Efficient Private Stream Aggregation with Labels in the Standard Model

Johannes Ernst
University St. Gallen

Alexander Koch
Karlsruhe Institute of Technology (KIT)

32th Crypto Day, 15 January 2021

A private stream aggregation (PSA) scheme is a protocol of n clients and one aggregator. At every time step, the clients send an encrypted value to the (untrusted) aggregator, who is able to compute the sum of all client values, but cannot learn the values of individual clients. PSA was introduced by Shi, Chan, Rieffel, Chow & Song (2011) and since than others have built PSA schemes that are more efficient or based on different assumptions.

One possible application of PSA is privacy-preserving smart metering, where a power supplier can learn the total power consumption, but not the consumption of individual households. Another possible use case is federated learning, where a server adds up local model updates from several clients to obtain a global model update. A PSA scheme can better protect the clients privacy here, because the server can only compute the sum of the updates. This makes it harder for the server to deduce information about the training data of individual clients.

We construct a simple and efficient PSA scheme that supports labels and which we prove to be secure in the standard model. Labels are useful to restrict the access of the aggregator, because it prevents the aggregator from combining ciphertexts with different labels (or from different time-steps) and thus avoids leaking information about values of individual clients.

The scheme is based on key-homomorphic pseudorandom functions as the only primitive, supports a large message space, scales well for a large number of users and has small ciphertexts.

As proof of concept we instantiated the scheme with a simple random oracle based key-homomorphic pseudorandom function mentioned by Boneh, Lewi, Montgomery & Raghunathan (2013) and implemented both in Python. The performance results show that both the encryption and the decryption algorithm are quite fast.

References

Dan Boneh, Kevin Lewi, Hart Montgomery & Ananth Raghunathan (2013). Key homomorphic PRFs and their applications. In *Annual Cryptology Conference*, 410–428. Springer.

crypto day matters 32 (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-16

Elaine Shi, TH Hubert Chan, Eleanor Rieffel, Richard Chow & Dawn Song (2011). Privacy-preserving aggregation of time-series data. In *Proc. NDSS*, volume 2, 1–17. Citeseer.