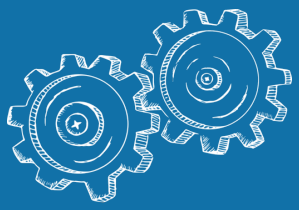


Designing approximated Machine Learning models in Python for Homomorphic evaluation.

Advisor: **Aikata**

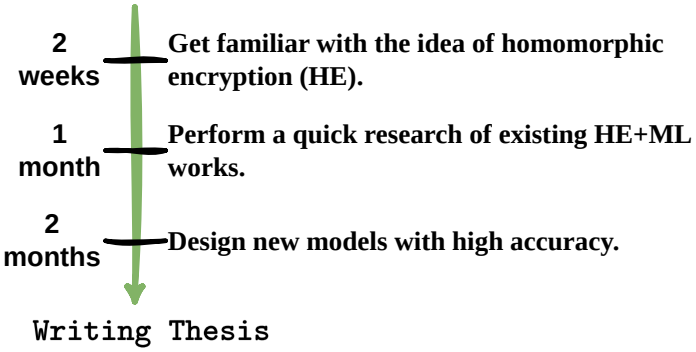
DATE: November 20, 2024

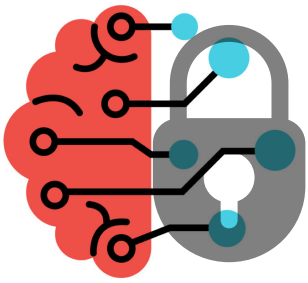
Motivation

Homomorphic encryption is the holy grail of privacy. It allows privacy-preserving data storage and computation. These computations include statistical analysis and several machine-learning applications. The non-linear components in machine-learning models, like ReLU or Max-Pool, cannot be computed using fast homomorphic encryption schemes. Thus, they need to be replaced by functions like a quadratic-ReLU or Average-Pool. This often results in a loss of accuracy.

The purpose of this thesis would be to approximate the existing ML models such that they can be homomorphically evaluated. Approaching the highest possible accuracy would help differentiate this work from naive approximations. In conclusion, this work would analyze the cost of such approximation in terms of runtime and accuracy for training as well as inference.

Goals and Tasks





Literature

- Alessandro Falcetta, Manuel Roveri
  Privacy-Preserving Deep Learning With Homomorphic Encryption: An Introduction
- Joon-Woo Lee, Hyungchul Kang, Yongwoo Lee, et. al.
  Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network

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 Python

Advisor Contact

aikata@iaik.tugraz.at