Post-Quantum Key-Exchange for FPGAs

Advisor(s): Peter Pessl

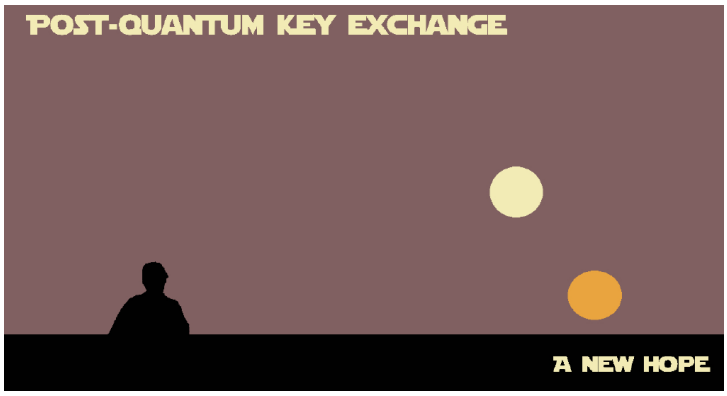
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Most modern public-key cryptosystems, such as RSA and ECC, are vulnerable to quantum computing. Although large quantum computers do not yet exist, the search for post-quantum alternatives has gained a lot of momentum. Especially cryptography based on lattices is a promising candidate.
Recently, a lattice-based key-exchange algorithm (named "A New Hope") was proposed. This algorithm is currently evaluated by Google and tested in their Chrome browser. Software implementation of "A New Hope" look promising, yet there are no results for hardware yet. The aim of this project is to change that, i.e., to create an efficient hardware (FPGA) implementation of this key-exchange algorithm.

Goals and Tasks

- Read into implementation techniques of lattice-based cryptography
- Evaluate different implementation options and optimization possibilities
- Implement "A New Hope" and run it on an FPGA



Researchers can be nerds. [1]

Literature

- E. Alkim et al.
  Post-quantum Key Exchange - A New Hope
  USENIX 2016

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

- VHDL programming

Advisor / Contact

peter.pessl@iaik.tugraz.at