Junhao Huang

PhD Student
BNU-HKBU United International College, Zhuhai, China
18626423381
huangjunhao@uic.edu.cn

Education

- **BNU-HKBU United International College** — Supervisor: Dr. Donglong Chen
  PhD student at Data Science and Technology — *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, Public-key Cryptography, Lattice-based Cryptography.

Research Activities

- **Teaching Assistant** — Zhuhai, China
  BNU-HKBU United International College, Computer and Network Security — *Sep. 2021-Now*
- **Research Assistant** — Whuhan, China
  Wuhan University, Cryptography and Blockchain Technology Lab — *Sep. 2019-Jan. 2020*

Publications

- Journal Publications

1. 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**)
2. 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**)
3. High-Speed AVX2 Implementation of AKCN-MLWE,
   YANG Hao, LIU Zhe, **HUANG Jun-Hao**, SHEN Shi-Yu ZHAO Yun-Lei.
   In Chinese Journal of Computers, 2021

- Conference Publications

1. Efficient Implementation of Kyber on Mobile Devices,
   Lirui Zhao, Jipeng Zhang, **Junhao Huang**, Zhe Liu, Gerhard Hancke,
   In IEEE International Conference on Parallel and Distributed Systems - ICPADS 2021 (**CCF-C**)
2. 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**)
3. An Efficient and Scalable Sparse Polynomial Multiplication Accelerator for LAC on FPGA,
   Jipeng Zhang, Zhe Liu, Hao Yang, **Junhao Huang**, Weibin Wu.
   In IEEE International Conference on Parallel and Distributed Systems - ICPADS 2020 (**CCF-C**)

Honor Certificates

- Nov.2019 Patent for An efficient implementation of Co-Z based Montgomery ladder algorithm using AVX2, CN112367172A.
- Oct. 2018 Postgraduate **First prize** Scholarship
- Oct. 2018 **First Prize** of Academic Scholarship
- Jun. 2018 Software Copyright for the University Association Information Management System
- Oct. 2017 National Encouragement Scholarship, **Third Prize** of Outstanding Student Scholarship
- Oct. 2016 National Encouragement Scholarship, **Second Prize** of Outstanding Student Scholarship
- Oct. 2015 National Encouragement Scholarship, **First Prize** of Outstanding Student Scholarship

Professional Skills

1. Language Level: CET-4: 597, CET-6: 513, **IELTS: 7.0**
2. Programming Language: C/C++, x86-64/Cortex-M4/Cortex-M3/RISC-V Assembly, AVX2 and CUDA programming, Python