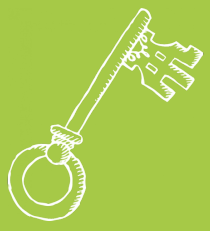

Verifiable LEAP

Advisor: **Lena Heimberger**

Motivation

LEAP [1] is a blazingly fast *oblivious pseudorandom function* (OPRF) built from lattices. It is actually a cool showcase for post-quantum cryptography, as it shows that lattice cryptography can be faster than elliptic curves (at the cost of higher communication).

OPRFs have many use-cases, from private set intersection (where LEAP excels) to private single-sign on and anonymous credentials. This is where a major drawback of LEAP becomes obvious: It is not *verifiable*, which means that the client cannot be sure a pre-committed key was used. If the server uses a special key for each client, the privacy guarantees fall, as the server may be able to distinguish the client from other clients.

This is where you come in: we have a number of nice (pre-quantum) zero-knowledge proofs. Harness them to get a verified version of LEAP.

In your thesis, you will

- Learn about LEAP and general-purpose zero-knowledge proofs.
- Discuss the possible limitations (even security vulnerabilities?) and scope of improvement in the existing protocols.
- Implement your ideas and discuss the results.

Contact me to discuss further about the topic specifics and your personal interest. Please note that I am on **leave from July until end of October**.

Goals and Tasks

- Understand LEAP and the necessary zero-knowledge proofs.
- Implement and discuss the verifiable solution.

Literature

- L. Heimberger et al.
  Leap: A Fast, Lattice-Based OPRF with Application to Private Set Intersection
  Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part VII
  doi:10.1007/978-3-031-91098-2_10
  https://doi.org/10.1007/978-3-031-91098-2_10

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

Advisor Contact

lena.heimberger@tugraz.at