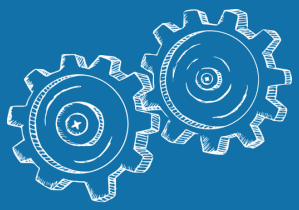


PQCRYPTO algorithms in WebAssembly

Advisor: **Lukas Prokop**

Motivation

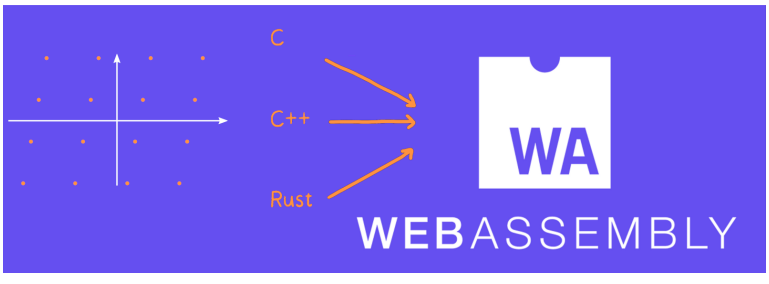
The Post-Quantum Standarization competition has reached its third round. Few algorithms are left as finalists to be standardized and real-world implementations are emerging. In this thesis, we want to broaden the field of implementations.

WebAssembly (WASM) is a portable binary-code format for executable programs including a textual representation for programs. The main goal of WASM is to enable high-performance applications on web pages, but the format is designed to be executed and integrated in other environments as well, including standalone ones.

The idea of this project is to take PQCRYPTO algorithm implementations (e.g. Kyber or Saber) and compile them for WASM targets. Besides potential non-optimality of compiler output, security issues such as random number generation need to be considered and evaluated. The second step is thus an evaluation of the status quo of WASM runtimes. Depending on the student's interest, we can put a focus on optimization (w.r.t. memory or runtime) or recommendations to increase security in the WASM runtime.

Goals and Tasks

- Compile rust/C/pqm4 implementation to WASM
- Verify correctness in browser setup
- Optimize or evaluate security in WASM



PQCRYPTO to WebAssembly

Literature

- NIST
  Post-Quantum Cryptography | CSRC
  https : / / csrc . nist . gov / Projects / post - quantum-cryptography/
- W. CG
  WebAssembly
  https://webassembly.org/

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
- Interest in compilers and native code

Advisor / Contact

lukas.prokop@iaik.tugraz.at