Chapter 7

Conclusions and Open Questions

In this thesis, we investigated properties of Private Stream Aggregation (PSA), a concept introduced by Shi et al. [SCR+11] for safe and distributed data analysis. We were able to prove that a secure PSA scheme in the non-adaptive compromise model can be built upon key-homomorphic weak PRFs. Using the notion of computational differential privacy, we provided a connection between a secure PSA scheme and a mechanism preserving differential privacy by showing that a differentially private mechanism preserves computational differential privacy, if it is executed through a secure PSA scheme. Moreover, we introduced the Skellam mechanism and compared its accuracy with the accuracy of the geometric and the binomial mechanisms. All three mechanisms preserve differential privacy and are suitable for an execution through a PSA scheme. While the practical performances of the geometric and the Skellam mechanisms are equally better than the performance of the binomial mechanism, we were able to provide a slightly better theoretical upper bound for the Skellam mechanism at high privacy levels. Based on the DDH assumption, we gave an instantiation of a key-homomorphic weak PRF that is used to construct a secure PSA scheme in the standard model (rather than the random oracle model). If the plaintext space is large enough, it has a substantially more efficient decryption algorithm than the scheme by Shi et al. [SCR+11] at the cost of a slightly less efficient encryption algorithm. Using the previous results, we constructed the first prospective post-quantum PSA scheme for data analyses under differential privacy using a weak PRF based on the DLWE assumption with Skellam noise that is used both for security of the scheme and for preserving differential privacy. We constituted the main result of the thesis, showing that the DDH assumption on the one hand and well-established lattice-based hardness assumptions on the other hand imply computational differential privacy with high accuracy in the distributed setting.

An interesting further direction is to reduce the size of the variance that is
necessary for the hardness of the LWE problem with errors following a symmetric Skellam distribution, especially to reduce or abolish the dependence on the number of LWE-samples in Theorem 6.11 resulting in a more widespread applicability of this new variant of the LWE problem. It would be also interesting to investigate whether the technique used in [BLL+15] (as described in Section 6.3) would lead to better parameters for the LWE problem with errors following a symmetric Skellam distribution. Another problem to face is showing the hardness of the Ring LWE problem (a more efficient version of LWE introduced in [LPR10]) with errors following a symmetric Skellam distribution and to establish a corresponding search-to-decision reduction. Sufficient conditions on the error distribution for the existence of a search-to-decision reduction for the Ring LWE problem were provided in [Lyu11]. A different proof is required for the symmetric Skellam distribution, since it does not satisfy these conditions.