Efficient Zero-Knowledge Proof Systems

Advisor: **Shibam Mukherjee**

Motivation

A zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that something is true, without revealing any information apart from the fact that this specific statement is true. In the recent years, several flavors of ZKP systems have appeared with their own merits and use-cases. In your thesis, you will

> Explore one of the ZKP techniques and implement parts of proof system

We are open to further discussions, please feel free to contact me.

Goals and Tasks

📕 Understand ZKP

🛠 Implement and evaluate a ZK proof system

Literature

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

☑ **Bachelor Project**
Project code and documentation

☑ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

> PETs, Cryptography or Cryptanalysis

Advisor Contact

shibam.mukherjee@tugraz.at