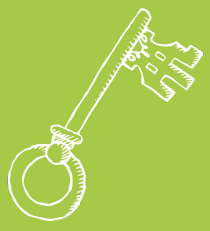

Practical Implementations for Future Cryptography

Advisor: **Florian Krieger**

Motivation

We are currently launching an exciting project for real-world deployments of cutting-edge cryptographic techniques. We especially focus on Fully Homomorphic Encryption (FHE) and Zero-Knowledge Proofs (ZKP) and aim to bridge the gap to concrete practicability.

We offer master projects and theses related to FHE and ZKP, spanning the whole hardware, software, and protocol stack of these schemes. Possible tasks for you could be:

- Developing encrypted AI applications using FHE
- Investigating FHE compilers for machine learning applications
- Designing and analyzing ZKP applications like voting or age verification
- Implementing performance-critical operations efficiently in hardware and software

We offer a broad range of possible topics, and we are flexible to adapt to your main interests. If you are curious and want to do a project or thesis with us, please reach out!

Goals and Tasks

- Get familiar with existing FHE and ZKP solutions
- Implement real-world applications using FHE and ZKP
- Evaluate and analyze your implementation

Literature

- A. A. Badawi et al.
  SoK: Private LLM Inference using Approximate Homomorphic Encryption
  Cryptology ePrint Archive 2026
  https://eprint.iacr.org/2026/935
- J. Liang et al.
  SoK: Understanding zk-SNARKs: The Gap Between Research and Practice
  USENIX Security 25
  https://www.usenix.org/conference/usenixsecurity25/presentation/liang-sok

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 FHE and ZKP applications
- Understanding of basic cryptography

Advisor Contact

florian.krieger@tugraz.at