

Junhao Huang

PhD Student

BNU-HKBU United International College, Zhuhai, China

18626423381

huangjunhao@uic.edu.cn



Education

- **BNU-HKBU United International College**
PhD student at Data Science and Technology
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 Interest

- Cryptographic Engineering, Public-key Cryptography, Lattice-based Cryptography.

Research Activities

- **Teaching Assistant**
BNU-HKBU UIC, Operating Systems, Dr. Sunny Seon Phil JEONG
Zhuhai, China
Feb. 2023-Jun. 2023
- **Teaching Assistant**
BNU-HKBU UIC, Computer and Network Security, Dr. Donglong Chen
Zhuhai, China
Sep. 2021-Dec. 2021
- **Research Assistant**
Wuhan University, Cryptography and Blockchain Technology Lab
Wuhan, China
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 \(CCF-C\)](#)

Reaserch Experiences

- Sep. 2022-Mar. 2023, Faster Kyber Implementation on Cortex-M3 and RISC-V
 - Further extend the input range of the improved Plantard arithmetic tailored for Kyber.
 - Efficient NTT/INTT implementation on Cortex-M3 and RISC-V.
 - Speed-ups for Kyber on Cortex-M3 and RISC-V.
- Sep. 2021-Apr. 2022, Improved Plantard Arithmetic for Lattice-based Cryptography
 - Present an improved Plantard arithmetic tailored for LBC.
 - Obtained speed-ups for Kyber and NTTTRU with 16-bit NTT on Cortex-M4.
 - The source code has been merged into pqm4, PR#244 (merged at 25th, Oct, 2022).
- Dec. 2020-Apr. 2021, Memory Efficient Implementation of Saber on RISC-V
 - Reduce the memory usage of Saber by using a **just-in-time** public matrix, secret, and noise generation technique.
 - Represent the secret, and noise with a new **smaller data-type**, which reduces the size of the secret and noise.
- Apr. 2019-Nov. 2020, Accelerating ECC utilizing the Double Precision Floating-point Number on GPU
 - Implement the prime field arithmetic for the prime modulus $p = 2^n - \delta$ by combining the computing power of **the fused multiply-add instruction of double-precision floating-point number** and the addition, subtraction, and shift instructions of integer number.
 - Propose how to perform multi-precision multiplication over unreduced-form big number, which optimizes the point multiplication, especially Montgomery ladder algorithm for Montgomery curves, with the **lazy reduction technique**.
- Apr. 2019-Oct. 2019, Parallel Implementation of SM2 Elliptic Curve with AVX2
 - Utilize SIMD AVX2 instruction set to implement 2-way SM2 prime field operations.
 - Reschedule the (X,Y)-only Co-Z Jacobian arithmetic and perform the symmetric operations using the 2-way prime field operations
 - Implement the Co-Z based Montgomery ladder algorithm based on the parallel Co-Z Jacobian arithmetic.
 - The number of the 2-way prime field operations of the Co-Z Jacobian arithmetic is reduced to a half compared to the sequential implementation.

- The AVX2 version Co-Z based Montgomery ladder algorithm is **1.31** times faster than the X64 assembly implementation.

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