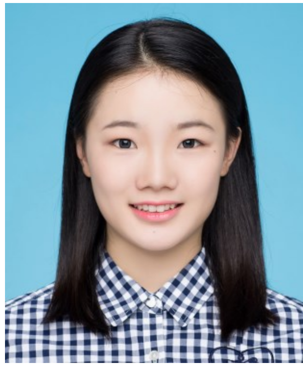
Department of Electrical Engineering
香港城市大學
City University of Hong Kong

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



High-Performance Implementation of ML-DSA on ARMv9-A Architecture

Hanyu WEI, PhD Candidate
Supervisor: Prof. Yunlei ZHAO, Fudan University

Abstract:

As quantum computing advances, traditional public-key cryptosystems are becoming increasingly vulnerable, prompting a global shift toward post-quantum cryptography (PQC). Integrating PQC into high-performance platforms is a critical objective for both cryptographers and system architects. ARM has become one of the mainstream processor architectures, and the growing adoption of ARMv9-A is accelerating the development of modern workloads such as artificial intelligence and cloud computing. Supported by the Scalable Vector Extension 2 (SVE2) and the Scalable Matrix Extension (SME), ARMv9-A enables high-performance computing and requires cryptographic solutions specifically optimized for its architecture. We present an efficient implementation of ML-DSA, the post-quantum digital signature algorithm standardized by NIST and recommended for general use, on the ARMv9-A architecture. We redesign the polynomial computation pipeline to align with scalable vector and parallel execution capabilities. This includes optimized modular arithmetic and high-throughput polynomial multiplications. To further harness data-level parallelism, we propose to utilize two variants of the number-theoretic transform (NTT): the merged NTT and the decomposed NTT. To the best of our knowledge, this is the first work to implement and evaluate ML-DSA using SVE2 and SME optimizations on real ARMv9-A hardware, providing a practical foundation for future PQC deployments on ARM-based platforms.

Biography:

Ms. Hanyu WEI received her bachelor’s degree in Cyber Science from Southeast University in 2022. She is currently a Ph.D. candidate at Fudan University, advised by Prof. Yunlei Zhao. Her research interests include post-quantum cryptography and cryptographic engineering.

6 October, 2025 (Mon); 2pm – 4pm; P1402; https://cityu.zoom.us/j/96742093029