Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis, Master's Thesis

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.

[1] https://csrc.nist.gov/projects/post-quantum-cryptography

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
- Basic knowledge of post-quantum cryptography as taught as e.g. in Quantum Computers and Quantum Secure Communications

Contact

If you are interested in the topic, please send a CV and your transcript of records to:
patrick.karl@tum.de

Advisors

Patrick Karl