

Junhao Huang

PhD Student

BNU-HKBU United International College, Zhuhai, China

+86-18626423381

jhuang_nuaa@126.com, 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

- **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** Wuhan, China
Wuhan University, Prof. Debiao He Sep. 2019-Jan. 2020

Publications

- Journal Publications

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)
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](#), Volume 2024, Issue 2. (CCF-B)

3. Research on Efficient Implementation of SM2 for Mobile Devices.
Jipeng Zhang, **Junhao Huang**, Xuan Yu, Zhe Liu*.
In [Acta Electronica Sinica](#).
4. 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, Volume 2022, Issue 4. \(CCF-B\)](#)
5. 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 \(CCF-A\)](#)
6. 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. 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. \(CCF-A\)](#)
2. 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. \(CCF-C\)](#)
3. 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. \(CCF-C\)](#)
4. 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

- Jul. 2023- Oct. 2023, Revisiting Keccak and Dilithium Implementations on ARMv7-M
 - Further improve Keccak’s performance using lazy rotation and better memory access scheduling on ARMv7-M.
 - Efficient multi-moduli NTT with Plantard arithmetic for the small polynomial multiplication in Dilithium on ARM Cortex-M3.
 - Obtain large speed-ups for Keccak and Dilithium on Cortex-M3 and Cortex-M4.
- Sep. 2022- Mar. 2023, Yet another Improvement of Plantard Arithmetic for Faster Kyber on Low-end 32-bit IoT Devices
 - 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

- 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.
- 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