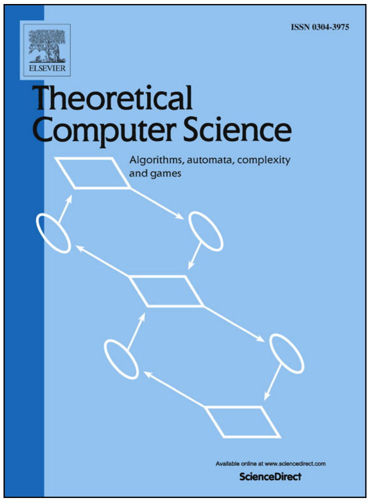
ISSN 0304-3975
ELSEVIER
Theoretical Computer Science
Algorithms, automata, complexity and games
Available online at www.sciencedirect.com
ScienceDirect

Rate-limited secure function evaluation

Özgür Dagdelen, Payman Mohassel, Daniele Venturi

PII: S0304-3975(16)30507-2
DOI: http://dx.doi.org/10.1016/j.tcs.2016.09.020
Reference: TCS 10936

To appear in: *Theoretical Computer Science*

Received date: 10 March 2016
Accepted date: 21 September 2016

Please cite this article in press as: Ö. Dagdelen et al., Rate-limited secure function evaluation, *Theoret. Comput. Sci.* (2016), http://dx.doi.org/10.1016/j.tcs.2016.09.020

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

Rate-Limited Secure Function Evaluation

Özgür Dagdelen[1], Payman Mohassel[2], and Daniele Venturi[3]

[1] *bridgingIT, N7 5, 68161 Mannheim, Germany*
[2] *Department of Computer Science, University of Calgary, Canada*
[3] *Department of Computer Science, Sapienza University of Rome, Italy*

October 4, 2016

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.

Keywords: secure function evaluation; secure metering; oracle attacks.

Contents