Leakage-Flexible CCA-secure Public-Key Encryption: Simple Construction and Free of Pairing

Baodong Qin[1,2] and Shengli Liu[1,⋆]

[1] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

[2] College of Computer Science and Technology, Southwest University of Science and Technology, Mianyang 621010, China

{qinbaodong,slliu}@sjtu.edu.cn

Abstract. In AsiaCrypt 2013, Qin and Liu proposed a new approach to CCA-security of Public-Key Encryption (PKE) in the presence of bounded key-leakage, from any universal hash proof system (due to Cramer and Shoup) and any one-time lossy filter (a simplified version of lossy algebraic filters, due to Hofheinz). They presented two instantiations under the DDH and DCR assumptions, which result in leakage rate (defined as the ratio of leakage amount to the secret-key length) of $1/2 - o(1)$. In this paper, we extend their work to broader assumptions and to flexible leakage rate, more specifically to leakage rate of $1 - o(1)$.

- We introduce the Refined Subgroup Indistinguishability (RSI) assumption, which is a subclass of subgroup indistinguishability assumptions, including many standard number-theoretical assumptions, like the quadratic residuosity assumption, the decisional composite residuosity assumption and the subgroup decision assumption over a group of known order defined by Boneh et al.
- We show that universal hash proof (UHP) system and one-time lossy filter (OT-LF) can be simply and efficiently constructed from the RSI assumption. Applying Qin and Liu's paradigm gives simple and efficient PKE schemes under the RSI assumption.
- With the RSI assumption over a specific group (free of pairing), public parameters of UHP and OT-LF can be chosen in a flexible way, resulting in a leakage-flexible CCA-secure PKE scheme. More specifically, we get the first CCA-secure PKE with leakage rate of $1 - o(1)$ without pairing.

Keywords: Public-key encryption, leakage flexibility, chosen-ciphertext security.

[⋆] Supported by the National Natural Science Foundation of China (Grant No. 61170229, 61133014 and 61373153), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 20110073110016), and the Scientific innovation projects of Shanghai Education Committee (Grant No. 12ZZ021).

H. Krawczyk (Ed.): PKC 2014, LNCS 8383, pp. 19–36, 2014.

1 Introduction

Traditional security models (e.g., semantic security [17]) of cryptographic schemes assume that the secret key or the internal secret state involved in a cryptosystem is completely unknown to adversaries. However, in the real world, an adversary may obtain partial knowledge of the secret information via a side channel attack [18]. Side channel attacks gain (secret) information from physical attributions (e.g., timing, power consumption, etc.) revealed by a computing device. Inspired by side channel attacks, many cryptographic researchers have contributed their work to design of cryptosystems that remain secure even if an adversary obtains some information on the secret keys, including symmetric-key encryption [11,13,30], public-key encryption [1,27,2,4,5,31], digital signatures [21,14], identity-based encryption [7,15,24].

To model security against side channel attacks, it is natural to consider an adversary that only learns a limited amount of information on the secret key. Otherwise, the security of the system will be compromised completely. A simple yet general model of key-leakage is the bounded-leakage model [1]. It is formalized by allowing an adversary to adaptively and repeatedly choose functions of the secret key and gain the outputs of the functions as long as the total amount of leaked information on the secret key is bounded by some parameter λ (called the leakage amount). Clearly, from this perspective, the leakage amount must be strictly smaller than the secret-key length $|sk|$. We call the ratio $\lambda/|sk|$ the relative leakage or the leakage rate of a cryptosystem. An obvious goal of designing a leakage-resilient cryptosystem is to make its leakage rate as close to 1 as possible. There are also other security models for leakage-resilience that consider more complicated scenarios of key leakage, e.g., auxiliary input model [11], continual-leakage model [5,9] and continual auxiliary input model [33]. Nevertheless, many works from those complicated models rely on the results from the bounded-leakage model as basic building blocks [19]. In this paper, we consider the bounded-leakage model in the setting of public-key encryption.

Prior Constructions and Limitations. Inspired by Halderman et al.'s "cool boot" attacks [18], Akavia et al. [1] formalized the notion of leakage-resilient chosen-plaintext security (LR-CPA) in the bounded-leakage model. Since then, many encryption schemes [32,16,3,27,19] have been proved secure in this model. In particular, Naor and Segev presented a generic construction of LR-CPA secure PKE schemes from any hash proof system (HPS) [8]. Moreover, they gave some efficient instantiations based on the DDH and k-linear assumptions, where the relative leakage is flexibly ranging over $[0, 1)$. We also call such PKE *leakage-flexible*. In [27], Naor and Segev also extended the framework of key leakage to the setting of chosen-ciphertext attacks, i.e., leakage-resilient chosen-ciphertext security (LR-CCA). They showed how to achieve LR-CCA secure PKE schemes by relying on the Naor-Yung paradigm which results in (impractical) leakage flexible PKE schemes or the hash proof systems which result in an efficient variant of the Cramer-Shoup cryptosystem with leakage-rate 1/6. Later, some new variants of the Cramer and Shoup cryptosystem [25,26] are showed to be

LR-CCA secure but with a leakage-rate smaller than 1/4. Very recently, Qin and Liu [31] proposed a novel approach to achieve LR-CCA security by replacing the universal$_2$ hash proof system in Naor and Segev's HPS-based framework with a new primitive called one-time lossy filter. This results in efficient constructions of LR-CCA secure PKE schemes based on the DDH and DCR assumptions with leakage rate $1/2 - o(1)$.

The open problem of constructing a practical LR-CCA secure PKE scheme with flexible leakage was solved by Dodis et al. [10]. They showed that Naor and Segev's generic construction in the Naor-Yung paradigm can be made efficient under the Symmetric External Diffie-Hellman (SXDH) and Decisional Linear (DLIN) assumptions related to bilinear pairing on elliptic curves. Another leakage-flexible CCA-secure PKE scheme was due to Galindo et al. [15]. Their construction is obtained by applying the CHK transform [6] to their identity-based encryption scheme with master-key leakage flexibility (without rigorous proof) under the DLIN assumption on pairing-friendly groups. We observe that all existing leakage-flexible CCA-secure PKE schemes rely on assumptions over pairing-friendly groups. Moreover, even though they are practical, the constructions are complicated and computations inevitably involve pairings.

Our Contributions. In this paper, we define a class of assumptions called *Refined Subgroup Indistinguishability (RSI)* assumptions which are similar to the *Subgroup Indistinguishability (SI)* assumptions (due to Brakerski and Goldwasser [4]) except for the restriction to cyclic groups. Specifically, a subgroup indistinguishability problem is defined by a finite commutative multiplicative group $\mathbb{G}$, which is a direct product of two groups $\mathbb{G} = G_{\tau_1} \times G_{\tau_2}$ of order τ_1, τ_2 respectively. It requires that $\gcd(\tau_1, \tau_2) = 1$ and G_{τ_2} is a cyclic group. The subgroup indistinguishability assumption states that a random element of $\mathbb{G}$ is computationally indistinguishable from a random element in G_{τ_1}. Brakerski and Goldwasser [4] showed that the DCR and QR assumptions are two special cases of the subgroup indistinguishability assumptions. In the Refined Subgroup Indistinguishability (RSI) problem, we further require that the subgroup G_{τ_1} is also cyclic. Nevertheless, all known instances of SI problems can be modified to RSI problems. Moreover, the instantiations of RSI assumption under the DCR and QR assumptions are operated over groups of unknown order. We can also instantiate the RSI assumption over a specific group of known order (without pairing).

We further show that the RSI assumption implies efficient construction of leakage-resilient CCA-secure PKE schemes by presenting simple and efficient constructions of universal hash proof systems and one-time lossy filters under the RSI assumption. Here we follow Qin and Liu's paradigm [31](details in Section 4.1) of constructing leakage-resilient CCA-secure PKE from universal HPS and OT-LF, but we extend their work to the RSI assumption.

When instantiating over a specific group of known order (without pairing), we obtain a simple and efficient CCA-secure PKE scheme with leakage-rate of $1 - o(1)$. This is the first leakage-resilient CCA-secure PKE with leakage rate $1 - o(1)$, but free of pairing.

Organization. The rest of this paper is organized as follows. Basic notations and definitions are introduced in Section 2. The definition of refined subgroup indistinguishability assumptions and instantiations are presented in Section 3. Our leakage-resilient CCA-secure PKE schemes from the refined subgroup indistinguishability assumptions are given in Section 4. Finally, we summarize this paper in Section 5.

2 Preliminary

Notations. Let $\kappa \in \mathbb{N}$ denote a security parameter and 1^κ denote the string of κ ones. We say that a function $\epsilon(\kappa)$ is negligible in κ if for all polynomial ploy and sufficiently large κ, $\epsilon(\kappa) \leq 1/\mathsf{ploy}(\kappa)$. For $n \in \mathbb{N}$, we write $[n]$ for the set $\{1, \ldots, n\}$. We denote by $|s|$ the length of a bitstring s and by $|S|$ the size of a set S. Moreover, $s \leftarrow_R S$ denotes the operation of sampling an element s from S uniformly at random. We denote $y \leftarrow A(x)$ the operation of running A with input x, and assigning y as the result. We write $\log s$ for logarithms over the reals with base 2.

Statistical Distance. The *statistical distance* between two random variables X and Y over a finite set Ω is defined as $\Delta(X,Y) = \frac{1}{2}\sum_{\omega\in\Omega} |\Pr[X = \omega] - \Pr[Y = \omega]|$. A random variable X is called ϵ-uniform over Ω, if $\Delta(X,Y) \leq \epsilon$, where Y is a uniform distribution. Let X and Y be two families of random variables indexed by a security parameter κ. We say that X and Y are statistically indistinguishable and write $X \approx_s Y$ if for all polynomial ploy and sufficiently large κ, $\Delta(X,Y) \leq 1/\mathsf{ploy}(\kappa)$. If for any PPT algorithm $\mathcal{A}$, its advantage in distinguishing between X and Y defined as $|\Pr[\mathcal{A}(X) = 1] - \Pr[\mathcal{A}(Y) = 1]|$ is negligible in κ, we say that X and Y are computationally indistinguishable and write $X \approx_c Y$.

Min-Entropy and Average Min-Entropy. The *min-entropy* of a random variable X is $\mathrm{H}_\infty(X) = -\log(\max_x \Pr[X = x])$. The average min-entropy X conditioned on a random variable Y is formally defined by Dodis et al. [12] as $\widetilde{\mathrm{H}}_\infty(X|Y) = -\log\left(E_{y\leftarrow Y}[2^{-\mathrm{H}_\infty(X|Y=y)}]\right)$.

Definition 1 (Universal hash). *A family of functions $\mathcal{H} = \{h : X \to Y\}$ is called universal if, for all distinct $x, x' \in X$, $\Pr_{h\leftarrow_R\mathcal{H}}[h(x) = h(x')] = 1/|Y|$.*

The following lemma shows that a universal hash function can be used as a randomness extractor.

Lemma 1 ([12]). *Let X and Y be random variables such that $X \in \{0,1\}^n$ and $\widetilde{\mathrm{H}}_\infty(X|Y) \geq v$. Let $\mathcal{H} = \{h : \{0,1\}^n \to \{0,1\}^m\}$ be a family of universal hash functions. If $m \leq v - 2\log(1/\epsilon)$, then for $h \leftarrow_R \mathcal{H}$ it holds that $\Delta((Y, h, h(X)), (Y, h, U_m)) \leq \epsilon$, where U_m is uniform over $\{0,1\}^m$.*

Public-Key Encryption. A public-key encryption scheme PKE with message space $\mathcal{M}$ consists of three PPT algorithms $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$. For a security parameter 1^κ, the randomized key generation algorithm $\mathsf{Kg}(1^\kappa)$ produces a public/secret key pair (PK, SK). For a public key PK, the randomized encryption algorithm $\mathsf{Enc}(PK, M)$ creates a ciphertext C of the message $M \in \mathcal{M}$. For a secret key SK and a ciphertext C, the decryption algorithm $\mathsf{Dec}(SK, C)$ returns a message $M \in \mathcal{M}$ or a special rejection symbol $\bot$. For consistency, we require that $\mathsf{Dec}(SK, \mathsf{Enc}(PK, M)) = M$ always holds, for all $\kappa \in \mathbb{N}$, all $(PK, SK) \leftarrow \mathsf{Kg}(1^\kappa)$ and all $M \in \mathcal{M}$.

For security, we consider the standard notion of leakage-resilient chosen-ciphertext (LR-CCA) security in the bounded leakage model [27]. In this model, the adversary is allowed to query a decryption oracle $\mathcal{D}_{sk}(\cdot)$ which returns $\mathsf{Dec}(sk, C)$ for a query C, and a leakage oracle $\mathcal{O}_{sk}^{\lambda}(\cdot)$ which returns $f_i(sk)$ for a leakage function $f_i : \{0,1\}^* \rightarrow \{0,1\}^{\lambda_i}$. The adversary can adaptively query either of these two oracles polynomial times, with the following restrictions: (1) the total amount of information leaked is bounded by $\sum_i \lambda_i \leq \lambda$; (2) after seeing the challenge ciphertext, the adversary is not allowed to query the decryption oracle with the challenge ciphertext and query the leakage oracle at all.

Definition 2 (Leakage-resilient CCA-secure PKE). *We say that a PKE scheme* $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ *is λ-LR-CCA secure if, for any PPT adversary, the following function* $\mathsf{Adv}^{\lambda\text{-lr-cca}}_{\mathsf{PKE},\mathcal{A}}(\kappa)$ *is negligible in κ:*

$$\mathsf{Adv}^{\lambda\text{-lr-cca}}_{\mathsf{PKE},\mathcal{A}}(\kappa) := \\ \left| \Pr\left[\gamma' = \gamma : \begin{array}{l} (PK, SK) \leftarrow \mathsf{Kg}(1^\kappa), \gamma \leftarrow_R \{0,1\}, \\ (M_0, M_1, St) \leftarrow \mathcal{A}^{\mathcal{D}_{sk}(\cdot), \mathcal{O}^{\lambda}_{sk}(\cdot)}(PK) \ s.t. \ |M_0| = |M_1|, \\ C^* \leftarrow \mathsf{Enc}(PK, M_\gamma), \gamma' \leftarrow \mathcal{A}^{\mathcal{D}_{sk}(\cdot)}(St, C^*). \end{array} \right] - \frac{1}{2} \right|.$$

The *leakage rate* of a λ-LR-CCA secure PKE scheme is defined as $\lambda/|SK|$, where $|SK|$ denotes the secret-key length. If $\lambda/|SK|$ can be made arbitrarily close to 1 by properly choosing the parameter of the scheme, we call such scheme *leakage-flexible.*

One-Time Lossy Filters. One-time lossy filter (OT-LF), a simplified lossy algebraic filter [20], is a special collection of one-way functions. It can be operated in either an "injective mode", in which the function is injective (not requiring efficiently invertible), or a "lossy mode", in which the function is non-injective.

Definition 3. *A collection of* $(\mathsf{Dom}, \ell_{\mathsf{LF}})$*-one-time lossy filter consists of three PPT algorithms* $(\mathsf{FGen}, \mathsf{FEval}, \mathsf{FTag})$*. The key generation algorithm* $\mathsf{FGen}(1^\kappa)$*, on input* 1^κ*, generates an evaluation key ek and a trapdoor td (that allows for efficiently sampling a lossy tag). The evaluation key ek defines a tag space* $\mathcal{T} = \{0,1\}^* \times \mathcal{T}_c$ *that contains the disjoint sets of lossy tags* $\mathcal{T}_{loss} \subseteq \mathcal{T}$ *and injective tags* $\mathcal{T}_{inj} \subseteq \mathcal{T}$*. For an evaluation key ek and a tag* $t \in \mathcal{T}$*, the evaluation algorithm* $\mathsf{FEval}(ek, t, x)$ *maps* $x \in \mathsf{Dom}$ *to a unique image* $y = f_{ek,t}(x)$*. For a trapdoor td and an auxiliary part* $t_a \in \{0,1\}^*$*, the lossy tag generation algorithm* $\mathsf{FTag}(td, t_a)$ *computes a core tag* $t_c \in \mathcal{T}_c$ *such that* $(t_a, t_c) \in \mathcal{T}_{loss}$*. We require that OT-LF has the following properties.*

Lossiness. *If t is injective, then so is the function $f_{ek,t}(x)$. If t is lossy, then $f_{ek,t}(x)$ computes a lossy function, which has only $2^{\ell_{\mathsf{LF}}}$ possible outputs.*

Additionally, it is possible to set the evaluation key so that the parameter ℓ_{LF} is constant even for larger domain.

Indistinguishability. *A lossy tag and a random tag are computationally indistinguishable for any PPT adversary $\mathcal{A}$, i.e.,*

$$\mathsf{Adv}^{\mathrm{ind}}_{\mathsf{LF},\mathcal{A}}(\kappa) := |\Pr\left[\mathcal{A}(ek,(t_a,t_c)) = 1\right] - \Pr\left[\mathcal{A}(ek,(t_a,t'_c)) = 1\right]|$$

is negligible in κ, where $(ek, td) \leftarrow \mathsf{FGen}(1^\kappa)$, $t_a \leftarrow \mathcal{A}(ek)$, $t_c \leftarrow \mathsf{FTag}(td, t_a)$ and $t'_c \leftarrow_R \mathcal{T}_c$.

Evasiveness. *It is hard to generate a fresh non-injective tag for any PPT adversary $\mathcal{A}$ even given a lossy tag, i.e.,*

$$\mathsf{Adv}^{\mathrm{eva}}_{\mathsf{LF},\mathcal{A}}(\kappa) := \Pr\left[\begin{array}{l} (t'_a,t'_c) \neq (t_a,t_c) \wedge \\ (t'_a,t'_c) \in \mathcal{T} \setminus \mathcal{T}_{inj} \end{array} : \begin{array}{l} (ek,td) \leftarrow \mathsf{FGen}(1^\kappa), \\ t_a \leftarrow \mathcal{A}(ek), t_c \leftarrow \mathsf{FTag}(td,t_a), \\ (t'_a,t'_c) \leftarrow \mathcal{A}(ek,(t_a,t_c)). \end{array}\right]$$

is negligible in κ.

Hash Proof System. Hash proof system (HPS) was introduced by Cramer and Shoup [8]. For simplicity, we describe it as a key-encapsulation mechanism, as did in [22].

Let $\mathcal{PK}$, $\mathcal{SK}$ and $\mathcal{K}$ be the sets of public keys, secret keys and encapsulated keys. Let $\mathcal{C}$ be the set of (all possible) ciphertexts and $\mathcal{V} \subset \mathcal{C}$ be the set of all *valid* ciphertexts. Let $\mathcal{W}$ be a set and let χ be an injective map from $\mathcal{W}$ to $\mathcal{V}$. If for any ciphertext $c \in \mathcal{V}$, there exists a $w \in \mathcal{W}$ such that $\chi(w) = c$, we say that $(\mathcal{C}, \mathcal{V}, \mathcal{W}, \chi)$ is a subset membership problem and w is a witness of c. We require that there are efficient algorithms for sampling $sk \in \mathcal{SK}$, $c \in \mathcal{V}$ together with a witness $w \in \mathcal{W}$ and $c \in \mathcal{C} \setminus \mathcal{V}$ uniformly at random.

Let $\Lambda_{sk} : \mathcal{C} \to \mathcal{K}$ be a family of hash functions indexed by $sk \in \mathcal{SK}$. We say that Λ_{sk} is projective if there exists a projection $\mu : \mathcal{SK} \to \mathcal{PK}$ such that $\mu(sk)$ defines the action of Λ_{sk} over the subset $\mathcal{V}$. In contrast, nothing is guaranteed for $c \in \mathcal{C} \setminus \mathcal{V}$. In a hash proof system, it should be hard to compute $\Lambda_{sk}(c)$ from $\mu(sk)$ and $c \in \mathcal{C} \setminus \mathcal{V}$, which is guaranteed by the universal property of HPS (defined later in Definition 4). A HPS assumes the hardness of the subset membership problem over $\mathcal{C}$, meaning that for any PPT adversary

$$\mathsf{Adv}^{\mathrm{smp}}_{\mathsf{HPS},\mathcal{A}}(\kappa) = \Pr[\mathcal{A}(\mathcal{C},\mathcal{V},c) = 1 \mid c \leftarrow_R \mathcal{V}] - \Pr[\mathcal{A}(\mathcal{C},\mathcal{V},c) = 1 \mid c \leftarrow_R \mathcal{C} \setminus \mathcal{V}]$$

is negligible in κ.

Definition 4 (Universal hash proof system). *A hash proof system (HPS) consists of a tuple of PPT algorithms* $(\mathsf{Param}, \mathsf{Priv}, \mathsf{Pub})$*. The parameter generation algorithm* $\mathsf{Param}(1^\kappa)$*, on input 1^κ, generates an instance of* $\mathsf{param} = (\mathsf{group}, \mathcal{C}, \mathcal{V}, \mathcal{PK}, \mathcal{SK}, \mathcal{K}, \mu, \Lambda_{(\cdot)})$*, where* group *may contain additional structural parameters. For $sk \in \mathcal{SK}$ and $c \in \mathcal{C}$, the private evaluation algorithm* $\mathsf{Priv}(sk, c)$ *computes* $\mathsf{Priv}(sk, c) = \Lambda_{sk}(c)$*. For $pk = \mu(sk)$ and a witness w indicating that $c \in \mathcal{V}$, the public evaluation algorithm* $\mathsf{Pub}(pk, c, w)$ *computes* $\mathsf{Pub}(pk, c, w) = \Lambda_{sk}(c)$*.*

We say that a hash proof system is ϵ-universal, if for all $pk = \mu(sk)$, all $c \in \mathcal{C} \setminus \mathcal{V}$ and all $K \in \mathcal{K}$, it holds that $\Pr[\mathsf{Priv}(sk, c) = K \mid \mu(sk) = pk] \leq \epsilon$, *where the probability space is defined by choosing $sk \in \mathcal{SK}$ uniformly at random. We sometimes call the above value ϵ as the error rate of HPS.*

Chameleon Hash Function. A chameleon hash function [23] CH is essentially a keyed and randomized hash function, which consists of three PPT algorithms $(\mathsf{HGen}, \mathsf{HEval}, \mathsf{HEquiv})$. The key generation algorithm $\mathsf{HGen}(1^\kappa)$, on input a security parameter 1^κ, returns a key pair (ek_{ch}, td_{ch}). Given a preimage $x \in \{0,1\}^*$ and a randomness $r \in \mathcal{R}$, $\mathsf{HEval}(ek_{ch}, x; r)$ computes a hash value y. If r is uniformly distributed over $\mathcal{R}$, so is y over its range. We require that CH is collision-resistant, meaning that for any PPT adversary $\mathcal{A}$, the following probability

$$\mathsf{Adv}^{\mathrm{cr}}_{\mathsf{CH},\mathcal{A}}(1^\kappa) :=$$
$$\Pr\left[\begin{array}{l}(x', r') \neq (x, r) \wedge \\ \mathsf{HEval}(ek_{ch}, x'; r') = \mathsf{HEval}(ek_{ch}, x; r)\end{array} : \begin{array}{l}(ek_{ch}, td_{ch}) \leftarrow \mathsf{HGen}(1^\kappa) \\ (x', r', x, r) \leftarrow \mathcal{A}(ek_{ch})\end{array}\right]$$

is negligible in κ. We further require that given x, r, x' and the trapdoor td_{ch}, $\mathsf{HEquiv}(td_{ch}, x, r, x')$ computes r' such that $\mathsf{HEval}(ek_{ch}, x'; r') = \mathsf{HEval}(ek_{ch}, x; r)$ and the distribution r' is uniform over $\mathcal{R}$ given only ek_{ch} and x.

3 Refined Subgroup Indistinguishability Assumption

In this section, we present the formal definition of Refined Subgroup Indistinguishability (RSI) assumption and instantiate it under two number-theoretical assumptions.

Let $\mathsf{Gen}(1^\kappa)$ be a group generation algorithm that, on input a security parameter 1^κ, outputs a description of a finite commutative multiplicative group $\mathcal{G} = (\mathbb{G}, T, g, h)$, where $\mathbb{G}$ is a direct product of two groups: $\mathbb{G} = G_{\tau_1} \times G_{\tau_2}$, such that each group G_{τ_i} is a cyclic group of order τ_i, and g, h are generators of G_{τ_1}, G_{τ_2} respectively. We require that: (1) elements in $\mathbb{G}$ are efficiently checkable; (2) $\gcd(\tau_1, \tau_2) = 1$. This implies that $\mathbb{G}$ is also a cyclic group with order $\tau_1\tau_2$; (3) an upper bound $T \geq \tau_1 \cdot \tau_2$ is given in the group description, such that for $x \leftarrow_R \mathbb{Z}_T$, $x \bmod \tau_1\tau_2$ is ϵ-uniform over $\mathbb{Z}_{\tau_1\tau_2}$, where $\epsilon = \epsilon(\kappa)$ is negligible in κ. This implies that for $x \leftarrow_R \mathbb{Z}_T$, g^x (resp. h^x) is ϵ-uniform over G_{τ_1} (resp. G_{τ_2}).

Definition 5. *Let $\mathcal{G} = (\mathbb{G}, T, g, h) \leftarrow \mathsf{Gen}(1^\kappa)$. The refined subgroup indistinguishability (RSI) assumption in group $\mathbb{G}$ states that for any PPT adversary $\mathcal{A}$, the advantage*

$$\mathsf{Adv}^{\mathrm{rsi}}_{\mathcal{G},\mathcal{A}}(\kappa) := |\Pr[\mathcal{A}(\mathcal{G}, x) = 1 \mid x \leftarrow_R G_{\tau_1}] - \Pr[\mathcal{A}(\mathcal{G}, x) = 1 \mid x \leftarrow_R \mathbb{G}|$$

is negligible in κ.

From the above refined subgroup indistinguishability assumption, it is not hard to derive the following lemma.

Lemma 2. *Let $\mathcal{G} = (\mathbb{G}, T, g, h) \leftarrow \mathsf{Gen}(1^\kappa)$. If the refined subgroup indistinguishability assumption in group $\mathbb{G}$ holds, then for any PPT adversary $\mathcal{B}$*

$$|\Pr[\mathcal{B}(\mathcal{G}, x) = 1 \mid x \leftarrow_R G_{\tau_1}] - \Pr[\mathcal{B}(\mathcal{G}, x) = 1 \mid x \leftarrow_R \mathbb{G} \setminus G_{\tau_1}]| \leq 2\mathsf{Adv}^{\text{rsi}}_{\mathcal{G},\mathcal{A}}(\kappa) \quad (1)$$

$$|\Pr[\mathcal{B}(\mathcal{G}, x) = 1 \mid x \leftarrow_R G_{\tau_1}] - \Pr[\mathcal{B}(\mathcal{G}, x \cdot h) = 1 \mid x \leftarrow_R G_{\tau_1}]| \leq 2\mathsf{Adv}^{\text{rsi}}_{\mathcal{G},\mathcal{A}}(\kappa) \quad (2)$$

Finally, we present two instantiations of the refined subgroup indistinguishability assumptions: one is over groups of unknown order and the other is over groups of known order.

Example 1 (Instantiation under the QR assumption). Let p, q, p', q' be distinct primes with $p = 2p' + 1$ and $q = 2q' + 1$. For security parameter κ, p' and q' are both at least κ bits in length. Let $N = pq$ and $N' = p'q'$. From [8], $\mathbb{Z}_N^*$ has a unique subgroup $\mathbb{J}_N$ which is the set of elements in $\mathbb{Z}_N^*$ with Jacobi symbol 1. Let $\mathbb{QR}_N$ be the set of the quadratic residues modulo N and $G_2 = \{\pm 1\}$. Then, $\mathbb{J}_N = \mathbb{QR}_N \times G_2$ and $\gcd(2, N') = 1$. Additionally, $h = -1$ generates G_2, and for a random $x \leftarrow_R \mathbb{Z}_N^*$, with overwhelming probability $g = x^2 \bmod N$ generates group $\mathbb{QR}_N$. Set $T = (N-1)/4$. Then, for $x \leftarrow_R \mathbb{Z}_T$, $x \bmod 2N'$ is $O(2^{-\kappa})$-uniform in $\mathbb{Z}_{2N'}$. The quadratic residuosity (QR) assumption states that it is hard to distinguish a random element in $\mathbb{J}_N$ from a random element in $\mathbb{QR}_N$. So, the QR assumption is an instantiation of the RSI assumption if we set $(\mathbb{G}, T, g, h) \leftarrow \mathsf{Gen}(1^\kappa)$, where $\mathbb{G} = \mathbb{J}_N$, $G_{\tau_1} = \mathbb{QR}_N$ (with $\tau_1 = N'$), $G_{\tau_2} = \{\pm 1\}$ (with $\tau_2 = 2$), $T = (N-1)/4$, $g = x^2 \bmod N$ (for $x \leftarrow_R \mathbb{Z}_N^*$) and $h = -1$.

Example 2 (Instantiation over a group of known order). Let $\mathbf{p}, p, q$ be distinct primes with $\mathbf{p} = 2pq+1$. For security parameter κ, p and q are both at least κ bits in length. Clearly, $\mathbb{Z}_{\mathbf{p}}^*$ has a unique subgroup of order $N = pq$, denoted by $\mathbb{QR}_{\mathbf{p}}$, which is the set of the quadratic residues modulo $\mathbf{p}$. Moreover, $\gcd(p, q) = 1$ and $\mathbb{QR}_{\mathbf{p}}$ can be uniquely decomposed as a direct product $\mathbb{QR}_{\mathbf{p}} = G_p \times G_q$, where G_p, G_q are cyclic groups of prime orders p, q respectively. For $x, y \leftarrow_R \mathbb{Z}_{\mathbf{p}}^*$, with overwhelming probability $g = x^q \bmod \mathbf{p}$ generates G_p and $h = y^p \bmod \mathbf{p}$ generates G_q. The refined subgroup indistinguishability assumption over group $\mathbb{QR}_{\mathbf{p}}$ is conjectured to hold if integer factorization of N is hard [28]. So, we obtain an instantiation of RSI assumption by setting $(\mathbb{G}, T, g, h) \leftarrow \mathsf{Gen}(1^\kappa)$, where $\mathbb{G} = \mathbb{QR}_{\mathbf{p}}$, $G_{\tau_1} = G_p$ (with $\tau_1 = p$), $G_{\tau_2} = G_q$ (with $\tau_2 = q$), $T = pq$, $g = x^q \bmod \mathbf{p}$ (for $x \leftarrow_R \mathbb{Z}_{\mathbf{p}}^*$) and $h = y^p$ (for $y \leftarrow_R \mathbb{Z}_{\mathbf{p}}^*$).

4 Leakage-Resilient CCA-secure PKE under the RSI Assumption

Following Qin and Liu's generic construction of leakage-resilient CCA-secure PKE schemes from any universal hash proof systems and any one-time lossy filters [31], we present an efficient instantiation under the refined subgroup indistinguishability assumption in this section.

The rest of this section is organized as follows. In Section 4.1, we give an overview of Qin and Liu's approach to leakage-resilient CCA-security. In section 4.2 and Section 4.3, we present efficient constructions of universal hash proof system and one-time lossy filter from any RSI assumption respectively. Finally, in Section 4.4, we show how to construct a leakage-flexible (with leakage rate of [0,1)) PKE scheme under a specific RSI assumption.

4.1 Review of Qin and Liu's Approach to LR-CCA Security

Recently, Qin and Liu [31] proved that a universal hash proof (UHP) system, combined with a one-time lossy filter (OT-LF), yields a public-key encryption (PKE) scheme that is secure against key-leakage chosen-ciphertext attacks. This approach results in a simple and efficient CCA-secure PKE scheme with a higher leakage rate than those constructions solely from UHPs [27,25].

More precisely, they applied a UHP system as a basic (CPA-secure) encryption scheme to hide the plaintext and then applied an OT-LF as a message authentication code (MAC) to verify the well-formedness of the ciphertext. In fact, the HPS is used as a key encapsulation mechanism and the encapsulated key is exactly the hash value $\Lambda_{sk}(c)$, which functions in two ways: (1) it is used as an input of a random extractor to distill a random string for hiding a plaintext; (2) it is used as a MAC key to authenticate one-time lossy filter's tag. By the hardness of the underlying subset membership problem and the universality property of HPS, $\Lambda_{sk}(c)$ is computationally indistinguishable from a random variable that has at least $\log(1/\epsilon)$ min-entropy if HPS is ϵ-universal. While in the security proof, the challenge ciphertext uses a lossy LF tag which results in a MAC that only reveals a constant amount of information on $\Lambda_{sk}(c)$. Thus, the PKE scheme can withstand almost $\log(1/\epsilon)$-bit leakage of the secret key. Suppose that $(\mathsf{Param}, \mathsf{Priv}, \mathsf{Pub})$ is an ϵ-universal HPS, $(\mathsf{FGen}, \mathsf{FEval}, \mathsf{FTag})$ is a $(\mathcal{K}, \ell_{\mathsf{LF}})$-one-time lossy filter, $\mathcal{H}$ is a family of universal hash functions from $\mathcal{K}$ to $\{0,1\}^m$. Then, the PKE scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\{0,1\}^m$ from [31] works as follows.

- $(PK, SK) \leftarrow \mathsf{Kg}(1^\kappa)$. Run $\mathsf{Param}(1^\kappa)$ to produce a HPS instance: $\mathsf{param} = (\mathsf{group}, \mathcal{C}, \mathcal{V}, \mathcal{PK}, \mathcal{SK}, \mathcal{K}, \mu, \Lambda_{(\cdot)})$. Pick $sk \leftarrow_R \mathcal{SK}$ and set $pk = \mu(sk)$. Run $(ek, td) \leftarrow \mathsf{FGen}(1^\kappa)$. Return $PK = (pk, ek)$ and $SK = sk$.
- $C \leftarrow \mathsf{Enc}(PK, M)$. For $M \in \{0,1\}^m$, it samples a random $c \in \mathcal{V}$ together with its witness w, and then computes $K = \mathsf{Pub}(pk, c, w)$. Next, it samples $h \leftarrow_R \mathcal{H}$ and $t_c \leftarrow_R \mathcal{T}_c$. Finally, it returns

$$C = (c, h, h(K) \oplus M, \mathsf{FEval}(ek, t, K), t_c)$$

  where $t = (t_a, t_c)$ and $t_a = (c, h, h(K) \oplus M)$.
- $M/\perp \leftarrow \mathsf{Dec}(SK, C)$: For $C = (c, h, \psi, v, t_c)$, it computes $K' = \mathsf{Priv}(sk, c)$, and then checks whether $\mathsf{FEval}(ek, t, K') = v$ where $t = ((c, h, \psi), t_c)$. If not, it returns $\perp$, else returns $M = h(K') \oplus \psi$.

From [31], the security of the above scheme is established by the following theorem.

Theorem 1. *If there exists an ϵ-universal HPS and a $(\mathcal{K}, \ell_{\mathsf{LF}})$-one-time lossy filter, then there exists a CCA-secure PKE scheme with any leakage of λ bits,* *as long as* $\lambda \leq \log(1/\epsilon) - m - \ell_{\mathsf{LF}} - \omega(\log \kappa)$*, where* m *is the plaintext length. Additionally, by reducing the error rate* ϵ *of HPS, the leakage rate in the above scheme can be arbitrarily close to* $\log(1/\epsilon)/|sk|$.

4.2 Universal Hash Proof System from the RSI Assumption

Let $\mathcal{G} = (\mathbb{G}, T, g, h)$, where $\mathbb{G} = G_{\tau_1} \times G_{\tau_2}$, be a group description returned by $\mathsf{Gen}(1^\kappa)$. We can build a subset membership problem by setting $\mathcal{C} = \mathbb{G}$ and $\mathcal{V} = G_{\tau_1}$ (with witness set $\mathcal{W} = \mathbb{Z}_T$). From Lemma 2, this subset membership problem is hard under the refined subgroup indistinguishability assumption. Next, we build a universal hash proof system for $(\mathcal{C}, \mathcal{V})$.

Construction 1 (UHP). *The hash proof system* $(\mathsf{Param}, \mathsf{Priv}, \mathsf{Pub})$ *is defined as follows:*

- $\mathsf{Param}(1^\kappa)$*: run* $\mathcal{G} = (\mathbb{G}, T, g, h) \leftarrow \mathsf{Gen}(1^\kappa)$*, where* $\mathbb{G} = G_{\tau_1} \times G_{\tau_2}$*. Define*

$$\mathcal{C} = \mathbb{G}, \quad \mathcal{V} = G_{\tau_1}, \quad \mathcal{W} = \mathbb{Z}_T, \quad \mathcal{PK} = \mathbb{G}, \quad \mathcal{SK} = \mathbb{Z}_T, \quad \mathcal{K} = \mathbb{G}.$$

  Clearly, for $c \in \mathcal{V}$*, there exists a witness* $w \in \mathcal{W}$ *such that* $c = g^w$*. For* $sk = x \in \mathcal{SK}$ *and* $c \in \mathcal{C}$*, we define*

$$\mu(sk) = g^x \in \mathbb{G}, \qquad \Lambda_{sk}(c) = c^x \in \mathbb{G}$$

  Finally, $\mathsf{Param}(1^\kappa)$ *outputs* $\mathsf{param} = (\mathcal{G}, \mathcal{C}, \mathcal{V}, \mathcal{PK}, \mathcal{SK}, \mathcal{K}, \mu, \Lambda_{(\cdot)})$.
- $\mathsf{Priv}(sk, c)$*: for* $sk \in \mathcal{SK}$ *and* $c \in \mathcal{C}$*, compute* $K = \Lambda_{sk}(c) = c^x$*, where* $sk = x$.
- $\mathsf{Pub}(pk, c, w)$*: for* $pk = \mu(sk) = g^x \in \mathbb{G}$ *and a witness* $w \in \mathcal{W}$ *such that* $c = g^w \in \mathbb{G}$*, compute* $K = pk^w$ *which equals* $\Lambda_{sk}(c) = c^x$.

Theorem 2. *Suppose that* $\widetilde{q} \geq 2$ *is the smallest prime factor of* τ_2*. Then, construction 1 gives a* $1/\widetilde{q}$*-universal hash proof system.*

Proof. Clearly, correctness follows from the definitions of the projection μ and the projective hash function $\Lambda_{sk}(\cdot)$, and the hardness of the subset membership follows from the RSI assumption and Lemma 2. It remains to prove its universality. To do so, it suffices to show that for all $pk = \mu(sk) \in \mathcal{PK}$, all $c \in \mathcal{C} \setminus \mathcal{V}$ and all $K \in \mathcal{K}$, it holds that $\Pr[\Lambda_{sk}(c) = K \mid \mu(sk) = pk] \leq 1/\widetilde{q}$. Recall that g has order τ_1. So, $pk = g^{sk} = g^{sk \bmod \tau_1}$ is determined only by the value $sk \bmod \tau_1$. If sk is uniform in $\mathbb{Z}_{\tau_1 \tau_2}$ and $\gcd(\tau_1, \tau_2) = 1$, by the Chinese Remainder Theorem, it holds that $sk \bmod \tau_2$ is still uniform over $\mathbb{Z}_{\tau_2}$ even for a fixed pk. Moreover, for any element $c \in \mathcal{C} \setminus \mathcal{V}$, it has a non-trivial component of order (at least) $\widetilde{q}$ and thus c^{sk} has at least $\widetilde{q}$ possible values uniformly distributed over its support. This means that $\Pr[\Lambda_{sk}(c) = K \mid \mu(sk) = pk] \leq 1/\widetilde{q}$. □

Reducing the error rate. As introduced in [8], we can reduce the error rate of a universal hash proof system from ϵ to $\epsilon^{\mathfrak{n}}$ by a trivial "$\mathfrak{n}$-fold parallelization".

4.3 One-Time Lossy Filter from the RSI Assumption

In this section, we first propose a variant of one-time lossy filters, namely all-but-one (ABO) lossy functions. Then, we show how to construct an ABO lossy function under the refined subgroup indistinguishability assumption. Finally, we show how to derive a one-time lossy filter from an ABO lossy function with large tag space, whose size is determined by κ.

All-But-One Lossy Functions. ABO lossy functions are a family of functions parameterized with a tag. All tags are injective, leading to injective functions, except for one lossy tag, leading to a lossy function. ABO lossy functions are conceptionally simpler than one-time lossy filters. For one-time lossy filters, a tag consists of an auxiliary and a core tag part; lossy tags are produced via a trapdoor for any auxiliary tags. For ABO lossy functions, it simply uses arbitrary bit strings as tags. There is only one lossy tag which can be predetermined.

Definition 6 (ABO lossy functions). *A collection of* (Dom, ℓ)*-ABO lossy functions with tag space* B *consists of two PPT algorithms* $(\mathsf{ABOGen}, \mathsf{ABOEval})$*. The key generation algorithm* $\mathsf{ABOGen}(1^\kappa, b^*)$ *takes as input a security parameter* 1^κ *and any* $b^* \in B$*, and samples an evaluation key* ek*. The evaluation algorithm* $\mathsf{ABOEval}(ek, b, x)$*, for* $b \in B$ *and* $x \in \mathsf{Dom}$*, computes* $f_{ek,b}(x)$*. We require the following properties.*

Lossiness. *For injective tags (i.e.,* $b \neq b^*$*),* $\mathsf{ABOEval}(ek, b, x)$ *computes an injective function* $f_{ek,b}(x)$*. For the lossy tag* b^**,* $\mathsf{ABOEval}(ek, b^*, x)$ *computes a lossy function* $f_{ek,b^*}(x)$ *which only reveals at most* ℓ*-bit information of* x*. We require that by setting the parameter of evaluation key* ek*, the size of domain* Dom *is flexible even for constant* ℓ*.*

Hidden lossy tag. *For any PPT adversary* $\mathcal{A}$ *and for any* $b_0^*, b_1^* \in B$*, the following advantage*

$$\mathsf{Adv}_{\mathsf{ABO},\mathcal{A}}(\kappa) := \left|\Pr\left[\mathcal{A}(1^\kappa, ek_0) = 1\right] - \Pr\left[\mathcal{A}(1^\kappa, ek_1) = 1\right]\right|$$

is negligible in κ*, where* $ek_0 \leftarrow \mathsf{ABOGen}(1^\kappa, b_0^*)$ *and* $ek_1 \leftarrow \mathsf{ABOGen}(1^\kappa, b_1^*)$*.*

The conception of ABO lossy functions is very similar to ABO lossy *trapdoor* functions introduced by Peikert and Waters [29]. However, we do not require efficient inversion. Instead, we require that the lossy function reveals only a constant amount of information on its input even for flexibly large domain. The following construction from an ABO lossy function $(\mathsf{ABOGen}, \mathsf{ABOEval})$ with a tag space B (even for $B = \{0, 1\}$) results in a new one $(\widetilde{\mathsf{ABOGen}}, \widetilde{\mathsf{ABOEval}})$ with tag space $B^{\widetilde{n}}$ for any positive integer $\widetilde{n}$ (the analogous construction for ABO lossy trapdoor functions are shown in [29]).

Construction 2. *Let* $(\mathsf{ABOGen}, \mathsf{ABOEval})$ *be a collection of* (Dom, ℓ)*-ABO lossy functions with tag space* B*. We define* $(\widetilde{\mathsf{ABOGen}}, \widetilde{\mathsf{ABOEval}})$ *as follows.*

- $\widetilde{\mathsf{ABOGen}}(1^\kappa, \widetilde{b^*})$: *for* $\widetilde{b^*} = (b_1^*, \cdots, b_{\widetilde{n}}^*) \in B^{\widetilde{n}}$, *it runs* $ek_i \leftarrow \mathsf{ABOGen}(1^\kappa, b_i^*)$, $i = 1, \ldots, \widetilde{n}$, *and returns* $\widetilde{ek} = (ek_1, \ldots, ek_{\widetilde{n}})$.
- $\widetilde{\mathsf{ABOEval}}(\widetilde{ek}, \widetilde{b}, x)$: *for* $\widetilde{b} = (b_1, \cdots, b_{\widetilde{n}}) \in B^{\widetilde{n}}$ *and* $x \in \mathsf{Dom}$, *it computes*
$$f_{\widetilde{ek},\widetilde{b}}(x) = (f_{ek_1,b_1}(x), \ldots, f_{ek_{\widetilde{n}},b_{\widetilde{n}}}(x)).$$

Lemma 3. *Construction 2 gives a collection of* $(\mathsf{Dom}, \widetilde{n}\ell)$*-ABO lossy functions with tag space* $B^{\widetilde{n}}$.

Proof. The proof is nearly straightforward. First, for a lossy tag $\widetilde{b^*}$, all $f_{ek_i,b_i^*}(x)$s work in lossy mode and thus reveal at most $\widetilde{n}\ell$-bit information of their common input x. Secondly, for an injective tag $\widetilde{b} \neq \widetilde{b^*}$, there must exist an index $i \in [\widetilde{n}]$ such that $b_i \neq b_i^*$. That is, $f_{ek_i,b_i}(x)$ computes an injective function and so does $f_{\widetilde{ek},\widetilde{b}}(x)$. □

From RSI Assumption to ABO lossy functions. We start from a RSI instance to derive a collection of ABO lossy functions with tag space $\{0,1\}$.

Construction 3. *Let* $\mathcal{G} = (\mathbb{G}, T, g, h)$ *and* $\mathbb{G} = G_{\tau_1} \times G_{\tau_2}$ *be defined as in Section 3. Let* $I = (I_{i,j}) \in G_{\tau_2}^{n\times n}$ *be an* $n \times n$ *matrix over group* G_{τ_2}, *where* $I_{i,j} = 1$ *if* $i \neq j$ *and* $I_{i,i} = h$ *for all* $i, j \in [n]$. *Set* $B = \{0,1\}$ *and* $\mathsf{Dom} = \mathbb{Z}_{\tau_2}^n$. *We define* $(\mathsf{ABOGen}, \mathsf{ABOEval})$ *as follows.*

- $\mathsf{ABOGen}(1^\kappa, b^*)$: *for* $b^* \in B$, *it picks* $r_1, \ldots, r_n, s_1, \ldots, s_n \leftarrow_R \mathbb{Z}_T$ *and sets*
$$R = \begin{pmatrix} g^{r_1} \\ g^{r_2} \\ \vdots \\ g^{r_n} \end{pmatrix} \qquad S = \begin{pmatrix} g^{r_1 s_1} h^{b^*} & g^{r_1 s_2} & \cdots & g^{r_1 s_n} \\ g^{r_2 s_1} & g^{r_2 s_2} h^{b^*} & \cdots & g^{r_2 s_n} \\ \vdots & \vdots & \ddots & \vdots \\ g^{r_n s_1} & g^{r_n s_2} & \cdots & g^{r_n s_n} h^{b^*} \end{pmatrix}$$
Finally, $\mathsf{ABOGen}(1^\kappa, b^*)$ *returns* $ek = (R, S) \in \mathbb{G}^n \times \mathbb{G}^{n\times n}$.
- $\mathsf{ABOEval}(ek, b, x)$: *for* $ek = (R, S)$, $b \in B$ *and* $x = (x_1, \ldots, x_n) \in \mathbb{Z}_{\tau_2}^n$, *it computes*
$$f_{ek,b}(x) := \big(x \cdot R, x \cdot (S \otimes I^{-b})\big) = \Big(g^{\sum_{i=1}^n x_i r_i}, \big(g^{s_j \cdot \sum_i^n x_i r_i} \cdot h^{(b^*-b)x_j}\big)_{j=1}^n\Big)$$
where $\otimes$ *denotes the component-wise product of matrices over* $\mathbb{G}$.

Lemma 4. *Construction 3 forms a collection of* $(\mathbb{Z}_{\tau_2}^n, \log \tau_1)$*-ABO lossy functions with tag space* $B = \{0,1\}$.

Proof. It is a straightforward calculation to verify that: (1) for $b = b^*$, $f_{ek,b^*}(x)$ is completely determined by $g^{\sum_{i=1}^n x_i r_i}$ which has only τ_1 possible values; (2) for $b \neq b^*$, $f_{ek,b}(x)$ completely determines the vector $(h^{(b^*-b)x_1}, \ldots, h^{(b^*-b)x_n})$, hence $(x_1, \ldots, x_n)$. So it is an injective map. The remainder is to show its hidden lossy tag property. Let $S[j,k]$ denote the entry of matrix S, located by row j and column k. For any $b_0^*, b_1^* \in B$, let $\mathcal{EK}_i = (R_i, S_i)$, $0 \leq i \leq n$, be the distribution on the function evaluation key, where $R_i = R$ and S_i is almost the same as S except that the first i diagonal elements of S_i are now $\left(S_i[j,j] = g^{r_j s_j} h^{b_1^*}\right)_{1 \leq j \leq i}$ while the last $n-i$ diagonal elements of S_i are $\left(S_i[j,j] = g^{r_j s_j} h^{b_0^*}\right)_{i+1 \leq j \leq n}$. Clearly, $\mathcal{EK}_0$ is the distribution output by $\mathsf{ABOGen}(1^\kappa, b_0^*)$ and $\mathcal{EK}_n$ is the distribution output by $\mathsf{ABOGen}(1^\kappa, b_1^*)$. It suffices to show that for any $1 \leq i \leq n$, $\mathcal{EK}_{i-1}$ and $\mathcal{EK}_i$ are computationally indistinguishable under the RSI assumption. To do so, we again define two distributions $\mathcal{EK}'_{i-1} = (R'_{i-1}, S'_{i-1})$ and $\mathcal{EK}'_i = (R'_i, S'_i)$, where $\mathcal{EK}'_{i-1}$ is almost the same as $\mathcal{EK}_{i-1}$ except for the value of $R'_{i-1}[i]$ and $(S'_{i-1}[i,k])_{k\in[n]}$. Now $R'_{i-1}[i] := g^{r_i}h$ while $R_{i-1}[i] = g^{r_i}$, and $(S'_{i-1}[i,k])_{k\in[n]} = \left((g^{r_i}h)^{s_k} h^{b_0^*}\right)_{k\in[n]}$ while $(S_{i-1}[i,k])_{k\in[n]} = \left(g^{r_i s_k} h^{b_0^*}\right)_{k\in[n]}$. Similarly, $\mathcal{EK}'_i$ is almost the same as $\mathcal{EK}_i$ except for the value of $R'_i[i]$ and $(S'_i[i,k])_{k\in[n]}$. Now $R'_i[i] := g^{r_i}h$ while $R_i[i] = g^{r_i}$, and $(S'_i[i,k])_{k\in[n]} = \left((g^{r_i}h)^{s_k} h^{b_1^*}\right)_{k\in[n]}$ while $(S_i[i,k])_{k\in[n]} = \left(g^{r_i s_k} h^{b_1^*}\right)_{k\in[n]}$. It is a straightforward reduction to show that if there exists a PPT algorithm $\mathcal{A}$ that can distinguish $\mathcal{EK}_{i-1}$ and $\mathcal{EK}'_{i-1}$, we can construct a PPT algorithm $\mathcal{D}$ to distinguish the distributions defined in the left side of Eq. (2). This also applies to $\mathcal{EK}_i$ and $\mathcal{EK}'_i$. From Lemma 2, it follows that

$$\Pr[\mathcal{A}(ek) = 1 \mid ek \leftarrow_R \mathcal{EK}_{i-1}] - \Pr[\mathcal{A}(ek) = 1 \mid ek \leftarrow_R \mathcal{EK}'_{i-1}] \leq 2\mathsf{Adv}^{\text{rsi}}_{\mathcal{G},\mathcal{D}}(\kappa) \quad (3)$$
$$\Pr[\mathcal{A}(ek) = 1 \mid ek \leftarrow_R \mathcal{EK}_i] - \Pr[\mathcal{A}(ek) = 1 \mid ek \leftarrow_R \mathcal{EK}'_i] \leq 2\mathsf{Adv}^{\text{rsi}}_{\mathcal{G},\mathcal{D}}(\kappa) \quad (4)$$

Additionally, given $r_1, \ldots, r_n, s_1, \ldots, s_n \leftarrow_R \mathbb{Z}_T$, (R'_{i-1}, S'_{i-1}) take exactly the same values as (R'_i, S'_i) except that $S'_{i-1}[i,i] = (g^{r_i}h)^{s_i} h^{b_0^*}$ but $S'_i[i,i] = (g^{r_i}h)^{s_i} h^{b_1^*}$. Next we will show that $S'_{i-1}[i,i]$ is statistically indistinguishable to $S'_i[i,i]$, given the value of $r_1, \ldots, r_n, s_1, \ldots, s_n$.

Observe that the information of s_i is characterized by g^{s_i} in both (R'_{i-1}, S'_{i-1}) and (R'_i, S'_i). If s_i is chosen from $\mathbb{Z}_{\tau_1\tau_2}$ uniformly at random, $s_i \bmod \tau_2$ is uniform over $\mathbb{Z}_{\tau_2}$ even conditioned on the value of $s_i \bmod \tau_1$, according to Chinese Remainder Theorem. Now that s_i is ϵ-uniform over $\mathbb{Z}_{\tau_1\tau_2}$, so $s_i \bmod \tau_2$ is also ϵ-uniform over $\mathbb{Z}_{\tau_2}$, even conditioned on the value of $g^{s_i} = g^{s_i \bmod \tau_1}$. Consequently,

$$S'_{i-1}[i,i] =$$
$$(g^{r_i}h)^{s_i} h^{b_0^*} = g^{r_i s_i} h^{s_i \bmod \tau_2 + b_0^*} \approx_s g^{r_i s_i} h^{s_i \bmod \tau_2 + b_1^*} = (g^{r_i}h)^{s_i} h^{b_1^*} = S'_i[i,i].$$

So, $\mathcal{EK}'_{i-1} \approx_s \mathcal{EK}'_i$. Combined with Eq. (3) and Eq. (4), we have that $\mathcal{EK}_{i-1} \approx_c \mathcal{EK}_i$ holds for all i. This completes the proof of Lemma 4. □

Applying the method of Construction 2, we can amplify the tag space $\{0,1\}$ in Construction 3 to space $\{0,1\}^{\widetilde{n}}$ for any positive integer $\widetilde{n}$, resulting in a $(\mathbb{Z}^n_{\tau_2}, \widetilde{n} \log \tau_1)$-ABO lossy function. However, the information revealed by the lossy function increases linearly with the extension factor (i.e., $\widetilde{n}$) of the tag space via this method. To solve this problem, we can set R as a global parameter. That is, each function evaluation key ek_i has the same R but different S_i. As we proved earlier, for a lossy tag b_i^*, $f_{ek_i, b^*}(x)$ is completely determined by the value $x \cdot R = g^{\sum_{i=1}^n x_i r_i}$ which has τ_1 possible values. Thus, the $\widetilde{n}$ concatenation

$f_{ek_1,b_1^*}(x)||\cdots||f_{ek_{\widetilde{n}},b_{\widetilde{n}}^*}(x)$ in Construction 2 still has τ_1 possible values. In this way, we have a $(\mathbb{Z}_{\tau_2}^n, \log\tau_1)$-ABO lossy function with large tag space $B = \{0,1\}^{\widetilde{n}}$ for any positive integer $\widetilde{n}$.

Next, we show that if the order τ_2 of G_{τ_2} is large enough, it is possible to obtain ABO lossy function with large tag space directly. For a security parameter κ, let $\theta = \omega(\log\kappa)$ be a suitable tag length. We assume that $\theta \leq \lfloor\log\tau_2\rfloor - 1$. Set $\tau_2' = \lfloor\tau_2/(2^\theta - 1)\rfloor$ and thus $\tau_2' \geq 2$. We introduce two variants of Construction 3.

Variant I. This variant is the same as Construction 3, except for the tag space and the domain. In this case, we set $B = \{0,1\}^\theta$ and $\mathsf{Dom} = \mathbb{Z}_{\tau_2'}^n$. Clearly, for an injective tag b and an input $x = (x_1, \ldots, x_n) \in \mathbb{Z}_{\tau_2'}^n$, $|(b^* - b)x_i| \leq \tau_2$ for all i. Since h has order τ_2, x_i is completely determined by the group element $h^{(b^*-b)x_i}$ and the value $(b^* - b)$, i.e., $x_i = (\log_h h^{(b^*-b)x_i})/(b^* - b)$. Thus, $f_{ek,b}(x)$ computes an injective function. While for the lossy tag b^*, $f_{ek,b^*}(x)$ reveals at most $\log\tau_1$ bits information of its input x. In this case, Construction 3 now becomes a collection of $(\mathbb{Z}_{\tau_2'}^n, \log\tau_1)$-ABO lossy functions with tag space $B = \{0,1\}^\theta$. Additionally, we can amplify the domain size with large n without increasing the parameter $\log\tau_1$. Construction 3 is in fact the special case of $\theta = 1$.

Variant II. If τ_2 is a prime or the smallest prime factor of τ_2 is larger than $2^\theta - 1$, we can set $B = \{0,1\}^\theta$ and $\mathsf{Dom} = \mathbb{Z}_{\tau_2}^n$. In this case, $\gcd(b^* - b, \tau_2) = 1$, hence $(b^* - b)^{-1} \mod \tau_2$ always exists. It is not hard to see that Construction 3 now becomes a collection of $(\mathbb{Z}_{\tau_2}^n, \log\tau_1)$-ABO lossy functions with tag space $B = \{0,1\}^\theta$.

If τ_1 is a prime, we further choose $n = 1$ and $\mathsf{Dom} = \mathbb{Z}_{\tau_1\tau_2}$ (note that the domain is now further enlarged to $\mathbb{Z}_{\tau_1\tau_2}$), and reduce the evaluation key ek to one group element $g^{r_1s_1}h^{b^*}$. Then, for $x \in \mathbb{Z}_{\tau_1\tau_2}$ and $b \neq b^*$, $f_{ek,b}(x) = g^{r_1s_1x}h^{(b^*-b)x}$ is injective, and gives a collection of $(\mathbb{Z}_{\tau_1\tau_2}, \log\tau_1)$-ABO lossy functions, which is just the case used later in Section 4.4.

From ABO lossy functions to One-time Lossy Filters. We start from a collection of ABO lossy functions with a large tag space determined by security parameter κ and a family of chameleon hash functions, to derive a collection of one-time lossy filters.

Construction 4. *Let* $(\mathsf{ABOGen}, \mathsf{ABOEval})$ *be a collection of* (Dom, ℓ)*-ABO lossy functions with tag space* B *and let* $(\mathsf{HGen}, \mathsf{HEval}, \mathsf{HEquiv})$ *be a chameleon hash function from* $\{0,1\}^* \times \mathcal{R}$ *to* B*. We define* $\mathsf{LF} = (\mathsf{FGen}, \mathsf{FEval}, \mathsf{FTag})$ *as follows.*

- $\mathsf{FGen}(1^\kappa)$*: for a security parameter* 1^κ*, it first runs* $(ek_{ch}, td_{ch}) \leftarrow \mathsf{HGen}(1^\kappa)$*. Then,* $\mathsf{FGen}(1^\kappa)$ *selects* $t_a^* \in \{0,1\}^*$ *and* $t_c^* \in \mathcal{R}$ *uniformly at random, and computes* $b^* = \mathsf{HEval}(ek_{ch}, t_a^*; t_c^*)$*; Next, it runs* $ek' \leftarrow \mathsf{ABOGen}(1^\kappa, b^*)$*. Finally, it returns* $ek = (ek_{ch}, ek')$ *and* $td = (td_{ch}, t_a^*, t_c^*)$*. Set* $\mathcal{T} = \{0,1\}^* \times \mathcal{R}$ *and* $\mathcal{T}_{loss} = \{(t_a, t_c) : \mathsf{HEval}(ek_{ch}, t_a; t_c) = b^*\}$*.*
- $\mathsf{FEval}(ek, t, x)$*: for* $t = (t_a, t_c) \in \mathcal{T}$ *and* $x \in \mathsf{Dom}$*, it computes*

$$b = \mathsf{HEval}(ek_{ch}, t_a; t_c) \text{ and } f_{ek,t}(x) = f_{ek',b}(x).$$

– $\mathsf{FTag}(td, t_a)$: *for* $td = (td_{ch}, t_a^*, t_c^*)$ *and* $t_a \in \{0,1\}^*$, *it computes*

$$t_c = \mathsf{HEquiv}(td_{ch}, t_a^*, t_c^*, t_a).$$

Theorem 3. *Construction 4 gives a collection of* (Dom, ℓ)*-one-time lossy filters.*

Proof. The proof is very similar to the concrete DCR-based construction in [31]. Due to space limitation, we give it in the full version of this paper. □

4.4 An Efficient Leakage-Flexible CCA-secure PKE

In the previous two subsections, we presented the generic constructions of universal hash proof systems and one-time lossy filters from the refined subgroup indistinguishability assumptions. According to Theorem 1, we immediately obtain the following theorem.

Theorem 4. *Let* $\mathcal{G} = (\mathbb{G}, g, h, T) \leftarrow \mathsf{Gen}(1^\kappa)$*, where* $\mathbb{G} = G_{\tau_1} \times G_{\tau_2}$*. Suppose that the smallest prime factor of* τ_2 *is* $\widetilde{q} \geq 2$*. If the refined subgroup indistinguishability assumption holds over group* $\mathbb{G}$*, then we can construct a* λ*-LR-CCA secure PKE scheme with message space* $\{0,1\}^m$*, where the amount of leakage is bounded by* $\lambda \leq \mathfrak{n} \log \widetilde{q} - \log \tau_1 - m - \omega(\log \kappa)$ *and* $\mathfrak{n}$ *is a positive integer. In particular, the leakage rate can be made to approach* $\log \widetilde{q} / \log T$*.*

Next, we instantiate our generic construction under the RSI assumption introduced in Example 2 and obtain a leakage-flexible CCA-secure PKE scheme without pairing. (However, in our QR-based instantiation both the leakage-rate and the parameter are rather poor. The main reason is that the universality of the underlying hash proof system and the lossiness of the underlying one-time lossy filter are not good. For details, see the full version of this paper.)

Parameters. Recall that in Example 2, $\mathbf{p} = 2pq + 1$ is a prime and p, q both are primes too. So, $\mathbb{G} = \mathbb{QR}_{\mathbf{p}}$ can be decomposed as a direct product of two prime-order groups: $\mathbb{QR}_{\mathbf{p}} = G_p \times G_q$. If we choose $\mathfrak{n} = 1$, then by Theorem 2, we may obtain a $1/q$-universal hash proof system with secret key space $\mathcal{SK} = \mathbb{Z}_{pq}$ and encapsulated key space $\mathcal{K} = \mathbb{QR}_{\mathbf{p}}$. While by Theorem 3 for **Variant II**, we can obtain a $(\mathbb{Z}_{pq}, \log p)$-one-time lossy filter. Observe that, every element $K \in \mathbb{QR}_{\mathbf{p}}$ can be efficiently encoded as an element $K' \in \mathbb{Z}_{pq}$ by setting $K' := K - 1$ if $1 \leq K \leq pq$ and $K' := \mathbf{p} - K - 1$ if $pq + 1 \leq K \leq \mathbf{p} - 1$. So, by Theorem 4, we obtain a PKE scheme with leakage $\lambda \leq \log q - \log p - m - \omega(\log \kappa)$. Particularly, the ciphertext only contains two group elements in $\mathbb{Z}_{\mathbf{p}}^*$ (ignoring the other length fixed elements, e.g., the description of a universal hash function and an auxiliary tag). For a 80-bit security level, we choose $m = 80$, $\omega(\log \kappa) = 160$, $|p| = 512$ and $|q| \geq 512$. It suffices to guarantee that pq is hard to factor and thus the refined subgroup indistinguishability assumption in group $\mathbb{QR}_{\mathbf{p}}$ holds. In this case, $\lambda \leq \log q - 752$ and $|SK| \leq \log q + 512$. Therefore, the leakage rate $\frac{\lambda}{|SK|} = \frac{\log q - 752}{\log q + 512} = 1 - \frac{1264}{\log q + 512}$ is arbitrarily close to 1 if we choose a sufficiently large q.

Finally, we give a parameter comparison (for 80-bit security level) of this scheme with known leakage-flexible schemes [10,15] in Table 1 where $1-\alpha$ denotes the leakage rate, "SXDH" denotes the symmetric external Diffie-Hellman assumption, "DLIN" denotes the decisional linear assumption and "RSI" denotes the refined subgroup indistinguishability assumption. Assume that elements in a group of order q can be encoded as bit strings of length $|q|$. From Table 1, we can see that the ciphertext size (in bits) in our scheme grows slightly faster than the other three schemes. Nevertheless, our scheme has some interesting properties that do not exist in other schemes: simple construction, constant number of group elements in ciphertext and free of pairing.

Table 1. Parameters of leakage-flexible CCA-secure PKE schemes

Scheme	Group Type	Assumption	Group Size	Ciphertext Size	Pairing
			# bits	# $\mathbb{G}$	
DHLW10 [10]	Prime	SXDH	160	$\lceil (2/\alpha)(2+1/2)\rceil + 16$	Yes
DHLW10 [10]	Prime	DLIN	160	$\lceil (3/\alpha)(3+1/2)\rceil + 35$	Yes
GHV12 [15]	Prime	DLIN	160	$2\lceil 4/\alpha\rceil + 6$	Yes
Ours	Composite	RSI	$\lceil 1264/\alpha\rceil$	2	**No**

5 Conclusion

We proposed a simple and efficient construction of LR-CCA secure PKE scheme based on the Refined Subgroup Indistinguishability (RSI) assumption, which is a more general group of assumptions and can be instantiated under many number-theoretical assumptions. Our construction follows a recently proposed approach for leakage-resilient chosen-ciphertext security [31]. However, the known results in [31] has only a small leakage rate of $1/2 - o(1)$. Our construction further improved the leakage rate to $1 - o(1)$ under the RSI assumption over a pairing-free group of known order. As far as we know, this is the first pairing-free LR-CCA secure PKE with leakage rate of $1 - o(1)$.

References

1. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 474–495. Springer, Heidelberg (2009)
2. Alwen, J., Dodis, Y., Naor, M., Segev, G., Walfish, S., Wichs, D.: Public-key encryption in the bounded-retrieval model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 113–134. Springer, Heidelberg (2010)
3. Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R.: Circular-secure encryption from decision Diffie-Hellman. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 108–125. Springer, Heidelberg (2008)
4. Brakerski, Z., Goldwasser, S.: Circular and leakage resilient public-key encryption under subgroup indistinguishability. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 1–20. Springer, Heidelberg (2010)

5. Brakerski, Z., Kalai, Y.T., Katz, J., Vaikuntanathan, V.: Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In: FOCS 2010, pp. 501–510. IEEE Computer Society (2010)
6. Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 207–222. Springer, Heidelberg (2004)
7. Chow, S.S.M., Dodis, Y., Rouselakis, Y., Waters, B.: Practical leakage-resilient identity-based encryption from simple assumptions. In: Al-Shaer, E., Keromytis, A.D., Shmatikov, V. (eds.) CCS 2010, pp. 152–161. ACM (2010)
8. Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (2002)
9. Dodis, Y., Haralambiev, K., López-Alt, A., Wichs, D.: Cryptography against continuous memory attacks. In: FOCS 2010, pp. 511–520. IEEE Computer Society (2010)
10. Dodis, Y., Haralambiev, K., López-Alt, A., Wichs, D.: Efficient public-key cryptography in the presence of key leakage. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 613–631. Springer, Heidelberg (2010)
11. Dodis, Y., Kalai, Y.T., Lovett, S.: On cryptography with auxiliary input. In: Mitzenmacher, M. (ed.) STOC 2009, pp. 621–630. ACM (2009)
12. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J. Comput. 38(1), 97–139 (2008)
13. Dziembowski, S., Pietrzak, K.: Leakage-resilient cryptography. In: FOCS 2008, pp. 293–302. IEEE Computer Society (2008)
14. Faust, S., Kiltz, E., Pietrzak, K., Rothblum, G.N.: Leakage-resilient signatures. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 343–360. Springer, Heidelberg (2010)
15. Galindo, D., Herranz, J., Villar, J.L.: Identity-based encryption with master key-dependent message security and leakage-resilience. In: Foresti, S., Yung, M., Martinelli, F. (eds.) ESORICS 2012. LNCS, vol. 7459, pp. 627–642. Springer, Heidelberg (2012)
16. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Dwork, C. (ed.) STOC 2008, pp. 197–206. ACM (2008)
17. Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. 28(2), 270–299 (1984)
18. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: Cold boot attacks on encryption keys. In: van Oorschot, P.C. (ed.) USENIX Security Symposium 2008, pp. 45–60. USENIX Association (2008)
19. Hazay, C., López-Alt, A., Wee, H., Wichs, D.: Leakage-resilient cryptography from minimal assumptions. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 160–176. Springer, Heidelberg (2013)
20. Hofheinz, D.: Circular chosen-ciphertext security with compact ciphertexts. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 520–536. Springer, Heidelberg (2013)
21. Katz, J., Vaikuntanathan, V.: Signature schemes with bounded leakage resilience. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 703–720. Springer, Heidelberg (2009)

22. Kiltz, E., Pietrzak, K., Stam, M., Yung, M.: A new randomness extraction paradigm for hybrid encryption. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 590–609. Springer, Heidelberg (2009)
23. Krawczyk, H., Rabin, T.: Chameleon signatures. In: NDSS 2000. The Internet Society (2000)
24. Lewko, A.B., Rouselakis, Y., Waters, B.: Achieving leakage resilience through dual system encryption. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 70–88. Springer, Heidelberg (2011)
25. Li, S., Zhang, F., Sun, Y., Shen, L.: A new variant of the Cramer-Shoup leakage-resilient public key encryption. In: Xhafa, F., Barolli, L., Pop, F., Chen, X., Cristea, V. (eds.) INCoS 2012, pp. 342–346. IEEE (2012)
26. Liu, S., Weng, J., Zhao, Y.: Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks. In: Dawson, E. (ed.) CT-RSA 2013. LNCS, vol. 7779, pp. 84–100. Springer, Heidelberg (2013)
27. Naor, M., Segev, G.: Public-key cryptosystems resilient to key leakage. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 18–35. Springer, Heidelberg (2009)
28. González Nieto, J.M., Boyd, C., Dawson, E.: A public key cryptosystem based on the subgroup membership problem. In: Qing, S., Okamoto, T., Zhou, J. (eds.) ICICS 2001. LNCS, vol. 2229, pp. 352–363. Springer, Heidelberg (2001)
29. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: Dwork, C. (ed.) STOC 2008, pp. 187–196. ACM (2008)
30. Pietrzak, K.: A leakage-resilient mode of operation. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 462–482. Springer, Heidelberg (2009)
31. Qin, B., Liu, S.: Leakage-resilient chosen-ciphertext secure public-key encryption from hash proof system and one-time lossy filter. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 381–400. Springer, Heidelberg (2013)
32. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) STOC 2005, pp. 84–93. ACM (2005)
33. Yuen, T.H., Chow, S.S.M., Zhang, Y., Yiu, S.M.: Identity-based encryption resilient to continual auxiliary leakage. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 117–134. Springer, Heidelberg (2012)