



Zero Knowledge Proofs and their Applications

Advisor: **Shibam Mukherjee**

Motivation

A zero-knowledge proof (ZKP) protocol allows a prover \mathcal{P} to convince a verifier \mathcal{V} the validity of a statement, using a public input (public data and the circuit) and potentially private witness data such that the public input reveals no information about the statement.

For instance, \mathcal{P} may want to convince \mathcal{V} that they know a preimage x such that $y = H(x)$ for a publicly known value y and a cryptographic hash function H .



A similar approach is also used for modern post-quantum signature schemes like Picnic, Banquet, Helium, FAEST, especially the ones based on MPCitH and VOLEitH ZKP paradigms. Moreover, ZKP also finds its application in many industries like blockchain, decentralized apps, anonymous credentials, crypto-assets, verifiable computation and decentralized storage, among others.

In your thesis, you will

- > Read about the underlying primitives in depth.
- > Discuss the possible limitations (even security vulnerabilities?) and scope of improvement in the existing protocols
- > Implement your ideas and discuss the results

Contact to discuss further about the topic specifics and your personal interest.

Goals and Tasks

-  Understand the open problems and the underlying primitives
-  Implement and discuss the solution

Literature

- > *depends on topic*

Courses & Deliverables

- Master Project**
Project code
Report
Presentation
- OR –
- Master's Thesis + DiplomandInnenseminar (CS)**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

- CS
- ICE
- SEM

Prerequisites

- > Interest in PETs and Cryptography (Recommended)
- > Familiarity with C,C++ or Rust

Advisor Contact

shibam.mukherjee@iaik.tugraz.at