Cesare Huang

Taipei, Taiwan | cesarehuang@icloud.com | cheng-wei-huang0612.github.io | 黃承瑋

github.com/cheng-wei-huang0612

Research Interests

Post-quantum cryptography; computational number theory; high-performance computing; low-level program optimization.

Research Experience

Institute of Information Science, Academia Sinica, Research Assistant — Aug 2024 – Present

- Develop high-performance, constant-time AArch64/NEON implementations of number-theoretic algorithms, with a focus on SafeGCD-based modular inversion.
- Verify low-level cryptographic implementations with CryptoLine or HOL Light, depending on the task.

Publications

Accelerating and verifying constant-time modular inversion. Daniel J. Bernstein, Han-Ting Chen, John R. Harrison, **Cesare Huang**, Gregory Maxwell, Bow-Yaw Wang, Pieter Wuille, and Bo-Yin Yang. 2026

- *Advances in Cryptology – EUROCRYPT 2026, Part VII*, LNCS 16547, pp. 598–627.
- Developed and formally verified the Armv8-A SafeGCD implementation.

Preprints

Strided Frobenius Additive FFT and its Application to HQC. Ming-Shing Chen, Tun-You Chien, Chun-Ming Chiu, **Cesare Huang**, Han-Hsuan Lin, Chun-Tao Peng, and Bo-Yin Yang. 2026

- *Cryptology ePrint Archive*, Paper 2026/1588. Preprint.
- Co-developed the algebraic theory of SFAFFT using quotient-ring isomorphisms and the Chinese Remainder Theorem to generalize FAFFT to strided and incomplete transforms. Authored the mathematical exposition and proofs.

Multiplying Not-So-Big Integers with FFTs
Finding and Pushing the Crossover on Large Modern OoO ARM CPUs
Cesare Huang, Daisy Meng-Wei Liu, David Shu-Yu Wu, Bow-Yaw Wang, and Bo-Yin Yang.

- *Cryptology ePrint Archive*, Paper 2026/2366. Preprint.
- Provided technical direction on AArch64 assembly optimization and formal verification, guiding two interns in the use of SLOTHY, CryptoLine, and HOL Light.

safeRNSgcd: Accelerating Falcon key generation with RNS in SafeGCD
Cesare Huang and Bo-Yin Yang.

- *Cryptology ePrint Archive*, Paper 2026/2507. Preprint.
- Designed an RNS-based SafeGCD algorithm, reducing Falcon-512/1024 private-key basis-generation cycles by 4–7% on Raspberry Pi 5, 12–15% on AMD EPYC 9754, and 9–12% on Intel Xeon Silver 4509Y versus half-ntrugen, a baseline with the same required output.

Education

National Taiwan University, B.S. in Mathematics — Sept 2020 – June 2024

Technical Skills

Programming: C, Python, AArch64/NEON assembly
Verification and optimization: CryptoLine, HOL Light, SLOTHY, qhasm

Talks

Accelerating and Verifying Constant-Time Modular Inversion May 2026
Conference presentation, EUROCRYPT 2026.

SafeGCD (Bernstein–Yang Inversion) Oct 2025
Invited lecture, cryptographic engineering course, National Taiwan University.

Number Theoretic Transform Aug 2025
Invited lecture, Core Program, ZK Education.

Teaching and Academic Service

IEEE Transactions on Computers, Peer Reviewer 2026

Topics in Cryptanalysis, Teaching Assistant Feb 2026 – June 2026

Cryptographic Engineering, Teaching Assistant Sep 2025 – Dec 2025

Post-Quantum Cryptography, Teaching Assistant Feb 2025 – June 2025

Quantum Information and Computation, Teaching Assistant Feb 2024 – June 2024

Mentorship

Academia Sinica, Summer Intern Program July 2025 – July 15, 2026

- Mentored two interns in AArch64 assembly programming and efficient big-integer multiplication, resulting in the coauthored preprint *Multiplying Not-So-Big Integers with FFTs* (ePrint 2026/2366).

Open-Source Contributions

SLOTHY Assembly Optimizer link

- Contributed AArch64 instruction-parser definitions and microarchitectural parameters.

last update: Nov 2026