The Best of Two Privacy Worlds – By Combining MPC and DP

Advisor: **Fredrik Meisingseth, Fabian Schmid**

Motivation

Differential privacy (DP) measures and limits the impact of individual input datapoints on a function output, thereby protecting the privacy of the input. Multiparty computation (MPC) allows a set of parties to compute a function on their combined dataset such that no information leaks about the inputs except for the function evaluation. The evaluation might however leak quite a lot, therefore it is tempting to use DP to bound that leakage.

Marrying these two privacy enhancing technologies does introduce many challenges though. On the theory side, the technologies have fundamentally different adversarial and computational models. On the practical side, one problem is that of distributedly generating noise from a specific distribution without revealing the outcome of the noise sampling. [1]

In your thesis, you will

> Study DP and MPC security definitions in their standard forms and discuss their compatability.

> Survey how the definitions can be adapted to fit better together.

> Implement DP mechanisms in an MPC framework.

Goals and Tasks

📕 Understand MPC and DP – their goals, limitations and formalities.

📕 Understand how the two disciplines can (and can not) be combined.

🔧 Demonstrate the feasibility of combining MPC and DP by implementation and benchmarks.

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

> Strong interest in mathematics, particularly probability theory and statistics

Advisor Contact

fredrik.meisingseth@iaik.tugraz.at