

Vincent Hwang

[Email](#) | [Github](#) | [Personal Website](#) | [Google Scholar](#) | [DBLP](#)

Education

PhD. Cryptographic Engineering

Max Planck Institute for Security and Privacy

Advisor: Peter Schwabe

Germany | Jan. 2023 - Now

MSc. Department of Computer Science and Information Engineering

National Taiwan University

Thesis: Case Studies on Implementing Number-Theoretic Transforms with Armv7-M, Armv7E-M, and Armv8-A
Code

Advisors: Yen-Huan Li and Bo-Yin Yang

Taiwan | Sept. 2021 - Jun. 2022

BSc. Department of Computer Science and Information Engineering

National Taiwan University

Taiwan | Sept. 2016 - Jun. 2021

Research Interests

- Assembly programming with Armv7-M, Armv7E-M, Armv8-A, AVX2
- Integer and polynomial multiplications
- Post-quantum cryptography (mainly lattice-based)
- Algorithmic partial order problems
- Graph algorithms

Programming Skills

Assembly (Armv7-M, Armv7E-M, Armv8-A, AVX2, very familiar), C (very familiar)

C++ (somewhat familiar)

Haskell (some experience)

Sevices

Reviewer of TCHES 2025, ArcticCrypt 2025, CT-RSA 2025, Crypto 2024, TCHES 2024

Artifact Review Committee member of TCHES 2023

Artifact Evaluation Committee member of TCHES 2025

Publications

- **Multiplying Polynomials without Powerful Multiplication Instructions (Long Paper)**
Vincent Hwang, YoungBeom Kim, and Seog Chung Seo
IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2025, Issue 1)
Paper Talk Slide Code Full version
- **Formal Verification of Emulated Floating-Point Arithmetic in Falcon**
Vincent Hwang
International Workshop on Security (IWSEC 2024)
Paper Talk Slide Code Full version
- **A Survey of Polynomial Multiplications for Lattice-Based Cryptosystems**
Vincent Hwang
Communications in Cryptology (CiC 2024, Issue 2)
Paper Talk Slide Code Full version
- **Pushing the Limit of Vectorized Polynomial Multiplication for NTRU Prime**
Vincent Hwang
Australasian Conference for Security and Privacy (ACISP 2024)
Paper Talk Slide Code Full version

- **Algorithmic Views of Vectorized Polynomial Multipliers – NTRU Prime**
Vincent Hwang, Chi-Ting Liu, and Bo-Yin Yang
 Applied Cryptography and Network Security (ACNS 2024)
 Paper Talk Slide Code Full version
- **Algorithmic Views of Vectorized Polynomial Multipliers – NTRU**
 Han-Ting Chen, Yi-Hua Chung, **Vincent Hwang**, and Bo-Yin Yang
 International Conference on Cryptology in India (INDOCRYPT 2023)
 Paper Talk Slide Code Full version
- **Verified NTT Multiplications for NISTPQC KEM Lattice Finalists: Kyber, SABER, and NTRU**
Vincent Hwang, Jiaxiang Liu, Gregor Seiler, Xiaomu Shi, Ming-Hsien Tsai, Bow-Yaw Wang, and Bo-Yin Yang
 IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2022, Issue 4)
 Paper Talk Slide Code Full version
- **Multi-Parameter Support with NTTs for NTRU and NTRU Prime on Cortex-M4**
 Erdem Alkim, **Vincent Hwang**, and Bo-Yin Yang
 IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2022, Issue 4)
 Paper Talk Slide Code Full version
- **Efficient Multiplication of Somewhat Small Integers using Number-Theoretic Transforms (Best Paper Award)**
 Hanno Becker, **Vincent Hwang**, Matthias J. Kannwischer, Lorenz Panny, and Bo-Yin Yang
 International Workshop on Security (IWSEC 2022)
 Paper Talk Slide Code Full version
- **Faster Kyber and Dilithium on the Cortex-M4**
 Amin Abdulrahman, **Vincent Hwang**, Matthias J. Kannwischer, and Daan Sprenkels
 Applied Cryptography and Network Security (ACNS 2022)
 Paper Talk Slide Code Full version
- **Neon NTT: Faster Dilithium, Kyber, and Saber on Cortex-A72 and Apple M1**
 Hanno Becker, **Vincent Hwang**, Matthias J. Kannwischer, Bo-Yin Yang, and Shang-Yi Yang
 IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2022, Issue 1)
 Paper Talk Slide Code Full version
- **Multi-moduli NTTs for Saber on Cortex-M3 and Cortex-M4**
 Amin Abdulrahman, Jiun-Peng Chen, Yu-Jia Chen, **Vincent Hwang**, Matthias J. Kannwischer, and Bo-Yin Yang
 IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2022, Issue 1)
 Paper Talk Slide Code Full version
- **NTT Multiplication for NTT-unfriendly Rings**
 Chi-Ming Marvin Chung, **Vincent Hwang**, Matthias J. Kannwischer, Gregor Seiler, Cheng-Jhih Shih, and Bo-Yin Yang
 IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2021, Issue 2)
 Paper Talk Slide Code Full version
- **Polynomial Multiplication in NTRU Prime**
 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
 IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2021, Issue 1)
 Paper Talk Slide Code Full version

Technical Reports