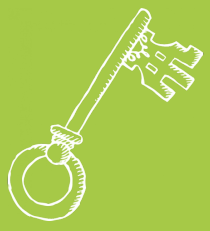


Privacy-Preserving Data Analysis

Advisor: **Lukas Helminger and Roman Walch**

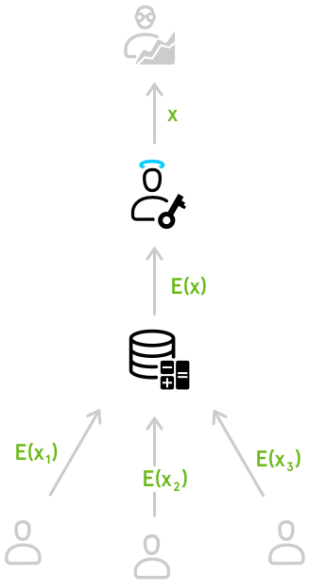
Motivation

In recent years, privacy of user data has become the focus of many interesting research topics. We are particularly interested in Privacy-Preserving Data Analysis, where companies and goverments want to compute on personal data (f.e. *Machine Learning as a Service*), but have to maintain GDPR compliance. We can use secure multi-party computation (MPC) and fully homomorphic encryption (FHE) to achieve privacy, while still being able to perform computation on the users data. MPC and FHE still add significant computational overhead, but due to increasing focus in research, first practical applications have been developed.

The goal of this project is to get an overview of the sate-of-the-art in this field and to then select and implement an analytical tool for a sample data set. Since this field is constantly developing we encourage you to meet us, so that we can give you a more concrete idea of the project/thesis.

Goals and Tasks

- Get familiar with the required background
- Review the state-of-the-art
- Implement a use-case



Source: https://medium.com/snips-ai/how-practical-is-somewhat-homomorphic-encryption-today-6818d1c6f7f6

Literature

- D. Evans, V. Kolesnikov, and M. Rosulek
  A Pragmatic Introduction to Secure Multi-Party Computation
  Foundations and Trends in Privacy and Security 2018
- 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++, Java, Python
- Interest in FHE and MPC

Advisor / Contact

lukas.helminger@iaik.tugraz.at,roman.walch@iaik.tugraz.at