Junhao Huang
Master Degree
Nanjing University of Aeronautics and Astronautics, Nanjing, China
jhhuang_nuaa@126.com

Education

- Nanjing University of Aeronautics and Astronautics — Supervisor: Prof. Zhe Liu
  Master Degree of Cyberspace Security — Sep. 2018-now
- 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

- Research Assistant — Whuhan, China
  Wuhan University, Cryptography and Blockchain Technology Lab — Sep. 2019 - Jan. 2020

Publication

1. 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
2. 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
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
4. Time-memory Trade-offs for Saber on Memory-constrained RISC-V,
   Jipeng Zhang, Junhao Huang, Zhe Liu, Sujoy Sinha Roy.
   To be in IACR Transactions on Cryptographic Hardware and Embedded Systems (Major Revision)

Reaserch Experiences

- Dec. 2020-now 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.
- Sep. 2019-Mar. 2020 Accelerating SM2 on GPU
  - Implement the prime field arithmetic for SM2 using the low-level PTX assembly language on GPU, which contributes to the performance of the high-level point arithmetic and cryptographic protocols of SM2.
- 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 Assembly, AVX2 and CUDA programming, Python

Self Introduction

I have been implementing elliptic curve cryptography since I was a graduate student. I tried to implement SM2 and other elliptic curves using different languages on different platforms, i.e. C, x86-64 assembly language, AVX2 on CPU, and CUDA programming on GPU. During the 5-month exchange study at Wuhan University, Lattice-based Cryptography and Blockchain are two other research areas of my interest. Recently, I've been trying to implement Kyber on a RISC-V chip, which further expands my experiences on cryptographic engineering.