Related-Key Security for Hybrid Encryption*

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

[1] Data Assurance and Communication Security Research Center,
Chinese Academy of Sciences, Beijing, China
[2] State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, 100093, China
{xhlu,lb,ddj}@is.ac.cn

Abstract. We prove that, for a KEM/Tag-DEM (Key Encapsulation Mechanism/ Tag Data Encapsulation Mechanism) hybrid encryption scheme, if the adaptive chosen ciphertext secure KEM part has the properties of key malleability and key fingerprint and the Tag-DEM part is a one-time secure tag authenticated encryption, then the hybrid encryption is seucure against related key attacks (RKA). We show that several classical KEM schemes satisfy these two properties.

Keywords: public key encryption, related-key attack, hybrid encryption.

1 Introduction

The traditional model for the security of public key encryption schemes assumes that cryptographic devices are black-boxes and the private keys are completely hidden and protected from the attackers. For example, in the definition of adaptive chosen ciphertext attacks (IND-CCA2), the adversary can only communicate with the challenger through the encryption oracle and the decryption oracle, and can not get any internal information of the cryptographic devices. However, real attacks demonstrate that the adversary may get or modify the private key by using physical side-channels [26,7,9,18].

Related-key attacks (RKAs) were first proposed in [25,6] as a cryptanalysis tool for block ciphers. Real attacks [7,9], in which the attacker can modify the keys stored in the memory, turned this theoretical analysis model for block ciphers to a practical attack model for all kinds of cryptographic primitives such as public key encryption (PKE), identity based encryption (IBE), digital signature and so on. The theoretical definition of RKA security was first proposed by Bellare and Kohno [4], who treated the case of PRFs (PseudoRandom Functions) and PRPs (PseudoRandom Permutations). Research then expanded to other primitives [1,3,16,17].

* Supported by the National Basic Research Program of China (973 project, No.2013CB338002), the National Nature Science Foundation of China (No.61070171, No.61272534).

S.S.M. Chow et al. (Eds.): ISC 2014, LNCS 8783, pp. 19–32, 2014.

The RKA security of public key encryption schemes was first considered by Bellare, Cash and Miller [3]. They showed how to leverage the RKA security of block ciphers to provide RKA security for high-level primitives including SE (symmetric encryption), PKE, IBE and digital signature. They also showed that IBE is an enabling primitive in the RKA domain: achieving RKA secure IBE schemes yields RKA secure CCA-PKE (chosen ciphertext secure PKE) and digital signature schemes. Their main idea is to protect the secret key of a high level primitive with a RKA secure PRG (PseudoRandom Generator) which can be constructed from a RKA secure PRF. Since affine functions and polynomial functions contain constant functions, RKA secure PRFs for these functions can not exist. That is, the framework of [3] can only get RKA security for linear functions. To overcome the linear barrier, Bellare et al. [5] proposed a framework enabling the constructions of RKA secure IBE schemes for affine functions and polynomial functions of bounded degree. To go beyond the algebraic barrier and achieve RKA security for arbitrary key relations, Damgård et al. [15] proposed the bounded tamper resilience model, in which the number of tampering queries the adversary is allowed to ask for is restricted.

Wee [31] firstly proposed direct constructions of RKA secure public key encryption schemes. Wee showed that the Cramer-Shoup CCA secure constructions [12,13] do not satisfy the property of finger-printing. To achieve this property, Wee turned to the "all-but-one extraction" paradigm [8]. Dingding Jia et al. [22] showed that the Cramer-Shoup paradigm satisfy a similar property as finger-printing and proposed two RKA secure public key encryption schemes based on the Cramer-Shoup paradigm.

1.1 Our Contribution

We focus on how to uniformly enhance an IND-CCA2 secure PKE schemes to CC-RKA (adaptive chosen ciphertext related key attack) security. Specifically, for the KEM/Tag-DEM framework [11], we prove that CC-RKA secure hybrid encryption schemes can be constructed from an IND-CCA2 or IND-CCCA [19](Constrained Chosen Ciphertext Attacks) secure KEM and a one-time secure tag authenticated encryption. In addition, we require that the KEM scheme has the properties of key-malleable and key-fingerprint. We show that several classical IND-CCA2 or IND-CCCA secure KEM schemes satisfy these two properties. Thus we get efficient RKA secure hybrid encryption schemes.

In the construction of RKA secure schemes, key malleability is a useful and widely used property [2,3,5] (also name as "key homomorphism" in [31]). Key malleability means that the decryption of a ciphertext C using a secret key $\phi(sk)$, where ϕ denotes a function, equals the decryption of some other ciphertext C' using the original secret key sk. If the adversary can not find a (ϕ, C) pair such that C' equals the challenge ciphertext C^*, then the key malleability property reduces the CC-RKA security to the IND-CCA2 security. To prevent the adversary from getting such pairs, Wee [31] combined a tag-based CCA secure scheme with a one-time signature scheme, where the tag is derived from the verification key of the one-time signature scheme. In addition, Wee required that C and C'

share the same tag. If C and C' are valid ciphertexts and share the same tag, then the one-time signature scheme tells us that $C = C'$. To achieve CC-RKA security, Wee required that C^* is an invalid ciphertext under any $\phi(sk) \neq sk$. As a result, the adversary can not find a (ϕ, C) pair such that $C = C' = C^*$ is a valid ciphertext under $\phi(sk)$. This property is another useful property named as "key fingerprint" in [2] and "finger-printing" in [31].

Instead of adding a one-time signature scheme to a tag-based CCA secure PKE scheme as in[31], we show that the AE-OT (one-time secure authenticated encryption) secure DEM part in the hybrid scheme itself is a good choice to prevent the adversary from finding a valid (ϕ, C) pair such that $C' = C^*$, here C, C', C^* denote the ciphertext of the KEM part. That is, the AE-OT secure DEM part can provide an integrity authentication service for the KEM part. When $C \neq C' = C^*$, the AE-OT property guarantees that the adversary can not construct a valid DEM part. More formally, we prove that the KEM/Tag-DEM hybrid encryption is CC-RKA secure if the IND-CCA2 (or IND-CCCA) secure KEM part has the properties of key malleability and key fingerprint and the Tag-DEM part is a one-time secure tag authenticated encryption.

Compared with Wee's construction [31], our construction can get CC-RKA secure public key encryption schemes from the "all-but-one extraction" paradigm and the Cramer-Shoup paradigm uniformly, while Wee's construction can only get CC-RKA secure public key encryption schemes from the "all-but-one extraction" paradigm.

1.2 Outline

In section 2 we review the definition of related key attacks, key encapsulation mechanism and data encapsulation mechanism with tag. In section 3 we propose our new construction. In section 4 we show that several classical IND-CCA2 secure KEM schemes satisfy key malleability and key fingerprint. Finally we give the conclusion in section 5.

2 Definitions

If S is a finite set, $s \xleftarrow{R} S$ denotes that s is sampled from the uniform distribution on S. If A is a probabilistic algorithm and x an input, then $A(x)$ denotes the output distribution of A on input x. Thus, we write $y \leftarrow A(x)$ to denote of running algorithm A on input x and assigning the output to the variable y.

2.1 Related Key Attacks

We follow the definition of related key attacks from [31]. A public key encryption scheme is secure against adaptive chosen ciphertext related key attacks (CC-RKA) if the advantage of any adversary in the following game is negligible in the security parameter k.

1. The challenger runs the key generation algorithm $(PK, SK) \leftarrow \text{KeyGen}(1^k)$ and sends the public key PK to the adversary.
2. The adversary makes a sequence of calls to the related key decryption oracle RKA.Dec$(\cdot,\cdot)$ with (ϕ, C). Here $\phi \in \Phi$, Φ is a class of related-key deriving functions, C is a ciphertext. The challenger decrypts the ciphertext C using $\phi(SK)$ and sends the result to the adversary.
3. The adversary queries the encryption oracle with (m_0, m_1). The challenger computes:
$$b \xleftarrow{R} \{0,1\}, C^* \leftarrow Enc_{PK}(m_b)$$
and responds with C^*.
4. The adversary queries the related key decryption oracle continuously with (ϕ, C). The challenger acts just as in step 2. The only restriction is that the adversary can not query the related key decryption oracle with (ϕ, C) that $\phi(sk) = sk$ and $C = C^*$.
5. Finally, the adversary outputs a guess b'.

The adversary's advantage in the above game is defined as $\text{Adv}^{\text{rka}}_{\mathcal{A},\Phi}(k) = |\Pr[b' = b] - 1/2|$. An encryption scheme is Φ-CC-RKA secure if for all PPT adversary the advantage $\text{Adv}^{\text{rka}}_{\mathcal{A},\Phi}(k)$ is a negligible function of k.

2.2 Key Encapsulation Mechanism

A key encapsulation mechanism consists of the following algorithms:

- KEM.KG(1^k): A probabilistic polynomial-time key generation algorithm takes as input a security parameter (1^k) and outputs a public key PK and a private key SK. We write $(PK, SK) \leftarrow \text{KEM.KG}(1^k)$
- KEM.E(PK): A probabilistic polynomial-time encapsulation algorithm takes as input the public key PK, and outputs a pair (K, ψ), where $K \in K_D$(K_D is the key space) is a key and ψ is a ciphertext. We write $(K, \psi) \leftarrow \text{KEM.E}(PK)$
- KEM.D(SK, ψ): A decapsulation algorithm takes as input a ciphertext ψ and the private key SK. It returns a key K. We write $K \leftarrow \text{KEM.D}(SK, \psi)$.

A KEM scheme is secure against adaptive chosen ciphertext attacks if the advantage of any adversary $\mathcal{A}$ in the following game is negligible in the security parameter k.

1. The adversary queries a key generation oracle. The key generation oracle computes $(PK, SK) \leftarrow \text{KEM.KG}(1^k)$ and responds with PK.
2. The adversary makes a sequence of calls to the decapsulation oracle. For each query the adversary submits a ciphertext ψ, and the decapsulation oracle responds with KEM.D(SK, ψ).
3. The adversary queries an encapsulation oracle. The encapsulation oracle computes:
$$b \xleftarrow{R} \{0,1\}, (K_1, \psi^*) \leftarrow \text{KEM.E}(PK), K_0 \xleftarrow{R} K_D,$$
and responds with (K_b, ψ^*).

4. The adversary makes a sequence of calls to the decapsulation oracle. For each query the adversary submits a ciphertext ψ, and the decapsulation oracle responds with KEM.D(SK, ψ). The only restriction is that the adversary can not request the decapsulation of ψ^*.
5. Finally, the adversary outputs a guess b'.

Let $\Pr[\mathcal{A}_{suc}]$ be the probability that the adversary $\mathcal{A}$ succeeds in the game above. The adversary's advantage in the above game is

$$\mathrm{Adv}^{\mathrm{cca}}_{\mathcal{A}}(k) = |\Pr[\mathcal{A}_{suc}] - 1/2| = |\Pr[b' = b] - 1/2|.$$

If a KEM is secure against adaptive chosen ciphertext attacks defined in the above game, we say it is IND-CCA2 secure.

Hofheinz and Kiltz [19] proposed a relaxed notion of IND-CCA2 named as "constrained chosen ciphertext security" (IND-CCCA). In the definition of IND-CCCA the adversary is allowed to make a decapsulation query if it already has some priori knowledge of the decapsulated key K. That is, the adversary need to provide an efficiently computable boolean predicate $pred : K \to \{0, 1\}$. To construct a predicate $pred(K)$ that evaluates to 1, the adversary has to have a high priori knowledge about the decapsulated session key K. The formal definition of IND-CCCA is similar to that of IND-CCA2, while the only difference is that the adversary provides a $(\psi, pred)$ pair in the decapsulation query, and the challenger verifies whether $pred(K) = 1$ or not. If $pred(K) = 1$ then K is returned, and $\perp$ otherwise. The adversary's advantage is defined as

$$\mathrm{Adv}^{\mathrm{ccca}}_{\mathcal{A}}(k) = |\Pr[\mathcal{A}_{suc}] - 1/2| = |\Pr[b' = b] - 1/2|.$$

Φ-Key malleability.We say that a KEM has the property of Φ-key malleability if there is a PPT algorithm T such that for all $\phi \in \Phi$, PK, SK and ψ:

$$\mathrm{KEM.D}(\phi(SK), \psi) = \mathrm{KEM.D}(SK, T(PK, \phi, \psi)).$$

Φ-Key fingerprint. For all PK, SK and ψ, we say that a KEM has the property of Φ-key fingerprint if for any PPT adversary the probability to find a function $\phi \in \Phi$ such that $\phi(SK) \neq SK$ and $T(PK, \phi, \psi) = \psi$ is a negligible value ϵ_{kf}.

2.3 Data Encapsulation Mechanism with Tag

A data encapsulation mechanism with tag consists of two algorithms:

- Tag-DEM.E(K, m, t): The encryption algorithm takes as inputs a key K, a message m, a tag t and outputs a ciphertext χ. We write $\chi \leftarrow$ Tag-DEM.E (K, m, t)
- Tag-DEM.D$(K, \chi$,t): The decryption algorithm takes as inputs a key K, a ciphertext χ, a tag t and outputs a message m or the rejection symbol $\perp$. We write $m \leftarrow$ Tag-DEM.D(K, χ, t)

We require that for all $K \in \{0,1\}^{l_e}$ (l_e denotes the length of K), $m \in \{0,1\}^*$ and $t \in \{0,1\}^*$,we have:

$$\text{Tag-DEM.D}(K, \text{Tag-DEM.E}(K, m, t), t) = m.$$

A Tag-DEM scheme is IND-OT (indistinguishability against one-time attacks) secure if the advantage of any PPT adversary $\mathcal{A}$ in the following game is negligible in the security parameter k:

1. The challenger randomly generates an appropriately sized key K and a tag t^*.
2. The adversary $\mathcal{A}$ queries the encryption oracle with two messages m_0 and m_1) such that $|m_0| = |m_1|$. The challenger computes

$$b \overset{R}{\leftarrow} \{0,1\}, \chi^* \leftarrow \text{Tag-DEM.E}(K, m_b, t^*)$$

   and responds with χ^* and t^*.
3. Finally, $\mathcal{A}$ outputs a guess b' .

The advantage of $\mathcal{A}$ is defined as $\text{Adv}_{\mathcal{A}}^{\text{ind-ot}}(k) = |\Pr[b = b'] - 1/2|$. We say that the Tag-DEM is one-time secure in the sense of indistinguishability if $\text{Adv}_{\mathcal{A}}^{\text{ind-ot}}(k)$ is negligible.

A Tag-DEM scheme is INT-OT (one-time secure in the sense of ciphertext integrity) secure if the advantage of any PPT adversary $\mathcal{A}$ in the following game is negligible in the security parameter k:

1. The challenger randomly generates an appropriately sized key K and a tag t^*.
2. The adversary $\mathcal{A}$ queries the encryption oracle with a message m. The challenger computes

$$\chi^* \leftarrow \text{Tag-DEM.E}(K, m, t^*)$$

   and responds with χ^* and t^*.
3. Finally, the adversary $\mathcal{A}$ outputs a ciphertext χ and a tag t such that $\text{Tag-DEM.D}(K, \chi, t) \neq \perp$.

The advantage of $\mathcal{A}$ is defined as

$$\text{Adv}_{\mathcal{A}}^{\text{int-ot}}(k) = \Pr[(\chi, t) \neq (\chi^*, t^*)].$$

We say that the Tag-DEM is one-time secure in the sense of ciphertext integrity if $\text{Adv}_{\mathcal{A}}^{\text{int-ot}}(k)$ is negligible.

A Tag-DEM is one-time secure in the sense of tag authenticated encryption (Tag-AE-OT) iff it is IND-OT secure and INT-OT secure. Similar to AE-OT secure ciphers in [24], Tag-AE-OT secure ciphers can also be constructed from a SE (symmetric encryption) scheme and a MAC (message authentication code) scheme. The only difference is that the MAC scheme takes the ciphertext of the SE scheme and the tag t as inputs.

3 Hybrid Encryption Against Related Key Attacks

In this section we prove that the KEM/Tag-DEM hybrid encryption [11] is Φ-CC-RKA secure if the IND-CCA2 (or IND-CCCA) secure KEM part has the properties of Φ-key malleability and Φ-key fingerprint and the Tag-DEM part is a one-time secure tag authenticated encryption. The KEM/Tag-DEM framework for hybrid encryption can be described as follows.

- KeyGen(1^k): The key generation algorithm is the same as that of the KEM scheme.
$$(PK, SK) \leftarrow \text{KEM.KG}(1^k)$$
- Encrypt(PK, m): The encryption algorithm works as follows:
$$(K, \psi) \leftarrow \text{KEM.E}(PK), \chi \leftarrow \text{Tag-DEM.E}(K, m, \psi), C \leftarrow (\psi, \chi)$$
- Decrypt(SK, C): The decryption algorithm works as follows:
$$K \leftarrow \text{KEM.D}(SK, \psi), m \leftarrow \text{Tag-DEM.D}(K, \chi, \psi)$$

Before formal proof, we give a direct understanding of the CC-RKA security of the KEM/Tag-DEM hybrid encryption scheme. Intuitively, for an IND-CCA2 secure public key encryption scheme, if the private key is completely protected, the ciphertext is non-malleable. That is, the adversary can not construct a ciphertext based a valid ciphertext C^*. However, in the CC-RKA model, the ciphertext may be malleable since the adversary can modify the private key. In the KEM/Tag-DEM framework the Tag-DEM part provides the integrity authentication service to the KEM part. The INT-OT security of the Tag-DEM scheme guarantees that the adversary can not extend an existing ciphertext to get a new valid ciphertext.

First we prove the CC-RKA security of the hybrid encryption scheme when the KEM part is IND-CCA2 secure.

Theorem 1. *If the KEM part is IND-CCA2 secure and has the properties of Φ-key malleability and Φ-key fingerprint, the Tag-DEM part is Tag-AE-OT secure, then the hybrid encryption above is Φ-CC-RKA secure.*

Proof. Suppose that an adversary $\mathcal{A}$ can break the Φ-CC-RKA security of the hybrid encryption. To prove the theorem, we construct an adversary $\mathcal{B}$ to break the IND-CCA2 security of the KEM scheme. The construction of $\mathcal{B}$ is described as follows.

Setup: The adversary $\mathcal{B}$ gets the public key PK from the challenger and sends it to the adversary $\mathcal{A}$.

Decryption oracle1: When $\mathcal{A}$ queries the related key decryption oracle with (ϕ, C), where $C = (\psi, \chi), \phi \in \Phi$, the adversary $\mathcal{B}$ computes m as follows and returns it to $\mathcal{A}$.

$$\psi' \leftarrow T(PK, \phi, \psi), K \leftarrow \text{D}_{kem}(\psi'), m \leftarrow \text{Tag-DEM.D}(K, \chi, \psi).$$

Here $\mathrm{D}_{kem}(\cdot)$ denotes the decapsulation oracle of the KEM scheme, T is the transform function according to the Φ-key malleability property. According to the Φ-key malleability property, we have

$$K = \mathrm{D}_{kem}(\psi') = \mathrm{KEM.D}(SK, \psi') = \mathrm{KEM.D}(\phi(SK), \psi).$$

Thus the adversary $\mathcal{B}$ simulates the related key decryption oracle perfectly in this step.

Challenge: The adversary $\mathcal{A}$ queries the encryption oracle with two messages m_0 and m_1. The adversary $\mathcal{B}$ computes as follows.

$$(K^*, \psi^*) \leftarrow \mathrm{E}_{kem}(PK), b \xleftarrow{R} \{0,1\},$$
$$\chi^* \leftarrow \text{Tag-DEM.E}(K^*, m_b, \psi^*), C^* \leftarrow (\psi^*, \chi^*).$$

Here $\mathrm{E}_{kem}(PK)$ is the encryption oracle of the KEM scheme, K^* is randomly chosen from the key space or equals to $\mathrm{KEM.D}(SK, \psi^*)$. The adversary $\mathcal{B}$ sends C^* the $\mathcal{A}$.

Decryption oracle2: When $\mathcal{A}$ queries the decryption oracle with (ϕ, C) continuously, $\mathcal{B}$ computes $\psi' \leftarrow T(PK, \phi, \psi)$ and acts as follows.

- Case 1: $\psi' \neq \psi^*$. The adversary $\mathcal{B}$ computes m as follows and returns it to $\mathcal{A}$.
$$K \leftarrow \mathrm{D}_{kem}(\psi'), m \leftarrow \text{Tag-DEM.D}(K, \chi, \psi).$$
- Case 2: $\psi \neq \psi' = \psi^*$. The adversary $\mathcal{B}$ returns a rejection symbol $\perp$. According to the INT-OT security of Tag-DEM, $\text{Tag-DEM.D}(K^*, \chi, \psi) = \perp$ except with the probability of $\mathrm{Adv}^{\text{int-ot}}_{\mathcal{A}}$.
- Case 3: $\psi = \psi' = \psi^*$ and $\chi = \chi^*$. The adversary $\mathcal{B}$ returns a rejection symbol $\perp$. Since the adversary $\mathcal{A}$ can not query $(\phi, (\psi, \chi))$ such that $(\psi, \chi) = (\psi^*, \chi^*)$ and $\phi(SK) = SK$, we have that $\phi(SK) \neq SK$. According to the Φ-key fingerprint property, the probability that $\mathcal{A}$ can find a function $\phi \in \Phi$ such that $\phi(SK) \neq SK$ and $T(PK, \phi, \psi) = \psi$ is a negligible value ϵ_{kf}.
- Case 4: $\psi = \psi' = \psi^*$ and $\chi \neq \chi^*$. The adversary $\mathcal{B}$ returns a rejection symbol $\perp$. According to the INT-OT security of Tag-DEM, $\text{Tag-DEM.D}(K^*, \chi, \psi) = \perp$ except with the probability of $\mathrm{Adv}^{\text{int-ot}}_{\mathcal{A}}$.

According to the four cases above, we have that $\mathcal{B}$ simulates the related key decryption oracle in this step perfectly except with the probability of $\mathrm{Adv}^{\text{int-ot}}_{\mathcal{A}} + \epsilon_{\text{kf}}$.

Guess: Finally when $\mathcal{A}$ outputs b', $\mathcal{B}$ outputs 1 if $b' = b$ and 0 otherwise.

To compute the advantage of $\mathcal{B}$ in breaking the IND-CCA2 security of the KEM scheme we first consider the probability that $\mathcal{B}$ succeeds in guessing $K^* = K_1$ or $K^* = K_0$. According to the algorithm above, we have:

$$\begin{aligned} \Pr[\mathcal{B}_{suc}] = \Pr[b' = b | K^* = K_1] \Pr[K^* = K_1] + \\ \Pr[b' \neq b | K^* = K_0] \Pr[K^* = K_0], \end{aligned} \tag{1}$$

where $\Pr[\mathcal{B}_{suc}]$ denotes the probability that $\mathcal{B}$ succeeds in guessing $K^* = K_1$ or $K^* = K_0$.

According to the definition of the IND-CCA2 security for KEM, we have that:

$$\Pr[K^* = K_1 = \text{KEM.D}(SK, \psi^*)] = \Pr[K^* = K_0] = 1/2. \tag{2}$$

If $K^* = K_1 = \text{KEM.D}(SK, \psi^*)$, we have that $\mathcal{B}$ simulates the Φ-CC-RKA challenger perfectly except with the probability of $\text{Adv}_{\mathcal{A}}^{\text{int-ot}} + \epsilon_{\text{kf}}$. Thus we have:

$$\Pr[b = b' | K^* = K_1] \geq 1/2 + \text{Adv}_{\mathcal{A},\Phi}^{\text{rka}} - (\text{Adv}_{\mathcal{A}}^{\text{int-ot}} + \epsilon_{\text{kf}}). \tag{3}$$

If $K^* = K_0$, since K_0 is randomly chosen from the key space we have that K^* is independent from the point view of $\mathcal{A}$ except the probability of $\text{Adv}_{\mathcal{A}}^{\text{int-ot}} + \epsilon_{\text{kf}}$. Thus we have:

$$\Pr[b \neq b' | K^* = K_0] \geq 1/2 - \text{Adv}_{\mathcal{A}}^{\text{ind-ot}} - (\text{Adv}_{\mathcal{A}}^{\text{int-ot}} + \epsilon_{\text{kf}}). \tag{4}$$

From equations (1), (2) and (3) we have that:

$$\begin{aligned} \Pr[\mathcal{B}_{suc}] &= \Pr[b' = b | K^* = K_1] \Pr[K^* = K_1] + \\ &\quad \Pr[b' \neq b | K^* = K_0] \Pr[K^* = K_0] \\ &\geq (1/2 - \text{Adv}_{\mathcal{A}}^{\text{ind-ot}} - (\text{Adv}_{\mathcal{A}}^{\text{int-ot}} + \epsilon_{\text{kf}}))1/2 + \\ &\quad (1/2 + \text{Adv}_{\mathcal{A},\Phi}^{\text{rka}} - (\text{Adv}_{\mathcal{A}}^{\text{int-ot}} + \epsilon_{\text{kf}}))1/2 \\ &= 1/2(\text{Adv}_{\mathcal{A},\Phi}^{\text{rka}} - \text{Adv}_{\mathcal{A}}^{\text{ind-ot}}) + 1/2 - (\text{Adv}_{\mathcal{A}}^{\text{int-ot}} + \epsilon_{\text{kf}}) \end{aligned} \tag{5}$$

Finally we can get the advantage of $\mathcal{B}$ as follows:

$$\begin{aligned} \text{Adv}_{\mathcal{B}}^{\text{cca}} &= |\Pr[\mathcal{B}_{suc}] - 1/2| \\ &\geq \tfrac{1}{2}\text{Adv}_{\mathcal{A},\Phi}^{\text{rka}} - \tfrac{1}{2}\text{Adv}_{\mathcal{A}}^{\text{ind-ot}} - \text{Adv}_{\mathcal{A}}^{\text{int-ot}} - \epsilon_{\text{kf}}. \end{aligned} \tag{6}$$

This completes the proof of theorem 1. □

Now we prove the CC-RKA security of the hybrid encryption scheme when the KEM scheme is IND-CCCA secure.

Theorem 2. *If the KEM part is IND-CCCA secure and has the properties of Φ-key malleability and Φ-key fingerprint, the Tag-DEM part is Tag-AE-OT secure, then the hybrid encryption above is Φ-CC-RKA secure.*

The proof of theorem 2 is similar to that of theorem 1. The only difference is that in the decryption oracle $\mathcal{B}$ needs to provide a boolean predicate function *pred* when querying the decapsulation oracle of the IND-CCCA secure KEM challenger. Just as in [19], we can use the ciphertext of the Tag-DEM scheme as the boolean predicate function. That is $pred_{\chi}(K) = 0$ if $\text{Tag-DEM.D}(K, \chi, \psi) = \perp$ and $pred_{\chi}(K) = 1$ otherwise.

4 Instantiations

In this section we show that several classical KEM schemes have the properties of key malleability and key fingerprint. Specifically, we consider the KEM schemes from the Cramer-Shoup paradigm and the "all-but-one extraction" paradigm.

4.1 KEM Schemes from the Cramer-Shoup Paradigm

We show that the IND-CCCA secure KEM scheme proposed in [24] has the properties of key malleability and key fingerprint. First we review the scheme as follows.

– KeyGen(1^k): Assume that G is a group of order q where q is large prime number.

$$(g_1, g_2) \xleftarrow{R} G, (x_1, x_2) \xleftarrow{R} Z_q^*, h \leftarrow g_1^{x_1} g_2^{x_2},$$

$$PK \leftarrow (g_1, g_2, h, \mathrm{H}), SK \leftarrow (x_1, x_2),$$

where H is a 4-wise independent hash function.

– Encapsulation(PK):

$$r \xleftarrow{R} Z_q^*, u_1 \leftarrow g_1^r, u_2 \leftarrow g_2^r, K \leftarrow \mathrm{H}(h^r), \psi \leftarrow (u_1, u_2).$$

– Decapsulation(SK, ψ): $K \leftarrow \mathrm{H}(u_1^{x_1} u_2^{x_2})$.

Now show that the KEM above satisfies $\Phi^\times$-key malleability and $\Phi^\times$-key fingerprint, where $\phi^\times(s) = as \mod q$, $\phi^\times \in \Phi^\times, a \in Z_q$.

$\Phi^\times$-Key malleability. For $PK = (g_1, g_2, h, H), SK = (x_1, x_2), \psi = (u_1, u_2)$ and $\phi^\times(x_1, x_2) = (a_1 x_1, a_2 x_2)$, the transform function T is defined as:

$$T(PK, \phi^\times, \psi) = (u_1^{a_1}, u_2^{a_2}).$$

The correctness of T can be verified as follows:

$$\mathrm{KEM.D}(\phi^\times(SK), \psi) = \mathrm{H}(u_1^{a_1 x_1} u_2^{a_2 x_2}).$$

$$\mathrm{KEM.D}(SK, T(PK, \phi^\times, \psi)) = \mathrm{KEM.D}(SK, (u_1^{a_1}, u_2^{a_2})) = \mathrm{H}(u_1^{a_1 x_1} u_2^{a_2 x_2}).$$

$\Phi^\times$-Key fingerprint. For $PK = (g_1, g_2, h, H), SK = (x_1, x_2), \psi = (u_1, u_2)$ and $\phi^\times(x_1, x_2) = (a_1 x_1, a_2 x_2)$, if $(a_1 x_1, a_2 x_2) \neq (x_1, x_2)$ we have that

$$T(PK, \phi^\times, \psi) = (u_1^{a_1}, u_2^{a_2}) \neq (u_1, u_2).$$

Thus the KEM above satisfies $\Phi^\times$-key fingerprint.

There are several KEM schemes from the Cramer-Shoup paradigm [14,27,24,20]. It is easy to verify that KEM scheme in [20] also satisfies these two properties, while the KEM schemes in [14] and [27] are not $\Phi^\times$-key malleability.

4.2 KEM Schemes from the All-But-One Extraction Paradigm

We show that the IND-CCA2 secure KEM scheme proposed in [21] satisfies key malleability and key fingerprint. First we review the scheme as follows.

– KeyGen: The key generation algorithm chooses uniformly at random a Blum integer $N = PQ = (2p+1)(2q+1)$, where P, Q, p, q are prime numbers, then computes:

$$g \xleftarrow{R} \mathrm{QR}_N, x \xleftarrow{R} [(N-1)/4], X \leftarrow g^{x 2^{l_K + l_H}},$$

$$PK \leftarrow (N, g, X), SK \leftarrow x,$$

where $\mathrm{H} : QR_N \rightarrow \{0,1\}^{l_H}$ is a TCR (Target Collision Resistant) hash function, l_H is the bit length of the output value of H, l_K is the bit length of the encapsulated key K.

– Encapsulation:

$$\mu \overset{R}{\leftarrow} [(N-1)/4], R \leftarrow g^{\mu 2^{l_K+l_H}}, t \leftarrow \mathrm{H}(R), S \leftarrow \left|\left(g^t X\right)^{\mu}\right|,$$

$$K \leftarrow \mathrm{BBS}_N(g^{\mu 2^{l_H}}),$$

where $\mathrm{BBS}_N(s) = \mathrm{LSB}(s), \cdots, \mathrm{LSB}(s^{2^{l_K-1}})$, $\mathrm{LSB}(s)$ denotes the least significant bit of s.

– Decapsulation: Given a ciphertext (R, S) and PK, the decapsulation algorithm verifies $R \in Z_N^*, S \in Z_N^* \cap [(N-1)/2]$, then computes:

$$t \leftarrow \mathrm{H}(R),$$

$$\text{if } \left(\frac{S}{R^x}\right)^{2^{l_K+l_H}} = R^t \text{ then computes}$$

$$2^{\gamma} = \gcd(t, 2^{l_K+l_H}) = \alpha t + \beta 2^{l_K+l_H},$$

$$\text{returns } K \leftarrow \mathrm{BBS}_N\left(\left(\left(SR^{-x}\right)^{\alpha} R^{\beta}\right)^{2^{l_H-\gamma}}\right),$$

$$\text{else returns the rejection symbol } \perp .$$

Now we show that the KEM scheme above has the properties of Φ^+-key malleability and Φ^+-key fingerprint, where $\phi^+(s) = s + a$, $\phi \in \Phi, a \in Z_N$.

Φ^+-Key malleability. For $PK = (N, g, X), SK = x$, $\phi^+(x) = x + a$, and $\psi = (R, S) = (g^{\mu 2^{l_K+l_H}}, \left|\left(g^t X g^{a 2^{l_K+l_H}}\right)^{\mu}\right|)$ the transform function T is defined as:

$$T(PK, \phi^+, \psi) = (R, SR^{-a}) = (g^{\mu 2^{l_K+l_H}}, \left|\left(g^t X\right)^{\mu}\right|).$$

The correctness of T can be verified as follows:

$$\mathrm{KEM.D}(\phi^+(SK), \psi) = \mathrm{BBS}_N(g^{\mu 2^{l_H}}).$$

$$\mathrm{KEM.D}(SK, T(PK, \phi^+, \psi)) = \mathrm{KEM.D}(SK, (R, SR^{-a})) = \mathrm{BBS}_N(g^{\mu 2^{l_H}}).$$

Φ^+-Key fingerprint. For $PK = (N, g, X), SK = (x)$, $\phi^+(x) = x + a$, and $\psi = (R, S) = (g^{\mu 2^{l_K+l_H}}, \left|(g^t X)^{\mu}\right|)$ if $x+a \neq x$ and $T(PK, \phi^+, \psi) = (R, SR^{-a}) = (R, S)$ we have $R^{-a} = 1 \mod N$. Since $a \in Z_N, R \in QR_N$ we have $pq \leq a = \delta pq \leq 4pq$, where $\delta \in \{1, 2, 3, 4\}$. Thus we can find pq from the equation $pq = a/\delta \approx \frac{N-1}{4}$ and then factor N. So the adversary can not find such ϕ^+ except with negligible probability.

There are several KEM schemes from the all-but-one extraction paradigm [10,23,21,30,29,28]. It is easy to verify that KEM schemes in [30,29,28] also satisfy these two properties, while the KEM schemes in [10,23] do not satisfy Φ^+-key malleability.

5 Conclusion

We proved that the KEM/Tag-DEM hybrid encryption is Φ-CC-RKA secure if the IND-CCA2 (or IND-CCCA) secure KEM part satisfies Φ-key malleability and Φ-key fingerprint and the Tag-DEM part is a one-time secure tag authenticated encryption. We showed that several KEM schemes satisfy these two properties. Thus we can get efficient CC-RKA secure hybrid encryption schemes.

Compared with Wee's construction [31] we do not need the one-time signature. In addition, we can get CC-RKA secure public key encryption schemes from the "all-but-one extraction" paradigm and the Cramer-Shoup paradigm uniformly. While Wee's framework can only get CC-RKA secure public key encryption schemes from the "all-but-one extraction" paradigm.

References

1. Applebaum, B., Harnik, D., Ishai, Y.: Semantic security under related-key attacks and applications. In: ICS, pp. 45–60 (2011)
2. 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)
3. 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)
4. 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)
5. 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)
6. Biham, E.: New types of cryptoanalytic attacks using related keys (extended abstract. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 398–409. Springer, Heidelberg (1994)
7. 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)
8. Boneh, D., Boyen, X.: Efficient selective-ID secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
9. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the importance of checking cryptographic protocols for faults (extended abstract). In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 37–51. Springer, Heidelberg (1997)
10. Boyen, X., Mei, Q., Waters, B.: Direct chosen ciphertext security from identity-based techniques. In: ACM Conference on Computer and Communications Security, pp. 320–329. ACM (2005)

11. Chen, Y., Dong, Q.: RCCA security for KEM+DEM style hybrid encryptions. In: Kutyłowski, M., Yung, M. (eds.) Inscrypt 2012. LNCS, vol. 7763, pp. 102–121. Springer, Heidelberg (2013)
12. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)
13. Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (2002)
14. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. 33, 167–226 (2004), http://dl.acm.org/citation.cfm?id=953065.964243
15. Damgård, I., Faust, S., Mukherjee, P., Venturi, D.: Bounded tamper resilience: How to go beyond the algebraic barrier. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 140–160. Springer, Heidelberg (2013)
16. Goldenberg, D., Liskov, M.: On related-secret pseudorandomness. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 255–272. Springer, Heidelberg (2010)
17. Goyal, V., O'Neill, A., Rao, V.: Correlated-input secure hash functions. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 182–200. Springer, Heidelberg (2011)
18. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: Cold boot attacks on encryption keys. In: USENIX Security Symposium, pp. 45–60 (2008)
19. Hofheinz, D., Kiltz, E.: Secure hybrid encryption from weakened key encapsulation. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 553–571. Springer, Heidelberg (2007)
20. 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)
21. Hofheinz, D., Kiltz, E.: Practical chosen ciphertext secure encryption from factoring. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 313–332. Springer, Heidelberg (2009)
22. Jia, D., Lu, X., Li, B., Mei, Q.: RKA secure PKE based on the DDH and HR assumptions. In: Susilo, W., Reyhanitabar, R. (eds.) ProvSec 2013. LNCS, vol. 8209, pp. 271–287. Springer, Heidelberg (2013)
23. Kiltz, E.: Chosen-ciphertext secure key-encapsulation based on gap hashed diffie-hellman. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 282–297. Springer, Heidelberg (2007)
24. 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)
25. Knudsen, L.R.: Cryptanalysis of loki 91. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 196–208. Springer, Heidelberg (1993), http://dx.doi.org/10.1007/3-540-57220-1_62
26. Kocher, P.C.: Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996)
27. Kurosawa, K., Desmedt, Y.: A new paradigm of hybrid encryption scheme. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 426–442. Springer, Heidelberg (2004)

28. Lu, X., Li, B., Liu, Y.: How to remove the exponent GCD in HK09. In: Susilo, W., Reyhanitabar, R. (eds.) ProvSec 2013. LNCS, vol. 8209, pp. 239–248. Springer, Heidelberg (2013)
29. Lu, X., Li, B., Mei, Q., Liu, Y.: Improved efficiency of chosen ciphertext secure encryption from factoring. In: Ryan, M.D., Smyth, B., Wang, G. (eds.) ISPEC 2012. LNCS, vol. 7232, pp. 34–45. Springer, Heidelberg (2012)
30. Lu, X., Li, B., Mei, Q., Liu, Y.: Improved tradeoff between encapsulation and decapsulation of HK09. In: Wu, C.-K., Yung, M., Lin, D. (eds.) Inscrypt 2011. LNCS, vol. 7537, pp. 131–141. Springer, Heidelberg (2012)
31. 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)