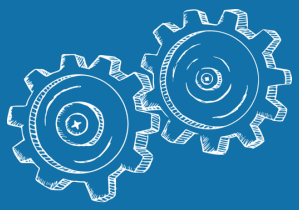


Metrics for analyzing Homomorphic Encryption acceleration works.

Advisor: **Aikata**

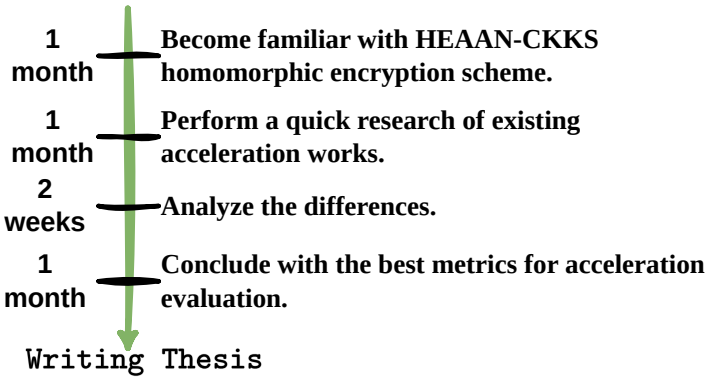
DATE: November 20, 2024

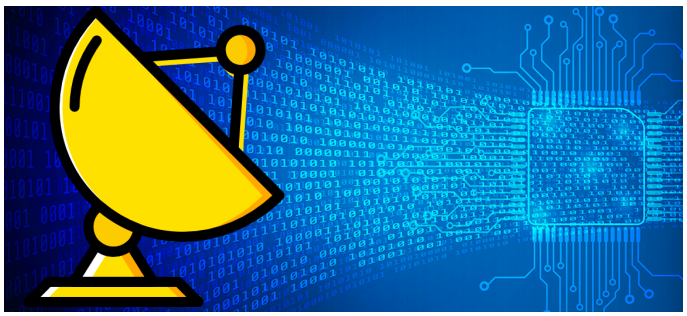
Motivation

Homomorphic encryption is the holy grail of privacy. It allows privacy-preserving data storage and computation. However, this powerful algorithm suffers from impracticality. This is because homomorphic computations are almost a million times slower than plain computations. To bridge this gap several implementations exist in the literature. Now the problem the community faces is how to analyze who is better. Since there are no standards, these implementations choose their own parameters and give acceleration results.

Hence, the goal of this thesis would be to analyze these works and come up with metrics that can help evaluate the acceleration potential of different works. Several such metrics exist, but they lack complete coverage. This thesis would converge to the best metric for the evaluation of acceleration potential.

Goals and Tasks





Literature

- www.openfhe.org/community/
  OpenFHE
  www.openfhe.org/
- Ahmet Can Mert, Aikata, Sunmin Kwon, Youngsam Shin, Donghoon Yoo, Yongwoo Lee, and Sujoy Sinha Roy
  Medha: Microcoded Hardware Accelerator for computing on Encrypted Data
  eprint.iacr.org/2022/480.pdf

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 the topic area, and basic knowledge of programming in C/C++

Advisor Contact

aikata@iaik.tugraz.at