A Post-Quantum Secure RISC-V application core for IoT: from hardware design to applications

Candidate: Alessandra Dolmeta

The emergence of quantum computing threatens to undermine the security foundations of modern cryptographic systems, calling for the adoption of Post-Quantum Cryptography (PQC) schemes resistant to quantum attacks. At the same time, the Internet of Things (IoT) ecosystem demands efficient and low-power solutions that can ensure secure communication even on resource-constrained devices. This thesis addresses this dual challenge by proposing a series of Post-Quantum Secure RISC-V application cores, specifically tailored for IoT environments, combining architectural flexibility with cryptographic robustness.

The work systematically explores the hardware–software co-design of PQC primitives across multiple integration paradigms, from loosely coupled accelerators to tightly coupled coprocessors. Leveraging the open RISC-V ISA and the Core-V eXtension Interface (CV-X-IF), the proposed framework enables efficient offloading of computationally intensive PQC kernels while preserving software transparency and full ISA compliance. The study encompasses several NIST-standardized algorithms, including ML-KEM (Kyber), ML-DSA (Dilithium), SLH-DSA (SPHINCS+), and HQC, as well as their building blocks such as Keccak, NTT/INTT, and modular reduction operations.

Four major architectures were developed and evaluated throughout this work: KRONOS, a unified SHA-3/Keccak accelerator integrated via multiple coupling strategies; LOKI and KALIPSO, lightweight NTT/INTT accelerators for ML-KEM; ATHOS, a hybrid multi-accelerator framework that unifies loosely and tightly coupled designs within a single SoC to demonstrate modularity and scalability; and TYRCA, a tightly-coupled HQC accelerator showcasing the flexibility and efficiency of the CV-X-IF interface across code-based cryptography.

Building upon these developments, the thesis culminates with HORCRUX, the final proposed architecture that achieves the best trade-off between performance and area efficiency. HORCRUX integrates a dedicated Instruction Set Extension (ISE) specifically designed for Post-Quantum Cryptography, enabling hardware acceleration of all NIST-standardized PQC algorithms within a unified RISC-V framework. This final design represents the convergence of the previous explorations, providing a consistent, secure, and efficient hardware substrate for next-generation quantum-resilient IoT systems.

Keywords: Post-Quantum Cryptography, Hardware Design, RISC-V, Accelerators Integration, Instruction Set Extension