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

Forschungspraxis, Master's Thesis

Post-Quantum Crypto on RISC-V

As the ongoing development of quantum computers poses a significant threat to classic assymetric cryptography, new approaches for assymetric encryption and signatures need to be developed. These post-quantum secure cryptography can be grouped into different subsets, among them schemes based on lattices, error-correcting codes, isogenies or multivariate equations.

The NIST (National Institute of Standards and Technology) chose 3 lattice-based Post-Quantum secure algorithms for standardization in July 2022.

The goals of this work is to implement one these algorithms on a State-of-the-Art RISC-V platform and evaluate its potential for hardware acceleration as well as its side-channel resilience.

References:

NIST Round 3 Report

Prerequisites

- Very good programming skills in C and RISC-V assembly
- Experience in hardware design with VHDL or SystemVerilog

Contact

Jonas Schupp

Advisors

Jonas Schupp