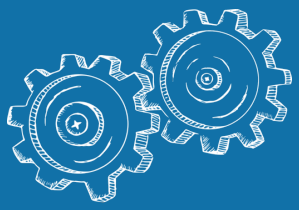

Extending the OpenNTT Framework

Advisor: **Florian Krieger**

Motivation

The Number Theoretic Transform is a crucial operation in many cryptographic schemes. To accelerate this heavy-weight computation, we developed OpenNTT, an open-source toolchain for NTT designs.

OpenNTT is a fully automated framework to generate high-performance and efficient hardware modules for NTT acceleration on FPGAs. This project is very flexible and aims to extend OpenNTT's capabilities for different aspects, like side-channel countermeasures, a wider parameter set, or more power/energy efficient designs.

Goals and Tasks

Some specific goals of this project are:

- Extend OpenNTT's parameter set for Zero-Knowledge Proofs
- Integrate new modular reduction methods
- Find efficient energy or power trade-offs
- Implement side-channel countermeasures + experimental evaluation

- Get familiar with the NTT and the OpenNTT framework
- Propose & implement new functionality for OpenNTT
- Optional: Evaluate the side-channel resistance of your implementation
- Compare your results to other configurations and related works

Literature

- OpenNTT source code
  https://github.com/flokrieger/OpenNTT
- F. Krieger et al.
  A Flexible Hardware Design Tool for Fast Fourier and Number-Theoretic Transformation Architectures
  IEEE TCAD 2025
  doi:10.1109/TCAD.2025.3595834

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.krieger@tugraz.at