Efficient Construction of Completely Non-Malleable CCA Secure Public Key Encryption

Shi-Feng Sun*
Shanghai Jiao Tong University
crypto99@sjtu.edu.cn

Dawu Gu
Shanghai Jiao Tong University
dwgu@sjtu.edu.cn

Joseph K. Liu
Monash Univerity
joseph.liu@monash.edu

Udaya Parampalli
The University of Melbourne
udaya@unimelb.edu.au

Tsz Hon Yuen
Huawei, Singapore
Yuen.Tsz.Hon@huawei.com

ABSTRACT

Non-malleability is an important and intensively studied security notion for many cryptographic primitives. In the context of public key encryption, this notion means it is infeasible for an adversary to transform an encryption of some message m into one of a related message m' under the given public key. Although it has provided a strong security property for many applications, it still does not suffice for some scenarios like the system where the users could issue keys on-the-fly. In such settings, the adversary may have the power to transform the given public key and the ciphertext. To withstand such attacks, Fischlin introduced a stronger notion, known as *complete non-malleability*, which requires that the non-malleability property be preserved even for the adversaries attempting to produce a ciphertext of some related message under the transformed public key. To date, many schemes satisfying this stronger security have been proposed, but they are either inefficient or proved secure in the random oracle model. In this work, we put forward a new encryption scheme in the common reference string model. Based on the standard DBDH assumption, the proposed scheme is proved completely non-malleable secure against adaptive chosen ciphertext attacks in the standard model. In our scheme, the well-formed public keys and ciphertexts could be publicly recognized without drawing support from unwieldy techniques like non-interactive zero knowledge proofs or one-time signatures, thus achieving a better performance.

Keywords

Public Key encryption; Complete non-malleability; Chosen-ciphertext attack; Standard model

*This work was done while the author visited the University of Melbourne.

ASIA CCS '16, May 30-June 03, 2016, Xi'an, China

DOI: http://dx.doi.org/10.1145/2897845.2897921

1. INTRODUCTION

Non-malleability is a crucial security requirement in many high-level protocols such as electronic auctions. This property has been formulated for various cryptographic primitives like commitments and signatures. Of particular interest in this work is the non-malleability of public key encryption (PKE), which was initially introduced by Dolev et al. [12]. Informally, an encryption scheme is called non-malleable if it is infeasible for any adversary provided with a public key and a ciphertext of some plaintext m to come up with a ciphertext of a related plaintext m' (under the same public key) and a relation $\mathtt{R}$, via which m' and m are related. When the adaptive chosen ciphertext attack is considered, the adversary is also given access to a decryption oracle even after seeing the challenge ciphertext. In this case, it is always thought of as the strongest security notion for public key encryption, which is usually called non-malleability against adaptive chosen ciphertext attacks (NM-CCA2). So far, many NM-CCA2 secure public key encryption schemes have been proposed such as [9, 21, 10, 7, 20, 16, 8, 17][1].

Although non-malleability could provide a strong security property for many applications, it still can not suffice for some scenarios like the system where users could issue keys on-the-fly. In such settings, the adversary may have the power to transform the given public key and the ciphertext. For example, in an auction system an honest user's bid is encrypted with her public key. An adversarial user, in the middle of the auction process, may be powerful enough to transform such a sealed bid into a new one that is related via the adversarially generated public key and thus easily beat the honest user with a slightly higher bid. The adversary may be able to open his bid only when the honestly sealed bid is opened, even without the corresponding secret key.

Initially motivated by constructing non-malleable commitment [11, 14] by means of encryption schemes, Fischlin [13] introduced a stronger notion, known as *complete non-malleability*. This notion requires that the non-malleability property be preserved even for the adversaries additionally allowed to choose a new public key (without necessarily knowing the associated private key) that may be related to the original one. More precisely, this notion mainly has two differences in contrast to the regular one. First, the adver-

[1]Recall that NM-CCA2 was proved equivalent to the notion of indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2) [4].

sary now is more powerful, who has the ability to tamper the given public key. Second, the goal of the adversary now is to generate a ciphertext (under the tampered public key) of some plaintext that is related to the original via a more general relation which also takes the given and adversarially chosen public key.

As indicated in [13], complete non-malleability is a strictly stronger notion. Particularly, Fischlin proposed some efficient attacks against the well-known Cramer-Shoup encryption scheme [10] and RSA-OAEP [5, 15], which showed that although being NM-CCA2 secure in the regular sense, they are not completely non-malleable even if the adversary is not given access to the decryption oracle. Moreover, a full analysis of relationships of security notions among indistinguishability, non-malleability and complete non-malleability was given in [22], which demonstrated that the complete non-malleability can provide the strongest security guarantee. Thus this notion offers a more adequate security for many scenarios such as the encryption scheme-based higher level protocols, and so as stressed in [12] it will have much more applications than the standard non-complete one.

1.1 Related Work

Although this new notion is more powerful and useful, it turns out in [13] that completely non-malleable PKE scheme is particularly difficult to construct *in the plain model*.

To further understanding the complete non-malleability of encryption schemes and immunize constructions from the random oracle idealization, Ventre and Visconti [24] revisited this concept and gave a game-based definition following the comparison-based approach in [4]. Under this new definition, they also presented two solutions without random oracles conditioned on some assumptions. The first is derived from any semantically secure encryption scheme based on the non-malleable non-interactive zero knowledge proof technique under the assumption that a common reference string is available to all parities (the so-called *common reference string model*). The second is constructed in the interactive setting assuming that oracle queries are issued sequentially. Due to relying on the unwieldy techniques like generic zero knowledge proof, these constructions are mostly feasibility proof of the concept.

Later, Libert and Yung [19] proposed two efficient NM-CCA2* secure PKE schemes in the common reference string model under the framework [24]. In particular, the first is derived from the selective identity-based encryption scheme [6] and a generic one-time signature scheme, which stems from the well-known Canetti-Halevi-Katz (CHK) paradigm [7]. Under the standard bilinear Diffie-Hellman assumption, the scheme is proved NM-CCA2* secure without random oracles. The second is derived from the lossy trapdoor function [20], which is more general but suffers from longer ciphtexts compared with the first one. Almost simultaneously, Barbosa and Farshim [3] put forth another completely non-malleable PKE scheme by using both the techniques from Waters identity-based encryption [25] and certificateless encryption [2]. This scheme is also proved secure in the standard model but suffers from a long public parameter, the length of which is proportional to the output-size of a cryptographic hash.

More recently, Sepahi et al. [23] investigated how to achieve complete non-malleability in the lattice-based setting and gave an efficient provably secure PKE scheme under the learning with errors assumption. As in [19], the scheme is also derived via the CHK methodology but from an lattice-based identity-based encryption [1].

1.2 Motivation

The main motivation for complete non-malleability is to construct higher-level protocols on top of public key encryptions. This notion is useful for guaranteeing the security of such protocols or systems that allow users to issue keys on-the-fly. As mentioned before, it is not easy to construct efficient schemes under this stronger security notion without random oracles. Although a few schemes have been proposed recently, they are either inefficient or proved secure in the random oracle model. As the basic building block of high-level systems, the security and efficiency of the underling PKE scheme plays an important role for the applicability of the whole system. So the scheme with high efficiency and security is more desirable.

1.3 Our Contribution

In this work, our goal is to construct more efficient and simpler PKE schemes in the common reference string model. More precisely, we put forward a new PKE scheme in the pairing-based setting and show that it is proven NM-CCA2* secure in the standard model under the decisional bilinear Diffie-Hellman assumption. In our construction, the well-formed public keys and ciphertexts could be publicly recognized without drawing support from heavy primitives like non-interactive zero knowledge proofs or one-time signatures. It thus requires short public parameters and ciphertexts, leading to a relatively lower communication cost. Moreover, the encryption only requires 3 exponentiations. Hence, it enjoys a good performance and is more suitable for higher-level applications, such as auctions where users encrypt their bids popularly using mobile devices now. The detailed analysis is shown in table 1.

In the comparison, we use $|\mathbb{G}|$ to denote the size of a group-element representation in $\mathbb{G}$, similarly for $\mathbb{G}_T$ and $\mathbb{Z}_p$. Let "$\exp_1$" denote an exponentiation operation over group $\mathbb{G}$ (some of the exponentiations are actually multi-exponentiation), "$\exp_2$" denote an exponentiation operation over $\mathbb{G}_T$, and "pair" be a bilinear pairing operation. For sake of simplicity, the non-expensive operations such as the computation of collision-resistant hash H are discarded. In addition, we assume that the one-time signature scheme used in [19] is denoted by $\mathcal{S}$=(Gen, Sig, Ver), where Gen outputs a signing and verification key $(sk_{\mathcal{S}}, vk)$ and Sig generates a signature σ for message m.

2. PRELIMINARIES

Notation. Throughout the paper, we use κ to denote the security parameter. For a finite set S, we write $s \leftarrow S$ to denote the operation of sampling s from S uniformly at random. For a distribution M, $m \leftarrow M$ denotes the operation of sampling m according to the distribution. If $A(\cdot)$ is a randomized algorithm, we use $a \leftarrow A(\cdot)$ to denote the operation of running the algorithm and assigning the result to a, and use $A(x;r)$ to denote the unique output of A on input x with random coins r. PPT is the abbreviation of probabilistic polynomial-time and $negl(\kappa)$ denotes some negligible function in κ.

Table 1: Comparison of Completely Non-Malleable CCA Secure Schemes

Scheme	CRS	public key†	ciphertext	Encryption	Decryption
LY[19]	$3\|\mathbb{G}\|+\mathcal{S}$	$\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|+vk+\sigma$	$2\exp_1+\exp_2+\mathsf{Sig}$	$3\text{pair}+2\exp_1+\mathsf{Ver}$
BF[3]	$(n+3)\|\mathbb{G}\|+H$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$2\text{pair}+2\exp_1+\exp_2$	$3\text{pair}+4\exp_1$
Ours	$4\|\mathbb{G}\|+H$	$\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|+\|\mathbb{Z}_p\|$	$2\exp_1+\exp_2$	$3\text{pair}+2\exp_1$

†: like the other schemes, the pairing $e(pk, u)$ in our construction can be pre-computed; n: the output-size of H.

2.1 Bilinear Pairing and Assumptions

Let $(\mathbb{G}, \mathbb{G}_T)$ be a couple of cyclic multiplicative groups of prime order p, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a map from $\mathbb{G}$ to $\mathbb{G}_T$. We call the map e a bilinear pairing if it satisfies the following properties: (1) Bilinearity: $e(g^a, h^b) = e(g, h)^{ab}$, for $\forall g, h \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p^*$, (2) Non-degeneracy: there exists $g \in \mathbb{G}$ such that $e(g, g) \neq 1_{\mathbb{G}_T}$, and (3) Computability: there exists an efficient algorithm to compute $e(g, h)$ for $\forall g, h \in \mathbb{G}$.

Definition 1. Let $(\mathbb{G}, \mathbb{G}_T)$ be cyclic groups of prime order p, which are endowed with a bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. The decisional bilinear Diffie-Hellman (DBDH) problem is to distinguish between the distributions $\{(g, g^a, g^b, g^c, e(g, g)^{abc})\}$ and $\{(g, g^a, g^b, g^c, e(g, g)^z)\}$, where g is a generator of $\mathbb{G}$ and a, b, c, z are selected uniformly at random from $\mathbb{Z}_p$. For any PPT distinguisher $\mathcal{D}$ given a random tuple (g, g^a, g^b, g^c, T), it outputs a bit β. If $\beta = 1$, it guesses $T = e(g, g)^{abc}$, otherwise $T = e(g, g)^z$. Formally, its advantage is defined as:

$$Adv^{DBDH}_{\mathcal{D},\mathbb{G},\mathbb{G}_T}(\kappa) = |\Pr[\mathcal{D}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[\mathcal{D}(g, g^a, g^b, g^c, e(g, g)^z) = 1]|.$$

Definition 2. We say that the DBDH assumption holds if for any PPT distinguisher $\mathcal{D}$, its advantage $Adv^{DBDH}_{\mathcal{D},\mathbb{G},\mathbb{G}_T}(\kappa)$ is negligible in κ.

Definition 3. A hash function $H : \mathcal{X} \to \mathcal{Y}$ is said to be collision-resistant if for any PPT algorithm $\mathcal{B}$, its advantage $Adv^{CR}_{\mathcal{B},H}(\kappa)$ defined as $\Pr[x' \neq x \wedge H(x') = H(x) : x, x' \leftarrow \mathcal{B}(H)$ and $x, x' \in \mathcal{X}]$, is negligible in κ.

2.2 Public Key Encryption

In the common reference string model, a PKE scheme consists of four polynomial time algorithms (CRSGen, KeyGen, Enc, Dec): given a security parameter κ, $\mathsf{CRSGen}(1^\kappa)$ outputs a common reference string CRS; given CRS, $\mathsf{KeyGen}(\text{CRS})$ generates a public and secret key pair (pk, sk); given a public key pk and a message m, $\mathsf{Enc}(pk, m)$ outputs a ciphertext c; given a secret key sk and a ciphertext c, $\mathsf{Dec}(sk, c)$ returns a plaintext or a symbol $\perp$ indicating that the ciphertext is invalid. For the standard correctness, it is required $m = \mathsf{Dec}(sk, \mathsf{Enc}(pk, m))$ for any message m, public parameters $\text{CRS} \leftarrow \mathsf{CRSGen}(1^\kappa)$ and $(pk, sk) \leftarrow \mathsf{KeyGen}(1^\kappa)$.

Note that the common reference string is generated by a trusted party and shared by all parties in the system, but not controlled by the adversary. In practice, it can be hard-wired into a device in the implementation.

In addition, all the other algorithms also take (partial) CRS as input, we don't present it explicitly for simplicity.

2.3 Completely Non-Malleable Security

In this work, we follow the game-based notion defined by [24]. First, let us recall an important ingredient termed complete relation. A complete relation $\mathtt{R}$ is an efficient (probabilistic) algorithm, which takes as input a public key pk, a message m, another public key pk^*, a vector of ciphertext $\vec{c}^*$ encrypted under pk^* and the vector of plaintext $\vec{m}^*$ associated with $\vec{c}^*$, and outputs a boolean value. Note that in the common reference string model, the relation also takes the reference string as input.

Definition 4. As defined in [24, 19], let PKE=(Gen, Enc, Dec) be a public key encryption scheme. For any security parameter $\kappa \in \mathbb{N}$ and adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, we define

$$Adv^{NM\text{-}CCA2^*}_{\mathcal{A},\mathsf{PKE}}(\kappa) = |\Pr[\mathbf{Expt}^{NM\text{-}CCA2^*\text{-}0}_{\mathcal{A},\mathsf{PKE}}(\kappa) = 1] - \Pr[\mathbf{Expt}^{NM\text{-}CCA2^*\text{-}1}_{\mathcal{A},\mathsf{PKE}}(\kappa) = 1]|.$$

where the experiment $\mathbf{Expt}^{NM\text{-}CCA2^*\text{-}\delta}_{\mathcal{A},\mathsf{PKE}}(\kappa)$ is defined as:

$\mathbf{Expt}^{NM\text{-}CCA2^*\text{-}\delta}_{\mathcal{A},\mathsf{PKE}}(\kappa)$:
$\text{CRS} \leftarrow \mathsf{CRSGen}(1^\kappa),\ (pk, sk) \leftarrow \mathsf{KeyGen}(\text{CRS})$
$(M, st) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(\text{CRS}, pk)$
$m_0, m_1 \leftarrow M,\ C = \mathsf{Enc}(pk, m_\delta)$
$(\mathtt{R}, pk^*, \vec{C}^*) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(st, M, pk, C)$
return 1 iff $\exists\ \vec{m}^*$ such that
$(\vec{C}^* = \mathsf{Enc}(pk^*, \vec{m}^*)) \wedge$
$(C \notin \vec{C}^* \vee pk \neq pk^*) \wedge$
$(\vec{m}^* \neq \perp) \wedge$
$(\mathtt{R}(m_0, \vec{m}^*, pk, pk^*, \vec{C}^*, \text{CRS}) = 1)$

In the experiment, $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ and $\mathcal{O}_2(\cdot) = \mathcal{D}^{(C)}_{sk}(\cdot)$, meaning the adversary has access to the decryption oracle for any ciphertext but C, even after the challenge phase.

As specified in the previous work [19, 24], the message distribution M is deemed valid if $|m| = |m'|$ for any m, m' with non-zero probability in the message space M. Moreover, the condition $\vec{m}^* \neq \perp$ means that there is at least one valid ciphertext in $\vec{C}^*$, i.e., at least one of the messages in $\vec{m}^*$ is not $\perp$.

Definition 5. The scheme PKE is called $NM\text{-}CCA2^*$ secure if for any PPT adversary, its advantage $Adv^{NM\text{-}CCA2^*}_{\mathcal{A},\mathsf{PKE}}(\kappa)$ is negligible in κ.

3. OUR PROPOSED SCHEME

In this section, inspired by the technique in [18], we present a new PKE scheme in the common reference string model. As argued in previous works, this model is crucial to achieve NM-CCA2* security without random oracles. In fact, we have to find a way to successfully conceal an escrow key in the common reference string, so that it could be used, in the security proof, to not only simulate the decryption oracle but also open the ciphertexts encrypted under the adversarially generated public key.

More concretely, our construction PKE is composed of four efficient algorithms (CRSGen, KeyGen, Encrypt, Decrypt):

CRSGen(1^κ): taking a security parameter κ as input, this algorithm generates cyclic groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order p, which are endowed with a bilinear pairing $e : \mathbb{G}\times\mathbb{G} \to \mathbb{G}_T$. It also randomly chooses $g, u, v, w \in \mathbb{G}$ and a collision-resistant hash function $H : \mathbb{G}\times\mathbb{G}_T\times\mathbb{G} \to \mathbb{Z}_p$. Finally, it sets the common reference string as CRS $= (\kappa, \mathbb{G}, \mathbb{G}_T, e, g, u, v, w, H)$.

KeyGen(CRS): given the common reference string CRS, the algorithm randomly picks $\alpha \in \mathbb{Z}_p$ and sets the public key $pk = g^\alpha$ and the secret key $sk = \alpha$.

Encrypt(pk, m): taking as input pk and a message $m \in \mathbb{G}_T$, the algorithm randomly chooses $r, s \in \mathbb{Z}_p$ and computes C_0, C_1 and C_2 as:

$$C_0 = e(pk, u)^r \cdot m,\ C_1 = g^r,\ C_2 = (u^t v^s w)^r,$$

where $t = H(pk, C_0, C_1)$. Eventually, it returns $C = (C_0, C_1, C_2, s)$ as the ciphertext.

Decrypt(pk, sk, C): given pk, sk and a ciphertext $C = (C_0, C_1, C_2, s)$, this algorithm first computes the value $t = H(pk, C_0, C_1)$, and then it checks if

$$e(C_1, u^t v^s w) = e(g, C_2).$$

If not, it returns $\perp$; otherwise, computes and outputs

$$m = C_0/e(C_1, u^\alpha).$$

Remark 1. As in the first construction of [19], for any group element in $\mathbb{G}$ (the public key space), there exists a corresponding private key in $\mathbb{Z}_p$, so all elements of $\mathbb{G}$ are admissible public keys[2] in our construction. Moreover, the validity of ciphertexts could be verified publicly, without relying on the non-interactive zero knowledge proofs or one-time signatures compared with the previous work. Obviously, our construction would enjoy a better efficiency.

4. SECURITY ANALYSIS

The correctness of the scheme could be easily verified. In the following, we give the security analysis of our construction based on the standard hardness assumptions.

THEOREM 1. *The proposed scheme is NM-CCA2* secure under the DBDH assumption and the collision-resistance of hash function H. Particularly, for any security parameter κ and efficient adversary $\mathcal{A}$, it holds that*

$$Adv^{NM\text{-}CCA2^*}_{\mathcal{A},PKE}(\kappa) \le 4Adv^{CR}_{\mathcal{B},H}(\kappa) + 2Adv^{DBDH}_{\mathcal{D},\mathbb{G},\mathbb{G}_T}(\kappa) + 2(q_d + q_c)/p + 2\epsilon,$$

where q_d denotes the number of decryption queries made by $\mathcal{A}$, and q_c the number of elements of $\vec{C}^*$ finally output by $\mathcal{A}$.

PROOF. For the limit of space, we only give a rough proof here, which is conducted via a sequence of games. Throughout the proof, we use $\text{Game}_i(\delta)$ to denote the i-th game and $S_i(\delta)$ to denote the event that the challenger finally succeeds.

Game$_0(\delta)$: This is essentially the real game. In more details, the challenger generates and returns the common reference string CRS and the public key pk, and answers the decryption queries using the secret key sk. During the challenge phase, the adversary makes a challenge query for a plaintext distribution M of his choice. For this query, the challenger chooses $m_0, m_1 \leftarrow M$, randomly picks $r, s \leftarrow \mathbb{Z}_p$ and computes C_0, C_1 and C_2 as follows:

$$C_0 = e(pk, u)^r \cdot m_\delta,\ C_1 = g^r,\ C_2 = (u^t v^s w)^r,$$

where $t = H(pk, C_0, C_1)$. Then it returns $C = (C_0, C_1, C_2, s)$ as the challenge ciphertext. After this, the adversary keeps on querying the decryption of any ciphertext except for C. Finally, the adversary $\mathcal{A}$ outputs a possibly new public key pk^*, a vector of ciphertext $\vec{C}^*$ (encrypted under pk^*) and the description of a relation R. At this point, the challenger calls an all powerful oracle that could compute $\alpha^* \in \mathbb{Z}_p$ satisfying $pk^* = g^{\alpha^*}$, and then uses α^* to open the ciphertexts $\vec{C}^*$. We denote the corresponding plaintext vector by $\vec{m}^* = \text{Decrypt}(pk^*, sk^*, \vec{C}^*)$. Then the challenger uses $\vec{m}^*$ and $\vec{C}^*$ to evaluate the relation $\mathtt{R}(m_0, \vec{m}^*, pk, pk^*, \vec{C}^*, \text{CRS})$ and checks whether $(C \notin \vec{C}^* \vee pk \neq pk^*)$ and $\vec{m}^* \neq \perp$ or not. If all these conditions are satisfied, the challenger outputs 1, otherwise 0. By definition, we have $Adv^{NM\text{-}CCA2^*}_{\mathcal{A},\mathsf{PKE}}(\kappa) = |\Pr[S_0(0)] - \Pr[S_0(1)]|$.

Game$_1(\delta)$: This game is the same as $\text{Game}_0(\delta)$, except that the common reference string is generated in the following way: the challenger chooses random elements b, x_v, x_w, y_v, y_w from $\mathbb{Z}_p$ at the outset of the game, and then sets $u = g^b, v = g^{bx_v+y_v}, w = g^{bx_w+y_w}$ rather than randomly choosing u, v, w from $\mathbb{G}$. Obviously, the common reference string generated in this way has the same distribution as the real game. Hence, we have $\Pr[S_1(\delta)] = \Pr[S_0(\delta)]$.

Game$_2(\delta)$: This game differs from the previous only in the generation of the challenge ciphertext. Concretely, the ciphertext $C = (C_0, C_1, C_2, s)$ is generated as follows:

1. Choose $m_0, m_1 \leftarrow M$ and randomly pick $r \leftarrow \mathbb{Z}_p$.
2. Compute $C_0 = e(pk, u)^r \cdot m_\delta$ and $C_1 = g^r$, and evaluate $t = H(pk, C_0, C_1)$.
3. Set $s = -(t + x_w)/x_v$ and $C_2 = C_1^{sy_v+y_w}$.

From the construction, we know that $C_2 = C_1^{sy_v+y_w} = g^{br(t+sx_v+x_w)} \cdot g^{r(sy_v+y_w)} = (u^t v^s w)^r$ and the values x_v and x_w are completely hidden by y_v and y_w respectively. Thus, the ciphertext is well-formed and properly-distributed, which implies that $\Pr[S_2(\delta)] = \Pr[S_1(\delta)]$.

Game$_3(\delta)$: This game is the same as $\text{Game}_2(\delta)$ except for the treatment of the decryption queries. For such a query $C' = (C'_0, C'_1, C'_2, s')$, the challenger answers it as follows.

If C' is queried before the challenge phase, the challenger computes $t' = H(pk, C'_0, C'_1)$ and verifies its validity. If invalid, outputs $\perp$. Otherwise, implying $C'_2 = (u^{t'} v^{s'} w)^{r'}$ for some $r' \in \mathbb{Z}_p$ s.t $g^{r'} = C'_1$, it further checks if $t' + s'x_v + x_w \neq 0$. If so, it computes $u^{r'} = (C'_2/C'^{\,s'y_v+y_w}_1)^{1/(t'+s'x_v+x_w)}$ and decrypts C' by evaluating $m' = C'_0/e(pk, u^{r'})$. Otherwise, it aborts and outputs a random bit.

If C' appears after the challenge phase, the challenger decrypts it via the following steps, recalling that $C' \neq C$ in this case:

1. Compute $t' = H(pk, C'_0, C'_1)$ and check if $(pk, C'_0, C'_1) \neq (pk, C_0, C_1)$ but $t' = t$. If true, the challenger aborts and outputs a random bit. Note that in this case we could find a collision of H by employing $\mathcal{A}$.

[2]Similar to our scheme and [19], the admissible public keys in [3] also need not to be guaranteed by non-interactive zero knowledge proofs like [24], but they have to satisfy some additional pairing equations.

2. In the case $(pk, C_0', C_1') \neq (pk, C_0, C_1)$ and $t' \neq t$, we have $t' + s'x_v + x_w \neq 0$ if $s' = s$. Provided that C' is valid, then it could be decrypted as before. If $s' \neq s$, the challenger checks if $t' + s'x_v + x_w \neq 0$. If so, the ciphertext is decrypted as above. Otherwise, it aborts and outputs a random bit.

3. For the last case $(pk, C_0', C_1') = (pk, C_0, C_1)$, the challenger directly returns $\perp$ since the ciphertext $C' \neq C$ is invalid except with a negligible probability ϵ.

It is easy to observe that the decryption oracle is perfectly simulated in the above game unless the challenger aborts or the adversary generates a *valid* C' such that $(C_0', C_1') = (C_0, C_1)$. From the above, we know that C' is valid with only a negligible probability ϵ. Moreover, the challenger aborts only when the collision of H happens or the equation $t'+s'x_v+x_w = 0$ holds. As mentioned before, the probability for the former case is bounded by $Adv^{CR}_{\mathcal{B},H}(\kappa)$ due to the collision-resistance of H. For the latter case, we analyze it as below.

At the beginning of this game, both x_v and x_w are blinded by y_v and y_w respectively, and so they are initially hidden from the adversary. For each decryption query $C' = (C_0', C_1', C_2', s')$, the challenger returns $\perp$ if C' is invalid and otherwise it outputs the corresponding plaintext. Actually, the adversary only obtains from the later case the linear combinations of $bx_v + y_v$ and $bx_w + y_w$, which was already known from the CRS. Hence, the answers to these queries leak no more information about x_v and x_w. After observing the challenge ciphertext C, the adversary gets the fact that $t + sx_v + x_w = 0$, but there still exist exactly p possible and equally likely pairs (x_v, x_w) satisfying this equation. Hence the probability that $t' + s'x_v + x_w = 0$ is at most $1/p$. Assuming that the adversary makes at most q_d decryption queries, the probability that $t' + s'x_v + x_w = 0$ holds for at least one query is at most q_d/p. Thus, we get that $|\Pr[S_3(\delta)] - \Pr[S_2(\delta)]| \leq Adv^{CR}_{\mathcal{B},H}(\kappa) + q_d/p + \epsilon$.

Game$_4(\delta)$: The only difference of this game from the previous is the processing of the vector of ciphertexts $\vec{C}^*$ output by the adversary in the end. Instead of decrypting the ciphertext $C^* = (C_0^*, C_1^*, C_2^*, s^*) \in \vec{C}^*$ with the help of all powerful oracle, we handle it by employing the trapdoor information x_v, x_w, y_v, y_w concealed in CRS. More precisely, for each C^* w.r.t the public key pk^*, it is treated as follows:

1. If $pk^* = pk$, we have $C^* \neq C$. In this case, it could be handled like the decryption queries before.

2. Otherwise, compute $t^* = H(pk^*, C_0^*, C_1^*)$ and check if $(pk^*, C_0^*, C_1^*) \neq (pk, C_0, C_1)$ but $t^* = t$. If true, the challenger aborts and outputs a random bit. Similarly, if this were happen, we would find a collision of H.

3. For the case $(pk^*, C_0^*, C_1^*) \neq (pk, C_0, C_1)$[3] and $t^* \neq t$, we have $t^* + s^*x_v + x_w \neq 0$ if $s^* = s$. Further, when C^* is a valid ciphertext, implying $C_2^* = (u^{t^*}v^{s^*}w)^{r^*}$ for some $r^* \in \mathbb{Z}_p$ s.t $g^{r^*} = C_1^*$, we can get $u^{r^*} = (C_2^*/{C_1^*}^{s^*y_v+y_w})^{1/(t^*+s^*x_v+x_w)}$ and recover the plaintext by computing $m^* = C_0^*/e(pk^*, u^{r^*})$. If $s^* \neq s$, check whether $t^* + s^*x_v + x_w \neq 0$ or not. If so, the ciphertext could be decrypted similarly. Otherwise, it aborts and outputs a random bit.

[3]Similar to the last case in Game$_3(\delta)$, the challenger will return $\perp$ for the ciphertext C^* such that $(C_0^*, C_1^*) = (C_0, C_1)$. The detailed analysis will be given in the full version.

It is easy to observe from the above simulation that all ciphertexts including the decryption queries and the elements of the final output $\vec{C}^*$ could be properly processed in polynomial time. Unless the challenger aborts, the treatment of C^* is perfectly simulated, just as it were decrypted using the associated secret key sk^*. Similar to the analysis before, we get $|\Pr[S_4(\delta)] - \Pr[S_3(\delta)]| \leq Adv^{CR}_{\mathcal{B},H}(\kappa) + q_c/p$, where q_c is the number of ciphertexts in $\vec{C}^*$ output by $\mathcal{A}$ in the end.

Game$_5(\delta)$: This game is identical to the above except that both the CRS and the ciphertext are computed using the DBDH tuple $(g, g^a, g^b, g^c, e(g,g)^{abc})$, where $a, b, c \leftarrow \mathbb{Z}_p$. Specifically, the challenger chooses $x_v, x_w, y_v, y_w \in \mathbb{Z}_p$ uniformly at random and sets $pk = g^a, u = g^b, v = g^{bx_v+y_v}$ and $w = g^{bx_w+y_w}$.

For the challenge ciphertext $C = (C_0, C_1, C_2, s)$, it is generated as:

1. Choose $m_0, m_1 \leftarrow M$, set $C_0 = e(g,g)^{abc} \cdot m_\delta$, $C_1 = g^c$ and evaluate $t = H(pk, C_0, C_1)$.

2. Set $s = -(t + x_w)/x_v$ and compute $C_2 = (g^c)^{(sy_v+y_w)}$.

This game is essentially identical to the previous, so we have $\Pr[S_5(\delta)] = \Pr[S_4(\delta)]$.

Game$_6(\delta)$: The final game is identical to the previous except that the challenge message m_δ is hidden by a uniformly random element $e(g,g)^z \in \mathbb{G}_T$, where $z \leftarrow \mathbb{Z}_p$.

Under the DBDH assumption, it is easy to show that Game$_6(\delta)$ is computationally indistinguishable from Game$_5(\delta)$, so we have $|\Pr[S_6(\delta)] - \Pr[S_5(\delta)]| \leq Adv^{DBDH}_{\mathcal{D},\mathbb{G},\mathbb{G}_T}(\kappa)$.

In combination of all the probability (in)equations, we get

$$\begin{aligned} & |\Pr[S_6(\delta)] - \Pr[S_0(\delta)]| \\ \leq\ & 2Adv^{CR}_{\mathcal{B},H}(\kappa) + Adv^{DBDH}_{\mathcal{D},\mathbb{G},\mathbb{G}_T}(\kappa) + (q_d + q_c)/p + \epsilon. \end{aligned}$$

Thus, for any PPT adversary $\mathcal{A}$, its advantage against our scheme is

$$\begin{aligned} & Adv^{NM\text{-}CCA2^*}_{\mathcal{A},\mathsf{PKE}}(\kappa) \\ =\ & |\Pr[S_0(0)] - \Pr[S_0(1)]| \\ \leq\ & |\Pr[S_0(0)] - \Pr[S_6(0)]| + |\Pr[S_6(0)] - \Pr[S_6(1)]| \\ & + |\Pr[S_6(1)] - \Pr[S_0(1)]| \\ \leq\ & 4Adv^{CR}_{\mathcal{B},H}(\kappa) + 2Adv^{DBDH}_{\mathcal{D},\mathbb{G},\mathbb{G}_T}(\kappa) + 2(q_d + q_c)/p + 2\varepsilon, \end{aligned}$$

where the last inequation follows from $\Pr[S_6(0)] = \Pr[S_6(1)]$. □

5. EFFICIENCY ANALYSIS

In this section, we give a brief efficiency analysis of our scheme and compare it with the efficient constructions proposed by Libert et al. [19] and Barbosa et al. [3] respectively. In this comparison, the modified version of RSA-OAEP [13] is not considered as its security is proved in the random oracle model. We also do not take into account the constructions given in [24] and [23], where the former is based on the inefficient non-interactive zero knowledge proof or the interaction techniques and the latter is constructed in the lattice-based setting (similar to [19], also with one-time signature as the basic building block). The detailed comparison is given in Table 1.

6. CONCLUSION

In this work, we put forward a new efficient public key encryption scheme, and show that it is provably completely non-malleable secure against adaptive chosen-ciphertext attacks in the common reference string model without random oracles. In contrast to the existing work, our scheme relies on neither the inefficient non-interactive zero knowledge proofs nor the one-time signature schemes, thus it achieves a better performance and is more suitable to be applied in the high-level systems where efficiency is extensively concerned, especially for mobile applications.

Acknowledgments

The authors are supported by the Major State Basic Research Development Program (No. 2013CB338004), the Natural Science Foundation of China (No. 61472250) and the Scientific Research Foundation of Ministry of Education of China and China Mobile (No. MCM20150301).

7. REFERENCES

[1] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In *Advances in Cryptology - EUROCRYPT 2010, French Riviera, May 30 - June 3, 2010*, pages 553–572, 2010.

[2] S. S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In *Advances in Cryptology - ASIACRYPT 2003, Taipei, Taiwan, November 30 - December 4, 2003*, pages 452–473, 2003.

[3] M. Barbosa and P. Farshim. Relations among notions of complete non-malleability: Indistinguishability characterisation and efficient construction without random oracles. In *ACISP 2010, Sydney, Australia, July 5-7, 2010*, pages 145–163, 2010.

[4] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology - CRYPTO '98, Santa Barbara, California, USA, August 23-27, 1998*, pages 26–45, 1998.

[5] M. Bellare and P. Rogaway. Optimal asymmetric encryption. In *Advances in Cryptology - EUROCRYPT '94, Perugia, Italy, May 9-12, 1994*, pages 92–111, 1994.

[6] D. Boneh and X. Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2004, Interlaken, Switzerland, May 2-6, 2004*, pages 223–238, 2004.

[7] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In *Advances in Cryptology - EUROCRYPT 2004, Interlaken, Switzerland, May 2-6, 2004*, pages 207–222, 2004.

[8] D. Cash, E. Kiltz, and V. Shoup. The twin diffie-hellman problem and applications. In *EUROCRYPT 2008, Istanbul, Turkey, April 13-17, 2008*, pages 127–145, 2008.

[9] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Advances in Cryptology - CRYPTO '98, Santa Barbara, California, USA, August 23-27, 1998*, pages 13–25, 1998.

[10] R. Cramer and V. Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT 2002, Amsterdam, The Netherlands, April 28 - May 2, 2002*, pages 45–64, 2002.

[11] G. D. Crescenzo, J. Katz, R. Ostrovsky, and A. Smith. Efficient and non-interactive non-malleable commitment. In *EUROCRYPT 2001, Innsbruck, Austria, May 6-10, 2001*, pages 40–59, 2001.

[12] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. *SIAM J. Comput.*, 30(2):391–437, 2000.

[13] M. Fischlin. Completely non-malleable schemes. In *ICALP 2005, Lisbon, Portugal, July 11-15, 2005*, pages 779–790, 2005.

[14] M. Fischlin and R. Fischlin. Efficient non-malleable commitment schemes. In *Advances in Cryptology - CRYPTO 2000, Santa Barbara, California, USA, August 20-24, 2000*, pages 413–431, 2000.

[15] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is secure under the RSA assumption. In *Advances in Cryptology - CRYPTO 2001, Santa Barbara, California, USA, August 19-23, 2001*, pages 260–274, 2001.

[16] G. Hanaoka and K. Kurosawa. Efficient chosen ciphertext secure public key encryption under the computational diffie-hellman assumption. In *Advances in Cryptology - ASIACRYPT 2008, Melbourne, Australia, December 7-11, 2008*, pages 308–325, 2008.

[17] D. Hofheinz, E. Kiltz, and V. Shoup. Practical chosen ciphertext secure encryption from factoring. *J. Cryptology*, 26(1):102–118, 2013.

[18] J. Lai, R. H. Deng, S. Liu, and W. Kou. Efficient CCA-secure PKE from identity-based techniques. In *Topics in Cryptology - CT-RSA 2010, San Francisco, CA, USA, March 1-5, 2010*, pages 132–147, 2010.

[19] B. Libert and M. Yung. Efficient completely non-malleable public key encryption. In *ICALP 2010, Bordeaux, France, July 6-10, 2010*, pages 127–139, 2010.

[20] C. Peikert and B. Waters. Lossy trapdoor functions and their applications. In *STOC '08, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 187–196, 2008.

[21] A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *FOCS '99, 17-18 October, 1999, New York, NY, USA*, pages 543–553, 1999.

[22] R. Sepahi, J. Pieprzyk, S. F. Shahandashti, and B. Schoenmakers. New security notions and relations for public-key encryption. *J. Mathematical Cryptology*, 6(3-4):183–227, 2012.

[23] R. Sepahi, R. Steinfeld, and J. Pieprzyk. Lattice-based completely non-malleable public-key encryption in the standard model. *Des. Codes Cryptography*, 71(2):293–313, 2014.

[24] C. Ventre and I. Visconti. Completely non-malleable encryption revisited. In *Public Key Cryptography - PKC 2008, Barcelona, Spain, March 9-12, 2008*, pages 65–84, 2008.

[25] B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT 2005, Aarhus, Denmark, May 22-26, 2005*, pages 114–127, 2005.