Side-channel Analysis of a Post-Quantum Signature Scheme

Advisor(s): Peter Peßl and Sebastian Ramacher

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

Motivation

Side-channel attacks have proven to be powerful tools to attack implementations of cryptosystems. For example, they allow to deduce secret key material by monitoring memory access, runtime characteristics, or power consumption.
The National Institute of Standards and Technology started a project to collect and standardize post-quanatum public-key cryptographic algorithms such as digital signature schemes and public-key encryption schemes. The digital signature scheme Picnic, which was submitted as part of this effort, bases its security guarantees on symmetric-key primitives such as block ciphers. In particular, it uses a relatively new designed named LowMC.
The goal of this project is to analyse potential side channel attack vectors on LowMC itself as well as its application in Picnic.

Goals and Tasks

- Getting familiar with the signature scheme and its building blocks.
- Implement the building blocks on a micro controller.
- Investigate side-channel attacks and counter-measures.

Literature

- M. Chase et al.
  Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives
  CCS
- M. R. Albrecht et al.
  Ciphers for MPC and FHE
  EUROCRYPT (1)

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

- Basic cryptographic background
- Programming

Advisor / Contact

sebastian.ramacher@iaik.tugraz.at