



Extending zkSNARK-Based Anonymous Credentials with Pseudonym Proofs

Advisor: **Dmytro Shvets**

Motivation

In recent years, there have been significant advances in *zkSNARK-based anonymous credentials*, making them practical and compatible with existing digital credentials. The upcoming rollout of the *EU Digital Identity Wallet* (EUDIW) has further increased interest in frameworks such as **Longfellow**, **Vega**, and **OpenAC**.

These frameworks enable the presentation of credentials via *zero-knowledge proofs* (ZKPs), which allow users to prove a statement about their credential, e.g., that they are older than 18, without revealing the credential itself or any other attributes. However, their proofs are “basic”: they lack advanced functionality expected in the EUDIW, such as *credential-bound pseudonyms*. Although mechanisms for proving pseudonym-related statements with ZKPs have been described, they have not yet been thoroughly evaluated in practice.

In this project, you will study the inner workings of **Vega** and **OpenAC**, extend them to prove statements about pseudonyms, and evaluate the overhead incurred by pseudonym proofs compared to standard (zero-knowledge) credential presentation.

Goals and Tasks

-  Learn how the selected frameworks work
-  Extend the existing proofs (and circuits) with pseudonym statements
-  Compare the overhead to standard presentations

Literature

- > [L. Eagen et al.](#)
OpenAC: Open Design for Transparent and Lightweight Anonymous Credentials
[IACR Cryptol. ePrint Arch. 2026](#)
<https://eprint.iacr.org/2026/251>
- > [D. Kaviani and S. Setty](#)
Vega: Low-Latency Zero-Knowledge Proofs over Existing Credentials
[IEEE SP 2026](#)
<https://doi.org/10.1109/SP63933.2026.00182>

Courses & Deliverables

- ☒ **Master Project**
Project code
Report
Presentation

Recommended if you're studying

- ☒ CS ☒ ICE ☒ SEM

Prerequisites

- > Interest in ZKPs
- > Programming (Rust)

Advisor Contact

dmytro.shvets@tugraz.at