RKA Secure PKE Based on the DDH and HR Assumptions*

Dingding Jia[1,2], Xianhui Lu[1], Bao Li[1], and Qixiang Mei[3]

[1] Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
[2] University of Chinese Academy of Sciences, Beijing, China
[3] College of Information, Guangdong Ocean University
{ddjia,xhlu,lb}@is.ac.cn, nupf@163.com

Abstract. In this paper, we prove the security against related key attacks of two public key encryption schemes in the standard model. The first scheme is a variation of the scheme (KYPS09) presented by Kiltz, Pietrzak et al. in Eurocrypt 2009. While KYPS09 has been proved CCA secure under the DDH assumption, we show that it is not secure against related key attacks when the class of related key functions includes affine functions. We make a modification on KYPS09 and prove that the resulted scheme is secure against related key attacks in which the related key functions could be affine functions. We also prove the security against related key attacks of the scheme presented by Hofheinz and Kiltz in Crypto 2009 based on the HR assumption. The security proofs rely heavily on a randomness extractor called 4-wise independent hash functions.

Keywords: related key attack, 4-wise independent hash, DDH assumption, HR assumption.

1 Introduction

Since "cold-boot" attacks demonstrated a practical threat to cryptography systems [13], researchers have contributed much effort to constructing schemes against side channel attacks. Among these attacks there is one kind called related key attacks (RKA), which means that attackers can modify keys stored in the memory and observe the outcome of the cryptographic primitive under this modified key [10,8].

In this work we study public key encryption (PKE) schemes against chosen ciphertext RKA (CC-RKA), which is formulated by Bellare et al. [4]. Following the original theory given by Bellare and Kohoo [5], the definition is parameterized

* This work is Supported by the National Basic Research Program of China (973 project)(No.2013CB338002), the National Nature Science Foundation of China (No.61070171, No.61272534), the Strategic Priority Research Program of Chinese Academy of Sciences under Grant XDA06010702 and IIE's Cryptography Research Project (No. Y3Z0027103, No.Y3Z0024103).

W. Susilo and R. Reyhanitabar (Eds.): ProvSec 2013, LNCS 8209, pp. 271–287, 2013.

by the class of Φ functions that the adversary can apply to the secret key. As denoted by Bellare et al. [7], let S be the secret key space. If S is a group, $\Phi^{\text{lin}} = \{\phi_a\}_{a \in S}$ is used to denote the class of linear functions; if S is a ring, $\Phi^{\text{affine}} = \{\phi_{a,b}\}_{a,b \in S}$ is used to denote the class of affine functions; $\Phi^{\text{poly}(d)}$ is used to denote the class of polynomial functions bounded by degree d.

Bellare, Cash and Miller [4] showed that CC-RKA secure PKE can be transformed from RKA secure pseudorandom functions (PRF) and RKA secure identity based encryption (IBE) separately for the same class of Φ. In [3] Bellare and Cash gave a framework of building RKA secure PRFs for $\Phi = \Phi^{\text{lin}}$. In [7] Bellare, Paterson and Thomson gave a framework of building RKA secure IBE for $\Phi = \Phi^{\text{poly}(d)}$. So by combining [4] and [3] we can get Φ-CC-RKA secure PKE for $\Phi = \Phi^{\text{lin}}$; and by combining [4] and [7] we can get Φ-CC-RKA secure PKE for $\Phi = \Phi^{\text{poly}(d)}$. In [19] Wee proposed a framework of constructing Φ-CC-RKA secure PKE from adaptive trapdoor relations for $\Phi = \Phi^{\text{lin}}$.

In [19] Wee pointed out that the Cramer-Shoup CCA secure construction [11] can not achieve CC-RKA security through their approach, since the property that the secret key has some residual entropy given only its evaluation on a non-DDH tuple makes it impossible to fulfill "finger-printing". However, whether all variants of the Cramer-Shoup construction can not achieve CC-RKA secure is still an open problem. Is "finger-printing" a necessary condition of CC-RKA security for PKE?

Our Result. In this work we prove the Φ-CC-RKA security of two PKE schemes for $\Phi = \Phi^{\text{affine}}$ in the standard model.

- The first scheme is based on the DDH assumption, and it achieves Φ-CC-RKA security by making a modification to the CCA secure PKE proposed by Kiltz et al. [16], which is a variant of the Cramer-Shoup construction. As in [16], here we use 4-wise independent hash functions as a randomness extractor. In the appendix we give a successful RKA attack on the PKE scheme in [16] when Φ includes affine functions. By applying the 4-wise independent hash function to more group elements, we get a PKE scheme that is secure against Φ-CC-RKA for $\Phi = \Phi^{\text{affine}}$.
- The second scheme is presented by Hofheinz and Kiltz [15] based on the HR assumption. The scheme is an instantiation in the group QR_N^+ of "Diffie-Hellman integrated encryption scheme" (DHIES) [2], which is contained in several standard bodies, e.g. in IEEE P1363a, SECG and ISO 18033-2.

In the security proof, queries of the form (C, ϕ) are easy to answer since the simulator holds the secret key. Although there exists many $sk' \neq sk$ corresponding to which the challenge ciphertext C^* is valid, it is difficult for any PPT adversary $\mathcal{A}$ to submit a ϕ such that $\phi(sk) \neq sk$ and C^* is valid corresponding to $\phi(sk)$ under reasonable intractable assumptions.

Table 1 shows a comparison of known CC-RKA secure PKE schemes in the standard model. Take the second row for example: by combining [4] and [3], we can get Φ-CC-RKA secure schemes for $\Phi = \Phi^{\text{lin}}$ separately based on the DDH and DLIN assumption. From the table we can see that [4]+[3] and [19] can only achieve Φ-CC-RKA security for $\Phi = \Phi^{\text{lin}}$. Although [4]+[7] can achieve Φ-CC-RKA security for $\Phi = \Phi^{\text{poly}(d)}$, it is based on a q-type hardness assumption which is not so standard. Only [4]+[7] and our result can achieve Φ-CC-RKA security for $\Phi = \Phi^{\text{affine}}$ under widely accepted assumptions like BDDH, DDH and HR in the standard model.

Table 1. A comparison of known CC-RKA secure PKE schemes

Works	Φ	Assumptions
[4]+[3]	lin	DDH,DLIN
[4]+[7]	affine	BDDH
[4]+[7]	poly(d)	q-EBDDH
[19]	lin	factoring,BDDH,LWE
Ours	affine	DDH,HR

The rest of our paper is organized as follows: in section 2 we give definitions and preliminaries; in section 3 we give complexity assumptions; in section 4 we describe the PKE constructions and prove the security; section 5 is the conclusion of the whole paper.

2 Definitions and Preliminaries

2.1 Notation

We use PPT as the abbreviation of probabilistic polynomial time. Let $l(X)$ denote the length of X. Let X and Y be probability spaces on a finite set S, the statistical distance $SD(X, Y)$ between X and Y is defined as $SD(X, Y) := \frac{1}{2}\Sigma_{\alpha \in S}|\Pr_X[\alpha] - \Pr_Y[\alpha]|$, The min-entropy of a random variable X is defined as $H_\infty(X) = -\log_2(max_{x\in D} \Pr[X = x])$, wherein D is the domain of X.

2.2 Security Definition

Here we give the security definition of Φ-CC-RKA security. The security of a PKE scheme is defined using the following game between an adversary $\mathcal{A}$ and a challenger.

Setup: The challenger runs the key generation algorithm $Keygen(pp) \to (pk, sk)$, sends pk to the adversary $\mathcal{A}$, and keeps the secret key sk to itself.

Phase 1: $\mathcal{A}$ adaptively issues queries (ϕ, C) where $\phi \in \Phi$, the challenger responds with $Dec(\phi(sk), C)$.

Challenge: $\mathcal{A}$ submits two messages (m_0, m_1) to the challenger. The challenger picks a random bit b and responds with $Encrypt(pk, m_b)$.

Phase 2: $\mathcal{A}$ adaptively issues additional queries as in Phase 1, with the restriction that $(\phi(sk), C) \neq (sk, C^*)$.

Guess: $\mathcal{A}$ outputs a guess b' of b.

The advantage of $\mathcal{A}$ is defined as $Adv_{\mathcal{A},\Phi} = \left|\Pr[b' = b] - \frac{1}{2}\right|$.

Definition 1 (Φ-CC-RKA Security). *A PKE scheme is Φ-CC-RKA secure if for all PPT adversary $\mathcal{A}$, $Adv_{\mathcal{A},\Phi}$ is negligible in λ.*

Here our security definition follows the definition given by Bellare et al. [4]. However, in [4] it is required that the public key is completely determined by the secret key, while in our paper part of the elements in the public key can be randomly chosen and irrelevant to the secret key.

Symmetric Encryption. A symmetric encryption scheme consists of two polynomial time algorithms: $(\mathcal{E}, \mathcal{D})$. Let $\mathcal{K}_{SE}$ be the secret key space. The encryption algorithm $\mathcal{E}$ takes as input a message m and a secret key K and outputs a ciphertext χ, $\mathcal{E}(K, m) = \chi$; the decryption algorithm $\mathcal{D}$ takes as input the ciphertext χ and a secret key K and outputs a message m or $\perp, \mathcal{D}(K, \chi) = m$ or $\perp$. Here we require both algorithms are deterministic. For correctness we require that $\mathcal{D}(K, \mathcal{E}(K, m)) = m$.
Ciphertext Indistinguishability. Let $SE = (\mathcal{E}, \mathcal{D})$ be a symmetric key encryption scheme, the advantage of an adversary $\mathcal{A}$ in breaking the ciphertext indistinguishability (IND-OT) of SE is defined as:

$$Adv_{\mathcal{A}}^{IND-OT} = \left|\Pr\left[b = b' : \begin{array}{l} K^* \leftarrow_R \mathcal{K}_{SE}; (m_0, m_1) \leftarrow \mathcal{A}; b \leftarrow_R \{0,1\}; \\ \chi^* \leftarrow \mathcal{E}(K^*, m_b); b' \leftarrow \mathcal{A}(\chi^*) \end{array}\right] - \frac{1}{2}\right|$$

We say that SE is one-time secure in the sense of indistinguishability (IND-OT) if for every PPT $\mathcal{A}, Adv_{\mathcal{A}}^{IND-OT}$ is negligible.
Ciphertext Integrity. Informally, ciphertext integrity requires that it is difficult to create a valid ciphertext corresponding to a random secret key for any PPT adversary $\mathcal{A}$, even $\mathcal{A}$ is given an encryption of a chosen message with the same key before. Let $SE = (\mathcal{E}, \mathcal{D})$ be a symmetric key encryption scheme, the advantage of an adversary $\mathcal{A}$ in breaking the ciphertext integrity (INT-OT) of SE is defined as:

$$Adv_{\mathcal{A}}^{INT-OT} = \left|\Pr\left[\chi \neq \chi^* \wedge \mathcal{D}(K^*, \chi) \neq \perp : \begin{array}{l} K^* \leftarrow_R \mathcal{K}_{SE}; m \leftarrow \mathcal{A}; \\ \chi^* \leftarrow \mathcal{E}(K^*, m); \chi \leftarrow \mathcal{A}(\chi^*) \end{array}\right]\right|$$

We say that SE is one-time secure in the sense of integrity (INT-OT) if for every PPT $\mathcal{A}, Adv_{\mathcal{A}}^{INT-OT}$ is negligible.

Authenticated Encryption. A symmetric encryption scheme SE is secure in the sense of one-time authenticated encryption (AE-OT) iff it is IND-OT and INT-OT secure. An AE-OT secure symmetric encryption can be easily constructed using a one-time symmetric encryption and an existentially unforgeable MAC [11,6].

2.3 Primitives

Here we introduce a primitive called 4-wise independent hash family [16] that can be used as a randomness extractor. A simple construction of 4-wise independent hash family is shown in [16].

Definition 2 (4-wise Independent Hash Family). *Let $\mathcal{HS}$ be a family of hash functions $\mathcal{H} : \mathcal{X} \to \mathcal{Y}$. We say that $\mathcal{HS}$ is 4-wise independent if for any distinct $x_1, x_2, x_3, x_4 \in \mathcal{X}$, the random variables $\mathcal{H}(x_1), ..., \mathcal{H}(x_4)$ are uniform and independently random, where $\mathcal{H} \leftarrow_R \mathcal{HS}$.*

The next two lemmata state that for a 4-wise independent hash function $\mathcal{H}$ and two random variables $X, \tilde{X}$ with $\Pr[X = \tilde{X}] = \delta$ negligible that even related, the random variable $(\mathcal{H}, \mathcal{H}(X))$ and $(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X}))$ is close to uniformly random as long as the min-entropy of X and $\tilde{X}$ are large enough.

Lemma 1 (Leftover Hash Lemma [14]). *Let $X \in \mathcal{X}$ be a random variable where $H_\infty(X) \geq \kappa$. Let $\mathcal{HS}$ be a family of pairwise independent hash functions with domain $\mathcal{X}$ and range $\{0,1\}^l$. Then for $\mathcal{H} \leftarrow_R \mathcal{HS}$ and $U_l \leftarrow_R \{0,1\}^l$,*

$$SD((\mathcal{H}, \mathcal{H}(X)), (\mathcal{H}, U_l)) \leq 2^{(l-\kappa)/2}.$$

Lemma 2 (A Generalization of the Leftover Hash Lemma [16]). *Let $(X, \tilde{X}) \in \mathcal{X} \times \mathcal{X}$ be two random variables having joint distribution where $H_\infty(X) \geq \kappa, H_\infty(\tilde{X}) \geq \kappa$ and $\Pr[X = \tilde{X}] = \delta$. Let $\mathcal{HS}$ be a family of 4-wise independent hash functions with domain $\mathcal{X}$ and range $\{0,1\}^l$. Then for $\mathcal{H} \leftarrow_R \mathcal{HS}$ and $U_{2l} \leftarrow_R \{0,1\}^{2l}$,*

$$SD((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), (\mathcal{H}, U_{2l})) \leq \sqrt{1+\delta} \cdot 2^{l-\kappa/2} + \delta.$$

From the above lemmata we can get the following lemma that will be used in our security proof. Lemma 3 states that for a 4-wise independent hash function $\mathcal{H}$ and two random variables $X, \tilde{X}$ with $\Pr[X = \tilde{X}] = \delta$ negligible that even related, the output $\mathcal{H}(\tilde{X})$ is close to uniformly random even $\mathcal{H}(X)$ is fixed as long as the min-entropy of X and $\tilde{X}$ are large enough.

Lemma 3. *Let $\delta \leq \frac{1}{2}, l \leq 6,$ $(X, \tilde{X}) \in \mathcal{X} \times \mathcal{X}$ be two random variables having joint distribution where $H_\infty(X) \geq \kappa, H_\infty(\tilde{X}) \geq \kappa$ and $\Pr[X = \tilde{X}] = \delta$. Let $\mathcal{HS}$ be a family of 4-wise independent hash functions with domain $\mathcal{X}$ and range $\{0,1\}^l$. Then for $\mathcal{H} \leftarrow_R \mathcal{HS}$ and $U_l \leftarrow_R \{0,1\}^l$,*

$$SD((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), (\mathcal{H}, \mathcal{H}(X), U_l)) \leq 2^{l-\frac{\kappa-1}{2}} + \delta.$$

Proof. Let Δ be the random variable $(\mathcal{H}, U_{2l})$, we can use the triangle inequality to get

$$\begin{aligned} &SD((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), (\mathcal{H}, \mathcal{H}(X), U_l)) \\ \leq\ &SD((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), \Delta) + SD(\Delta, (\mathcal{H}, \mathcal{H}(X), U_l), \end{aligned} \tag{1}$$

Since we know that $H_\infty(X) \geq \kappa, \quad H_\infty(\tilde{X}) \geq \kappa$ and $X \neq \tilde{X}$. By using Lemma 2 we can upper bound the first term of (1) as

$$SD((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), \Delta) \leq \sqrt{1+\delta} \cdot 2^{\frac{2l-\kappa}{2}} + \delta \leq \sqrt{\frac{3}{2}} \cdot 2^{\frac{2l-\kappa}{2}} + \delta.$$

Similarly by using Lemma 1 we can upper bound the second term of (1) as

$$SD(\Delta, (\mathcal{H}, \mathcal{H}(X), U_l) \leq 2^{\frac{l-\kappa}{2}} \leq \frac{1}{8} \cdot 2^{\frac{2l-\kappa}{2}}.$$

□

3 Complexity Assumptions

Decisional Diffie-Hellman Assumption (DDH). To formally define our assumption, we let $\mathcal{G}$ denote a group generation algorithm, which takes in a security parameter λ and outputs p and a group description G of order p.

Run $\mathcal{G}(1^\lambda)$ to get (p, G), and randomly choose $g_1, g_2 \in G, r \neq w \in \mathbb{Z}_p$. Set $T_0 = (g_1^r, g_2^r), T_1 = (g_1^r, g_2^w)$. The advantage of $\mathcal{A}$ is defined as

$$Adv_{\mathcal{A}}^{DDH} = \Big| \Pr[\mathcal{A}(g_1, g_2, T_1) = 1] - \Pr[\mathcal{A}(g_1, g_2, T_0) = 1] \Big|.$$

Definition 3 (DDH). *We say that $\mathcal{G}$ satisfies the DDH assumption if for all PPT algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{DDH}$ is negligible in λ.*

Higher Residuosity Assumption (HR). Next we give the HR assumption as that in [15]. There are also similar assumptions in literatures [12,17,18]. We let RSA_{gen} denote a RSA generation algorithm, which takes in a security parameter λ and outputs (P, Q, N, S) such that $N = PQ, S | \varphi(N)/4$, let G_S denote the unique subgroup of order S of $\mathbb{Z}_N^*$. Generally speaking, HR assumption means that it is difficult to distinguish a random element in G_S from a random element in J_N, where $J_N = \{x \in \mathbb{Z}_N^* | (\frac{x}{N}) = 1\}$.

To formulate this notion precisely, run $RSA_{gen}(1^\lambda)$ to get (P, Q, N, S), and randomly choose $g, u_0 \in G_S, \ u_1 \in J_N$. The advantage of $\mathcal{A}$ is defined as

$$Adv_{\mathcal{A}}^{HR} = \Big| \Pr[\mathcal{A}(g, u_1) = 1] - \Pr[\mathcal{A}(g, u_0) = 1] \Big|.$$

Definition 4 (HR). *We say that $\mathcal{G}$ satisfies the HR assumption if for all PPT algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{HR}$ is negligible in λ.*

For $\lambda = 80$ bits security one may choose $l(N) = 1024, l(S) = 256$. Then N may be chosen as follows: $P = 2P_S P_T + 1, Q = Q_S Q_T + 1, N = PQ, S = P_S Q_S$, where Q_S, Q_T, P_S, P_T are primes and $l(P_S), l(P_T) \approx 128$.

4 RKA Secure PKE Schemes

4.1 Construction Based on the DDH Assumption

In this section we describe a RKA secure PKE scheme based on the DDH assumption. The structure of our scheme inherits that in [16]. In the appendix we will show that the original PKE scheme in [16] is not RKA secure if Φ includes a function of the form $\phi_a^*(s) = as$. By applying a 4-wise independent hash function to more group elements, our scheme is Φ-RKA secure for Φ is a family of affine functions.

Run $\mathcal{G}(1^\lambda)$ to obtain (p, G), Let SE be an AE-OT secure symmetric encryption scheme with secret key space $\{0,1\}^l$. Let $\mathcal{HS}$ be a family of 4-wise independent hash functions with domain G^3 and image $\{0,1\}^l$. Public parameters are set as $pp = (p, G)$.

$Keygen(pp)$: The key generation algorithm chooses random $g_1, g_2 \in G$ and $\mathcal{H} \in \mathcal{HS}$. It picks random $x_1, x_2 \in \mathbb{Z}_p$ and computes $X = g_1^{x_1} g_2^{x_2}$. The public key is set as $pk = (g_1, g_2, X, \mathcal{H})$ and the secret key is set as $sk = (x_1, x_2)$.

$Enc(pk, m)$: The encryption algorithm chooses random $r \in \mathbb{Z}_p$ and computes the ciphertext $C = (C_1, C_2, C_3)$ as:

$$C_1 = g_1^r, C_2 = g_2^r, Y = X^r, K = \mathcal{H}(C_1, C_2, Y), C_3 = \mathcal{E}(K, m).$$

$Dec(C, sk)$: The decryption algorithm computes the message as:

$$Y = C_1^{x_1} C_2^{x_2}, K = \mathcal{H}(C_1, C_2, Y), m = \mathcal{D}(K, C_3).$$

Correctness can be easily verified for the correctness of the symmetric encryption scheme and $Y = C_1^{x_1} C_2^{x_2} = g_1^{rx_1} g_2^{rx_2} = X^r$. In terms of concrete security, it requires the image $\{0,1\}^l$ of $\mathcal{H}$ to be sufficiently small, i.e. $l \leq \frac{1}{4}\log_2 p$. Consequently for a symmetric cipher with $l = 80$ bits keys we should use groups of order $\log_2 p \geq 4l = 320$ bits.

Security Proof

Theorem 1. *If the DDH assumption holds, SE is an AE-OT secure symmetric encryption scheme with secret key space $\{0,1\}^l$, $\mathcal{HS}$ is a family of 4-wise independent hash functions with domain G^3 and image $\{0,1\}^l$, then our PKE scheme is Φ-CC-RKA secure for the class of affine functions Φ. In particular, for every advasary $\mathcal{A}$ on CC-RKA security of the above scheme, there exist adversaries $\mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{E}$ with*

$$Adv_{\mathcal{A}}^{CC-RKA} \leq Adv_{\mathcal{B}}^{DDH} + q(2^{l-(\kappa-1)} + Adv_{\mathcal{C}}^{DL} + Adv_{SE,\mathcal{D}}^{INT-OT}) + Adv_{SE,\mathcal{E}}^{IND-OT}$$

where $\kappa = log_2(|G|)$.

First let us introduce two lemmata that will be used in our proof.

Lemma 4. *[11] Let S_1, S_2, F be events defined on some probability space that the events $S_1 \wedge \neg F$ occurs iff $S_2 \wedge \neg F$ occurs, then*

$$|\Pr[S_1] - \Pr[S_2]| \leq \Pr[F].$$

Lemma 5. *[11] Let k, n be integers with $1 \leq k \leq n$, and let K be a finite field. Consider a probability space with random variables $\overrightarrow{\alpha} \in K^{n\times 1}$, $\overrightarrow{\beta} = (\beta_1, ..., \beta_k)^T \in K^{k\times 1}$, $\overrightarrow{\gamma} \in K^{k\times 1}$ and $M \in K^{k\times n}$ such that $\overrightarrow{\alpha}$ is uniformly distributed over $K^{n\times 1}$, $\overrightarrow{\beta} = M\overrightarrow{\alpha} + \overrightarrow{\gamma}$, and for $1 \leq i \leq k$, the i-th row of M and $\overrightarrow{\gamma}$ are determined by $\beta_1, ..., \beta_{i-1}$.*

Then conditioning on any fixed values of $\beta_1, ..., \beta_{k-1}$ such that the resulting matrix M has rank k, the value of β_k is uniformly distributed over K in the resulting conditional probability space.

Proof (of Theorem 1). Suppose that the public key is $(X, \mathcal{H})$ and the secret key is (x_1, x_2). The challenge ciphertext is denoted by $C^* = (C_1^*, C_2^*, C_3^*)$. We also denote by r^*, Y^*, K^* the values corresponding with r, Y, K related to C^*. We say that a ciphertext C is invalid if $C_1 = g_1^{r_1}, C_2 = g_2^{r_2}$ for some $r_1 \neq r_2$.

Let $\log(\cdot)$ denote $\log_{g_1}(\cdot)$ and $\omega = \log g_2$, then

$$logX = x_1 + \omega x_2 \tag{2}$$

To prove the security of our scheme, we define a sequence of games that any PPT adversary can not tell the difference between two adjacent games. Let q denote the number of decryption queries that the adversary makes during the whole game, here we denote an affine function as $\phi(sk) = (\phi_1(sk), \phi_2(sk)) = (a_1x_1 + b_1, a_2x_2 + b_2)$.

Game$_0$: the real security game.

Game$_1$: the same as *Game*$_0$ except that the challenge ciphertext is generated using the secret key. That is

$$Y^* = C_1^{*x_1} C_2^{*x_2}.$$

Game$_2$: the same as *Game*$_1$ except that the challenge ciphertext is invalid. That is (C_1^*, C_2^*) is replaced with a random pair $(g_1^{r_1^*}, g_2^{r_2^*})$ with $r_1^* \neq r_2^*$.

Game$_3$: the same as *Game*$_2$ except that the decryption oracle rejects all queries (ϕ, C) that satisfy $a_1r_1 \neq a_2r_2$, where $C_1 = g_1^{r_1}, C_2 = g_2^{r_2}$.

Game$_4$: the same as *Game*$_3$, except that SE encrypts m_b using a random key K^+ instead of K^*.

Let $Adv_{\mathcal{A}}^i$ denote $\mathcal{A}$'s advantage in *Game*$_i$ for $i = 0, 1, ..., 4$.

Clearly, $Adv_{\mathcal{A}}^0 = Adv_{\mathcal{A}}^1$.

Lemma 6. *Suppose that there exists a PPT adversary $\mathcal{A}$ such that $Adv_{\mathcal{A}}^1 - Adv_{\mathcal{A}}^2 = \epsilon$, then there exists a PPT adversary $\mathcal{B}$ with advantage ϵ in breaking the DDH assumption.*

Proof. $\mathcal{B}$ receives
$$D = (g_1, g_2, T := (u_1, u_2))$$
and its task is to decide whether D is a DDH tuple. $\mathcal{B}$ picks random $x_1, x_2 \in \mathbb{Z}_p$ and $\mathcal{H} \in \mathcal{HS}$. $\mathcal{B}$ computes $X = g_1^{x_1} g_2^{x_2}$ and sends $(pk = (g_1, g_2, X, \mathcal{H}))$ to $\mathcal{A}$.

Whenever $\mathcal{A}$ submits (ϕ, C), $\mathcal{B}$ simply runs the decryption oracle with the secret key $\phi(sk)$.

When $\mathcal{A}$ submits $(m_0, m_1), \mathcal{B}$ randomly chooses $b \leftarrow_R \{0,1\}$, it sets $C_1^* = u_1, C_2^* = u_2, Y^* = u_1^{x_1} u_2^{x_2}, K^* = \mathcal{H}(C_1^*, C_2^*, Y^*), C_3^* = \mathcal{E}(K^*, m_b)$ and responds with $C^* = (C_1^*, C_2^*, C_3^*)$.

When $\mathcal{A}$ outputs b', $\mathcal{B}$ outputs 1 if $b' = b$ and 0 otherwise.

Note that when D is a DDH tuple, then the above game perfectly simulates $Game_1$; when D is not a DDH tuple, the above game perfectly simulates $Game_2$. □

Lemma 7. *Suppose that there exists a PPT adversary $\mathcal{A}$ in $Game_2$ and $Game_3$ such that it can submit a query (C, ϕ) satisfying $(C_1, C_2) = (C_1^*, C_2^*)$, $\phi(sk) \neq sk, Y = Y^*$ with probability δ, then there exists a PPT adversary $\mathcal{B}$ with advantage δ in breaking the DL assumption.*

Proof. $\mathcal{B}$ receives
$$D = (g, h)$$
and its task is to compute $\gamma \in \mathbb{Z}_p$ such that $h = g^\gamma$. $\mathcal{B}$ chooses random $s, t \in \mathbb{Z}_p$ with the constraint $h \neq g^t$ and computes $g_1 = g^s, g_2 = g_1^t$, so (g_1, g_2, g, h) is not a DDH tuple. Then it picks $x_1, x_2 \in \mathbb{Z}_p$, $\mathcal{H} \in \mathcal{HS}$. $\mathcal{B}$ computes $X = g_1^{x_1} g_2^{x_2}$ and sends $(pk = (g_1, g_2, X, \mathcal{H}))$ to $\mathcal{A}$.

Whenever $\mathcal{A}$ submits $(\phi, C), \mathcal{B}$ simply runs the decryption oracle with the secret key $\phi(sk)$.

When $\mathcal{A}$ submits $(m_0, m_1), \mathcal{B}$ randomly chooses $b \leftarrow_R \{0,1\}, \gamma \in \mathbb{Z}_p$, it sets $C_1^* = g, C_2^* = h, Y^* = C_1^{*x_1} C_2^{*x_2}, K^* = \mathcal{H}(C_1^*, C_2^*, Y^*), C_3^* = \mathcal{E}(K^*, m_b)$ and responds with $C^* = (C_1^*, C_2^*, C_3^*)$.

Whenever $\mathcal{A}$ submits (ϕ, C) satisfying $(C_1, C_2) = (C_1^*, C_2^*), \phi(sk) \neq sk, Y = Y^*$, then we have $C_1^{x_1} C_2^{x_2} = C_1^{\phi_1(sk)} C_2^{\phi_2(sk)}$, and $h = g^\theta$, where $\theta = \frac{\phi_1(sk) - x_1}{x_2 - \phi_2(sk)}$, thus solve the DL problem. □

Lemma 8. *Assume that the symmetric key encryption scheme is AE-OT secure, $\mathcal{HS}$ is a family of 4-wise independent hash functions, the DDH assumption holds, then $Adv_{\mathcal{A}}^2 - Adv_{\mathcal{A}}^3$ is negligible.*

Proof.
$$\log Y^* = r_1^* x_1 + \omega r_2^* x_2 \qquad (3)$$

Let E be the event that a query (C, ϕ) is rejected in $Game_3$ but not rejected in $Game_2$. Then we have $|Adv_{\mathcal{A}}^2 - Adv_{\mathcal{A}}^3| \leq Pr[E]$.

Case 1: $(C_1, C_2) = (C_1^*, C_2^*)$.

- $\phi(sk) = sk$. We have

$$\begin{pmatrix} \log X \\ \log Y^* \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & \omega \\ r_1^* & \omega r_2^* \end{pmatrix}}_{=:M^*} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

  Since $\det(M^*) = \omega(r_1^* - r_2^*) \neq 0$, as stated by Lemma 5, the distribution of Y^* is randomly distributed in G, so $H_\infty(Y^*) \geq \kappa$. From the leftover hash lemma, we know that K^* is randomly distributed. From the INT-OT property of the SE scheme, we can see that it is difficult to generate a $C_3 \neq C_3^*$ s.t. $\mathcal{D}(K^*, C_3) \neq \perp$.
- $\phi(sk) \neq sk$. Let Γ^* be the random variable (C_1^*, C_2^*, Y^*), Γ be the random variable (C_1, C_2, Y). From Lemma 7 it can be seen that $\Pr[Y = Y^*] = \delta$, hence $\Pr[\Gamma = \Gamma^*] = \delta$, where δ is negligible assuming DL problem is hard to solve.

$$\begin{pmatrix} \log X \\ \log Y \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & \omega \\ a_1 r_1^* & \omega a_2 r_2^* \end{pmatrix}}_{:=M_1} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 0 \\ b_1 r_1^* + \omega b_2 r_2^* \end{pmatrix}$$

  As analyzed above we have $H_\infty(\Gamma) \geq \kappa$. From Lemma 3 we know:

$$SD((pk, \mathcal{H}, \mathcal{H}(\Gamma^*), \mathcal{H}(\Gamma)), (pk, \mathcal{H}, \mathcal{H}(\Gamma^*), U_l)) \leq 2^{l-(\kappa-1)/2} + \delta.$$

  Here U_l is uniformly random chosen from $\{0,1\}^l$. So the distribution of K looks random to the adversary $\mathcal{A}$, then from the INT-OT property of the SE scheme, with overwhelming probability $Dec(sk, C) = \perp$.

Case 2: $(C_1, C_2) \neq (C_1^*, C_2^*)$, and $a_1 r_1 \neq a_2 r_2$. In the following we let Γ^* be the random variable (C_1^*, C_2^*, Y^*), Γ be the random variable (C_1, C_2, Y), then $\Gamma \neq \Gamma^*$. Here we have

$$\begin{pmatrix} \log X \\ \log Y \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & \omega \\ a_1 r_1 & \omega a_2 r_2 \end{pmatrix}}_{:=M_2} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 0 \\ b_1 r_1 + \omega b_2 r_2 \end{pmatrix}$$

Since $\det(M_2) \neq 0$, we have $H_\infty(Y) \geq \kappa$. Similar as Case 1, we have $H_\infty(\Gamma^*) \geq \kappa$, $H_\infty(\Gamma) \geq \kappa$ and $\Gamma^* \neq \Gamma$. From Lemma 3 we know:

$$SD((pk, \mathcal{H}, \mathcal{H}(\Gamma^*), \mathcal{H}(\Gamma)), (pk, \mathcal{H}, \mathcal{H}(\Gamma^*), U_l)) \leq 2^{l-(\kappa-1)/2}.$$

Here U_l is uniformly random chosen from $\{0,1\}^l$. So the distribution of K looks random to the adversary $\mathcal{A}$, then from the INT-OT property of the SE scheme, with overwhelming probability $Dec(sk, C) = \perp$.

From the above analysis, we can see that it is difficult to distinguish $Game_2$ and $Game_3$ for any PPT adversary. □

Lemma 9. *Assume that $\mathcal{HS}$ is a family of 4-wise independent hash functions, then $Adv_{\mathcal{A}}^3 - Adv_{\mathcal{A}}^4$ is negligible.*

Proof. Since in both $Game_3$ and $Game_4$, all decryption queries are rejected except those $((C_1, C_2, C_3), \phi)$ satisfying $Y = C_1^{a_1x_1+b_1}C_2^{a_2x_2+b_2}$ with $a_1r_1 = a_2r_2$, so for any information-theoretical adversary $\mathcal{A}$, all it can get from the decryption queries is :

$$\log Y - \theta = arx_1 + \omega arx_2. \qquad (4)$$

Here $\theta = b_1r_1 + \omega b_2r_2$ and $ar = a_1r_1 = a_2r_2$. Since eq. (4) is a linearly correlation of eq. (1). Conditioned on the the decryption answers, the distribution of Y^* is still randomly distributed in G, then $Game_3$ and $Game_4$ are indistinguishable. □

Lemma 10. *Suppose that there exists a PPT adversary $\mathcal{A}$ such that $Adv_{\mathcal{A}}^4 = \epsilon$, then there exists a PPT adversary $\mathcal{B}$ with the same advantage in breaking the IND-OT of the SE scheme.*

Proof. $\mathcal{B}$ chooses random $x_1, x_2 \in \mathbb{Z}_p$ and $\mathcal{H} \in \mathcal{HS}$. $\mathcal{B}$ computes $X = g_1^{x_1}g_2^{x_2}$ and sends $(pp = (G, p, g_1, g_2), pk = (X, \mathcal{H}))$ to $\mathcal{A}$.

Whenever $\mathcal{A}$ submits $(\phi, C), \mathcal{B}$ simply runs the decryption oracle using the secret key $\phi(sk)$.

When $\mathcal{A}$ submits $(m_0, m_1), \mathcal{B}$ sends (m_0, m_1) to its challenger and receives C_3^*. Then $\mathcal{B}$ chooses random $r_1^* \neq r_2^*$ and sets $C_1^* = g_1^{r_1^*}, C_2^* = g_2^{r_2^*}$ and responds with $C^* = (C_1^*, C_2^*, C_3^*)$.

When $\mathcal{A}$ outputs b', $\mathcal{B}$ outputs b'. □

4.2 Construction Based on the HR Assumption

In this section we prove that the scheme proposed in [15] is Φ-CC-RKA secure for the class of affine functions Φ. This scheme is contained in several standard bodies, e.g., in IEEE P1363a, SECG and ISO 18033-2 as "Diffie-Hellman integrated encryption scheme" (DHIES) [2].

In the following we use $|u|$ to denote the absolute value of u, where u is represented as a signed integer in the set $\{-(N-1)/2, ..., (N-1)/2\}$. Let $QR_N^+ := \{|x| : x \in QR_N\}$ and $G_S^+ := \{|x| : x \in G_S\}$.

Let SE be an AE-OT secure symmetric encryption scheme with secret key space $\{0, 1\}^l$. Let $\mathcal{HS}$ be a family of 4-wise independent hash functions with domain $(QR_N^+)^2$ and range $\{0, 1\}^l$. In the following we let g^x denote $|g^x \bmod N|$.

Keygen(pp) : The key generation algorithm runs $RSA_{gen}(1^\lambda)$ to obtain (P, Q, N, S) and chooses random $g \in G_S^+$, it picks random $x \in [N/4]$ and $\mathcal{H} \in \mathcal{HS}$, it computes $X = g^x$. The public key is set as $pk = (N, g, X, \mathcal{H})$ and the secret key is set as $sk = x$.

Enc(pk, m) : The encryption algorithm chooses random $r \in [N/4]$ and computes the ciphertext $C = (C_1, C_2)$ as:

$$C_1 = g^r, Y = X^r, K = \mathcal{H}(C_1, Y), C_2 = \mathcal{E}(K, m).$$

$Dec(C, sk)$: The decryption algorithm first checks whether $C_1 \in QR_N^+$ and rejects if not. Then it computes the message as:

$$Y = C_1^x, K = \mathcal{H}(C_1, Y), m = \mathcal{D}(K, C_3).$$

Correctness can be easily verified from the correctness of the symmetric encryption scheme and $Y = C_1^x = g^{rx} = X^r$.

In the security proof we will use the following assumption HR$'$ directly.

Run $RSA_{gen}(1^\lambda)$ to get (P, Q, N, S), and randomly choose $g, u_0 \in G_S^+,\ u_1 \in QR_N^+$. The advantage of $\mathcal{A}$ is defined as

$$Adv_{\mathcal{A}}^{HR'} = \Big| \Pr[\mathcal{A}(g, u_1) = 1] - \Pr[\mathcal{A}(g, u_0) = 1] \Big|.$$

Definition 5 (HR$'$). *We say that $\mathcal{G}$ satisfies the HR$'$ assumption if for all PPT algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{HR'}$ is negligible in λ.*

Clearly, the HR$'$ assumption is implied by the HR assumption.

Theorem 2. *If the HR$'$ assumption holds, SE is an AE-OT secure symmetric encryption scheme with secret key space $\{0,1\}^l$, $\mathcal{HS}$ is a family of 4-wise independent hash functions with domain G^3 and image $\{0,1\}^l$, then our PKE scheme is Φ-CC-RKA secure for the class of affine functions Φ. In particular, for every advasary $\mathcal{A}$ on CC-RKA security of the above scheme, there exist adversaries $\mathcal{B}, \mathcal{C}, \mathcal{D}$ with*

$$Adv_{\mathcal{A}}^{CC-RKA} \leq (q+1) Adv_{\mathcal{B}}^{HR} + q(2^{l-(\kappa-1)} + Adv_{SE,\mathcal{C}}^{INT-OT}) + Adv_{SE,\mathcal{D}}^{IND-OT}.$$

where $\kappa = log_2(\lfloor N/4S \rfloor)$.

The proof methodology of Theorem 2 is similar to Theorem 1 and we put the concrete proof in Appendix B.

5 Conclusion

In this paper, we prove the security against related key attacks of two public key encryption schemes in the standard model. The first scheme is a variation of the KYPS09. While KYPS09 has been proved CCA secure under the DDH assumption, we show in the appendix that it is not secure against related key attacks when the key related function includes affine functions. We make a modification on KYPS09 and prove that the resulting scheme is Φ-CC-RKA secure for $\Phi = \Phi^{\text{affine}}$. We also prove the scheme in [15] is Φ-CC-RKA secure for $\Phi = \Phi^{\text{affine}}$ based on the HR assumption. The security relies heavily on a randomness extractor called 4-wise independent hash functions and we use game sequences in the proof. In the future we will study the CC-RKA security property for universal-1 hash proof systems.

Acknowledgments. We are very grateful to anonymous reviewers for their helpful comments. We also thank Yamin Liu for helpful discussions.

References

1. Abdalla, M., et al.: Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (2005)
2. Abdalla, M., Bellare, M., Rogaway, P.: The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 143–158. Springer, Heidelberg (2001)
3. Bellare, M., Cash, D.: Pseudorandom Functions and Permutations Provably Secure against Related-Key Attacks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 666–684. Springer, Heidelberg (2010)
4. Bellare, M., Cash, D., Miller, R.: Cryptography Secure against Related-Key Attacks and Tampering. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 486–503. Springer, Heidelberg (2011)
5. Bellare, M., Kohno, T.: A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer, Heidelberg (2003)
6. Bellare, M., Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 531–545. Springer, Heidelberg (2000)
7. Bellare, M., Paterson, K.G., Thomson, S.: RKA Security beyond the Linear Barrier: IBE, Encryption and Signatures. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 331–348. Springer, Heidelberg (2012)
8. Biham, E., Shamir, A.: Differential Fault Analysis of Secret Key Cryptosystems. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 513–525. Springer, Heidelberg (1997)
9. Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem (1999)
10. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the Importance of Checking Cryptographic Protocols for Faults. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 37–51. Springer, Heidelberg (1997)
11. Cramer, R., Shoup, V.: Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack. SIAM J. Compt. 33(1), 167–226 (2003)
12. Groth, J.: Cryptography in subgroups of z_n. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 50–65. Springer, Heidelberg (2005)
13. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest We Remember: Cold-boot Attacks on Encryption Keys. Commun. ACM 52(5), 91–98 (2009)
14. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A Pseudorandom Generator from any One-way Function. SIAM J. Comput 28(4), 1364–1396 (1999)
15. Hofheinz, D., Kiltz, E.: The Group of Signed Quadratic Residues and Applications. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 637–653. Springer, Heidelberg (2009)
16. Kiltz, E., Pietrzak, K., Stam, M., Yung, M.: A New Randomness Extraction Paradigm for Hybrid Encryption. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 590–609. Springer, Heidelberg (2009); also Cryptology ePrint Archive, 2008/304

17. Kurosawa, K., Katayama, Y., Ogata, W., Tsujii, S.: General Public Key Residue Cryptosystems and Mental Poker Protocols. In: Damgård, I.B. (ed.) EUROCRYPT 1990. LNCS, vol. 473, pp. 374–388. Springer, Heidelberg (1991)
18. Naccache, D., Stern, J.: A new Public Key Cryptosystem based on Higher Residues. In: CCS 1998, pp. 59–66 (1998)
19. Wee, H.: Public Key Encryption against Related Key Attacks. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 262–279. Springer, Heidelberg (2012)

Appendix A: A RKA attack on KPSY09

The PKE Scheme by KPSY09

The PKE scheme of [16] is given as follows:

$Keygen(1^\lambda)$: The key generation algorithm chooses random $x_1, x_2 \in \mathbb{Z}_p$ and $\mathcal{H} \in \mathcal{HS}$, it computes $X = g_1^{x_1} g_2^{x_2}$. The public key is set as $pk = (X, \mathcal{H})$ and the secret key is set as $sk = (x_1, x_2)$

$Enc(pk, m)$: The encryption algorithm chooses random $r \in \mathbb{Z}_p$ and computes the ciphertext $C = (C_1, C_2, C_3)$ as:

$$C_1 = g_1^r, C_2 = g_2^r, Y = X^r, K = \mathcal{H}(Y), C_3 = \mathcal{E}(K, m).$$

$Dec(C, sk)$: The decryption algorithm computes the message as:

$$Y = C_1^{x_1} C_2^{x_2}, K = \mathcal{H}(Y), m = \mathcal{D}(K, C_3).$$

The above scheme is not RKA secure if Φ includes a function $\phi^*_{a_1,a_2}(x_1, x_2) = (a_1 x_1, a_2 x_2)$. Once the adversary sees the challenge ciphertext C_1^*, C_2^*, C_3^*, it can create a query as $(C = ({C_1^*}^{\frac{1}{a_1}}, {C_2^*}^{\frac{1}{a_2}}, C_3^*), \phi^*)$, and it can get the decryption of the challenge ciphertext since $Y^* = {C_1^*}^{x_1} {C_2^*}^{x_2}$.

Appendix B: Proof of Theorem 2

Proof. Suppose that the public key is $(N, g, X, \mathcal{H})$ and the secret key is x. The challenge ciphertext is denoted by $C^* = (C_1^*, C_2^*)$. We also denote by r^*, Y^*, K^* the values corresponding with r, Y, K related to C^*. We say that a ciphertext C is invalid if $C_1 \in QR_N^+ \backslash G_S^+$. Let $\log(\cdot)$ denote $\log_g(\cdot)$. Then we have

$$x = logX + t \cdot S, \text{ where } t \in \{0, 1, ..., \lfloor N/4S \rfloor\} \tag{5}$$

To prove the security of our scheme, we define a sequence of games that any PPT adversary can not tell the difference between two adjacent games. Let q denote the number of decryption queries that the adversary makes during the whole game, here we write an affine function as $\phi(sk) = ax + b,\ a, b \in [N/4]$.

$Game_0$**:** the real security game.

$Game_1$**:** the same as $Game_0$ except that the challenge ciphertext is generated using the secret key. That is

$$Y^* = {C_1^*}^x.$$

$Game_2$**:** the same as $Game_1$ except that the challenge ciphertext is invalid. That is $C_1^* \in QR_N^+ \backslash G_S^+$.

$Game_3$**:** the same as $Game_2$ except that the decryption oracle rejects all invalid queries.

$Game_4$**:** the same as $Game_3$, except that SE encrypts m_b using a random key K^+ instead of K^*.

Let $Adv_{\mathcal{A}}^i$ denote $\mathcal{A}$'s advantage in $Game_i$ for $i = 0, 1, ..., 4$.

Clearly, $Adv_{\mathcal{A}}^0 = Adv_{\mathcal{A}}^1$.

Lemma 11. *Suppose that there exists a PPT adversary $\mathcal{A}$ such that $Adv_{\mathcal{A}}^1 - Adv_{\mathcal{A}}^2 = \epsilon$, then there exists a PPT adversary $\mathcal{B}$ with advantage ϵ in breaking the HR' assumption.*

Proof. $\mathcal{B}$ receives

$$D = (g, T)$$

and its task is to decide whether $T \in G_S^+$. $\mathcal{B}$ picks random $x \in [N/4]$ and $\mathcal{H} \in \mathcal{HS}$. $\mathcal{B}$ computes $X = g^x$ and sends $pk = (N, g, X, \mathcal{H}))$ to $\mathcal{A}$.

Whenever $\mathcal{A}$ submits (ϕ, C), $\mathcal{B}$ simply runs the decryption oracle with the secret key $\phi(sk)$.

When $\mathcal{A}$ submits $(m_0, m_1), \mathcal{B}$ randomly chooses $b \leftarrow_R \{0, 1\}$, it sets $C_1^* = T, Y^* = T^x, K^* = \mathcal{H}(C_1^*, Y^*), C_2^* = \mathcal{E}(K^*, m_b)$ and responds with $C^* = (C_1^*, C_2^*)$.

When $\mathcal{A}$ outputs b', $\mathcal{B}$ outputs 1 if $b' = b$ and 0 otherwise.

Note that when $T \in G_S^+$, then the above game perfectly simulates $Game_1$; when $T \notin G_S^+$, the above game perfectly simulates $Game_2$. □

Lemma 12. *Suppose that there exists a PPT adversary $\mathcal{A}$ in $Game_2$ and $Game_3$ such that it can submit a query (C, ϕ) satisfying $C_1 = C_1^*, \phi(sk) \neq sk, Y = Y^*$ with probability δ, then there exists a PPT adversary $\mathcal{B}$ with advantage δ in breaking the HR' assumption.*

Proof. $\mathcal{B}$ receives

$$D = (g, u)$$

and its task is to decide whether $u \in G_S^+$. Then $\mathcal{B}$ picks random $x \in [N/4]$, $\mathcal{H} \in \mathcal{HS}$. $\mathcal{B}$ computes $X = g^x$ and sends $pk = (N, g, X, \mathcal{H})$ to $\mathcal{A}$.

Whenever $\mathcal{A}$ submits $(\phi, C), \mathcal{B}$ simply runs the decryption oracle with the secret key $\phi(sk)$.

When $\mathcal{A}$ submits $(m_0, m_1), \mathcal{B}$ randomly chooses $b \leftarrow_R \{0, 1\}, t \in QR_N^+$, then with overwhelming probability we have $ut \notin G_S^+$. It sets $C_1^* = ut, Y^* = {C_1^*}^x, K^* = \mathcal{H}(C_1^*, Y^*), C_2^* = \mathcal{E}(K^*, m_b)$ and responds with $C^* = (C_1^*, C_2^*)$.

Whenever $\mathcal{A}$ submits (ϕ, C) satisfying $C_1 = C_1^*, \phi(sk) \neq sk, Y = Y^*$, then we have $C_1 = C_1^{*\frac{\phi(x)}{x}}$. Since $C_1^* \in QR_N^+ \backslash G_S^+$, with overwhelming probability we have $\frac{\varphi(N)}{4} | ord(C_1^*)$, so $\frac{4\phi(x)}{x}$ is a multiple of $\varphi(N)$, then we can solve the factoring problem according to the method in [[9],Fact 1.]. □

Lemma 13. *Assume that the symmetric encryption scheme is AE-OT secure, $\mathcal{HS}$ is a family of 4-wise independent hash functions, the HR′ assumption holds, then $Adv_{\mathcal{A}}^2 - Adv_{\mathcal{A}}^3$ is negligible.*

Proof. Let F be the event that a query (C, ϕ) is rejected in $Game_3$ but not rejected in $Game_2$. Then we have $|Adv_{\mathcal{A}}^2 - Adv_{\mathcal{A}}^3| \leq \Pr[F]$. We consider the following cases:

Case 1: $C_1 = C_1^*$.

- $\phi(sk) = sk$. From eq. (5) we can see that t is information-theoretically hidden for any PPT adversary $\mathcal{A}$, so $H_\infty(Y^*) \geq \kappa$. As stated by the left-over hash lemma, K^* is randomly distributed. As a result, it is difficult to generate a $C_2 \neq C_2^*$ s.t. $\mathcal{D}(K^*, C_2) \neq \perp$ according to the INT-OT property of the SE scheme.
- $\phi(sk) \neq sk$. Let Γ^* be the random variable (C_1^*, Y^*), Γ be the random variable (C_1, Y). According to Lemma 12 we know that $\delta = \Pr[\Gamma = \Gamma^*] = \Pr[Y = Y^*]$ is negligible. From the choice of sk we know that $H_\infty(Y) \geq \kappa$, so $H_\infty(\Gamma^*) \geq \kappa,\ H_\infty(\Gamma) \geq \kappa$. From Lemma 3 we know:

$$SD((pk, \mathcal{H}, \mathcal{H}(\Gamma^*), \mathcal{H}(\Gamma)), (pk, \mathcal{H}, \mathcal{H}(\Gamma^*), U_l)) \leq 2^{l-(\kappa-1)/2} + \delta.$$

Here U_l is uniformly random chosen from $\{0,1\}^l$. So the distribution of K looks random to the adversary $\mathcal{A}$, then from the INT-OT property of the SE scheme, with overwhelming probability $Dec(sk, C) = \perp$.

Case 2: $C_1 \neq C_1^*$, and $C_1 \notin G_S^+$. Let Γ^* be the random variable (C_1^*, Y^*), Γ be the random variable (C_1, Y), then we have $\Gamma^* \neq \Gamma$. From the distribution of sk, we have $H_\infty(\Gamma^*) \geq \kappa,\ H_\infty(\Gamma) \geq \kappa$. Then according to Lemma 3 we have:

$$SD((pk, \mathcal{H}, \mathcal{H}(\Gamma^*), \mathcal{H}(\Gamma)), (pk, \mathcal{H}, \mathcal{H}(\Gamma^*), U_l)) \leq 2^{l-(\kappa-1)/2}.$$

Therefore, the distribution of K looks random to the adversary $\mathcal{A}$, then from the INT-OT property of the SE scheme, with overwhelming probability $Dec(sk, C) = \perp$.

From the above analysis, we can see that it is difficult to distinguish $Game_2$ and $Game_3$ for any PPT adversary. □

Lemma 14. *Assume that $\mathcal{HS}$ is a family of 4-wise independent hash functions, then $Adv_{\mathcal{A}}^3 - Adv_{\mathcal{A}}^4$ is negligible.*

Proof. Since in both $Game_3$ and $Game_4$, all queries (C, ϕ) that are not rejected satisfy $C_1 \in G_S^+$, so for any information-theoretical adversary $\mathcal{A}$, all it can get from the decryption queries is :

$$\begin{aligned}\log Y &= arx + b \bmod S \\ &= ar \log X + b \bmod S\end{aligned}$$

As a result, t is information-theoretically hidden, $H_\infty(Y^*) \geq \kappa$, then according to the leftover hash lemma we can see that K^* is randomly distributed, $Game_3$ and $Game_4$ are indistinguishable.

Lemma 15. *Suppose that there exists a PPT adversary $\mathcal{A}$ such that $Adv_{\mathcal{A}}^4 = \epsilon$, then there exists a PPT adversary $\mathcal{B}$ with the same advantage in breaking the IND-OT property of the SE scheme.*

Proof. $\mathcal{B}$ runs $RSA_{gen}(1^\lambda)$ to obtain (P, Q, N, S) and choose random $g \in G_S^+$. $\mathcal{B}$ computes $X = g^x$ and sends $pk = (N, g, X, \mathcal{H})$ to $\mathcal{A}$.

Whenever $\mathcal{A}$ submits $(\phi, C), \mathcal{B}$ simply runs the decryption oracle with the secret key $\phi(sk)$.

When $\mathcal{A}$ submits $(m_0, m_1), \mathcal{B}$ sends (m_0, m_1) to its challenger and receives C_2^*. Then $\mathcal{B}$ chooses random $C_1^* \in QR_N^+ \backslash G_S^+$ and responds with $C^* = (C_1^*, C_2^*)$.

When $\mathcal{A}$ outputs b', $\mathcal{B}$ outputs b'. □