

# Accepted Manuscript

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>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



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<sup>1</sup>, Payman Mohassel<sup>2</sup>, and Daniele Venturi<sup>3</sup>

<sup>1</sup>*bridgingIT, N7 5, 68161 Mannheim, Germany*

<sup>2</sup>*Department of Computer Science, University of Calgary, Canada*

<sup>3</sup>*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

<b>1</b>	<b>Introduction</b>	<b>1</b>	<b>4</b>	<b>Rate-Limited SFE</b>	<b>13</b>
1.1	Our Contribution . . . . .	2	5	<b>Compilers for Rate-Limited SFE</b>	<b>16</b>
1.2	Additional Related Work . . . . .	4	5.1	A Rate-Hiding Compiler . . . . .	16
1.3	Roadmap . . . . .	5	5.2	A Rate-Revealing Compiler . . . . .	20
<b>2</b>	<b>Preliminaries</b>	<b>5</b>	5.3	A Pattern-Revealing Compiler . . . . .	23
2.1	Notation . . . . .	5	<b>6</b>	<b>Making the Compilers Stateless</b>	<b>26</b>
2.2	Basic Cryptographic Tools . . . . .	5	<b>7</b>	<b>Rate-Limited OPE</b>	<b>31</b>
<b>3</b>	<b>Commit-First SFE</b>	<b>8</b>	7.1	Rate-Revealing OPE . . . . .	32
3.1	The Definition . . . . .	8	7.2	Rate-Hiding OPE . . . . .	33
3.2	Instantiations . . . . .	10	<b>8</b>	<b>Conclusions and Open Problems</b>	<b>34</b>

Download English Version:

<https://daneshyari.com/en/article/4952450>

Download Persian Version:

<https://daneshyari.com/article/4952450>

[Daneshyari.com](https://daneshyari.com)