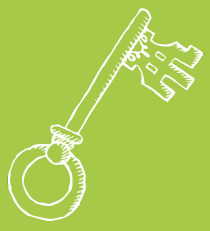

Cryptanalyzing Leap

Advisor: **Lena Heimberger**

Motivation

The OPRF Leap is currently among the fastest OPRFs in the world. While the construction is very simple, its non-standard parameter regime is a challenge since traditional cryptanalysis frameworks, like the lattice estimator does not give reliable results for the specific parameter regime used in Leap.

You will conduct a practical cryptanalysis of Leap. You will select a known lattice attack (e.g., Primal or Dual attack), study it in depth, and implement it. The goal is to apply your implementation to the specific instances of Leap and test their concrete security.

Note: This project is ideal for a combination of ISW, project and thesis, as it involves both a significant implementation component and a theoretical write-up.

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
- A. Banerjee et al.
  SPRING: Fast Pseudorandom Functions from Rounded Ring Products
  FSE 2014
  doi: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

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 ☑ MATH

Prerequisites

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