

Junhao Huang

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

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



Education

- **Beijing Normal-Hong Kong Baptist University**
PhD Degree of Hong Kong Baptist University
Supervisor: Dr. Donglong Chen
Sep. 2021-now
- **Nanjing University of Aeronautics and Astronautics**
Master Degree of Cyberspace Security
Supervisor: Prof. Zhe Liu
Sep. 2018-Jun. 2021
- **Nanjing University of Aeronautics and Astronautics**
Bachelor Degree of Computer Science and Technology
GPA: 3.7
Sep. 2014-Jun. 2018

Research/Visiting Activities

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

Research Interests

- Lattice-based Cryptography, Fully Homomorphic Encryption, ARM, RISC-V.

Research Projects/Proposals

- **Research on Real-Time Privacy-Preserving Sign Language Translation and Production**
Guangdong and Hong Kong Universities "1+1+1" Cross-Campus Research Collaboration Scheme
2024-2027
 - Proposal writing & Main participant
 - Secure the sensitive information in AI models with lattice-based fully-homomorphic encryption (FHE)
 - Efficient lattice-based FHE and privacy-preserving techniques on end-to-end platforms
 - One publication in ACM SIGMETRICS 2025
- **Heterogeneous Platform Optimization for Post-quantum 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
 - Two papers submitted to TCHES 2025 and IEEE TC 2025
- **Research on Efficient and Lightweight Multi-platform Implementation of Lattice-based Cryptosystems**
CCF-Zhejiang Laboratory Joint Innovation Fund 2023-2024
 - Proposal writing & Main participant
 - Further improve Plantard arithmetic and extend it to other schemes and 32-bit platforms
 - Two publications in IEEE TIFS 2024 & IACR TCHES 2024
 - **Research on Software/Hardware Co-design of Computing Platform for Lattice-Based Cryptosystems**
National Nature Science Fund of China 2021-2023
 - Main participant
 - Proposed an improved Plantard arithmetic for efficient lattice-based cryptographic implementation
 - One publication in IACR TCHES 2022

Representative Publications (Total Publications: 13)

1. **Junhao Huang**, Jipeng Zhang, Weijia Wang, Xuan Yu, Donglong Chen*, Efficient High-order Masking Raccoon on ARM Cortex-M4[J]. **(In Submission)**
2. 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)**
3. 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)**
4. **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)**
5. **Junhao Huang**, Alexandre Adomnică, 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)**
6. **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)**
7. 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)**

8. Jipeng Zhang, Yuxing Yan, **Junhao Huang**, 蔡etin Kaya Ko莽*, 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)
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 & JCR Q1)
10. **Junhao Huang**, Zhe Liu*, Zhi Hu, and Johann Gro脗sch盲dl, Parallel Implementation of SM2 Elliptic Curve on Intel Processor with AVX2, *Australasian Conference on Information Security and Privacy - ACISP 2020*. (CCF-C)
11. 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 & JCR Q1)

Academic Referee

1. **Dr. Donglong Chen**: Associate Professor of BNU-HKBU United International College, 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. etin Kaya Ko**: IEEE Life Fellow, Co-founder of CHES, Professor of University of California Santa Barbara, cetinkoc@ucsb.edu