

Implementing SQIsign on the ESP32

Advisor: **Maciej Czuprynko**

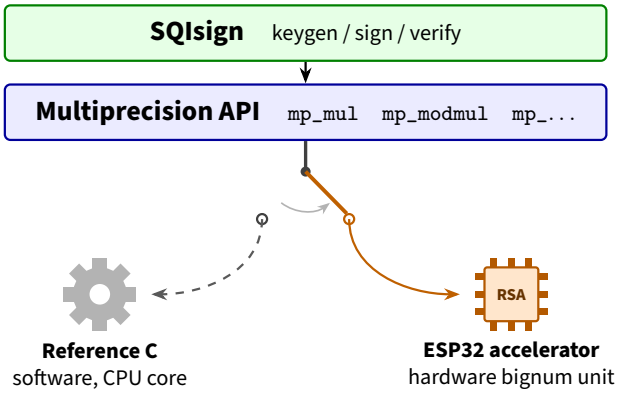
Motivation

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.

Many current microcontrollers already include hardware accelerators for RSA and ECC. Since these schemes also operate on large integers, their accelerators effectively support bignum operations such as multiplication, modular multiplication, and modular exponentiation. This project investigates how far such hardware, designed for classical cryptography, can accelerate SQIsign.

Goals and Tasks

- Understand the operations that need to be modified and the ESP32 bignum library.
- Modify the reference multiprecision library to use the ESP32 bignum library.
- Benchmark the two implementations.



Literature

- EPS32 bignum library
  https : / / mbed - tls . readthedocs . io / projects/api/en/v3.6.5/api/file/bignum_8h/#
- 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 and C/C++

Advisor Contact

maciej.czuprynko@tugraz.at