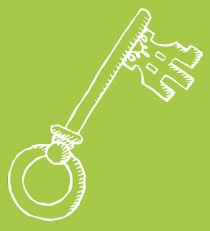

Applications for the GL Homomorphic Encryption Scheme

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. You will use existing GL software libraries to implement machine learning tasks like image classification over encrypted data.

Goals and Tasks

- Get familiar with the GL scheme
- Implement encrypted ML applications
- 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

- ☑ **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

Prerequisites

- Interest in combining FHE and ML
- Basic programming skills (C/C++, Python)

Advisor Contact

florian.krieger@tugraz.at