Exploring wider usage scenarios of differential privacy

Advisor: **Fredrik Meisingseth**

Motivation

Differential privacy (DP) is a mathematical notion precisely quantifying the privacy loss caused by releasing the result of a computation with secret input. It gives very strong mathematical guarantees and they are pretty well understood in general. This is no longer the case when the DP definition needs to be adapted in order to be achievable whilst using privacy enhancing technologies (PETs) such as multiparty computation (MPC), homomorphic encryption (HE) and zero-knowledge proofs (ZKPs). [1]

In your thesis, you will

> Study DP in both its standard formulation and in various relaxed forms.

> Survey how the variations can be combined with some PET.

> Derive new theoretical results on the feasibility of said combination, or

> Implement DP mechanisms whilst using said PET.

We have some ideas of specific topics, but are open to further discussion. Simply contact me if you are interested in the overall topic!

Goals and Tasks

▤ Understand differential privacy in a few different formulations.

▤ Provide new theoretical understanding of the difference between the DP formulations.

⚒ Demonstrate the feasibility of combining DP and another PET.

Literature

> F. Meisingseth, C. Rechberger, and F. Schmid
Practical Two-party Computational Differential Privacy with Active Security.
Proceedings on Privacy Enhancing Technologies 2025
https://eprint.iacr.org/2024/004

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 ☑ MATH

Prerequisites

> PETs, Cryptography or Cryptanalysis

> Strong interest in mathematics, more specifically probability theory and statistics

Advisor Contact

fredrik.meisingseth@tugraz.at