J. Math. Cryptol. **7** (2013), 297–312
DOI 10.1515/jmc-2013-5007

New leakage-resilient CCA-secure public key encryption

Kaoru Kurosawa, Ryo Nojima and Le Trieu Phong

Communicated by Spyros Magliveras

Dedicated to Professor Tran Van Trung on the occasion of his 65th birthday

Abstract. This paper shows a generic method of constructing CCA-secure public key encryption schemes with leakage-resilience on the secret key. It is based on a new kind of universal$_2$ hash proof system which accepts an auxiliary parameter. Specifically, two schemes are presented, basing on the DCR assumption and DLIN assumption respectively.

Keywords. Public key encryption, CCA security, leakage-resilience, hash proof system.

2010 Mathematics Subject Classification. 11T71, 68P25.

1 Introduction

1.1 Background

Building cryptographic schemes secure even if the secrets are partially leaked is a trend in cryptography, motivating partially from side channel attacks. In this paper we are interested in public key encryption (PKE) schemes with leakage-resilience. Let us first summarize the literature.

In 2009, Akavia, Goldwasser, and Vaikuntanathan [1] gave the model and the first leakage-resilient chosen plaintext attack (IND-lrCPA) secure scheme under the LWE assumption. Afterwards, Naor and Segev [8] presented both IND-lrCPA-secure and leakage-resilient chosen ciphertext attack (IND-lrCCA) secure schemes based on the decisional Diffie–Hellman (DDH) assumption. More precisely, they used universal$_1$ hash proof systems (HPS) [2] to build IND-lrCPA-secure schemes. For IND-lrCCA-secure schemes, they used the Naor–Yung paradigm yielding systems with good leakage tolerance, but which are quite inefficient and thus of theoretical interest only. To achieve efficiency, they considered the Cramer–Shoup scheme [2] under the DDH assumption.

Dodis et al. [4] continued by schemes with very good leakage tolerance, but with a big trade-off in efficiency (see Table 1).

Schemes	#Exps [enc; dec]	Ciphertext size (in bits)	Leakage rate	Assumption
[8]	[4.5; 3]	$\lvert s\rvert + \lvert m\rvert + 3\lvert q\rvert$	$1/6$	DDH
[4]	—	$\geq (36 + 9/\delta)\lvert q\rvert$	$1 - \delta$	DLIN (pairing)
Ours	—	$\lvert s\rvert + \lvert m\rvert + (2 + \frac{1}{3})\lvert N_1\rvert$	$1/12$	DCR
Ours	[4.5; 1.5]	$\lvert s\rvert + \lvert m\rvert + (3 + \frac{1}{3})\lvert q\rvert$	$1/18$	DLIN (no pairing)

Table 1. IND-lrCCA-secure PKE schemes. s seed; m message; $q, \lvert q\rvert$ base group order and its bit length; N_1 base modulus; $0 < \delta < 1$ and $\ell_2 < \lvert q\rvert, \lvert N_1\rvert$. We treat one multi-exponentiation as 1.5 single exponentiation, and only consider schemes in $\mathbb{G} = \langle g\rangle$ for computational cost. The scheme in [4] requires heavy computation, including pairing, so we do not put the cost for comparison.

It might be quite curious that Naor and Segev did not mention anything on universal$_2$ HPS in [8]. Furthermore, they did not examine other well-known variants of Cramer–Shoup like the Kurosawa–Desmedt scheme [3, 7]. In fact, there are certain difficulties for settling these, as we show below.

1.2 Our contributions

Results. We show how to build IND-lrCCA-secure PKE schemes from universal$_2$ HPS *accepting an auxiliary input*. Specifically, two schemes are presented, basing on the decisional composite residuosity (DCR) assumption and DLIN assumption respectively. Our DCR-based scheme is the first one with IND-lrCCA security in the literature. Likewise, our DLIN-based scheme is the first one without pairing operations. Hence it is much more efficient than the previous scheme [4] albeit the leakage rate is smaller.

A comparison is given in Table 1, where the leakage rate is defined as the supremum of

$$\frac{\text{total leakage size}}{\text{secret key size}}$$

when considering large base groups.

Technical hurdles. For illustrative discussions, let us consider the Kurosawa–Desmedt scheme which is IND-CCA secure under the DDH assumption [7]. It serves as a warm up for our generic construction although the leakage rate is smaller than that of [8]. (The leakage rate is $1/12$ compared to $1/6$ in [8].)

The secret key is $sk = (x_1, x_2, y_1, y_2)$ and the public key contains $c = g_1^{x_1} g_2^{x_2}$ and $d = g_1^{y_1} g_2^{y_2}$, and a target collision resistant function TCR. A ciphertext on message m is of the form (u_1, u_2, e, t) where $u_1 = g_1^r$, $u_2 = g_2^r$, $e = \mathsf{SE}_{k_1}(m)$, $t = \mathsf{MAC}_{k_2}(e)$, where (k_1, k_2) is derived from $v = c^r d^{r \cdot \mathsf{TCR}(u_1, u_2)}$.

Roughly speaking, the crux in proving CCA security in [3,7] is to show that any v is randomly distributed given c, d and a fixed v^*. This implies that (k_1, k_2) is random, so that symmetric encryption $e = \mathsf{SE}_{k_1}(m)$ together with authentication $\mathsf{MAC}_{k_2}(e)$ will guarantee CCA security.

However, in the leakage setting, it is not ensured that v is random. This is because $v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$ (for $\alpha = \mathsf{TCR}(u_1, u_2)$) is written as a function of *sk*, and hence the adversary can ask for some information on it. A natural attempt to deal with this situation would be to extract random bits from v. Namely let $(k_1, k_2) = \mathsf{Ext}(v; s)$ for a randomness extractor Ext, with a random seed s additionally put in the ciphertext (to enable decryption). If v has high entropy, (k_1, k_2) should be random as required.

The attempt, while intuitively appealing, does not work! The reason is that the seed s is completely controlled by the adversary in decryption, and thus is not random. In turn, $(k_1, k_2) = \mathsf{Ext}(v; s)$ is not random as desired.

Looking into [8], the same issue occurs, and is resolved as follows. The value v itself is directly used for authentication, namely check $v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$ for every decryption request. However, the symmetric encryption key k_1 comes from another random source (an extra public key $h = g_1^{z_1} g_2^{z_2}$), which is *unavailable* in our setting. (In fact, that source causes additional computation and ciphertext size in [8], compared to ours.)

We overcome the above difficulty as follows. Let us split v into three equal parts, namely $v = k_0 \| k_1 \| k_2$, and note that k_0, k_1, k_2 have enough entropy when v does. Here we at least need the leakage amount $\lambda < |v|/3$. The leakage rates in our schemes are worsened by this step. The authentication (i.e. MAC) is now of the form $t = k_1 e \oplus k_2$. When k_1, k_2 have high entropy, this authentication will reject all ill-formed ciphertexts, since passing the authentication amounts to computing $k_2 = t \oplus k_1 e$. In addition, let the challenge $e^* = \mathsf{Ext}(k_0^*; s^*) \oplus m_b$ for random seed s^*. It seems that the same issue on the seed is repeated here, but it is not, since ill-formed ciphertexts are anyway rejected by the authentication, and s^* in forming the challenge ciphertext is not controlled by the adversary.

Generally, the same technique works for PKE derived from universal$_2$ HPS accepting an auxiliary parameter (which is the extractor's seed), as shown in Section 4.2.

Organization of this paper. We present the leakage-resilient scheme based on the Kurosawa–Desmedt scheme in Section 3. We show how to generalize the idea to universal$_2$ hash proof systems in Section 4.2, which additionally yields schemes based on DLIN and decisional composite residuosity (DCR) assumptions.

2 Preliminaries

Notations. For a set A, let $|A|$ denote its cardinality. Taking a randomly from A is expressed by $a \xleftarrow{\$} A$. Let $|a|$ denote the number of bits representing a. Hence $|a| - 1 \leq \log_2 a < |a|$.

DDH assumption. Let $\mathbb{G} = \langle g \rangle$ be a group of prime public order q generated by g. The DDH assumption on $\mathbb{G}$ asserts that for all poly-time distinguishers $\mathcal{D}$, $g_1, g_2 \xleftarrow{\$} \mathbb{G}$, and $r \neq s \xleftarrow{\$} \mathbb{Z}_q$, the distance

$$\epsilon_{\mathrm{ddh}} = \left|\Pr[\mathcal{D}(g_1, g_2, g_1^r, g_2^r) = 1] - \Pr[\mathcal{D}(g_1, g_2, g_1^r, g_2^s) = 1]\right|$$

is negligible on parameter $\log_2 q$.

Entropy and extractor. The statistical distance of random variables X, Y over a finite domain Ω is $\mathbf{SD}(X, Y) = \frac{1}{2} \sum_{a \in \Omega} |\Pr[X = a] - \Pr[Y = a]|$. The min-entropy of X is $\mathbf{H}_\infty(X) = -\log_2(\max_x \Pr[X = x])$. The average min-entropy of X conditioned on Y is

$$\tilde{\mathbf{H}}_\infty(X|Y) = -\log_2\big(E_{y \leftarrow Y}[2^{-H_\infty(X|Y=y)}]\big),$$

as defined in [5], which also proved the following result.

Lemma 2.1 ([5, Lemma 2.2]). *If Y has 2^λ possible values and Z is any random variable, then*

$$\tilde{\mathbf{H}}_\infty(X|Y, Z) \geq \tilde{\mathbf{H}}_\infty(X, Y|Z) - \lambda \geq \tilde{\mathbf{H}}_\infty(X|Z) - \lambda \geq \mathbf{H}_\infty(X, Z) - \lambda.$$

When applying the lemma in our context, Y stands for the leakage on secret key X, while Z is another information on X such as given by the public key. The lemma then says that, given a leakage amount of λ bits, the secret key's entropy is decreased by λ. Hereafter, when referring to entropy, we mean average min-entropy unless otherwise stated.

A function $\mathsf{Ext} : \{0, 1\}^n \times \mathsf{Seed} \to \{0, 1\}^\ell$ is called a $(k, \epsilon_{\mathsf{Ext}})$-randomness extractor if for all pairs of random variables (X, I) such that X is an n-bit string satisfying $\tilde{\mathbf{H}}_\infty(X|I) \geq k$,

$$\mathbf{SD}\big((\mathsf{Ext}(X, s), s, I), (\mathsf{rand}, s, I)\big) \leq \epsilon_{\mathsf{Ext}},$$

where $s \xleftarrow{\$} \mathsf{Seed}$ and $\mathsf{rand} \xleftarrow{\$} \{0, 1\}^\ell$. In other words, $\mathsf{Ext}(X, s)$ is nearly random given s and I (when ϵ_{Ext} is small enough). Randomness extractors can be realized via pairwise independent hash functions.

PKE with IND-lrCCA security. A PKE consists of key generation KG, encryption Enc, and decryption Dec algorithms. KG outputs public key pk and secret key sk. The algorithm $\mathsf{Enc}_{pk}(m)$ returns a ciphertext c which can be decrypted by $\mathsf{Dec}_{sk}(c)$.

To define leakage-resilient CCA security for PKE, consider the following game with adversary $\mathcal{A}$. First, $(pk, sk) \leftarrow \mathsf{KG}$ and pk is given to $\mathcal{A}$. In the so-called find stage, $\mathcal{A}$ can access to a decryption oracle $\mathsf{Dec}_{sk}(\cdot)$ to decrypt any string of its choice. Furthermore, $\mathcal{A}$ can query arbitrary functions f to a leakage oracle $\mathsf{Leak}_{sk}(\cdot)$ which returns $f(sk)$. We require that the total length of all returned $f(sk)$ must be less than a fixed λ in bits.

Then $\mathcal{A}$ submits a pair of m_0, m_1 such that $|m_0| = |m_1|$ to a challenge oracle. The oracle returns a challenge ciphertext $C^* = \mathsf{Enc}_{pk}(m_b)$, where $b \in \{0, 1\}$ is randomly chosen.

After that, in the guess stage, $\mathcal{A}$ can access to the decryption oracle $\mathsf{Dec}_{sk}(\cdot)$ but cannot to the leakage oracle $\mathsf{Leak}_{sk}(\cdot)$. (This restriction is necessary since otherwise $\mathcal{A}$ uses $f(\cdot) = \mathsf{Dec}_{(\cdot)}(C^*)$ to get partial information on m_b, so the game is trivial.) $\mathcal{A}$ is not allowed to query the challenge ciphertext C^* to the decryption oracle either. Finally, $\mathcal{A}$ returns b' as a guess of the hidden b.

The PKE scheme is IND-lrCCA-secure if

$$\left|\Pr[b' = b] - \frac{1}{2}\right|$$

is negligible for all poly-time $\mathcal{A}$.

3 Leakage-resilient Kurosawa–Desmedt scheme

In this section, we show a leakage-resilient variant of Kurosawa–Desmedt encryption scheme [3, 7] with the leakage rate $1/12$ under the DDH assumption. This is a warm up of our generic construction later in Section 4 although the leakage rate is smaller than $1/6$ in [8].

Let $\mathbb{G}$ be a group of order q. We assume that there exists an injection $\mathsf{KDF} : \mathbb{G} \to \{0, 1\}^{|q|}$. For example, let $\mathbb{G} = (\mathbb{Z}_q^*)^2$ be the q-order subgroup of $\mathbb{Z}_p^*$ (where $p = 2q + 1$ is also a prime). Then the following KDF satisfies our condition:[1]

$$\mathsf{KDF}(x) = \begin{cases} x & \text{if } 0 < x < p/2, \\ p - x & \text{if } p/2 < x < p. \end{cases}$$

Let $\mathsf{Ext} : \{0, 1\}^{|q|/3} \times \mathsf{Seed} \to \{0, 1\}^{\ell}$ be a $(|q|/3 - \lambda, \epsilon_{\mathsf{Ext}})$-randomness extractor, and $\mathsf{PRG} : \{0, 1\}^{\ell} \to \{0, 1\}^*$ be a pseudo-random generator. Also needed are

[1] This is because $-1 \in \mathbb{Z}_p^*$ is a quadratic non-residue, so $x \neq p - x'$ for $x, x' \in (\mathbb{Z}_p^*)^2$.

target collision resistant (TCR) functions $\mathsf{TCR} : \mathbb{G}^2 \times \mathsf{Seed} \to \mathbb{Z}_q$, and a collision resistant hash function $H : \{0,1\}^* \to \{0,1\}^{|q|/3}$.

Key generation: Let a secret key be $sk = (x_1, x_2, y_1, y_2) \xleftarrow{\$} \mathbb{Z}_q^4$. Compute $c = g_1^{x_1} g_2^{x_2}$ and $d = g_1^{y_1} g_2^{y_2}$, where $g_1, g_2 \xleftarrow{\$} \mathbb{G}$. The public key is $pk = (g_1, g_2, c, d)$.

Encryption of $m \in \{0,1\}^*$:

$$r \xleftarrow{\$} \mathbb{Z}_q,\ u_1 \leftarrow g_1^r,\ u_2 \leftarrow g_2^r,\ s \xleftarrow{\$} \mathsf{Seed},\ \alpha \leftarrow \mathsf{TCR}(u_1, u_2, s) \in \mathbb{Z}_q$$

$$v \leftarrow c^r d^{r\alpha},\ k_0 \| k_1 \| k_2 \leftarrow \mathsf{KDF}(v), \text{where } |k_0| = |k_1| = |k_2| = |q|/3$$

$$e \leftarrow \mathsf{PRG}(\mathsf{Ext}(k_0; s)) \oplus m,\ t \leftarrow k_1 H(e) + k_2 \ (\text{over GF}(2^{|q|/3}))$$

Output (u_1, u_2, e, t, s)

Decryption of (u_1, u_2, e, t, s):

$$\alpha \leftarrow \mathsf{TCR}(u_1, u_2, s),\ v \leftarrow u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2},\ k_0 \| k_1 \| k_2 \leftarrow \mathsf{KDF}(v).$$

If $t = k_1 H(e) + k_2$, then output $m = \mathsf{PRG}(\mathsf{Ext}(k_0; s)) \oplus e$. Else output $\perp$.

The leakage rate. Remember that the total leakage on sk which an adversary can learn from the leakage oracle is less than λ bits. Setting $2^{\lambda - |q|/3}$ (see below) to be negligible, i.e., $\lambda - \frac{|q|}{3} = -\eta$ for η-bit security leads to $\lambda = \frac{|q|}{3} - \eta$, which means the leakage rate $\frac{\lambda}{|sk|} = \frac{\lambda}{4|q|}$ approaches $\frac{1}{12}$ when the group size q becomes large.

Theorem 3.1. *The above scheme is IND-lrCCA-secure with leakage rate* 1/12 *under the DDH assumption.*

Proof. Let K_i denote the random variable induced by k_i for $i = 0, 1, 2$. We say that a ciphertext (u_1, u_2, e, t, s) is invalid if $u_1 = g_1^{r_1}$, $u_2 = g_2^{r_2}$ and $r_1 \neq r_2$. We will proceed in games, each of which is a modification of the previous one. Below, $\Pr[X_i] = \Pr[b' = b \text{ in } \mathbf{Game}_i]$.

Game$_0$: This game is the IND-lrCCA attack game with an adversary $\mathcal{A}$.

The challenge ciphertext is denoted by $C^* = (u_1^*, u_2^*, e^*, t^*, s^*)$. We denote by $r^*, \alpha^*, v^*, k_0^*, k_1^*, k_2^*$ the corresponding intermediate quantities. We also assume that $r^*, u_1^*, u_2^*, \alpha^*, v^*, k_0^*, k_1^*, k_2^*$ are computed at the beginning of the game because they do not depend on m_0, m_1 which are provided by $\mathcal{A}$ later.

Game$_1$: The challenge oracle computes v^* as

$$v^* = (u_1^*)^{x_1 + \alpha^* y_1} (u_2^*)^{x_2 + \alpha^* y_2},$$

where $u_1^* = g_1^{r^*}, u_2^* = g_2^{r^*}$ for $r^* \xleftarrow{\$} \mathbb{Z}_q, s^* \xleftarrow{\$} \mathsf{Seed}$ and $\alpha^* = \mathsf{TCR}(u_1^*, u_2^*, s^*)$. Then we have $\Pr[X_0] = \Pr[X_1]$ because the value of v^* remains the same in the two games.

Game$_2$**:** The challenge oracle chooses $r_1^* \neq r_2^* \in \mathbb{Z}_q$ randomly, and computes

$$(u_1^*, u_2^*) = (g_1^{r_1^*}, g_2^{r_2^*}).$$

We can show that $|\Pr[X_1] - \Pr[X_2]|$ is negligible under the DDH assumption in the same way as in [3,7]. In particular, the DDH distinguisher can simulate the leakage oracle which returns $f(sk)$ because sk is chosen by the DDH distinguisher.

Game$_3$**:** The decryption oracle is given not only sk but also ω such that $g_2 = g_1^{\omega}$. We can do this because we do not use the DDH distinguisher from now on. Then in the find stage, the decryption oracle returns $\perp$ for (u_1, u_2, e, t, s) if $u_2 \neq u_1^{\omega}$. That is, the simulator rejects all invalid ciphertexts in the find stage.

We show $|\Pr[X_2] - \Pr[X_3]|$ is negligible. Namely, we prove that in **Game**$_2$, any invalid ciphertext is rejected by the decryption oracle with overwhelming probability. Note that, from the adversary's point of view, $sk = (x_1, x_2, y_1, y_2)$ is uniformly random subject to $c = g_1^{x_1} g_2^{x_2}$ and $d = g_1^{y_1} g_2^{y_2}$, ignoring the leakage functions f for now.

Let $C' = (u_1, u_2, e, t, s)$ be the first invalid ciphertext queried by $\mathcal{A}$, where $u_1 = g_1^{r_1}, u_2 = g_2^{r_2}$ and $r_1 \neq r_2$. Let $v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$. Then

$$\begin{bmatrix} \log_{g_1} c \\ \log_{g_1} d \\ \log_{g_1} v \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 0 & \omega \\ r_1 & r_1\alpha & r_2\omega & r_2\omega\alpha \end{bmatrix}}_{U} \begin{bmatrix} x_1 \\ y_1 \\ x_2 \\ y_2 \end{bmatrix},$$

and the matrix U is of rank 3. This means that v is random from $\mathcal{A}$'s point of view.

Now $\mathcal{A}$ learns at most λ bits leakage $f(sk)$. Given $f(sk)$ and (c, d), the entropy of v is at least $\log q - \lambda$ from Lemma 2.1. The entropy of (K_0, K_1, K_2) is also $\log q - \lambda$ because $k_0 \| k_1 \| k_2 = \mathsf{KDF}(v)$ and KDF is an injection. Therefore for any k_0, k_1, k_2, we have

$$\Pr[K_0 = k_0, K_1 = k_1, K_2 = k_2] \leq \frac{2^{\lambda}}{q}.$$

Hence

$$\Pr[K_1 = k_1, K_2 = k_2] = \sum_{k_0} \Pr[K_0 = k_0, K_1 = k_1, K_2 = k_2] \leq 2^{|q|/3} \cdot \frac{2^{\lambda}}{q}.$$

Let $B = \{(k_1, k_2) \mid t = k_1 H(e) + k_2\}$. Then $|B| \le 2^{|q|/3}$. Finally we have

$$\begin{aligned}
\Pr_{k_1,k_2}[t = k_1 e' \oplus k_2] &= \sum_{(k_1,k_2)\in B} \Pr[K_1 = k_1, K_2 = k_2] \\
&\le \sum_{(k_1,k_2)\in B} 2^{|q|/3} \cdot \frac{2^\lambda}{q} \\
&\le 2^{2|q|/3} \cdot \frac{2^\lambda}{q} \\
&\le \frac{2^{\lambda+1}}{2^{|q|/3}} \quad (\text{since } \log_2 q \ge |q| - 1).
\end{aligned}$$

This means that C' is rejected with overwhelming probability. An almost identical argument holds for all the subsequent invalid decryption queries.

Game$_4$: In the guess stage, if $\mathcal{A}$ queries an invalid ciphertext with $(u_1, u_2, s) \neq (u_1^*, u_2^*, s^*)$ but $\alpha = \alpha^*$, then the decryption oracle returns $\perp$.

We can show that $|\Pr[X_3] - \Pr[X_4]|$ is negligible in the same way as in [3, 7] because TCR is a target collision resistant function.

Game$_5$: In the guess stage, if $\mathcal{A}$ queries an invalid ciphertext with $(u_1, u_2, s) \neq (u_1^*, u_2^*, s^*)$ and $\alpha \neq \alpha^*$, then the decryption oracle returns $\perp$.

We show that $|\Pr[X_4] - \Pr[X_5]|$ is negligible by proving such ciphertext is also rejected with overwhelming probability in **Game$_4$**. The situation is similar to **Game$_3$**. The difference is that $\mathcal{A}$ may know v^* as well as c and d.

Suppose that $\mathcal{A}$ queries such an invalid ciphertext $C = (u_1, u_2, e, t, s)$ with $u_1 = g_1^{r_1}$ and $u_2 = g_2^{r_2}$. Let $v = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2}$. Then

$$\begin{bmatrix} \log_{g_1} c \\ \log_{g_1} d \\ \log_{g_1} v^* \\ \log_{g_1} v \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 0 & \omega \\ r_1^* & r_1^*\alpha^* & r_2^*\omega & r_2^*\omega\alpha^* \\ r_1 & r_1\alpha & r_2\omega & r_2\omega\alpha \end{bmatrix}}_{M} \begin{bmatrix} x_1 \\ y_1 \\ x_2 \\ y_2 \end{bmatrix},$$

in which $\det(M) = \omega^2(r_2^* - r_1^*)(r_2 - r_1)(\alpha - \alpha^*) \neq 0$. Hence by using the same argument as given in **Game$_3$**, we can see that C is rejected with overwhelming probability.

Game$_6$: In the guess stage, if $\mathcal{A}$ queries an invalid ciphertext $C \neq C^*$ such that $(u_1, u_2, s) = (u_1^*, u_2^*, s^*)$, then the decryption oracle returns $\perp$.

We show that $|\Pr[X_5] - \Pr[X_6]|$ is negligible, by proving that in **Game**$_5$, any such ciphertext is also rejected with overwhelming probability. Let $C' = (u_1, u_2, e, t, s)$ be the first such ciphertext queried by $\mathcal{A}$. Since $(u_1, u_2, s) = (u_1^*, u_2^*, s^*)$, we have $v = v^*$. Hence $(k_1, k_2) = (k_1^*, k_2^*)$. If C' is accepted, then

$$t^* = k_1^* H(e^*) + k_2^* \quad \text{and} \quad t = k_1^* H(e) + k_2^*.$$

If $e = e^*$, then $t = t^*$ which means that $C' = C^*$. Therefore it must be that $e \neq e^*$. In this case, $H(e) \neq H(e^*)$ since H is collision resistant. Then there exists a unique solution (k_1^*, k_2^*) which satisfies the above linear equations. Let (a_1, a_2) denote this solution.

On the other hand, in **Game**$_5$, $\mathcal{A}$ does not learn any more information on (x_1, x_2, y_1, y_2) from the invalid ciphertexts such that $(u_1, u_2, s) \neq (u_1^*, u_2^*, s^*)$ because they are all rejected. Hence it is enough to consider

$$\begin{bmatrix} \log_{g_1} c \\ \log_{g_1} d \\ \log_{g_1} v^* \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 0 & \omega \\ r_1^* & r_1^*\alpha^* & r_2^*\omega & r_2^*\omega\alpha^* \end{bmatrix}}_{V} \begin{bmatrix} x_1 \\ y_1 \\ x_2 \\ y_2 \end{bmatrix}.$$

Since the matrix V has rank 3, v^* is random from $\mathcal{A}$'s point of view if we ignore the leakage functions f and C^*. Note that $k_0^* \| k_1^* \| k_2^* = \mathsf{KDF}(v^*)$ and e^* is independent of (k_1^*, k_2^*). Hence given $f(sk)$, and $t^* \in \{0,1\}^{|q|/3}$ and (c, d), the entropy of (k_1^*, k_2^*) is at least

$$\frac{2}{3}|q| - 1 - \lambda - |t^*| \geq \frac{|q|}{3} - \lambda - 1.$$

Therefore,

$$\Pr[C' \text{ is accepted}] = \Pr[K_1^* = a_1, K_2^* = a_2] \leq \frac{2^{\lambda+1}}{2^{|q|/3}}.$$

This means that C' is rejected with overwhelming probability. All the subsequent such ciphertexts are rejected similarly.

Game$_7$**:** Replace $\mathsf{PRG}(\mathsf{Ext}(K_0^*, s^*))$ with a random string in the challenge ciphertext C^*. We show that $|\Pr[X_6] - \Pr[X_7]|$ is negligible.

In **Game**$_6$, all invalid ciphertexts are rejected by the decryption oracle. In addition, by submitting valid ciphertexts, $\mathcal{A}$ only learns a linear combination of $\log_{g_1} c = x_1 + \omega x_2$ and $\log_{g_1} d = y_1 + \omega y_2$ which $\mathcal{A}$ already knew from the public key. Hence as shown in **Game**$_6$, v^* is random from $\mathcal{A}$'s point of view if we ignore the leakage functions f and C^*. Further $k_0^* \| k_1^* \| k_2^* = \mathsf{KDF}(v^*)$ and k_0^* is independent of t^*. Hence given $f(sk), t^*$ and (c, d), the entropy of K_0^* is at least

$$\frac{|q|}{3} - \lambda - 1.$$

Hence $\mathsf{Ext}(K_0^*, s^*)$ is statistically indistinguishable from a random string. Thus, $\mathsf{PRG}(\mathsf{Ext}(K_0^*, s^*))$ is computationally indistinguishable from a random string.

Now in **Game**$_7$, $e^* = R \oplus m_b$, where R is a random string. Therefore $\mathcal{A}$ learns no information on m_b from e^*. Hence

$$\Pr[X_7] = \Pr[b' = b \text{ in } \mathbf{Game}_7] = \frac{1}{2}.$$

This means that $|\Pr[b' = b] - 1/2|$ is negligible in the original attack game. □

4 Generalization to universal hash proof system

In this section, we generalize our leakage-resilient scheme of Section 3 to universal hash proof systems (HPS).

4.1 HPS with auxiliary input

The notion of hash proof systems was introduced by Cramer and Shoup to construct an IND-CCA secure hybrid encryption scheme [2]. In key encapsulation mechanism (KEM), let $\mathcal{SK}$, $\mathcal{PK}$, and $\mathcal{K}$ be sets of secret keys, public keys, and encapsulated symmetric keys. $\mathcal{E}$ is the set of all ciphertexts of KEM, and $\mathcal{V} \subset \mathcal{E}$ is the set of all “valid" ones. In addition, $\mathcal{S}$ is a set of seeds. In Kurosawa–Desmedt scheme, $\mathcal{SK} = \mathbb{G}^4$, $\mathcal{PK} = \mathbb{G}^2$, $\mathcal{E} = \mathbb{G}^2$, $\mathcal{K} = \mathbb{G}$, $\mathcal{V} = \{(g_1^r, g_2^r) : r \in \mathbb{Z}_q\}$, and $\mathcal{S} = \mathsf{Seed}$.

The subset membership assumption says that $\mathcal{V}$ is indistinguishable from $\mathcal{E}$. If $\mathcal{V} = \{(g_1^r, g_2^r) : r \in \mathbb{Z}_q\}$ and $\mathcal{E} = \mathbb{G}^2$ as above, this is exactly the DDH assumption.

A function $\Lambda_{sk} : \mathcal{E} \times \mathcal{S} \to \mathcal{K}$ is *projective* if there exists a projection $\mu : \mathcal{SK} \to \mathcal{PK}$ such that $pk = \mu(sk)$ defines $\Lambda_{sk} : \mathcal{V} \times \mathcal{S} \to \mathcal{K}$. Namely, for every $E \in \mathcal{V}$, the value $K = \Lambda_{sk}(E, s)$ is uniquely determined by $pk = \mu(sk)$ and (E, s), where $s \in \mathcal{S}$.

A projective function Λ_{sk} is called computationally universal$_2$ if for all $E, E^* \notin \mathcal{V}$ with $(E, s) \neq (E^*, s^*)$,

$$\big(pk, \Lambda_{sk}(E^*, s^*), \Lambda_{sk}(E, s)\big) \quad \text{and} \quad \big(pk, \Lambda_{sk}(E^*, s^*), K\big)$$

are computationally indistinguishable, where sk and K are random. It is worth noting that Λ_{sk} has an *additional input* s, compared to previous works. While the original HPS in [2] requires $E \neq E^*$, our property here allows $E = E^*$ if $s \neq s^*$.

In our scheme of Section 3,

$$\Lambda_{sk}\big(E = (u_1, u_2), s\big) = u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2},$$

where $\alpha = \mathsf{TCR}(E, s)$. To prove that $\Lambda_{sk}(E, s)$ is random conditioned on pk and $\Lambda_{sk}(E^*, s^*)$, since

$$\begin{bmatrix} \log_{g_1} c \\ \log_{g_1} d \\ \log_{g_1} \Lambda_{sk}(E^*, s^*) \\ \log_{g_1} \Lambda_{sk}(E, s) \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & \omega & 0 \\ 0 & 1 & 0 & \omega \\ r_1^* & r_1^*\alpha^* & r_2^*\omega & r_2^*\omega\alpha^* \\ r_1 & r_1\alpha & r_2\omega & r_2\omega\alpha \end{bmatrix}}_{M} \begin{bmatrix} x_1 \\ y_1 \\ x_2 \\ y_2 \end{bmatrix},$$

it suffices to show that $\det(M) \neq 0$. Again, this holds true because $\det(M) = \omega^2(r_2^* - r_1^*)(r_2 - r_1)(\alpha - \alpha^*)$, and $r_2^* \neq r_1^*$, $r_2 \neq r_1$ (since $E, E^* \notin \mathcal{V}$), and $\alpha = \mathsf{TCR}(E, s) \neq \alpha^* = \mathsf{TCR}(E^*, s^*)$ since $(E, s) \neq (E^*, s^*)$.

Hash proof system. A hash proof system $\mathcal{HPS}$ consists of three algorithms $(\mathsf{Param}, \mathsf{Pub}, \mathsf{Priv})$. Param generates

$$(\text{group}, \mathcal{SK}, \mathcal{PK}, \mathcal{K}, \mathcal{E}, \mathcal{V}, \Lambda_{(\cdot)}(\cdot), \mu : \mathcal{SK} \to \mathcal{PK}, \mathcal{S}).$$

$\mathsf{Pub}(pk, E, s, r)$ returns $\Lambda_{sk}(E, s)$ for $E \in \mathcal{V}$, where $s \in \mathcal{S}$ and r is a witness of the fact that $E \in \mathcal{V}$. $\mathsf{Priv}(sk, E, s)$ returns $\Lambda_{sk}(E, s)$ (without knowing a witness).

4.2 Leakage resilient CCA-secure PKE from HPS

Let $q = |\mathcal{K}|$ (prime, except in Section 4.4). We assume that there exists an injection $\mathsf{KDF} : \mathcal{K} \to \{0, 1\}^{|q|}$. Let $\mathsf{Ext} : \{0, 1\}^{|q|/3} \times \mathsf{Seed} \to \{0, 1\}^{\ell}$ be a $(|q|/3 - \lambda, \epsilon_{\mathsf{Ext}})$-randomness extractor, and $\mathsf{PRG} : \{0, 1\}^{\ell} \to \{0, 1\}^*$ be a pseudo-random generator. Also needed is a collision resistant hash function $H : \{0, 1\}^* \to \{0, 1\}^{|q|/3}$.

Key generation: Run Param to define

$$(\text{group}, \mathcal{SK}, \mathcal{PK}, \mathcal{K}, \mathcal{E}, \mathcal{V}, \Lambda_{(\cdot)}(\cdot), \mu : \mathcal{SK} \to \mathcal{PK}, \mathcal{S}).$$

Let a public key be $pk = \mu(sk)$ for a random secret $sk \in \mathcal{SK}$. Below $|k_0| = |k_1| = |k_2| = \frac{\log_2 |\mathcal{K}|}{3}$.

Encryption of $m \in \{0,1\}^*$:

$$\begin{aligned}
&E(\text{witness } r) \xleftarrow{\$} \mathcal{V},\ s \xleftarrow{\$} \mathsf{Seed},\ v \leftarrow \mathsf{Pub}(pk, E, s, r)\\
&k_0\|k_1\|k_2 \leftarrow \mathsf{KDF}(v), \text{where } |k_0| = |k_1| = |k_2| = |q|/3\\
&e \leftarrow \mathsf{PRG}(\mathsf{Ext}(k_0; s)) \oplus m,\ t \leftarrow k_1 H(e) + k_2 \text{ (over GF}(2^{|q|/3}))\\
&\text{Output } (E, e, t, s)
\end{aligned}$$

Decryption of (E, e, t, s):

$$v \leftarrow \mathsf{Priv}(sk, E, s),\ k_0\|k_1\|k_2 \leftarrow \mathsf{KDF}(v)$$

If $t = k_1 H(e) + k_2$, then output $\mathsf{PRG}(\mathsf{Ext}(k_0; s)) \oplus e$. Else output $\perp$.

Theorem 4.1. *The above generic construction is IND-lrCCA-secure.*

The proof idea is almost the same as that of Theorem 3.1. More details are given below.

Proof. We proceed in games as follows.

Game$_0$: This game is the IND-CCA attack game with leakage. Without loss of generality, assume that E^*, s^*, r^* are generated at the beginning of the game. Let $k_0^*\|k_1^*\|k_2^* = \mathsf{Priv}(sk, E^*, s^*)$. When the adversary submits (m_0, m_1), the simulator computes

$$e^* = \mathsf{PRG}(\mathsf{Ext}(k_0^*; s^*)) \oplus m_b, \quad t^* = k_1^* \cdot H(e^*) \oplus k_2^*.$$

Also, decryption queries are handled as in Table 2.

Game$_1$: Compute $\mathsf{Pub}(pk, E^*, s^*, r^*)$ as $\mathsf{Priv}(sk, E^*, s^*)$. We have $\Pr[X_0] = \Pr[X_1]$.

Game$_2$: Take $E^* \xleftarrow{\$} \mathcal{C} \setminus \mathcal{V}$. We have $|\Pr[X_1] - \Pr[X_2]| \le \epsilon_{\text{sm}}$ thanks to the subset membership problem.

Game$_3$: Any decryption query (e, E, t, s) with $(s, E) \neq (s^*, E^*)$ and $E \notin \mathcal{V}$ is answered by $\perp$. We have $|\Pr[X_2] - \Pr[X_3]| \le \epsilon_{\text{hash}}$ thanks to the ϵ_{hash}-computationally universal$_2$ property. Namely, $\Lambda_{sk}(E, s) = \mathsf{Pub}(pk, E, s, r) = k_0\|k_1\|k_2$ is random-like conditioned on pk and $\Lambda_{sk}(E^*, s^*)$. Conditioned further on the leakage amount λ, the entropy of $k_1\|k_2$ is still high, so that the check $k_2 = t \oplus k_1 e$ goes through with negligible probability (which is computed like in the proof of Theorem 3.1.)

In **Game**$_{0,1,2}$

```
if $(E, s) = (E^*, s^*)$ then
    if $t \neq k_1^* e \oplus k_2^*$ then
        return $\perp$
    else
        return $\mathsf{Ext}(k_0^*; s^*) \oplus e$
    end if
else if $E \notin \mathcal{V}$ then
    $k_0 \| k_1 \| k_2 \leftarrow \Lambda_{sk}(E, s)$
    if $t \neq k_1 e \oplus k_2$ then return $\perp$
    else return $\mathsf{Ext}(k_0; s) \oplus e$
else
    $k_0 \| k_1 \| k_2 \leftarrow \Lambda_{sk}(E, s)$
    if $t \neq k_1 e \oplus k_2$ then return $\perp$
    return $\mathsf{Ext}(k_0; s) \oplus e$
end if
```

In **Game**$_{3,4}$

```
if $(E, s) = (E^*, s^*)$ then
    if $t \neq k_1^* e \oplus k_2^*$ then
        return $\perp$
    else
        return $\mathsf{Ext}(k_0^*; s^*) \oplus e$
    end if
else if $E \notin \mathcal{V}$ then
    return $\perp$
else
    $k_0 \| k_1 \| k_2 \leftarrow \Lambda_{sk}(E, s)$
    if $t \neq k_1 e \oplus k_2$ then return $\perp$
    return $\mathsf{Ext}(k_0; s) \oplus e$
end if
```

Table 2. Decryption of query (e, E, t, s).

Game$_4$**:** Replace $\mathsf{Ext}(k_0^*; s^*)$ in the challenge ciphertext by a random string, so that $e^* = \mathsf{Ext}(k_0^*; s^*) \oplus m_b$ completely hides the challenge bit b. We have $|\Pr[X_3] - \Pr[X_4]| \leq \epsilon_{\text{hash}}$ and $\Pr[X_4] = 1/2$.

The reason is that, thanks to the ϵ_{hash}-computationally universal$_2$ property,

$$\Lambda_{sk}(E^*, s^*) = k_0^* \| k_1^* \| k_2^*$$

still has high entropy, given $\Lambda_{sk}(E, s), pk$ and leakage amount λ. To obtain any further information on K_0^*, the adversary must submit for decryption queries of the form (s^*, E^*, e, t) with $(e, t) \neq (e^*, t^*)$. However, since $k_1^* \| k_2^*$ has high entropy, those decryption queries will be rejected. □

4.3 Instantiation under the d-linear assumption

We use the HPS based on the decisional d-linear assumption (DLIN) given by [6, Section 5.2] for $d = 2$. In this HPS, $\mathcal{SK} = \mathbb{Z}_q^6$, $\mathcal{PK} = \mathbb{G}^4$, $\mathcal{K} = \mathbb{G}$, $\mathcal{S} = \mathsf{Seed}$. Also $\mathcal{E} = \mathbb{G}^3$ and $\mathcal{V} = \{(g_1^{r_1}, g_2^{r_2}, h^{r_1+r_2}) : r_1, r_2 \in \mathbb{Z}_q\}$, where $g_1, g_2, h \in \mathbb{G}$. The DLIN assumption says that $\mathcal{E}$ and $\mathcal{V}$ are indistinguishable.

Key generation: Let a secret key be $sk = (x_1, x_2, y_1, y_2, z, z') \xleftarrow{\$} \mathbb{Z}_q^6$. Compute $c_1 = g_1^{x_1} h^z$, $c_2 = g_2^{x_2} h^z$, $d_1 = g_1^{y_1} h^{z'}$, $d_2 = g_2^{y_2} h^{z'}$, where $g_1, g_2, h \xleftarrow{\$} \mathbb{G}$. The public key is $pk = (g_1, g_2, h, c_1, c_2, d_1, d_2)$.

Encryption of $m \in \{0, 1\}^*$:

$$r_1, r_2 \xleftarrow{\$} \mathbb{Z}_q,\ u_1 \leftarrow g_1^{r_1},\ u_2 \leftarrow g_2^{r_2},\ u_3 \leftarrow h^{r_1+r_2}$$

$$s \xleftarrow{\$} \mathsf{Seed},\ \alpha \leftarrow \mathsf{TCR}(u_1, u_2, u_3, s) \in \mathbb{Z}_q,\ v \leftarrow (c_1^\alpha d_1)^{r_1} (c_2^\alpha d_2)^{r_2}$$

$$k_0 \| k_1 \| k_2 \leftarrow \mathsf{KDF}(v), \text{where } |k_0| = |k_1| = |k_2| = |q|/3$$

$$e \leftarrow \mathsf{PRG}(\mathsf{Ext}(k_0; s)) \oplus m,\ t \leftarrow k_1 H(e) + k_2 \text{ (over } \mathrm{GF}(2^{|q|/3}))$$

$$\text{Output } (u_1, u_2, u_3, e, t, s)$$

Decryption of (u_1, u_2, u_3, e, t, s):

$$\alpha \leftarrow \mathsf{TCR}(u_1, u_2, u_3, s),\ v \leftarrow u_1^{x_1+\alpha y_1} u_2^{x_2+\alpha y_2} u_3^{z+\alpha z'}$$

$$k_0 \| k_1 \| k_2 \leftarrow \mathsf{KDF}(v).$$

If $t = k_1 H(e) + k_2$, then output $m = \mathsf{PRG}(\mathsf{Ext}(k_0; s)) \oplus e$. Else output $\perp$.

Let λ be the leakage amount on sk. We need $2^{\lambda - |q|/3}$ to be negligible. For η-bit security, let $2^{\lambda-|q|/3} = 2^{-\eta}$, so $\lambda = \frac{|q|}{3} - \eta$. This means the leakage rate

$$\frac{\lambda}{|sk|} = \frac{(1/3)|q| - \eta}{6|q|}$$

approaches $1/18$ when the group order q becomes large.

Theorem 4.2. *The above encryption scheme is IND-lrCCA-secure with leakage rate* $1/18$ *under the DLIN assumption.*

4.4 Instantiation under the DCR assumption

We use the HPS based on the decisional composite residuosity assumption (DCR) given by [2]. Let $p_1 = 2p_2 + 1$ and $q_1 = 2q_2 + 1$ be primes, where p_2 and q_2 are also primes. Let $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$. Let $\mathbb{G}$ be the subgroup of $Z_{N_1^2}^*$ with order $N_1 N_2$. Note that $\mathbb{G}$ is written as $\mathbb{G} = \mathbb{G}_{N_1} \cdot \mathbb{G}_{N_2}$ where $\mathbb{G}_n$ denotes a cyclic group of order n. Let g be a generator of $\mathbb{G}$, so that $g_1 = g^{N_2}$ is a generator of $\mathbb{G}_{N_1}$ and $g_2 = g^{N_1}$ is a generator of $\mathbb{G}_{N_2}$.

In this HPS, $\mathcal{SK} = \{0, \ldots, \lfloor N_1^2/2 \rfloor\}^2$, $\mathcal{PK} = \mathbb{G}_{N_2}^2$, $\mathcal{K} = \mathbb{Z}_{N_1}$, and $\mathcal{S} = \mathsf{Seed}$. Also $\mathcal{E} = \mathbb{G}$ and $\mathcal{V} = \{g_2^r \bmod N_1^2 : r \in \{0, \ldots, N_1/4\}\}$. The DCR assumption says that $\mathcal{E}$ and $\mathcal{V}$ are indistinguishable.

Let $\mathsf{Ext} : \{0,1\}^{|N_1|/3} \times \mathsf{Seed} \to \{0,1\}^{\ell}$ be a $(|N_1|/3 - \lambda, \epsilon_{\mathsf{Ext}})$-randomness extractor, and $\mathsf{PRG} : \{0,1\}^{\ell} \to \{0,1\}^{*}$ be a pseudo-random generator. Also needed are a collision resistant hash function $H : \{0,1\}^{*} \to \{0,1\}^{|N_1|/3}$, and a target collision resistant $\mathsf{TCR} : \{0,1\}^{*} \to \mathbb{Z}_{\lfloor N_1^2/2 \rfloor}$. Below $\mathsf{KDF} : \mathbb{Z}_{N_1} \to \mathbb{Z}_{N_1}$ is the identity function.

Key generation: Let a secret key be $sk = (x, y) \xleftarrow{\$} \mathcal{SK}$. Compute $c = g_2^x \bmod N_1^2$ and $d = g_2^y \bmod N_1^2$. The public key is $pk = (N_1, g_2, c, d)$.

Encryption of $m \in \{0,1\}^*$:

$$\begin{aligned}
&r \xleftarrow{\$} \{0,\dots,N_1/4\},\ u \leftarrow g_2^r \bmod N_1^2,\ s \xleftarrow{\$} \mathsf{Seed},\ \alpha \leftarrow \mathsf{TCR}(u,s)\\
&v \leftarrow (c^{\alpha} d)^r \bmod N_1\\
&k_0 \| k_1 \| k_2 \leftarrow \mathsf{KDF}(v), \text{where } |k_0| = |k_1| = |k_2| = |N_1|/3\\
&e \leftarrow \mathsf{PRG}(\mathsf{Ext}(k_0; s)) \oplus m,\ t \leftarrow k_1 H(e) + k_2 \ (\text{over } \mathrm{GF}(2^{|N_1|/3}))\\
&\text{Output } (u, e, t, s)
\end{aligned}$$

Decryption of (u, e, t, s):

$$\alpha \leftarrow \mathsf{TCR}(u,s),\ v \leftarrow u^{x\alpha+y} \bmod N_1,\ k_0 \| k_1 \| k_2 \leftarrow \mathsf{KDF}(v)$$

If $t = k_1 H(e) \oplus k_2$, then output $\mathsf{PRG}(\mathsf{Ext}(k_0; s)) \oplus e$. Else output $\perp$.

Again, set $\lambda = (1/3)\log_2 N_1 - \eta$. Note that $|sk| \approx 4 \log_2 N_1$ so the leakage rate $\lambda/|sk|$ approaches $1/12$.

Theorem 4.3. *The above encryption scheme is IND-lrCCA-secure with leakage rate* $1/12$ *under the DCR assumption.*

Bibliography

[1] A. Akavia, S. Goldwasser and V. Vaikuntanathan, Simultaneous hardcore bits and cryptography against memory attacks, in: *TCC*, Lecture Notes in Comput. Sci. 5444, Springer (2009), 474–495.

[2] R. Cramer and V. Shoup, Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption, in: *EUROCRYPT*, Lecture Notes in Comput. Sci. 2332, Springer (2002), 45–64.

[3] Y. Desmedt, R. Gennaro, K. Kurosawa and V. Shoup, A new and improved paradigm for hybrid encryption secure against chosen-ciphertext attack, *J. Cryptology* **23** (2010), 91–120.

[4] Y. Dodis, K. Haralambiev, A. López-Alt and D. Wichs, Efficient public-key cryptography in the presence of key leakage, in: *ASIACRYPT*, Lecture Notes in Comput. Sci. 6477, Springer (2010), 613–631.

[5] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, *SIAM J. Comput.* **38** (2008), 97–139.

[6] D. Hofheinz and E. Kiltz, Secure hybrid encryption from weakened key encapsulation, preprint (2007), `http://eprint.iacr.org/2007/288`.

[7] K. Kurosawa and Y. Desmedt, A new paradigm of hybrid encryption scheme, in: *CRYPTO*, Lecture Notes in Comput. Sci. 3152, Springer (2004), 426–442.

[8] M. Naor and G. Segev, Public-key cryptosystems resilient to key leakage, in: *CRYPTO*, Lecture Notes in Comput. Sci. 5677, Springer (2009), 18–35.

Received January 16, 2013; accepted August 4, 2013.

Author information

Kaoru Kurosawa, Department of Computer and
Information Sciences, Ibaraki University, Japan.
E-mail: `kurosawa@mx.ibaraki.ac.jp`

Ryo Nojima, National Institute of Information and
Communications Technology (NICT), Japan.
E-mail: `ryo-no@nict.go.jp`

Le Trieu Phong, National Institute of Information and
Communications Technology (NICT), Japan.
E-mail: `phong@nict.go.jp`