On the (Im)possibility Results for Strong Attack Models for Public Key Cryptsystems

Yutaka Kawai
University of Tokyo
5-1-5 Kashiwanoha, Kashiwa-shi
Chiba 277-8561, Japan
kawai@it.k.u-tokyo.ac.jp

Yusuke Sakai
The University of Electro-Communications
1-5-1 Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan
y-sakai@uec.uec.ac.jp

Noboru Kunihiro
University of Tokyo
5-1-5 Kashiwanoha, Kashiwa-shi
Chiba 277-8561, Japan
kunihiro@k.u-tokyo.ac.jp

Abstract

In this paper, we discuss the strong attack model security for public key encryption scheme and digital signature scheme. Recently, Barbosa and Farshim introduced strong chosen ciphertext attack (SCCA) which is stronger than chosen ciphertext attack. The main motivation of this paper is to find an essential mechanism of secure schemes under strong attack model. So, we prove several impossibility results under SCCA model. For the purpose, we classify two types of public key encryption schemes: First model is $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ which we call the setup-free model, second model is $\Pi = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ which we call the setup model. We prove that it is impossible to reduce indistinguishability under strong chosen ciphertext attack (IND-SCCA) security to any other weaker security notion under black-box analysis in the standard model. Second, when a public key encryption scheme is modeled as $\Pi = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, we show that it is impossible that the security of SCCA is proven if the reduction is setup-preserving black-box reductions which we define in this paper. From the similar discussion, we prove impossibilities for digital signature schemes. Finally, we discuss the essential mechanism to construct IND-SCCA secure public key encryption scheme in the standard model.

Keywords: public key cryptsystems, attack models, encryptions

1 Introduction

1.1 Background

The security notion of cryptographic primitives can be formalized by the combination of an adversarial goal (GOAL) and an attack model (ATK). Moreover, the securities of schemes are analyzed from the view point of security notion, with or without random oracle, and computational assumptions. For public key encryption scheme, indistinguishability under chosen ciphertext attack is the most common security notions. For achieving chosen ciphertext attack security, there are many researches. Recently, in [2, 3], Barbosa and Farshim introduced strong chosen ciphertext attack in order to show the relationship among various notions of complete non-malleability which is introduced in [10]. Since an adversary can obtain a plaintext of a ciphertext under *an arbitrarily chosen public key* in this attack model, this attack model is the more powerful than standard chosen ciphertext attack model and multi-user setting attack model [5, 13]. In [2], Barbosa and Farshim proposed the efficient scheme which satisfies indistinguishability against strong chosen ciphertext attack in the standard model. This scheme is based on the construction of [20, 7] and efficient construction. However, an essential mechanism that a scheme is secure under strong chosen ciphertext attack is not very clear (e.g. it is not known whether previous proposed chosen ciphertext secure public key encryption scheme is secure under strong chosen ciphertext attack). Therefore, the further evaluation of (im)possibility of strong attack model security for public key encryption schemes is considered to be beneficial.

1.2 Our Contributions

In this paper, we discuss the strong attack model security for a public key encryption scheme and a digital signature scheme. In the strong chosen ciphertext attack model (SCCA) which is introduced in [2], an adversary access to an oracle that encrypted plaintext under arbitrary public key which the adversary chooses. Since a practical attack under strong attack model might be happened in the real-world, strong attack model should be investigated in this field. The main motivation of this paper is to find an essential property of secure schemes under strong attack model for public key encryption schemes and digital signature schemes.

We introduce *strong chosen message attack* for digital signature schemes. In this attack model, an adversary access to an oracle that signs messages of the adversary's choice with respect to an arbitrary public key. First, in order to discuss the security under strong attack models rigorously, in this paper, we classify two types of public key encryption schemes; (1) Setup-free model, and (2) Setup model. Setup-free model is ordinary model, that is a triple of algorithms, $\Pi_{\mathsf{f}} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. Here, Gen is public and secret key generation algorithm, Enc is an encryption algorithm, and Dec is a decryption algorithm. Setup model is a slightly different model from setup-free model, is a fourth of algorithms, $\Pi_{\mathsf{s}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. Here, Setup is the probabilistic setup algorithm which takes as input the security parameter and returns the common parameter I. The scheme which was proposed in [2] is the setup model public key encryption scheme. Similarly, we distinguish two types of a digital signature scheme: (1)Basic model is $\Sigma_{\mathsf{f}} = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$, (2)Setup model is $\Sigma_{\mathsf{s}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$. In this paper, we show several impossibility results for strong attack model in the setup-free/setup model.

Our first impossibility result is that it is impossible to reduce indistinguishability under strong chosen ciphertext attack ($\mathsf{IND\text{-}SCCA}$) security on *any setup-free model* public key encryption scheme to any non-interactive computationally hard problem under black-box analysis without random oracle model. From the similar discussion, we show it is impossible to reduce existential unforgeability under strong chosen message attack ($\mathsf{EuF\text{-}SCMA}$) security on *any setup-free model* digital signature scheme to any non-interactive computationally hard problem under black-box analysis. These results mean that if each user who uses public key encryption or digital signature scheme has a public key that all parameter of the key is different from any other, its schemes cannot be proven $\mathsf{IND\text{-}SCCA}/\mathsf{EuF\text{-}SCMA}$ security under any non-interactive computationally hard problem.

Fischlin prove similar impossibility results for complete non-malleability which he introduced in [10]. Fischlin initiated the research of complete non-malleability and further showed that no completely non-malleable schemes exist for general relations[10]. Lately Barbosa and Farshim proved equivalence between security against strong decryption oracles and some kind of complete non-malleability [2]. Unfortunately, the definition of complete non-malleability used by Barbosa and Farshim [2] is slightly different from that of Fischlin's [10], and moreover, no implications between the two variants of complete non-malleability are clearly shown for the present. This fact implies that Fischlin's impossibility result is not directly converted to the context of strong decryption scenarios, which is what this paper investigates.

Our second impossibility results is that it is impossible that $\mathsf{IND\text{-}SCCA}/\mathsf{EuF\text{-}SCMA}$ security is proven if the reduction is *setup-preserving black-box reductions* i.e. reductions is always call the adversarial oracle with the common parameter I they were given as input. The above discussion is similar to [16]. Our impossibility results do not contradict the result of [2]. In fact, in [2], the scheme is setup model and a reduction of the security proof is not setup-preserving.

Our second result is that we show several public key encryption and digital signature schemes which are secure under the strong chosen ciphertext/chosen message attack model *in the random oracle model*. Specifically, we prove that DHIES scheme and Schnorr signature scheme are secure in the random oracle model as examples.

Finally, we discuss the essential mechanism to construct IND-SCCA secure public key encryption scheme. Concretely, we show that it is possible to construct IND-SCCA secure scheme using the extended Naor-Yung paradigm [14].

1.3 Related Works

So far, the security for strong attack models on cryptographic primitives has been intensively studied in the literatures. In [10], Fischlin introduced the concept of complete non-malleability, where an adversary can tamper with ciphertext and public keys, and indistinguishability of ciphertexts. He shows several impossibility result of complete non-malleability for any public encryption and digital signature scheme. Moreover, he shows several secure schemes on complete non-malleability in the random oracle model. In [2, 3], Barbosa and Farshim discuss relations among various notions of complete non-malleability. In order to discuss relations, they introduce indistinguishability based security model based on a strong decryption oracle (IND-SCCA) and they proposed efficient scheme which is secure for IND-SCCA. In [12], Libert and Yung proposed efficient scheme which is secure for complete non-malleability under decision bilinear Diffie-Hellman assumption.

2 Setup-Free and Setup Model for Public Key Encryption and Digital Signature

2.1 Public Key Encryption and Digital Signature

In this paper, we discuss two models for digital signature schemes and public key encryption schemes, the *setup-free* model and the *setup* model.

Setup-free Models. First, we consider a *setup-free* public key encryption and digital signature model. A *setup-free* public key encryption scheme is given by a triple of algorithms, $\Pi_{\mathsf{f}} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. Gen, the key generation algorithm, takes as inputs a security parameter and returns a pair (pk, sk) of matching public and secret keys, denoted as $(pk, sk) \leftarrow \mathsf{Gen}(k)$. Enc, the encryption algorithm, takes as inputs a public key pk and a plaintext m, and returns a ciphertext c, denoted as $c \leftarrow \mathsf{Enc}_{pk}(m)$. Dec, the decryption algorithm, is a deterministic algorithm which takes as inputs a secret key sk and a ciphertext c, and outputs a plaintext m or a special symbol $\perp$ which indicates that the ciphertext was invalid, denoted as $m/\perp \leftarrow \mathsf{Dec}_{sk}(c)$.

A *setup-free* digital signature scheme is given by a triple of algorithms, $\Sigma_{\mathsf{f}} = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$. Gen, the key generation algorithm, takes as input a security parameter and returns a pair (pk, sk) of matching public and secret keys, denoted as $(pk, sk) \leftarrow \mathsf{Gen}(k)$. Sig, the signature generation algorithm, takes as inputs a secret key sk and a message m, and returns a signature σ, denoted as $\sigma \leftarrow \mathsf{Sig}_{sk}(m)$. Ver, the verification algorithm, takes as inputs a public key, a message, and a signature, and outputs 1 if and only if σ is valid on m, or 0 otherwise.

Setup Model. In this paper, we consider a slightly different model "Setup model" with the extra Setup algorithm. So, a public key encryption scheme in setup model is $\Pi_{\mathsf{s}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ and a public key encryption scheme $\Sigma_{\mathsf{s}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$. Setup is the probabilistic setup algorithm which takes as input the security parameter and returns the common parameter I, denoted as $I \leftarrow \mathsf{Setup}(k)$. In setup model, Gen takes as inputs I and returns a pair $(pk.sk)$ of matching public and secret keys, denoted as $(pk, sk) \leftarrow \mathsf{Gen}(I, k)$.. Enc and Dec denoted as $c \leftarrow \mathsf{Enc}_{I,pk}(m)$ and $m/\perp \leftarrow \mathsf{Dec}_{I,sk}(c)$, respectively. Also, in the signature scheme, Sig and Ver denoted as $\sigma \leftarrow \mathsf{Sig}_{I,sk}(m)$ and $0/1 \leftarrow \mathsf{Ver}_{I,pk}(m, \sigma)$ in setup model.

2.2 Security Notions for Public Key Encryption

Security notions for public key encryption schemes are defined by pairing an adversarial goal (GOAL) and an attack model (ATK) [8, 4, 15]. We review three main adversarial goals for Π_{f} or Π_{s} where Π_{f} is a public key encryption scheme in the setup-free model and Π_{s} is a public key encryption scheme in setup model.

Total unBreakable (TuB): Π_{f} or Π_{s} is said to be TuB when no PPT adversary can compute the secret key

One-wayness (OW): Π_{f} or Π_{s} is said to be OW when for a given ciphertext $c^* = \mathsf{Enc}_{pk}(m^*)$ where m^* is a randomly chosen plaintext from the plaintext space M, no PPT adversary can recover m^*.

Indistinguishability (IND): Π_{f} or Π_{s} is said to be IND when for a given ciphertext $c_b = \mathsf{Enc}_{pk}(m_b)$ where a plaintext $m_b \in \{m_0, m_1\}$ and (m_0, m_1) are chosen by the adversary, no PPT adversary can output $b' = b$ with a non-negligibly higher probability than 1/2.

Three main attack models (atk) for Π_{f} or Π_{s} are as follows.

Chosen plaintext attack (CPA): In this model, an adversary is allowed to access the empty oracle ε which for any input, return $\perp$.

Plaintext checking attack (PCA)[15]: In this model, an adversary is allowed to access the plaintext-checking oracle C which on input (m, c), returns 1 if $m = \mathsf{Dec}_{sk}(c)$, otherwise returns 0.

Chosen ciphertext attack (CCA): In this model, an adversary is allowed to access the decryption oracle D which on input a ciphertext c, returns a plaintext $m = \mathsf{Dec}_{sk}(c)$ or a special symbol $\perp$ which indicates that the ciphertext was invalid.

In this paper, we define strong chosen ciphertext and message attack (SCCA) [2].

Strong chosen ciphertext attack (SCCA): In SCCA model, an adversary access to an oracle SD that encrypted plaintext of the adversary's choice with respect to arbitrary public key.

```
proc. SCCA$(c, pk)$:
$m \leftarrow \{m : \exists sk, m = \mathsf{Dec}_{sk}(c)\}$ Return $m$.
```

The above adversarial goals are considered not achieved if the adversary submits a query whose answer from the oracle can be trivially transformed into the correct output.

Definition 1 ({TuB,OW}.ATK Secure). *Let* $\Pi_{\mathsf{f}} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *and* $\Pi_{\mathsf{s}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a public key encryption scheme. We say* Π_{f} *or* Π_{s} *is* GOAL-ATK *secure for all PPT adversary* A*, when the following probability is negligible for a security parameter k:*

$$\Pr[(sk, pk) \leftarrow \mathsf{Gen}(1^k); (x) \leftarrow A^{O_{\mathsf{ATK}}}(y)] \textit{(in the case of the setup-free model } \Pi_{\mathsf{f}}\textit{,)}$$

where $(x,y) = (sk,pk)$*, or* $(m,(pk,c))$ *where m is chosen from the message space uniform at random and* $c = \mathsf{Enc}_{pk}(m)$*, if* GOAL=TuB *or* OW*, respectively, and* $O_{\mathsf{ATK}} = \varepsilon$*, C, or D, if* ATK=CPA*,* PCA*, or* CCA*, respectively.*

$$\Pr[I \leftarrow \mathsf{Setup}(1^k), (sk,pk) \leftarrow \mathsf{Gen}(1^k); (x) \leftarrow A^{O_{\mathsf{ATK}}}(y)] (\textit{ in the case of the setup model } \Pi_{\mathsf{s}})$$

where $(x,y) = (sk,(I,pk))$*, or* $(m,(I,pk,c))$ *where m is chosen from the message space uniform at random and* $c = \mathsf{Enc}_{pk}(m)$*, if* GOAL=TuB *or* OW*, respectively, and* $O_{\mathsf{ATK}} = \varepsilon$*, C, D, or SD if* ATK=CPA*,* PCA*,* CCA*, or* SCCA*, respectively.*

Definition 2 (IND-ATK Secure)**.** *Let* $\Pi_{\mathsf{f}} = (\mathsf{Gen},\mathsf{Enc},\mathsf{Dec})$ *and* $\Pi_{\mathsf{s}} = (\mathsf{Setup},\mathsf{Gen},\mathsf{Enc},\mathsf{Dec})$ *be a public key encryption scheme. We say* Π_{f} *or* Π_{s} *is* IND-ATK *secure for all PPT adversary* A*, when the following probability is negligible for a security parameter k:*

$$\Pr[(sk,pk) \leftarrow \mathsf{Gen}(1^k); (m_0,m_1) \leftarrow \mathsf{A}^{O_{\mathsf{ATK}}}_{\mathsf{IND\text{-}ATK}[\Pi]}(pk,state); b \leftarrow \{0,1\};$$

$$c_b = \mathsf{Enc}_{pk}(m_b) : b \leftarrow \mathsf{A}^{O_{\mathsf{ATK}}}_{\mathsf{IND\text{-}ATK}[\Pi]}(pk,state)] - \frac{1}{2} \textit{ in the case of setup-free model } \Pi_{\mathsf{f}},$$

$$\Pr[I \leftarrow \mathsf{Setup}(1^k), (sk,pk) \leftarrow \mathsf{Gen}(1^k); (m_0,m_1) \leftarrow \mathsf{A}^{O_{\mathsf{ATK}}}_{\mathsf{IND\text{-}ATK}[\Pi]}(pk,state); b \leftarrow \{0,1\};$$

$$c_b = \mathsf{Enc}_{pk}(m_b) : b \leftarrow \mathsf{A}^{O_{\mathsf{ATK}}}_{\mathsf{IND\text{-}ATK}[\Pi]}(pk,state)] - \frac{1}{2} \textit{ in the case of setup model } \Pi_{\mathsf{s}}$$

where $O_{\mathsf{ATK}} = \varepsilon$*, C, D, or SD if* ATK=CPA*,* PCA*,* CCA*, or* SCCA*, respectively.*

2.3 Security Notions for Digital Signature

Security notions for a digital signature scheme are defined by pairing an adversarial goal (GOAL) and an attack model (ATK) [11]. We first review three main adversarial goals (goal) for Σ_{f} or Σ_{s} where Σ_{f} is a digital signature scheme in the setup-free model and Σ_{s} is a digital signature scheme in setup model.

Total unBreakable (TuB)**:** Σ_{f} or Σ_{s} is said to be TuB when no PPT adversary can compute the secret key *sk* which corresponds to *pk*.

Universal unForgery (UuF)**:** Σ_{f} or Σ_{s} is said to be UuF when for a randomly chosen message m^* from the message space M, no PPT adversary can forge a valid signature σ^* on m^*.

Existential unForgery (EuF)**:** Σ_{f} or Σ_{s} is said to be EuF when no PPT adversary can forge a pair of a message m^* and its valid signature σ^*.

Three main attack models (atk) for Σ_{f} or Σ_{s} are as follows.

Key only attack (KOA)**:** In this model, an adversary is allowed to access the empty oracle ε which for any input, return $\perp$.

Known message attack (KMA)**:** In this model, an adversary is allowed to access the restrictive signing oracle *RS* which on input 0, returns a pair of a message *m* and its signature $\sigma = \mathsf{Sig}_{sk}(m)$ where *m* is chosen from a pre-determined distribution.[1]

Chosen message attack (CMA)**:** In this model, an adversary is allowed to access the signing oracle *S* which on input a message *m*, returns its signature $\sigma = \mathsf{Sig}_{sk}(m)$.

The above goals are considered not achieved if the adversary submits a query whose answer from the oracle can be trivially transformed into the correct output. In this paper, we introduce strong chosen message attack (SCMA) for digital signature schemes.

[1] Rigorously, it is necessary to specify the distribution of the messages for defining KMA, but since our results hold for any distribution, here we do not strictly specify it.

Strong chosen message attack (SCMA)**:** In SCMA model, an adversary access to an oracle *SS* that signs messages of the adversary's choice with respect to arbitrary public key.

```
proc. SCMA$(m, pk)$:
$\sigma \leftarrow \{\sigma : \exists sk, \sigma = \mathsf{Sig}_{sk}(m)\}$ Re-
turn $\sigma$.
```

Definition 3. *Let $\Sigma_\mathsf{f} = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ and $\Sigma_\mathsf{s} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ be a digital signature scheme. We say Σ_f or Σ_s is* GOAL-ATK *secure for all PPT adversary A, when the following probability is negligible for a security parameter k:*

$$\Pr[(sk, pk) \leftarrow \mathsf{Gen}(1^k); (x) \leftarrow A^{O_{\mathsf{ATK}}}(y)] (\textit{ in the case of the setup-free model } \Sigma_\mathsf{f},)$$

where $(x, y) = (sk, pk)$, $(\sigma, (pk, m))$ where m is chosen from the message space uniform at random, or $((m, \sigma), pk)$, if GOAL=TuB, UuF*, or* EuF*, respectively.*

$$\Pr[I \leftarrow \mathsf{Setup}(1^k), (sk, pk) \leftarrow \mathsf{Gen}(I); (x) \leftarrow A^{O_{\mathsf{ATK}}}(y)] (\textit{ in the case of the setup model } \Sigma_\mathsf{s})$$

where $(x, y) = (sk, (I, pk))$, $(\sigma, (I, pk, m))$ where m is chosen from the message space uniform at random, or $((m, \sigma), (I, pk))$, if GOAL=TuB, UuF*, or* EuF*, respectively. $O = \varepsilon, RS, Sor$ SS, if* ATK=KOA, KMA, CMA*, or* SCMA*, respectively.*

Black Box Reduction. Let P_1 and P_2 be two computational problems. A black-box reduction from P_1 to P_2 is represented by probabilistic algorithm R which solves P_1 using an algorithm to solve P_2. Here, the input of R is the same as the input of the algorithm that solves P_1. Also, the input of an algorithm to solve P_2 is reduced by R. The success probability of R is ε_1 which is non-negligible. If the probability of an algorithm to solve P_2 is ε_2, the probability of solving P_1 is $\varepsilon_1 \times \varepsilon_2$. The notation $P_1 \Leftarrow_R P_2$ means that there exists a polynomial time black-box reduction R from P_1 to P_2. The case in which $P_1 \Leftarrow P_2$ and $P_2 \Leftarrow P_1$ hold simultaneously is denoted as $P_1 \equiv P_2$.

In this paper, we will represent computational problems P as follows; First, we treat only computational problem P which can be equivalent to some security notion GOAL-ATK. For example, in Gap-Diffie-Hellman problem [15] GOAL is CDH problem and ATK is DDH oracle.

Definition 4. *We say that* GOAL1 *is harder (resp. easier) than* GOAL2 *if for all scheme X and* ATK*, it is always possible to explicitly construct a BB reduction R such that $\mathsf{A}_{\mathsf{GOAL2.ATK}[X]} \Leftarrow_R \mathsf{A}_{\mathsf{GOAL1.ATK}[X]}$ (resp. $\mathsf{A}_{\mathsf{GOAL1.ATK}[X]} \Leftarrow_R \mathsf{A}_{\mathsf{GOAL2.ATK}[X]}$). Similarly, we say that* ATK1 *is weaker (resp. stronger) than* ATK2 *if for all X and* GOAL*, it is always possible to explicitly construct a BB reduction R such that $\mathsf{A}_{\mathsf{GOAL.ATK2}[X]} \Leftarrow_R \mathsf{A}_{\mathsf{GOAL.ATK1}[X]}$ (resp. $\mathsf{A}_{\mathsf{GOAL1.ATK}[X]} \Leftarrow_R \mathsf{A}_{\mathsf{GOAL2.ATK}[X]}$).*

3 Impossibility results in the Setup-Free Model

In this section, we show impossibility results that IND-SCCA/EuF-SCMA security under a non-interactive computationally hard problem P in the setup-free model. We assume that an instance of P y can be generated with a security parameter k using an instance generator $\mathsf{IGen}(k)$.

Specifically, we show that there does not exists any black-box reduction R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_\mathsf{f}]}$ for all public key encryption scheme in the setup-free model Π_f. By similar discussion, we show that there does not exists any black-box reduction R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{f}]}$ for all digital signature scheme in the setup-free model Σ_f.

Definition 5 (Non-interactive Hardness Problem.)**.** *A non-interactive cryptographic problem $P = (\mathsf{IGen}, \mathsf{IVer})$ consists of two efficient algorithms:*

IGen. *The instance generation algorithm takes as input the security parameter k and outputs an instance y.*

IVer. *The instance verification algorithm takes as input a value x as well as an instance y of a cryptographic problem, and outputs a decision bit.*

We say that a PPT algorithm A solves P if the probability that $\mathsf{A}(y)$ outputs x' such that $\mathsf{IVer}(x', y) = 1$ is non-negligible. We say that P is hard if no efficient algorithm solves it.

Theorem 1. *For all public key encryption scheme in the setup-free model Π_{f}, if P is a (non-interactive) computationally hard problem, there does not exist black-box reduction R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_{\mathsf{f}}]}$.*

Proof. First, we explain the overview of this proof. In the first step of this proof, $\mathsf{OW\text{-}CPA}$ adversary B is constructed by using a black box reduction R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_{\mathsf{f}}]}$. Since $\mathsf{IND\text{-}SCCA}$ adversary is constructed from B trivially, P can be solved by combining R and B. Since this contradicts P is a computationally hard problem, we obtain the impossibility that there does not exist R.

Towards a contradiction, we assume that a black-box reduction R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_{\mathsf{f}}]}$ is given. Then, the theorem is proven by constructing another algorithm B which breaks Π_{f} in the sense of $\mathsf{OW\text{-}CPA}$ ($\mathsf{A}_{\mathsf{OW\text{-}CPA}[\Pi_{\mathsf{f}}]}$).

We can construct such B by using R as follows. B first is given a public key and a ciphertext (pk^*, c^*) from OW challenger. B generate an instance of the problem P; $y \leftarrow \mathsf{IGen}(k)$, and inputs y to R in order to run R. Since R can simulate SCCA oracle SD, B obtain m^* such that $m^* \leftarrow \mathsf{Dec}_{sk^*}(c^*)$ by submitting (pk^*, c^*) to R. Finally, B outputs m^* as an answer of OW. Therefore, B works as a successful $\mathsf{OW\text{-}CPA}$ adversary $\mathsf{A}_{\mathsf{OW\text{-}CPA}[\Pi_{\mathsf{f}}]}$.

Since an $\mathsf{OW\text{-}CPA}$ adversary is easily converted to an $\mathsf{IND\text{-}SCCA}$ adversary, we obtain an $\mathsf{IND\text{-}SCCA}$ adversary B' converted from B. Now, we obtain a solver of P by combining B' and R. It can be explicitly constructed if we are given any implementation of R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_{\mathsf{f}}]}$, and this contradicts that P is computationally hard problem. □

Theorem 2. *For all digital signature scheme in the setup-free model Σ_{f}, if P is a (non-interactive) computationally hard problem, there does not exist black-box reduction R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_{\mathsf{f}}]}$.*

Proof. First, we explain the overview of this proof. In the first step of this proof, $\mathsf{UuF\text{-}KOA}$ adversary B is constructed by using a black box reduction R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_{\mathsf{f}}]}$. Since $\mathsf{EuF\text{-}SCMA}$ adversary is constructed from B trivially, P can be solved by combining R and B. Since this contradicts P is a computationally hard problem, we obtain the impossibility that there does not exist R.

Towards a contradiction, we assume that a black-box reduction R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_{\mathsf{f}}]}$ is given. Then, the theorem is proven by constructing another algorithm B which breaks Σ_{f} in the sense of $\mathsf{UuF\text{-}KOA}$ ($\mathsf{A}_{\mathsf{UuF\text{-}KOA}[\Sigma_{\mathsf{f}}]}$).

We can construct such B by using R as follows. B first is given a public key and a ciphertext (pk^*, m^*) from UuF challenger. B generate an instance of the problem P; $y \leftarrow \mathsf{IGen}(k)$, and inputs y to R in order to run R. Since R can simulate SCMA oracle SS, B obtain σ^* such that $1 \leftarrow \mathsf{Ver}_{sk^*}(m^*, \sigma^*)$ by submitting (pk^*, m^*) to R. Finally, B outputs σ^* as an answer of UuF. Therefore, B works as a successful $\mathsf{UuF\text{-}KOA}$ adversary $\mathsf{A}_{\mathsf{UuF\text{-}KOA}[\Sigma_{\mathsf{f}}]}$.

Since an $\mathsf{UuF\text{-}KOA}$ adversary is easily converted to an $\mathsf{EuF\text{-}SCMA}$ adversary, we obtain an $\mathsf{EuF\text{-}SCMA}$ adversary B' converted from B. Now, we obtain a solver of P by combining B' and R. It can be explicitly constructed if we are given any implementation of R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_{\mathsf{f}}]}$, and this contradicts that P is computationally hard problem. □

Remark 1. *In Theorem 1 and 2, we prove impossibility results for* $\mathsf{IND\text{-}SCCA}/\mathsf{EuF\text{-}SCMA}$ *security in the standard model. On the other hand, there exist several schemes that is* $\mathsf{IND\text{-}SCCA}/\mathsf{EuF\text{-}SCMA}$

secure in the random oracle model. We show several public key encryption and digital signature schemes which are secure under the strong attack model in the random oracle model. We prove that DHIES scheme and Schnorr signature scheme are secure as examples in Appendix A. This result is similar to the results of [10].

4 Impossibility Results in the Setup Model

In this section, we show that there does not exists *setup-preserving* black-box (SPBB) reduction R such that $P \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_s]}$ for all digital signature scheme in the setup model Σ_s and all $\mathsf{GOAL\text{-}ATK}$ if ATK is weaker than SCMA. Here, P is a $\mathsf{GOAL\text{-}ATK}$ computationally hard problem on a setup model scheme. By similar discussion, we that there does not exists setup-preserving black-box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_s]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_s]}$ for all public key encryption scheme in the setup model Π_s.
Setup Preserving Black Box Reduction. Black-box reduction R is called a "setup-preserving black-box (SPBB) reduction" if R makes oracle calls to the adversary *with the same common parameter I* as its own input[2]. Here, since we assume that the solver of P is equivalent to $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}}$, we also assume that the input of $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}}$ includes the common parameter I explicitly. A SPBB reduction is transitive, that is, if there exist SPBB reductions R_1 and R_2 such that $\mathsf{A}_{\mathsf{GOAL1-ATK1}} \Leftarrow_{R_1} \mathsf{A}_{\mathsf{GOAL2-ATK2}}$ and $\mathsf{A}_{\mathsf{GOAL3-ATK3}} \Leftarrow_{R_2} \mathsf{A}_{\mathsf{GOAL1-ATK1}}$, there exists a SPBB reduction $R_3 = R_1 \circ R_2$ such that $\mathsf{A}_{\mathsf{GOAL3-ATK3}} \Leftarrow_{R_3} \mathsf{A}_{\mathsf{GOAL2-ATK2}}$.

Theorem 3. *For all public key encryption scheme in the setup model Π_s, there does not exist a setup-preserving black-box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_s]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_s]}$ where GOAL is harder than IND or ATK is weaker than SCCA.*

Proof. We prove this theorem by combining the following two lemmas. In Lemma 1, we prove this theorem in the case that GOAL is harder than IND In Lemma 2, we prove this theorem in the case that ATK is weaker than SCCA.

Lemma 1. *For all public key encryption scheme in the setup model Π_s, if Π_s is $\mathsf{GOAL\text{-}ATK}$ secure, there does not exist a setup-preserving black-box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_s]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_s]}$ where GOAL is harder than IND.*

Proof. We assume that a SPBB R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_s]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_s]}$ is given. We first treat with the case when ATK is weaker than SCCA, and then the case when SCCA is stronger than ATK.

(i) The case when ATK is weaker than SCCA. First, we prove the case that ATK is weaker than SCCA. We can construct such $\mathsf{GOAL\text{-}SCCA}$ adversary B by using R as follows. B first is given a GOAL challenge (I, y) from a GOAL challenger. B inputs (I, y) to R in order to run R. Then, R starts interacting with a (virtual) oracle O_{ATK} (which is determined by ATK) and a (virtual) $\mathsf{IND\text{-}SCCA}$ adversary on Π_s by inputting (I, pk). Here, since R is setup-preserving black-box reduction, R inputs the same I as the input of SCCA which B applies. When R submits a query to the virtual O_{ATK}, B responds to it in such a way that B uses his own strong decryption oracle SD, and returns the answer from O_{ATK} as it is. Now, SCCA is stronger than ATK, R can simulate O_{ATK} using SD. At some point, B is enforced to commit two plaintexts m_0 and m_1 which will be challenged, and R returns the challenge ciphertext $\tilde{c}_b \leftarrow \mathsf{Enc}_{pk}(m_b)$. B submits $(pk, \tilde{c}_b)$ to SD and takes m_b such that $m_b \leftarrow \mathsf{Dec}_{I,sk}(\tilde{c}_b)$. B submits b to R and R outputs the answer x of GOAL. Finally, B outputs x. Therefore, B works as a successful $\mathsf{GOAL\text{-}SCCA}$ adversary $\mathsf{A}_{\mathsf{GOAL\text{-}SCCA}[\Pi_s]}$.

[2] This similar concept was introduced in [16].

Since an GOAL-SCCA adversary is easily converted to an IND-SCCA adversary, we obtain an IND-SCCA adversary B' converted from B. Now, we obtain an GOAL-ATK adversary by combining B' and R. It can be explicitly constructed if we are given any implementation of R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_\mathsf{s}]}$, and this contradicts that Π_s is GOAL-ATK secure.

(ii) The case when SCCA is weaker than ATK. Second, we prove the case that SCCA is weaker than ATK. Then, this case is proven by constructing another algorithm B which breaks Π_s in the sense of GOAL-ATK. We can construct such GOAL-ATK adversary B by using R as follows. B first is given a GOAL challenge (I,y) from a GOAL challenger. B inputs (I,y) to R in order to run R. Then, R starts interacting with a (virtual) oracle O_{ATK} and a (virtual) IND-SCCA adversary on Π_s by inputting (I,pk). Here, since R is setup-preserving black-box reduction, R inputs the same I as the input of SCCA which B applies. When R submits a query to the virtual O_{ATK}, B responds to it in such a way that B uses his own O_{ATK}, and returns the answer from O_{ATK} as it is. Now, SCCA is weaker than ATK, R can simulate O_{ATK} using SD.

At some point, B is enforced to commit two plaintexts m_0 and m_1 which will be challenged, and R returns the challenge ciphertext $\tilde{c}_b \leftarrow \mathsf{Enc}_{pk}(m_b)$. Now, since SCCA is weaker than ATK, R can simulate SD using O_{ATK} and SD can outputs m_b, B can obtain m_b such that $m_b \leftarrow \mathsf{Dec}_{I,sk}(\tilde{c}_b)$ using O_{ATK}. B submits b to R and R outputs the answer x of GOAL. Finally, B outputs x. Therefore, B works as a successful GOAL-ATK adversary $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_\mathsf{s}]}$. Now, we obtain an GOAL-ATK adversary by combining B. It can be explicitly constructed if we are given any implementation of R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_\mathsf{s}]}$, and this contradicts that Π_s is GOAL-ATK secure. □

Lemma 2. *For all public key encryption scheme in the setup model Π_s, there does not exist a setup-preserving black-box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_\mathsf{s}]}$ where* ATK *is weaker than* SCCA.

First, we explain the overview of this proof. This proof is similar to Theorem1. In the first step of this proof, OW-ATK adversary B is constructed by using a black box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_\mathsf{s}]}$. Since IND-SCCA adversary is constructed from B trivially, $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_\mathsf{s}]}$ can be solved by combining R and B. Since this contradicts Π_s is GOAL-ATK secure, we obtain the impossibility that there does not exist R.

Towards a contradiction, we assume that a black-box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_\mathsf{s}]}$ is given. Then, the theorem is proven by constructing another algorithm B which breaks Π_s in the sense of OW-ATK ($\mathsf{A}_{\mathsf{OW\text{-}ATK}[\Pi_\mathsf{s}]}$).

We can construct such B by using R as follows. B first is given a public key and a ciphertext (pk^*,I^*,c^*) from OW challenger. B generates a GOAL challenge y, and inputs (I^*,y) to R in order to run R. When R submits a query to the virtual O_{ATK}, B responds to it in such a way that B uses his own O_{ATK}, and returns the answer from O_{ATK} as it is. Since R can simulate SCCA oracle, B obtain m^* such that $m^* \leftarrow \mathsf{Dec}_{I^*,sk^*}(c^*)$ by submitting (pk^*,c^*) to R. Notice that SCCA oracle is performed on same common parameter I^*. Finally, B outputs m^* as an answer of OW. Therefore, B works as a successful OW-ATK adversary $\mathsf{A}_{\mathsf{OW\text{-}ATK}[\Pi_\mathsf{s}]}$.

Since an OW-ATK adversary is easily converted to an IND-SCCA adversary, we obtain an IND-SCCA adversary B' converted from B. Now, we obtain an GOAL-ATK adversary by combining B' and R. It can be explicitly constructed if we are given any implementation of R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Pi_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{IND\text{-}SCCA}[\Pi_\mathsf{s}]}$, and this contradicts that Π_s is GOAL-ATK secure. □

Theorem 4. *For all digital signature scheme in the setup model Σ_s, there does not exist a setup-preserving black-box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{s}]}$ where* GOAL *is harder than* EuF *or* ATK *is weaker than* SCMA.

Proof. We prove this theorem by combining the following two lemmas. In Lemma 1, we prove this theorem in the case that GOAL is harder than EuF In Lemma 2, we prove this theorem in the case that ATK is weaker than SCMA.

Lemma 3. *For all public key encryption scheme in the setup model Σ_s, if Σ_s is GOAL-ATK secure, there does not exist a setup-preserving black-box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{s}]}$ where GOAL is harder than EuF.*

Proof. We assume that a SPBB R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{s}]}$ is given. Then, this lemma is proven by constructing another algorithm B which breaks Σ_s in the sense of GOAL-SCMA or GOAL-ATK.

First, we prove the case that ATK is weaker than SCMA. We can construct such GOAL-SCMA adversary B by using R as follows. B first is given a GOAL challenge (I,y) from a GOAL challenger. B inputs (I,y) to R in order to run R. Then, R starts interacting with a (virtual) oracle O_ATK (which is determined by ATK) and a (virtual) EuF-SCMA adversary on Σ_s by inputting (I,pk). Here, since R is setup-preserving black-box reduction, R inputs the same I as the input of SCMA which B applies. When R submits a query to the virtual O_ATK, B responds to it in such a way that B uses his own strong signing oracle SS, and returns the answer from O_ATK as it is. Now, SCMA is stronger than ATK, R can simulate O_ATK using SS. At some point, B submits (pk,m^*) to his own strong signing oracle and receives σ^* where m^* is chosen randomly. B submits (m^*,σ^*) to R and R outputs the answer x of GOAL. Finally, B outputs x. Therefore, B works as a successful GOAL-SCMA adversary $\mathsf{A}_{\mathsf{GOAL\text{-}SCMA}[\Sigma_\mathsf{s}]}$.

Since an GOAL-SCMA adversary is easily converted to an EuF-SCMA adversary, we obtain an EuF-SCMA adversary B' converted from B. Now, we obtain an GOAL-ATK adversary by combining B' and R. It can be explicitly constructed if we are given any implementation of R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{s}]}$, and this contradicts that Σ_s is GOAL-ATK secure.

Second, we prove the case that SCMA is weaker than ATK. Then, this case is proven by constructing another algorithm B which breaks Σ_s in the sense of GOAL-ATK. We can construct such GOAL-ATK adversary B by using R as follows. B first is given a GOAL challenge (I,y) from a GOAL challenger. B inputs (I,y) to R in order to run R. Then, R starts interacting with a (virtual) oracle O_ATK and a (virtual) EuF-SCMA adversary on Σ_s by inputting (I,pk). Here, since R is setup-preserving black-box reduction, R inputs the same I as the input of SCMA which B applies. When R submits a query to the virtual O_ATK, B responds to it in such a way that B uses his own O_ATK, and returns the answer from O_ATK as it is.

Now, since SCMA is weaker than ATK, R can simulate SS using O_ATK and B can generate (m^*,σ^*) using SS such that $1 \leftarrow \mathsf{Dec}_{I,sk}(m^*,\sigma^*)$ with O_ATK. B submits b to R and R outputs the answer x of GOAL. Finally, B outputs x. Therefore, B works as a successful GOAL-ATK adversary $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]}$. Now, we obtain an GOAL-ATK adversary by combining B. It can be explicitly constructed if we are given any implementation of R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{s}]}$, and this contradicts that Σ_s is GOAL-ATK secure. □

Lemma 4. *For all public key encryption scheme in the setup model Σ_s, there does not exist a setup-preserving black-box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{s}]}$ where ATK is weaker than SCMA.*

First, we explain the overview of this proof. This proof is similar to Theorem1. In the first step of this proof, UuF-ATK adversary B is constructed by using a black box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{s}]}$. Since EuF-SCMA adversary is constructed from B trivially, $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]}$ can be solved by combining R and B. Since this contradicts Σ_s is GOAL-ATK secure, we obtain the impossibility that there does not exist R.

Towards a contradiction, we assume that a black-box reduction R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{s}]}$ is given. Then, the theorem is proven by constructing another algorithm B which breaks Σ_s in the sense of UuF-ATK ($\mathsf{A}_{\mathsf{UuF\text{-}ATK}[\Sigma_\mathsf{s}]}$).

We can construct such B by using R as follows. B first is given a public key and a ciphertext (pk^*, I^*, m^*) from UuF challenger. B generates a GOAL challenge y, and inputs (I^*, y) to R in order to run R. When R submits a query to the virtual O_{ATK}, B responds to it in such a way that B uses his own O_{ATK}, and returns the answer from O_{ATK} as it is. Since R can simulate SCMA oracle, B obtain σ^* such that $1 \leftarrow \mathsf{Ver}_{I^*,pk^*}(m^*, \sigma^*)$ by submitting (pk^*, m^*) to R. Notice that SCMA oracle is performed on same common parameter I^*. Finally, B outputs σ^* as an answer of UuF. Therefore, B works as a successful UuF-ATK adversary $\mathsf{A}_{\mathsf{UuF\text{-}ATK}[\Sigma_\mathsf{s}]}$.

Since an UuF-ATK adversary is easily converted to an EuF-SCMA adversary, we obtain an EuF-SCMA adversary B' converted from B. Now, we obtain an GOAL-ATK adversary by combining B' and R. It can be explicitly constructed if we are given any implementation of R such that $\mathsf{A}_{\mathsf{GOAL\text{-}ATK}[\Sigma_\mathsf{s}]} \Leftarrow_R \mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_\mathsf{s}]}$, and this contradicts that Σ_s is GOAL-ATK secure. □

In this section, we show impossibility results of SCMA/SCCA in the standard model. Whereas, we show that there exists scheme is secure in SCMA/SCCA model in the *random oracle model*, and it is possible that digital signature scheme or public key encryption scheme in *setup* model is secure in SCMA/SCCA model.

5 How to Construct IND-SCCA Secure Public Key Encryption

In this section, we discuss the essential mechanism to construct IND-SCCA secure public key encryption scheme in the standard model.

During the security proof, a simulator B should simulate a SCCA oracle *SD*, that is B should decrypt a ciphertext under arbitrarily chosen public key. If B use different parameter for each public key when B simulates *SD*, B should create an exponential number of parameter in order to decrypt under any *pk*. One solution to the problem is to decrypt ciphertexts under any public key using a same parameter.

For example, IND-SCCA secure scheme can be constructed by using similar technique of the Naor-Yung paradigm [14]. Then, a ciphertext contains three IND-CPA secure encryptions of the same plaintext under each user's two public key (pk_1, pk_2) and a common parameter I, along with a non-interactive zero-knowledge (NIZK) proof that indeed the same plaintext were encrypted. During the security proof, first, a simulator will generate s as a secret key of I. Next, the simulator generates I from s as the common parameter and run a IND-SCCA adversary on I. Note that in order to implement the strong decryption oracle *SD*, the simulator only needs to decrypt one ciphertext component which depends on I and rely on the soundness of the NIZK proof. Since the simulator generate I, this security proof does not use setup-preserving black-box manner. So, this construction does not contradict the impossibility result in Sec. 3. From above discussion, IND-SCCA scheme can be constructed in the setup model.

References

[1] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES. In *Proc. of the Cryptographers' Track at RSA Conference 2001 (CT-RSA'01), San Francisco, CA, USA, LNCS*, volume 2020, pages 143–158. Springer-Verlag, April 2001.

[2] Manuel Barbosa and Pooya Farshim. Relations among notions of complete non-malleability: Indistinguishability characterisation and efficient construction without random oracles. In *Proc. of the 15th Australasian Conference on Information Security and Privacy (ACISP'10), Sydney, Australia, LNCS*, volume 6168, pages 145–163. Springer-Verlag, July 2010.

[3] Manuel Barbosa and Pooya Farshim. Strong Knowledge Extractors for Public-Key Encryption Schemes. In *Proc. of the 15th Australasian Conference on Information Security and Privacy (ACISP'10), Sydney, Australia, LNCS*, volume 6168, pages 164–181. Springer-Verlag, July 2010.

[4] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among Notions of Security for Public-Key Encryption Schemes. In *Proc. of the 18th Annual International Cryptology Conference (CRYPTO'98), Santa Barbara, California, USA, LNCS*, volume 1462, pages 26–45. Springer-Verlag, August 1998.

[5] Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements. In *Proc. of the 19th International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'00), Bruges, Belgium, LNCS*, volume 1807, pages 259–274. Springer-Verlag, May 2000.

[6] Dan Boneh and Matthew Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM Journal on Computing*, 32(3):586–615, November 2003.

[7] Alexander Dent, Benoit Libert, and Kenneth Paterson. Certificateless Encryption Schemes Strongly Secure in the Standard Model. In *Proc. of the 11th International Workshop on Practice and Theory in Public-Key Cryptography (PKC'08), Barcelona, Spain, LNCS*, volume 4939, pages 344–359. Springer-Verlag, March 2008.

[8] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable Cryptography. *SIAM Journal on Computing*, 45(4):727–784, December 2003.

[9] Amos Fiat and Adi Shamir. How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Proc. of the 6th Annual International Cryptology Conference (CRYPTO'86), Santa Barbara, California, USA, LNCS*, volume 263, pages 186–194. Springer-Verlag, August 1986.

[10] Marc Fischlin. Completely Non-malleable Schemes. In *Proc. of the 32nd International Colloquium on the Automata, Languages and Programming (ICALP'05),Lisbon, Portugal, LNCS*, volume 3580 of *LNCS*, pages 779–790. Springer-Verlag, July 2005.

[11] S. Goldwasser, S. Micali, and R. Rivest. A Digital Signature Scheme against Adaptive Chosen Message Attack. *SIAM Journal on Computing*, 17(2):281–308, April 1988.

[12] Benoı̂t Libert and Moti Yung. Efficient Completely Non-malleable Public Key Encryption. In *Proc. of the 37nd International Colloquium on the Automata, Languages and Programming (ICALP'10), Bordeaux, France, LNCS*, volume 6198, pages 127–139. Springer-Verlag, July 2010.

[13] Alfred Menezes and Nigel Smart. Security of signature schemes in a multi-user setting. *Designs, Codes and Cryptography*, 33(3):261–274, November 2004.

[14] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proc. of the 22nd annual ACM symposium on Theory of computing (STOC'90), Baltimore, Maryland, USA*, pages 427–437. ACM Press, May 1990.

[15] T. Okamoto and D. Pointcheval. REACT: Rapid enhanced-security asymmetric cryptosystem transform. In *Proc. of the Cryptographer's Track at RSA Conference 2001 (CT-RSA'01), San Francisco, CA, USA, LNCS*, volume 2020, pages 159–174. Springer-Verlag, April 2001.

[16] Pascal Paillier and Jorge L. Villar. Trading One-Way Against Chosen-Ciphertext Security in Factoring-Based Encryption. In *Proc. of the 12th International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT'06), Shanghai, China, LNCS*, volume 4284, pages 252–266. Springer-Verlag, December 2006.

[17] D. Pointcheval. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, December 2000.

[18] C. P. Schnorr. Efficient identification and signatures for smart cards. In *Proc. of the 9th Annual International Cryptology Conference (CRYPTO'89), Santa Barbara, California, USA, LNCS*, volume 435, pages 239–252. Springer-Verlag, August 1989.

[19] C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, January 1991.

[20] Brent Waters. Efficient identity-based encryption without random oracles. In *Proc. of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Aarhus, Denmark, LNCS*, volume 3494, pages 114–127. Springer-Verlag, May 2005.

A Secure Schemes in the Random Oracle Model

In this section, we show a public key encryption/digital signature scheme which is proved to be IND-SCCA/ EuF-SCMA secure in the *random oracle model*, in order to show that the impossibility result in Section 3. does not cover random oracle constructions. Specifically we show that the DHIES [1] with a slight modification is actually IND-SCCA secure in the random oracle model.

A.1 Computationally hard Problem

In this subsection, we define discrete logarithm assumption and gap Diffie-Hellman assumption.

Definition 6 (Gap Diffie-Hellman Assumption). *Let $\mathbb{G}$ be a group of prime order p. We say that the* (τ,ε)-GDH assumption on $\mathbb{G}$ *holds when for all τ-time algorithm* A *it holds that* $\Pr[\mathsf{A}^{\mathscr{O}}(g,g^{\alpha},g^{\beta}) = g^{\alpha\beta}] \leq \varepsilon$ *where the probability is taken over the random choices of α, β and the generator g here the oracle $\mathscr{O}(g,g^{a},g^{b},g^{c})$ returns* 1 *when $ab = c$ and returns* 0 *otherwise.*

Definition 7 (Discrete Logarithm Assumption). *The discrete logarithm (DL) problem in $\mathbb{G}$ is defined as follows. We say that a PPT algorithm* A *has an advantage $\mathsf{Adv}_{\mathsf{A}}^{\mathsf{DL}}(l)$ in solving the DL problem in $\mathbb{G}$ if $\mathsf{Adv}_{\mathsf{A}}^{\mathsf{DL}}(l) = Pr[\mathsf{A}(g^{x},g) = x : x \leftarrow_R \mathbb{Z}_p, g \in \mathbb{G}]$. We say that the DL assumption holds in $\mathbb{G}$ if no PPT algorithm has a non-negligible $\mathsf{Adv}_{\mathsf{A}}^{\mathsf{DL}}(l)$ in l in solving the DL problem in $\mathbb{G}$.*

A.2 DHIES scheme

First, we show that the DHIES [1] with a slight modification is actually IND-SCCA secure in the random oracle model. For simplicity of presentation, we only give a brief sketch of a proof that the KEM part of the scheme is IND-SCCA secure. Even though no KEM/DEM composition theorem is known for SCCA security, the full-fledged DHIES can be proved to be IND-SCCA secure with a natural extension of the following.

For completeness we give the concrete description of the KEM part of the DHIES public key encryption. Let $\mathbb{G}$ be a multiplicative group of a prime order q. The DHIES key encapsulation mechanism consists of the following three algorithms:

Gen**:** The key generation algorithm Gen chooses a random generator g of $\mathbb{G}$ and a random $x \leftarrow \mathbb{Z}_q$ and computes $y \leftarrow g^{x}$. And then Gen chooses a cryptographic hash function H. The public key pk is set to $pk = (g,y,H)$ and the secret key sk is $sk = x$.

Enc**:** The encapsulation algorithm Enc takes $pk = (g,y,H)$ as input and chooses a random $r \leftarrow \mathbb{Z}_q$. The algorithm then computes $C \leftarrow g^{r}$ and $K \leftarrow H(pk,y^{r})$ $(= H(g,y,y^{r}))$. The ciphertext is C and its corresponding session key is K.

Dec**:** The decapsulation algorithm Dec takes a ciphertext C, a public key $pk = (g,y,H)$, and a secret key $sk = x$ and outputs $K = H(pk,C^{x})$.

As the following, it can be proven that the above DHIES key encapsulation mechanism has strong chosen-ciphertext security under gap Diffie-Hellman assumption:

Theorem 5. *If the gap Diffie-Hellman assumption holds on $\mathbb{G}$ and H is modeled as a random oracle, the DHIES key encapsulation mechanism is* IND-SCCA *secure.*

Proof. Given an adversary A against the DHIES key encapsulation mechanism, we will construct a simulator B solving the gap Diffie-Hellman problem. The construction of B is as follows:

Setup The simulator B is given a tuple $(g, g^{\alpha}, g^{\beta})$, and sets $pk^* = (g, g^{\alpha})$. Then $\mathscr{S}$ sends pk^* to the adversary A.

Strong Decapsulation Query (Phase I) When A makes a decapsulation query (pk, C), where pk is parsed as (g, y), B proceeds as follows: At first B searches for the entry of the form (g, y, C, Z, h) such that (g, y, C, Z) forms a DDH tuple (that is, the equation $\log_g C = \log_y Z$ holds). This operation can be done by querying (pk, C, Z) to B's own DDH oracle. (i) When such an entry is found, B returns h to A. (ii) Otherwise if no such an entry found, B chooses h at uniformly random, adds $(g, y, C, \perp, h)$ to the hash list, and returns h to A.

Phase I (Hash Query) When A makes a hash query (g, y, C, K), B proceeds as follows: (i) If the hash list contains an entry of the form $(g, y, C, \perp, h)$ (for some h) and (g, y, C, K) forms a DDH tuple (To examine whether (g, y, C, K) forms a DDH tuple, B can use an access to its own DDH oracle.), B replaces the entry $(g, y, C, \perp, h)$ with (g, y, C, K) and returns h to A. (ii) Otherwise if no such an entry is found or (g, y, C, K) does not form a DDH tuple, B chooses a uniformly random h, add (g, y, C, K)

Challenge When A requests a challenge, B sets C^* be g^{β} and K^* be an independent random session key. Then B sends (C^*, R^*) to A.

Phase II The adversary again submits decapsulation queries and hash queries. The simulator responds as before.

Guess Finally A outputs a bit b. The simulator tries to find from the hash list the entry of the form $(g, g^{\alpha}, g^{\beta}, Z, h)$ such that $(g, g^{\alpha}, g^{\beta}, K, h)$ forms a DDH tuple. If such an entry is found, B outputs Z as a solution for the gap Diffie-Hellman problem.

It can be proved that the above simulator can find the correct solution of the gap Diffie-Hellman problem with a high probability. Intuitively, it is due to the fact that the adversary A with a high advantage must queries $(g, g^{\alpha}, g^{\beta}, g^{\alpha\beta})$ to the random oracle with a high probability, because otherwise $H(g, g^{\alpha}, g^{\beta}, g^{\alpha\beta})$, which is what A has to guess, is independently distributed from the A's view. The formal proof can be given by adopting similar discussions in [6], but it is omitted due to the limitation of pages. □

A.3 Schnorr Signature

Next, we show that the Schnorr signature scheme is actually $\mathsf{EuF\text{-}SCMA}$ secure in the random oracle model. Schnorr's identification protocol was introduced [18, 19] as a means to prove knowledge of the discrete logarithm of a publicly known group element. Schnorr signatures derive from Schnorr's identification protocol by applying the Fiat-Shamir transform [9] with respect to a hash function $H : \{0,1\}^* \to \mathbb{Z}_q$. The Fiat-Shamir-transformed protocol is changed into a signature scheme by making it non-interactive. We define Schnorr Signature scheme in the setup-free model $\Sigma_{\mathsf{f}} = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ as follows.

Gen. Given a security parameter k, Gen picks $g \in \mathbb{Z}_p$, $x \in \mathbb{Z}_q$, and a hash function $H : \{0,1\}^* \to \mathbb{Z}_q$. Next, Gen computes $y = g^x \bmod p$. The output is $pk = (g, y, p, q, H)$ and $sk = x$.

Sig. Given a message $m \in \{0,1\}^*$, pk and sk, Sig picks a random $r \leftarrow \mathbb{Z}_q$, computes $h = g^r \bmod p, c = H(pk, h, m)$ and $s = r + cx$. The output signature is $\sigma = (s, c)$.

Ver. Given a message $m \in \{0,1\}^*$, pk and $\sigma = (s, c)$, Ver returns valid if $c = H(pk, g^s / y^c, m)$ and 0 otherwise.

As the following, it can be proven that the Schnorr signature scheme has strong chosen-message security:

Theorem 6. *If the discrete logarithm assumption holds and H is modeled as a random oracle, Schnorr signature scheme is* EuF-SCMA *secure.*

Proof (Sketch). Given an adversary A against the Schnorr signature scheme, we will construct a simulator B solving the discrete logarithm problem. The construction of B is as follows: B uses a counter *cnt*, initially set to 0.

Setup For given (g, y, p, q), B input $pk = (g, y, p, q)$ to $\mathsf{A}_{\mathsf{EuF\text{-}SCMA}[\Sigma_f]}$.

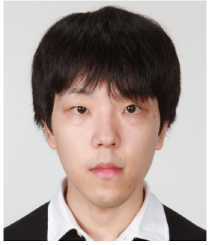
Hash Query When A makes hash query (pk_i, h, m), B proceeds as follows: (i) If the hash list contains an entry of the form (cnt, pk_i, h, m, c) (sor some c and cnt) returns c to A. (ii) Otherwise if no such an entry is found, B chooses a uniformly random h, add (cnt, pk_i, h, m, c) to the hash list and sets $cnt \leftarrow cnt + 1$.

Strong Chosen Message Query When A makes strong chosen message query (pk_i, m), A proceeds as follows: At first A chooses $(s, c) \leftarrow \mathbb{Z}_{q_i}$ randomly and responds them to A. Next, A computes $h = \frac{g^s}{y^c}$ and adds $(\perp, pk_i = (g_i, y_i, p_i, q_i), h, m, c)$ to the hash list.

Output Since A breaks EuF, A outputs (m_1^*, σ_1^*). Then, from the Forking Lemma [17], B obtain $(m_1^*, \sigma_1^* = (s_1^*, c_1^*))$ and $(m_2^*, \sigma_2^* = (s_2^*, c_2^*))$ such that $\frac{g^{s_1^*}}{y^{c_1^*}} = \frac{g^{s_2^*}}{y^{c_2^*}}$ and computes $x = \frac{s_1^* - s_2^*}{c_1^* - c_2^*}$. Finally, B outputs x as an answer of the discrete logarithm problem

□

Yutaka Kawai received B.E. and M.E. degrees from the University of Electro-Communications, Tokyo, Japan, in 2007 and 2009, respectively. He has been a doctor course student at the University of Tokyo since 2009. He is supported by JSPS research fellowships for young scientists.



Yusuke Sakai received his B.E. and M.E. degrees from the University of Electro-Communications, Tokyo, Japan, in 2009 and 2011, respectively. He has been currently a doctor course student in the University of Electro-Communications, Tokyo, Japan. He is presently engaged in research on cryptography. He received SCIS Paper Prize from IEICE in 2011 and the Best Student Paper Award in IWSEC 2010.

Noboru Kunihiro received his B. E., M. E. and Ph. D. in mathematical engineering and information physics from the University of Tokyo in 1994, 1996 and 2001, respectively. He is an Associate Professor of the University of Tokyo. He was a researcher of NTT Communication Science Laboratories from 1996 to 2002. He was a associate professor of the University of Electro-Communications from 2002 to 2008. His research interest includes cryptography and information security. He received the SCIS'97 Paper Prize and the Best Paper Award of IEICE in 2010.