5, its lower half; **Hypothesis J.31, item (1)**; **Hypotheses J.48 and J.47**, named by Lemma J.56]

(L9) $\forall z \in C:\ \frac{\widetilde{acc}_c(z)}{acc(z)} \leq 2^{-64} \cdot 2(1+e_{\text{poly}})\, 2^{si} e^{E_s}$

[Lemma J.57, item 3; (L7), (L8); **Hypothesis J.48**, named by Lemma J.57]

(L10) $\forall z \in C:\ \frac{\widetilde{acc}_c(z)}{acc(z)} \leq 2^{s_c-63}\,(1+e_{\text{poly}})\, e^{E_s}$

[(L9); Lemma J.56, item 4; **Hypothesis J.31, item (1)**; **Hypotheses J.48 and J.47**, named by Lemma J.56]

(L11) $\forall z:\ \frac{\widetilde{B}(z)}{\widetilde{D}(z)} = \frac{\widetilde{acc}_c(z)}{acc(z)} \cdot \frac{T}{\widetilde{T}} \cdot \frac{P_0(z)}{\widetilde{D}(z)}$

[Fact A.45, item 4, at the proposal q with the acceptance $\widetilde{acc}_c$ for $\widetilde{B}$ and with acc for P_0; Lemma G.64, item 2, its assumptions by $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$ (the statement)]

(L12) $\frac{T}{\widetilde{T}} \leq \frac{acc_{\text{hi}}}{acc_{\min}}$

[Lemma J.58, items 1 and 2; $acc_{\min} > 0$ (Lemma J.58, item 4); **Hypothesis J.31, item (1)**; **Hypotheses J.48, J.47 and J.54**, named by Lemma J.58]

(L13) $\forall z:\ P_0(z) = \rho_{\widetilde{\sigma}}(z-r)\, w(\bar{z}_0(z))/\Sigma_w$

[Lemma G.64, item 2, its assumptions by $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$ (the statement); Σ_w (Lemma J.58)]

(L14) $\forall z:\ \widetilde{D}(z) = \rho_{\widetilde{\sigma}}(z-r)/\rho_{\widetilde{\sigma},r}(\mathbb{Z})$

[Section 3.1, at $\widetilde{t} = \lfloor \widetilde{t} \rceil + r$]

(L15) $\forall z:\ \frac{P_0(z)}{\widetilde{D}(z)} = \frac{w(\bar{z}_0(z))\, \rho_{\widetilde{\sigma},r}(\mathbb{Z})}{\Sigma_w}$

[(L13), (L14)]

(L16) $\forall z:\ \frac{P_0(z)}{\widetilde{D}(z)} \leq \frac{w_{\text{hi}}}{w_{\text{lo}}\,(1-t_{18})}$

[(L15); Lemma J.58, item 3; $w \leq w_{\text{hi}}$ (Lemma J.58); **Hypothesis J.31, item (1)**; **Hypotheses J.48, J.47 and J.54**, named by Lemma J.58]

(L17) $\forall z \in C:\ \frac{\widetilde{B}(z)}{\widetilde{D}(z)} \leq 2^{s_c-63}\,(1+\epsilon_C)$

[(L10), (L11), (L12), (L16); ϵ_C (the statement)]

(L18) $\bar{U}(\tau) \leq 2^{s_c-63}\,(1+\epsilon_C)$

[(L17) at every $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_{\max}]$, $\widetilde{t} \in \mathbb{R}$ and $z \in C$; $\bar{U}(\tau)$ (Definition J.55)]

(L19) $\Rightarrow$ item 2

[(L18)]

□ (items 1 and 2)

Lemma J.60 (The fringe set's probability [to table])**.** *The computed probability of the fringe set is at most 2^{-64} over the floor of the computed trial acceptance, times twice the table's tail mass.*
***Under Hypotheses J.48**, J.31, J.47 and J.54, define:*

- $\sigma_{\min}$ *and* σ_0*, those of Definition J.55.*

Let:

- $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_0]$*, a leaf's computed standard deviation;*
- $\widetilde{t} \in \mathbb{R}$*, its computed center.*

Define:

- $\sigma_{\max}$*,* r*,* $\widetilde{B}$*,* C*,* τ *and* $\bar{p}_C(\tau)$*, those of Definition J.55;*
- C_0*, that of* SamplerZ *(Algorithm 8), Require;*
- u*,* z_0 *and* x*, those of Lemma J.49 at* $(\widetilde{\sigma}, \widetilde{t})$*;*
- g*, that of Lemma J.56;*
- $\widetilde{acc}_c$*, that of Lemma H.26;*
- q*,* $\widetilde{T}$ *and* $acc_{\min}$*, those of Lemma J.58;*
- $m(z_0)$*,* $w(z_0)$ *and* ρ_{σ_0}*, those of Lemma G.64;*

- $z_c = \min\{\, z_0 \le 18 : g(z_0) \ge 64 \ln 2\,(1-3u) \,\}$.

Measured at the stored words:

- $\max_{z_0 \le 18} w(z_0) \le 2$ *[gate: verify/gates/sampler/table_weight.py].*

Then

$$\bar{p}_C(\tau) \le \frac{2^{-64}}{acc_{\min}} \cdot \frac{2\sum_{z_0 \ge z_c} e^{-z_0^2 C_0}}{\rho_{\sigma_0}(\mathbb{Z}_{\ge 0})}.$$

Proof. (L1) $\forall z \in C :\ x(z) \ge 64 \ln 2\,(1-3u)$
[Lemma J.53, item 1, at $si(z) \ge 64$ (C, Definition J.55); $x \ge 0$ (Lemma J.56, item 3); **Hypothesis J.31, item (1)**]

(L2) $\forall z_0 < z_c :\ g(z_0) < 64 \ln 2\,(1-3u)$
[z_c (the statement); Lemma J.56, item 1; **Hypothesis J.31, item (1)**; **Hypotheses J.48 and J.47**, named by Lemma J.56]

(L3) $\forall z :\ \bar{z}_0(z) < z_c \Rightarrow\ x(z) < 64 \ln 2\,(1-3u)$
[(L2); Lemma J.56, item 2; **Hypothesis J.31, item (1)**; **Hypotheses J.48 and J.47**, named by Lemma J.56]

(L4) $C \subseteq \{\, z : \bar{z}_0(z) \ge z_c \,\}$
[(L1), (L3)]

(L5) $\forall z :\ \widetilde{B}(z) = \frac{q(z)\,\widetilde{acc}_c(z)}{\widetilde{T}}$
[Fact A.45, item 4, at q and $\widetilde{acc}_c$; $\widetilde{T}$ (Lemma J.58)]

(L6) $\widetilde{T} \ge acc_{\min}$
[Lemma J.58, item 2; **Hypothesis J.31, item (1)**; **Hypotheses J.48, J.47 and J.54**, named by Lemma J.58]

(L7) $\forall z_0 :\ \rho_{\sigma_0}(z_0) = e^{-z_0^2 C_0}$
[$C_0 = 1/(2\sigma_0^2)$ (SamplerZ (Algorithm 8), Require)]

(L8) $\forall z_0 :\ m(z_0) = w(z_0)\, e^{-z_0^2 C_0} / \rho_{\sigma_0}(\mathbb{Z}_{\ge 0})$
[w (Lemma G.64); (L7)]

(L9) $\forall z \in C :\ \widetilde{B}(z) \le \frac{2^{-64}}{acc_{\min}\,\rho_{\sigma_0}(\mathbb{Z}_{\ge 0})}\, e^{-\bar{z}_0(z)^2 C_0}$
[(L5), (L6); $\forall z \in C :\ \widetilde{acc}_c(z) = 2^{-64}$ (Lemma J.57, item 3); $acc_{\min} > 0$ (Lemma J.58, item 4); $q(z) = m(\bar{z}_0(z))/2$ (Lemma J.58); (L8); the first measured row; **Hypothesis J.31, item (1)**; **Hypothesis J.48**, named by Lemma J.57]

(L10) $\widetilde{B}(C) \le \frac{2^{-64}}{acc_{\min}\,\rho_{\sigma_0}(\mathbb{Z}_{\ge 0})} \sum_{z \in C} e^{-\bar{z}_0(z)^2 C_0}$
[(L9) summed over $z \in C$]

(L11) $\sum_{z \in C} e^{-\bar{z}_0(z)^2 C_0} \le 2 \sum_{z_0 \ge z_c} e^{-z_0^2 C_0}$
[(L4); two candidates per z_0]

(L12) $\widetilde{B}(C) \le \frac{2^{-64}}{acc_{\min}} \cdot \frac{2\sum_{z_0 \ge z_c} e^{-z_0^2 C_0}}{\rho_{\sigma_0}(\mathbb{Z}_{\ge 0})}$
[(L10), (L11); $acc_{\min} > 0$ (Lemma J.58, item 4)]

(L13) $\bar{p}_C(\tau) \le \frac{2^{-64}}{acc_{\min}} \cdot \frac{2\sum_{z_0 \ge z_c} e^{-z_0^2 C_0}}{\rho_{\sigma_0}(\mathbb{Z}_{\ge 0})}$
[(L12) at every $\widetilde{\sigma} \in [\sigma_{\min}, \sigma_{\max}]$ and $\widetilde{t} \in \mathbb{R}$; $\bar{p}_C(\tau)$ (Definition J.55)]

(L14) $\Rightarrow$ the statement
[(L13)]

□

J.5 The loss

Against the ideal level λ of ffSampling$^{\mathbb{R}}$, how many bits does ffSampling$^{\mathcal{F}}$ lose once Theorem F.4 is applied to the probability of the adversary's event?

The variables of the loss. The loss $\lambda - \lambda_{\mathcal{F}}$ is a function of the precision p with $u = 2^{-p}$, the degree n, the pair (λ, α), the number Q_s of signatures, and of the bounds on the leaf perturbations, of which this section reads two: the derived bounds of the rounding model with the key's constants, and the Gaussian quantiles of the code's leaf perturbations under **Hypothesis J.64**. The signer is the floating-point signer, the plain C build of `c-fn-dsa`, at $p = 53$ and at the hypothetical precisions $p = 64$, 113 of the same format.

The ideal pairs and the conventions. The ideal pairs are $(\lambda, \alpha) = (128, 257)$ at $n = 512$ and $(256, 513)$ at $n = 1024$, the order being $\alpha = 2\lambda + 1$, the convention of [PRR19] [L2: PRR19, Section 5], whose published form takes $2\lambda - 1$ [L2: HPRR20, p. 17]; [ZSS19], [Pre17] and the Falcon specification take 2λ [L2: ZSS19, Section 4; Pre17, Section 4; FGdG+26, Section 1], and [FGdG+26] optimizes the order per scheme [L2: FGdG+26, Section 5.3]. All numbers are $\log_2$ and per signature unless a table says otherwise; the arithmetic inputs are level 0; the key's constants are measured on keys of the reference key generation and are read as the tuple of maxima defined below. `verify/reports/fp/terms.py`

The derived bounds assume no hypothesis on the basis image. The derived bounds carry the computed Gram matrix's own perturbation. Lemma J.37 derives it from the checked key generation's four checks, and the derived bounds assume no hypothesis on the basis image.

The six key constants. The key is read through six numbers that say how well-behaved its tree is, and every perturbation bound of the report is a rounding's perturbation times one of them: the root node's κ_{root} and the nodes' κ_k, how far the key's Gram matrix is from diagonal, the amount by which each rounding is amplified down the tree; the norms Ξ', Ξ'_{root} of the factor $\mathcal{L}_\nu$ and Ξ of its inverse, how far a perturbation at a node travels to the leaves; and the largest off-diagonal factor $\ell = \max|l_{10}|$ (Definition 4.6):

$$K = (\kappa_{\text{root}}, \kappa_k, \Xi', \Xi'_{\text{root}}, \Xi, \ell),$$

$$\hat{K}_{512} = (3697.7664,\ 16.9267,\ 4.1965,\ 27.4884,\ 4.1965,\ 17.8150),$$

$$\hat{K}_{1024} = (14468.5872,\ 11.5347,\ 4.8885,\ 43.2837,\ 4.8885,\ 29.1742).$$

The measured maxima of the key constants. $\hat{K}_n$ is measured: the maximum of each constant over 16 keys of the checked key generation at degree n, generated from fixed seeds, G rebuilt from (f, g, F) and checked exactly, the tree built as the code builds it and every subtree map $\mathcal{L}_\nu$ taken to its two extreme singular values (Table 39, which also lists the medians; **Hypothesis J.63**). Every number below is for a key no worse than these maxima; a particular key has its own six numbers. On every key measured, $\Xi_k = \Xi'_k$ at every depth: the map $\mathcal{L}_\nu$ and its inverse have the same norm. The key generation's two checks bound the six for every accepted key (Proposition G.38, Definition 4.6), but by amounts that grow with n and yield nothing at binary64, so they are not used.

Constant	Max, $n = 512$	Median, $n = 512$	Max, $n = 1024$	Median, $n = 1024$
κ_{root}	3697.7664	2609.8992	14468.5872	6148.6960
κ_k	16.9267	4.6208	11.5347	6.4247
Ξ'	4.1965	3.1916	4.8885	3.7863
Ξ'_{root}	27.4884	22.7221	43.2837	34.2927
Ξ	4.1965	3.1940	4.8885	3.7863
ℓ	17.8150	15.7601	29.1742	23.6397
$\max_\psi \lvert g_{01}\rvert^2 g_{00}/q^2$	306443455.9090	154308416.4550	1392587881.0465	337677716.0602
$\min_\psi g_{00}$	1785.9793	1034.2193	1120.5992	728.7636
$\max_\psi g_{00}$	91492.3002	64839.4761	96249.0578	68845.7856

Table 39: Both signers: key constants, maximum and median over 16 checked keys per degree (Definition 5.5); $\hat{K}_n$ the maxima. Gate (sampled): `verify/reports/key/keyconst_checked.py`.

The sample of leaf perturbations. The inputs of **Hypothesis J.64** are the leaf perturbations of the code itself: the sample $\mathcal{X}$ of 16 keys of the same key generation and 16 messages per degree signed by the plain build with every call of the base sampler traced, ffSampling$^{\mathbb{R}}$ replayed in Decimal at 50 digits on the same prefix, and per signature the sum $W = \sum_i \Delta_i^2/\sigma_i^2$ and every leaf's standard deviation perturbation δ_i (Table 40): the means and standard deviations of **Hypothesis J.64** are the sample's, and W^G and δ^G of Lemma J.65 the Gaussian quantiles they define (**Hypothesis J.64, item 3**).

Center	n	Signatures	W^*	Mean W	max rms_t	$\bar{\delta}^*$	rms δ	$\hat{\sigma}_W$	$W^G(2^{64})$	$\hat{\mu}_\delta$	$\hat{\sigma}_\delta$	$\delta^G(2^{64})$
t	512	256	-75.5	-76.8	-42.2	-46.6	-49.2	-78.2	-74.0	$-2^{-51.9}$	-49.3	-45.2
t	1024	256	-71.4	-74.5	-40.6	-45.1	-48.6	-74.5	-70.1	$+2^{-51.2}$	-48.6	-44.1

Table 40: Floating-point signer at binary64: the leaf perturbations measured over 16 keys and 16 messages per degree, $\log_2$; the inputs of **Hypothesis J.64**, with $W^G = \hat{\mu}_W + z\hat{\sigma}_W$, $z = \sqrt{2\ln(Q_s 2^\lambda)}$, $\hat{\mu}_W$ the mean and $\hat{\sigma}_W$ the standard deviation of W over the sample, and $\delta^G = |\hat{\mu}_\delta| + z_\delta \hat{\sigma}_\delta$, $z_\delta = \sqrt{2\ln(2Q_s N 2^\lambda)}$, $\hat{\mu}_\delta$ (its sign and $\log_2$ of its absolute value), $\hat{\sigma}_\delta$ the mean and standard deviation of δ_i over every leaf of the sample, N the leaves per signature. Report (sampled): `verify/reports/tree/leaferrors.py`.

J.5.1 The terms and the signer's inputs

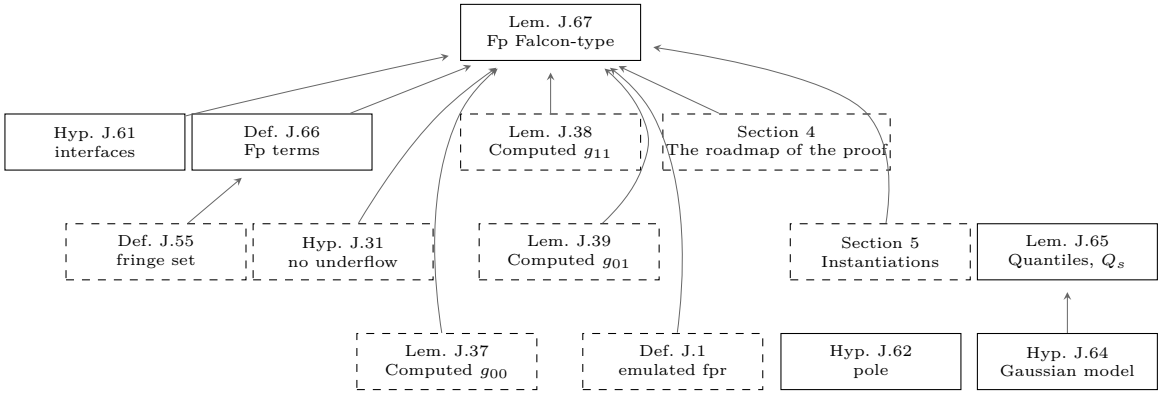


Figure 108: Dependencies, Appendix J.5.1.

Structure. Definition J.66 states the terms of $\ln R$ at $\zeta = 0$; Lemma J.67 the signer's inputs; Appendix J.5.2 the preconditions; Appendix J.5.3 the base sampler's inputs; Appendix J.5.4 the loss in bits.

Hypothesis J.61 (The two interfaces of an instantiation [to table])**.** A mathematical hypothesis on a Falcon-type signer. Let:

- The signer be a Falcon-type signer at (u, ζ) (Definition 4.5).

We assume

1. Every value w the signer computes in $\mathcal{F}$ satisfies $\mathrm{fl}(w)\ \mathcal{N}\,(u,\zeta)\ w$ (Definition A.4);
2. $\exists\, e_{+,k} \geq 0$, $k \leq 18$, $\exists\, e_{\mathrm{ccs}} \in [0,1)$, $\exists\, e_{+} \geq \max_k e_{+,k}$: $e_{+,k}$ and e_{ccs} bound the base sampler's relative perturbation of the acceptance on the row k at every leaf, and the relative rounding of its computed $\widetilde{ccs}$, as Lemma G.73 assumes, on $\mathcal{Y} := \mathcal{Z}_i \setminus C_i$ (Definitions A.26, A.28).

[L3: mathematical]

Hypothesis J.62 (The pole [to table])**.** A mathematical hypothesis: the leaves' deviation stays below the pole of the one-leaf divergence. Let:

- $\bar{\delta} \geq 0$ (Definition A.27).

Define:

- $\alpha_L/(\alpha_L - 1)$, the pole of Lemma 4.1 at order α_L.[1]

We assume

$$(1+\bar{\delta})^2 < \frac{\alpha_L}{\alpha_L - 1}.$$

[L3: mathematical]

Why the key constants are read at the sample maxima. The floating-point analysis reads the key constants at the maxima of a sample of checked keys, not at the bounds every checked key meets. The two readings conflict at binary64. Read at the bounds of Proposition 5.8 and Lemma H.21, the chain of Lemma 4.9 at $u = 2^{-53}$ fails its assumption $\gamma + \gamma_S < 1$ (Lemma J.70, item 3) at both degrees. It meets the precondition only from $p = 60$. The bounds are loose where u multiplies them, at κ_{root} above all. At $u = 0$ these terms vanish, so the fixed-point signer (Appendix I) reads its key constants at the proved bounds (Definition I.62). The floating-point signer therefore rests on **Hypothesis J.63**, and its bit security holds for the key's own constants, not for every checked key.

The Gaussian model of the leaf perturbations. **Hypothesis J.64** is the Gaussian model of the leaf perturbations at binary64, and Lemma J.65 bounds the leaf sum and each leaf's perturbation over Q_s signatures by the model's quantiles; Propositions J.74 and J.78 read the terms and the bit security under them.

Hypothesis J.63 (Floating-point key constants within the sample maxima [to table])**.** A sampled hypothesis: the key constants of the key the floating-point signer generates signatures with are at most the maxima of a sample of checked keys. Let:

- (f, g, F, G) be a checked key (Definition 5.5) of degree n.

Define:

- $(\kappa_{\mathrm{root}}, \kappa_k, \Xi', \Xi'_{\mathrm{root}}, \Xi, \ell)$, the first six entries of its key constants $\hat{K}$ (Definition 4.6);
- $\hat{K}_n$, the maxima of $\hat{K}$ over 16 checked keys of degree n (Table 39).

We assume

1. $(\kappa_{\mathrm{root}}, \kappa_k, \Xi', \Xi'_{\mathrm{root}}, \Xi, \ell)$ is at most the first six entries of $\hat{K}_n$, componentwise `verify/reports/key/keyconst_checked.py`.

[L3: sampled] Not discharged.

[1] The pole is far away for the tree's $\bar{\delta}$ (Definition A.27).

Hypothesis J.64 (Gaussian model of the leaf perturbations [to table])**.** A sampled hypothesis on the floating-point signer at binary64: over the signer's outputs, the leaf sum W and each leaf's standard deviation perturbation δ_i follow Gaussians with the means and standard deviations of a sample, and the sample's Gaussian quantiles are those its tables report. Let:

- $K \in \mathbb{Z}_{>0}$;
- $M \in \mathbb{Z}_{>0}$;
- $\mathcal{X} \subset \mathbb{Z}^N$, a sample of the outputs of P on K keys and M messages, $|\mathcal{X}| = KM$.

Define:

- The signer's words and parameters
  - $(\lambda, \alpha) := (128, 257)$ at $n = 512$;
  - $(\lambda, \alpha) := (256, 513)$ at $n = 1024$;
  - $\eta := 2^{-\lambda}$;
  - $\sigma_{\min}$, the signer's stored `SIGMA_MIN`$[\log_2 n]$ of SamplerZ (Algorithm 8), Require (Definition J.28);
  - $\sigma_{\max} := 1.17^2 \sigma_{\min}$;
- The leaf perturbations
  - $W(z) := \sum_{i \le N} \Delta_i(z_{<i})^2 / \sigma_i(z_{<i})^2$;
- The sample's moments
  - $\hat{\mu}_W := |\mathcal{X}|^{-1} \sum_{z \in \mathcal{X}} W(z)$;
  - $\hat{\sigma}_W := \left((|\mathcal{X}| - 1)^{-1} \sum_{z \in \mathcal{X}} (W(z) - \hat{\mu}_W)^2\right)^{1/2}$;
  - $\hat{\mu}_\delta := (N|\mathcal{X}|)^{-1} \sum_{z \in \mathcal{X}} \sum_{i \le N} \delta_i(z_{<i})$;
  - $\hat{\sigma}_\delta := \left((N|\mathcal{X}| - 1)^{-1} \sum_{z \in \mathcal{X}} \sum_{i \le N} (\delta_i(z_{<i}) - \hat{\mu}_\delta)^2\right)^{1/2}$;
- The Gaussian quantiles
  - $\xi_W(Q_s) := \sqrt{2 \ln(Q_s/\eta)}$, $Q_s \in \mathbb{Z}_{>0}$;
  - $W^G(Q_s) := \hat{\mu}_W + \xi_W(Q_s)\hat{\sigma}_W$;
  - $\xi_\delta(Q_s) := \sqrt{2 \ln(2Q_sN/\eta)}$;
  - $\delta^G(Q_s) := |\hat{\mu}_\delta| + \xi_\delta(Q_s)\hat{\sigma}_\delta$;
- The normalizer
  - $\varepsilon_0^\circ(Q_s)$, the ε_0° of Definition A.40 at $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \delta^G(Q_s), \sigma_{\max} W^G(Q_s)^{1/2})$, at every Q_s where items 4 to 6 hold.

We assume, at the floating-point signer at binary64, at $n \in \{512, 1024\}$:

1. $\forall z$ an output of P: $W(z)$ is Gaussian of mean $\hat{\mu}_W$ and standard deviation $\hat{\sigma}_W$;
2. $\forall z$ an output of P $\forall i \le N$: $\delta_i(z_{<i})$ is Gaussian of mean $\hat{\mu}_\delta$ and standard deviation $\hat{\sigma}_\delta$;
3. $(\hat{\mu}_W, \hat{\sigma}_W, \hat{\mu}_\delta, \hat{\sigma}_\delta, W^G(2^{64}), \delta^G(2^{64}))$ is the row of Table 40 `verify/reports/tree/leaferrors.py`;
4. $\forall Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$: $\delta^G(Q_s) \in [0, 1)$ **[hypothesis, sampled gate: `verify/gates/fx/meas_quantiles.py`]**;
5. $\forall Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$: $(1 + \delta^G(Q_s))^2 < \alpha_L/(\alpha_L - 1)$ **[hypothesis, sampled gate: `verify/gates/fx/meas_quantiles.py`]**;
6. $\forall Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$: $W^G(Q_s) \ge 0$ **[hypothesis, sampled gate: `verify/gates/fx/meas_quantiles.py`]**;
7. $\forall Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$: $\varepsilon_0^\circ(Q_s) < 1$ `verify/reports/tree/leaferrors.py`.

The sample fits the model loosely: over its two degrees, $K = 16$ keys and $M = 16$ messages each, the skewness of W is 1.2 to 4.4 and its excess kurtosis 1.9 to 25.0, and the excess kurtosis of δ_i is 7.7 to 23.3, where a Gaussian has 0 for each `verify/reports/tree/leaferrors.py`. [L3: sampled]: $\mathcal{X}$ is a sample of P, and the hypothesis extends its first two moments to a Gaussian over every

output; it is of the kind of [L2: BFLP26, (33), (34)], which their Section 7.5 instantiates by root mean squares over sampled executions.

Lemma J.65 (Quantiles over Q_s outputs [to table])**.** *Under the Gaussian model of the leaf perturbations, each Gaussian quantile is exceeded over Q_s outputs with probability at most η. **Under Hypothesis J.64**, let:*

- $Q_s \in \mathbb{Z}_{>0}$;
- $\eta \in (0,1)$.

Define:

- N, P, W, δ_i, $\hat{\mu}_W$, $\hat{\sigma}_W$, $\hat{\mu}_\delta$ *and* $\hat{\sigma}_\delta$, *those of* ***Hypothesis J.64***;
- $P^{\otimes Q_s}$, *the probability measure of Q_s independent outputs* $(z^{(1)}, \dots, z^{(Q_s)})$ *on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1)*;
- $\xi_W := \sqrt{2\ln(Q_s/\eta)}$;
- $W^G := \hat{\mu}_W + \xi_W \hat{\sigma}_W$;
- $\xi_\delta := \sqrt{2\ln(2Q_sN/\eta)}$;
- $\delta^G := |\hat{\mu}_\delta| + \xi_\delta \hat{\sigma}_\delta$.

Then

1. $P^{\otimes Q_s}\left(\exists j \le Q_s :\ W(z^{(j)}) > W^G\right) \le \eta$;
2. $P^{\otimes Q_s}\left(\exists j \le Q_s\ \exists i \le N :\ |\delta_i(z^{(j)}_{<i})| > \delta^G\right) \le \eta$.

Proof. Proof of items 1 and 2.

(L1) $Q_s/\eta > 1$
[$Q_s \ge 1$, $\eta \in (0,1)$ (the statement)]

(L2) $\ln(Q_s/\eta) \ge 0$
[(L1); Fact A.41, item 28, at $y := Q_s/\eta$]

(L3) $\xi_W^2 = 2\ln(Q_s/\eta)$
[(L2); ξ_W (the statement); Fact A.41, item 28, at $t := 2\ln(Q_s/\eta)$]

(L4) $Q_s e^{-\xi_W^2/2} = Q_s e^{-\ln(Q_s/\eta)}$
[(L3)]

(L5) $e^{-\ln(Q_s/\eta)} = \eta/Q_s$
[(L1); Fact A.41, item 28, at $y := Q_s/\eta$]

(L6) $\Rightarrow\ Q_s e^{-\xi_W^2/2} = \eta$
[(L4), (L5)]

(L7) $\forall j \le Q_s :\ P^{\otimes Q_s}(W(z^{(j)}) > W^G) \le e^{-\xi_W^2/2}$
[Fact A.45, item 13, at $X := W(z^{(j)})$, $m := \hat{\mu}_W$, $s := \hat{\sigma}_W$, $\xi := \xi_W$: $z^{(j)}$ an output of P ($P^{\otimes Q_s}$, the statement), Gaussian by **Hypothesis J.64, item 1**; $\hat{\sigma}_W \ge 0$ (**Hypothesis J.64**); $\xi_W \ge 0$ and $W^G = \hat{\mu}_W + \xi_W\hat{\sigma}_W$ (the statement)]

(L8) $P^{\otimes Q_s}(\exists j \le Q_s :\ W(z^{(j)}) > W^G) \le \sum_{j \le Q_s} P^{\otimes Q_s}(W(z^{(j)}) > W^G)$
[Fact A.45, item 5]

(L9) $\Rightarrow\ P^{\otimes Q_s}(\exists j \le Q_s :\ W(z^{(j)}) > W^G) \le Q_s e^{-\xi_W^2/2}$
[(L7), (L8)]

(L10) $\Rightarrow\ P^{\otimes Q_s}(\exists j \le Q_s :\ W(z^{(j)}) > W^G) \le \eta$
[(L6), (L9)]

(L11) $\Rightarrow$ item 1
[(L10)]

(L12) $2Q_sN/\eta > 1$
[$Q_s \ge 1$, $\eta \in (0,1)$ (the statement); $N \ge 1$ ($N = 2n$, Definition A.25)]

(L13) $\ln(2Q_sN/\eta) \ge 0$
[(L12); Fact A.41, item 28, at $y := 2Q_sN/\eta$]

(L14) $\xi_\delta^2 = 2\ln(2Q_sN/\eta)$

[(L13); ξ_δ (the statement); Fact A.41, item 28, at $t := 2\ln(2Q_sN/\eta)$]

(L15) $2Q_sNe^{-\xi_\delta^2/2} = 2Q_sNe^{-\ln(2Q_sN/\eta)}$

[(L14)]

(L16) $e^{-\ln(2Q_sN/\eta)} = \eta/(2Q_sN)$

[(L12); Fact A.41, item 28, at $y := 2Q_sN/\eta$]

(L17) $\Rightarrow\ 2Q_sNe^{-\xi_\delta^2/2} = \eta$

[(L15), (L16)]

(L18) $\forall j \le Q_s\ \forall i \le N:\ |\delta_i(z_{<i}^{(j)})| \le |\delta_i(z_{<i}^{(j)}) - \hat{\mu}_\delta| + |\hat{\mu}_\delta|$

[Fact A.41, item 1, at $(x, y) := (\delta_i(z_{<i}^{(j)}) - \hat{\mu}_\delta, \hat{\mu}_\delta)$]

(L19) $\Rightarrow\ \forall j \le Q_s\ \forall i \le N:\ \{|\delta_i(z_{<i}^{(j)})| > \delta^G\} \subseteq \{|\delta_i(z_{<i}^{(j)}) - \hat{\mu}_\delta| > \xi_\delta\hat{\sigma}_\delta\}$

[(L18); $\delta^G = |\hat{\mu}_\delta| + \xi_\delta\hat{\sigma}_\delta$ (the statement)]

(L20) $\forall j \le Q_s\ \forall i \le N:\ P^{\otimes Q_s}(|\delta_i(z_{<i}^{(j)}) - \hat{\mu}_\delta| > \xi_\delta\hat{\sigma}_\delta) \le 2e^{-\xi_\delta^2/2}$

[Fact A.45, item 13, at $X := \delta_i(z_{<i}^{(j)})$, $m := \hat{\mu}_\delta$, $s := \hat{\sigma}_\delta$, $\xi := \xi_\delta$: $z^{(j)}$ an output of P ($P^{\otimes Q_s}$, the statement), Gaussian by **Hypothesis J.64, item 2**; $\hat{\sigma}_\delta \ge 0$ (**Hypothesis J.64**); $\xi_\delta \ge 0$ (the statement)]

(L21) $\Rightarrow\ \forall j \le Q_s\ \forall i \le N:\ P^{\otimes Q_s}(|\delta_i(z_{<i}^{(j)})| > \delta^G) \le 2e^{-\xi_\delta^2/2}$

[(L19), (L20); Fact A.45, item 12]

(L22) $P^{\otimes Q_s}(\exists j \le Q_s\ \exists i \le N:\ |\delta_i(z_{<i}^{(j)})| > \delta^G) \le \sum_{j\le Q_s}\sum_{i\le N} P^{\otimes Q_s}(|\delta_i(z_{<i}^{(j)})| > \delta^G)$

[Fact A.45, item 5]

(L23) $\Rightarrow\ P^{\otimes Q_s}(\exists j \le Q_s\ \exists i \le N:\ |\delta_i(z_{<i}^{(j)})| > \delta^G) \le 2Q_sNe^{-\xi_\delta^2/2}$

[(L21), (L22)]

(L24) $\Rightarrow\ P^{\otimes Q_s}(\exists j \le Q_s\ \exists i \le N:\ |\delta_i(z_{<i}^{(j)})| > \delta^G) \le \eta$

[(L17), (L23)]

(L25) $\Rightarrow$ item 2

[(L24)]

□ (items 1 and 2)

The symbols of the Gaussian model. Table 41: the symbols of **Hypothesis J.64** and Lemma J.65.

Symbol	Definition	Where
$\mathcal{X}$	A sample of the outputs of P	**Hypothesis J.64**
$\hat{\mu}_W$, $\hat{\sigma}_W$	The sample mean and standard deviation of W	**Hypothesis J.64**
$\hat{\mu}_\delta$, $\hat{\sigma}_\delta$	The sample mean and standard deviation of δ_i over every leaf	**Hypothesis J.64**
ξ_W, ξ_δ	$\sqrt{2\ln(Q_s/\eta)}$, $\sqrt{2\ln(2Q_sN/\eta)}$	Lemma J.65
W^G, δ^G	$\hat{\mu}_W + \xi_W\hat{\sigma}_W$, $\lvert\hat{\mu}_\delta\rvert + \xi_\delta\hat{\sigma}_\delta$	Lemma J.65

Table 41: Symbols of **Hypothesis J.64** and Lemma J.65.

Definition J.66 (The floating-point signer's terms [to table])**. Under Hypothesis J.63**, let:

- $p \in \{53, 64, 113\}$;
- $\zeta = 0$;
- (f, g, F, G) be a checked key (Definition 5.5);
- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$.

Define:

- The signer's words and parameters
  - $u = 2^{-p}$;
  - $\lambda = 128$ at $n = 512$ and $\lambda = 256$ at $n = 1024$;

  - $\alpha = 2\lambda + 1$;
  - $\sigma_{\min}$, that of SamplerZ (Algorithm 8), Require;
- The key bounds
  - $\hat{K}_n$, the sample maxima of **Hypothesis J.63, item 1** (Definition 4.6);
  - ℓ and κ_{root}, those of $\hat{K}_n$;
  - m_0, M_0, $\bar{g}_{11}$, d_{lo} and d_{hi}, those of Proposition 5.8;
  - $\bar{\Xi}_0$, that of Lemma H.21;
  - $\bar{e}_{00}$, that of Lemma J.37;
  - $\bar{e}_{11}$, that of Lemma J.38;
  - $\bar{E}_a$, that of Lemma J.39;
  - $E_{00} = \bar{e}_{00} M_0$;
  - $E_{11} = \bar{e}_{11} \bar{g}_{11}$;
  - $E_{01} = \max_\psi \bar{E}_a$;
- The sampler's bounds
  - $e_{+,k}$, $k \le 18$, and $\mathcal{K}_C$, those of Lemma J.52;
  - $e_+ = \max_k e_{+,k}$;
  - $e_{\text{ccs}} = u$;
  - $p_C^D = \sum_{k \in \mathcal{K}_C} \bar{e}_{\text{fl},k}$, with $\bar{e}_{\text{fl},k}$ of Lemma G.73 at $\sigma_{\min}$ and e_{ccs};
- The fringe sets
  - $C_i := \lfloor \widetilde{t}_i \rfloor + C$, the samples of the candidates in the set C of Definition J.55 at $(\widetilde{\sigma}_i, \widetilde{t}_i)$;
  - $\bar{U} = 2^{s_c - 63}(1 + \epsilon_C)$, the bound of Lemma J.59, item 2, on the $\bar{U}(\tau)$ of Definition J.55, with s_c of Lemma J.56 and ϵ_C of Lemma J.59;
  - $\bar{p}_C$, the right side of Lemma J.60, the bound on the $\bar{p}_C(\tau)$ of Definition J.55;
  - κ_C, that of Definition A.28 at C_i, $\bar{U}$ and $\bar{p}_C$;
  - $M_C = 3$;
- The error chain
  - $\chi_{\text{root}} = \max(\bar{e}, \max_\psi \chi_{11})$, with $\bar{e}$ of Corollary J.43 and χ_{11} of Corollary J.44;
  - χ_{leaf}, that of Corollary J.42;
- The leaf deviations
  - $\sigma_{\max} = 1.17^2 \sigma_{\min}$;
  - $\bar{\delta} := \chi_\sigma / (1 - \chi_\sigma)$, the bound of Definition A.27, with χ_σ of Corollary G.41 at u and χ_{leaf};
  - $s_\star = \sigma_{\min}(1 - \bar{\delta}) \left(\alpha_L + (1 - \alpha_L)(1 - \bar{\delta})^2\right)^{-1/2}$;
  - $\epsilon = 2 \sum_{k \ge 1} e^{-2\pi^2 s_\star^2 k^2}$, the normalizer deviation at $s_\star$;
- The node bounds
  - $E_l = \max(E_l^{\text{child}}, E_l^{\text{root}})$ of Corollary G.43 at $\zeta = 0$, $\chi = \chi_{\text{leaf}}$, d_{lo}, d_{hi}, ℓ, m_0, $e_{00} = E_{00}/m_0$, E_{01} and κ_{root};
- The center shifts
  - $\bar{T}$, that of Lemma H.22;
  - $\bar{e}_{\text{root}}$, that of Corollary J.46;
  - D° and γ_S, those of Corollary G.62;
  - γ, that of Theorem G.59;
  - D_Z° and $\bar{Z}$, those of Lemma H.23 at $\zeta = 0$, $\hat{K}_n$, $\bar{T}$, $\bar{e} := \bar{e}_{\text{root}}$, $\bar{\sigma} := \sigma_{\max}$, $\bar{\Xi}_0$ and $\bar{\delta}$;
- The terms
  - $D_S = D^\circ / (1 - \gamma - \gamma_S)$, that of Corollary G.62, at $\zeta = 0$, $\bar{T}$, $\bar{e}_{\text{root}}$ in place of $\|e_{\text{root}}\|$ and $Z := \bar{Z}$;
  - $W^\circ = D_S^2 / \sigma_{\min}^2$;
  - ϖ, that of Lemma G.73 at $\sigma_{\min}$, $\sigma_{\max}$ and e_{ccs};
  - $\bar{e}_{\text{norm}}$, that of Lemma G.73 at $(e_{+,k})_k$;
  - A, $\mathfrak{L}_B$, $\mathfrak{L}_{\bar{\delta}}$, $\mathfrak{L}_\Delta$, $\mathfrak{L}_\Phi$, $\bar{\phi}$, $M_{2\alpha}$, p_τ and p'_τ: the terms of $\ln R$ of Corollary 4.10, preconditions 1 to 3, and Theorem 4.11, precondition 1, at $e_{+,k}$, e_{ccs}, p_C^D, χ_{root}, χ_{leaf}, $\bar{\delta}$, E_l, D_S

and W°;
- $\lambda_{\mathcal{F}}$, that of Definition 5.3 at A, κ_C, $\bar{p}_C$ and M_C.

Measured:

- The values of the terms (Table 44) `verify/reports/fp/terms.py`;
- $\sigma_{\max}(1+\bar{\delta}) \le 1.778$ at both degrees `verify/reports/fp/terms.py`;
- $\varpi \le 2^{-77.22}$ at both degrees `verify/reports/fp/terms.py`;
- $\varepsilon_0^\circ < 1$ at both degrees, ε_0° that of Definition A.40 at $(\alpha_L, \sigma_{\min}, \sigma_{\max}, \bar{\delta}, \sigma_{\max}(W^\circ)^{1/2})$ `verify/reports/fp/terms.py`;
- $\bar{e}_{\text{norm}} \le 2^{-48.64}$ at both degrees `verify/reports/fp/terms.py`.

Lemma J.67 (The floating-point signer as a Falcon-type signer [to table])**.** *On a checked key, the floating-point signer is a Falcon-type signer at $(u, 0)$, its computed Gram matrix entries lie within E_{00}, E_{11} and E_{01} of the exact ones, and its diagonals lie within their floors and ceilings.* ***Under Hypotheses J.61*** *and J.31, let:*

- *(f, g, F, G) be a checked key (Definition 5.5).*

Define:

- *m_0 and M_0, those of Proposition 5.8;*
- *$\bar{g}_{11}$, d_{lo}, d_{hi} and the signer, those of Definition J.66;*
- *E_{00}, E_{11} and E_{01}, those of Definition J.66;*
- *$\forall j \in \{00, 11\}:$ d_j^ν, the diagonals of the nodes ν of the key's tree, those of Corollary G.36;*
- *d_ν, a diagonal d_j^ν of the node ν.*

Then

1. *The signer is a Falcon-type signer at $(u, 0)$ (Definition 4.5);*
2. *$\forall w$ the signer computes: $\text{fl}(w)\ \mathcal{N}\,(u, 0)\ w$;*
3. *$\forall \psi:\ |\widetilde{g}_{00} - g_{00}| \le E_{00}$;*
4. *$\forall \psi:\ |\widetilde{g}_{11} - g_{11}| \le E_{11}$;*
5. *$\forall \psi:\ |\widetilde{g}_{01} - g_{01}| \le E_{01}$;*
6. *$\forall \psi:\ m_0 \le g_{00} \le M_0$;*
7. *$\forall \nu\ \forall \psi:\ d_{\text{lo}} \le d_\nu \le d_{\text{hi}}$.*

Proof. (L1) the signer is a Falcon-type signer at $(u, 0)$
[Definition 4.5 at the reference key generation (line 3 of keygen (Algorithm 11)) and ffSampling$^{\mathcal{F}}$ (Algorithm 10) in $\mathcal{F}$; Definition J.1: $(u, \zeta) = (2^{-p}, 0)$, $2^{-p} \in [0, 1)$; the code's complex layer, that of Definition A.8: Lemma J.26, items 1 to 4]

(L2) $\Rightarrow$ item 1
[(L1)]

(L3) $\forall w$ the signer computes : $\text{fl}(w)\ \mathcal{N}\,(u, 0)\ w$
[the rounded operations: Lemma J.15, items 1 and 2; Lemma J.17, items 1 and 2; Lemma J.18, items 1 and 2; Lemma J.19, items 1 and 2; Lemma J.16, items 1 to 5; the exact ones: Lemmas J.23 and J.24; Lemma J.25, items 1 to 4; **Hypothesis J.31, item (1)**: no value leaves the domain of Definition J.1; **Hypothesis J.61, item 1**]

(L4) $\Rightarrow$ item 2
[(L3)]

(L5) $\forall \psi:\ |\widetilde{g}_{00} - g_{00}| \le E_{00}$
[Lemma J.37 at $g_{00}(\psi) \le M_0$ (Lemma H.19, item 4); E_{00} (Definition J.66); **Hypothesis J.31, item (1)**]

(L6) $\Rightarrow$ item 3
[(L5)]

(L7) $\forall \psi :\ |\widetilde{g}_{11} - g_{11}| \le E_{11}$
[Lemma J.38 at $g_{11}(\psi) \le \bar{g}_{11}$ (Lemma H.19, item 5); E_{11} (Definition J.66); **Hypothesis J.31, item (1)**]

(L8) $\Rightarrow$ item 4
[(L7)]

(L9) $\forall \psi :\ |\widetilde{g}_{01} - g_{01}| \le E_{01}$
[Lemma J.39; E_{01} (Definition J.66); **Hypothesis J.31, item (1)**]

(L10) $\Rightarrow$ item 5
[(L9)]

(L11) $\forall \psi :\ g_{00} \in [m_0, M_0]$
[Lemma H.19, item 4, at a checked key]

(L12) $\Rightarrow$ item 6
[(L11)]

(L13) $\forall \nu\ \forall \psi :\ d_\nu \in [d_{\mathrm{lo}}, d_{\mathrm{hi}}]$
[Proposition 5.8, item 1, at a checked key]

(L14) $\Rightarrow$ item 7
[(L13)]

□ (items 1 to 7)

J.5.2 The preconditions

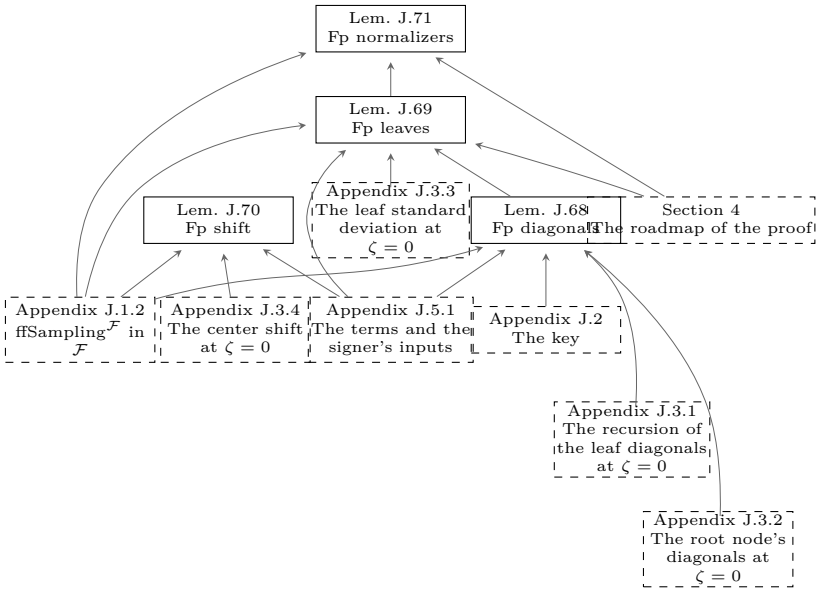


Figure 109: Dependencies, Appendix J.5.2.

Lemma J.68 (The floating-point signer's diagonal preconditions [to table])**.** *On a checked key, the floating-point signer's root bound and leaf bound are those the theorem's first two preconditions define.* ***Under Hypotheses J.61*** *and J.31, let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The signer and its constants, those of Definition J.66;*
- χ_{root} *and* χ_{leaf}*, those of Definition J.66.*

Then

1. χ_{root} *meets Lemma 4.7, precondition 1;*
2. χ_{leaf} *meets Lemma 4.7, precondition 2.*

Proof. (L1) $\forall\psi$ at the root node : $\widetilde{d}_{00}\ \mathcal{I}\left(\chi^{\pm}_{\text{root}}, 0\right)\ d_{00}$
[Corollary J.43, at the bounds of Lemmas J.37, J.38 and J.39; $\chi_{\text{root}} = \max(\bar{e}, \chi_{11})$ (Definition J.66); **Hypothesis J.31, item (1)**]

(L2) $\forall\psi$ at the root node : $\widetilde{d}_{11}\ \mathcal{I}\left(\chi^{\pm}_{\text{root}}, 0\right)\ d_{11}$
[Corollary J.44, at the bounds of Lemmas J.37, J.38 and J.39; $\chi_{\text{root}} = \max(\bar{e}, \chi_{11})$ (Definition J.66); **Hypothesis J.31, item (1)**]

(L3) $\Rightarrow$ item 1
[(L1), (L2); χ_{11} the signer's own bound (Lemma 4.7, precondition 1)]

(L4) $\forall\nu\ \forall\psi$: $d_\nu \in [d_{\text{lo}}, d_{\text{hi}}]$
[Lemma J.67, item 7; **Hypotheses J.61 and J.31**, named by Lemma J.67]

(L5) $\Rightarrow$ item 2
[(L1), (L2), (L4); Corollary J.42, item 2, at $d \in [d_{\text{lo}}, d_{\text{hi}}]$ and κ_k of $\hat{K}_n$; χ_{leaf} (Definition J.66)]
□ (items 1 and 2)

Lemma J.69 (The floating-point signer's leaf preconditions [to table])**.** *On a checked key, the floating-point signer's leaf bound and off-diagonal bound are those the theorem's third and fourth preconditions define, and the theorem's assumption on χ^{ζ}_{σ} holds.* ***Under Hypotheses J.61*** *and J.31, let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The signer and its constants, those of Definition J.66;*
- χ_{leaf}, $\bar{\delta}$ *and* E_l, *those of Definition J.66;*
- χ_σ, *that of Corollary G.41 at* χ_{leaf};
- $s_{\min}$ *and* χ^{ζ}_{σ}, *those of Lemma 4.7, precondition 3;*
- $\bar{e}_0$, *that of Corollary G.43 at* (u, ζ), $\chi := \chi_{\text{leaf}}$ *and* d_{lo}.

Measured:

- $\chi_\sigma < 1$ *at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/tree/general_assume.py];*
- $\bar{e}_0 < 1$ *at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/tree/general_assume.py];*
- $\bar{\delta} < 1$ *at* $n = 512$ *and* $n = 1024$ *[gate: verify/gates/tree/general_assume.py].*

Then

1. $\bar{\delta}$ *meets Lemma 4.7, precondition 4;*
2. E_l *meets Lemma 4.8, precondition 1;*
3. $\chi^{\zeta}_{\sigma} < 1$;
4. $\bar{e}_0 < 1$;
5. $\bar{\delta} < 1$.

Proof. (L1) $\chi^{\zeta}_{\sigma} = \chi_\sigma$
[$\chi^{\zeta}_{\sigma} = \chi_\sigma + k_J\zeta/s_{\min}$ (Lemma 4.7, precondition 3); $\zeta = 0$ (Definition J.66)]

(L2) $\chi^{\zeta}_{\sigma} < 1$
[(L1); the measured row]

(L3) $\Rightarrow$ item 3
[(L2)]

(L4) $\forall\nu$ of depth $h-1$ $\forall\psi$: $\widetilde{d}_\nu\ \mathcal{I}\left(\chi^{\pm}_{\text{leaf}}, 0\right)\ d_\nu$
[Lemma J.68, item 2; **Hypotheses J.61 and J.31**, named by Lemma J.68]

(L5) $\Rightarrow$ item 1
[(L2), (L4); Corollary J.45 at $c_n := 1/s$, s of Definition A.25, its assumption A3 by Lemma J.29; $\bar{\delta}$ (Definition J.66)]

(L6) $\Rightarrow$ item 2

[(L4); Corollary G.43 at $\zeta = 0$; E_l (Definition J.66)]

(L7) $\bar{e}_0 < 1$

[the measured row]

(L8) $\Rightarrow$ item 4

[(L7)]

(L9) $\bar{\delta} < 1$

[the measured row]

(L10) $\Rightarrow$ item 5

[(L9)]

□ (items 1 to 4)

Lemma J.70 (The floating-point signer's shift preconditions [to table])**.** *On a checked key, the floating-point signer's center lies within $\bar{T}$, its shift at the root node's entry within $\bar{e}_{\text{root}}$ and its samples on the tail-cut event within $\bar{Z}$; its shift bound is the one the theorem's fifth precondition defines, and the theorem's assumption on $\gamma + \gamma_S$ holds.* ***Under Hypotheses J.61*** *and J.31, let:*

- *(f, g, F, G) be a checked key (Definition 5.5).*

Define:

- *The signer and its constants, those of Definition J.66;*
- *$\mathsf{h}(\mathsf{m})$, the hashed message, the input of ffSampling$^{\mathcal{F}}$ (Algorithm 10);*
- *t, the root node's center (ffSampling$^{\mathcal{F}}$, lines 9 to 20);*
- *$\widetilde{t}_T$, its computed value (ffSampling$^{\mathcal{F}}$, lines 9 to 20);*
- *z', that of ffSampling$^{\mathcal{F}}$, line 27;*
- *$\sigma_{\max}$, $\bar{\delta}$, $\bar{Z}$, $\bar{e}_{\text{root}}$, D°_Z, D_S and W°, those of Definition J.66;*
- *$\bar{T}$, that of Lemma H.22;*
- *$\bar{\Xi}_0$, that of Lemma H.21;*
- *γ, that of Theorem G.59;*
- *γ_S, that of Corollary G.62.*

Measured:

- *$\gamma + \gamma_S < 1$ at $n = 512$ and $n = 1024$ [gate: `verify/gates/tree/general_assume.py`];*
- *$\bar{\Xi}_0 D^{\circ}_Z < 1 - \gamma - \gamma_S$ at $n = 512$ and $n = 1024$ [gate: `verify/gates/tree/general_norm.py`].*

Then

1. *$\|t\| \le \bar{T}$;*
2. *$\|\widetilde{t}_T - t\| \le \bar{e}_{\text{root}}$;*
3. *$\gamma + \gamma_S < 1$;*
4. *$\forall z \in S : \ \|z'\| \le \bar{Z}$;*
5. *D_S and W° meet Lemma 4.9, preconditions 1 and 2.*

Proof. (L1) $\|t\| \le \bar{T}$

[Lemma H.22 at the checked key (Definition J.66) and $\mathsf{h}(\mathsf{m})$; $\bar{T}$ (Lemma H.22)]

(L2) $\Rightarrow$ item 1

[(L1)]

(L3) $\|\widetilde{t}_T - t\| \le \bar{e}_{\text{root}}$

[Corollary J.46, item 3, at the checked key (Definition J.66) and $\mathsf{h}(\mathsf{m})$; **Hypothesis J.31, item (1)**; $\bar{e}_{\text{root}}$ (Definition J.66)]

(L4) $\Rightarrow$ item 2

[(L3)]

(L5) $\gamma + \gamma_S < 1$

[the first measured row]

(L6) $\Rightarrow$ item 3

[(L5)]

(L7) $\forall i \le N\ \forall z_{<i}\ \exists\, \delta_i \in \mathbb{R},\ |\delta_i| \le \bar{\delta} :\ \widetilde{\sigma}_i = \sigma_i(1+\delta_i)$

[Lemma 4.7 at the floating-point signer and the checked key, its assumptions by Lemma J.67, items 2 to 7, Lemma J.68, items 1 and 2, Lemma J.69, item 3, and Lemma J.29; δ_i (Definition A.27); **Hypotheses J.61 and J.31**, named by Lemma J.67, Lemma J.68 and Lemma J.69]

(L8) $\forall i \le N :\ \sigma_i \le \sigma_{\max}$

[Lemma J.30, item 2, at the floating-point signer; $\sigma_{\max} = 1.17^2\sigma_{\min}$ (Definition J.66)]

(L9) $\|\mathcal{L}_T^{-1}\| \le \bar{\Xi}_0$

[Lemma H.21 at the checked key]

(L10) $\forall z \in S :\ \|z'\| \le \bar{Z}$

[Lemma H.23 at $\zeta = 0$, $\hat{K}_n$, $\bar{T}$, $\bar{e} := \bar{e}_{\mathrm{root}}$, $\bar{\sigma} := \sigma_{\max}$, $\bar{\Xi}_0$ and $\bar{\delta}$: its assumptions by (L1) to (L9) and the second measured row]

(L11) $\Rightarrow$ item 4

[(L10)]

(L12) $D_S = D^\circ/(1-\gamma-\gamma_S)$

[D_S (Definition J.66): Corollary G.62, at $\zeta = 0$, $\hat{K}_n$, $\bar{e}_{\mathrm{root}}$ in place of $\|e_{\mathrm{root}}\|$, $\bar{T}$, $Z := \bar{Z}$, τ, $\sigma_{\max} = 1.17^2\sigma_{\min}$; its assumptions by (L1), (L3), (L7) and (L10)]

(L13) $W^\circ = D_S^2/\sigma_{\min}^2$

[W° (Definition J.66)]

(L14) $\Rightarrow$ item 5

[(L12), (L13); Lemma 4.9, preconditions 1 and 2; its assumptions by (L1), (L10)]

□ (items 1 to 5)

Lemma J.71 (The floating-point signer's normalizers [to table])**.** *At every leaf of the floating-point signer, the normalizer of the computed Gaussian is within a factor $1 \pm \epsilon$ of its integral, and $\epsilon < 1$.* ***Under Hypotheses J.48**, J.61 and J.31, let:*

- *(f, g, F, G) be a checked key (Definition 5.5).*

Define:

- *$\sigma_{\min}$, α, $\bar{\delta}$, $s_\star$, ϵ and the signer, those of Definition J.66;*
- *χ_σ^ζ, that of Lemma J.69;*
- *N, σ_i, $\texttt{isigma}_i$ and $\widetilde{\sigma}_i = 1/\texttt{isigma}_i$, $i \le N$, those of Definition A.25 at $\texttt{isigma} := \texttt{isigma}_i$;*
- *$\widetilde{ccs}_i := \mathrm{fl}(\texttt{isigma}_i \cdot \sigma_{\min})$ (line 6 of SamplerZ (Algorithm 8) at the leaf i);*
- *$\rho_{s,c}(\mathbb{Z})$, that of Section 3.1.*

Measured:

- *$\epsilon < 1$ at $n = 512$ and $n = 1024$ [gate: `verify/gates/tree/general_assume.py`].*

Then

1. *$\epsilon \in [0, 1)$;*
2. *$\forall i \le N\ \forall z_{<i}\ \forall c \in \mathbb{R} :\ \rho_{\widetilde{\sigma}_i, c}(\mathbb{Z}) \in [(1-\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i, (1+\epsilon)\sqrt{2\pi}\,\widetilde{\sigma}_i]$.*

Proof. (L1) $\epsilon \ge 0$

[ϵ (the statement); $e^t > 0$ (Fact A.41, item 12)]

(L2) $\epsilon < 1$

[the measured row]

(L3) $\Rightarrow$ $\epsilon \in [0, 1)$

[(L1), (L2)]

(L4) $\Rightarrow$ item 1

[(L3)]

(L5) $\chi_\sigma^\zeta \in [0,1)$

[Lemma 4.7, (L7); Lemma J.69, item 3; **Hypotheses J.61 and J.31**, named by Lemma J.69]

(L6) $\bar{\delta} \geq 0$

[(L5); $\bar{\delta} = \chi_\sigma^\zeta/(1-\chi_\sigma^\zeta)$ (Definition J.66; Corollary J.45)]

(L7) $\bar{\delta} < 1$

[Lemma J.69, item 5; **Hypotheses J.61 and J.31**, named by Lemma J.69]

(L8) $\alpha_L + (1-\alpha_L)(1-\bar{\delta})^2 = 1 + (\alpha_L - 1)(1-(1-\bar{\delta})^2)$

[expand]

(L9) $\alpha_L + (1-\alpha_L)(1-\bar{\delta})^2 \geq 1$

[(L6), (L7), (L8); $\alpha > 1$ (Definition J.66); Fact A.41, item 8]

(L10) $s_\star \leq \sigma_{\min}$

[(L6), (L9); $s_\star$ (the statement); $t \mapsto t^{-1/2}$ nonincreasing on $(0,\infty)$ (Fact A.41, item 5)]

(L11) $s_\star > 0$

[(L7), (L9); $s_\star$ (the statement); the stored word $\sigma_{\min} > 0$ [L0: `sign_sampler.c:44-56`]]

(L12) $\forall i \leq N\ \forall z_{<i}:\ \widetilde{cc}\widetilde{s}_i < 1$

[**Hypothesis J.48, item 1**]

(L13) $\forall a \in \mathbb{R},\ a \geq 1:\ \mathrm{fl}(a) \geq 1$

[Fact J.2, item 8, at $(1,a)$; $1 \in \mathcal{F}$ (Fact J.2, item 4)]

(L14) $\forall i \leq N\ \forall z_{<i}:\ \texttt{isigma}_i\, \sigma_{\min} < 1$

[(L12), (L13) at $a := \texttt{isigma}_i\, \sigma_{\min}$]

(L15) $\forall i \leq N\ \forall z_{<i}\ \exists \delta_i \in \mathbb{R},\ |\delta_i| \leq \bar{\delta}:\ \widetilde{\sigma}_i = \sigma_i(1+\delta_i)$

[Lemma 4.7 at the floating-point signer and the checked key, its assumptions by Lemma J.70, (L7); **Hypotheses J.61 and J.31**, named by Lemma J.70]

(L16) $\forall i \leq N:\ \sigma_i > \sigma_{\min}$

[Lemma J.30, item 1, at the floating-point signer]

(L17) $\forall i \leq N\ \forall z_{<i}:\ \widetilde{\sigma}_i > 0$

[(L7), (L15), (L16); the stored word $\sigma_{\min} > 0$ [L0: `sign_sampler.c:44-56`]]

(L18) $\forall i \leq N\ \forall z_{<i}:\ \widetilde{\sigma}_i > \sigma_{\min}$

[(L14), (L17); $\widetilde{\sigma}_i = 1/\texttt{isigma}_i$ (the statement)]

(L19) $\forall s > 0\ \forall c \in \mathbb{R}:\ \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\, s) - 1 = 2\sum_{k\geq 1} e^{-2\pi^2 s^2 k^2} \cos(2\pi k c)$

[Lemma E.2, item 1; $d(s,c) = \rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\, s) - 1$ (Definition A.29)]

(L20) $\forall s > 0\ \forall c \in \mathbb{R}:\ |\rho_{s,c}(\mathbb{Z})/(\sqrt{2\pi}\, s) - 1| \leq 2\sum_{k\geq 1} e^{-2\pi^2 s^2 k^2}$

[(L19); $|\cos| \leq 1$ (Fact A.41, item 12); $|x+y| \leq |x| + |y|$, $|xy| = |x||y|$ (Fact A.41, item 1)]

(L21) $\forall s \geq s' > 0:\ 2\sum_{k\geq 1} e^{-2\pi^2 s^2 k^2} \leq 2\sum_{k\geq 1} e^{-2\pi^2 s'^2 k^2}$

[exp increasing (Fact A.41, item 5), term by term]

(L22) $\forall i \leq N\ \forall z_{<i}\ \forall c \in \mathbb{R}:\ |\rho_{\widetilde{\sigma}_i, c}(\mathbb{Z})/(\sqrt{2\pi}\, \widetilde{\sigma}_i) - 1| \leq \epsilon$

[(L20) at $s := \widetilde{\sigma}_i$; (L21) at $(s,s') := (\widetilde{\sigma}_i, s_\star)$ by (L10), (L11), (L18); ϵ (the statement)]

(L23) $\Rightarrow$ item 2

[(L22); $\sqrt{2\pi}\, \widetilde{\sigma}_i > 0$ by (L17)]

$\square$ (items 1 and 2)

J.5.3 The base sampler's inputs

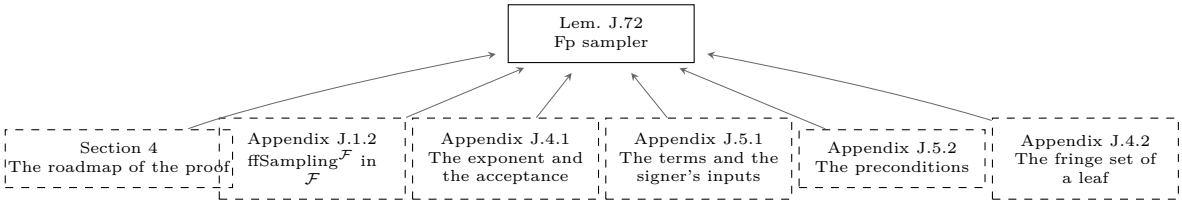


Figure 110: Dependencies, Appendix J.5.3.

Lemma J.72 (The floating-point signer's base sampler inputs [to table])**.** *At every leaf, the row bounds of the floating-point base sampler meet the assumptions of Lemma G.73 off the fringe set. On the fringe set, the ideal mass is at most p_C^D, the computed measure is at most $\bar{U}$ times the ideal one, and the computed mass is at most $\bar{p}_C$.* ***Under Hypotheses J.48****, J.47, J.54, J.61 and J.31, let:*

- (f, g, F, G) *be a checked key (Definition 5.5).*

Define:

- *The signer and its constants, those of Definition J.66;*
- e_{ccs}, p_C^D, C_i, $\bar{U}$, $\bar{p}_C$ *and* $\bar{\delta}$, *those of Definition J.66;*
- $\forall k \leq 18:\ e_{+,k}$, *that of Lemma J.52;*
- $\sigma_{\min}$ *and* σ_0, *those of* SamplerZ *(Algorithm 8), Require;*
- *acc, ccs and x, those of Lemma G.64;*
- $\widetilde{acc}$ *and* z_{acc}, *those of Fact G.66;*
- $\bar{U}(\tau)$ *and* $\bar{p}_C(\tau)$, *those of Definition J.55.*

Then

1. $\forall i \leq N\ \forall z_{<i}$: $e_{+,k}$ *and* e_{ccs} *meet Lemma G.73's assumptions at* $\mathcal{Y} := \mathcal{Z}_i \setminus C_i$;
2. $\forall i \leq N\ \forall z_{<i}:\ \widetilde{D}_i(C_i) \leq p_C^D$;
3. $\forall i \leq N\ \forall z_{<i}\ \forall z \in C_i:\ \widetilde{B}_i(z) \leq \bar{U}\,\widetilde{D}_i(z)$;
4. $\forall i \leq N\ \forall z_{<i}:\ \widetilde{B}_i(C_i) \leq \bar{p}_C$.

Proof.

DEFINES τ, that of Lemma H.23
DEFINES s_c, that of Lemma J.56
DEFINES ϵ_C, that of Lemma J.59

(L1) $\forall z:\ acc(z) = ccs\, e^{-x(z)}$

[Lemma G.64]

(L2) $\forall z:\ \widetilde{acc}(z) = z_{\mathrm{acc}}/2^{64}$

[Fact G.66 at each candidate's computed si and r' (Lemma J.50); $si \geq 0$ (Lemma J.50, item 1, at x, its assumption A1 by Lemma J.56, item 3), assumption A1 of Fact G.66; **Hypothesis J.31**, named by Lemmas J.50 and J.56]

(L3) $\forall i \leq N\ \forall z_{<i}:\ \widetilde{\sigma}_i \in [\sigma_{\min}, \sigma_0]$

[**Hypothesis J.48, item 1**; **Hypothesis J.47**]

(L4) $\forall i \leq N\ \forall z_{<i}:\ \widetilde{\sigma}_i \leq 1.17^2 \sigma_{\min}(1 + \bar{\delta})$

[$\sigma_i < 1.17^2\sigma_{\min}$ (Lemma J.30, item 2, at the floating-point signer); $|\delta_i| \leq \bar{\delta}$ (Lemma 4.7 at the floating-point signer and the checked key, its assumptions by Lemma J.67, items 2 to 7, Lemma J.68, items 1 and 2, Lemma J.69, items 1 and 3, and Lemma J.29; **Hypothesis J.61**, the clauses of Lemmas J.67, J.68 and J.69); $\widetilde{\sigma}_i = \sigma_i(1 + \delta_i)$ (Definition A.27)]

(L5) $\Rightarrow$ $\forall i \le N\ \forall z_{<i}:\ e_{+,k},\ e_{\mathrm{ccs}}$ meet Lemma G.73's assumptions at $\mathcal{Y} := \mathcal{Z}_i \setminus C_i$
[(L1), (L2), (L3), (L4); Lemma J.52, items 1 to 6; C_i the samples of the candidates with $si \ge 64$ (Definition J.66); $e_{+,k}$, e_{ccs} (Definition J.66); **Hypothesis J.31, item (1)**; **Hypotheses J.48 and J.47**, named by Lemma J.52]

(L6) $\Rightarrow$ item 1
[(L5)]

(L7) $\forall i \le N\ \forall z_{<i}:\ \widetilde{D}_i(C_i) \le p_C^D$
[(L3), (L4); Lemma G.73, item 4, at $C := C_i$; p_C^D (Definition J.66)]

(L8) $\Rightarrow$ item 2
[(L7)]

(L9) $\forall i \le N\ \forall z_{<i}\ \forall z \in C_i:\ \widetilde{B}_i(z) \le \bar{U}(\tau)\,\widetilde{D}_i(z)$
[(L3), (L4); Lemma J.59, item 1, at $(\widetilde{\sigma}, \widetilde{t}) := (\widetilde{\sigma}_i, \widetilde{t}_i)$; $C_i = \lfloor \widetilde{t}_i \rfloor + C$ (Definition J.66); $\widetilde{B}_i(\lfloor \widetilde{t}_i \rfloor + z) = \widetilde{B}(z)$, $\widetilde{D}_i(\lfloor \widetilde{t}_i \rfloor + z) = \widetilde{D}(z)$ at the candidates z (Definition J.55); **Hypotheses J.48, J.47, J.31 and J.54**, named by Lemma J.59]

(L10) $\bar{U}(\tau) \le 2^{s_c - 63}(1 + \epsilon_C)$
[Lemma J.59, item 2; **Hypotheses J.48, J.47, J.31 and J.54**, named by Lemma J.59]

(L11) $\Rightarrow$ $\forall i \le N\ \forall z_{<i}\ \forall z \in C_i:\ \widetilde{B}_i(z) \le \bar{U}\,\widetilde{D}_i(z)$
[(L9), (L10); $\bar{U}$ (Definition J.66)]

(L12) $\Rightarrow$ item 3
[(L11)]

(L13) $\forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(C_i) \le \bar{p}_C(\tau)$
[(L3), (L4); $\bar{p}_C(\tau)$ (Definition J.55); $C_i = \lfloor \widetilde{t}_i \rfloor + C$ (Definition J.66); $\widetilde{B}_i(\lfloor \widetilde{t}_i \rfloor + z) = \widetilde{B}(z)$ at the candidates z (Definition J.55)]

(L14) $\Rightarrow$ $\forall i \le N\ \forall z_{<i}:\ \widetilde{B}_i(C_i) \le \bar{p}_C$
[(L13); Lemma J.60; $\bar{p}_C$ (Definition J.66); **Hypotheses J.48, J.47, J.31 and J.54**, named by Lemma J.60]

(L15) $\Rightarrow$ item 4
[(L14)]

□ (items 1, 2, 3 and 4)

J.5.4 The loss in bits

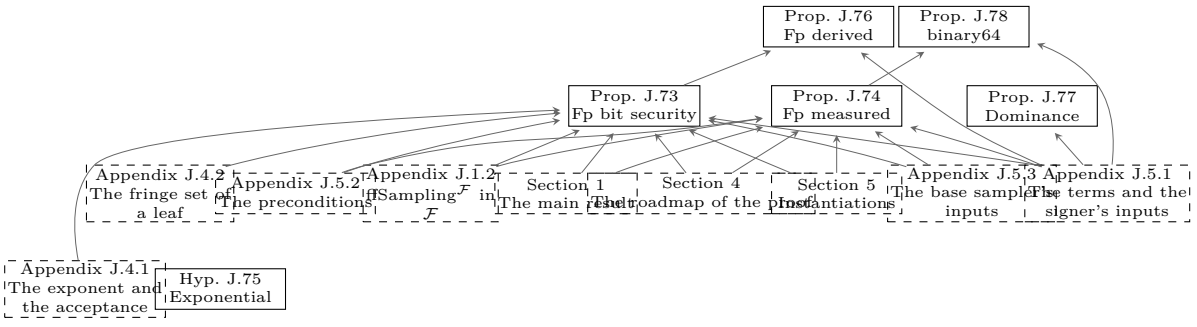


Figure 111: Dependencies, Appendix J.5.4.

Structure. Proposition J.73 states the floating-point signer's bit security; Proposition J.74 the same under **Hypothesis J.64**; Proposition J.76 the bit security on the derived bounds; Proposition J.77 the dominant term; Proposition J.78 binary64's measured bit security.

Proposition J.73 (The floating-point signer's bit security [to table])**.** *On a checked key, the floating-point signer meets the bounds Theorem 4.11 takes, and its signatures keep the bit security of Definition J.66.* ***Under Hypotheses J.62, J.54, J.48, J.61, J.47 and J.31, let:***

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $Q_s \in \{2^{32}, 2^{36}, \dots, 2^{64}\}$.

Define:

- m_0 *and* M_0*, those of Proposition 5.8;*
- $\hat{K}_n$, d_{lo}, d_{hi}, (λ, α), τ, $\bar{T}$, $\bar{Z}$, $\bar{e}_{\mathrm{root}}$, e_+, C_i, $\bar{U}$, $\bar{p}_C$, κ_C, M_C, χ_{root} *to* p'_τ, $\lambda_{\mathcal{F}}$ *and the signer, those of Definition J.66;*
- $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$*, the probability measures of* Q_s *independent signatures on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1).*

Let:

- $A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s}$ *with* $Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda}$.

Define:

- S *and* S_k*, those of Definition A.26;*
- $R_\alpha^{S_k}(P \,\|\, Q)$*, that of Definition A.28 at* $\mathcal{Y} := S_k$*;*
- δ_i *and* $\bar{W}_S$*, those of Definition A.27.*

Then

1. $\forall z \in S\ \forall i \le N :\ |\delta_i| \le \bar{\delta}$*;*
2. $\bar{W}_S \le W^\circ$*;*
3. $\ln R \le A$*;*
4. $\forall k \le N :\ R_\alpha^{S_k}(P \,\|\, Q)^{\alpha-1} \le \binom{N}{k} \kappa_C^k R^{\alpha-1}$*;*
5. $P(S^c) \le N\, p'_\tau$*;*
6. $P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$.

Proof. (L1) $M_{2\alpha}$, p_τ, $\mathfrak{L}_B$, $\mathfrak{L}_{\bar{\delta}}$, $\mathfrak{L}_\Delta$, $\mathfrak{L}_\Phi$, A : Corollary 4.10, Theorem 4.11

[Lemma G.73 at order 2α and $\mathcal{Y} := \mathcal{Z}_i \setminus C_i$, its assumptions by the row bounds (Lemma J.72, items 1 and 2); $\sigma_{\max}(1+\bar{\delta})$, ϖ, $\bar{e}_{\mathrm{norm}}$ (the measured rows of Definition J.66); the terms (Definition J.66); **Hypotheses J.48, J.61, J.47, J.31 and J.54**, named by Lemma J.72]

(L2) $\Rightarrow$ item 1

[(L1); Lemma 4.7, item 2, at $S' := S$, $\bar{\delta}_{S'} := \bar{\delta}$ and $W^\circ_{S'} := W^\circ$, $\bar{\delta} \in [0, 1)$ by Lemma 4.7, (L7), and Lemma J.69, items 3 and 5, $W^\circ \ge 0$ by Lemma 4.9, precondition 2, its assumptions A7 and A8 by Lemma 4.7, item 2, and Lemma 4.9, item 2, and at Lemma J.67, items 1 to 7; Lemma J.68; Lemma J.69, items 1 to 5; Lemma J.70, items 1 to 5; $\hat{K}_n$ (the statement); **Hypotheses J.62**, J.54, J.48, J.61 and J.47 (the statement); Definition 5.3 at A; its assumptions by Lemma J.70, items 1 and 4; Theorem 4.11's assumptions A1 and A2 by the stored word $\sigma_{\min}$ [LO: `sign_sampler.c:31-56`] and Lemma J.30, items 1 and 2, at the floating-point signer; its assumption A3 by Lemma J.71, (L18); Corollary 4.10's assumption A1 by **Hypothesis J.61, item 2**; Lemma 4.7's assumption A6 by Lemma J.29; its assumption A6 by the ε_0° row of Definition J.66; Theorem 4.11's assumption A4 by **Hypothesis J.62**, and Corollary 4.10's assumption A7 by Lemma J.71, item 2, at ϵ of Definition J.66, in $[0, 1)$ by item 1; Theorem 4.11's Let on $M_{2\alpha}$ and p_τ by Corollary 4.10, items 7 and 8; Corollary 4.10, its assumptions by the measured rows of Definition J.66, Lemma J.69, item 5, Lemma J.30 and Theorem 4.11's assumption A5; Lemma 4.9, its assumptions by Lemma J.70, items 1 to 4, and Lemma J.30; **Hypothesis J.31**, named by Lemma J.67, Lemma J.68, Lemma J.69, Lemma J.70 and Lemma J.71]

(L3) $\Rightarrow$ item 2

[Lemma 4.9, item 3; Lemma 4.9, its assumptions by Lemma J.70, items 1 to 4, and Lemma J.30; as at (L2)]

(L4) $\Rightarrow$ item 3

[Theorem 4.11, item 1, as at (L2)]

(L5) $\Rightarrow$ item 4

[Theorem 4.11, item 2, as at (L2)]

(L6) $\Rightarrow$ item 5

[Corollary 4.10, item 5; Corollary 4.10, its assumptions by the measured rows of Definition J.66, Lemma J.69, item 5, Lemma J.30 and Theorem 4.11's assumption A5; as at (L2)]

(L7) $\Rightarrow$ item 6

[Theorem 1.2 at $(\lambda, \alpha, Q_s, A, \tau, M_C)$, $S' := S$, R of Definition A.30 at S and the A_{adv} of Definition 5.1 at (λ, Q_s): its $R > 0$ by Theorem 4.11, (L18), (L21), (L22), its assumptions A1, A2 and A3 by Theorem 4.11, items 1 and 2, and Corollary 4.10, item 6, as at (L2); Corollary 4.10, its assumptions by the measured rows of Definition J.66, Lemma J.69, item 5, Lemma J.30 and Theorem 4.11's assumption A5; Definition 5.3 at A]

□ (items 1, 2, 3, 4, 5 and 6)

Proposition J.74 (Under **Hypothesis J.64**, the measured bit security [to table]). *Under the Gaussian model of the leaf perturbations, the floating-point signer's signatures keep the bit security the Gaussian quantiles imply, less the quantiles' failure probability.* ***Under Hypotheses J.54****, J.48, J.61, J.47, J.31 and J.64, let:*

- (f, g, F, G) *be a checked key (Definition 5.5);*
- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$.

Define:

- m_0 *and* M_0*, those of Proposition 5.8;*
- $\hat{K}_n$, d_{lo}, d_{hi}, (λ, α), τ, $\bar{T}$, $\bar{Z}$, $\bar{e}_{\text{root}}$, e_+, C_i, $\bar{U}$, $\bar{p}_C$, κ_C, M_C, $\mathfrak{L}_B$, $M_{2\alpha}$, p_τ, p'_τ *and the signer, those of Definition J.66;*
- $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$*, the probability measures of* Q_s *independent signatures* $(z^{(1)}, \ldots, z^{(Q_s)})$ *on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1).*

Let:

- $A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s}$ *with* $Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda}$.

Define:

- $\eta := 2^{-\lambda}$;
- W^G *and* δ^G*, those of Lemma J.65 at* (Q_s, η);
- W *and* δ_i*, those of* ***Hypothesis J.64****;*
- $E := \{\, z \in \mathbb{Z}^N : W(z) \le W^G,\ \forall i \le N\ |\delta_i(z_{<i})| \le \delta^G \,\}$;
- $\mathfrak{L}_{\bar{\delta}}$, $\mathfrak{L}_\Delta$ *and* $\mathfrak{L}_\Phi$*, those of Theorem 4.11, precondition 1, at* $W^\circ_{S'} := W^G$ *and* $\bar{\delta}_{S'} := \delta^G$;
- $A := \mathfrak{L}_B + \mathfrak{L}_{\bar{\delta}} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$;
- $\lambda'_{\mathcal{F}}$*, that of Definition 5.3 at* A, κ_C, $\bar{p}_C$ *and* M_C;
- $\lambda_{\mathcal{F}}$*, by* $2^{-\lambda_{\mathcal{F}}} := 2^{-\lambda'_{\mathcal{F}}} + 2\eta$*, the* 2η *the failure probability of the two quantiles* W^G *and* δ^G.

Then

1. $P^{\otimes Q_s}(\exists j \le Q_s :\ z^{(j)} \notin E) \le 2\eta$;
2. $P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$.

Proof.

DEFINES $\lambda''_{\mathcal{F}}$, that of Definition 5.3 at A, κ_C, $\bar{p}_C$, M_C and $S' := S \cap E$

Proof of items 1 and 2.

(L1) $P^{\otimes Q_s}(\exists j \le Q_s :\ W(z^{(j)}) > W^G) \le \eta$

[Lemma J.65, item 1, at (Q_s, η), $\eta \in (0, 1)$ by $\lambda > 0$ (Definition J.66); **Hypothesis J.64** (the statement)]

(L2) $P^{\otimes Q_s}(\exists j \le Q_s\ \exists i \le N :\ |\delta_i(z^{(j)}_{<i})| > \delta^G) \le \eta$

[Lemma J.65, item 2, at (Q_s, η); as at (L1); **Hypothesis J.64**, named by Lemma J.65]

(L3) $\{\exists j \le Q_s :\ z^{(j)} \notin E\} = \{\exists j \le Q_s :\ W(z^{(j)}) > W^G\} \cup \{\exists j \le Q_s\ \exists i \le N :\ |\delta_i(z^{(j)}_{<i})| > \delta^G\}$

[E (the statement)]

(L4) $\Rightarrow$ $P^{\otimes Q_s}(\exists j \le Q_s :\ z^{(j)} \notin E) \le 2\eta$

[(L1), (L2), (L3); Fact A.45, item 5]

(L5) $\Rightarrow$ item 1

[(L4)]

(L6) $P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda''_{\mathcal{F}}}$

[Theorem 1.2 at $(\lambda, \alpha, Q_s, A, \tau, M_C)$, $S' := S \cap E$, R of Definition A.30 at $S \cap E$ and the A_{adv} of Definition 5.1 at (λ, Q_s): its $R > 0$ by Theorem 4.11, (L18), (L21), (L22), its assumptions A1, A2 and A3 by Theorem 4.11, items 1 and 2, and Corollary 4.10, item 6, at $S' := S \cap E$, $\bar{\delta}_{S'} := \delta^G$ and $W^{\circ}_{S'} := W^G$: $S \cap E \subseteq S$ (Fact A.41, item 17); $\bar{\delta}_{S'} := \delta^G \in [0, 1)$ and $W^G \ge 0$ by **Hypothesis J.64, items 4 and 6**, at Q_s and the floating-point signer [gate: `verify/gates/fx/meas_quantiles.py`]; its assumptions A7 and A8 by E (the statement) on $S \cap E \subseteq E$ (Fact A.41, item 17); Lemma J.67, items 1 to 7; Lemma J.72, items 1 to 4; Lemma J.68; Lemma J.69, items 1 to 5; Lemma J.70, items 1 to 5; Definition 5.3 at A and $S' := S \cap E$, its $\lambda_{\mathcal{F}}$ the $\lambda''_{\mathcal{F}}$ of the proof's block; its assumptions by Lemma J.70, items 1 and 4; Theorem 4.11's assumptions A1 and A2 by the stored word $\sigma_{\min}$ [L0: `sign_sampler.c:31-56`] and Lemma J.30, items 1 and 2, at the floating-point signer; its assumption A3 by Lemma J.71, (L18); Corollary 4.10's assumption A1 by **Hypothesis J.61, item 2**; Lemma 4.7's assumption A6 by Lemma J.29; its assumption A6 by **Hypothesis J.64, item 7**, at Q_s `verify/reports/tree/measured_levels.py`; Theorem 4.11's assumption A4 at $\bar{\delta}_{S'} := \delta^G$ by **Hypothesis J.64, item 5**, at Q_s [gate: `verify/gates/fx/meas_quantiles.py`], and Corollary 4.10's assumption A7 by Lemma J.71, item 2, at ϵ of Definition J.66, in $[0, 1)$ by item 1; Theorem 4.11's Let on $M_{2\alpha}$ and p_τ by Corollary 4.10, items 7 and 8; Corollary 4.10, its assumptions by the measured rows of Definition J.66, Lemma J.69, item 5, Lemma J.30 and Theorem 4.11's assumption A5; Lemma 4.9, its assumptions by Lemma J.70, items 1 to 4, and Lemma J.30; Lemma 4.7, its assumptions by Lemmas J.68 and J.69; **Hypotheses J.47 and J.54**, named by Lemma J.72; **Hypothesis J.48**, named by Lemma J.72 and Lemma J.71; **Hypothesis J.31**, named by Lemma J.67, Lemma J.72, Lemma J.68, Lemma J.69, Lemma J.70 and Lemma J.71]

(L7) $2^{-\lambda''_{\mathcal{F}}} = 2^{-\lambda'_{\mathcal{F}}} + Q_s P((S \cap E)^c) - Q_s P(S^c)$

[$\lambda''_{\mathcal{F}}$ (the proof's block) and $\lambda'_{\mathcal{F}}$ (the statement), Definition 5.3 at the same A, κ_C, $\bar{p}_C$ and M_C]

(L8) $(S \cap E)^c = S^c \cup E^c$

[Fact A.41, item 17, at $(A, B) := (S, E^c)$, its $A \setminus B$ the set $S \cap E$]

(L9) $P((S \cap E)^c) \le P(S^c) + P(E^c)$

[(L8); Fact A.45, item 5]

(L10) $E^c = \{z : W(z) > W^G\} \cup \{z : \exists i \le N \ |\delta_i(z_{<i})| > \delta^G\}$

[E (the statement)]

(L11) $Q_s P(W(z) > W^G) \le \eta$

[Lemma J.65, (L6), (L7), at (Q_s, η) and $j := 1$, $z^{(1)}$ an output of P ($P^{\otimes Q_s}$, the statement); **Hypothesis J.64** (the statement)]

(L12) $Q_s P(\exists i \le N : \ |\delta_i(z_{<i})| > \delta^G) \le \eta$

[Lemma J.65, (L17), (L21), at (Q_s, η) and $j := 1$, as at (L11); Fact A.45, item 5, over $i \le N$; **Hypothesis J.64**, named by Lemma J.65]

(L13) $\Rightarrow$ $Q_s P(E^c) \le 2\eta$

[(L10), (L11), (L12); Fact A.45, item 5]

(L14) $\Rightarrow$ $P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda'_{\mathcal{F}}} + 2\eta$

[(L6), (L7), (L9), (L13)]

(L15) $\Rightarrow$ $P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$

[(L14); $\lambda_{\mathcal{F}}$ (the statement)]

(L16) $\Rightarrow$ item 2

[(L15)]

□ (items 1 and 2)

Hypothesis J.75 (Precision of the computed exponential [to table])**.** A mathematical hypothesis: the signers at the precisions $p = 64$ and $p = 113$ are a model. No code computes at these precisions,

and the hypothesis defines their base sampler's exponential as one within a relative $2^{1.95}u$ of its exact value, the bound Lemma H.25 proves at $p = 53$ scaled to $u = 2^{-p}$. Let:

- $p \in \{64, 113\}$.

Define:

- $u = 2^{-p}$;
- L, that of Lemma H.25;
- $y(r', ccs)$, the value BerExp (Algorithm 9) computes for $e^{-r'}ccs$ at the precision p, the y of Lemma H.25.

We assume

(1) $\forall r' \in [0, L]\ \forall ccs \in [1/2, 1) :\ |y(r', ccs)/(e^{-r'}ccs) - 1| \le 2^{1.95}u$.

[L3: mathematical] Not discharged.

Proposition J.76 (The floating-point bit security on the derived bounds [eyes only] [to table])**.** *Under the derived bounds, the floating-point signer keeps no bit security at binary64 or at $p = 64$. It keeps a bit security at $p = 113$. **Under Hypotheses J.62**, J.54, J.48, J.61, J.47, J.31 and J.75, let:*

- $p \in \{53, 64, 113\}$*;*
- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$.

Define:

- n, λ *and* $\lambda_{\mathcal{F}}$*, those of Definition J.66;*
- $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$*, the probability measures of* Q_s *independent signatures on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1).*

Define:

- $\tau = \arg\min_\tau(\lambda - \lambda_{\mathcal{F}})$*, at each* (n, λ, Q_s).

Measured (Table 42, Figure 112) `verify/reports/fp/loss.py`*:*

- $\lambda_{\mathcal{F}}$ *at every* (n, Q_s, p), $p \in \{53, 64, 113\}$.

Then

1. $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$*;*
2. *Assume:*

   (A1) $p \in \{53, 64\}$.

   Then $\lambda - \lambda_{\mathcal{F}} \ge \lambda$.
3. *Assume:*

   (A2) $(n, Q_s, p) = (512, 2^{48}, 113)$.

   Then $\lambda - \lambda_{\mathcal{F}} = 25.74$.

Proof. (L1) $\forall A_{\text{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\text{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$
[Proposition J.73, item 6, at each such A_{adv}; at $p \ne 53$, the exponential by **Hypothesis J.75, item (1)**; **Hypotheses J.48, J.61, J.62, J.47, J.31 and J.54**, named by Proposition J.73]

(L2) $\Rightarrow$ item 1
[(L1)]

(L3) $\lambda - \lambda_{\mathcal{F}} \ge \lambda$
[the measured row at every (n, Q_s, p) with $p \in \{53, 64\}$; at $p = 64$, the exponential by **Hypothesis J.75, item (1)**; assumption A1]

(L4) $\Rightarrow$ item 2
[(L3)]

(L5) $\lambda - \lambda_{\mathcal{F}} = 25.74$
[the measured row at $(512, 2^{48}, 113)$, by **Hypothesis J.75, item (1)**; assumption A2]

(L6) $\Rightarrow$ item 3

[(L5)]

□ (items 1 to 3)

Proposition J.77 (Dominance of the term $\mathfrak{L}_\Delta$ [eyes only] [to table])**.** *Under the derived bounds, the center shift's term is the largest of the four terms of* $\ln R$*. Let:*

- $p \in \{53, 64, 113\}$*;*
- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$*.*

Define:

- $\mathfrak{L}_B$*,* $\mathfrak{L}_{\bar\delta}$*,* $\mathfrak{L}_\Delta$*,* $\mathfrak{L}_\Phi$ *and* A*, those of Definition J.66;*
- τ*, that of Proposition J.76.*

Measured (Table 44) `verify/reports/fp/terms.py`*:*

- $\mathfrak{L}_B$*,* $\mathfrak{L}_{\bar\delta}$*,* $\mathfrak{L}_\Delta$ *and* $\mathfrak{L}_\Phi$ *at every* (p, n, Q_s)*;*
- τ *at every* (p, n, Q_s)*.*

Then

1. $A = \mathfrak{L}_B + \mathfrak{L}_{\bar\delta} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$*;*
2. $\mathfrak{L}_\Delta = \max(\mathfrak{L}_B, \mathfrak{L}_{\bar\delta}, \mathfrak{L}_\Delta, \mathfrak{L}_\Phi)$*;*
3. $\tau \in [4.3, 21.0]$*.*

Proof. (L1) $A = \mathfrak{L}_B + \mathfrak{L}_{\bar\delta} + \mathfrak{L}_\Delta + \mathfrak{L}_\Phi$

[A (Definition J.66; Theorem 4.11, precondition 1)]

(L2) $\Rightarrow$ item 1

[(L1)]

(L3) $\mathfrak{L}_\Delta = \max(\mathfrak{L}_B, \mathfrak{L}_{\bar\delta}, \mathfrak{L}_\Delta, \mathfrak{L}_\Phi)$

[the first measured row]

(L4) $\Rightarrow$ item 2

[(L3)]

(L5) $\tau \in [4.3, 21.0]$

[the second measured row]

(L6) $\Rightarrow$ item 3

[(L5)]

□ (items 1 to 3)

Proposition J.78 (Under **Hypothesis J.64**, binary64's measured bit security [eyes only] [to table])**.** *Under the Gaussian model of the leaf perturbations, the floating-point signer at binary64 keeps the bit security below, and the center shift's term exceeds the base sampler's; every term is read at one tail-cut rate, the least multiple of* 0.01 *whose tail costs at most* $2^{-\lambda-10}$*.* ***Under Hypotheses J.54****,* ***J.48****,* ***J.61****,* ***J.47****,* ***J.31*** *and* ***J.64****, let:*

- $p = 53$*;*
- $Q_s \in \{2^{32}, 2^{36}, \ldots, 2^{64}\}$*.*

Define:

- n *and* λ*, those of Definition J.66;*
- δ^G*, that of Proposition J.74;*
- $P^{\otimes Q_s}$ *and* $Q^{\otimes Q_s}$*, the probability measures of* Q_s *independent signatures on* $(\mathbb{Z}^N)^{Q_s}$ *(Fact A.45, item 1);*
- $\epsilon_{\mathrm{hi}} := 4.519 \cdot 10^{-3}$*, the table's upward deviation* `verify/reports/sampler/table.py`*;*
- $\epsilon_G := \epsilon$ *(Definition J.66 at* $\bar\delta := \delta^G$*);*
- τ*, at each* (n, λ, Q_s)*, the least* $\tau \in 0.01\mathbb{Z}$*,* $\tau > 1$*, with* $Q_s N(1 + \epsilon_{\mathrm{hi}})(1 + \epsilon_G)(1 - \epsilon_G)^{-1}\tau e^{(1-\tau^2)/2} \le 2^{-\lambda-10}$*;*

- $\lambda_{\mathcal{F}}$ *and* $\mathfrak{L}_{\Delta}$*, those of Proposition J.74 at* τ*;*
- $\mathfrak{L}_{B}$*, that of Definition J.66 at* τ*.*

Measured (Table 43) `verify/reports/tree/measured_levels.py`*:*

- $\lambda_{\mathcal{F}}$*,* $\mathfrak{L}_{\Delta}$ *and* $\mathfrak{L}_{B}$ *at every* (n, λ, Q_s)*.*

Then

1. $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$*;*
2. *Assume:*
   (A1) $(n, \lambda, Q_s) = (512, 128, 2^{60})$.
   Then $\lambda_{\mathcal{F}} = 86.28$*;*
3. *Assume:*
   (A2) $(n, \lambda, Q_s) = (512, 128, 2^{64})$.
   Then $\lambda_{\mathcal{F}} = 78.28$*;*
4. *Assume:*
   (A3) $(n, \lambda, Q_s) = (1024, 256, 2^{60})$.
   Then $\lambda_{\mathcal{F}} = 194.17$*;*
5. *Assume:*
   (A4) $(n, \lambda, Q_s) = (1024, 256, 2^{64})$.
   Then $\lambda_{\mathcal{F}} = 181.21$*;*
6. *Assume:*
   (A5) $(n, \lambda, Q_s) = (512, 128, 2^{64})$.
   Then $\mathfrak{L}_{\Delta} = 2^{-66.0}$*;*
7. *Assume:*
   (A6) $(n, \lambda, Q_s) = (512, 128, 2^{64})$.
   Then $\mathfrak{L}_{B} = 2^{-68.9}$*;*
8. *Assume:*
   (A7) $(n, \lambda, Q_s) = (512, 128, 2^{64})$.
   Then $\mathfrak{L}_{\Delta} > \mathfrak{L}_{B}$.

Proof. (L1) $\forall A_{\mathrm{adv}} \subseteq (\mathbb{Z}^N)^{Q_s},\ Q^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda} :\ P^{\otimes Q_s}(A_{\mathrm{adv}}) \le 2^{-\lambda_{\mathcal{F}}}$ [Proposition J.74, item 2, at each such A_{adv}; **Hypotheses J.48, J.61, J.64, J.47, J.31 and J.54**, named by Proposition J.74]

(L2) $\Rightarrow$ item 1 [(L1)]

(L3) $\lambda_{\mathcal{F}} = 86.28$ [the measured row at $(512, 128, 2^{60})$; assumption A1]

(L4) $\Rightarrow$ item 2 [(L3)]

(L5) $\lambda_{\mathcal{F}} = 78.28$ [the measured row at $(512, 128, 2^{64})$; assumption A2]

(L6) $\Rightarrow$ item 3 [(L5)]

(L7) $\lambda_{\mathcal{F}} = 194.17$ [the measured row at $(1024, 256, 2^{60})$; assumption A3]

(L8) $\Rightarrow$ item 4

[(L7)]

(L9) $\lambda_{\mathcal{F}} = 181.21$

[the measured row at $(1024, 256, 2^{64})$; assumption A4]

(L10) $\Rightarrow$ item 5

[(L9)]

(L11) $\mathfrak{L}_{\Delta} = 2^{-66.0}$

[the measured row at $(512, 128, 2^{64})$; assumption A5]

(L12) $\Rightarrow$ item 6

[(L11)]

(L13) $\mathfrak{L}_{B} = 2^{-68.9}$

[the measured row at $(512, 128, 2^{64})$; assumption A6]

(L14) $\Rightarrow$ item 7

[(L13)]

(L15) $\mathfrak{L}_{\Delta} > \mathfrak{L}_{B}$

[the measured row at $(512, 128, 2^{64})$; assumption A7]

(L16) $\Rightarrow$ item 8

[(L15)]

$\square$ (items 1 to 8)

The three parts of the loss. The three parts of the loss (Definition 5.3) are the Rényi divergence argument's own cost λ/α, half a bit at $\alpha = 2\lambda + 1$; the divergence β, which the arithmetic and the base sampler's table set; and the tail. No bit security is assumed for ffSampling$^{\mathcal{F}}$: $\lambda_{\mathcal{F}}$ is what the theorem carries. Table 42 lists the bit security $\lambda_{\mathcal{F}}$ from the derived bounds, the loss being $\lambda - \lambda_{\mathcal{F}}$ and a dash the cells where it exceeds λ; Figure 112 draws that loss against $\log_2 Q_s$, one graph per precision; Table 43 lists the bit security under **Hypothesis J.64**.

n	λ	Q_s	$p = 53$	$p = 64$	$p = 113$
512	128	2^{32}	–	10.96	102.33
512	128	2^{36}	–	–	102.31
512	128	2^{40}	–	–	102.29
512	128	2^{44}	–	–	102.28
512	128	2^{48}	–	–	102.26
512	128	2^{52}	–	–	101.26
512	128	2^{56}	–	–	94.27
512	128	2^{60}	–	–	86.28
512	128	2^{64}	–	–	78.28
1024	256	2^{32}	–	–	215.31
1024	256	2^{36}	–	–	215.23
1024	256	2^{40}	–	–	207.81
1024	256	2^{44}	–	–	195.82
1024	256	2^{48}	–	–	195.12
1024	256	2^{52}	–	–	195.10
1024	256	2^{56}	–	–	195.07
1024	256	2^{60}	–	–	194.81
1024	256	2^{64}	–	–	182.23

Table 42: Floating-point signer: level $\lambda_{\mathcal{F}}$ in bits and loss $\lambda - \lambda_{\mathcal{F}}$ (Proposition J.76), $\hat{K}_n$, $\alpha = 2\lambda+1$, by precision p, $u = 2^{-p}$; a dash where the loss exceeds λ.

n	λ	2^{32}	2^{36}	2^{40}	2^{44}	2^{48}	2^{52}	2^{56}	2^{60}	2^{64}
512	128	102.33	102.31	102.29	102.28	102.26	101.26	94.27	86.28	78.28
1024	256	215.31	215.23	207.81	195.82	195.12	195.10	195.03	194.17	181.21

Table 43: Floating-point signer at binary64: level $\lambda_{\mathcal{F}}$ in bits under **Hypothesis J.64** (Proposition J.78) with the quantiles W^G, δ^G of Table 40 and $2\eta = 2^{1-\lambda}$, $\alpha = 2\lambda + 1$, by Q_s.

What the rounding model certifies. The rounding model certifies the floating-point signer at $p = 113$ and at no lower precision: the derived rows read none at binary64 and at $p = 64$ (Proposition J.76), the center-shift term $\mathfrak{L}_\Delta$ setting the loss (Proposition J.77) at the computed Gram matrix's own perturbation (Lemma J.37). At binary64 the certificate is **Hypothesis J.64**'s: under it the same signer keeps 78.28 of 128 bits at $(512, 2^{64})$ and 181.21 of 256 at $(1024, 2^{64})$ (Proposition J.78). What separates the $p = 53$ column of Table 42 from Table 43 is the bound on the leaf perturbations, not the theorem.

The saturation of the shift. Every cell of this signer is read under the saturation of the shift of BerExp (Algorithm 9): a candidate whose shift saturates carries a ratio $\widetilde{B}_i/\widetilde{D}_i$ no relative perturbation bounds, so it leaves $\bar{\rho}_B$ and reaches the bit security as $\bar{U}$ and $\bar{p}_C$ of Definition J.55 and the term $\Pi_C(y)$ of Definition 5.2, one summand per total number of fringe leaves among the $Q_s N$.

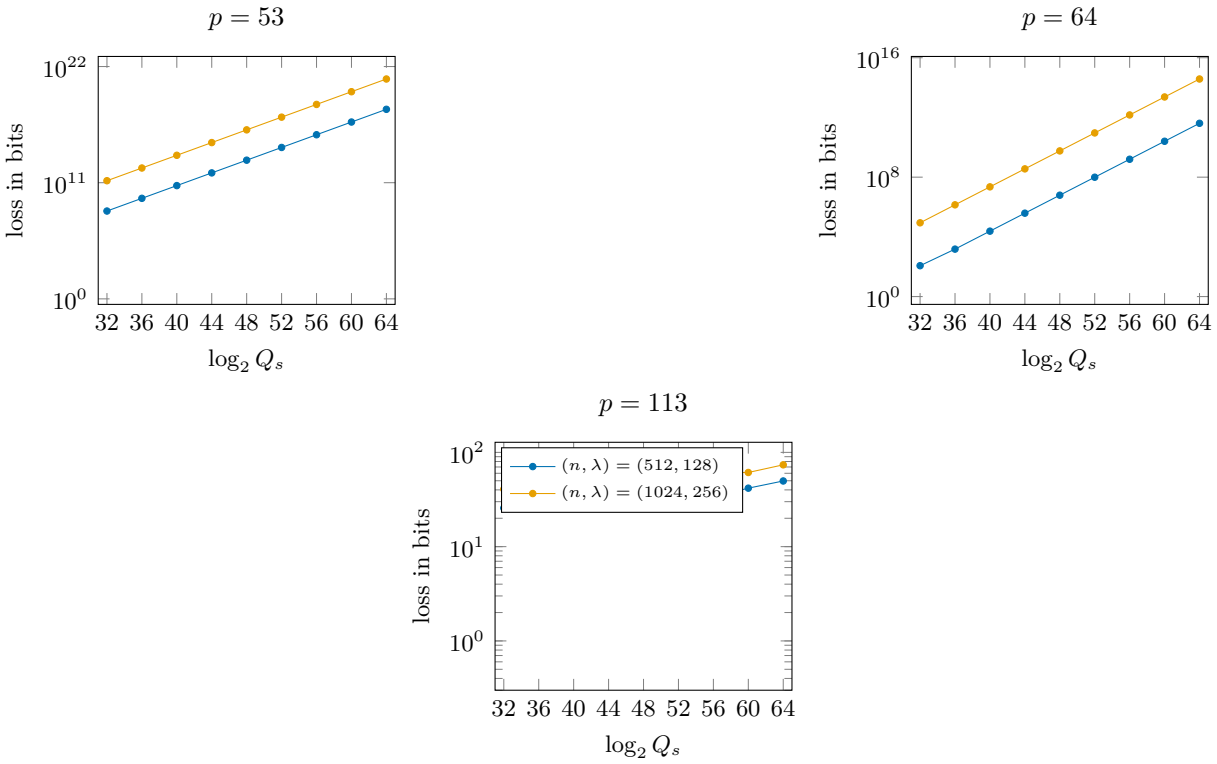


Figure 112: Loss in bits from the derived bounds against $\log_2 Q_s$, $\hat{K}_n$, one graph per precision p; the data of Table 42. Gate: `verify/reports/fp/loss.py`.

Table 44: Floating-point signer: the terms of $\ln R$ that set the loss, $\log_2$ per signature. Gate: `verify/reports/fp/terms.py`, `verify/reports/tree/measured_levels.py` for the Gaussian quantiles.

Term	Symbol	$n = 512$	$n = 1024$
Under **Hypothesis J.64**			
Gaussian quantile of the leaf sum at 2^{64}	W^G	$2^{-74.0}$	$2^{-70.1}$
Gaussian quantile of the deviations at 2^{64}	δ^G	$2^{-45.2}$	$2^{-44.1}$
Center shifts	$\mathfrak{L}_\Delta$	$2^{-66.0}$	$2^{-61.1}$
Base sampler	$\mathfrak{L}_B$	$2^{-68.9}$	$2^{-63.8}$
Leaf standard deviations	$\mathfrak{L}_{\bar\delta}$	$2^{-71.3}$	$2^{-67.3}$
Normalizer ratio	$\mathfrak{L}_\Phi$	$2^{-81.0}$	$2^{-83.0}$
Derived bounds, $p = 53$			
Leaf standard deviations	$\bar\delta$	$2^{-23.3}$	$2^{-19.8}$
Tail parameter over the cells	τ	4.3 to 21.0	

The bit security under the Gaussian model. Under Hypothesis J.64 the bit security at $n = 512$ is the floor of the $p = 113$ column at every count of the sweep, 102.33 at 2^{32} and 78.28 at 2^{64}, and at 2^{64} the center shift's term $\mathfrak{L}_\Delta$, read at the quantile W^G, exceeds the base sampler's $\mathfrak{L}_B$ (Table 44, Table 42, Table 43).

The dominant part of D_S at binary64. At binary64, D_S is dominated by its offset part, $\Xi\tau\sigma_{\max}(n/2)^{1/2}$ times the factors ℓ and Ξ'_k of Corollary G.62, and the root node's d_{11} cancels by κ_{root}, in the thousands, so $\bar\delta$ lies far above the quantile δ^G, $2^{-19.8}$ against $2^{-44.1}$ at $n = 1024$ (Table 44).

The floor of the loss. Beyond $p = 64$ the loss stops at a floor no arithmetic removes: the half bit of λ/α and the base sampler's 79-bit table, whose part grows with the pair, since row 18's term in $M_{2\alpha}$ carries the weight $(1 + \epsilon_{\text{hi}})^{2\alpha-2}$, exponential in α (Table 42, the $p = 113$ column).

What separates the derived bounds from the Gaussian model. What separates the derived bounds from **Hypothesis J.64**, in order: D_S carries τ in the offsets R_k, where the sample's offsets are about σ; D_S is a worst-case sum of norms over the depths with the key's maxima Ξ, Ξ', ℓ; and $\bar\delta$ carries κ_{root}. **Hypothesis J.64** assumes a Gaussian model with the sample's moments; the derived bounds are proved.

J.6 The gates, the machine-checked proofs and the imported facts

Structure. This subsection lists the rows of Appendix M that concern this signer alone.

Checker	What it verifies	Backs
`verify/gates/fp/node.py` `make.py` `verify/reports/fp/grids.py` `verify/gates/sampler/sigma0.py` `verify/reports/key/ccs.py`	Lemma G.32, item 2, at $\zeta = 0$, the node map of Definition J.40, exact and first order; the valuation calculus of ν_2 (Algorithm 18) and ν_2-walk (Algorithm 19) and the `make` probe of **Hypothesis J.31**; **Hypotheses J.47**, J.48	Appendix J, Section 4.5.2
`verify/gates/fp/twiddle.py`	Exhaustive: the stored twiddles bit for bit against the roots rounded to nearest, Lemma J.4	Appendix J.1.1
`verify/gates/fp/complex_roundings.py`	Exhaustive: the roundings per complex result on the code's plain branch, Lemma J.26	Appendix J
`verify/reports/fp/basisimage.py`	Sampled: Lemma H.11 read $\forall\psi$ on keys of the checked key generation, the derived bounds $\bar{e}_{00}$ (Lemma J.37), $\bar{e}_{11}$ (Lemma J.38) and $\bar{E}_a$ (Lemma J.39) beside the root node diagonal's measured deviation	Appendix J
`verify/reports/sampler/cap.py`	Partly sampled: the fringe set of Definition J.55: the closed forms of Lemmas J.59 and J.60 exact at the stored words, the maxima $\bar{U}(\tau)$ and $\bar{p}_C(\tau)$ over a sweep of $(\widetilde{\sigma}, r)$ sampled	Appendix J
`verify/reports/key/keyconst_reference.py`	Sampled: the six key constants on keys of the reference key generation (`c-fn-dsa`)	Appendix J.5
`verify/reports/fp/loss.py` `verify/reports/tree/measured_levels.py` `falcon_general.py`	The loss of Theorem F.4 by precision (`verify/reports/fp/loss.py`); the bit security under **Hypothesis J.64** (`verify/reports/tree/measured_levels.py`): Proposition J.78; the chain of Theorem 4.11 at (u, ζ) against this signer's bit security cells (`verify/reports/tree/falcon_general.py`)	Appendix J.5
`verify/reports/tree/leaferrors.py`	Sampled: the leaf perturbations of this signer: every base-sampler call traced in the code, ffSampling$^{\mathbb{R}}$ replayed in Decimal on the same prefix; the sample maxima, the moments of **Hypothesis J.64** and the quantiles of Lemma J.65	Appendix J.5

Proof	What it proves	Backs
`lemmas/fpr_cfndsa/mul`	The word of `fpr_mul` is xy rounded to nearest, a tie to even, for normal x, y with a normal product; the zero of sign $x_s \oplus y_s$ at a zero operand; Cortex-M4, `arm-none-eabi-gcc -O2`	Lemma J.11
`lemmas/fpr_cfndsa/add`	The word of `fpr_add` is $x + y$ rounded to nearest, a tie to even, for normal x, y at most 63 exponents apart with a normal sum; the far, cancellation and zero cases; Cortex-M4, `arm-none-eabi-gcc -O2`	Lemma J.12
`lemmas/fpr_cfndsa/div`	The word of `fpr_div` is x/y rounded to nearest, a tie to even, for normal x, y with a normal quotient; the loop's path, its body as a contract applied 55 times; Cortex-M4, `arm-none-eabi-gcc -O2`	Lemma J.13
`lemmas/fpr_cfndsa/sqrt`	The word of `fpr_sqrt` is $\sqrt{x}$ rounded to nearest, a tie to even, for normal x; the loop's path, its body as a contract carrying the invariant, applied 53 times; Cortex-M4, `arm-none-eabi-gcc -O2`	Lemma J.14

The trusted base of the machine-checked proofs. The trusted base of these proofs adds, for the `-O2` objects of `fpr_mul` and `fpr_add`, every rule their traces use, each against QEMU on nine vectors with its registers and flags, and each with a misreading that the vectors refute. A Lean theorem of `lean/FFSampling/FprRound.lean` derives the report's statement from `cv`'s claim (Lemmas J.11 and J.12).

Level	Fact	Source
L0	The format of `fpr`, no subnormals	`sign_inner.h:21-38`
L0	Rounding to nearest even through a sticky bit	`sign_fpr.c:20`
L0	Inversion is one division	`sign_inner.h:292`
L0	The four-multiplication complex product	`sign_inner.h:327`
L0	The twiddle table and its comment	`sign_fpoly.c:8-13`
L3	No underflow in ffSampling$^{\mathcal{F}}$	Assumption, by decision
L3	The floating-point signer's leaf perturbations are Gaussian with the sample's moments (**Hypothesis J.64**)	Assumption, of the kind of BFLP26 (33), (34); the moments measured

What is not gated.

- This signer's key constants (Definition 4.6). They are read off a sample of keys (**Hypothesis J.63**); the fixed-point signer's are proved from the key generation's checks (Definition I.62).
- **Hypothesis J.31**. It stays an assumption on ffSampling$^{\mathcal{F}}$: the valuation calculus of the integer inputs certifies the FFTs and admits both of its bounds to fail from the root node on.
- **Hypothesis J.64**: its inputs, the sample's means and standard deviations, are measured; the Gaussian model over every output is an assumption, and the derived bounds are the report's claim without it.

K The relative-error lemma

Table 45 lists how this appendix's lemma is verified.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Lemma K.1	✓				
Lemma K.2	✓				L2: Pre17, Lem. 3

Table 45: Appendix K: how each lemma is verified.

The question. Given a bound on how far one probability measure deviates from another, what does the Rényi divergence cost?

Three bounds and what each consumes. Three bounds answer it, and they differ in what they consume. [Pre17, Lem. 3], which [L1: FGdG+26, Lem. 6] imports unchanged, consumes a pointwise δ with $1-\delta \le U \le 1+\delta$ and returns $1+\alpha(\alpha-1)\delta^2/(2(1-\delta)^{\alpha+1})$. Lemma K.1 consumes the range $[r_{\mathrm{lo}}, r_{\mathrm{hi}}]$ of U and returns the chord of $u \mapsto u^\alpha$ over it, a bound attained by a two-point distribution. Lemma G.65 consumes the deviation's weighted second moment $M_{\alpha,\mathcal{Y}}$ on a set $\mathcal{Y} \subseteq \mathbb{Z}$ together with the mass $D(\mathcal{Y}^c)$ it leaves out and returns $1+\alpha D(\mathcal{Y}^c)\epsilon_{\mathcal{Y}}+\alpha(\alpha-1)M_{\alpha,\mathcal{Y}}/2$.

The three bounds at the base sampler. Table 46 reads the three at the base sampler's own deviation, one call, at the report's orders; the second moment is read on $\mathcal{Z}_i$ (Definition A.28), the set Theorem F.4 sums over, and the chord on the sampler's candidate set.

n	2α	ϵ_-	ϵ_+	Second moment	Chord	[Pre17, Lem. 3]	Floored
512	514	-2.82e-02	4.52e-03	-79.1	-22.7	-4.7	6
1024	1026	-2.43e-01	4.52e-03	-74.8	-19.9	-1.8	4

Table 46: $\ln R$ at the base sampler's own deviation, one call, $\log_2$: Lemma G.65's weighted second moment, on $\mathcal{Z}_i$ (Definition A.28, $\tau = 11$); Lemma K.1's chord and [Pre17, Lem. 3], each at the largest value it takes over the section's (σ, μ) values; floored: the candidate points whose acceptance floors to zero. Report: `verify/reports/renyi/relerr_compare.py`; gate: `verify/gates/renyi/moment_chord.py`.

The second moment is the tightest at the base sampler. At the base sampler, the second moment is the tightest of the three (Table 46), and it is what Theorem F.4 uses: the base sampler's deviation is largest at the last rows of its table, of small mass (Lemma G.64), so a bound that charges each deviation at its own probability pays those rows at their own mass where a bound on the range pays them at every call.

The chord is the tight form of the imported lemma. The chord is what the range alone can imply, and it is the tight form of the imported lemma: it is below [Pre17, Lem. 3] (Table 46) and it is attained (Table 47). Lemma K.2 proves the first at every order $\alpha > 1$ over the symmetric range $[1-\delta, 1+\delta]$ that [Pre17, Lem. 3] consumes. There, at $\delta \in (0,1)$, the chord's value at 1 is the mean of $(1+\delta)^\alpha$ and $(1-\delta)^\alpha$.

Why the base sampler is read in two halves. Neither range bound applies to the base sampler as a whole: $D_{\mathbb{Z},\sigma,\mu}$ has mass outside the candidate set $z \in [-18, 19]$ of SamplerZ (Algorithm 8), where $\widetilde{B}(z) = 0$ and $r_{\mathrm{lo}} = 0$, and the acceptance of some points of the candidate set floors to zero (Lemma H.26). This is why the base sampler is read in two halves (Appendix G.6): $\widetilde{B}$ against $D_{\mathbb{Z},\widetilde{\sigma},\widetilde{\mu}}$ by the second moment on $\mathcal{Z}_i$, and the truncation as an absolute term at the leaf, which no relative bound expresses.

Lemma K.1 (The chord bound on a ratio's moment [to table])**.** *The ratio of two probability measures with values in* $[r_{\mathrm{lo}}, r_{\mathrm{hi}}]$ *has its order-*α *moment below the chord of* $u \mapsto u^\alpha$ *over* $[r_{\mathrm{lo}}, r_{\mathrm{hi}}]$ *at its mean* 1*, and a two-point measure attains the bound. Let:*

- $\alpha > 1$, *an order;*
- D *and* D_δ *be probability measures on a countable set with* $\mathrm{Supp}(D_\delta) \subseteq \mathrm{Supp}(D)$*;*
- $r_{\mathrm{lo}}, r_{\mathrm{hi}} \in \mathbb{R}$.

Define:

- $U = D_\delta / D$ *on* $\mathrm{Supp}(D)$*;*
- $p = (1 - r_{\mathrm{lo}})/(r_{\mathrm{hi}} - r_{\mathrm{lo}})$*;*
- $D_\star = (p, 1-p)$ *on* $\{0, 1\}$*;*
- $D_{\star\delta} = (p\, r_{\mathrm{hi}}, (1-p)\, r_{\mathrm{lo}})$ *on* $\{0, 1\}$*;*
- $U_\star = D_{\star\delta} / D_\star$ *on* $\mathrm{Supp}(D_\star)$.

Assume:

(A1) $0 \le r_{\mathrm{lo}}$*;*

(A2) $r_{\mathrm{lo}} < r_{\mathrm{hi}}$.

Then

1. *Assume:*

   (A3) $\forall i \in \mathrm{Supp}(D) : \ r_{\mathrm{lo}} \le U(i) \le r_{\mathrm{hi}}$.

   Then $R_\alpha(D_\delta \,\|\, D)^{\alpha-1} = \mathbb{E}_{i \leftarrow D}[U(i)^\alpha] \le \dfrac{(1 - r_{\mathrm{lo}}) r_{\mathrm{hi}}^\alpha + (r_{\mathrm{hi}} - 1) r_{\mathrm{lo}}^\alpha}{r_{\mathrm{hi}} - r_{\mathrm{lo}}}$.

2. *Assume:*

   (A4) $r_{\mathrm{lo}} < 1 < r_{\mathrm{hi}}$.

   Then $D_\star$ *and* $D_{\star\delta}$ *are probability measures on* $\{0, 1\}$*,* $U_\star(0) = r_{\mathrm{hi}}$*,* $U_\star(1) = r_{\mathrm{lo}}$*, and* $R_\alpha(D_{\star\delta} \,\|\, D_\star)^{\alpha-1} = \mathbb{E}_{i \leftarrow D_\star}[U_\star(i)^\alpha] = \dfrac{(1 - r_{\mathrm{lo}}) r_{\mathrm{hi}}^\alpha + (r_{\mathrm{hi}} - 1) r_{\mathrm{lo}}^\alpha}{r_{\mathrm{hi}} - r_{\mathrm{lo}}}$.

Proof. Proof of item 1.

(L1) $\mathbb{E}_{i \leftarrow D}[U(i)] = \sum_{i \in \mathrm{Supp}(D)} D_\delta(i)$

[U (the statement)]

(L2) $\sum_{i \in \mathrm{Supp}(D)} D_\delta(i) = 1$

[D_δ a probability measure with $\mathrm{Supp}(D_\delta) \subseteq \mathrm{Supp}(D)$ (the statement)]

(L3) $\forall i \in \mathrm{Supp}(D) : \ U(i)^\alpha \le r_{\mathrm{lo}}^\alpha + (U(i) - r_{\mathrm{lo}})(r_{\mathrm{hi}}^\alpha - r_{\mathrm{lo}}^\alpha)/(r_{\mathrm{hi}} - r_{\mathrm{lo}})$

[Fact A.41, item 14, at $a := r_{\mathrm{lo}}$, $b := r_{\mathrm{hi}}$, $t := U(i)$; assumptions A1, A2 and A3]

(L4) $\sum_{i \in \mathrm{Supp}(D)} D(i) = 1$

[D a probability measure (the statement)]

(L5) $\sum_{i \in \mathrm{Supp}(D)} D(i)\, U(i)^\alpha < \infty$

[(L3) multiplied by $D(i) \ge 0$; Fact A.45, item 9, its right-hand side's series a combination of those of (L2) and (L4)]

(L6) $\mathbb{E}_{i \leftarrow D}[U(i)^\alpha] \le r_{\mathrm{lo}}^\alpha + (\mathbb{E}_{i \leftarrow D}[U(i)] - r_{\mathrm{lo}})(r_{\mathrm{hi}}^\alpha - r_{\mathrm{lo}}^\alpha)/(r_{\mathrm{hi}} - r_{\mathrm{lo}})$

[(L3) multiplied by $D(i) \ge 0$ and summed over $\mathrm{Supp}(D)$ (Fact A.45, item 9); (L4), (L5)]

(L7) $\mathbb{E}_{i \leftarrow D}[U(i)^\alpha] \le r_{\mathrm{lo}}^\alpha + (1 - r_{\mathrm{lo}})(r_{\mathrm{hi}}^\alpha - r_{\mathrm{lo}}^\alpha)/(r_{\mathrm{hi}} - r_{\mathrm{lo}})$

[(L6), (L1), (L2)]

(L8) $r_{\mathrm{lo}}^\alpha + (1 - r_{\mathrm{lo}})(r_{\mathrm{hi}}^\alpha - r_{\mathrm{lo}}^\alpha)/(r_{\mathrm{hi}} - r_{\mathrm{lo}}) = \dfrac{(1 - r_{\mathrm{lo}}) r_{\mathrm{hi}}^\alpha + (r_{\mathrm{hi}} - 1) r_{\mathrm{lo}}^\alpha}{r_{\mathrm{hi}} - r_{\mathrm{lo}}}$

[expand over $r_{\mathrm{hi}} - r_{\mathrm{lo}} > 0$ (assumption A2)]

(L9) $R_\alpha(D_\delta \,\|\, D)^{\alpha-1} = \mathbb{E}_{i \leftarrow D}[U(i)^\alpha]$

[Definition A.3, item 1, at $(\mu, \nu) := (D_\delta, D)$ and $\mathrm{Supp}(D_\delta) \subseteq \mathrm{Supp}(D)$; U (the statement)]

(L10) $\Rightarrow$ item 1

[(L7), (L8), (L9)]

□ (item 1)

Proof of item 2.

(L11) $p > 0$

[p (the statement); $1 - r_{\mathrm{lo}} > 0$ (assumption A4); $r_{\mathrm{hi}} - r_{\mathrm{lo}} > 0$ (assumption A2)]

(L12) $p < 1$

[p (the statement); $1 - r_{\mathrm{lo}} < r_{\mathrm{hi}} - r_{\mathrm{lo}}$ (assumption A4); assumption A2]

(L13) $D_\star(0) + D_\star(1) = 1$

[$D_\star$ (the statement)]

(L14) $D_{\star\delta}(0) + D_{\star\delta}(1) = p(r_{\mathrm{hi}} - r_{\mathrm{lo}}) + r_{\mathrm{lo}}$

[$D_{\star\delta}$ (the statement)]

(L15) $p(r_{\mathrm{hi}} - r_{\mathrm{lo}}) + r_{\mathrm{lo}} = 1$

[p (the statement)]

(L16) $\Rightarrow$ $D_\star$, $D_{\star\delta}$ probability measures on $\{0, 1\}$

[(L11) to (L15); $r_{\mathrm{lo}}, r_{\mathrm{hi}} \geq 0$ (assumptions A1, A2)]

(L17) $U_\star(0) = r_{\mathrm{hi}}$

[$U_\star$, $D_\star$, $D_{\star\delta}$ (the statement); (L11)]

(L18) $U_\star(1) = r_{\mathrm{lo}}$

[$U_\star$, $D_\star$, $D_{\star\delta}$ (the statement); (L12)]

(L19) $\mathbb{E}_{i \leftarrow D_\star}[U_\star(i)^\alpha] = p\, r_{\mathrm{hi}}^\alpha + (1-p)\, r_{\mathrm{lo}}^\alpha$

[$D_\star$ (the statement); (L17), (L18)]

(L20) $1 - p = (r_{\mathrm{hi}} - 1)/(r_{\mathrm{hi}} - r_{\mathrm{lo}})$

[p (the statement)]

(L21) $p\, r_{\mathrm{hi}}^\alpha + (1-p)\, r_{\mathrm{lo}}^\alpha = \dfrac{(1 - r_{\mathrm{lo}}) r_{\mathrm{hi}}^\alpha + (r_{\mathrm{hi}} - 1) r_{\mathrm{lo}}^\alpha}{r_{\mathrm{hi}} - r_{\mathrm{lo}}}$

[p (the statement); (L20)]

(L22) $R_\alpha(D_{\star\delta} \,\|\, D_\star)^{\alpha-1} = \mathbb{E}_{i \leftarrow D_\star}[U_\star(i)^\alpha]$

[Definition A.3, item 1, at $(\mu, \nu) := (D_{\star\delta}, D_\star)$, $\mathrm{Supp}(D_{\star\delta}) \subseteq \{0,1\}$, $\{0,1\} = \mathrm{Supp}(D_\star)$ ((L11), (L12)); $U_\star$ (the statement)]

(L23) $\Rightarrow$ item 2

[(L16) to (L22)]

□ (item 2)

α	r_{lo}	r_{hi}	**Two-point**	**Tight**
513	0.99	1.01	82.385342616	82.385342616
513	0.999	1.001	1.134204811	1.134204811
1025	0.99	1.01	13439.345906029	13439.345906029
1025	0.999	1.001	1.572140449	1.572140449

Table 47: Attainment by the two-point distribution. Gate: `verify/gates/renyi/two_point.py`.

Lemma K.2 (The chord's value against [Pre17, Lem. 3] [to table])**.** *The mean of* $(1+\delta)^\alpha$ *and* $(1-\delta)^\alpha$ *is at most the constant of [Pre17, Lem. 3] at every order* $\alpha > 1$*. Let:*

- $\alpha > 1$*, an order;*
- $\delta \in [0, 1)$*.*

Define:

- $\mathrm{tight}(\alpha, \delta) = ((1+\delta)^\alpha + (1-\delta)^\alpha)/2$*;*
- $\mathrm{prest}(\alpha, \delta) = 1 + \alpha(\alpha-1)\delta^2/(2(1-\delta)^{\alpha+1})$*, the constant of [L2: Pre17, Lem. 3].*

Then

$$\mathrm{tight}(\alpha, \delta) \leq \mathrm{prest}(\alpha, \delta).$$

Proof. (L1) $1 - \delta > 0$

[δ (the statement)]

(L2) $(1-\delta)^{-1} > 0$

[(L1)]

(L3) $(1+\delta)(1-\delta) \le 1$

[expand; Fact A.41, item 13: $t^{2j} \ge 0$ at $(t,j) := (\delta, 1)$]

(L4) $1+\delta \le (1-\delta)^{-1}$

[(L3) multiplied by $(1-\delta)^{-1} > 0$ (L2)]

(L5) $1 \le (1-\delta)^{-1}$

[(L4); δ (the statement)]

(L6) $1 \le ((1-\delta)^{-1})^{\alpha+1}$

[(L5); Fact A.41, item 5: $t \mapsto t^p$ nondecreasing on $[0,\infty)$ at $p := \alpha+1$; α (the statement)]

(L7) $\mathrm{prest}(\alpha,\delta) = 1 + \alpha(\alpha-1)\delta^2((1-\delta)^{-1})^{\alpha+1}/2$

[prest (the statement); multiply the exponents; (L1)]

(L8) $\alpha(\alpha-1)\delta^2/2 \ge 0$

[α (the statement); Fact A.41, item 13: $t^{2j} \ge 0$ at $(t,j) := (\delta,1)$; Fact A.41, item 8: $ab \le a'b'$ at $(a,a',b,b') := (0, \alpha(\alpha-1)/2, 0, \delta^2)$]

(L9) $\max(\delta, 0) = \delta$

[δ (the statement)]

(L10) $\max(-\delta, 0) = 0$

[δ (the statement)]

(L11) $\alpha \ge 2 \Rightarrow\ (1+\delta)^\alpha \le 1 + \alpha\delta + \frac{\alpha(\alpha-1)}{2}(1+\delta)^{\alpha-2}\delta^2$

[Fact A.41, item 6, at $\epsilon := \delta$; δ (the statement); (L9)]

(L12) $\alpha \ge 2 \Rightarrow\ (1-\delta)^\alpha \le 1 - \alpha\delta + \frac{\alpha(\alpha-1)}{2}\delta^2$

[Fact A.41, item 6, at $\epsilon := -\delta$; δ (the statement); (L10)]

(L13) $\alpha \ge 2 \Rightarrow\ \mathrm{tight}(\alpha,\delta) \le 1 + \alpha(\alpha-1)\delta^2((1+\delta)^{\alpha-2}+1)/4$

[(L11), (L12); tight (the statement); collect]

(L14) $\alpha \ge 2 \Rightarrow\ (1+\delta)^{\alpha-2} \le ((1-\delta)^{-1})^{\alpha-2}$

[(L4); Fact A.41, item 5: $t \mapsto t^p$ nondecreasing on $[0,\infty)$ at $p := \alpha-2$; δ (the statement)]

(L15) $((1-\delta)^{-1})^{\alpha-2} \le ((1-\delta)^{-1})^{\alpha+1}$

[(L5); Fact A.41, item 23: $b^p \le b^q$ at $(b,p,q) := ((1-\delta)^{-1}, \alpha-2, \alpha+1)$]

(L16) $\alpha \ge 2 \Rightarrow\ ((1+\delta)^{\alpha-2}+1)/2 \le ((1-\delta)^{-1})^{\alpha+1}$

[(L14), (L15), (L6)]

(L17) $\alpha \ge 2 \Rightarrow\ \mathrm{tight}(\alpha,\delta) \le \mathrm{prest}(\alpha,\delta)$

[(L16) multiplied by $\alpha(\alpha-1)\delta^2/2 \ge 0$ (L8); (L13), (L7)]

(L18) $\min(\delta, 0) = 0$

[δ (the statement)]

(L19) $\min(-\delta, 0) = -\delta$

[δ (the statement)]

(L20) $\alpha \in (1,2) \Rightarrow\ (1+\delta)^\alpha \le 1 + \alpha\delta + \frac{\alpha(\alpha-1)}{2}\delta^2$

[Fact A.41, item 23, at $(p,\epsilon) := (\alpha,\delta)$; δ (the statement); (L18)]

(L21) $\alpha \in (1,2) \Rightarrow\ (1-\delta)^\alpha \le 1 - \alpha\delta + \frac{\alpha(\alpha-1)}{2}(1-\delta)^{\alpha-2}\delta^2$

[Fact A.41, item 23, at $(p,\epsilon) := (\alpha,-\delta)$; δ (the statement); (L19)]

(L22) $\alpha \in (1,2) \Rightarrow\ \mathrm{tight}(\alpha,\delta) \le 1 + \alpha(\alpha-1)\delta^2(1+(1-\delta)^{\alpha-2})/4$

[(L20), (L21); tight (the statement); collect]

(L23) $(1-\delta)^{\alpha-2} = ((1-\delta)^{-1})^{2-\alpha}$

[multiply the exponents; (L1)]

(L24) $2-\alpha \le \alpha+1$

[α (the statement)]

(L25) $((1-\delta)^{-1})^{2-\alpha} \le ((1-\delta)^{-1})^{\alpha+1}$

[(L5), (L24); Fact A.41, item 23: $b^p \le b^q$ at $(b,p,q) := ((1-\delta)^{-1}, 2-\alpha, \alpha+1)$]

(L26) $(1+(1-\delta)^{\alpha-2})/2 \le ((1-\delta)^{-1})^{\alpha+1}$

[(L23), (L25), (L6)]

(L27) $\alpha \in (1,2) \Rightarrow \ \mathrm{tight}(\alpha,\delta) \le \mathrm{prest}(\alpha,\delta)$

[(L26) multiplied by $\alpha(\alpha-1)\delta^2/2 \ge 0$ (L8); (L22), (L7)]

(L28) $\Rightarrow$ the statement

[(L17), (L27), the two cases covering every $\alpha > 1$ (α, the statement)]

□

Corollary K.3 ([Pre17, Lem. 3] at the symmetric range [to table])**.** *The relative-error bound of [Pre17, Lem. 3] follows from the chord's bound at the symmetric range* $[1-\delta, 1+\delta]$*. Let:*

- $\alpha > 1$*, an order;*
- D *and* D_δ *be probability measures on a countable set with* $\mathrm{Supp}(D_\delta) = \mathrm{Supp}(D)$*;*
- $\delta \in (0,1)$*.*

Define:

- $U = D_\delta / D$ *on* $\mathrm{Supp}(D)$*.*

Assume:

(A1) $\forall i \in \mathrm{Supp}(D) : \ U(i) \in [1-\delta, 1+\delta]$*.*

Then [L1: Pre17, Lem. 3] the Rényi divergence to the power $\alpha - 1$ *is bounded:*

$$R_\alpha(D_\delta \,\|\, D)^{\alpha-1} \le 1 + \frac{\alpha(\alpha-1)\delta^2}{2(1-\delta)^{\alpha+1}}.$$

Proof. (L1) $0 \le 1-\delta$

[$\delta \in (0,1)$ (the statement)]

(L2) $1-\delta < 1+\delta$

[$\delta > 0$ (the statement)]

Lemma K.1, item 1	This proof
Shared: $\alpha,\ D, D_\delta,\ U$	
Shared: $\alpha > 1,\ D, D_\delta$ probability measures on a countable set	
(I1) $(r_{\mathrm{lo}}, r_{\mathrm{hi}})$ $\mathrm{Supp}(D_\delta) \subseteq \mathrm{Supp}(D)$ $r_{\mathrm{lo}}, r_{\mathrm{hi}} \in \mathbb{R}$	$(1-\delta, 1+\delta)$ $\mathrm{Supp}(D_\delta) = \mathrm{Supp}(D)$ (the statement) $\delta \in (0,1)$ (the statement)
Assumption A1 Assumption A2 Assumption A3	(L1) (L2) Assumption A1
Its item 1: $R_\alpha(D_\delta \,\|\, D)^{\alpha-1} = \mathbb{E}_{i \leftarrow D}[U(i)^\alpha] \le \frac{(1-r_{\mathrm{lo}})r_{\mathrm{hi}}^\alpha + (r_{\mathrm{hi}}-1)r_{\mathrm{lo}}^\alpha}{r_{\mathrm{hi}} - r_{\mathrm{lo}}}$	

(L3) $R_\alpha(D_\delta \,\|\, D)^{\alpha-1} \le \frac{(1-(1-\delta))(1+\delta)^\alpha + ((1+\delta)-1)(1-\delta)^\alpha}{(1+\delta)-(1-\delta)}$

[(I1)]

(L4) $\frac{(1-(1-\delta))(1+\delta)^\alpha + ((1+\delta)-1)(1-\delta)^\alpha}{(1+\delta)-(1-\delta)} = \frac{(1+\delta)^\alpha + (1-\delta)^\alpha}{2}$

[expand; divide by $2\delta > 0$ ($\delta > 0$, the statement)]

Lemma K.2	This proof
Shared: $\alpha,\ \delta$	
(I2) Shared: $\alpha > 1$	
$\delta \in [0,1)$	$\delta \in (0,1)$ (the statement)
Its conclusion: $\mathrm{tight}(\alpha,\delta) \le \mathrm{prest}(\alpha,\delta)$	

(L5) $\frac{(1+\delta)^\alpha + (1-\delta)^\alpha}{2} \le 1 + \frac{\alpha(\alpha-1)\delta^2}{2(1-\delta)^{\alpha+1}}$

[(I2); tight, prest (Lemma K.2)]

(L6) $\Rightarrow$ the statement

[(L3), (L4), (L5)]

□

L Indexes: the Lean theorems, the routines and the definitions

This appendix lists the Lean theorems, the routines and the definitions. Table 48 lists the Lean theorems that check the statements.

What is outside the kernel. The following lie outside the kernel.

- The core's rounding rules. `FixedFormat.lean` transcribes them, and the CryptoLine lemmas of the word operations close the transcription against the compiled object of the C code (Lemmas I.2, I.3, I.4, I.5 and I.6).
- The FFT's output order. A gate reads it off the monomial x and compares it with the tower's angle indices at every degree [gate: `verify/gates/tree/tower_index.py`].
- The sampler's probability measure as the product of the leaves' conditional probabilities. The leaf rule of Definition G.9 and Fact A.45, item 1, identify the two.
- The conditionals of P and Q at each leaf as $\widetilde{B}_i$ and $D_{\mathbb{Z},\sigma_i,t_i}$ (Definition A.25, items 1, 2). The Lean theorem of Theorem F.4 takes them as its two hypotheses, on the sequence of leaves and on their tails. The report derives them at (L1) to (L5) and (L11).
- The indexing of the leaves. The kernel's leaf lists, `FTree.centers` and `FTree.zcoords`, put the right subtree before the left at every node and the right leaf before the left at a leaf node, the recursion of Definition A.19. Their entry j is the leaf diagonal d_{j+1} at the positions $2j+1$ and $2j+2$, and the tail-cut event of Definition A.26 is read at that entry (Lemma G.60, (L1) to (L4)).
- The Gram form of Lemma H.6. The report's form sums over the roots with positive imaginary part, and `gramForm` sums over the code's roots, a root and its negative at the paired positions. The lemma identifies the two. `GramPairing.lean` carries the algebra of the re-pairing.

Table 48: Lean theorems by statement.

Statement	Items	Theorems	File
Thm. 1.1		`thm_main_simple`	`LeadingOrder.lean`
Thm. 1.2		`cap_loss_msum`	`Cap.lean`
		`cap_tail_cover`	`Cap.lean`
		`cap_loss_split`	`Cap.lean`
		`thm_falcon_capped`	`Falcon.lean`
		`rpow_le_exp_of_log_le`	`Main.lean`
		`loss_from_bridge_prod`	`Main.lean`
		`loss_from_bridge_prod_of_finite_support`	`Main.lean`
Thm. 1.3		`fx_security_level`	`LeafTail.lean`
		`fx_security_tail`	`LeafTail.lean`
		`fx_security_of_checks`	`LeafTail.lean`
Lemma 4.1	1	`lem_oneleaf_identity`	`Bridge.lean`
Prop. 4.2	4	`prop_csZ_set`	`Renyi.lean`
Thm. 4.3	1	`lem_bridge_cond`	`Compose.lean`
	2	`thm_bridge`	`Compose.lean`
Thm. 4.4		`cap_pow_Sk_le`	`Cap.lean`
		`cond_expect_power_sum`	`CondExpect.lean`

Statement	Items	Theorems	File
		cond_expect_hcond	CondExpect.lean
		thm_main_sub	Main.lean
Def. 4.6		FTree.opBoundC	Shift.lean
		FTree.invBoundC	Shift.lean
Lemma 4.7		falcon_dbar	Falcon.lean
		falcon_chi_sigma_nonneg	Falcon.lean
Lemma 4.8		falcon_El	Falcon.lean
		falcon_el_child	Falcon.lean
Lemma 4.9		falcon_W	Falcon.lean
Cor. 4.10		falcon_dbar_range	Falcon.lean
		falcon_out_mass	Falcon.lean
		cor_falcon_sampler	Falcon.lean
Thm. 4.11		falcon_of_item1_sub	Falcon.lean
		falcon_cond	Falcon.lean
		falcon_core_mass	Falcon.lean
Lemma 4.13		leaf_linear_identity	LeafTail.lean
		leaf_linear_tri	LeafTail.lean
		leaf_linear_K_mul	LeafTail.lean
Lemma 4.14		leafsum_W_le	LeafTail.lean
		leafsum_inv_sigma	LeafTail.lean
		leafsum_delta_le	LeafTail.lean
		leafsum_inv_sigma_le	LeafTail.lean
		leafsum_rem_le	LeafTail.lean
		leafsum_rows_off	LeafTail.lean
		leafsum_cover	LeafTail.lean
		leafsum_dom	LeafTail.lean
		leafsum_tail_prob	LeafTail.lean
		leafsum_rows	LeafTail.lean
		leafsum_eta	LeafTail.lean
		leafsum_xi	LeafTail.lean
		leafsum_wtail_nonneg	LeafTail.lean
		tail_event_le	LeafTail.lean
Def. 5.2		satTerm	Cap.lean
Def. 5.3		levelMass	Cap.lean
		loss_log2	Main.lean
Lemma 5.4		cap_prob_Sk_le	Cap.lean
		sum_prod_choose	Cap.lean
		cap_pow_Em_le	Cap.lean
		cap_prob_Em_le_of_set	Cap.lean
		cap_pow_Em_le_of_finite_support	Cap.lean
Lemma 5.7		fx_thresholds_hold	LeafTail.lean
Prop. 5.8		split_eig_mem	Centers.lean
		split_l10_le_one	Centers.lean
	3, 4	fx_key_root_bounds	FixedKey.lean
	3	fx_key_kappa_root	FixedKey.lean
	1	fx_key_leaf_range	FixedKey.lean
	1	fx_key_diag_range	FixedKey.lean
Prop. 5.9		dom_lb	Dominance.lean
		prop_fx_terms	Falcon.lean

Statement	Items	Theorems	File
Cor. 5.10		satTerm_mono	Cap.lean
		dom_lb	Dominance.lean
		dom_level	Dominance.lean
		prop_fx_terms	Falcon.lean
Thm. 5.11		satBound	Cap.lean
		satBoundG	Cap.lean
		sat_choose_le	Cap.lean
		sat_factor	Cap.lean
		sat_holder_le	Cap.lean
		sat_union_le	Cap.lean
		sat_summand_le	Cap.lean
		satTerm_le_bound	Cap.lean
		satTerm_nonneg	Cap.lean
		sat_cost	Cap.lean
		sat_cost_paper	Cap.lean
		sat_cost_empty	Cap.lean
		sat_ubar_nonneg	Cap.lean
		sat_pbar_nonneg	Cap.lean
		loss_y_pos	Cap.lean
		sat_level_split	Cap.lean
Thm. 5.12		satTerm_empty	Cap.lean
		checks_impact_level	Cap.lean
		checks_level_eta	Cap.lean
		checks_level_loss	Cap.lean
Def. A.4		Rounds	Model.lean
Def. A.8		CAdd	Model.lean
		CMul	Model.lean
		CSub	Model.lean
		CConj	Model.lean
Def. A.10		RelI	Depth.lean
Fact A.16		fact_splitmerge_iso	DefsFacts.lean
		fact_splitmerge_mul	DefsFacts.lean
Def. A.18		FTree	TreeRec.lean
Def. A.19		posNode	DefsFacts.lean
		posR	DefsFacts.lean
		posL	DefsFacts.lean
		pos_split	DefsFacts.lean
		pos_min	DefsFacts.lean
		FTree.rd	Ldl.lean
Def. A.21		FTree.centers	TreeRec.lean
Def. A.23		fusedProb	Fused.lean
Def. A.25		chainMeasure	LeafTail.lean
Def. A.28		renyiPowZ_set	Renyi.lean
		renyiDivZ_set	Renyi.lean
Def. A.29		dev	Bridge.lean
Def. A.30		factorR	LeadingOrder.lean
Fact A.31		fact_counts_depth	DefsFacts.lean
		fact_counts_split	DefsFacts.lean

Statement	Items	Theorems	File
Def. A.32		gramRoot	GramPairing.lean
		gramQuadAt	GramPairing.lean
Fact A.33	3	fact_ntru_g00pos	Tree.lean
	2, 4, 5	fact_ntru	Tree.lean
	6	fact_ntru_max	Tree.lean
Def. A.38		epsJ	Normratio.lean
Def. A.39		normPhi	Normratio.lean
		sMinN	Normratio.lean
		Qform	Normratio.lean
Def. A.40		phiBox	Normratio.lean
Fact A.41	24, 25	dom_minmax_mono	Dominance.lean
	26	elem_scale	Dominance.lean
	1	fact_elem_modulus	Facts.lean
	2	fact_elem_parallelogram	Facts.lean
	3	fact_elem_minkowski	Facts.lean
	4	fact_elem_cauchy_schwarz	Facts.lean
	5	fact_elem_monotone	Facts.lean
	1	fact_elem_conj	Facts.lean
	5	fact_elem_recip	Facts.lean
	9	fact_elem_means	Facts.lean
	10	fact_elem_quot	Facts.lean
	11	fact_elem_taylor2	Facts.lean
	6	fact_elem_taylor	Facts.lean
	7	fact_elem_geom	Facts.lean
	12	fact_elem_exp	Facts.lean
	13	fact_elem_conj_mul	Facts.lean
	14	fact_elem_chord	Facts.lean
	3	fact_elem_pair_bounds	Facts.lean
	8	fact_elem_mul_mono	Facts.lean
	8	fact_elem_prod_floor	Facts.lean
	1, 3	fact_elem_nonneg	Facts.lean
	16	fact_elem_affine	Facts.lean
	17	fact_elem_sets	Facts.lean
	18	fact_elem_limit	Facts.lean
	19	fact_elem_chain	Facts.lean
	3	fact_elem_pair_vec	Facts.lean
	20	fact_elem_minmax	Facts.lean
	21	fact_elem_cosh	Facts.lean
	17	fact_elem_sets_inter	Facts.lean
	20	fact_elem_sup	Facts.lean
	12	fact_elem_two_rpow	Facts.lean
	22	fact_elem_floor	Facts.lean
	5	fact_elem_deriv_mono	Facts.lean
	29	fact_elem_lnprod	Facts.lean
	30	fact_elem_lnexp	Facts.lean
	31	fact_elem_logseries	Facts.lean
	32	fact_elem_geomtail	Facts.lean
	33	fact_elem_sqsum	Facts.lean

Statement	Items	Theorems	File
	34	fact_elem_sqdiff	Facts.lean
	35	fact_elem_conjconj	Facts.lean
	36	fact_elem_reconj	Facts.lean
	37	fact_elem_choose	Facts.lean
	40	fact_elem_rpow	Facts.lean
	47	fact_elem_lemin	Facts.lean
		fact_elem_expge	LeafTail.lean
	28	fact_elem_explog	Meas.lean
	15	abs_log_one_add_sub_le	Normratio.lean
	23	rpow_taylor_bound_lt_two	TightPrest.lean
	23	fact_elem_rpow_le_rpow_of_exponent_le	TightPrest.lean
Fact A.42	1	fact_poly_abs	FactPoly.lean
	2	fact_poly_conj	FactPoly.lean
	3	fact_poly_sum	FactPoly.lean
	4	fact_poly_split	FactPoly.lean
	6	fact_poly_evaladd	FactPoly.lean
	7	fact_poly_evalmul	FactPoly.lean
	8	fact_poly_evalconst	FactPoly.lean
	9	fact_poly_roots	FactPoly.lean
Fact A.43		fact_roots_half_roots	DefsFacts.lean
		fact_roots_half_conj	DefsFacts.lean
		fact_roots_half_neg	DefsFacts.lean
		fact_roots_half_sqrt	DefsFacts.lean
		fact_roots_half_square	DefsFacts.lean
		fact_roots_half_sum	DefsFacts.lean
		fact_roots_half_half	DefsFacts.lean
Fact A.44	2	fact_matrix_eig	Facts.lean
	2	fact_matrix_eig_symm	Facts.lean
	3	fact_matrix_rayleigh	Facts.lean
	4	fact_matrix_psd	Facts.lean
	5	fact_matrix_unit_lower_inv	Facts.lean
Fact A.45	7	holder_event	Cap.lean
		condExpLast	CondExpect.lean
		cond_expect_power_sum	CondExpect.lean
	4	fact_prob_rejection	Facts.lean
	6	fact_prob_gaussian	Facts.lean
	5	fact_prob_compl	Facts.lean
	9	fact_prob_series	Facts.lean
	12	fact_prob_mono	Facts.lean
	12	fact_prob_empty	Facts.lean
	13	gaussianReal_tail_upper_lt	Meas.lean
	13	gaussianReal_tail_two_lt	Meas.lean
	13	hasLaw_gaussian_tail_upper	Meas.lean
	13	hasLaw_gaussian_tail_two	Meas.lean
	8	renyi_mono_order	Renyi.lean
	8	renyi_mono_order_set	Renyi.lean

Statement	Items	Theorems	File
Def. A.46		Cascade	Tree.lean
Lemma B.1		rel_of_norm_le	Elementary.lean
Lemma B.2	1	lem_A	Elementary.lean
	2	lem_A_sub	Elementary.lean
	4	lem_C	Elementary.lean
	3	lem_B	Elementary.lean
	5	lem_F	Elementary.lean
Lemma B.3		lem_D	Elementary.lean
Lemma B.4		dgauss_term	LeafTail.lean
		dgauss_mgf_shift	LeafTail.lean
		dgauss_mgf_bound	LeafTail.lean
Lemma B.5		azuma_mgf_rec	LeafTail.lean
		azuma_exponent	LeafTail.lean
		azuma_tail	LeafTail.lean
Lemma C.1		Cascade.lem_mixed_pure	Tree.lean
Lemma C.2		Cascade.lem_mixed	Tree.lean
Fact D.1		fact_means_split	DefsFacts.lean
Fact D.2		fact_means	Tree.lean
Fact D.3		fact_means_kappa	Tree.lean
Lemma D.4		lem_G_ldl	Slots.lean
		lem_G_ldl_matrix	Slots.lean
Lemma D.5		lem_ffldl_interval	Leafrange.lean
Lemma D.6		lem_ffldl_pos	Leafrange.lean
Lemma D.7		cascade_of_stepsDiag	Leafrange.lean
Lemma D.8		ffLDL_weights_mem	Leafrange.lean
Prop. D.9		prop_leafrange	Leafrange.lean
		leafrange_const	LeafrangeChecks.lean
	2	leafrange_hA2	LeafrangeChecks.lean
Lemma D.11		inv_rounded_bounds	Leafrange.lean
		leaf_sigma_bounds	Leafrange.lean
Lemma E.1		lem_identity	Bridge.lean
Lemma E.2		lem_normdev_series	Normratio.lean
		cor_normdev_bound	Normratio.lean
Cor. E.3		cor_dgauss_mgf_mp	Normratio.lean
Fact E.4		fact_eps_mono	Normratio.lean
Lemma E.5		lem_normratio_identity	Bridge.lean
Lemma E.6		lem_normratio_second	Normratio.lean
Lemma E.7		lem_normratio_theta	Normratio.lean
Lemma E.8		abs_devA1_le	Normratio.lean
		abs_devA2_le	Normratio.lean
Lemma E.9		dev_taylor	Normratio.lean

Statement	Items	Theorems	File
Lemma E.10		lem_normratio_bound	Normratio.lean
Lemma E.11		box_theta	Normratio.lean
		box_s	Normratio.lean
Lemma E.12		box_vs_bound	Normratio.lean
		box_vc_bound	Normratio.lean
		box_diff_s	Normratio.lean
		box_diff_c	Normratio.lean
Cor. E.13		cor_normratio_box	Normratio.lean
Cor. E.14		cor_oneleaf_phi	Normratio.lean
Lemma E.15		lem_trajectory_leaf	Bridge.lean
Lemma E.16		compose_step	Compose.lean
		seq_bound	Compose.lean
Lemma E.17		lem_trajectory	Compose.lean
		lem_trajectory_weight_max	Normratio.lean
Lemma E.18	1	lem_tail	Tail.lean
	2	cor_tail_norm	Tail.lean
Cor. E.19		cor_tail_banaszczyk	Tail.lean
Lemma E.20		tail_step	Compose.lean
		cor_bridge_tail	Compose.lean
Cor. E.21		thm_bridge_tail	Compose.lean
Lemma F.1		cond_expect_power_sum	CondExpect.lean
		cond_expect_hcond	CondExpect.lean
		thm_main_leaf	Main.lean
Lemma F.2		cond_expect_power_sum	CondExpect.lean
		cond_expect_hcond	CondExpect.lean
		lem_compose_R	Main.lean
Lemma F.3		lem_condition	Main.lean
Thm. F.4		thm_main	Main.lean
		thm_main_sub	Main.lean
Cor. F.5		cor_lnR_leading_theta	LeadingOrder.lean
		cor_lnR_leading_w	LeadingOrder.lean
		cor_lnR_leading_lnR	LeadingOrder.lean
Lemma G.1		rel_of_abs_le	Elementary.lean
Lemma G.2		lem_factors	Elementary.lean
Lemma G.3		sum_weighted_mem	Elementary.lean
Lemma G.4		norm_prod_one_add_sub_one_le	Elementary.lean
Fact G.5		fusedWeights_eq	Fused.lean
		fusedRootCenters_eq	Fused.lean
Def. G.6		coeffAt	DefsFacts.lean

Statement	Items	Theorems	File
		tmEll	DefsFacts.lean
		tmQ	DefsFacts.lean
		tmC	DefsFacts.lean
		tmP	DefsFacts.lean
		tmCF	DefsFacts.lean
		tmCoord	DefsFacts.lean
		FTree.rco	Ldl.lean
		FTree.rzc	Ldl.lean
		FTree.Lmat	Ldl.lean
		FTree.coords	TreeRec.lean
Fact G.7		fact_coords_split_halves	DefsFacts.lean
		coords_digit_sum_lt	DefsFacts.lean
		coords_digits_unique	DefsFacts.lean
		coords_digits_exist	DefsFacts.lean
		coords_leaf_table	DefsFacts.lean
		coords_left_shift	DefsFacts.lean
		coords_first_digit	DefsFacts.lean
		coords_rest	DefsFacts.lean
		coords_parity	DefsFacts.lean
		coords_child_index	DefsFacts.lean
		coords_coeff_linear	DefsFacts.lean
		tm_offset	DefsFacts.lean
		tm_ell_digits	DefsFacts.lean
		tm_first_digit	DefsFacts.lean
		tm_child_digits	DefsFacts.lean
		tm_child_index	DefsFacts.lean
		coeffAt_split	DefsFacts.lean
		fact_coords_split_coeff	DefsFacts.lean
		fact_coords_split_half	DefsFacts.lean
		fact_coords_split_child	DefsFacts.lean
		fact_coords_split_node	DefsFacts.lean
		fact_coords_split_subtree	DefsFacts.lean
		fact_coords_split_subtree0	DefsFacts.lean
		fact_coords_split_index_bij	DefsFacts.lean
		fact_coords_split_bij	DefsFacts.lean
		pos_min	DefsFacts.lean
		tm_p_leaf	DefsFacts.lean
		coords_right_ell	DefsFacts.lean
		tm_ell_first	DefsFacts.lean
		coords_child_min	DefsFacts.lean
Fact G.8		FTree.fact_treemap_linear	TreeRec.lean
Def. G.9		FTree.Qset	Integrality.lean
		FTree.outputProb	Output.lean
Lemma G.10		FTree.zcoords_unzc	Ldl.lean
		splitV_mergeV	TreeRec.lean
Lemma G.11		FTree.rco_eq_add_sum	Ldl.lean
		FTree.node_left_correction	Ldl.lean
		FTree.Lmat_node_left_right	Ldl.lean
		FTree.Lmat_node_right	Ldl.lean

Statement	Items	Theorems	File
		FTree.Lmat_node_left	Ldl.lean
Fact G.12		fusedRootProb_eq	Fused.lean
Lemma G.13		sq_pair_le	Slots.lean
Lemma G.14		lem_C_root_norm	Integrality.lean
Prop. G.15		prop_parseval	Parseval.lean
Lemma G.16		lem_D	Elementary.lean
Lemma G.17		lem_D	Elementary.lean
Lemma G.18		lem_E	Elementary.lean
Prop. G.19		split_eq_evenOdd	Integrality.lean
		prop_parseval_split	Parseval.lean
		pairSqC_splitV	Shift.lean
		vecNormC_mergeV	Shift.lean
Lemma G.20		lem_I	Slots.lean
Lemma G.21		lem_J	Slots.lean
Lemma G.22		lem_H_diag	Slots.lean
Lemma G.23		lem_H_off	Slots.lean
Lemma G.24		LDLSlot_of_div	Slots.lean
	1, 4	lem_G	Slots.lean
	2	lem_G_l10_bound	Slots.lean
Lemma G.25		lem_G_d11_raw	Slots.lean
		lem_G_kappa	Slots.lean
Lemma G.26		node_off_form	Node.lean
Lemma G.27		lem_node_pair	NodeMixed.lean
Lemma G.28		lem_node_d0_mean	NodeMixed.lean
Lemma G.29		lem_node_d1_mod	NodeMixed.lean
Lemma G.30		lem_node_num	NodeMixed.lean
Lemma G.31		lem_node_num_bound	NodeMixed.lean
Lemma G.32	1, 2	lem_node_mixed	NodeMixed.lean
Lemma G.33		PhiM	Depth.lean
		PhiM_mono	Depth.lean
Lemma G.34	1	first_diag_le_PhiM	Depth.lean
Lemma G.35		kappa_computed_le	Depth.lean
Cor. G.36		PhiM_iterate_path_either	Depth.lean
		PhiM_iterate_path_exact	Depth.lean
		nodeU0_nonneg_of_lt	Depth.lean
		le_first_diag	Depth.lean
		PhiM_chain_step_ge	Depth.lean
		PhiM_iterate_mono	Depth.lean
Lemma G.37		child_off_error	Depth.lean
Prop. G.38		prop_kappa	Leafrange.lean
Lemma G.39		fx_root_numerator	FixedRoot.lean
Lemma G.40	1, 2	lem_root_direct	FixedRoot.lean
Cor. G.41		lem_Jabs_mono	Tree.lean
		cor_dbar_of_leaf	Tree.lean
Lemma G.42		l10_error_mixed	Depth.lean

Statement	Items	Theorems	File
Cor. G.43		cor_l10_nodes	Depth.lean
Lemma G.44		FTree.center_update	TreeRec.lean
Lemma G.45		FTree.centers_sub_zcoords_base	TreeRec.lean
Lemma G.46		FTree.centers_sub_zcoords_node	TreeRec.lean
Lemma G.47		FTree.centers_sub_zcoords	TreeRec.lean
Prop. G.48	1	FTree.centers_sub_zcoords_real	Ldl.lean
	2	FTree.cor_centerres	Ldl.lean
Lemma G.49		FTree.centers_add	Centers.lean
Fact G.50		fact_pairnorm	Entries.lean
Lemma G.51	1	lem_fresh_updateC	Shift.lean
	2	lem_fresh_updateC_exact	Shift.lean
Lemma G.52		lem_fresh_merge_halfC	Shift.lean
Lemma G.53	1	lem_fresh_splitC	Shift.lean
	2	lem_fresh_leftC	Shift.lean
	1, 2	lem_fresh_leafC	Shift.lean
Lemma G.54		FTree.centersInj_eq	Shift.lean
Lemma G.55		thm_centers_boundC	Shift.lean
Lemma G.56		FTree.entryEnergy_leC	Entries.lean
Lemma G.57		lem_fresh_node	Shift.lean
Lemma G.58		energyAtC_le_of_freshDepthC	Entries.lean
Thm. G.59		thm_centers_of_runNodesC	Entries.lean
Lemma G.60		runNodesC_res_depth	Entries.lean
		runNodesC_res_le	Entries.lean
		centers_rk_depth_sum	Shift.lean
Lemma G.61		runNodesC_tt_chain	Entries.lean
		centers_depth_sums_pair	Shift.lean
Cor. G.62		cor_centers_first_S_shift	Entries.lean
		cor_centers_first_S_shift_of_runNodesC	Entries.lean
		cor_centers_first_S_shift_of_goodEvent	Entries.lean
		centers_first_S_Mk_nonneg	Entries.lean
		centers_first_S_GZ_nonneg	Entries.lean
		centers_first_S_GZ_Mk_le	Entries.lean
Lemma G.63		acceptance_le_one	Sampler.lean
Lemma G.64		lem_sampler_measure	Sampler.lean
Lemma G.65		lem_varianceZ_set	Renyi.lean
Fact G.66		fact_acc	Budget.lean
Lemma G.67		leafF_weight_le	Renyi.lean
Lemma G.68		lem_leafFZ_set	Renyi.lean
Lemma G.69		rhoZ_ge_eta	MomentLeaves.lean
		moment_rows_dist_eq	MomentLeaves.lean
		moment_rows_dist_mem	MomentLeaves.lean
		moment_rows_dist	MomentLeaves.lean
		moment_rows_tail_le	MomentLeaves.lean

Statement	Items	Theorems	File
		moment_rows_reach	MomentLeaves.lean
Lemma G.70		eps_tab_mem	MomentLeaves.lean
		moment_tab_mean_dev	MomentLeaves.lean
		moment_tab_dev_le	MomentLeaves.lean
Lemma G.71		floor_mass_eq	MomentLeaves.lean
		floor_mass_sq_le	MomentLeaves.lean
Lemma G.72		eps_ar_le	MomentLeaves.lean
		abs_eps_ar_le	MomentLeaves.lean
Lemma G.73	1, 2	lem_moment_leaves	MomentLeaves.lean
		moment_leaves_weights_le	MomentLeaves.lean
		moment_leaves_tab_sq_le	MomentLeaves.lean
Lemma G.74		dom_sum_mul	Dominance.lean
		dom_minmax_mono	Dominance.lean
		dom_mul_interval	Dominance.lean
		dom_Dbar	Dominance.lean
		dom_sq_interval	Dominance.lean
		dom_min_breakpoints	Dominance.lean
		dom_Dbar_all	Dominance.lean
		dom_varpi	Dominance.lean
		dom_w_nonneg	Dominance.lean
		dom_eps	Dominance.lean
		dom_affine_sum	Dominance.lean
		dom_sum_superset	Dominance.lean
		dom_min_mono	Dominance.lean
		dom_floor	Dominance.lean
		dom_max_index	Dominance.lean
		dom_wbar_ar	Dominance.lean
		dom_rpow_interval	Dominance.lean
		dom_fl_term	Dominance.lean
		dom_min_compare	Dominance.lean
		dom_moment_sq	Dominance.lean
		moment_mono_s_lt_two	Dominance.lean
		moment_mono_eps0_gap	Dominance.lean
Cor. G.75	2	renyi_pow_floor	Cap.lean
	2, 3	cor_logrho_floor	Cap.lean
	2	cap_mass_floor	Cap.lean
		renyi_pow_floor_of_finite_support	Cap.lean
		cor_logrho_tau	Main.lean
Lemma G.76		falcon_chi_root	Falcon.lean

Statement	Items	Theorems	File
Lemma G.77		iterMap_kappaHat	Depth.lean
		falcon_leaf_mono	Depth.lean
Lemma G.78		lower_mass_ge	Main.lean
		goodevent_pos	Main.lean
		goodevent_pos_base_mass	Main.lean
		goodevent_pos_sigma	Main.lean
Lemma G.79		terms_nonneg	Falcon.lean
Fact G.80		cap_reject_mass	Falcon.lean
		cap_reject_empty	Falcon.lean
		cap_reject_zero	Falcon.lean
		fact_cap_reject	Falcon.lean
Def. H.1		FTree.Q	TreeRec.lean
Lemma H.2		FTree.Q_eq_sum_real	Ldl.lean
Lemma H.3		FTree.Q_node	TreeRec.lean
		FTree.Q_base	TreeRec.lean
Fact H.4		pair_form_split	Gram.lean
Lemma H.5		node_form_ldl	Gram.lean
Lemma H.6		sum_pair_forms	Gram.lean
		gramRoot_reflect_exp	GramPairing.lean
		gramRoot_reflect_conj	GramPairing.lean
		gramQuadAt_conj	GramPairing.lean
		gramQuadAt_real	GramPairing.lean
		gramQuadAt_conj_eq	GramPairing.lean
		gramQuadAt_pair_sum	GramPairing.lean
Prop. H.7	3	Q_rootTree_eq_gramForm	Gram.lean
	1	FTree.prop_ldl	Ldl.lean
	2	FTree.weight_eq_exp	TreeRec.lean
Lemma H.8		lem_fft_levels	FftImage.lean
Lemma H.9		fft_level_error	FftImage.lean
Lemma H.10		fft_error_closed	FftImage.lean
Lemma H.11		lem_fft_perm	FftImage.lean
Lemma H.12		lem_fft_entry	FftImage.lean
Lemma H.13		g00_floor_key	KeyFloor.lean
Lemma H.14		fx_key_gram_diag	FixedKey.lean
		fx_key_gram_off	FixedKey.lean
Lemma H.15		fx_image_dev_free	GramDevFree.lean
		fx_image_ceiling	GramDevFree.lean
Lemma H.16		g00t_floor	GramDevFree.lean
		gram_floor_pow_lt	GramDevFree.lean

Statement	Items	Theorems	File
		gram_floor_dev_lt	GramDevFree.lean
		gram_floor_dev_lt_g00	GramDevFree.lean
Lemma H.17	1, 2	checks_slot	KeyChecksRounded.lean
	3	checks_hyb	KeyChecksRounded.lean
	4	checks_root	KeyChecksRounded.lean
		checks_thr_sq	KeyChecksRounded.lean
		checks_grid_sub	KeyChecksRounded.lean
		checks_thr_exact	KeyChecksRounded.lean
		checks_lo_pos	KeyChecksRounded.lean
		checks_num_ge	KeyChecksRounded.lean
		checks_g00_sq_gap	KeyChecksRounded.lean
		checks_sq_pos	KeyChecksRounded.lean
Lemma H.18		fx_key_image_slots	FixedKey.lean
Lemma H.19		fx_key_g00_range	FixedKey.lean
		fx_key_g11_le	FixedKey.lean
Lemma H.20		opnorm_gram_fwd	Centers.lean
		opnorm_gram_inv	Centers.lean
		opnorm_gram_leaf_floor	Dominance.lean
		opnorm_gram_leaf_ceil	Dominance.lean
		opnorm_gram_form_eq	Dominance.lean
		opnorm_gram_parseval	Dominance.lean
		opnorm_gram_ray_floor	Dominance.lean
		opnorm_gram_ray_floor_coef	Dominance.lean
		opnorm_gram_ray_ceil	Dominance.lean
		opnorm_gram_ray_ceil_coef	Dominance.lean
Lemma H.21		lem_fx_root_inv	Centers.lean
		opnorm_ge_one	Centers.lean
		root_eig_prod	Dominance.lean
		root_eig_hi_le	Dominance.lean
		root_unit_coords	Dominance.lean
		root_unit_norm	Dominance.lean
		root_unit_image	Dominance.lean
		root_unit_image_norm	Dominance.lean
		root_opNormC_eq	Dominance.lean
Lemma H.22		lem_center_normC	CenterBounds.lean
		center_norm_hm_sq	CenterBounds.lean

Statement	Items	Theorems	File
Lemma H.23		lem_fx_output_norm_solve	Entries.lean
		sample_norm_event	Entries.lean
		sample_norm_tlsigma_le	Entries.lean
		sample_norm_gap_pos	Entries.lean
		sample_norm_shift_solve	Entries.lean
Lemma H.24		lem_budget_ranges	Budget.lean
Lemma H.25		lem_budget_poly	BudgetPoly.lean
Lemma H.26		lem_budget_floors	Budget.lean
		lem_budget_floors_ratio	Budget.lean
	3	floors_seam	Floors.lean
Def. I.1	1	fxAdd_rounds	FixedFormat.lean
	1	roundAway	FixedFormat.lean
	1	roundAway_real	FixedFormat.lean
	1	fxMul_rounds	FixedFormat.lean
	1	fxDiv_rounds	FixedFormat.lean
	1	fxSqrt_rounds	FixedFormat.lean
	1	fxHalf_rounds	FixedFormat.lean
	1	fxDiv2e_rounds	FixedFormat.lean
	2	halved_sum_rounds	FixedFormat.lean
	2	fxHalf_add_rounds	FixedFormat.lean
	1	fxCAdd_cadd	FixedFormat.lean
	1	fxCMul_cmul	FixedFormat.lean
		roundAway_eq_formula	MachineWords.lean
		isqrtNearest_eq_formula	MachineWords.lean
Lemma I.2	1	cl_fx_add_of_contract	MachineWords.lean
	2	cl_fx_sub_of_contract	MachineWords.lean
	3	cl_fx_neg_of_contract	MachineWords.lean
Lemma I.3		MulW_of_contract	FxKernels.lean
		cl_fx_mul	MachineWords.lean
		cl_fx_mul_of_contract	MachineWords.lean

Statement	Items	Theorems	File
		cl_fx_mul_apply_of_contract	MachineWords.lean
Lemma I.4		DivW_of_contract	FxKernels.lean
		cl_fx_div	MachineWords.lean
		cl_fx_div_of_contract	MachineWords.lean
		cl_fx_div_apply_of_contract	MachineWords.lean
Lemma I.5		cl_fx_sqrt_apply_of_contract	FxKernels.lean
		cl_fx_sqrt	MachineWords.lean
		cl_fx_sqrt_of_contract	MachineWords.lean
Lemma I.6	2	cl_fx_div2e	MachineWords.lean
		cl_fx_div2e_of_contract	MachineWords.lean
	1	cl_fx_half	MachineWords.lean
		cl_fx_half_of_contract	MachineWords.lean
	3	cl_fx_mul2e_of_contract	MachineWords.lean
Lemma I.7	2	cl_fx_floor	MachineWords.lean
		cl_fx_floor_of_contract	MachineWords.lean
	3	cl_fx_trunc	MachineWords.lean
		cl_fx_trunc_of_contract	MachineWords.lean
	4	cl_fx_rint	MachineWords.lean
		cl_fx_rint_of_contract	MachineWords.lean
	1	cl_fx_of_of_contract	MachineWords.lean
Lemma I.8	2	cl_fx_max	MachineWords.lean
		cl_fx_max_of_contract	MachineWords.lean
	3	cl_fx_min	MachineWords.lean
		cl_fx_min_of_contract	MachineWords.lean
	1	cl_fx_lt_of_contract	MachineWords.lean
Cor. I.9	3	lem_B_fx	FixedPoint.lean

Statement	Items	Theorems	File
		lem_D_fx	FixedPoint.lean
		lem_E_fx	FixedPoint.lean
	5	lem_F_fx	FixedPoint.lean
Lemma I.10		kern_cmul	FxKernels.lean
	1, 4, 7	kern_butterfly	FxKernels.lean
	2	kern_split	FxKernels.lean
	3	kern_selfadj	FxKernels.lean
	5, 6	kern_ldl	FxKernels.lean
		kern_selfadj_words	FxKernels.lean
		kern_ldl_words	FxKernels.lean
		kern_ldlroot_words	FxKernels.lean
		kern_add_of_contract_2	FxKernels.lean
		kern_add_of_contract_3	FxKernels.lean
		kern_add_of_contract_4	FxKernels.lean
		kern_add_of_contract_5	FxKernels.lean
		kern_sub_of_contract_2	FxKernels.lean
		kern_sub_of_contract_3	FxKernels.lean
		kern_sub_of_contract_4	FxKernels.lean
		kern_sub_of_contract_5	FxKernels.lean
		kern_ldl_of_contract_2	FxKernels.lean
		kern_ldl_of_contract_3	FxKernels.lean
		kern_ldl_of_contract_4	FxKernels.lean
		kern_ldl_of_contract_5	FxKernels.lean
		kern_ldlroot_of_contract_2	FxKernels.lean
		kern_ldlroot_of_contract_3	FxKernels.lean
		kern_merge_of_contract_2	FxKernels.lean
		kern_merge_of_contract_3	FxKernels.lean
		kern_merge_of_contract_4	FxKernels.lean
		kern_merge_of_contract_5	FxKernels.lean
		kern_mulfft_of_contract_2	FxKernels.lean
		kern_mulfft_of_contract_3	FxKernels.lean
		kern_mulfft_of_contract_4	FxKernels.lean
		kern_mulfft_of_contract_5	FxKernels.lean
		kern_selfadj_of_contract_2	FxKernels.lean
		kern_selfadj_of_contract_3	FxKernels.lean
		kern_selfadj_of_contract_4	FxKernels.lean
		kern_selfadj_of_contract_5	FxKernels.lean
		kern_split_of_contract_2	FxKernels.lean
		kern_split_of_contract_3	FxKernels.lean
		kern_split_of_contract_4	FxKernels.lean
		kern_split_of_contract_5	FxKernels.lean
		deep_words	FxKernels.lean
		ffsamp_deep_of_contract_2	FxKernels.lean
		ffsamp_deep_of_contract_3	FxKernels.lean
		ffsamp_deep_of_contract_4	FxKernels.lean
		ffsamp_deep_of_contract_5	FxKernels.lean

Statement	Items	Theorems	File
	8	kern_setsmall	FxNoWrapFft.lean
	9	kern_neg	FxNoWrapFft.lean
Lemma I.11		FxRec.cCodeOf_kernelRuns_2_10	FxDataflowClaims.lean
Lemma I.12		sv_eq_of_bound	FxNoWrap.lean
		fxMul_abs_le	FxNoWrap.lean
		fxDiv_abs_le	FxNoWrap.lean
		fxHalf_abs_le	FxNoWrap.lean
		mul_nowrap	FxNoWrap.lean
		div_nowrap	FxNoWrap.lean
		half_nowrap	FxNoWrap.lean
		add_nowrap	FxNoWrap.lean
		sub_nowrap	FxNoWrap.lean
		neg_nowrap	FxNoWrap.lean
Def. I.19		tailVerdict	LeafTail.lean
Def. I.20		ffsamp_level_of_contract_2_t3	FxKernels.lean
		ffsamp_level_of_contract_2_t4	FxKernels.lean
		ffsamp_level_of_contract_2_t5	FxKernels.lean
		ffsamp_level_of_contract_3_t4	FxKernels.lean
		ffsamp_level_of_contract_3_t5	FxKernels.lean
Cor. I.24		lem_G_fx	FixedPoint.lean
Lemma I.25		lem_fx_root_relI	FixedRoot.lean
Lemma I.26		lem_fx_root_identity_q	FixedRoot.lean
Lemma I.27		lem_fx_root_identity_bounds_relI	FixedRoot.lean
Def. I.28		PhiM0	FixedNode.lean
Lemma I.29		lem_fx_node_d0	FixedNode.lean
Lemma I.30		lem_fx_node_d11	FixedNode.lean
Lemma I.31		lem_fx_node_rec	FixedNode.lean
Def. I.32		fxChain	FixedNode.lean
Cor. I.33		cor_fx_recursion_path_either	FixedNode.lean
		cor_fx_recursion_path_exact	FixedNode.lean
Lemma I.34		setsmall_value	FxNoWrapFft.lean
		cpair_norm_le	FxNoWrapFft.lean
		kern_butterfly_mod	FxNoWrapFft.lean
		fftModBound_le	FxNoWrapFft.lean
		fftModBound_le8	FxNoWrapFft.lean
		fftModBound_int8	FxNoWrapFft.lean
		fftModBound_int9	FxNoWrapFft.lean
		fftModBound_ceil_lt	FxNoWrapFft.lean

Statement	Items	Theorems	File
		fftGen_base	FxNoWrapFft.lean
		fftGen_step	FxNoWrapFft.lean
		fftGen_mono	FxNoWrapFft.lean
		fft_stage_gen	FxNoWrapFft.lean
		fft_stages_gen	FxNoWrapFft.lean
		fft_stages_gen_le	FxNoWrapFft.lean
Lemma I.35		gram_entry_nowrap	FxNoWrapGram.lean
		gram_g01_nowrap	FxNoWrapGram.lean
		gram_bounds_81	FxNoWrapGram.lean
		gram_off_bound_81	FxNoWrapGram.lean
Lemma I.36		key_check_num_512	KeyCheckWords.lean
		key_check_num_1024	KeyCheckWords.lean
Lemma I.37		sqr_word_pos	KeyCheckWords.lean
Lemma I.38	2	key_check_ratio	KeyCheckWords.lean
Lemma I.39		quot_nowrap	FxNoWrapRoot.lean
Lemma I.40		node_bounds	FxNoWrapNode.lean
		half_sum_floor	FxNoWrapNode.lean
Lemma I.41		node_bounds	FxNoWrapNode.lean
		half_sum_floor	FxNoWrapNode.lean
		zo_le	FxNoWrapRoot.lean
Lemma I.42		deepest_leaf_bounds	FxNoWrapNode.lean
Lemma I.43	1	diag_range_of_chi	FxNoWrapNode.lean
Lemma I.44		node_bounds	FxNoWrapNode.lean
Fact I.45		fact_fx_input16	Integrality.lean
Lemma I.46		fftModBound_le9	FxNoWrapCenter.lean

Statement	Items	Theorems	File
		fftModBound_q9	FxNoWrapCenter.lean
		load_value	FxNoWrapCenter.lean
		inv_q_word_lt	FxNoWrapCenter.lean
		center_bounds	FxNoWrapCenter.lean
Lemma I.47		fftModBound_le9	FxNoWrapCenter.lean
		fftModBound_q9	FxNoWrapCenter.lean
		load_value	FxNoWrapCenter.lean
		inv_q_word_lt	FxNoWrapCenter.lean
		center_bounds	FxNoWrapCenter.lean
Lemma I.48		parts_scale_le	FxNoWrapSamples.lean
		root_l10_le	FxNoWrapSamples.lean
		child_l10_le	FxNoWrapSamples.lean
		splitsa_odd_le	FxNoWrapSamples.lean
Lemma I.49		node_dev_step	FxNoWrapSamples.lean
		child_center_le	FxNoWrapSamples.lean
		tb_le	FxNoWrapSamples.lean
		leaf_dev_le	FxNoWrapSamples.lean
		half0_dev_le	FxNoWrapSamples.lean
		recursion_mono	FxNoWrapSamples.lean
		fx64_le_of_le	FxNoWrapSamples.lean
		floor_int32	FxNoWrapSamples.lean
Lemma I.50		ccs_le	FxNoWrapSamples.lean
Lemma I.51		sigma_le	FxNoWrapSamples.lean
		sigma_gt	FxNoWrapSamples.lean
Lemma I.52		berexp_r_le	FxNoWrapSamples.lean

Statement	Items	Theorems	File
Lemma I.53		ifft_butterfly_le	FxNoWrapSamples.lean
Thm. I.54		sv_bounds	FxNoWrap.lean
Lemma I.55		ifft_stage_inverse	FxNoWrapSamples.lean
Lemma I.56		merge_dev_step	FxNoWrapSamples.lean
		ifft_err_step	FxNoWrapSamples.lean
		int_eq_of_close	FxNoWrapSamples.lean
Cor. I.57		lem_fresh_splitC_fx	Shift.lean
	2	lem_fresh_updateC_fx	Shift.lean
	3	lem_fresh_leftC_fx	Shift.lean
	4	lem_fresh_merge_halfC_fx	Shift.lean
Lemma I.58		lem_fx_sampler_arg	FixedSampler.lean
Lemma I.59		lem_fx_sampler_split	FixedSampler.lean
Lemma I.60		fx_sampler_poly_ccs	FxWidths.lean
		lem_fx_sampler_poly	FxWidths.lean
Lemma I.61		lem_fx_sampler_acc	FixedSampler.lean
Lemma I.63		fx_key_gram_diag	FixedKey.lean
		fx_key_leaf_range	FixedKey.lean
Lemma I.64		fact_cap_reject	Falcon.lean
		fx_eplus_corner	FixedSampler.lean
		fx_split_neg_si	FixedSampler.lean
		fx_split_neg_r	FixedSampler.lean
		fx_acc_word_le	FixedSampler.lean
Lemma I.66		cor_fx_recursion_path_exact	FixedNode.lean
		lem_fx_root_relI	FixedRoot.lean
		lem_fx_root_identity_bounds_relI	FixedRoot.lean
Lemma I.67		cor_dbar_of_leaf	Tree.lean
Lemma I.69		lem_fx_widths_eps	FxWidths.lean
		fx_widths_dbar_nonneg	FxWidths.lean
		fx_widths_pole_ge	FxWidths.lean
		fx_widths_sstar	FxWidths.lean
		lem_fx_widths_norm	FxWidths.lean
Lemma I.71		dom_chain	Dominance.lean
		dom_dbar	Dominance.lean
		dom_ebar0	Dominance.lean
		dom_El_child	Dominance.lean
		dom_El_root	Dominance.lean
		dom_gamma_sum	Dominance.lean
		dom_sum_mul	Dominance.lean

Statement	Items	Theorems	File
		dom_quot	Dominance.lean
		dom_consts_nonneg	Dominance.lean
		dom_minmax_mono	Dominance.lean
		dom_K	Dominance.lean
		dom_g_GZ	Dominance.lean
		dom_Theta	Dominance.lean
		dom_Upsilon	Dominance.lean
		dom_mul_interval	Dominance.lean
		dom_rcirc	Dominance.lean
		dom_D0	Dominance.lean
		dom_num	Dominance.lean
		dom_sigma	Dominance.lean
		dom_lb	Dominance.lean
		dom_xi_max	Dominance.lean
		dom_xip_leaf	Dominance.lean
		dom_xip_range	Dominance.lean
		dom_xi_range	Dominance.lean
		dom_gram_det	Dominance.lean
		dom_gram_pos	Dominance.lean
		dom_kappa_nonneg	Dominance.lean
		dom_gamma_gap	Dominance.lean
Prop. I.72		satTerm_mono	Cap.lean
		dom_level	Dominance.lean
		falcon_of_item1_sub	Falcon.lean
		fx_terms_sub_level	LeafTail.lean
Lemma I.73		fxSigmaMin_pos	FxWidths.lean
		fx_leafsum_inputs	FxWidths.lean
Lemma I.75		fx_ref_slot_error	FixedCenter.lean
		lem_fx_ref_target_delta	FixedCenter.lean
		lem_fx_ref_target	FixedKey.lean
Lemma I.76		lem_fx_ref_center_errorC	FixedCenter.lean
Lemma I.77		dom_zbar	Dominance.lean
		lem_fx_output_norm_solve	Entries.lean
Lemma I.81		dom_root_shift	Dominance.lean
	3	lem_fx_output_norm_solve	Entries.lean
		lem_fx_ntt_target_deltaT	FixedCenter.lean
		lem_fx_ntt_target	FixedCenter.lean
	2	lem_fx_center_normC	FixedCenter.lean
		ntt_leaf_offset_le	FixedCenter.lean
Lemma I.83		zcoords_gaussInt	Integrality.lean
		zcoords_gaussInt_tower	Integrality.lean

Statement	Items	Theorems	File
Lemma I.84		leafProb_shift	Integrality.lean
	2	outputProb_shift_node	Integrality.lean
Prop. I.85		Qset_shift	Integrality.lean
Lemma I.86		lem_fx_ntt_target_shift	Integrality.lean
Def. J.1		InF	FprRound.lean
Def. J.5		wordVal	FprRound.lean
		fprVal	MachineWords.lean
Lemma J.6		InF_split	FprRound.lean
Lemma J.7		word_of_sig	FprRound.lean
Lemma J.8		nearest_mult	FprRound.lean
Lemma J.9		fpr_nearest_of_qr	FprRound.lean
		fpr_nearest_of_qd	FprRound.lean
Lemma J.10		fpr_nearest_of_real	FprRound.lean
Lemma J.11		cl_fpr_mul	FprRound.lean
		cl_fpr_mul_of_contract	FprRound.lean
		fpr_edge_mul_zero_of_contract	FprRound.lean
Lemma J.12		cl_fpr_add	FprRound.lean
		cl_fpr_add_of_contract	FprRound.lean
		fpr_edge_add_zero_of_contract	FprRound.lean
		fpr_edge_add_zero_y_of_contract	FprRound.lean
		fpr_edge_add_cancel_of_contract	FprRound.lean
		fpr_edge_add_far_of_contract	FprRound.lean
		fpr_edge_add_far_y_of_contract	FprRound.lean
Lemma J.13		cl_fpr_div	FprRound.lean
		cl_fpr_div_of_contract	FprRound.lean
Lemma J.14		cl_fpr_sqrt	FprRound.lean
		cl_fpr_sqrt_of_contract	FprRound.lean
Lemma J.15		cl_fpr_mul	FprRound.lean
		cl_fpr_mul_of_contract	FprRound.lean
		cl_fpr_add	FprRound.lean
		cl_fpr_add_of_contract	FprRound.lean
Lemma J.16	1	fpr_edge_mul_zero	FprRound.lean
	2	fpr_edge_add_zero	FprRound.lean
	3	fpr_edge_add_cancel	FprRound.lean
	4, 5	fpr_edge_add_far	FprRound.lean
		fpr_edge_mul_zero_of_contract	FprRound.lean
		fpr_edge_add_zero_of_contract	FprRound.lean
		fpr_edge_add_zero_y_of_contract	FprRound.lean
		fpr_edge_add_cancel_of_contract	FprRound.lean
		fpr_edge_add_far_of_contract	FprRound.lean
Lemma J.17		cl_fpr_sub	FprRound.lean
		cl_fpr_sub_of_contract	FprRound.lean
Lemma J.18		cl_fpr_div	FprRound.lean
		cl_fpr_div_of_contract	FprRound.lean
Lemma J.19		cl_fpr_sqrt	FprRound.lean

Statement	Items	Theorems	File
		cl_fpr_sqrt_of_contract	FprRound.lean
Lemma J.20		fpr_half_hcl_of_contract	FprExact.lean
		fpr_double_hcl_of_contract	FprExact.lean
		fpr_div2e_hcl_of_contract	FprExact.lean
		fpr_mul2e_hcl_of_contract	FprExact.lean
Lemma J.21		fpr_trunc_hcl_of_contract	FprExact.lean
		fpr_floor_hcl_of_contract	FprExact.lean
		fpr_rint_hcl_of_contract	FprExact.lean
Lemma J.22		fpr_of_hcl_of_contract	FprExact.lean
Lemma J.23	1	fpr_half_val	FprExact.lean
		wordVal_move	FprExact.lean
	2	fpr_double_val	FprExact.lean
	3	fpr_div2e_val	FprExact.lean
	4	fpr_mul2e_val	FprExact.lean
Lemma J.24		fpr_of_val	FprExact.lean
Lemma J.25	1	fpr_trunc_val	FprExact.lean
	2	fpr_floor_val	FprExact.lean
	3, 4	fpr_rint_val	FprExact.lean
Cor. J.27	3	lem_B_rel	Elementary.lean
Fact J.34		fact_val_mult	DefsFacts.lean
		fact_val_floor	DefsFacts.lean
		fact_val	DefsFacts.lean
Lemma J.35	1, 2	key_image_dev	KeyImage.lean
Lemma J.36		gram_pair_dev_rel	KeyImage.lean
Lemma J.37		lem_image_g00	KeyImage.lean
Lemma J.38		lem_image_g11	KeyImage.lean
Lemma J.39		lem_image_g01	KeyImage.lean
Def. J.40		Phi	Depth.lean
Def. J.41		PhiIter	Depth.lean
Cor. J.42		cor_recursion_fp_path_exact	Depth.lean
		cor_recursion_fp_path_either	Depth.lean
Cor. J.43		lem_image_g00	KeyImage.lean
Cor. J.44		lem_root_relI	Depth.lean
Cor. J.45		cor_dbar_fp	Tree.lean
Cor. J.46		fp_ref_slot_error	CenterBounds.lean
Lemma J.49		lem_budget_arg	Budget.lean
Lemma J.50		lem_budget_split_of_code	Budget.lean
Lemma J.51		lem_budget_rpos_off	Budget.lean
Lemma J.52		acc_row_bounds	MomentLeaves.lean
		acc_capped	MomentLeaves.lean
Lemma J.53		floors_capped_x	Floors.lean
Hyp. J.54		NormBounds	Bridge.lean
		epsPoisson_eq	Normalizer.lean
		normBounds_poisson	Normalizer.lean

Statement	Items	Theorems	File
		epsPoisson_anti	Normalizer.lean
		sLeast_le	Normalizer.lean
		normBounds_of_le	Normalizer.lean
		hyp_widths_leaf	Normalizer.lean
Def. J.55		capSet	Falcon.lean
Lemma J.56		floors_cap_si_le	Floors.lean
		floors_cap_Es	Floors.lean
	2	floors_cap_acc_range	Floors.lean
		floors_cap_rprime_le	Floors.lean
		floors_cap_rprime_nonneg	Floors.lean
		floors_cap_rrange	Floors.lean
		floors_cap_ccs	Floors.lean
Lemma J.57		floors_cap_word	Floors.lean
Lemma J.58		floors_cap_off	Floors.lean
		floors_cap_on	Floors.lean
		floors_cap_trial	Floors.lean
		floors_cap_accmin	Floors.lean
		floors_cap_total	Floors.lean
		floors_cap_Sw	FloorsSum.lean
Lemma J.59		floors_cap_half	Floors.lean
		floors_cap_ratio	Floors.lean
		floors_cap_PD	Floors.lean
		floors_cap_epsC	Floors.lean
		floors_cap_BD_split	Floors.lean
Lemma J.60		floors_cap_prob	Floors.lean
		floors_cap_mass_le	Floors.lean
Lemma J.65		quantile_mul_exp	Meas.lean
	1	meas_quantile_W	Meas.lean
	2	meas_quantile_delta	Meas.lean
Lemma J.67		lem_image_abs	KeyImage.lean
Lemma J.68		lem_root_relI	Depth.lean
		cor_recursion_fp_path_exact	Depth.lean
Lemma J.69		l10_error_mixed	Depth.lean
		cor_dbar_fp	Tree.lean
Lemma J.70		lem_fx_output_norm_solve	Entries.lean
Lemma J.72		acc_row_bounds	MomentLeaves.lean
		acc_capped	MomentLeaves.lean
Prop. J.73		falcon_of_item1	Falcon.lean
		prop_fp_loss	Falcon.lean
Prop. J.74		falcon_of_item1_sub	Falcon.lean
		meas_each_W	Meas.lean
		meas_each_delta	Meas.lean
	5	meas_tail_two	Meas.lean
		meas_level_sub	Meas.lean

Statement	Items	Theorems	File
Lemma K.1	1	`lem_chord`	`Chord.lean`
	2	`lem_chord_attained`	`Chord.lean`
Lemma K.2		`tight_le_prest`	`TightPrest.lean`
		`tight_le_prest_lt_two`	`TightPrest.lean`
		`tight_le_prest_all`	`TightPrest.lean`
Cor. K.3		`cor_chord_prest`	`Chord.lean`

The indexes of the routines and of the definitions. Table 49 lists every routine the report writes as an algorithm, with its code anchors and the statements whose text cites it; Table 50 lists every definition with the symbols it defines. Both are generated from the sections by `paper/gen_index.py` at every build.

Table 49: The routines: every algorithm, its code anchors and the statements that bound it.

Routine	Algorithm	Page	Code anchors	Statements
$\oplus$, $\ominus$, $\otimes$, the code's complex operations of Definition A.8	Algorithm 1	16	[L0: `sign_inner.h:327`] [L0: `fxp/sign_fxp.h:436-447`]	
split(f), the split butterflies of one level	Algorithm 2	19	[L0: `sign_fpoly.c:2258-2272`] [L0: `fxp/sign_fxpoly.c:168-193`]	Lemma B.3, Lemma G.16, Lemma I.10, Lemma I.49, Def. I.82, Lemma I.84
$\text{split}_{\text{sa}}(f)$, the split butterflies of one level for a self-adjoint f	Algorithm 3	19	[L0: `sign_fpoly.c:2351-2362`] [L0: `fxp/sign_fxpoly.c:195-215`]	Fact D.1, Fact D.2, Lemma G.26, Lemma G.28, Lemma G.29, Lemma G.30, Lemma G.32, Lemma G.37, Fact H.4, Lemma I.10, Lemma I.29, Lemma I.30, Lemma I.40, Lemma I.41, Lemma I.44
merge(f_0, f_1), the merge butterflies of one level	Algorithm 4	20	[L0: `sign_fpoly.c:2452-2463`] [L0: `fxp/sign_fxpoly.c:217-241`]	Lemma I.10, Lemma I.56, Def. I.82
$\text{LDL}^\dagger(\mathcal{G})$, the $LDL^\dagger$ step of one node	Algorithm 5	21	[L0: `sign_fpoly.c:2136-2149`] [L0: `fxp/sign_fxpoly.c:131-148`]	Def. 4.12, Prop. 5.8, Fact A.33, Fact D.2, Fact D.3, Lemma D.4, Lemma D.7, Lemma G.24, Lemma G.25, Lemma G.30, Lemma G.32, Cor. G.36, Prop. G.38, Lemma G.40, Lemma G.42, Cor. G.43, Lemma I.10, Lemma I.11, Lemma I.30, Lemma I.39, Lemma I.41, Lemma I.44, Lemma I.48, Cor. I.57, Cor. J.43, Cor. J.44

Routine	Algorithm	Page	Code anchors	Statements
ffsamp$(t, \mathcal{G}, \texttt{root})$, the code's recursion: the $LDL^\dagger$ step of a node when the recursion reaches it, no tree stored	Algorithm 6	24	[L0: `sign_sampler.c:1245-1350`] [L0: `fxp/sign_fxsampler.c:287-329`]	Def. 4.5, Lemma 4.7, Lemma 4.9, Def. 4.12, Prop. 5.9, Cor. 5.10, Def. A.23, Def. A.25, Fact D.1, Fact D.2, Lemma D.11, Fact G.5, Fact G.12, Lemma G.20, Lemma G.51, Lemma G.52, Lemma G.53, Lemma G.54, Lemma G.55, Lemma G.56, Lemma G.57, Lemma G.58, Thm. G.59, Lemma G.60, Cor. G.62, Fact H.4, Lemma H.23, Lemma I.10, Lemma I.11, Def. I.20, Lemma I.26, Lemma I.27, Lemma I.39, Lemma I.42, Lemma I.49, Thm. I.54, Lemma I.56, Cor. I.57, Prop. I.72, Lemma I.77, Lemma I.81, Lemma J.30, Hyp. J.31, Hyp. J.48
deepest$(t, l_{10}, d_{00}, d_{11})$, the recursion's deepest level	Algorithm 7	25	[L0: `sign_sampler.c:1185-1234`] [L0: `fxp/sign_fxsampler.c:228-269`]	Def. A.23, Def. A.25, Lemma D.11, Fact G.5, Lemma G.51, Lemma G.53, Lemma G.54, Lemma G.55, Lemma G.56, Lemma G.57, Lemma G.58, Thm. G.59, Lemma G.60, Cor. G.62, Lemma I.10, Lemma I.11, Lemma I.42, Lemma I.49, Lemma I.50, Lemma I.51, Lemma I.52, Thm. I.54, Lemma I.56, Lemma J.30, Hyp. J.48

Routine	Algorithm	Page	Code anchors	Statements
SamplerZ(μ, `isigma`), the base sampler `sampler_next`	Algorithm 8	26	[L0: `sign_sampler.c:916-968`] [L0: `fxp/sign_fxsampler.c:183-216`] [L0: `sign_sampler.c:89-108`]	Def. 4.5, Def. A.24, Def. A.25, Def. A.28, Lemma G.63, Lemma G.64, Fact G.66, Lemma G.67, Lemma G.68, Lemma G.71, Lemma G.72, Lemma G.73, Lemma G.80, Lemma H.24, Lemma H.26, Lemma I.10, Lemma I.11, Def. I.20, Hyp. I.21, Lemma I.50, Lemma I.51, Lemma I.52, Thm. I.54, Lemma I.56, Lemma I.58, Lemma I.60, Lemma I.61, Lemma I.64, Def. J.28, Hyp. J.31, Hyp. J.47, Hyp. J.48, Lemma J.49, Lemma J.51, Lemma J.52, Lemma J.53, Def. J.55, Lemma J.56, Lemma J.58, Lemma J.60, Hyp. J.64, Def. J.66, Lemma J.71, Lemma J.72
BerExp(x, ccs), the acceptance `ber_exp` with `expm_p63`	Algorithm 9	27	[L0: `sign_sampler.c:780-912`] [L0: `fxp/sign_fxsampler.c:88-181`]	Def. 4.5, Def. A.24, Fact G.66, Lemma G.72, Lemma G.73, Lemma G.80, Lemma H.25, Lemma H.26, Def. I.20, Hyp. I.21, Lemma I.52, Thm. I.54, Lemma I.59, Lemma I.60, Lemma I.61, Def. I.62, Lemma I.64, Lemma I.71, Hyp. J.48, Lemma J.50, Lemma J.58, Hyp. J.75
ffSampling$^{\mathcal{F}}(B, s, t)$, the signer's sampler	Algorithm 10	28	[L0: `sign_core.c:130-204`] [L0: `fxp/sign_fxcore.c:158-216`] [L0: `sign_fpoly.c:2663-2712`] [L0: `fxp/sign_fxcore.c:198`]	Def. 4.5, Lemma 4.9, Prop. 5.9, Cor. 5.10, Def. A.5, Def. A.13, Def. A.25, Fact A.33, Lemma H.22, Lemma H.23, Lemma I.10, Def. I.20, Hyp. I.21, Lemma I.25, Lemma I.27, Lemma I.35, Lemma I.39, Lemma I.47, Lemma I.53, Thm. I.54, Lemma I.56, Prop. I.72, Def. I.74, Lemma I.75, Lemma I.76, Lemma I.77, Lemma I.81, Lemma I.86, Hyp. J.31, Lemma J.35, Lemma J.37, Lemma J.38, Lemma J.39, Cor. J.46, Lemma J.70

Routine	Algorithm	Page	Code anchors	Statements
keygeneration(seed, c), the reference's key generation under the four checks of [L2: BFLP26, Alg. 2] and the three tail checks at the center c	Algorithm 11	29	[L0: `fxp/kgen_fx.c:113-212`]	Def. 4.5, Def. 5.5, Def. 5.6, Def. A.5, Def. A.13, Def. A.25, Def. A.35, Lemma H.13, Lemma H.15, Lemma H.16, Lemma H.17, Lemma I.36, Lemma I.37, Lemma I.38, Lemma I.39, Lemma I.46, Lemma I.47
keychecks(f, g, F, G), the four coefficient checks of [L2: BFLP26, Alg. 2] on a key	Algorithm 12	30	[L0: `fxp/kgen_fx.c:60-94`] [L0: `fxp/kgen_fx.c:186-202`]	Def. 4.5, Def. 5.5, Prop. 5.8, Lemma H.17, Lemma H.18, Lemma H.19, Lemma H.21, Hyp. I.22, Lemma I.25, Lemma I.27, Lemma I.35, Lemma I.36, Lemma I.37, Lemma I.38
Gram(B), the Gram matrix in FFT form	Algorithm 13	215	[L0: `sign_fpoly.c:2625-2652`] [L0: `fxp/sign_fxpoly.c:243-275`]	Def. 4.5, Def. 4.6, Def. 5.5, Lemma G.22, Lemma G.23, Lemma H.14, Lemma H.15, Lemma H.16, Lemma I.10, Lemma I.25, Lemma I.27, Lemma I.35
FFT(f), the coefficients to $(f(\psi_k))_{k<n/2}$	Algorithm 14	371	[L0: `sign_fpoly.c:1242-1267`] [L0: `fxp/sign_fxpoly.c:11-40`]	Def. 5.5, Prop. 5.8, Lemma H.8, Lemma H.9, Lemma H.10, Lemma H.11, Lemma H.12, Lemma H.15, Lemma H.16, Lemma H.18, Lemma H.19, Lemma H.21, Lemma H.22, Lemma I.10, Def. I.16, Lemma I.25, Lemma I.27, Lemma I.34, Lemma I.55, Def. I.74, Lemma I.75, Lemma I.76, Lemma I.77, Cor. I.78, Cor. I.79, Lemma I.81, Lemma I.86, Cor. I.87, Cor. I.88, Lemma J.35, Lemma J.37, Lemma J.38, Lemma J.39, Cor. J.46
tailcheck(f, g, F, G, c), the three tail checks of a key at one center	Algorithm 15	442	[L0: `fxp/kgen_fx.c:516-618`] [L0: `fxp/kgen_fx.c:1690-1785`]	Def. 5.6, Def. I.15, Def. I.16, Def. I.17, Def. I.18, Def. I.19, Hyp. I.91
tailbounds(c), the upper bounds $\mu^{\uparrow}$ and $B^{\uparrow}$ of the tail checks at one center	Algorithm 16	443	[L0: `fxp/kgen_fx.c:1748-1778`]	Def. 5.6, Def. I.14, Def. I.17, Def. I.18, Def. I.19, Hyp. I.91
$\mathrm{center}_{\mathrm{frac}}(\mathsf{h}(\mathsf{m}), f, F)$, the center split over the integers [L2: BFLP26, Alg. 7]	Algorithm 17	622	[L0: `fxp/sign_fxcore.c:60-81`] [L0: `fxp/sign_fxpoly.c:292-304`]	Prop. 5.9, Cor. 5.10, Def. A.13, Lemma I.10, Fact I.45, Lemma I.46, Prop. I.72, Lemma I.81, Lemma I.86

Routine	Algorithm	Page	Code anchors	Statements
ν_2: a lower bound on ν_2, one rule per operation	Algorithm 18	689		Def. J.33
ν_2-walk: ν_2 along a straight-line program over $\mathcal{F}$	Algorithm 19	689		Hyp. J.31, Def. J.33

Table 50: The defined symbols by definition.

Definition	Title	Page	Symbols
Definition 4.5	A Falcon-type signer	40	
Definition 4.6	The key constants	40	T, κ_{root}, κ_k, $\|A\|$, Ξ'_k, Ξ_k, Ξ'_{root}, h, Ξ', Ξ, ℓ, $\bar{g}_2$, $\bar{g}_0$, $\hat{K}$
Definition 4.12	The three quantities of a key at a center	47	q, N, $\mathcal{L}$, T', $\widetilde{\mathcal{L}}$, K, B, δB, D_L, D_R, t_{leaf}, $\widetilde{t}_{\mathrm{leaf}}$, $\widetilde{c}$, (t,T), Δ, e, r, $\widetilde{\sigma}_i$, S_{τ_K}, τ, $\bar{\delta}_K$, μ_{key}, $\bar{B}_K$
Definition 5.1	The adversary's event A_{adv}	49	A_{adv}
Definition 5.2	The fringe leaves' term Π_C	50	$\Pi_C(y)$
Definition 5.3	The loss	50	S, $\mathcal{K}(z)$, S'_k, β, y
Definition 5.5	A checked key	52	$(\gamma_{fg},\gamma_{\mathrm{hyb}},\gamma_{FG},\gamma_{\mathrm{root}})$, B_{fg}, q, Ψ_n, m, $\forall z \in \mathbb{C}:\ z_r,\ z_i$, $\forall p \in \{f,g,F,G\}:\ \hat{p}$, $\forall p \in \{f,g,F,G\}:\ \widetilde{p}$, (g_{00},g_{01},g_{11}), $(\widetilde{g}_{00},\widetilde{g}_{01},\widetilde{g}_{11})$, sq_{fg}, sq_{hyb}, sq_{FG}, sq_{root}, $\widetilde{sq}_{fg}$, $\widetilde{sq}_{\mathrm{hyb}}$, $\widetilde{sq}_{FG}$, $\widetilde{sq}_{\mathrm{root}}$
Definition 5.6	A key passing the tail checks at c	53	q, υ, $\forall x \in \mathbb{R}:\ \lceil x \rceil_\upsilon$, N, M_n, D_n, B_n, t_c, S_{τ_K}, τ, $\bar{\delta}_K$, μ_{key}, $\bar{B}_K$, $\delta^{\uparrow}$, $\mu^{\uparrow}$, $B^{\uparrow}$
Definition A.1	The integers' ranges, the ring of real polynomials and its FFT form	69	$\mathbb{Z}_{>0}$, $\mathbb{Z}_{\geq 0}$, $\mathcal{R}_m$, $\|f\|$, ψ, ψ_k
Definition H.1	Induced form	361	$\mathrm{split}(a)$, a_0, a_1, $Q_d(x)$, $Q_{T'}(x)$, $Q_{T'}(f)$
Definition I.1	The fixed-point realization	413	$\mathcal{F}_{\mathrm{fx}}$, ζ_{op}, ζ, u, $\forall v \in \mathbb{R}:\ \mathrm{roundAway}(v)$, $\forall v \in \mathbb{Z}\ \forall d > 0:\ \mathrm{roundAway}(v,d)$, $\forall v \in \mathbb{R}:\ \mathrm{roundEven}(v)$, $\forall k < 1024:\ \mathrm{rev}_{10}(k)$, $\forall k < 1024:\ \psi_k$, (u,ζ), $\texttt{fxp_inv}(x)$, $\mathrm{fl}(-x)$, $\forall \mathfrak{p} \in \{\mathrm{Re},\mathrm{Im}\}\ \forall k < 1024:\ \mathfrak{p}(\widetilde{\psi}_k)$
Definition J.1	The emulated `fpr`	652	$\mathcal{F}$, u, ζ
Definition A.2	The Gaussian function and the discrete Gaussian	69	$\|x\|$, $\rho_{s,c}(x)$, ρ_s, $\rho_{s,c}(A)$, $D_{A,s,c}(x)$, $D_{\mathbb{Z},s,c}$, k, A
Definition A.3	The Rényi divergence and the expectations	69	$\mathrm{Supp}(\mu)$, $R_\alpha(\mu \,\|\, \nu)$, $\mathbb{E}_\mu[f]$, $\mu(A \,|\, E)$, $\mathbb{E}_\mu[f \,|\, E]$
Definition A.4	The model	70	$\mathbb{C}$, (δ,η), λu, ζ
Definition A.5	The fixed-point representation	71	$v \ll e$, $v \gg e$, $v \gg_{\mathrm{a}} e$, $\mathrm{u}_w(v)$, $v \,\&\, 1$, a_{fx64}, $\mathcal{V}_{\mathrm{fx}}$, W
Definition J.5	The value of a word	655	s_W, e_W, m_W, $\mathrm{val}(s,e,M)$, $\mathrm{val}(W)$
Definition G.6	Node factor, tree map, coordinates and matrices [to table]	192	$m \geq 4:\ \mathrm{split}(a)$, a_0, a_1, L_ν, xL_ν, $x \in \mathcal{R}_2:\ x\mathcal{L}_d$, $x \in \mathcal{R}_2^2:\ x\mathcal{L}_\nu$, $x\mathcal{L}_\nu$, $\forall v \leq n:\ (x\mathcal{L}_T)_{2v-1}$, $\forall v \leq n:\ (x\mathcal{L}_T)_{2v}$, a, ℓ_i, q_i, p_i, $\forall x = (x_0,x_1) \in \mathcal{R}_{m'}^2:\ x_i$, $I(d) = \{j, j+1\}$ $\forall x \in \mathcal{R}_2:\ x_j$, x_{j+1}, $e^{(j)}$, $i \in I(T'):\ (\mathcal{L}_{T'})_{ji}$, D
Definition A.8	The complex layer	72	$C_{\mathcal{F}}$, $a \oplus b$, $a \ominus b$, $a \otimes b$, $c \otimes a$, $a \otimes c$, $\mathrm{conj}\, a$
Definition A.9	Sign convention	73	$x^{\pm}$
Definition G.9	Samples, leaf product and output measures [to table]	196	(σ_i,c_i), z, $z_{T'}$, $\varrho_{T'}(t_{T'},z_{T'})$, $Q_{T',t'}(A)$, $t_{T'}$
Definition A.10	Relation on approximation	73	
Definition A.11	Relation on the bound of the difference	73	
Definition A.12	The basis of a key, its lattice and its Gram matrix	74	$\mathcal{R}_n$, B, $\Lambda(B)$, $D_{\Lambda(B),s,c}$, k, A, $\psi^n = -1:\ \mathcal{G}(\psi)$

Definition	Title	Page	Symbols
Definition A.13	The center of a hashed message and its parts	74	q, $\mathcal{R}_n$, B, t, (t_0, t_1), qt, t_{int}, t_{frac}
Definition I.13	The arithmetic of the tail checks	439	υ, $\mathcal{W}$, $\forall x \in \mathbb{R}:\ \lfloor x \rfloor_\upsilon$, $\forall x \in \mathbb{R}:\ \lceil x \rceil_\upsilon$, $\mathcal{J}$, $\mathcal{J}_{\mathrm{c}}$, ζ_{op}, $-2^{63} \le i < 2^{63}:\ \mathtt{fxw_of_int}(i)$, $-2^{63} \le x < 2^{63}:\ \mathtt{fxw_of_fxp}(W_x)$, $\forall x \in \mathcal{W}:\ \mathtt{fxi_point}(x)$, $b + d \in \mathcal{W}:\ \mathtt{fxi_add}([a,b],[c,d])$, $b - c \in \mathcal{W}:\ \mathtt{fxi_sub}([a,b],[c,d])$, $-a \in \mathcal{W}:\ \mathtt{fxi_neg}([a,b])$, $b + \upsilon \in \mathcal{W}:\ \mathtt{fxi_half}([a,b])$, $\mathtt{fxi_mul}([a,b],[c,d])$, $\mathtt{fxi_sqr}([a,b])$, $\lvert b \rvert < 2^{158} c:\ \mathtt{fxi_div}([a,b],[c,d])$, $c > 0:\ \mathtt{fxi_inv}([c,d])$, $a \ge 0:\ \mathtt{fxi_sqrt}([a,b])$, $\max_{x \in x_r \cup x_i} \lvert x \rvert \max_{y \in y_r \cup y_i} \lvert y \rvert < 2^{157}:\ \mathtt{xcmul}(x_r, x_i, y_r, y_i)$, $\lvert b \rvert < 2^{158}:\ \mathtt{fxi_mag}([a,b])$, $y < 2^{31}:\ \mathtt{fxw_mulu}(x,y)$, $x + \upsilon \in \mathcal{W}:\ \mathtt{fxw_halfu}(x)$, $\mathtt{FXW_U65}$, $[a,b] \in \mathcal{J}_{\mathrm{c}}:\ \mathtt{fxc_of_fxi}([a,b])$, $[\ell', \ell' + w'\upsilon] \in \mathcal{J}_{\mathrm{c}}:\ \mathtt{fxc_add}([\ell, \ell + w\upsilon], [\ell', \ell' + w'\upsilon])$, $\mathtt{fxc_sub}([\ell, \ell + w\upsilon], [\ell', \ell' + w'\upsilon])$, $\forall [\ell, \ell + w\upsilon] \in \mathcal{J}_{\mathrm{c}}:\ \mathtt{fxc_half}([\ell, \ell + w\upsilon])$, $\forall [\ell, \ell + w\upsilon] \in \mathcal{J}_{\mathrm{c}}\ \forall W \in \mathcal{F}_{\mathrm{fx}}:\ \mathtt{fxc_mulw}([\ell, \ell + w\upsilon], W)$, $[\ell', \ell' + w'\upsilon] \in \mathcal{J}_{\mathrm{c}}:\ \mathtt{fxc_mult}([\ell, \ell + w\upsilon], [\ell', \ell' + w'\upsilon])$, $\forall [\ell, \ell + w\upsilon] \in \mathcal{J}_{\mathrm{c}}:\ \mathtt{fxc_mag}([\ell, \ell + w\upsilon])$, e, w
Definition A.14	The Gram matrices Gram_m	74	$\mathcal{G}$, Gram_m
Definition I.14	The tail checks' stored words	443	υ, $\forall x \in \mathbb{R}:\ \lfloor x \rfloor_\upsilon$, $\forall x \in \mathbb{R}:\ \lceil x \rceil_\upsilon$, $\mathcal{W}$, $\mathcal{J}$, q, N, N_{m}, h_c, M_n, D_n, B_n, τ_K, $\tau_K^{\uparrow}$, $(1/s)^{\mathcal{J}}$
Definition A.15	The split and the merge	75	a_0, a_1, $V_m(a)$, $M_m(a)$, $\mathrm{split}(a)$, $\mathrm{merge}(f_0, f_1)$, $b\rangle$, $(g_0, g_1)\rangle$
Definition I.15	The interval twiddles	444	$y \in \mathcal{J}:\ (x,y)_r$, $(x,y)_i$, $\forall z \in \mathbb{C}:\ z_r$, z_i, $\forall m \ge 1\ \forall a \in (\mathcal{J}^2)^m \cup \mathbb{C}^m\ \forall k < m:\ a_{k,r}$, $a_{k,i}$, $\forall k < 1024:\ \mathrm{rev}_{10}(k)$, $\forall j \in \{1, \ldots, 1023\}:\ \mathrm{low}(j)$, $\mathtt{bc}_1$, $\mathtt{bs}_1$, $\forall m \in \{1, \ldots, 9\}:\ \mathtt{bc}_{m+1}$, $\forall m \in \{1, \ldots, 9\}:\ \mathtt{bs}_{m+1}$, Ψ_0, $\forall j \in \{1, \ldots, 1023\}:\ \Psi_{\mathrm{rev}_{10}(j)}$
Definition I.16	The key's images and tree over the intervals	445	j_2, (z_r, z_i), $\Lambda_\ell^{\mathcal{J}}(a)_{j_1}$, $\Lambda_\ell^{\mathcal{J}}(a)_{j_2}$, $\forall p \in \{f, g, F, G\}:\ \hat{p}^{\mathcal{J}}$, $\forall k < n/2:\ \mathtt{xg}_k$, $\forall k < n/2:\ \mathtt{xf}_k$, $\forall k < n/2:\ g_{01,k}^{\mathcal{J}}$, υ, $\mathtt{xu}_j$, (L'', D''), $\mathtt{xtree}(a,b,d)$, $((l_{10,\nu}^{\mathcal{J}})_\nu, (d_i^{\mathcal{J}})_{i \le N})$, ℓ
Definition A.17	The $LDL^\dagger$ step	75	$\mathcal{G}$, $\psi^m = -1:\ l_{10}(\psi)$, d_{00}, $\psi^m = -1:\ d_{11}(\psi)$, $\mathrm{LDL}^\dagger(\mathcal{G})$
Definition I.17	The leaf words and the message bound	446	$((\widetilde{l}_{10,\nu})_\nu, (\mathtt{isigma}_i)_{i \le N})$, $\forall i \le N:\ \Sigma_i$, $w:\ \pi_1(u,v,w)$, $b_i \ge 0:\ \mathtt{msb_cmul}(a_r, a_i, b_r, b_i)$, $\forall C \in \mathcal{F}_{\mathrm{fx}}\ \forall a \in \mathcal{W}^n\ \forall k < n:\ \mathtt{msb_const}(a, C)_k$, j_2, (y_r, y_i), $\Lambda_\ell^{\uparrow}(a)_{j_1}$, $\Lambda_\ell^{\uparrow}(a)_{j_2}$, $\Lambda_\ell^{\uparrow}(a)_{j_1+n/2}$, $\Lambda_\ell^{\uparrow}(a)_{j_2+n/2}$, $\mathtt{msb_fft}$, $\mathtt{ti}_j$, $(\mathtt{ur}_j, \mathtt{ui}_j)$, a_j^0, $a_{j+h/2}^0$, a_j^1, $a_{j+h/2}^1$, $\mathtt{msb_split}(a)$, $\mathtt{msb_merge}(a^0, a^1)_{2j}$, $\mathtt{msb_merge}(a^0, a^1)_{2j+1}$, $\mathtt{msb_merge}(a^0, a^1)_{2j+h}$, $\mathtt{msb_merge}(a^0, a^1)_{2j+1+h}$, (M', y^0, y^1), z, $(\mathtt{pr}_k, \mathtt{pi}_k)$, b_k^0, $b_{k+2^{\ell-1}}^0$, (M'', w^0, w^1), $\mathtt{msb_rec}(a^0, a^1, \lambda)$, $\mathtt{a}_0$, $\mathtt{a}_1$, $(m_i^{\uparrow})_{i \le N}$
Definition A.18	Tree, subtrees and depth	76	h, $L(\nu)$, $R(\nu)$, $\forall d \in \mathbb{R}:\ \mathrm{Sub}(d)$, $\mathrm{Sub}(\nu)$, $\forall d \in \mathrm{Sub}(T) \cap \mathbb{R}:\ \mathrm{depth}(d)$, $\forall T' \in \mathrm{Sub}(T) \cap \mathcal{T}_{m'}:\ \mathrm{depth}(T')$
Definition I.18	The remainder's matrices	448	$K_{i,j+k}^{\mathcal{J}}$, $R_{i,j+k}^{\mathrm{m}}$, $R_{i,j+k}^{\mathrm{z}}$, $\forall i \le N:\ \mathtt{a_r}_i$, $\forall i \le N:\ \mathtt{b_r}_i$

Definition	Title	Page	Symbols
Definition A.19	Sample positions and leaf diagonals	77	N, $I(T)$, $I(R(\nu))$, $I(L(\nu))$, d_i, d_v
Definition I.19	The tail checks	448	$\delta^{\uparrow}$, $\mu^{\uparrow}$, $\forall i \le N:$ $\mathtt{b_rem}_i$, $B^{\uparrow}$, ok_δ, ok_μ, ok_B
Definition A.20	The ffLDL† tree of a Gram matrix	78	split(a), a_0, a_1, (l_{10}, d_{00}, d_{11}), ffLDL$^\dagger(\mathcal{G})$, $\mathcal{G}_{d_{00}}$, (d_0, d_1), $\mathcal{G}_{d_{11}}$, (d_0', d_1'), T_{00}, T_{11}
Definition I.20	The fixed-point signer's sampling	450	ζ_{op}, σ_0, $\widetilde{c}$, $si(x) \ge 64:$ z_{acc}
Definition A.21	The sampler ffSampling on a tree and its output measure	79	N, split(a), a_0, a_1, merge(f_0, f_1), $D_{\mathbb{Z},\sigma,c}(z)$, leaf$(d, t_d)$, ffSampling$(t_\nu, \nu)$, z, $Q_{T,t}(A)$, (σ_j, σ_{j+1}), (c_j, c_{j+1}), $\hat{z}_d$, t_T, (t_0, t_1), $t_{T_{11}}$, $\hat{z}_{T_{11}}$, tb_0, $t_{T_{00}}$, $\hat{z}_{T_{00}}$, $\hat{z}_\nu$, z_1, z_0
Definition A.23	The sampler ffsamp on a Gram matrix and its output measure	81	N, LDL$^\dagger(\mathcal{G})$, d_{00}, $l_{10}(\psi)$, $d_{11}(\psi)$, split(a), a_0, a_1, merge(f_0, f_1), $\mathcal{G}_d$, (d_0, d_1), $D_{\mathbb{Z},\sigma,c}(z)$, leaf$_s(d, c)$, (l_{10}, d_{00}, d_{11}), $\mathtt{INV_SIGMA}$, y_1, y_0, ffsamp$(t', \mathcal{G}')$, z, $Q'_{\mathcal{G},t}(A)$
Definition A.24	The base sampler's probability measure on $\mathbb{Z}$ in a realization	83	σ, $B^{\mathcal{F}}_{\sigma,c}(A)$, μ, σ'
Definition A.25	The two probability measures	83	N, s, B, Λ, $D_{\Lambda,s,tB}$, c, t_{frac}, ffSampling$^{\mathcal{F}}$, t, ffSampling$^{\mathbb{R}}$, $P(A)$, $Q(A)$, $z_{<i}$, SamplerZ$(\mu, \mathtt{isigma})$, $\widetilde{t}_i$, $\widetilde{\sigma}_i$
Definition A.26	The tail-cut event and its subevents	84	S, S^c, $\mathcal{K}(z)$, $\forall k \le N:$ S_k, $\forall A \subseteq \mathbb{Z}^N:$ $P_S(A)$, $Q_S(A)$, S', S'^c, $\forall i \le N:$ $S'_{<i}$, $S_{<i}$, $\forall k \le N:$ S'_k, $P_{S'_0}(A)$, $Q_{S'_0}(A)$
Definition A.27	The leaf perturbations of one signature	85	$\Delta_i(z_{<i})$, $\bar{W}_{S'}$, $\bar{W}_S$, S'
Definition A.28	A leaf's computed and ideal probability measures on $\mathcal{Z}_i$	85	$D_{\mathbb{Z},\sigma,c}(z)$, $B^{\mathcal{F}}_{\sigma,c}(A)$, $\widetilde{B}_i$, $\widetilde{D}_i$, $P_D(z)$, $\mathcal{Z}_i$, $R^{\mathcal{Y}}_a(\mu \,\|\, \nu)$, $\bar{\rho}_B$, $\sup \emptyset$, $\bar{U}$, $\bar{p}_C$, κ_C
Definition I.28	The node map at $u = 0$	458	c_{sa}, k_{sa}, u, $\forall x \ge 0:$ $k_{zo}(x)$, $\lvert g_{01}\rvert$, m_1, u_0, M_1, M_2, r', $\mathcal{Q}_0$, $\mathcal{U}^0_\kappa(\chi)$
Definition J.28	The stored sampling constants of `c-fn-dsa`	686	
Definition A.29	The normalizer ratio at a leaf	86	$\rho_{s,c}(\mathbb{Z})$, $d(s, c)$, $\theta_{\alpha_L}(\delta)$, s''_i, m_i, $\Phi_{\alpha_L,i}$
Definition A.30	The divergence factor R	86	$\theta_{\alpha_L}(\delta)$, R_B, R_σ, R_t, R
Definition A.32	Gram form and the nodes' Gram matrices	87	ψ_k, $Q_{\mathcal{G}}(x)$, T, $\mathcal{G}_T$, $\mathcal{G}_{T_{00}}$, $\mathcal{G}_{T_{11}}$
Definition I.32	The chain of the leaf diagonals at $u = 0$	462	$\mathcal{A}$, $\forall k \in \{1, \ldots, h-1\}:$ ϑ_{k-1}, $\forall k \in \{1, \ldots, h-1\}:$ $\hat{\kappa}_k$, $\forall k \in \{1, \ldots, h-1\}:$ χ_k
Definition J.32	The 2-adic valuation	688	$\nu_2(w)$
Definition J.33	The valuation walk $\underline{\nu_2}$	688	$\underline{\nu_2}$
Definition A.35	The rounded thresholds of the key checks	88	$(\gamma_{fg}, \gamma_{\mathrm{hyb}}, \gamma_{FG}, \gamma_{\mathrm{root}})$, q, $\check{\gamma}_{fg}$, $\check{\gamma}_{FG}$, $\check{\gamma}_{\mathrm{hyb}}$, $\check{\gamma}_{\mathrm{root}}$
Definition A.36	The Gram deltas of a checked key	88	$\check{\gamma}_{fg}$, $\check{\gamma}_{FG}$, R_{h-1}, A_0, A_{j+1}, k_H, k'_H, δ_{fg}, δ_{FG}, γ'_{fg}, γ'_{FG}, E_{00}, E_{11}, E_{01}
Definition A.37	The perturbation bounds of a checked key	89	$\check{\gamma}_{\mathrm{hyb}}$, γ'_{FG}, E_{00}, m_0, M_0, d_{lo}, d_{hi}, $\bar{\varsigma}$, $\bar{g}_{11}$
Definition A.38	The series of the normalizer deviation	89	$\varepsilon_j(s)$
Definition A.39	The normalizer ratio, its differences and the remainder form	90	s_1, s_2, c, $\theta_\alpha(\delta)$, s'', m, $d(s, c)$, $\varepsilon_j(s)$, $\Phi(s, \delta, c', \Delta)$, v_1, v'', s_-, s_+, $Q(v)$
Definition A.40	The uniform bound $\bar{\phi}_{\mathrm{u}}$	90	$\theta_\alpha(\delta)$, r_-, r_+, $\underline{s}$, $\overline{s}$, $\varepsilon_j(s)$, ε°_j, $g(\delta)$, a_s, a_c, b_s, b_c, $\bar{Q}(x, y)$, $\bar{\phi}_{\mathrm{u}}$
Definition J.40	The node map at $\zeta = 0$	697	$\zeta = 0$
Definition J.41	The chain of the leaf diagonals' bounds at $\zeta = 0$	697	$\zeta = 0$
Definition A.46	The arithmetic and harmonic means, their compositions	97	AM(a, b), HM(a, b), AM$_{\mathrm{all}}$, HM$_{\mathrm{all}}$, $\forall k \ge 1:$ $\mathcal{C}_k$
Definition J.55	The fringe set of a leaf	714	$\sigma_{\max}$, r, $\mathcal{Z}$, C, $\bar{U}(\tau)$, $\bar{p}_C(\tau)$

Definition	Title	Page	Symbols
Definition I.62	The fixed-point signer's terms	556	h, ζ_{op}, (λ, α), $\bar{\kappa}_{\mathrm{root}}$, $\forall 1 \le k \le h-1:\ \bar{\kappa}_k$, $\bar{\Xi}'$, $\bar{\Xi}'_{\mathrm{root}}$, $\bar{\Xi}$, $\bar{\ell}$, $\bar{K}_n^{\mathrm{fx}}$, E_x, E_s, e_{poly}, e_+, $\forall k \le 18:$ $E_{x,k}$, $\forall k \le 18:\ e_{+,k}$, e_{ccs}, e_{00}, $\bar{G}$, Z_I, χ_{root}, $\forall 1 \le k \le h-1:\ \vartheta_{k-1}$, $\forall 1 \le k \le h-1:\ \hat{\kappa}_k$, κ_k, χ_0, $\forall 1 \le k \le h-1:\ \chi_k$, χ_{leaf}, s, c_n, $\sigma_{\max}$, χ_σ, $\sqrt{\widetilde{d}_{11}}$, χ_σ^ζ, $s_{\min}$, $\bar{\delta}$, $s_\star$, ϵ, $\underline{s}$, ε_0°, u_0, χ, $\bar{\delta}_\mu$, c_{sa}, k_{sa}, M_2, $\bar{e}_0$, $\bar{a}_1$, E_l^{child}, E_l^{root}, ℓ, κ_{root}, E_l, $\widetilde{\ell}$, c_{split}, c_{merge}, $\forall 1 \le k \le h:\ M_k$, G_X, G_R, G_γ, G_Z, K_ζ, $\forall 1 \le k \le h:\ \Theta_k$, $\forall 1 \le k \le h:\ \Upsilon_k$, R°, Ξ, c_S, γ, γ_S, D_0°, D_Z°, D°, D_S, W°
Definition J.66	The floating-point signer's terms	729	C_i, $\bar{\delta}$, $\bar{e}$, $\bar{\sigma}$, Z
Definition I.74	The root node's entry bound at the center t	607	n, ζ_{op}, c_{merge}, k_E, u, R_{h-1}, A_0, $\forall j < h-1:$ A_{j+1}, $\delta_{\mathsf{h(m)}}$, $e_p(\gamma', \delta)$, $e_t(\gamma', \delta)$
Definition I.82	The shift of the output measure at a subtree	628	n, $\forall a \in \mathbb{Z}^{I(T_{11})}:\ A(a)$, $\mu_{T'}(a)$, $\mu_d(y)$, $t'_{T_{11}}$, $\forall a \in \mathbb{Z}^{I(T_{11})}:\ t'_{T_{00}}(a)$, $\forall t'' \in \mathcal{R}_{m'} \times \mathcal{R}_{m'}$ $\forall B \subseteq \mathbb{Z}^{I(T')}:\ Q_{T',t''}(B)$, $t_{T'}$

The fixed-point signer's routines. Table 51 names the fixed-point signer's routines by their code names, with the operations each performs per ψ.

Object	Routine	Algorithm	`fxp/`	Operations per ψ
B in FFT form	`basis_to_FFT`	FFT, line 2 of ffSampling$^{\mathcal{F}}$	[L0: `fxp/sign_fxcore.c:24-42`]	$(h-1)$ levels of Lemma G.18
$\mathcal{G} = BB^\dagger$	`fxpoly_gram_fft`	Gram	[L0: `fxp/sign_fxpoly.c:243-275`]	$\lvert b\rvert^2$, $b \operatorname{conj} b'$, $\oplus$
$LDL^\dagger$ of one node	`fxpoly_LDL_fft`	$\mathrm{LDL}^\dagger$	[L0: `fxp/sign_fxpoly.c:131-148`]	$2/$, $2\times$, $+$, $-$
$d \to (d_0, d_1)$	`fxpoly_split_selfadj_fft`	$\mathrm{split}_{\mathrm{sa}}$	[L0: `fxp/sign_fxpoly.c:195-215`]	Lemma B.3, real
$t \to (t_0, t_1)$	`fxpoly_split_fft`	split	[L0: `fxp/sign_fxpoly.c:168-193`]	Lemma B.3
$(z_0, z_1) \to z$	`fxpoly_merge_fft`	merge	[L0: `fxp/sign_fxpoly.c:217-241`]	Lemma G.18
$t_0 + (t_1 - z_1)\, l_{10}$	`fxpoly_mul_fft` and adds	ffsamp, line 26	[L0: `fxp/sign_fxsampler.c:313-317`]	$\otimes$ (Lemma B.2, item 5), $\oplus$, $\ominus$
Leaf (t_i, σ_i)	`fxp_ffsamp_fft_deepest`	deepest, lines 1 to 18	[L0: `fxp/sign_fxsampler.c:228-269`]	$\sqrt{d} \cdot$ `INV_SIGMA`
Base sampler	`fxp_sampler_next`	SamplerZ	[L0: `fxp/sign_fxsampler.c:183-216`]	Appendix G.6

Table 51: The fixed-point signer's routines, the algorithm each one is, its lines, and the lemma that bounds it.

M The gates, the machine-checked proofs and the imported facts

Structure. This appendix lists what Section 2 defines. Appendix M.1 lists the gates; Appendix M.2 the machine-checked proofs; Appendix M.3 the imported facts; Appendix M.4 the conditions of every measurement; Appendix M.5 what is not gated; Appendix M.6 describes the dependency graphs.

M.1 The gates

This subsection lists the gates and the reports, one script under `verify/` each; a report prints a quantity and compares nothing. An entry that opens with "sampled" names a sampled gate of Section 2.1; the others are exhaustive over their finite domain or compute the quantity they report, in the arithmetic Appendix M.4 names.

Checker	What it verifies	Backs
`verify/gates/renyi/two_point.py`	Sampled: the chord bound's attainment by the two-point distribution	Appendix K

`verify/gates/fp/mul.py`
`split.py`
`merge.py`
`ldl.py`
	Sampled: Lemma B.2, item 3, Lemmas B.3, G.18, G.24 against exact rationals	Section 3.1, Appendices G.3 and B

`verify/gates/tree/centers_map.py`
`subtree.py`
`form.py`
	Sampled: Proposition G.48 as an exact equality, and Proposition H.7, item 3 at degrees 1 to 8 (`verify/gates/tree/form.py`, no longer cited by the proof)	Appendix G.5, Appendix H.2.1

`verify/reports/sampler/table.py`
`glitch.py`
`floors.py`
`expm.py`
`renyi.py`
	Partly sampled: the table, the split scan, the floored region's bound and the polynomial's covering bound exact, `fxp_expm_p63` compared with the plain `expm_p63` statement for statement, the sampler's Rényi divergence from the ideal sampled	Appendix G.6

`verify/gates/renyi/identity.py`
`bound.py`
`tail.py`
	Sampled: Lemma 4.1 identity and bound, Lemma E.18 by brute force	Section 4

`verify/reports/key/keyconst_checked.py`	Sampled: with `--checked`, the six key constants on keys of the checked key generation (`fxp/`), with the root node's maxima over ψ	Appendix I

`verify/reports/fx/terms.py`
`verify/reports/tree/falcon_general.py`
`verify/gates/fx/center_shared.py`
	The loss of Theorem F.4 for both centers of the fixed-point signer (`verify/reports/fx/terms.py`): Proposition 5.8, Proposition 5.9, Corollaries I.78, I.87; the chain of Theorem 4.11 at (u, ζ) against the fixed-point signer's level cells (`verify/reports/tree/falcon_general.py`); the terms free of the center (`verify/gates/fx/center_shared.py`), a test cited by no statement	Appendix I to Appendix I.7

Checker	What it verifies	Backs
`verify/gates/fx/consts.py` `make_check.py` `interval_ops.py` `tail_copy_words.py` `tail_bounds.py`	Exhaustive: the stored constants, each away from a tie (Definitions I.1, I.20), the tail checks' thresholds and τ_K against `verify/reports/fx/leafsum_key.py`; sampled: the C against a Haskell core (**Hypothesis I.21**), the core against the ring identities and the Gaussian, the scheme against the reference (Statistics I.23); the tail checks of Definition 5.5: their interval arithmetic against exact rationals (**Hypothesis I.21**), their upper bounds at or above `verify/reports/fx/leafsum_key.py`'s values (Statistics I.23, item 12) and at or below the thresholds on its checked keys, a doctored threshold rejecting	Appendix I
`verify/reports/tree/leaferrors.py`	Sampled: the leaf perturbations of the fixed-point signer: every base-sampler call traced in the code, ffSampling$^{\mathbb{R}}$ replayed in Decimal on the same prefix; the sample maxima (Statistics I.23)	Section 5.2, Appendix I
`verify/reports/fx/leafsum_key.py` `tail_levels.py`	Sampled: per checked key at each center (`--centert` at t), μ_{key} of the exact K, $\max_i\lvert\delta_i\rvert$ and the remainder's bound, exact in the constants, against that center's M_n, D_n, B_n (Statistics I.23); exact at the thresholds: W^{tail} and the bit security of Corollaries I.80 and I.89	Appendices I.6 and I.7
`verify/reports/key/keychecks.py`	Sampled: the four checked quantities over 2000 keys of the reference key generation per degree, every check disabled; the acceptance of the degree's thresholds and of BFLP26's set (Statistics I.23); the sets an acceptance rate needs	Appendix I
`verify/gates/tree/tower_index.py`	The reference's FFT root layout is the angle-halving tower `rootTower` at every degree (Lemma I.83), exactly on the angle indices of `GM`; the FFT is the evaluation map	Appendix I.7

M.2 The machine-checked proofs

This subsection lists the proofs of Section 2.2 by folder under `real_approx/`. Every proof is on a compiled aarch64 object, clang `-O3`, at the CPU setting its folder's build names, `-mcpu=cortex-a72` or `-mcpu=apple-m1`.

Proof	Backs
`lemmas/fxp64_64/`	
`  mul_rounding`	Lemma I.3
`  div`	Lemma I.4
`  sqrt`	Lemma I.5
`  split_compose`	Lemma I.10, items 2 to 4, 8 and 11
`selfadj_compose`	
`merge_compose`	
`mul_fft_compose`	
`gram_compose`	
`  splitcall_compose`	Lemma I.10, item 14
`  fft_compose`	Lemma I.10, items 1 and 13
`ifft_compose`	
`  ldl_compose`	Lemma I.10, items 5 and 6
`ldlroot_compose`	
`  addsub_compose`	Lemma I.10, items 8 to 10
`neg_compose`	
`setsmall_compose`	
`  center_compose`	Lemma I.10, item 12
`  ffsamp_compose`	Lemma I.10, item 7
`  ffsamp_dataflow`	Lemma I.11
`lemmas/fxp64_64/ops/`	
`  add`	Lemma I.2
`sub`	
`neg`	
`  half`	Lemma I.6, items 1 and 2
`div2e`	
`  mul2e`	Lemma I.6, item 3; Lemma I.7, item 1
`of`	
`  floor`	Lemma I.7, items 2 to 4
`trunc`	
`rint`	
`  lt`	Lemma I.8; line 4 of BerExp (Algorithm 9); lines 5
`max`	to 11 of keychecks (Algorithm 12)
`min`	

The claims with no failing control. The algebraic halves of the claims of `fxp_div` and `fxp_sqrt` have no failing control: a false identity over their loops exhausts Singular's memory. They are not vacuous: their vacuity controls fail, every fact their algebra uses is proved, and the pinned validations of their models hold.

The trusted base, as built. Section 2.2 lists what a proof trusts. As built:

- `cv`, to be released; a second build of the same source, in a new build directory, yielded the binary that ran the proofs byte for byte (2026-11-06).

The Lean step from a claim to the report's statement. Where `cv` proves a claim in the forms of its predicates (a congruence, a shift, a case split), a Lean theorem of `lean/FFSampling/MachineWords.lean` derives the report's statement from it (Lemmas I.3 to I.8).

M.3 Provenance of every imported fact

Level	Fact	Source
L0	The per-node operation order of the recursion	`sign_sampler.c:1245-1350`
L0	The leaf standard deviation $\sqrt{d} \cdot$ `INV_SIGMA`	`sign_sampler.c:1208`
L0	The Gram, LDL, split, merge kernels	`sign_fpoly.c:2033,2156,2279,2369,2470`
L0	The root node's center $t = (\mathsf{h}(\mathsf{m}), 0)B^{-1}$, its computation	`sign_fpoly.c:2663`
L0	The basis rows and the Gram's layout	`sign_core.c:11-30,112-120`
L0	The reconstruction rounds z, then Bz modulo q	`sign_core.c:192-203`
L0	The base sampler, `ber_exp`, `expm_p63`, the table	`sign_sampler.c:84-128,780-969`
L0	$\sigma_{\min}$, σ_{sig}, σ_0	`sign_sampler.c:18-56`
L0	The key generation's coefficient-norm threshold 16823	`kgen.c:41-49`
L0	The key generation's orthogonalized-norm threshold	`kgen.c:53`, `kgen_ntru.c:1904-1934`
L0	The key generation solves $fG - gF = q$	`kgen.c:57-59`
L1	The lattice $\Lambda(B)$ of a basis	FGGJK26, Def. 4
L1	$\rho_{s,c}$ and $D_{\Lambda+t,s}$	FGGJK26, Def. 6
L1	The Gram–Schmidt norm, the smoothing parameter	FGGJK26, Def. 7, Section 2.3
L1	The Rényi divergence	FGGJK26, Def. 8
L1	The split operators V_m, M_m, the isometry and $V_m(ab) = V_m(b)M_m(a)$	FGGJK26, App. F.3
L1	The algorithms ffLDL† and ffSampling	FGGJK26, Alg. 2, Alg. 3
L1	Probability preservation	LSS14, Lem. 4.1
L1	The real-arithmetic output probability measure of the sampler	FGGJK26, Lem. 22
L1	The ideal signer's security against an attack that reads Q_s signatures	FGGJK26, Thm. 1
L0	The fixed-point type, its rounded operations and its constants	`fxp/sign_fxp.h:28-30`, `fxp/sign_fxp.c:101,149,181`, `fxp/gen_consts.py:145`
L0	The fixed-point FFT, split, $LDL^\dagger$, sampler and the two centers t, t_{frac}	`fxp/sign_fxpoly.c:11,128,176,258,273`, `fxp/sign_fxsampler.c:88-216`, `fxp/sign_fxcore.c:60-105`
L0	The four key checks in fixed point	`fxp/kgen_fx.c:60-191`
L2	The four key checks, the split $t = t_{\text{int}} + t_{\text{frac}}$	BFLP26, Alg. 2, Alg. 7

The statements of other works at ours. Table 52 lists how each corollary stating another work's statement in our symbols is verified, Corollaries E.3, E.19 and K.3; the one imported as stated, Fact A.45, item 14, sits with the facts in Table 12.

Statement	Lean	CryptoLine	Gate	Hypotheses	Source
Cor. E.3	✓				L1: MP12, Lem. 2.8
Cor. E.19	✓				L1: Ban93, Lem. (1.5)(ii)
Cor. K.3	✓				L1: Pre17, Lem. 3

Table 52: Appendix M: how each corollary is verified.

M.4 Conditions

The measurements were made under the following conditions; a record that names its own seed or date carries that one.

Item	Value
Code	`c-fn-dsa`, plain C build, commit `a5f1589` of 2026-08-29; each cited table and constant checked against the bytes of the compiled object [gate: `verify/gates/bytes/const_data.py`]
Runtime	Python 3.14.7; floats are binary64, round to nearest even, no fused multiply-add
Exact references	`fractions.Fraction`; `decimal` at 60 digits
The bit security's cells	Table 34 and Theorem 1.3: computed in binary64, the logarithm, the exponential and the square root those of Python's `math` (`verify/lib/loss_terms.py`)
Seeds	20260902 unless the record names its own
Date	2026-09-02
Fixed-point signer	`fxp/`, `makecheck` with Apple clang version 21.0.0 (clang-2100.1.1.101) and GHC 9.14.1; date 2026-09-04

The plain build does not link as shipped. The plain C build of `c-fn-dsa` does not link at commit `a5f1589`: the reference's `mq.c:2521` keeps `mqpoly_sqnorm_int_to_signed` under `#if0` while its `sign_core.c:244` still calls it in the plain branch; the fixed-point signer's gates carry that function under the reference's exported name (`fxp/mq_shim.c`), which is how the plain build modeled here is built and run.

M.5 What is not gated

- A statement's first-order reading is not gated: the gates check the exact inequality, and the reading's remainder has a name and no gate.
- The statements tagged eyes only (Section 2.1) and the three code-alignment hypotheses, which are not discharged.

M.6 The dependency graphs

This subsection describes the dependency graph of every numbered statement. Figures 113,114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 37, 38, 39, 40, 41, 108, 110, 109, 111, 66, 69, 70, 72, 73, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 95, 98, 99, 102, 103, 104, 105, 106, 92, 93, 90, 91, 94 describe the graphs of the statements; Figures 47,48, 51, 52, 54, 55, 56, 57, 58, 59, 60, 61, 64, 65, 42, 43, 44, 45, 46 those of the intermediate statements of the proof appendices.

How a graph is read. Each figure describes one section or subsection: its own statements, and dashed the statements they use from elsewhere. An arrow runs from a statement to the statement whose proof uses it, so every path ends at an end result of the report. A box's color is its statement's kind: a definition blue, a hypothesis or a fact orange, a lemma or a proposition green, a theorem or a corollary vermilion; a figure's own statements are filled. A box of another section or subsection and the items taken from [FGdG+26] are grey and dashed; the graphs show no other import. Section 3's catalogs are outside the graph: Definitions A.1, A.2, A.3, A.8, A.25, A.26 to A.30 and Facts A.6, A.7, A.41 to A.45 are the report's vocabulary, cited the way one cites an identity of the field: drawing them would put an arrow from Fact A.41 alone into the 195 statements that cite it. Definition A.4, which the realizations instantiate, is in the graph. The figures are TikZ, generated from one edge list keyed by the statements' labels, with the numbers read from the build's own auxiliary file, so figure and text agree by construction; Graphviz supplies only the coordinates. [gate: `paper/gen_deps.py`]

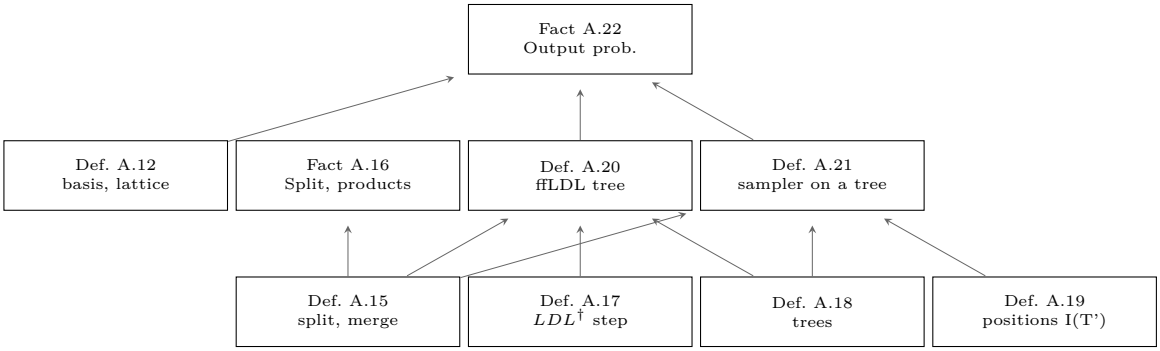


Figure 113: Dependencies, Section 3.2.

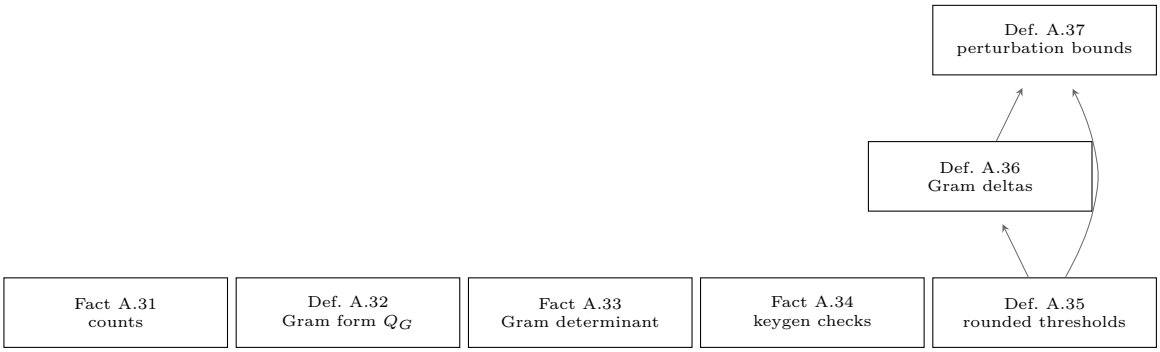


Figure 114: Dependencies, Section 3.2: the tree of a key.

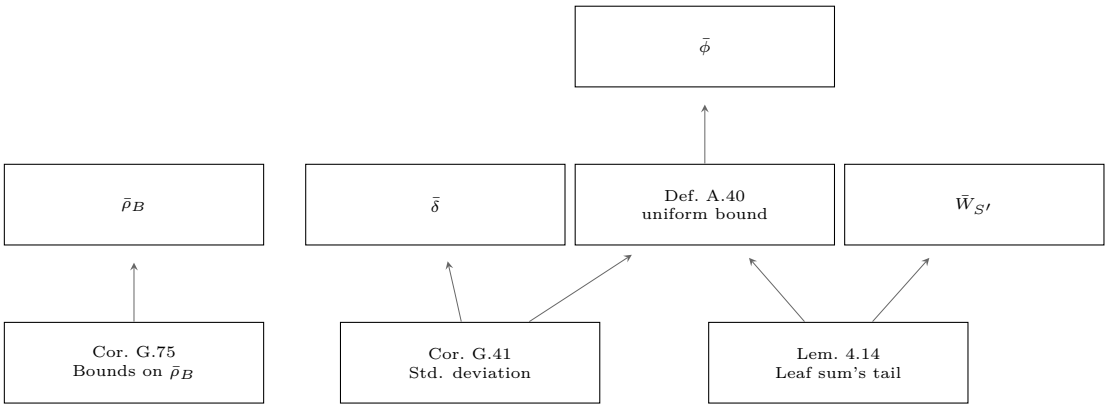


Figure 115: The terms of $\ln R$ and the statements that set them.

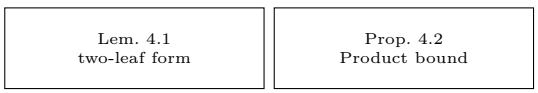


Figure 116: Dependencies, Section 4.2.

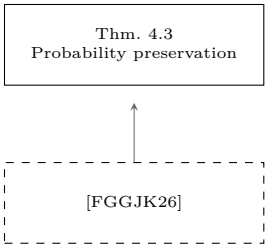


Figure 117: Dependencies, Section 4.3.

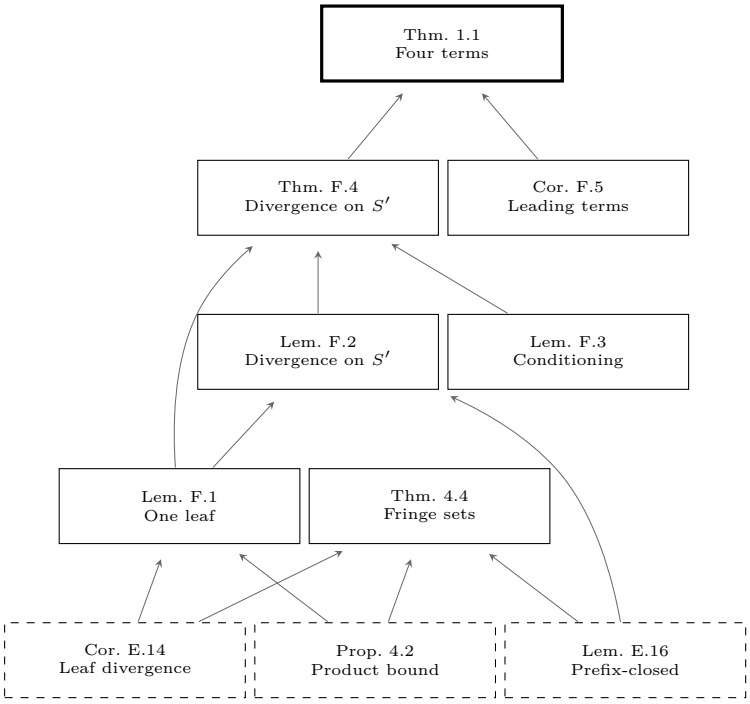


Figure 118: Dependencies, Section 4.

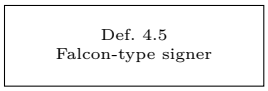


Figure 119: Dependencies, Section 4.5.1.

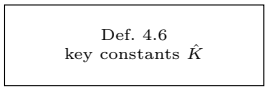


Figure 120: Dependencies, Section 4.5.2.

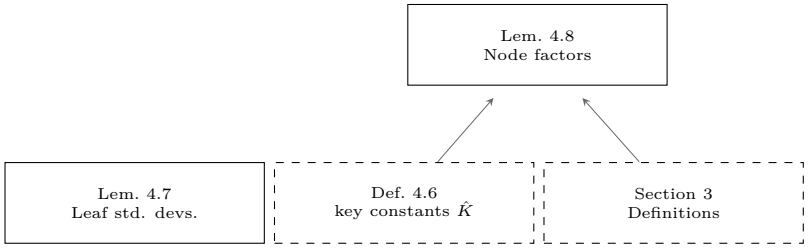


Figure 121: Dependencies, Section 4.5.3.

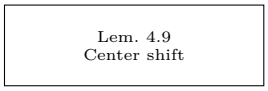


Figure 122: Dependencies, Section 4.5.4.

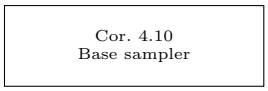


Figure 123: Dependencies, Section 4.5.5.

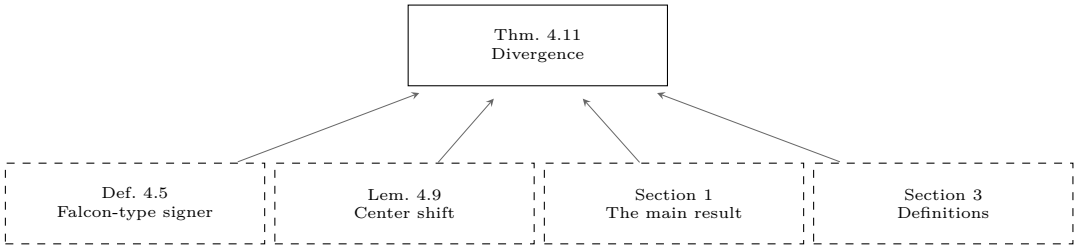


Figure 124: Dependencies, Section 4.5.6.

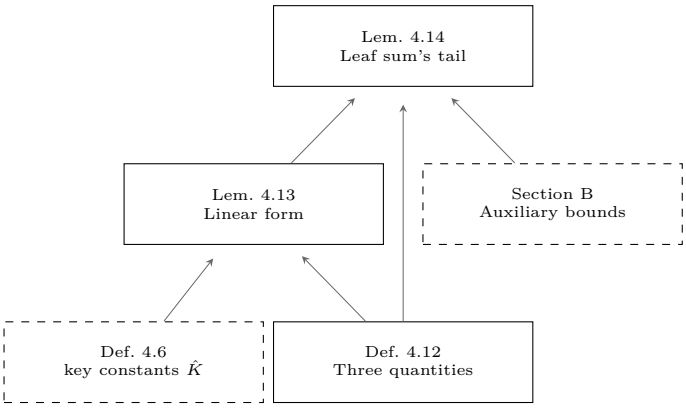


Figure 125: Dependencies, Section 4.5.7.

List of Algorithms

1 $\oplus$, $\ominus$, $\otimes$, the code's complex operations of Definition A.8 . . . 16
2 split(f), the split butterflies of one level . . . 19
3 $\text{split}_{\text{sa}}(f)$, the split butterflies of one level for a self-adjoint f . . . 19
4 merge(f_0, f_1), the merge butterflies of one level . . . 20
5 $\text{LDL}^\dagger(\mathcal{G})$, the $LDL^\dagger$ step of one node . . . 21
6 ffsamp$(t, \mathcal{G}, \texttt{root})$, the code's recursion: the $LDL^\dagger$ step of a node when the recursion reaches it, no tree stored . . . 24
7 deepest$(t, l_{10}, d_{00}, d_{11})$, the recursion's deepest level . . . 25
8 SamplerZ$(\mu, \texttt{isigma})$, the base sampler `sampler_next` . . . 26
9 BerExp(x, ccs), the acceptance `ber_exp` with `expm_p63` . . . 27
10 $\text{ffSampling}^{\mathcal{F}}(B, s, t)$, the signer's sampler . . . 28
11 keygeneration(seed, c), the reference's key generation under the four checks of [L2: BFLP26, Alg. 2] and the three tail checks at the center c . . . 29
12 keychecks(f, g, F, G), the four coefficient checks of [L2: BFLP26, Alg. 2] on a key . . . 30
13 Gram(B), the Gram matrix in FFT form . . . 215
14 FFT(f), the coefficients to $(f(\psi_k))_{k<n/2}$ . . . 371
15 tailcheck(f, g, F, G, c), the three tail checks of a key at one center . . . 442
16 tailbounds(c), the upper bounds $\mu^\uparrow$ and $B^\uparrow$ of the tail checks at one center . . . 443
17 $\text{center}_{\text{frac}}(\mathsf{h}(\mathsf{m}), f, F)$, the center split over the integers [L2: BFLP26, Alg. 7] . . . 622
18 ν_2: a lower bound on ν_2, one rule per operation . . . 689
19 ν_2-walk: ν_2 along a straight-line program over $\mathcal{F}$ . . . 689

List of Figures

1 The reference tree. . . . 10
2 The chain of a machine-checked proof and the path of a gate. . . . 12
3 The call graph of the algorithms. . . . 17
4 The terms of $\ln R$ on the tree of Figure 22 (Theorem 1.1; Definitions A.27, A.28 and A.29). . . . 34
5 One leaf of the tree of Figure 22: the two Gaussians of Lemma 4.1 and the three measures of Proposition 4.2 . . . 36
6 The composition along the samples on the tree of Figure 22 (Theorem 4.3; Definition A.26). . . . 37
7 The fringe sets on the tree of Figure 22 (Theorem 4.4; Definitions A.26 and A.28). 39
8 The deviations down the tree of Figure 23 (Theorem 4.11; Corollary G.36; Theorem G.59). . . . 40
9 The Lean declarations carrying Definition 4.6 . . . 41
10 The Lean declarations carrying Definition 5.2 . . . 50
11 The Lean declarations carrying Definition 5.3 . . . 51
12 The objects of Proposition 5.9 and Corollary 5.10, each with the statement that bounds it, and the way to Theorem 1.3; an arrow runs from a statement to the statement whose proof cites it. . . . 56
13 The inputs the rejection at the saturated exponent sets and the terms it moves, each arrow labeled by its statements. . . . 59
14 The terms of $\ln R$ of Theorem 1.1, the inputs that set them and the changes that set the inputs, each arrow labeled by its statements, $S' := S_\tau \cap E$ (Theorem 5.12). 61
15 The terms of the bit security $2^{-\lambda_{\mathcal{F}}} = Q_s\, P(S'^c) + y + \Pi_C(y)$ of Theorem 1.2, the inputs that set them and the changes that set the inputs, each arrow labeled by its statements, $S' := S_\tau \cap E$ (Theorem 5.12). . . . 61

16 The inputs the root's identity sets, the assumptions of the tree, the centers, the base sampler and the summary they meet, and the items of Proposition 5.9 that state them, each arrow labeled by its statements. . . . 62
17 The inputs the one division sets and the realization it defines for the signer, the first item of Proposition 5.9, each arrow labeled by its statements. . . . 62
18 The Lean declarations carrying Definition A.4 . . . 70
19 The Lean declarations carrying Definition A.8 . . . 73
20 The Lean declarations carrying Definition A.10 . . . 73
21 The Lean declarations carrying Definition A.18 . . . 76
22 A tree $T \in \mathcal{T}_4$ (Definition A.18): a node as a rectangle with its constructor, a leaf diagonal as a circle, the left subtree on the left as in FHK+20, Figure 3.1; the sample positions (Definition A.19) read from right to left. . . . 77
23 The subtrees of the tree of Figure 22: $\mathrm{Sub}(T) = \{T, T_{00}, T_{11}, d'_{00}, d'_{11}, d''_{00}, d''_{11}\}$ (Definition A.18, the subtrees); an edge is L or R, a row is a depth. . . . 77
24 The Lean declarations carrying Definition A.19 . . . 78
25 The sample positions on the tree of Figure 22, $N = 8$ (Definition A.19): at every node the right subtree's positions precede the left's; the leaf diagonals at the positions are $d_1 = d_2 = d''_{11}$, $d_3 = d_4 = d''_{00}$, $d_5 = d_6 = d'_{11}$, $d_7 = d_8 = d'_{00}$ (Definition A.19, the leaf diagonal). . . . 78
26 The Lean declarations carrying Definition A.21 . . . 80
27 The Lean declarations carrying Definition A.23 . . . 82
28 The Lean declarations carrying Definition A.25 . . . 84
29 The Lean declarations carrying Definition A.28 . . . 86
30 The Lean declarations carrying Definition A.29 . . . 86
31 The Lean declarations carrying Definition A.30 . . . 86
32 The Lean declarations carrying Definition A.32 . . . 87
33 The Lean declarations carrying Definition A.38 . . . 89
34 The Lean declarations carrying Definition A.39 . . . 90
35 The Lean declarations carrying Definition A.40 . . . 92
36 The Lean declarations carrying Definition A.46 . . . 97
37 Dependencies, Section B.1. . . . 98
38 Dependencies, Section B.2. . . . 99
39 Dependencies, Section B.3. . . . 103
40 Dependencies, Section B.4. . . . 104
41 Dependencies, Section C.1. . . . 108
42 Dependencies, Section D.1. . . . 112
43 Dependencies, Section D.2. . . . 115
44 Dependencies, Section D.3. . . . 120
45 Dependencies, Section E.2. . . . 132
46 Dependencies, Section E.3. . . . 150
47 Dependencies, Section G.1. . . . 186
48 Dependencies, Section G.2. . . . 190
49 The Lean declarations carrying Definition G.6 . . . 193
50 The Lean declarations carrying Definition G.9 . . . 196
51 Dependencies, Section G.3. . . . 200
52 Dependencies, Section G.3.2. . . . 204
53 Section G.4: the relative deviation χ of the computed diagonals, from the root node to the leaves, and the two quantities the rest of the report takes from it. . . . 223
54 Dependencies, Section G.4.1. . . . 224
55 Dependencies, Section G.4.2. . . . 250
56 Dependencies, Section G.5.1. . . . 261
57 Dependencies, Section G.5.2. . . . 267

58 Dependencies, Section G.6.1. . . . 298
59 Dependencies, Section G.7.1. . . . 316
60 Dependencies, Section G.7.2. . . . 317
61 Dependencies, Section H.2.1. . . . 360
62 The objects of Section H.2.1 by the part of the tree of Figure 22 that carries them. 360
63 The Lean declarations carrying Definition H.1 361
64 Dependencies, Section H.2.2. . . . 370
65 Dependencies, Section H.2.3. . . . 378
66 Dependencies, Appendix I.1.1. . . . 413
67 The Lean declarations carrying Definition I.1 415
68 The declarations, the precondition and the postcondition of the CryptoLine lemma of item 5 at $h = 2$, as its file states them (`lemmas/fxp64_64/ldl_compose/lem_ldln_2.cl`); a line longer than the page is wrapped at a space. . . . 433
69 Dependencies, Appendix I.1.2. . . . 439
70 Dependencies, Appendix I.1.3. . . . 441
71 The Lean declarations carrying Definition I.19 449
72 Dependencies, Appendix I.1.4. . . . 450
73 Dependencies, Appendix I.3.1. . . . 454
74 The Lean declarations carrying Definition I.28 458
75 The Lean declarations carrying Definition I.32 462
76 Dependencies, Appendix I.3.2. . . . 468
77 Dependencies, Appendix I.3.3. . . . 488
78 Dependencies, Appendix I.3.4. . . . 504
79 Dependencies, Appendix I.3.5. . . . 512
80 Dependencies, Appendix I.3.6. . . . 525
81 Dependencies, Appendix I.3.7. . . . 534
82 Dependencies, Appendix I.3.8. . . . 544
83 Dependencies, Appendix I.3.9. . . . 550
84 Dependencies, Appendix I.4. . . . 552
85 Dependencies, Appendix I.5.1. . . . 556
86 Dependencies, Appendix I.5.2. . . . 564
87 Dependencies, Appendix I.5.3. . . . 573
88 Dependencies, Appendix I.5.5. . . . 600
89 Dependencies, Appendix I.5.6. . . . 605
90 Dependencies, Appendix I.6.1. . . . 607
91 Dependencies, Appendix I.6.2. . . . 614
92 Dependencies, Appendix I.7.1. . . . 623
93 Dependencies, Appendix I.7.2. . . . 634
94 Dependencies, Appendix I.8. . . . 641
95 Dependencies, Appendix J.1. . . . 652
96 The Lean declarations carrying Definition J.1 653
97 The Lean declarations carrying Definition J.5 655
98 Dependencies, Appendix J.2. . . . 690
99 Dependencies, Appendix J.3.1. . . . 697
100 The Lean declarations carrying Definition J.40 697
101 The Lean declarations carrying Definition J.41 697
102 Dependencies, Appendix J.3.2. . . . 699
103 Dependencies, Appendix J.3.3. . . . 701
104 Dependencies, Appendix J.3.4. . . . 702
105 Dependencies, Appendix J.4.1. . . . 705
106 Dependencies, Appendix J.4.2. . . . 714
107 The Lean declarations carrying Definition J.55 715

108 Dependencies, Appendix J.5.1. 725
109 Dependencies, Appendix J.5.2. 732
110 Dependencies, Appendix J.5.3. 737
111 Dependencies, Appendix J.5.4. 738
112 Loss in bits from the derived bounds against $\log_2 Q_s$, $\hat{K}_n$, one graph per precision p; the data of Table 42. Gate: `verify/reports/fp/loss.py`. 746
113 Dependencies, Section 3.2. 792
114 Dependencies, Section 3.2: the tree of a key. 792
115 The terms of $\ln R$ and the statements that set them. 792
116 Dependencies, Section 4.2. 792
117 Dependencies, Section 4.3. 793
118 Dependencies, Section 4. 793
119 Dependencies, Section 4.5.1. 793
120 Dependencies, Section 4.5.2. 793
121 Dependencies, Section 4.5.3. 794
122 Dependencies, Section 4.5.4. 794
123 Dependencies, Section 4.5.5. 794
124 Dependencies, Section 4.5.6. 794
125 Dependencies, Section 4.5.7. 794