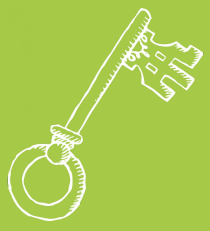


# ZK-friendly PQ KEMs

Advisor: **Verena Schröppel**

## Motivation

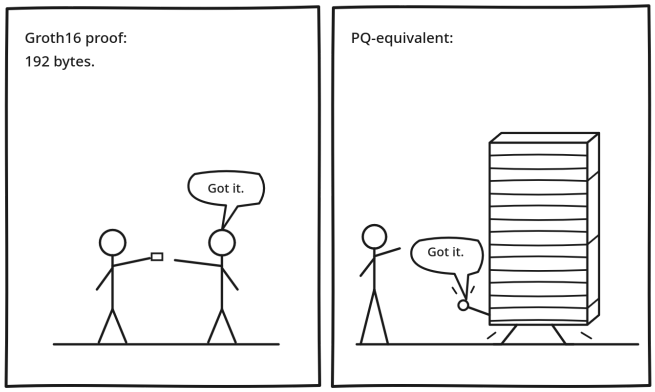
**Post-quantum cryptography** is becoming an increasingly important part of modern secure communication. At the same time, many applications require more than simply executing a cryptographic protocol: they need to provide *verifiable* evidence that a computation was performed correctly, while keeping sensitive information private.

**Zero-knowledge proofs** provide a natural way to achieve this. However, integrating post-quantum cryptographic primitives into proof systems introduces new challenges, as algorithms designed for efficient conventional execution are not necessarily efficient when represented as verifiable computations.

In this thesis, you will investigate the integration of a post-quantum **key encapsulation mechanism** into a zero-knowledge proof system, evaluate its practical costs, and explore approaches for making such cryptographic computations more suitable for efficient verification.

## Goals and Tasks

- Study Key Encapsulation Mechanisms such as ML-KEM and proof systems.
- Implement a PQ KEM inside a proof system.
- Propose and evaluate design changes that make the KEM cheaper to prove.




## Literature


- J. Bos et al.
  CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM
  IEEE EuroS&P 2018
- M. Bellés-Muñoz et al.
  Circom: A Circuit Description Language for Building Zero-Knowledge Applications
  IEEE Transactions on Dependable and Secure Computing 2023


## 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 lattice cryptography and ZK proofs
- Motivation to implement modern protocols

## Advisor Contact

verena.schroeppel@tugraz.at