Towards Tightly Secure Deterministic Public Key Encryption

Daode Zhang[1,2,3], Bao Li[1,2,3], Yamin Liu[1], Haiyang Xue[1(✉)], Xianhui Lu[1], and Dingding Jia[1]

[1] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
{zhangdaode,lb}@is.ac.cn,
{liuyamin,xuehaiyang,luxianhui,jiadingding}@iie.ac.cn
[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[3] Science and Technology on Communication Security Laboratory, Chengdu, China

Abstract. In this paper, we formally consider the construction of tightly secure deterministic public key encryption (D-PKE). Initially, we compare the security loss amongst the D-PKE schemes under the concrete assumptions and also analyze the tightness of generic D-PKE constructions. Furthermore, we prove that the CPA secure D-PKE scheme of Boldyreva et al. (Crypto'08) is tightly PRIV-IND-CPA secure for block-sources. Our security reduction improves the security loss of their scheme from $\mathcal{O}(n_{c^*})$ to $\mathcal{O}(1)$. Additionally, by upgrading the all-but-one trapdoor function (TDF) in the construction of Boldyreva et al. to all-but-n TDF defined by Hemenway et al. (Asiacrypt'11), we give general construction of PRIV-IND-$\frac{n}{2}$-CCA secure (i.e., the number of challenge ciphertexts n_{c^*} is bounded by $\frac{n}{2}$) D-PKE scheme for block-sources. And we observe that if the security reduction of the all-but-n TDF is tight, the D-PKE scheme can be tightly PRIV-IND-$\frac{n}{2}$-CCA secure. Finally, we prove that the all-but-n TDF given by Hemenway et al. is tightly secure, which results in the first tightly PRIV-IND-$\frac{n}{2}$-CCA secure D-PKE scheme for block-sources, based on the s-DCR assumption.

Keywords: Deterministic public key encryption
Tight security reduction · Lossy trapdoor functions · Standard model

1 Introduction

Currently, the formal way to prove the security of cryptographic primitives is providing a security reduction, i.e., any adversary A breaking the security of a scheme with advantage ε_A implies an adversary B that can solve the underlying hard problem with advantage ε_B. Specially, we call the quotient $L = \varepsilon_A/\varepsilon_B$ the security loss of a reduction. Naturally, we hope that the quotient L is small.

S. Qing et al. (Eds.): ICICS 2017, LNCS 10631, pp. 154–161, 2018.
https://doi.org/10.1007/978-3-319-89500-0_13

Tight Security Reduction. Standard security notions for public key encryption (PKE) schemes, e.g., IND-CCA security [6], only consider one user and one ciphertext. However, in the reality setting, the adversary can know at most n_u public keys of users and obtain at most n_{c^*} challenge ciphertexts from per user. These two parameters can be very large, e.g., $n_u = n_{c^*} = 2^{40}$. In general, L will depend on n_u and n_{c^*} [1]. In order to compensate for the security loss, we have to increase the strength of the underlying intractability assumption which worsens the parameters of the encryption scheme and affects the performance of the implementation. For example, for encryption schemes from the Decisional Diffie-Hellman assumption over cyclic groups, we have to increase the size of the underlying groups, which in turn increases the running time of the implementation, as exponentiation in an l-bit group takes time about $\mathcal{O}(l^3)$ as stated in [7]. Hence, it is important to study tight security reductions where the security loss L is a small constant that in particular does not depend on parameters under the adversary's control, such as n_u, n_{c^*}. In the case of CCA security, L should also be independent of the parameter n_c, which is the number of queries that the adversary can make to each decryption oracle at most.

Tight Security in Deterministic-PKE. Deterministic-PKE (D-PKE), namely, deterministic public-key encryption, was introduced by Bellare et al. [2], in which the encryption algorithm is deterministic.

Bellare et al. [2] defined a strongest possible security notion for D-PKE, called PRIV, over plaintext distributions with high min-entropy independent of the public key. The definition of PRIV considers a message block containing multi-plaintext. If the size of block is one, then the security definition is called PRIV1. The security notions of D-PKE evolved in a series of literatures [3–5,11]. Many D-PKE constructions have been proposed based on concrete assumptions as depicted in Fig. 1. These D-PKE constructions are all secure in the one-user, multi-ciphertext case. However, all of these constructions have a security loss about $\mathcal{O}(n_{c^*})$.

Our Contributions. It seems that the tight security reduction of D-PKE has not been deliberately studied in literatures. We compare the security loss amongst the D-PKE schemes based on the concrete assumptions in Fig. 1. In this paper, we formally consider the construction of tightly secure D-PKE scheme which is either PRIV-IND-CPA or PRIV-IND-CCA secure for block-sources in the standard model.

We start from [4] which introduced two D-PKE schemes based on lossy TDFs and all-but-one TDFs [10]. One is PRIV1-IND-CPA secure and the other is PRIV1-IND-CCA secure, for block-sources. Initially, we prove that their PRIV1-IND-CPA secure D-PKE scheme is tightly PRIV-IND-CPA secure for block-sources. Our security reduction improves the security loss of this scheme from $\mathcal{O}(n_{c^*})$ to $\mathcal{O}(1)$. So we can obtain tightly PRIV-IND-CPA secure D-PKE schemes for block-sources by instantiating D-PKE constructions based on the DDH, s-DCR, LWE assumption.

	CPA-schemes($n_u = 1, n_{c^*}$)	
Reference	security loss	assumption
BBO07 [2]	$\geq \mathcal{O}(n_{c^*})$	RSA+RO Model
BFO08 [4]	$\mathcal{O}(n_{c^*})$	DDH/s-DCR/LWE
BS11 [5]	$\mathcal{O}(n_{c^*})$	DLin
Wee12 [12]	$\mathcal{O}(n_{c^*})$	DDH/DLin/QR/s-DCR/LWE
XXZ12 [13]	$\mathcal{O}(n_{c^*})$	LWE
MPRS12 [9]	$\mathcal{O}(n_{c^*})$	DDH
Our Results of BFO08 [4]	$\mathcal{O}(1)$	DDH/s-DCR/LWE
	CCA-schemes ($n_u = 1, n_{c^*}, n_c$)	
BFO08 [4]	$\mathcal{O}(n_{c^*})$	DDH/s-DCR
Ours	bounded-$\mathcal{O}(1)$	s-DCR

Fig. 1. The security loss amongst the D-PKE schemes under the concrete assumptions.

However, their PRIV1-IND-CCA D-PKE scheme in [4] (The sect. 7.2) is not tightly PRIV-IND-CCA secure for block-sources. In their PRIV1-IND-CCA D-PKE scheme, the ciphertext of a message m contains an item as follows

$$\mathcal{F}_{abo}(ek_{abo}, \mathcal{H}_{cr}(k_{cr}, \mathcal{H}_{inv}(k_{inv}, m)), \mathcal{H}_{inv}(k_{inv}, m)),$$

where $\mathcal{F}_{abo}$ is a collection of all-but-one TDFs, $\mathcal{H}_{cr}$ is a family of collision-resistant hash functions, $\mathcal{H}_{inv}$ is a collection of pairwise-independent permutations with invertibility. Let function f be

$$f = \mathcal{F}_{abo}(ek_{abo}, \mathcal{H}_{cr}(k_{cr}, \cdot), \cdot) \quad \text{and} \quad ek_{abo} \xleftarrow{R} \mathcal{K}_{abo}(\mathcal{H}_{cr}(k_{cr}, \cdot)),$$

where $\mathcal{K}_{abo}$ is the key generation algorithm of $\mathcal{F}_{abo}$. According to the generalized "Crooked" leftover hash lemma, the statistical distance between $f(\mathcal{H}_{inv}(k_{inv}, m))$ and $f(h)$ is negligible, where $h \xleftarrow{\$} U_{inv}$ and U_{inv} denotes the uniform distribution on the range of $\mathcal{H}_{inv}$. So that $f(h)$ includes no information of the message m. In order to use the generalized "Crooked" leftover hash lemma, $\mathcal{H}_{cr}(k_{cr}, \mathcal{H}_{inv}(k_{inv}, m))$ and $\mathcal{H}_{cr}(k_{cr}, h)$ must belong to the lossy branch of the respective all-but-one TDF $\mathcal{F}_{abo}$. As a result, the security loss of their scheme is 2 times of the security loss of the all-but-one TDF $\mathcal{F}_{abo}$. However, the tight security reduction considers $n_{c^*} > 1$ challenge ciphertexts in the PRIV-IND-CCA security game for block-sources. Though PRIV1-IND-CCA and PRIV-IND-CCA are proved to be equivalent in [4], there is a security loss of $2 \cdot n_{c^*}$ due to the employment of the hybrid technique.

Furthermore, to address this problem, we upgrade the all-but-one TDF in the constructions of [4] to all-but-n TDF [8] whose number of the lossy branches is n. When the number of the lossy branches is two times of the number of the challenge ciphertexts, i.e., $n = 2 \cdot n_{c^*}$ (because we additionally need $\mathcal{H}_{cr}(k_{cr}, h)$ to be in the lossy branches of the all-but-n TDF), every challenge ciphertext can be evaluated on the lossy branches in the PRIV-IND-CCA security game for block-sources. In addition, apparently that if the security loss of the all-but-n

TDF is independent of n (tightly secure), then the security loss of the D-PKE scheme can also be independent of n_{c^*}, i.e., the D-PKE scheme can be tightly PRIV-IND-CCA secure for block-sources. However, because the number of the lossy branches of the all-but-n TDF in the construction is bounded by n, so that the number of the challenge ciphertexts n_{c^*} is bounded by $\frac{n}{2}$. As a result, our D-PKE schemes are only able to be tightly PRIV-IND-$\frac{n}{2}$-CCA secure for block-sources, where PRIV-IND-$\frac{n}{2}$-CCA security for block-sources is very similar to PRIV-IND-CCA security for block-sources except with the restriction the number of the challenge ciphertexts is bounded by $\frac{n}{2}$.

As aforementioned, the most important part of our constructions is to find tightly secure all-but-n TDFs. Finally, we prove that the all-but-n TDF given by Hemenway et al. [8] is tightly secure with a security loss of only 2. This improves their original security reduction which has a security loss of $2n$ due to the use of the hybrid technique. Applying this result to our constructions, we obtain the first D-PKE scheme which is tightly PRIV-IND-$\frac{n}{2}$-CCA secure for block-sources based on the s-DCR assumption.

2 Preliminaries

Notations. For a random variable X, we write $x \xleftarrow{R} X$ to denote sampling x according to X's distribution. For a random variable X, its min-entropy is defined as $\mathrm{H}_\infty(X) = -\log(\max_x P_X(x))$. Given Y, the worst-case conditional min-entropy of X is $\mathrm{H}_\infty(X|Y) = -\log(\max_{x,y} P_{X|Y=y}(x))$ and the average-case conditional min-entropy of X is $\widetilde{\mathrm{H}}_\infty(X|Y) = -\log(\sum_y P_Y(y) \cdot \max_x P_{X|Y=y}(x))$. A random variable $X \in \{0,1\}^l$ is called a (t,l)-source if it satisfies that $\mathrm{H}_\infty(X) \geq t$. And a vector $\overrightarrow{X}$ is called a (t,l)-block-source of length n if it is a list of random variables $(X_1, \cdots, X_n)$ over $\{0,1\}^l$ and satisfies that $\mathrm{H}_\infty(X_i|X_1, \cdots, X_{i-1}) \geq t$ for all $i \in [n] = \{1, \cdots, n\}$. The statistical distance between two distributions X, Y over a finite or countable domain D is $\triangle(X,Y) = \frac{1}{2}\sum_{w \in D} |P_X(w) - P_Y(w)|$. A hash function $\mathbf{H} = (\mathcal{K}, \mathcal{H})$ with range $\mathbb{R}$ is pairwise-independent if for all $x_1 \neq x_2 \in \{0,1\}^l$ and all $y_1, y_2 \in \mathbb{R}$, $\Pr[\mathcal{H}(K, x_1) = y_1 \wedge \mathcal{H}(K, x_2) = y_2 : K \xleftarrow{R} \mathcal{K}] \leq \frac{1}{|\mathbb{R}|^2}$. A hash function $\mathbf{H}(\mathcal{K}, \mathcal{H})$ is collision resistant if for all probabilistic polynomial-time adversary $\mathcal{A}$, the advantage $Adv^{\mathrm{cr}}_{\mathbf{H}}(\mathcal{A})$ is negligible, where $Adv^{\mathrm{cr}}_{\mathbf{H}} = \Pr\left[\mathcal{H}(K, x_1) = \mathcal{H}(K, x_2) \middle| K \xleftarrow{R} \mathcal{K}; (x_1, x_2) \xleftarrow{R} \mathcal{A}(K);\right]$.

Definition 1 *(Invertible Pairwise-Independent Permutation [4]). A pairwise-independent hash function $\mathbf{H}_{inv} = (\mathcal{K}_{inv}, \mathcal{H}_{inv})$ is an invertible pairwise-independent permutation if it satisfies the following two conditions: (1) Invertible. There exists a PPT algorithm $\mathcal{I}nv$ such that $\mathcal{I}nv(k_{inv}, \mathcal{H}_{inv}(k_{inv}, m)) = m$, where $m \in \{0,1\}^l$ and $k_{inv} \xleftarrow{R} \mathcal{K}_{inv}$; (2) Permutable. $\mathbf{H}_{inv}$ is a permutation.*

Definition 2 *(Lossy TDF [10]). A collection of $(l, l-r)$-lossy trapdoor function $\mathcal{LTDF}$ is defined by four probabilistic polynomial-time algorithms $(\mathcal{K}_{lt}, \widetilde{\mathcal{K}}_{lt}, \mathcal{F}_{lt}, \mathcal{F}_{lt}^{-1})$ satisfying the following properties. (1) $\widetilde{\mathcal{K}}_{lt}$ **induces a lossy***

function. *When algorithm* $\widetilde{\mathcal{K}}_{lt}(1^k)$ *outputs* $(\widetilde{ek}, \perp)$, $\mathcal{F}_{lt}$ *on inputs* $\widetilde{ek}$, $x \in \{0,1\}^l$ *returns* $\mathcal{F}_{lt}(\widetilde{ek}, x)$. *In addition, we also require that the size of* $\mathcal{F}_{lt}(\widetilde{ek}, \cdot)$ *is bounded by* 2^r *for all* $\widetilde{ek}$. ***(2)*** $\mathcal{K}_{lt}$ ***induces an injective function with trapdoor.*** *The key generation algorithm* $\mathcal{K}_{lt}(1^k)$ *outputs* (ek, tk). *Then* $\mathcal{F}_{lt}$ *takes* ek *and an input* $x \in \{0,1\}^l$ *to return an unique value* $c = \mathcal{F}_{lt}(ek, x)$. *Finally, on inputs* $(tk, \mathcal{F}_{lt}(ek, x))$, $\mathcal{F}_{lt}^{-1}$ *returns* x *or* $\perp$. ***(3) Security.*** *Let* EK *denote the fist random variable output by* $\mathcal{K}_{lt}$, *and let* $\widetilde{EK}$ *denote the first random variable output by* $\widetilde{\mathcal{K}}_{lt}$. *For all probabilistic polynomial-time adversary* $\mathcal{A}$, *the advantage of* $\mathcal{A}$ *in distinguishing* EK *from* $\widetilde{EK}$, *denoted by* $Adv^{\mathrm{ind}}_{\mathcal{LTDF}}(\mathcal{A})$, *is negligible, i.e.,* $EK \overset{c}{\approx} \widetilde{EK}$.

Definition 3 *(All-But-n TDF [8]). A collection of* $(l, l-r)$ *all-but-n trapdoor function* $\mathcal{ABN}$ *with the branch set* $\mathbb{B}$ *is defined by a tuple of* 3 *probabilistic polynomial-time algorithms* $(\mathcal{K}_{abn}, \mathcal{F}_{abn}, \mathcal{F}_{abn}^{-1})$ *satisfying the properties below.* ***(1)*** $\mathcal{K}_{abn}$ ***with a given lossy set*** $\mathbb{I}$**.** *For any* n*-subset* $\mathbb{I} \subseteq \mathbb{B}$, *the key generation algorithm* $\mathcal{K}_{abn}(\mathbb{I})$ *returns* (ek, tk). *It requires that for each* $b \in \mathbb{I}$, *the size of* $\mathcal{F}_{abn}(ek, b, \cdot)$ *is bounded by* 2^r *for all* ek. *Additionally, for any branch* $b \in \mathbb{B} \backslash \mathbb{I}$, $\mathcal{F}_{abn}(ek, b, \cdot)$ *is an injective function on* $\{0,1\}^l$, *and* $\mathcal{F}_{abn}^{-1}(tk, b, \mathcal{F}_{abn}(ek, b, x)) = x$ *for all* x. ***(2) Security.*** *For any two distinct* $n-$*subsets* $\mathbb{I}_0, \mathbb{I}_1 \subseteq \mathbb{B}$, *let* EK_0 *denote the first random variable generated by* $\mathcal{K}(\mathbb{I}_0)$ *and* EK_1 *denote the first random variable generated by* $\mathcal{K}(\mathbb{I}_1)$. *For all probabilistic polynomial-time adversary* $\mathcal{A}$, *the advantage of* $\mathcal{A}$ *in distinguishing* EK_0 *from* EK_1, *denoted by* $Adv^{\mathrm{ind}}_{\mathcal{ABN}}(\mathcal{A})$, *is negligible, i.e.,* $EK_0 \overset{c}{\approx} EK_1$.

If the quotient $L = Adv^{\mathrm{ind}}_{\mathcal{ABN}}(\mathcal{A})/Adv(\mathcal{A}')$ is a small constant, we say that the all-but-n TDF $\mathcal{ABN}$ is tightly secure, where $\mathcal{A}'$ is the adversary who attacks the underlying hard problem.

Definition 4 *(*PRIV-IND *Security for Block-Sources [4]). We say that an* l*-bit deterministic public encryption scheme* $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *is* PRIV-IND *secure for* (t, l)*-block-sources if for any* (t, l)*-block-sources* $\overrightarrow{M_0}, \overrightarrow{M_1}$ *of polynomial length* n_{c^*} *and all probabilistic polynomial-time adversary* $\mathcal{A}$, *the* PRIV-IND*-advantage*

$$Adv^{\mathrm{priv-ind}}_{\mathcal{AE}}(\mathcal{A}, \overrightarrow{M_0}, \overrightarrow{M_1}) = Guess_{\mathcal{AE}}(\mathcal{A}, \overrightarrow{M_0}) - Guess_{\mathcal{AE}}(\mathcal{A}, \overrightarrow{M_1})$$

of $\mathcal{A}$ *against* $\mathcal{AE}$ *is negligible, where for* $\beta \in \{0,1\}$

$$Guess_{\mathcal{AE}}(\mathcal{A}, \overrightarrow{M_\beta}) = \Pr\left[\mathcal{A}^{\mathcal{O}}(pk, \mathcal{E}(pk, \overrightarrow{m_\beta})) = 1 \middle| (pk, sk) \overset{R}{\leftarrow} \mathcal{K}; \overrightarrow{m_\beta} \overset{R}{\leftarrow} \overrightarrow{M_\beta}\right].$$

When $n_{c^*} = 1$, we call the scheme PRIV1-IND secure for block-sources; when $\mathcal{O}$ is the encryption oracle $\mathcal{E}(pk, \cdot)$, we call the scheme PRIV-IND-CPA secure for block-sources; when $\mathcal{O}$ includes the encryption and decryption oracle $\mathcal{E}(pk, \cdot) \vee \mathcal{D}(sk, \cdot)^{\neg \overrightarrow{c}^*}$, we call the scheme PRIV-IND-CCA secure for block-sources.

We also define a notion of PRIV-IND-q-CCA security for block-sources which is very similar to PRIV-IND-CCA security for block-sources except with the restriction that the length n_{c^*} of block-sources is bounded by q.

3 Tightly Secure D-PKE Constructions

Let $\mathbf{H}_{inv} = (\mathcal{K}_{inv}, \mathcal{H}_{inv})$ be an l-bit invertible pairwise-independent permutation with the inversion algorithm $\mathcal{I}nv$, and U_{inv} denote the uniform distribution on its range $\mathbb{R}_{inv} = \{0,1\}^l$. Let $\mathcal{LTDF} = (\mathcal{K}_{lt}, \widetilde{\mathcal{K}}_{lt}, \mathcal{F}_{lt}, \mathcal{F}_{lt}^{-1})$ be a collection of $(l, l-r_{lt})$ lossy TDF. Let $\mathcal{ABN} = (\mathcal{K}_{abn}, \mathcal{F}_{abn}, \mathcal{F}_{abn}^{-1})$ be a collection of $(l, l-r_{abn})$ all-but-n TDF with a branch set $\mathbb{B}$ and let $\mathbf{H}_{cr} = (\mathcal{K}_{cr}, \mathcal{H}_{cr})$ be an l-bit collision resistant hash function. And the range $\mathbb{R}_{cr} \subseteq \mathbb{B}$ of $\mathbf{H}_{cr}$ is bounded by $2^{r_{cr}}$.

Key Generation $\mathcal{K}_{cpa}(1^k)$	**Encryption** $\mathcal{E}_{cpa}(pk, m)$	**Decryption** $\mathcal{D}_{cpa}(sk, c)$
$k_{inv} \xleftarrow{R} \mathcal{K}_{inv}(1^k)$;	$h \leftarrow \mathcal{H}_{inv}(k_{inv}, m)$;	$h \leftarrow \mathcal{F}_{lt}^{-1}(tk_{lt}, c)$;
$(ek_{lt}, tk_{lt}) \xleftarrow{R} \mathcal{K}_{lt}(1^k)$;	$c \leftarrow \mathcal{F}_{lt}(ek_{lt}, h)$;	$m' \leftarrow \mathcal{I}nv(k_{inv}, h)$;
$pk := (k_{inv}, ek_{lt})$;	Return c.	Return m'.
$sk := (tk_{lt})$.		

(a) Tightly PRIV-IND-CCA Bounded-Secure D-PKE $\mathcal{AE}_{CCA}$ for Block-Sources

Key Generation $\mathcal{K}_{cca}(1^k)$	**Encryption** $\mathcal{E}_{cca}(pk, m)$	**Decryption** $\mathcal{D}_{cca}(sk, c = b\|\|c_1\|\|c_2)$
$k_{inv} \xleftarrow{R} \mathcal{K}_{inv}(1^k)$;	$h \leftarrow \mathcal{H}_{inv}(k_{inv}, m)$;	$h' \leftarrow \mathcal{F}_{lt}^{-1}(tk_{lt}, c_1)$;
$k_{cr} \xleftarrow{R} \mathcal{K}_{cr}(1^k)$;	$b \leftarrow \mathcal{H}_{cr}(k_{cr}, h)$;	$m' \leftarrow \mathcal{I}nv(k_{inv}, h')$;
$(ek_{lt}, tk_{lt}) \xleftarrow{R} \mathcal{K}_{lt}(1^k)$;	$c_1 \leftarrow \mathcal{F}_{lt}(ek_{lt}, h)$;	$c' \leftarrow \mathcal{E}(pk, m')$;
$\mathbb{I} = \{I_i, i \in [n]\}$, $I_i \xleftarrow{\$} \mathbb{B} \setminus \mathbb{R}_{cr}$;	$c_2 \leftarrow \mathcal{F}_{abn}(ek_{abn}, b, h)$;	If $c' = b\|\|c_1\|\|c_2$, return m',
$(ek_{abn}, tk_{abn}) \xleftarrow{R} \mathcal{K}_{abn}(\mathbb{I})$;	Return $b\|\|c_1\|\|c_2$.	Else return $\perp$.
$pk := (k_{inv}, k_{cr}, ek_{lt}, ek_{abn})$;		
$sk := (tk_{lt})$.		

(b) Tightly PRIV-IND-CCA Bounded-Secure D-PKE $\mathcal{AE}_{CCA}$ for Block-Sources

Fig. 2. Tightly secure D-PKE constructions

Theorem 1. *(1) Let $\mathcal{AE}_{CPA} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be defined in Fig. 2(a). Then, the decryption algorithm can recover the message correctly. And for any probabilistic polynomial-time adversary $\mathcal{A}$, any (t,l)-block-sources $\overrightarrow{M_0}, \overrightarrow{M_1}$ of length n_{c^*}, there exists an adversary $\mathcal{A}_{lt}$ such that*

$$Adv^{\mathrm{priv-ind-cpa}}_{\mathcal{AE}_{CPA}}(\mathcal{A}, \overrightarrow{M_0}, \overrightarrow{M_1}) \leq 2 \cdot Adv^{\mathrm{ind}}_{\mathcal{LTDF}}(\mathcal{A}_{lt}) + 2n_{c^*} \cdot \epsilon, \tag{1}$$

where $\epsilon \leq 2^{\frac{r_{lt}-2-t}{2}}$. (2) Let the D-PKE scheme $\mathcal{AE}_{CCA}$ be depicted in Fig. 2(b). Then the decryption algorithm can recover the message correctly. And for any probabilistic polynomial-time adversary $\mathcal{A}$, any (t,l)-block-sources $\overrightarrow{M_0}, \overrightarrow{M_1}$ of length $n_{c^*} \leq \frac{n}{2}$, there exist adversaries $\mathcal{A}_{cr}, \mathcal{A}_{lt}, \mathcal{A}_{abn}$ such that

$$\begin{aligned} &Adv^{\mathrm{priv-ind-}\frac{n}{2}\mathrm{-cca}}_{\mathcal{AE}_{CCA}}(\mathcal{A}, \overrightarrow{M_0}, \overrightarrow{M_1}) \\ \leq &2 \cdot Adv^{\mathrm{cr}}_{\mathbf{H}_{cr}}(\mathcal{A}_{\mathrm{cr}}) + 2 \cdot Adv^{\mathrm{ind}}_{\mathcal{LTDF}}(\mathcal{A}_{lt}) + 4 \cdot Adv^{\mathrm{ind}}_{\mathcal{ABN}}(\mathcal{A}_{abn}) + 2n_{c^*} \cdot \epsilon, \end{aligned} \tag{2}$$

where $\epsilon \leq 2^{\frac{r_{cr}+r_{lt}+r_{abn}-2-t}{2}}$. Additionally, if the all-but-n TDF $\mathcal{ABN}$ is tightly secure, then the D-PKE construction $\mathcal{AE}_{CCA}$ is tightly PRIV-IND-$\frac{n}{2}$-CCA

secure for block-sources. In the above, $\mathcal{A}_{cr}$ is the adversary who wants to find collisions of $\mathbf{H}_{cr}$, and $\mathcal{A}_{lt}$ (respectively, $\mathcal{A}_{abn}$) is the adversary who attacks the security of $\mathcal{LTDF}$ (respectively, $\mathcal{ABN}$).

Tightly Secure All-But- n **TDF Under the s-DCR Assumption.** Look ahead, tightly PRIV-IND-$\frac{n}{2}$-CCA secure deterministic public-key encryption construction needs the primitive of tightly secure all-but-n TDF. In this paper, we also prove the all-but-n TDF given by [8] is tightly secure with a security loss of only 2. This improves their original security reduction which has a security loss of $2n$ due to the use of the hybrid technique. Please see more details in our full version paper.

Acknowledgments. We thank the anonymous ICICS'2017 reviewers for their helpful comments. This work is supported by the National Cryptography Development Fund MMJJ20170116 and the National Nature Science Foundation of China (Nos. 61602473, 61502480, 61672019, 61772522, 61379137, 61572495).

References

1. Bellare, M., Boldyreva, A., Micali, S.: Public-key encryption in a multi-user setting: security proofs and improvements. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 259–274. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_18
2. Bellare, M., Boldyreva, A., O'Neill, A.: Deterministic and efficiently searchable encryption. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 535–552. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5_30
3. Bellare, M., Fischlin, M., O'Neill, A., Ristenpart, T.: Deterministic encryption: definitional equivalences and constructions without random oracles. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 360–378. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_20
4. Boldyreva, A., Fehr, S., O'Neill, A.: On notions of security for deterministic encryption, and efficient constructions without random oracles. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 335–359. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_19
5. Brakerski, Z., Segev, G.: Better security for deterministic public-key encryption: the auxiliary-input setting. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 543–560. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_31
6. Dolev, D., Dwork, C., Naor, M.: Non-malleable cryptography (extended abstract). In: STOC 1991, pp. 542–552
7. Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 1–27. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_1
8. Hemenway, B., Libert, B., Ostrovsky, R., Vergnaud, D.: Lossy encryption: constructions from general assumptions and efficient selective opening chosen ciphertext security. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 70–88. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_4

9. Mironov, I., Pandey, O., Reingold, O., Segev, G.: Incremental deterministic public-key encryption. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 628–644. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_37
10. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: STOC 2008, pp. 187–196
11. Raghunathan, A., Segev, G., Vadhan, S.: Deterministic public-key encryption for adaptively chosen plaintext distributions. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 93–110. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_6
12. Wee, H.: Dual projective hashing and its applications — lossy trapdoor functions and more. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 246–262. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_16
13. Xie, X., Xue, R., Zhang, R.: Deterministic public key encryption and identity-based encryption from lattices in the auxiliary-input setting. In: Visconti, I., De Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 1–18. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32928-9_1