A new DDH-based PRF with Application to Distributed Private Data Analysis [*]

Filipp Valovich
Horst Görtz Institute for IT Security
Faculty of Mathematics
Ruhr-Universität Bochum, Universitätsstrasse 150, 44801 Bochum, Germany
Email: filipp.valovich@rub.de

Abstract

The emerging technologies for big data analytics raise new challenges to the security and privacy of sensitive user data. For the distributed and semi-honest setting, the problem of private data analysis was considered in a work by Shi et al. 2011. That work introduced the Private Stream Aggregation (PSA) scheme, a cryptographic protocol for the aggregation of data in a network. It enables each user of the network to securely send encrypted time-series data to an (untrusted) aggregator. The aggregator is then able to decrypt the aggregate of all data by means of time-series queries, but cannot retrieve any further information about the individual data. The execution of a PSA scheme requires each user of the network to send exactly one message per time-series query to the aggregator. Thus, a PSA scheme has a minimal communication cost in this setting (assuming the independence of all time-series queries and all time-series data). Shi et al. 2011 instantiated a PSA scheme with strong security guarantees based on the Decisional Diffie-Hellman (DDH) assumption in the multiplicative group $\mathbb{Z}_p^*$ modulo a prime p. However, their construction has the limitation that the decryption on the aggregator's side requires the solution of a discrete logarithm and thus can be inefficient if the range is exponentially large in the given security parameter. Moreover, the security of their scheme only holds in the random oracle model.

To solve these issues, we first show the hardness of the DDH problem in the group $\mathcal{QR}_{p^2}$ of quadratic residues modulo a squared safe prime p, if DDH is hard in $\mathbb{Z}_p^*$. We then construct a *key-homomorphic weak pseudo-random function* (PRF) from it. We use this key-homomorphic weak PRF to construct a new PSA scheme with a very *efficient* decryption algorithm (whereas encryption time is almost unaffected) and with security guarantees in the *standard model.* We provide a rigorous security analysis for this new PSA scheme and an experimental comparison with the PSA scheme by Shi et al. 2011.

[*] The research was supported by the DFG Research Training Group GRK 1817/1