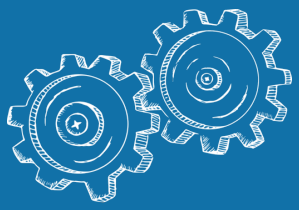


Optimized implementation of Homomorphic Encryption modules

Advisor: **Anisha Mukherjee**

Motivation

Homomorphic Encryption (HE) is a rapidly evolving area in cryptography that allows computations to be performed directly on encrypted data without needing to decrypt it, safeguarding privacy in outsourced computations. Ring-LWE-based homomorphic encryption schemes that use operations over polynomials have become significantly popular due to their efficiency and many software libraries such as the Microsoft SEAL provide optimized implementations for these computations.

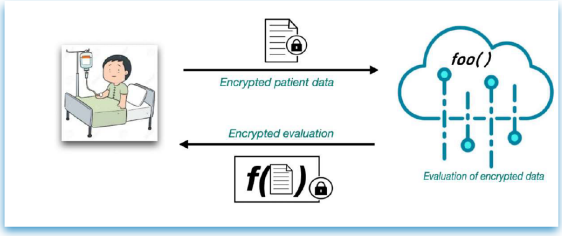
The focus of this thesis is on the implementation of a slightly different (and under-explored) HE variant based on module-LWE (MLWE) as switching to MLWE can provide better flexibility and scalability. You will generalize and optimize parts of the p-o-c SageMath implementation by porting to C++. Implementation methods from efficient software libraries for ring-LWE-HE can be utilized as all algorithms boil down to polynomial arithmetic.

Goals and Tasks

Get familiar with existing methods: Study the basics of HE (only a general idea is enough) and understand the current SageMath implementation (primarily polynomial arithmetic). [4 - 5 weeks]

Validate your code: Ensure that the new implementation produces results consistent with the original code. [4 - 5 weeks]

Identify scopes of improvement and finalize: Look for possible optimizations and finalise documentation. [4 - 5 weeks]



Literature

- Anisha Mukherjee, Aikata Aikata, Ahmet Can Mert, Yongwoo Lee, Sunmin Kwon, Maxim Deryabin, and Sujoy Sinha Roy
  ModHE: Modular Homomorphic Encryption Using Module Lattices: Potentials and Limitations
  https://eprint.iacr.org/2023/895
- Microsoft SEAL (release 4.1)
  https://github.com/Microsoft/SEAL
  2023
  Microsoft Research, Redmond, WA.

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 ☑ MATH

Prerequisites

- Interest in the topic area
- Programming (C/C++, Python)

Advisor Contact

anisha.mukherjee@iaik.tugraz.at