Cryptology ePrint Archive: Report 2013/021

Rate-Limited Secure Function Evaluation: Definitions and Constructions

Özgür Dagdelen and Payman Mohassel and Daniele Venturi

Abstract: We introduce the notion of rate-limited secure function evaluation (RL-SFE). Loosely speaking, in an RL-SFE protocol participants can monitor and limit the number of distinct inputs (i.e., rate) used by their counterparts in multiple executions of an SFE, in a private and verifiable manner. The need for RL-SFE naturally arises in a variety of scenarios: e.g., it enables service providers to ``meter'' their customers' usage without compromising their privacy, or can be used to prevent oracle attacks against SFE constructions.

We consider three variants of RL-SFE providing different levels of security. As a stepping stone, we also formalize the notion of commit-first SFE (cf-SFE) wherein parties are committed to their inputs before each SFE execution. We provide compilers for transforming any cf-SFE protocol into each of the three RL-SFE variants. Our compilers are accompanied with simulation-based proofs of security in the standard model and show a clear tradeoff between the level of security offered and the overhead required. Moreover, motivated by the fact that in many client-server applications clients do not keep state, we also describe a general approach for transforming the resulting RL-SFE protocols into stateless ones.

As a case study, we take a closer look at the oblivious polynomial evaluation (OPE) protocol of Hazay and Lindell, show that it is commit-first and instantiate efficient rate-limited variants of it.

Category / Keywords: foundations / secure function evaluation, secure metering, oracle attacks, oblivious polynomial evaluation

Publication Info: An extended abstract of this paper is published in the proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography – PKC 2013. This is the full version.

Date: received 13 Jan 2013, last revised 18 Feb 2013

Contact author: oezguer dagdelen at cased de

Available formats: PDF | BibTeX Citation

Version: 20130218:144647 (All versions of this report)

Discussion forum: Show discussion | Start new discussion