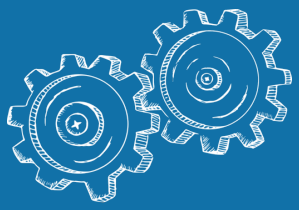


PQCRYPTO in rusttls

Advisor: **Lukas Prokop**

Motivation

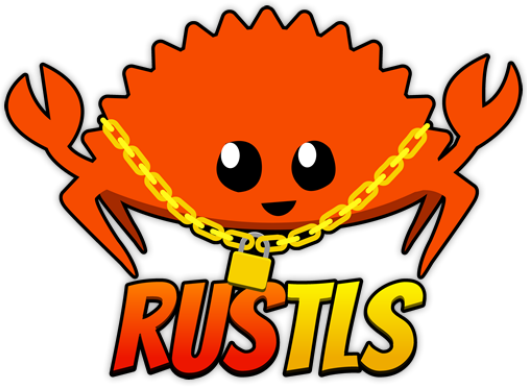
Rustls is a modern TLS library written in Rust. It's pronounced 'rustles'. It uses ring for cryptography and libwebpki for certificate verification. In June 2020, rustls received a security audit. The audit document reads,

> *The team of auditors considered the general code quality to be exceptional and can attest to a solid impression left consistently by all scope items.*

However, unlike the competitors OpenSSL and mbedTLS, rustls does not have any experimental PQCRYPTO support yet. The goal of this master thesis is to extend rustls for post-quantum cryptographic algorithms.

Goals and Tasks

- Sum up approaches to bring PQCRYPTO to TLS
- Implement feasible approach in rustls
- Evaluate performance and reason about security



rustls project logo

Literature

- P. Schwabe, D. Stebila, and T. Wiggers
  Post-quantum TLS without handshake signatures
  https://eprint.iacr.org/2020/534
  2020
- C. Paquin, D. Stebila, and G. Tamvada
  Benchmarking Post-quantum Cryptography in TLS
  PQCrypto

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 the rust language
- Interest in IT-Security
- Interest in PQCRYPTO

Advisor / Contact

lukas.prokop@iaik.tugraz.at