Bowen ZHANG

bowen.zhang.002@student.uni.lu

Education

University of Luxembourg, M.Sc. in Computer Sciences (cryptography track). Sept. 2023 – Sept. 2025

- Grade: 16.4/20 (très bien)

Northwestern Polytechnical University, B.Eng. in Information Security. Sept. 2018 – July 2022

- Grade: 85.44/100

Professional Experiences

Student Research Assistant Nov. 2023 - Sept. 2024
APSIA, SnT, University of Luxembourg - Esch-sur-Alzette, Luxembourg

- Extended the AVXECC [link here] project, developed the Ed25519 verification software in AVX2, and AVX512 extensions.

Research Experiences

Masking UOV Feb. 2025 - Sept. 2025
Supervised by **Jean-Sébastien Coron** and **François Gerard**

- Designed new gadgets for securely solving linear equations system in UOV-like signatures.
- Proved the security of our new techniques in the t-probing model.
- Implemented our fully masked UOV signature scheme at first- and high-order, which achieves a significant improvement in CPU cycles compared with previous masked implementations.

Source code will be released soon.

Masking NewHope Oct. 2024 - Jan. 2025
Supervised by **François Gerard**

- Implemented the high-order masking on NewHope-CPA-PKE.
- Implemented the masked ciphertext comparison in the NewHope IND-CCA KEM.

Source code available at: https://github.com/zh-bw/Masking-NewHope

High-Throughput Ed25519 using SIMD intrinsics Nov. 2023 - Sept. 2024
Supervised by **Hao Cheng** and **Johann Großschädl**

- Developed the first throughput-optimized implementation of the Ed25519 signature verification, which exceeds the throughput of the currently-best latency-optimized implementation by a factor of 1.33.
- Analyzed different algorithms for double-scalar multiplication to identify the best implementation option for maximizing throughput.

Source code available at: https://github.com/zh-bw/AVXEd25519

Papers

- **Bowen Zhang**, Hao Cheng, Johann Großschädl, Peter Y. A. Ryan. High-Throughput EdDSA Verification on Intel Processors with Advanced Vector Extensions. *SAC 2025*.
- Jinhui Liu, Jiaming Wen, **Bowen Zhang** et al. A post quantum secure multi-party collaborative signature with deterability in the Industrial Internet of Things. *Future Generation Computer Systems 141 (2023): 663-676.*

Skills

Language: English (C1), Chinese (native).
Programming skills: C (familiar), Python (somewhat familiar), LaTeX (somewhat familiar), SageMath (some experience).