

Junhao Huang

Phone: +86-18626423381, Email: jhhuang_nuaa@126.com

Homepage: <https://junhaohuang.github.io/>

Postal Address: Department of Electrical Engineering, City University of Hong Kong,
83 Tat Chee Avenue, Kowloon, Hong Kong SAR

Postal code: 999077



Education

- | | |
|--|-------------------------------|
| • Beijing Normal-Hong Kong Baptist University | Supervisor: Dr. Donglong Chen |
| <i>PhD Degree of Computer Science (Hong Kong Baptist University)</i> | <i>Sep. 2021-Jul. 2025</i> |
| • Nanjing University of Aeronautics and Astronautics | Supervisor: Prof. Zhe Liu |
| <i>Master Degree of Cyberspace Security</i> | <i>Sep. 2018-Jun. 2021</i> |
| • Nanjing University of Aeronautics and Astronautics | GPA: 3.7 |
| <i>Bachelor Degree of Computer Science and Technology</i> | <i>Sep. 2014-Jun. 2018</i> |

Research/Visiting Activities

- | | |
|--|----------------------------|
| • Research Assistant, Electrical Engineering | Hong Kong, China |
| <i>City University of Hong Kong (Prof. Ray C.C. Cheung)</i> | <i>Oct. 2025-Now</i> |
| • IACR CHES 2025 Artifact Evaluation Committee | Kuala Lumpur, Malaysia |
| <i>International Association for Cryptologic Research (IACR)</i> | <i>Oct. 2024-Oct. 2025</i> |
| • IACR CHES 2024 Artifact Evaluation Committee | Halifax, Canada |
| <i>International Association for Cryptologic Research (IACR)</i> | <i>Oct. 2023-Oct. 2024</i> |
| • Visiting Scholar, Electrical Engineering | Hong Kong, China |
| <i>City University of Hong Kong (Prof. Ray C. C. Cheung)</i> | <i>Jul. 2023-Dec. 2023</i> |
| • Visiting Scholar, Cyberspace Security | Wuhan, China |
| <i>Wuhan University (Prof. Debiao He)</i> | <i>Sep. 2019-Jan. 2020</i> |

Scientific Services

I have been actively participating as a reviewer for the following journals/conferences:

- *ACM Transactions on Architecture and Code Optimization (TACO).*
- *The Journal of Supercomputing.*
- *Journal of Cryptographic Engineering (JCEN).*

Research Interests

- Modular Arithmetic, Lattice-based Cryptography, Fully Homomorphic Encryption, ARM & RISC.

Research Projects/Proposals

- **Research on Real-Time Privacy-Preserving Sign Language Translation and Production**

Guangdong & Hong Kong Universities Cross-Campus Research Collaboration Project 2024-2027

- Proposal writing & Main participant
- Secure the sensitive information in AI models with lattice-based FHE
- Efficient lattice-based FHE and privacy-preserving techniques on end-to-end platforms
- One publication in ACM SIGMETRICS 2025

- **Heterogeneous Platform Optimization for Lattice-based Privacy Computing System**

Guangdong Provincial Natural Science Foundation-General Project 2024-2026

- Proposal writing & Main participant
- Efficient and side-channel secure lattice-based cryptographic scheme Raccoon in IoT platforms
- RISC-V customized instruction set design for Plantard arithmetic and lattice-based schemes
- One publication in IEEE TC 2025

- **Efficient, Lightweight, and Multi-platform Lattice-based Cryptosystems**

CCF-Zhejiang Laboratory Joint Innovation Fund 2023-2024

- Proposal writing & Main participant
- Further improve Plantard arithmetic, Keccak and Dilithium on 32-bit ARM and RISC-V platforms
- Two publications in IEEE TIFS 2024 & IACR TCHES 2024

- **Software/Hardware Co-design of Lattice-Based Cryptosystems Computing Platforms**

National Nature Science Fund of China 2021-2023

- Main participant
- Proposed an improved Plantard arithmetic and efficient lattice-based cryptographic implementations on ARM Cortex-M4
- One publication in IACR TCHES 2022

Representative Publications (Total Publications: 15)

1. **Junhao Huang**, Haosong Zhao, Jipeng Zhang, Wangchen Dai, Lu Zhou, Çetin Kaya Koç, Ray C.C. Cheung, Donglong Chen*, Yet another Improvement of Plantard Arithmetic for Faster Kyber on Low-end 32-bit IoT Devices, *IEEE Transactions on Information Forensics & Security*, 2024. (**CCF-A & JCR Q1**)

2. **Junhao Huang**, Alexandre Adomnicăi, Jipeng Zhang, Wangchen Dai, Yao Liu, Ray C. C. Cheung, Çetin Kaya Koç, Donglong Chen*, Revisiting Keccak and Dilithium Implementations on ARMv7-M, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2024. (**CCF-B & Top-tier conference in cryptographic engineering**)
3. **Junhao Huang**, Jipeng Zhang, Haosong Zhao, Zhe Liu, Ray C. C. Cheung, Çetin Kaya Koç, Donglong Chen*, Improved Plantard Arithmetic for Lattice-based Cryptography, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022. (**CCF-B & Top-tier conference in cryptographic engineering**)
4. **Junhao Huang**, Zhe Liu*, Zhi Hu, and Johann Großschädl, Parallel Implementation of SM2 Elliptic Curve on Intel Processor with AVX2, *Australasian Conference on Information Security and Privacy - ACISP 2020*. (**CCF-C**)
5. Zewen Ye, **Junhao Huang**, Tianshun Huang, Yudan Bai, Jinze Li, Hao Zhang, Guangyan Li, Donglong Chen, Ray CC Cheung, Kejie Huang, PQNTRU: Acceleration of NTRU-based Schemes via Customized Post-Quantum Processor[J]. *IEEE Transactions on Computers*, 2025 (**CCF-A**)
6. Haosong Zhao, **Junhao Huang**, Zihang Chen, Kunxiong Zhu, Donglong Chen, Zhuoran Ji, Hongyuan Liu, VESTA: A Secure and Efficient FHE-based Three-Party Vectorized Evaluation System for Tree Aggregation Models[C]. *ACM SIGMETRICS*, 2025 (**CCF-B**)
7. Jipeng Zhang, Yuxing Yan, **Junhao Huang**, Çetin Kaya Koç*, Optimized Software Implementation of Keccak, Kyber, and Dilithium on RV{32,64}IM{B}{V}, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025. (**CCF-B & Top-tier conference in cryptographic engineering**)
8. Jipeng Zhang, **Junhao Huang**, Lirui Zhao, Donglong Chen, Çetin Kaya Koç*, ENG25519: Faster TLS 1.3 handshake using optimized X25519 and Ed25519, *Usenix Security*, 2024. (**CCF-A & Top-tier conference in security & Distinguished Paper Award**)
9. Jipeng Zhang, **Junhao Huang**, Zhe Liu*, Sujoy Sinha Roy, Time-memory Trade-offs for Saber on Memory-constrained RISC-V, *IEEE Transactions on Computers*, 2022. (**CCF-A**)
10. Xinyi Ji, Jiankuo Dong, **Junhao Huang**, Zhijian Yuan, Wangchen Dai, Fu Xiao, Jingqiang Lin, ECO-CRYSTALS: Efficient Cryptography CRYSTALS on Standard RISC-V ISA, *IEEE Transactions on Computers*, 2024. (**CCF-A**)

Awards

- Dec. 2024 **First prize** of Guangdong Province Computer Society Outstanding Paper Award.
- Aug. 2024 **Distinguished Paper Award** of the 33rd USENIX Security Symposium.
- May. 2023 **Third prize** of Guangdong Province Cyberspace Security Outstanding Paper Award.
- Oct. 2018 Postgraduate **First prize** Scholarship
- Oct. 2018 **First Prize** of Academic Scholarship

Academic Referee

1. **Dr. Donglong Chen:** Associate Professor of Beijing Normal-Hong Kong Baptist University,
donglongchen@uic.edu.cn
2. **Prof. Ray C.C. Cheung:** Associate Provost, Professor of City University of Hong Kong,
r.cheung@cityu.edu.hk
3. **Prof. Çetin Kaya Koç:** IEEE Life Fellow, Co-founder of CHES, University of California Santa Barbara,
cetinkoc@ucsb.edu