HW implementations for Post-Quantum Cryptography

Classic asymmetric cryptography is based on mathematical problems like discrete logarithm or integer factorization. With large-scale quantum computers, these problems can be solved in very short time, which causes a serious threat to cryptographic systems.

Post-Quantum Cryptography (PQC) describes cryptographic approaches that are secure even in the presence of such quantum computers. To evaluate the security and efficiency of such systems, NIST started a competition that aims to define a new standard [1].

Depending on the scope of this work, the goal is to implement HW accelerators for commonly used operations in PQC, integrate them into a RISC-V environment and evaluate their impact on performance for PQC.


Prerequisites

Ideally, you should have knowledge of the following:

- A hardware description language like VHDL/Verilog/SystemVerilog
- Experience running simulations using ModelSim
- Basic C programming skills

Contact

patrick.karl@tum.de

Advisors

Patrick Karl