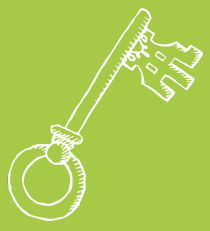

Fully Homomorphic Encryption Usability Report

Advisor: **Roman Walch**

Motivation

Fully homomorphic encryption (FHE) is often called the "holy grail" of cryptography, allowing one to operate on encrypted data without knowing the secret decryption key. Currently, several different FHE schemes exist, with implementations in several different libraries. Unfortunately, these libraries tend to be tedious to use, requiring expert knowledge about how to choose parameters correctly. This thesis aims to create a usability report of three FHE schemes, and their implementations in three different libraries. More specifically, we want to evaluate the schemes BFV, BGV, and CKKS, in the libraries HElib, SEAL, and PALISADE. Evaluate, how easy it is to install those libraries, their documentation, and how difficult the parameter selection is. Demonstrate your findings by comparing an implementation and benchmarks of a small use-case.

Goals and Tasks

- Understand necessary background (FHE)
- Evaluate the different FHE libraries in terms of usability
- Implement a small use case in different FHE libraries
- Benchmark the small use-case

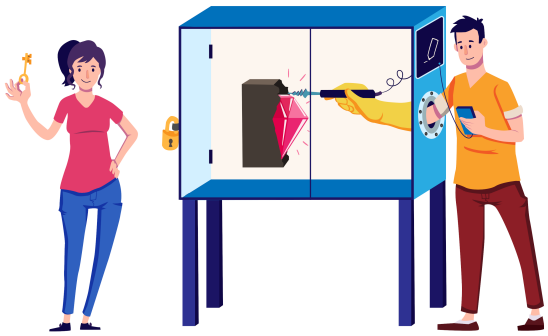

Illustration of Homomorphic Encryption

Literature

- Microsoft SEAL (release 3.5) https://github.com/Microsoft/SEAL 2020 Microsoft Research, Redmond, WA.
- HElib(release 1.1.0) https://github.com/homenc/HElib 2020
- PALISADE Lattice Cryptography Library (release 1.10.5) https://palisade-crypto.org/ 2020

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 cryptography and mathematical basics
- C++

Advisor / Contact

roman.walch@iaik.tugraz.at