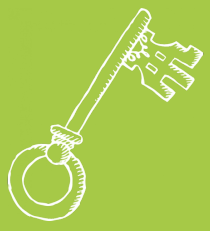

Evaluating Primitives for Efficient coSNARKs

Advisor: **Florian Lugstein, Fabian Schmid**

Motivation

Zero-knowledge proofs (ZKPs) in the form of SNARKs are versatile cryptographic tools for proving statements about secret data without revealing the secrets. They allow us to build fundamental cryptographic protocols and privacy-preserving applications for digital identity or blockchain systems.

While traditional SNARKs are limited to a single party, collaborative SNARKs (coSNARKs) allow multiple parties to jointly prove statements about their individual secrets. In addition to enabling new types of applications, coSNARKs can mitigate efficiency issues on constrained devices by securely outsourcing proof computation.

To achieve this, coSNARKs combine ZKPs with multi-party computation (MPC). A major challenge for designing efficient coSNARKs lies in finding building blocks that are simultaneously ZKP- and MPC-friendly.

The research goal is to explore and evaluate the suitability of cryptographic primitives such as hash functions for their use in efficient coSNARK protocols.

Goals and Tasks

- Learn the basics of SNARK and MPC protocols
- Get familiar with existing implementations and understand their performance bottlenecks
- Implement and benchmark a candidate primitive in a SNARK or MPC system

Literature

- A. Ozdemir and D. Boneh
  Experimenting with collaborative zk-SNARKs: Zero-Knowledge proofs for distributed secrets
  USENIX Security 22
  https://eprint.iacr.org/2021/1530

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

- Interest in efficient implementations of advanced cryptographic protocols
- Programming (Rust or C/C++)

Advisor Contact

florian.lugstein@tugraz.at