



Verifiable Leap with Zero-Knowledge Proofs

Advisor: **Lena Heimberger** heimberger.xyz/supervision.html

Motivation

The OPRF Leap is currently among the fastest OPRFs in the world. While the construction is very simple, a few attacks can result in malicious users or servers leaking information they should not have. The objective of the thesis is to integrate a modern zero-knowledge proof system (such as STARKs, but you are free to explore others) with the Leap protocol. You will design and implement a protocol extension that makes Leap's operations verifiable without revealing any secret information. This project has direct applications in privacy-preserving authentication and other systems where trustless verification is critical.

In your thesis, you will

- > Study a specific lattice attack.
- > Analyze its applicability to Leap.
- > Implement your own approximation script for small-moduli LWR cryptography.

Goals and Tasks

-  Understand a specific lattice attack and its constraints.
-  Understand Leap.
-  Implement the attack and verify existing implementations.

Literature

- > [M. R. Albrecht et al.](#)
Estimate All the {LWE, NTRU} Schemes!
SCN 2018
[doi:10.1007/978-3-319-98113-0_19](https://doi.org/10.1007/978-3-319-98113-0_19)
- > [A. Banerjee et al.](#)
SPRING: Fast Pseudorandom Functions from Rounded Ring Products
FSE 2014
[doi:10.1007/978-3-662-46706-0_3](https://doi.org/10.1007/978-3-662-46706-0_3)
- > [L. Heimberger et al.](#)
Leap: A Fast, Lattice-Based OPRF with Application to Private Set Intersection
EUROCRYPT 2025
[doi:10.1007/978-3-031-91098-2_10](https://doi.org/10.1007/978-3-031-91098-2_10)

Courses & Deliverables

- ☒ **Master's Thesis**
 - Initial presentation
 - Project code
 - Thesis (60+ pages)
 - Final presentation

Recommended if you're studying

- ☒ CS ☒ ICE ☒ SEM

Prerequisites

- > I am on leave until the 3rd of November. Please read the note on supervision on heimberger.xyz/supervision.html.

Advisor Contact

lena.heimberger@tugraz.at