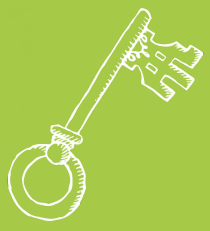


RISC-V instruction set extension for SQIsign acceleration

Advisor: **Maciej Czuprynko**

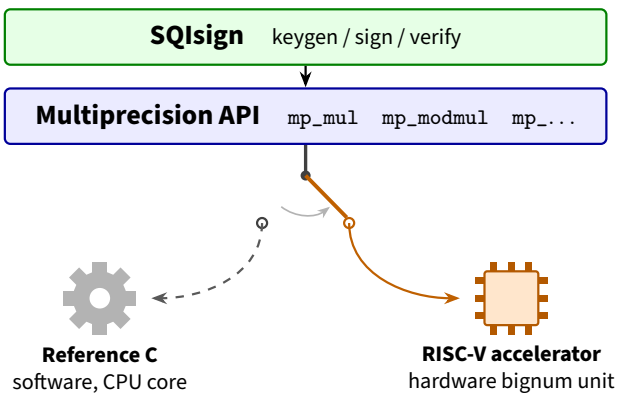
Motivation

A sufficiently powerful quantum computer would break today's digital signature schemes. In response, NIST launched a call for post-quantum signatures, prompting several new candidates. One of them, SQIsign, is an isogeny-based scheme with the most compact keys and signatures, but it relies on demanding large-integer arithmetic that requires a multiprecision library.

Open-source RISC-V platforms often include big-number accelerators for RSA and ECC, whose instruction sets are tailored to classical cryptography. This project investigates how an instruction set extension (ISE) for such an accelerator can speed up SQIsign.

Goals and Tasks

- Understand SQIsign's multiprecision bottlenecks and the target accelerator's architecture.
- Design and implement new instructions in the RTL, simulator, and toolchain.
- Adapt the multiprecision library to use them.
- Benchmark cycle count and hardware cost against the baseline.



Literature

- Example RISC-V bignum accelerator (Open Titan) https://opentitan.org/book/hw/ip/otbn/
- SQIsign multiprecision library https://github.com/SQISign/the-sqisign/blob/main/src/mp/ref/lvlx/mp.c

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in Post Quantum Cryptography
- Knowledge of Python, C/C++ and an HDL language
- Experience with FPGAs

Advisor Contact

maciej.czuprynko@tugraz.at