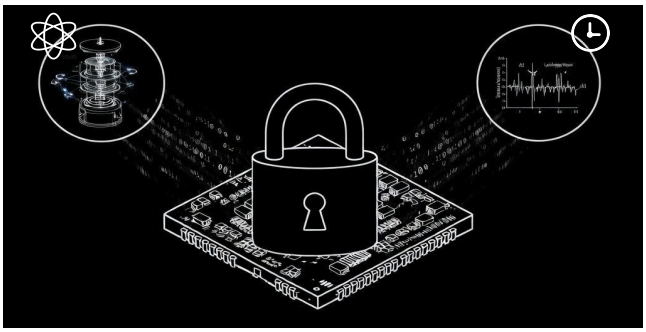
Constant-Time Instructions for Post-Quantum Cryptography on RISC-V



As quantum computing advances, currently deployed public-key cryptography is expected to become vulnerable. In response, the cryptographic community is transitioning toward quantum-resistant algorithms collectively known as post-quantum cryptography (PQC). In 2025, the National Institute of Standards and Technology standardized two lattice-based schemes for general-purpose use: CRYSTALS-Kyber (also known as ML-KEM) for key establishment and CRYSTALS-Dilithium (also known as ML-DSA) for digital signatures[1]. Because these schemes are expected to be widely deployed and are computationally more expensive than classical cryptography, efficient hardware support is increasingly important.

Despite protection against quantum adversaries, PQC remains vulnerable to classical *side-channel attacks*. In particular, the realistic threat of *timing* side-channel attacks has forced all PQC schemes to support *constant-time* implementations. Constant-time execution ensures that all observable timing behavior is independent of secret data. However, achieving this property is not purely an algorithmic concern: it emerges from the interaction between compiler, instruction set, and hardware micro-architecture. While several tools exist to verify timing-independent behavior of software, techniques for validating this property in cryptographic hardware remain surprisingly underexplored.

This thesis starts out with implementing RISC-V instruction set extensions for processors to accelerate the known bottlenecks in lattice-based schemes. A central challenge is ensuring that these accelerators preserve constant-time execution, when integrated into the processor. The project will therefore develop a robust methodology to validate constant-time behavior in hardware, possibly combining formal verification, simulation-based analysis, and statistical timing tests. The goal is to establish practical techniques for verifying constant-time properties of hardware cryptographic accelerators. Students are encouraged to contact the supervisors if they are interested in the topic.

Practicalities

Promoter:	Ingrid Verbauwhede		
Daily supervisor:	Eden Desmet	eden.desmet@esat.kuleuven.be	office 01.18
	Suparna Kundu	suparna.kundu@esat.kuleuven.be	office 01.20
Nature of the work:	25% literature, 75% applied work		
Number of students:	1		

[1] https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/selected-algorithms