Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Regular lossy functions and their applications in leakage-resilient cryptography

Yu Chen [a,b,c,*], Baodong Qin [d,b], Haiyang Xue [a]

[a] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[b] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China
[c] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
[d] National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

ARTICLE INFO

Article history:
Received 15 January 2018
Received in revised form 12 April 2018
Accepted 22 April 2018
Available online xxxx
Communicated by G. Yang

Keywords:
Regular lossy functions
Hash proof system
Leakage resilience
One-way functions
Message authentication codes
(Identity-based) key encapsulation mechanism

ABSTRACT

In STOC 2008, Peikert and Waters introduced a powerful primitive called *lossy trapdoor functions* (LTFs). In a nutshell, LTFs are functions that behave in one of two modes. In the normal mode, functions are injective and invertible with a trapdoor. In the lossy mode, functions statistically lose information about their inputs. Moreover, the two modes are computationally indistinguishable. In this work, we put forward a relaxation of LTFs, namely, *regular lossy functions* (RLFs). Compared to LTFs, the functions in the normal mode are not required to be efficiently invertible or even unnecessary to be injective. Instead, they could also be lossy, but in a regular manner. We also put forward richer abstractions of RLFs, namely *all-but-one regular lossy functions* (ABO-RLFs) and *one-time regular lossy filters* (OT-RLFs).

We show that (ABO)-RLFs admit efficient constructions from both a variety of number-theoretic assumptions and hash proof system (HPS) for subset membership problems satisfying natural algebraic properties. Thanks to the relaxations on functionality, the constructions enjoy much compact key size and better computational efficiency than that of (ABO)-LTFs.

We demonstrate the utility of RLFs and their extensions in the leakage-resilient cryptography.

- As a special case of RLFs, lossy functions imply leakage-resilient injective one-way functions with optimal leakage rate $1 - o(1)$.
- ABO-RLFs (or OT-RLFs) immediately imply leakage-resilient one-time message authentication code (MAC) with optimal leakage rate $1 - o(1)$.
- ABO-RLFs together with HPS give rise to leakage-resilient chosen-ciphertext (CCA) secure key encapsulation mechanisms (KEM) (this approach extends naturally to the identity-based setting). Combining the construction of ABO-RLFs from HPS, this gives the first leakage-resilient CCA-secure public-key encryption (PKE) with optimal leakage rate based solely on HPS, and thus goes beyond the barrier posed by Dodis et al. (Asiacrypt 2010). Our construction also applies to the identity-based setting, yielding LR-CCA secure IB-KEM with higher leakage rate than previous works.

© 2018 Elsevier B.V. All rights reserved.

* Corresponding author at: State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China.
E-mail address: cycosmic@gmail.com (Y. Chen).

https://doi.org/10.1016/j.tcs.2018.04.043
0304-3975/© 2018 Elsevier B.V. All rights reserved.

Please cite this article in press as: Y. Chen et al., Regular lossy functions and their applications in leakage-resilient cryptography, Theoret. Comput. Sci. (2018), https://doi.org/10.1016/j.tcs.2018.04.043

1. Introduction

In STOC 2008, Peikert and Waters [39] introduced a powerful primitive called lossy trapdoor function (LTF). Informally, LTF is a collection of functions $\mathcal{F} = \{f_{ek}\}$ whose evaluation key (i.e., function index or code) is created in one of two modes. One is injective (i.e., normal) mode: given a suitable trapdoor td for ek, the entire input x can be efficiently recovered from $f_{ek}(x)$. The other is lossy mode: f_{ek} statistically loses a significant amount of information about its input. Moreover, the two modes are computationally indistinguishable: given just ek, no efficient adversary can tell whether f_{ek} is injective or lossy. They also introduced a richer abstraction called all-but-one lossy trapdoor functions (ABO-LTFs). A collection of ABO-LTFs is associated with a set B called branches. The key generation algorithm takes a given branch $b^* \in B$ as an extra parameter, and outputs an evaluation key ek and a trapdoor td. The function $f_{ek,b}(\cdot)$ is injective and invertible with td for any branch $b \neq b^*$, while the function $f_{ek,b^*}(\cdot)$ is lossy. Moreover, the lossy branch b^* is computationally hidden by ek.

Using LTFs and ABO-LTFs, Peikert and Waters [39] develop new approaches for constructing several important cryptographic tools, such as injective TDFs, collision-resistant hash functions (CRHFs), oblivious transfer and CCA-secure PKE.

1.1. Related work

Since the initial work of [39], there has been much additional work on LTFs and related concepts.

One direction of research is to find additional realizations of LTFs. Boyen and Waters [11] gave a technique to shrink the public key of matrix construction of [39] with the help of pairing. Rosen and Segev [43] and Boldyreva et al. [5] independently described simple, compact constructions of LTFs and ABO-LTFs under the decisional composite residuosity (DCR) assumption. Freeman et al. [17] provided more constructions of LTFs from the quadratic residuosity (QR) and d-linear assumptions. Kiltz et al. [30] and Xue et al. [47] gave constructions of LTFs based on factoring assumptions. Hemenway and Ostrovsky [23] gave a construction of LTFs based on the extended decisional Diffie–Hellman (eDDH) assumption, which generalizes the DDH, QR and DCR assumption. They also showed a generic construction of LTFs from homomorphic smooth HPS. Wee [46] presented an alternative generic construction of LTFs from dual HPS.

Another direction of research is to explore variations and more applications. Rosen and Segev [43] and Kiltz et al. [28] showed LTFs imply correlated-product TDFs and adaptive TDFs respectively. Boldyreva et al. [5] constructed CCA-secure deterministic encryption based on LTFs and ABO-LTFs. Hemenway et al. [22] generalized ABO-LTFs to all-but-N lossy trapdoor functions (ABN-LTFs) that have N lossy branches. Hofheinz [24] further generalized ABN-LTFs to all-but-many (ABM) LTFs in which the number of lossy branches is not bounded by any polynomial. Recently, Boyen and Li [10] realized ABM LTFs based on the learning with errors assumptions. So far, ABM-LTFs have shown their usefulness in constructing PKE with strong security properties including selective opening security [24] and key-dependent message security [25]. Mol and Yilek [36] constructed a CCA-secure PKE from any slightly lossy trapdoor functions that lose only a noticeable fraction of a bit. On the contrary, Zhandry [48] introduced extremely lossy functions (whose functions in the lossy mode only have polynomial-sized image), and demonstrated extremely lossiness is useful for instantiating random oracles in several settings.

1.2. Motivations

Due to the strong requirement for the normal mode (injective and efficiently invertible with trapdoor), the concrete constructions of (ABO)-LTFs are typically not efficient in terms of the size of evaluation key and complexity of evaluation. The generic constructions of (ABO)-LTFs require advanced property for the basing primitives, such as homomorphic and invertible properties.

In all the known applications of LTFs, the normal mode is used to fulfill functionality, while the lossy mode is used to establish security. However, in many scenarios we do not require the full power of LTFs. As observed by Peikert and Waters [39, Section 3.4], some applications (such as injective OWFs, CRHFs) *do not require a trapdoor*, but only indistinguishability between normal mode and lossy mode. Thereby, they conjectured "realizing the weaker notion of lossy (non-trapdoor) functions (LFs) could be achieved more simply or efficiently than the full notion of LTFs", and left the investigation of this question as an interesting problem.

A central goal in cryptography is to base cryptosystems on primitives that are as week as possible. With the question raised by Peikert and Waters [39] in mind, we ask the following questions:

How to realize LFs efficiently? Are there any other applications of LFs? Can we further weaken the notion of LFs while still being useful?

1.3. Our contributions

We answer the above questions affirmatively. An overview of our contributions is as below.

1.3.1. Regular lossy functions and extensions

As discussed above, when building cryptographic protocols the normal mode of LTF is used to fulfill functionality. For some applications that invertible property for the normal mode is overkilled, the injective property may also be unnecessary. This suggests that we may further relax the notion of LFs.

Please cite this article in press as: Y. Chen et al., Regular lossy functions and their applications in leakage-resilient cryptography, Theoret. Comput. Sci. (2018), https://doi.org/10.1016/j.tcs.2018.04.043

Download English Version:

https://daneshyari.com/en/article/6875411

Download Persian Version:

https://daneshyari.com/article/6875411

Daneshyari.com