Junhao Huang (黄军浩)

PhD Student, +86-18626423381, jhhuang_nuaa@126.com

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**
  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 publications: 12)

1. Yet another Improvement of Plantard Arithmetic for Faster Kyber on Low-end 32-bit IoT Devices,
   Junhao Huang et al.
   In IEEE Transactions on Information Forensics & Security, 2024. (**CCF-A, 信息安全顶刊**)
2. Revisiting Keccak and Dilithium Implementations on ARMv7-M,
   Junhao Huang et al.
   In IACR Transactions on Cryptographic Hardware and Embedded Systems, Volume 2024, Issue 2. (**CCF-B, 密码顶会**)
3. Improved Plantard Arithmetic for Lattice-based Cryptography,
   Junhao Huang et al.
   In IACR Transactions on Cryptographic Hardware and Embedded Systems, Volume 2022, Issue 4. (**CCF-B, 密码顶会**)
4. ENG25519: Faster TLS 1.3 handshake using optimized X25519 and Ed25519,
   Jipeng Zhang, **Junhao Huang** et al.
   In Usenix Security, 2024. (**CCF-A, 安全四大顶会, 杰出论文奖**)
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, Volume 2025, Issue 1 (**CCF-B, 密码顶会**)

6. ECO-CRYSTALS: Efficient Cryptography CRYSTALS on Standard RISC-V ISA,
   Xinyi Ji, Jiankuo Dong, **Junhao Huang** et al.
   In IEEE Transactions on Computers, 2024. (**CCF-A, SCI二区**)
7. Time-memory Trade-offs for Saber on Memory-constrained RISC-V,
   Jipeng Zhang, **Junhao Huang** et al.
   In IEEE Transactions on Computers, 2022 (**CCF-A, SCI二区**)
8. Parallel Implementation of SM2 Elliptic Curve on Intel Processor with AVX2.
   Junhao Huang et al.
   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*

Academic Referee

1. Dr. Donglong Chen: Associate Professor, Associate Head of BNU-HKBU United International College.
2. Prof. Çetin Kaya Koç: IEEE Life Fellow, Co-founder of CHES, University of California Santa Barbara.
3. Prof. Ray C.C. Cheung: Professor, Associate Provost of City University of Hong Kong.