Privacy-Preserving Data Analysis

Advisor(s): Lukas Helminger

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

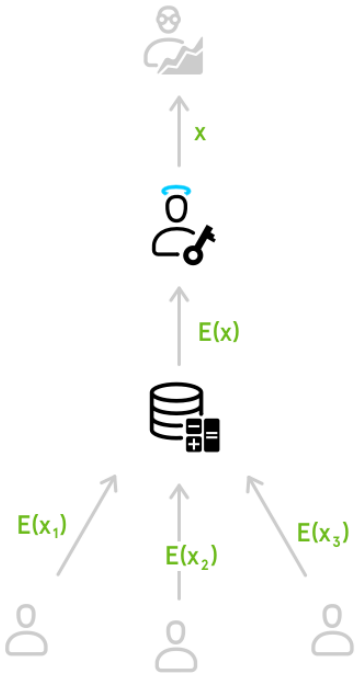
Motivation

There is an urgent need for Privacy-Preserving Data Analysis. This demand is created because companies and goverments want to compute on personal data while maintaining GDPR compliance. Theoretical solutions for this issuse exist since the 1980s but these lack the perfomance to operate on large data sets. The increasing computational power and newly developed spezialized protocols lead to first practial applications.

The goal of this project is to get an overview of the sate-of-the-art in this field and to then to select and implement an analytical tool for a sample data set.

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. Bogdanov et al.
  Rmind: A Tool for Cryptographically Secure Statistical Analysis
  IEEE Trans. Dependable Sec. Comput. 2018
  https://doi.org/10.1109/TDSC.2016.2587623

Deliverables

- Project files
- Thesis or project report (pdf)
- Poster (pdf)
- Presentation (pdf)

Schedule

- Start immediately
- Reading related work and taking first steps
- Intermediate presentation or poster
- Implementing
- Thesis writing
- Final presentation

Studies

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Programming: C, C++, Java, Python
- Interest in public key crypto

Advisor / Contact

lukas.helminger@iaik.tugraz.at