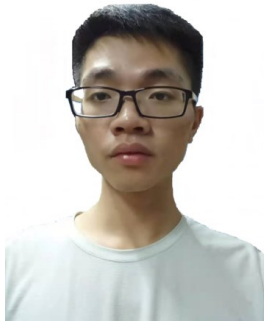
Department of Electrical Engineering
香港城市大學
City University of Hong Kong

**CityU Architecture Lab for Arithmetic and Security (CALAS) Seminar Series**

# PQNTRU: Acceleration of NTRU-based Schemes via Customized Post-Quantum Processor

Zewen Ye, PhD Student

Supervisor: Prof. Ray C.C. CHEUNG, Prof. Kejie Huang



## Abstract:

Post-quantum cryptography (PQC) has rapidly evolved in response to the emergence of quantum computers, with the US National Institute of Standards and Technology (NIST) selecting four finalist algorithms for PQC standardization in 2022. The latest round of digital signature schemes introduced Hawk, both based on the NTRU lattice, offering compact signatures, fast generation, and verification suitable for deployment on resource-constrained Internet-of-Things (IoT) devices. Despite the popularity of Crystal-Dilithium and Crystal-Kyber, research on NTRU-based schemes has been limited due to their complex algorithms and operations. Falcon and Hawk's performance remains constrained by the lack of parallel execution in crucial operations like the Number Theoretic Transform (NTT) and Fast Fourier Transform (FFT), with data dependency being a significant bottleneck. We enhances NTRU-based schemes Falcon and Hawk through hardware/software co-design on a customized Single-Instruction-Multiple-Data (SIMD) processor, proposing new SIMD hardware units and instructions to expedite these schemes along with software optimizations to boost performance. Our NTT optimization includes a novel layer merging technique for SIMD architecture to reduce memory accesses, and the use of modular algorithms (Signed Montgomery and Improved Plantard) targets various modulus data widths to enhance performance. We explore applying layer merging to accelerate fixed-point FFT at the SIMD instruction level and devise a dual-issue parser to streamline assembly code organization to maximize dual-issue utilization. A System-on-chip (SoC) architecture is devised to improve the practical application of the processor in real-world scenarios.

## Biography:

Zewen Ye received his bachelor's degree in microelectronics science and engineering from Zhejiang University in 2020. He is currently pursuing a joint PhD degree at Zhejiang University and the City University of Hong Kong, advised by Prof. Kejie Huang and Prof. Ray C. C. Cheung. His research interests include post-quantum cryptography, hardware design and RISC-V.

14 April 2025 (Mon); 9:00pm - 11:30pm; P4704; https://cityu.zoom.us/j/89767977156