Vincent Hwang

Email | Github | Personal Website | Google Scholar | DBLP

Date of this document: 2025-09-17.

1 Education

PhD, Cryptographic Engineering — Germany | Jan. 2023 – 2025 (expected, defense scheduling)
Max Planck Institute for Security and Privacy
Advisor: Peter Schwabe

MSc., Department of Computer Science and Information Engineering — Taiwan | Sept. 2021 - Jun. 2022
National Taiwan University
Advisors: Yen-Huan Li and Bo-Yin Yang

BSc., Department of Computer Science and Information Engineering — Taiwan | Sept. 2016 - Jun. 2021
National Taiwan University

2 Programming Skills

- Assembly (very familiar): Armv7-M, Armv7E-M, Armv8-A, AVX2. Low-level optimizations.
- Assembly (somewhat familiar): Armv9-A, AVX-512. Low-level optimizations. Ongoing research.
- C (very familiar): Primary for interfacing between the assembly and the high-level api. Sometimes I use function pointers for unit tests.
- C++ (somewhat familiar): Primary about templates for scalability. I rarely use standard libraries as they are not built for cryptographic uses where various secure programming practice must be employed.
- CUDA (somewhat familiar): Ongoing research.
- Haskell (some experience): Scripts for generating some programs and constants used in low-level optimizations.

3 Research Interests

I'm doing research in cryptographic engineering. Cryptographic engineering is a field exploring how the mathematical constructs in cryptography could/should be best implemented in real-world computing devices. I position myself as a computer scientist turning the high-level ideas into optimized computer programs. Frequently, this amounts to several iterations of refinements for the high-level ideas and experiments through assembly programming. I programmed the computationally-intensive polynomial arithmetic in lattice-based cryptosystems for embedded devices (Armv7-M onward) and high performance processors (Armv8-A onward for `aarch64`, AVX2 extension onward for `x86-64`). I coauthored implementations papers targeting candidates NTRU, NTRU Prime, and Saber, and standards `ml-kem` and `ml-dsa` (previously known as Kyber and Dilithium) of the Post-Quantum Cryptography Standardization by the National Institute of Standards and Technology (NIST). Optimizing polynomial arithmetic for crypto usually involves some basics of algebra and various assembly languages. I also work on other topics like formal verification, and explore interesting computational devices from time to time. Recently, I'm mainly programming for the elliptic-curve discrete logarithm on the H100 GPU, and also optimizing the mathematically-heavy NIST standard `fn-dsa` (previously known as Falcon) in assembly.

Key words: Cryptographic engineering, assembly programming, post-quantum cryptography, and practical integer and polynomial multiplications.

4 Services

- 2026: (Incoming) Artifact Committee Member of TCHES 2026.
- 2025: Reviewer of TCHES 2025 (×8), ArcticCrypt 2025 (×1), CT-RSA 2025 (×2), JCEN (×1); Artifact Committee Member of TCHES 2025 (×5).
- 2024: Reviewer of Crypto 2024 (×1), TCHES 2024 (×3).
- 2023: Artifact Committee Member of TCHES 2023 (×2).

TCHES = Transactions on Cryptographic Hardware and Embedded Systems;
CT-RSA = The Cryptographers' Track at RSA Conference;
JCEN = Journal of Cryptographic Engineering;
(·) = The number of reviews submitted.

5 Publications (Reversed Chronological Order)

Author names in alphabetical order. * = Contributions included in the PhD thesis. ** = Contributions included in the Master's thesis.

PhD program ongoing.

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. IACR ePrint. Reference [AAB^{+}25].

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. IACR ePrint. Reference [HKS24].

13*. Vincent Hwang. Formal Verification of Emulated Floating-Point Arithmetic in Falcon. 2024. In *International Workshop on Security*, pages 125-141. Springer, 2024. Paper. Artifact. Slides. IACR ePrint. Reference [Hwa24b].

12*. Vincent Hwang. A Survey of Polynomial Multiplications for Lattice-Based Cryptosystems. *IACR Communications in Cryptology*, 1(2), 2024. Paper. IACR ePrint. Reference [Hwa24a].

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. IACR ePrint. Reference [Hwa24c].

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. IACR ePrint. Reference [HLY24].

9*. Han-Ting Chen, Yi-Hua Chung, Vincent Hwang, and Bo-Yin Yang. Algorithmic Views of Vectorized Polynomial Multipliers – NTRU. In Anupam Chattopadhyay, Shivam Bhasin, Stjepan Picek, and Chester Rebeiro, editors, *Progress in Cryptology – INDOCRYPT 2023*, pages 177–196. Springer, 2024. Paper. Artifact. Slides. IACR ePrint. Reference [CCHY24].

Master's degree conferral.

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. 2022. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(4):718–750, 2022. Paper. Reference [HLS^{+}22].

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. IACR ePrint. Reference [AHY22].

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. IACR ePrint. Reference [BHK^{+}22].

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. IACR ePrint. Reference [AHKS22].

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. IACR ePrint. Reference [BHK^{+}21].

3**. Amin Abdulrahman, Jiun-Peng Chen, Yu-Jia Chen, Vincent Hwang, Matthias J. Kannwischer, and Bo-Yin Yang. Multimoduli 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. IACR ePrint. Reference [ACC^{+}21].

Bachelor's degree conferral.

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. IACR ePrint. Reference [CHK$^+$21].

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. IACR ePrint. Reference [ACC$^+$20].

References

[AAB+25] José Bacelar Almeida, Gustavo Xavier Delerue Marinho Alves, Manuel Barbosa, Gilles Barthe, Luís Esquível, Vincent Hwang, Tiago Oliveira, Hugo Pacheco, Peter Schwabe, and Pierre-Yves Strub. Faster Verification of Faster Implementations: Combining Deductive and Circuit-Based Reasoning in EasyCrypt. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 3820–3838. IEEE, 2025.

[ACC+20] 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. https://tches.iacr.org/index.php/TCHES/article/view/8733.

[ACC+21] 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. https://tches.iacr.org/index.php/TCHES/article/view/9292.

[AHKS22] Amin Abdulrahman, Vincent Hwang, Matthias J. Kannwischer, and Amber Sprenkels. Faster Kyber and Dilithium on the Cortex-M4. In *Applied Cryptography and Network Security: 20th International Conference, ACNS 2022, Rome, Italy, June 20–23, 2022, Proceedings*, pages 853–871. Springer, 2022. https://link.springer.com/chapter/10.1007/978-3-031-09234-3_42.

[AHY22] 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. https://tches.iacr.org/index.php/TCHES/article/view/9823.

[BHK+21] 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. https://tches.iacr.org/index.php/TCHES/article/view/9295.

[BHK+22] 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. https://link.springer.com/chapter/10.1007/978-3-031-15255-9_1.

[CCHY24] Han-Ting Chen, Yi-Hua Chung, Vincent Hwang, and Bo-Yin Yang. Algorithmic Views of Vectorized Polynomial Multipliers – NTRU. In Anupam Chattopadhyay, Shivam Bhasin, Stjepan Picek, and Chester Rebeiro, editors, *Progress in Cryptology – INDOCRYPT 2023*, pages 177–196. Springer, 2024. https://link.springer.com/chapter/10.1007/978-3-031-56235-8_9.

[CHK+21] 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. https://tches.iacr.org/index.php/TCHES/article/view/8791.

[HKS24] 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. https://tches.iacr.org/index.php/TCHES/article/view/11926. Extended from https://eprint.iacr.org/2023/1955. Full version available at https://eprint.iacr.org/2024/1649.

[HLS+22] 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*, pages 718–750, 2022. https://tches.iacr.org/index.php/TCHES/article/view/9838.

[HLY24] 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. https://link.springer.com/chapter/10.1007/978-3-031-54773-7_2.

[Hwa24a] Vincent Hwang. A Survey of Polynomial Multiplications for Lattice-Based Cryptosystems. *IACR Communications in Cryptology*, 1(2), 2024. https://cic.iacr.org/p/1/2/1.

[Hwa24b] Vincent Hwang. Formal Verification of Emulated Floating-Point Arithmetic in Falcon. In *International Workshop on Security*, pages 125–141. Springer, 2024. https://dl.acm.org/doi/10.1007/978-981-97-7737-2_7.

[Hwa24c] 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. https://link.springer.com/chapter/10.1007/978-981-97-5028-3_5.