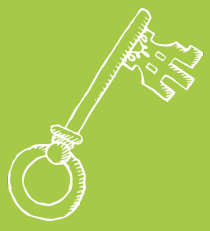

Applications for the GL Homomorphic Encryption Scheme

Advisor: **Florian Krieger**

Motivation

Fully Homomorphic Encryption (FHE) is a highly relevant technique allowing computations on encrypted data. The Gentry-Lee (GL) scheme is one type of FHE which is designed for efficient matrix operations, making GL important for machine learning and AI tasks.

The goal of this thesis is to investigate the GL FHE scheme and to leverage the efficient matrix operations. Depending on your interests, you can use existing GL software libraries to implement some machine learning task (e.g. image classification). If you are interested in FPGA acceleration, you can design a dedicated hardware accelerator specifically for GL.

Goals and Tasks

- Get familiar with the GL scheme
- Implement encrypted ML applications, or design a high-end hardware accelerator for GL
- Evaluate and compare your implementation

Literature

- C. Gentry and Y. Lee
  Fully Homomorphic Encryption for Matrix Arithmetic
  CRYPTO 2026
  doi:10.1007/978-3-032-35374-0_12
  https://doi.org/10.1007/978-3-032-35374-0_12

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 combining FHE and ML
- Understanding of basic cryptography

Advisor Contact

florian.krieger@tugraz.at