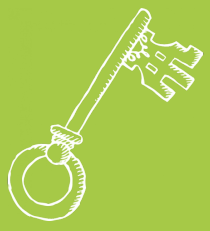


Ciphers for Prevention of FHE Ciphertext Expansion

Advisor: **Roman Walch**

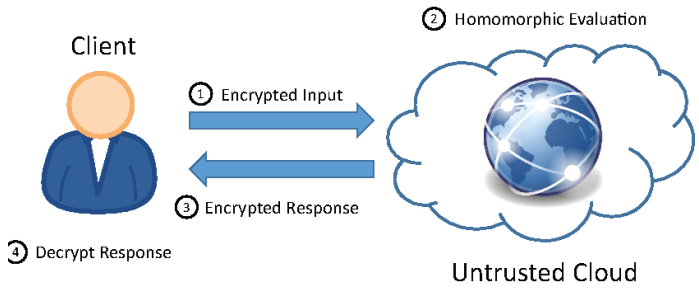
Motivation

In 2009 Gentry succeeded in constructing the first fully homomorphic encryption (FHE) scheme ever. While being a major breakthrough, his scheme lacked the performance for practical usage. Since then, many new schemes have been proposed - with BGV, BFV, CKKS and TFHE being the most prominent ones. One of the many practical constraints in using FHE schemes is called ciphertext expansion: A ciphertext is significantly larger than its corresponding plaintext. When using FHE in cloud-applications (like Machine Learning as a Service), a (often constraint) client has to send many of this large ciphertexts to the server, which is not desirable. We can use special symmetric cryptographic primitives, like RASTA, LowMC, FiLIP and others, to limit this ciphertext expansion.

The goal of this thesis is to implement several cryptographic primitives for existing FHE libraries and evaluate their usefulness in different settings and a specific use case.

Goals and Tasks

- Get familiar with FHE and symmetric schemes, like RASTA
- Implement the symmetric schemes in several FHE libraries
- Evaluate the performance of different schemes in different libraries



Source: *Fully Homomorphic Encryption: Cryptography's holy grail* in ACM Crossroads Journal 2015

Literature

- C. Dobraunig et al.
  Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit
  CRYPTO (1)
- C. Gentry
  Fully homomorphic encryption using ideal lattices
  STOC

Schedule

- Reading related work and first steps
- Intermediate presentation or poster
- Implementing, experiments, …
- Writing thesis
- Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Programming: C, C++
- Interest in FHE

Advisor / Contact

roman.walch@iaik.tugraz.at