Vincent Hwang

Senior Software Engineer, Qinvicta Inc., Boston, USA

vincentvbh7@gmail.com · vincentvbh.github.io · github.com/vincentvbh · Google Scholar · DBLP

Publications

Reverse chronological order; author names in alphabetical order. * = included in the PhD thesis; ** = included in the Master's thesis.

PhD (Jan. 2023 – Apr. 2026)

16. Phillip Gajland, Vincent Hwang, and Jonas Janneck. Shadowfax: Hybrid Security and Deniability for AKEMs. To appear in *USENIX Security Symposium*, 2026. [ePrint] [Artifact]
Shadowfax shows how deniability can be preserved in post-quantum and hybrid settings, with several portable implementations. Instantiated with ML-KEM and Falcon, it yields 1728-byte ciphertexts and 2036-byte public keys, and encapsulation and decapsulation cost 1.8M and 0.7M cycles on an Apple M1 Pro at 3 GHz. I was responsible for the portable implementations.

15.* Gilles Barthe, Gustavo Xavier Delerue Marinho Alves, Hugo Pacheco, José Bacelar Almeida, Luís Esquível, Manuel Barbosa, Peter Schwabe, Pierre-Yves Strub, Tiago Oliveira, and Vincent Hwang. Faster Verification of Faster Implementations: Combining Deductive and Circuit-Based Reasoning in EasyCrypt. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 3526–3544. IEEE Computer Society, 2025. [Paper] [ePrint]
We combined deductive and circuit-based reasoning in EasyCrypt, verified the AVX2-optimized rejection sampling in Kyber for the first time and the equivalence of the optimized compression functions, and simplified the verification of the AVX2-optimized Keccak permutation. I proposed the compression-function optimizations and wrote the corresponding part of the paper.

14.* Vincent Hwang, YoungBeom Kim, and Seog Chung Seo. Multiplying Polynomials without Powerful Multiplication Instructions. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025(1):160–202, 2024. [Paper] [Artifact] [Slides] [ePrint]
We optimized Dilithium and Saber on Cortex-M3 and 8-bit AVR: for the prime-modulus ring of Dilithium we generalized Barrett multiplication to multi-limb arithmetic on platforms without powerful multiplication instructions; for the power-of-two-modulus ring we showed that Nussbaumer performs best absent precision issues. I proposed the ideas, implemented the Cortex-M3 optimizations, and wrote the corresponding parts of the paper.

13.* Vincent Hwang. Formal Verification of Emulated Floating-Point Arithmetic in Falcon. In *International Workshop on Security*, pages 125–141. Springer, 2024. [Paper] [Artifact] [Slides] [ePrint]
With the domain-specific language CryptoLine, this paper verified the functional equivalence of the software-emulated floating-point additions and multiplications, and the ranges of the intermediate values of the floating-point FFT, in the signature generation of Falcon.

12.* Vincent Hwang. A Survey of Polynomial Multiplications for Lattice-Based Cryptosystems. *IACR Communications in Cryptology*, 1(2), 2024. [Paper] [ePrint]
This survey reviews practical techniques for multiplying polynomials in rings of the form $\mathbb{Z}_q[x]/\langle x^n - \alpha x - \beta \rangle$, with emphasis on modular arithmetic, homomorphisms, and vectorization.

11.* Vincent Hwang. Pushing the Limit of Vectorized Polynomial Multiplication for NTRU Prime. In *Australasian Conference on Information Security and Privacy*, pages 84–102. Springer, 2024. [Paper] [Artifact] [Slides] [ePrint]
We furthered the NTRU Prime optimizations on Cortex-A72 with Armv8-A Neon and on Haswell with AVX2, systematically reviewed the notion of vectorization across platforms, and replaced Rader's FFT with truncated Rader's FFT.

10.* Vincent Hwang, Chi-Ting Liu, and Bo-Yin Yang. Algorithmic Views of Vectorized Polynomial Multipliers – NTRU Prime. In *International Conference on Applied Cryptography and Network Security*, pages 24–46. Springer, 2024. [Paper] [Artifact] [Slides] [ePrint]
We optimized NTRU Prime on Cortex-A72 with Armv8-A Neon by integrating Schönhage's and Bruun's FFTs with Good–Thomas and Rader's FFTs, which significantly reduced the number of small-dimensional

polynomial multiplications. I proposed the optimizations, implemented Bruun's FFT and the fastest approach, and wrote the paper.

9.* Han-Ting Chen, Yi-Hua Chung, Vincent Hwang, and Bo-Yin Yang. Algorithmic Views of Vectorized Polynomial Multipliers – NTRU. In *Progress in Cryptology – INDOCRYPT 2023*, pages 177–196. Springer, 2024. [Paper] [Artifact] [Slides] [ePrint]
We optimized NTRU on Cortex-A72 with Armv8-A Neon, improving the design of Toom–Cook and implementing the Toeplitz matrix-vector product approach. I proposed the Toom–Cook improvement, integrated and further optimized the coauthors' polynomial multipliers, and wrote the non-implementation part of the paper.

MSc (Sep. 2021 – Jun. 2022)

8.* Vincent Hwang, Jiaxiang Liu, Gregor Seiler, Xiaomu Shi, Ming-Hsien Tsai, Bow-Yaw Wang, and Bo-Yin Yang. Verified NTT Multiplications for NISTPQC KEM Lattice Finalists: Kyber, SABER, and NTRU. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(4):718–750, 2022. [Paper] [Artifact]
We verified the assembly-optimized NTT-based polynomial multiplications of Kyber, Saber, and NTRU on Cortex-M4 and on Skylake with AVX2 with the domain-specific language CryptoLine. I rewrote the Cortex-M4 assembly polynomial multiplication for NTRU and described the structure of the Cortex-M4 assembly programs in the paper.

7.** Erdem Alkim, Vincent Hwang, and Bo-Yin Yang. Multi-Parameter Support with NTTs for NTRU and NTRU Prime on Cortex-M4. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(4):349–371, 2022. [Paper] [Artifact] [Talk] [ePrint]
We revisited NTRU and NTRU Prime on Cortex-M4, improving the initial and odd-radix butterflies of the Good–Thomas FFT and proposing incomplete Good–Thomas FFT for code-size optimization. I proposed and implemented the optimizations and wrote the paper.

6.* Hanno Becker, Vincent Hwang, Matthias J. Kannwischer, Lorenz Panny, and Bo-Yin Yang. Efficient Multiplication of Somewhat Small Integers using Number-Theoretic Transforms. In *International Workshop on Security*, pages 3–23. Springer, 2022. [Paper] [Artifact] [ePrint]
We explored FFT-based integer multiplication on Cortex-M3 and Cortex-M55 and located the crossover between FFT-based and $\Theta(n^2)$ non-FFT-based integer multiplication at around 2048 bits. I was involved in the Cortex-M3 implementation.

5.* Amin Abdulrahman, Vincent Hwang, Matthias J. Kannwischer, and Amber Sprenkels. Faster Kyber and Dilithium on the Cortex-M4. In *International Conference on Applied Cryptography and Network Security*, pages 853–871. Springer, 2022. [Paper] [Artifact] [ePrint]
We revisited Dilithium and Kyber on Cortex-M4, incorporating assembly optimizations from prior Cortex-M4 and Cortex-A72 work and optimizing the challenge polynomial multiplication in Dilithium. I proposed the Fermat number transform for that multiplication and an optimization of the base multiplication in Kyber, and cowrote the corresponding parts of the paper.

4.** Hanno Becker, Vincent Hwang, Matthias J. Kannwischer, Bo-Yin Yang, and Shang-Yi Yang. Neon NTT: Faster Dilithium, Kyber, and Saber on Cortex-A72 and Apple M1. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(1):221–244, 2021. [Paper] [Artifact] [ePrint]
We rediscovered the multiplicative form of Barrett reduction, found a correspondence between Montgomery and Barrett multiplications, and applied the resulting optimizations to Dilithium, Kyber, and Saber on Cortex-A72 and Apple M1 with Armv8-A Neon. I implemented the optimizations and wrote the corresponding parts of the paper.

3.** Amin Abdulrahman, Jiun-Peng Chen, Yu-Jia Chen, Vincent Hwang, Matthias J. Kannwischer, and Bo-Yin Yang. Multi-moduli NTTs for Saber on Cortex-M3 and Cortex-M4. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(1):127–151, 2021. [Paper] [Artifact] [Talk] [Slides] [ePrint]
Continuing the Saber optimizations on Cortex-M4, we optimized Saber on Cortex-M3, the memory footprint on both cores, and the masked implementation on Cortex-M4, and concluded that NTT is the fastest approach for Saber. I proposed the ideas, implemented the Cortex-M4 optimizations and the fastest Cortex-M3 approach, and wrote the corresponding parts of the paper.

BSc (Sep. 2016 – Jun. 2021)

2.* Chi-Ming Marvin Chung, Vincent Hwang, Matthias J. Kannwischer, Gregor Seiler, Cheng-Jhih Shih, and Bo-Yin Yang. NTT Multiplication for NTT-unfriendly Rings: New Speed Records for Saber and NTRU on Cortex-M4 and AVX2. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(2):159–188, 2021. [Paper] [Artifact] [Talk] [Slides] [ePrint]
We migrated the Good–Thomas approach to all parameter sets of NTRU on Cortex-M4, and optimized Saber on Cortex-M4 and NTRU and Saber on Skylake with AVX2. I was deeply involved in the Cortex-M4 implementations.

1.* Erdem Alkim, Dean Yun-Li Cheng, Chi-Ming Marvin Chung, Hülya Evkan, Leo Wei-Lun Huang, Vincent Hwang, Ching-Lin Trista Li, Ruben Niederhagen, Cheng-Jhih Shih, Julian Wälde, and Bo-Yin Yang. Polynomial Multiplication in NTRU Prime: Comparison of Optimization Strategies on Cortex-M4. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(1):217–238, 2020. [Paper] [Artifact] [Talk] [Slides] [ePrint]
We proposed three assembly-optimized NTT-based implementations of the polynomial multiplication in NTRU Prime on Cortex-M4. I was deeply involved in the Good–Thomas implementation.

Technical reports

– Vincent Hwang, YoungBeom Kim, and Seog Chung Seo. Barrett Multiplication for Dilithium on Embedded Devices. IACR ePrint 2023/1955, 2023. [ePrint] [Artifact]
Extended into the TCHES 2025 paper on multiplying polynomials without powerful multiplication instructions.

– Han-Ting Chen, Yi-Hua Chung, Vincent Hwang, Chi-Ting Liu, and Bo-Yin Yang. Algorithmic Views of Vectorized Polynomial Multipliers for NTRU and NTRU Prime (Long Paper). IACR ePrint 2023/541, 2023. [ePrint]
Split into the INDOCRYPT 2023 (NTRU) and ACNS 2024 (NTRU Prime) papers above.