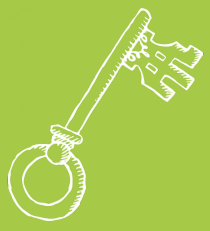


Private Proof Outsourcing for the EU Digital Identity Wallet

Advisor: **Florian Lugstein**

Motivation

The upcoming *EU Digital Identity (EUDI) Wallet* will store credentials like your ID card on your phone. With *zero-knowledge proofs*, the wallet can show "I am over 18" without revealing anything else. Proof systems such as **Crescent**, **Longfellow**, **Vega**, and **OpenAC** already do this for today's ECDSA-signed credentials.

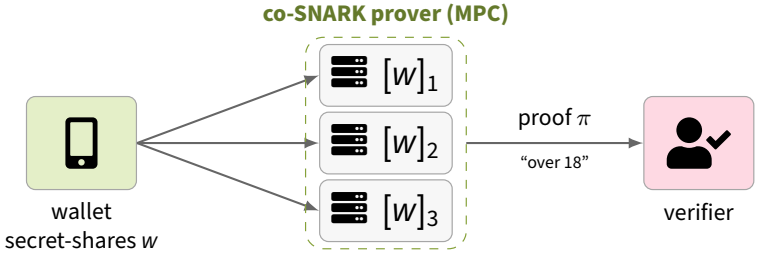
However, each credential is bound to a **device key** stored in the phone's secure hardware, so that it cannot be copied to another device. Since this hardware supports only a fixed set of algorithms such as ECDSA, proofs become more expensive, post-quantum signatures are not yet possible, and phones without certified hardware are excluded.

Collaborative SNARKs (co-SNARKs) could lift this restriction: several servers hold the credential and device key in secret-shared form and jointly compute the proof using *multi-party computation* (MPC).

In this thesis, you will explore how **MPC-friendly** existing credential proof systems are, and whether co-SNARKs could enable cheaper and hardware-independent proofs.

Goals and Tasks

- Learn how EUDI credentials, device binding, and co-SNARKs work
- Compare credential proof systems in MPC
- Build a prototype and find out when it beats proving on the phone



Outsourcing the proof without giving up privacy.

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
- M. Frigo and abhi shelat
  Anonymous Credentials from ECDSA
  Cryptology ePrint Archive 2024
  https://eprint.iacr.org/2024/2010

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 ZKPs and MPC
- Programming (Rust)

Advisor Contact

florian.lugstein@tugraz.at