Cryptology ePrint Archive: Report 2011/655

Privacy-Preserving Stream Aggregation with Fault Tolerance

T-H. Hubert Chan, Elaine Shi and Dawn Song

Abstract: We consider applications where an untrusted aggregator would like to collect privacy sensitive data from users, and compute aggregate statistics periodically. For example, imagine a smart grid operator who wishes to aggregate the total power consumption of a neighborhood every ten minutes; or a market researcher who wishes to track the fraction of population watching ESPN on an hourly basis.

We design novel mechanisms that allow an aggregator to accurately estimate such statistics, while offering provable guarantees of user privacy against the untrusted aggregator. Our constructions are resilient to user failure and compromise, and can efficiently support dynamic joins and leaves. Our constructions also exemplify the clear advantage of combining applied cryptography and differential privacy techniques.

Category / Keywords: applications / Differential Privacy, Periodic Aggregation, Untrusted Aggregator, Fault Tolerance, Dynamic Users

Publication Info: Financial Cryptography and Data Security 2012

Date: received 3 Dec 2011, last revised 10 Dec 2011

Contact author: hubert at cs hku hk

Available formats: PDF | BibTeX Citation

Note: A conference version of the paper will appear at Financial Cryptography and Data Security 2012. We will put the full version of the paper here.

Version: 20111211:052420 (All versions of this report)

Discussion forum: Show discussion | Start new discussion