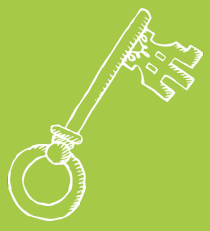

Combining Proofs of Knowledge and Differential Privacy

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. It does however require trusting that a specific curator adds a specific type of noise to the function evaluation. One can remove this trust by making the curator *prove* that it has added the right noise distribution. Importantly, this can be done without leaking too much information about what the noise value actually is.

Marrying DP with such proofs of knowledge (PoK) does introduce many challenges though. On the theory side, the technologies have different adversarial and computational models. On the practical side, it is widely open how to best sample noise so that it can be proven to have a specific distribution. In your thesis, you will

- Study DP and PoK 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 a certifiable way.

Goals and Tasks

- Understand DP and PoKs – their goals, limitations and formalities.
- Understand how the two techniques can (and can not) be combined.
- Demonstrate the feasibility of combining PoKs and DP by implementation and benchmarks.

Literature

- Z. R. Bell et al.
  Certifying Private Probabilistic Mechanisms
  Advances in Cryptology – CRYPTO 2024
  doi:10.1007/978-3-031-68391-6_11

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM ☑ MATH

Prerequisites

- Strong interest in mathematics, particularly probability theory, and cryptography

Advisor Contact

fredrik.meisingseth@tugraz.at