ARMed NTRU Prime - Post-Quantum Key-Encapsulation on Embedded Devices

Advisor(s): Peter Pessl

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Quantum-secure cryptography has gained a lot of momentum, with many new constructions proposed in the last few years. A large number of these constructions are based on lattices with special structures. While this additional structure allows efficient implementation, it also casts some doubt on their post-quantum security.
Recently, a new algorithm called NTRU Prime was proposed. It does not utilize such a structure, but requires new implementation techniques for its main component, a polynomial multiplication. The aim of this project to design an efficient implementation of this new scheme. The target platform are ARM Cortex-M microcontrollers, which, due to their limited resources, are an especially interesting platform for development.

Goals and Tasks

- Read into lattice-based cryptography and NTRU Prime
- Evaluate different methods for efficient polynomial multiplication
- Implement your design for an ARM microcontroller
- Compare your implementation to other constructions

Literature

- D. J. Bernstein et al.
  NTRU Prime
  IACR Cryptology ePrint Archive 2016
  http://eprint.iacr.org/2016/461

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- C/C++ programming
- Assembly programming

Advisor / Contact

peter.pessl@iaik.tugraz.at