

Junhao Huang

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

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



Education

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

Research Interest

- Cryptographic Engineering, Post-quantum Cryptography, Lattice-based Cryptography, Modular Arithmetic.

Representative Publications (Total: 13)

1. Yet another Improvement of Plantard Arithmetic for Faster Kyber on Low-end 32-bit IoT Devices,
Junhao Huang, Haosong Zhao, Jipeng Zhang, Wangchen Dai, Lu Zhou, Çetin Kaya Koç, Ray C.C. Cheung, Donglong Chen*.
In [IEEE Transactions on Information Forensics & Security, 2024](#). (CCF-A, 安全顶刊)
2. Revisiting Keccak and Dilithium Implementations on ARMv7-M,
Junhao Huang, Alexandre Adomnicăi, Jipeng Zhang, Wangchen Dai, Yao Liu, Ray C. C. Cheung, Çetin Kaya Koç, Donglong Chen*.
In [IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024](#). (CCF-B, 密码顶会)
3. Improved Plantard Arithmetic for Lattice-based Cryptography,
Junhao Huang, Jipeng Zhang, Haosong Zhao, Zhe Liu, Ray C. C. Cheung, Çetin Kaya Koç, Donglong Chen*.
In [IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022](#). (CCF-B, 密码顶会)

4. ENG25519: Faster TLS 1.3 handshake using optimized X25519 and Ed25519,
Jipeng Zhang, **Junhao Huang**, Lirui Zhao, Donglong Chen, Çetin Kaya Koç*.
In [Usenix Security, 2024](#). (CCF-A, 安全四大顶会, Distinguished Paper Award)
5. Optimized Software Implementation of Keccak, Kyber, and Dilithium on RV{32,64}IM{B}{V},
Jipeng Zhang, Yuxing Yan, **Junhao Huang**, Çetin Kaya Koç*.
In [IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025](#). (CCF-B, 密码顶会)
6. ECO-CRYSTALS: Efficient Cryptography CRYSTALS on Standard RISC-V ISA.
Xinyi Ji, Jiankuo Dong, **Junhao Huang**, Zhijian Yuan, Wangchen Dai, Fu Xiao, Jingqiang Lin.
In [IEEE Transactions on Computers, 2024](#). (CCF-A)
7. Time-memory Trade-offs for Saber on Memory-constrained RISC-V,
Jipeng Zhang, **Junhao Huang**, Zhe Liu*, Sujoy Sinha Roy.
In [IEEE Transactions on Computers, 2022](#). (CCF-A)
8. Parallel Implementation of SM2 Elliptic Curve on Intel Processor with AVX2.
Junhao Huang, Zhe Liu*, Zhi Hu, and Johann Großschädl.
In [Australasian Conference on Information Security and Privacy - ACISP 2020](#). (CCF-C)

Research Activities

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

Honor Certificates

- Aug. 2024 **Distinguished Paper Award** of the 33rd USENIX Security Symposium.
- May. 2023 Third prize for the Guangdong Province Cyberspace Security Outstanding Paper Award, GDCA.
- Apr. 2023 Best RPG Poster Award of Faculty of Science & Technology, BNU-HKBU UIC.

Professional Skills

1. Language Level: CET-4: 597, CET-6: 513, IELTS: 7.0
2. Skills: C/C++, x86-64, ARM, RISC-V, AVX2, CUDA, Python