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/Visiting Activities

- **IACR CHES 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*

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
- **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 side-channel secure lattice-based scheme Raccoon (Submitted to TCHES2025)
- **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 TIFS2024 & IACR TCHES2024
- **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 and efficient Plantard arithmetic for lattice-based cryptography
- One publication in IACR TCHES2022

Research Interests

- Cryptographic Engineering, Lattice-based Cryptography, Modular Arithmetic, ARM & RISC-V.

Representative Publications (Total Publications: 13)

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 & SCI I**)
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. 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**)
6. 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**)
7. 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 & SCI II**)

Academic Referee

1. **Dr. Donglong Chen**: Associate Professor of BNU-HKBU United International College, donglongchen@uic.edu.cn
2. **Prof. Çetin Kaya Koç**: IEEE Life Fellow, Co-founder of CHES, University of California Santa Barbara, cetinkoc@ucsb.edu