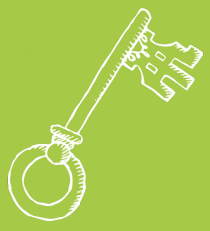


Lattice-Based Zero Knowledge Proofs

Advisor: **Anisha Mukherjee & Selim Kirbiyik**

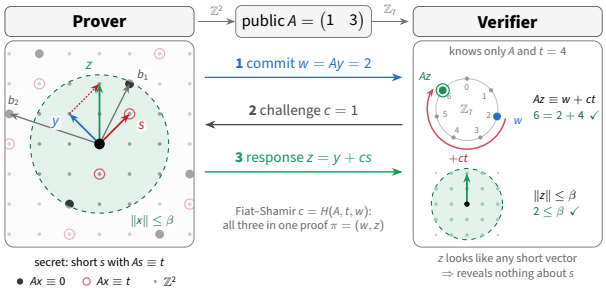
Motivation

Zero-Knowledge proofs are an advanced cryptographic primitive that allows a party to prove with high confidence that they hold a secret witness. Recently there has been increasing interest in making these proof systems post-quantum secure. Lattice-based problems such as SIS and LWE are behind the NIST standardized PQC algorithms such as ML-KEM, ML-DSA, and modern Fully Homomorphic Encryption schemes. There are numerous attempts at building post-quantum proof systems using lattices, but there is no systematic overview and comparison of these schemes.

In this project you will answer the question 'How well does lattice-based proof systems perform?'. Using lattice-based proof systems in group signatures or verifying non-trivial relations is of interest.

Goals and Tasks

- Systematically categorize lattice-based proof systems
- Identify the building blocks
- Perform a trade-off analysis of lattice-based proof systems
- Improve upon the existing lattice-based proof systems



An example Lattice Based ZKP interaction

Literature

- H. Perez
  Lattice-Based ZK Explained
  2025
  zkv.xyz/lattice-based-zk-explained/
- N. K. Nguyen and G. Seiler
  Greyhound: Fast Polynomial Commitments from Lattices
  2024

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 ☑ MATH

Prerequisites

- Interest in lattice-based cryptography
- Programming (C/C++, Python)

Advisor Contact

firstname.lastname@tugraz.at