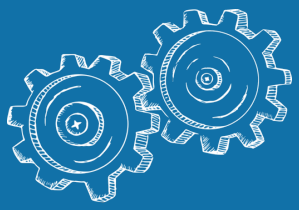

Unified hardware design for Reed Solomon and Spielman Encoding

Advisor: **Florian Hirner**

Motivation

Zero-knowledge Proofs (ZKP) allow a prover to produce a proof about some statement without revealing any secret witness. In the literature, many kinds of ZKPs have been proposed in recent years. A class of ZKP schemes use encoding using the Number Theoretic Transform or Spielman error correcting encoding. Such encoding is very slow and hence hardware acceleration is playing a crucial role in making these ZKPs practical. The goal of this thesis+project is to design a unified hardware design for both types of encoding.

Goals and Tasks

Some specific goals of this project are:

- Understand NTT and Spielman encoding
- Design a new unified core for arithmetic
- Use SystemVerilog to describe the core
- Perform benchmark using FPGA tool-based simulation

- Get familiar with ZKP framework
- Propose & implement hardware architecture for unified encoding
- Experimentally evaluate
- Compare your results with related works

Literature

- OpenNTT source code
  https://github.com/flokrieger/OpenNTT
- F. Hirner et al.
  Orion's Ascent: Accelerating Hash-Based Zero Knowledge Proof on Hardware Platforms
  IACR Cryptol. ePrint Arch. 2024
  https://eprint.iacr.org/2024/1918

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in efficient hardware design
- Cryptography on Hardware Platforms course is highly recommended

Advisor Contact

florian.Hirner@tugraz.at