

Relation between simulator-based and comparison-based definitions of semantic security

Yodai Watanabe^{1*} and Junji Shikata²

¹ Laboratory for Mathematical Neuroscience, RIKEN Brain Science Institute, 2-1 Hirosawa, Wako-shi, Saitama 351-0198, Japan (yodai@brain.riken.go.jp).

² Graduate School of Environment and Information Sciences, Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan (shikata@ynu.ac.jp).

April 25, 2003

Abstract. This paper studies the relation between simulator-based and comparison-based definitions of semantic security. If any side information of a plaintext is not accessible to an adversary, then these two notions are shown to be equivalent. Otherwise, the comparison-based notion is shown to be strictly stronger than the simulator-based one.

1 Introduction

The notion of semantic security is a direct formulation of the intuition of privacy[8]. An encryption scheme is called semantically secure if any adversary (a polynomial-time algorithm attacking an encryption scheme of interest) cannot extract, from a given ciphertext, any non-negligible information about the corresponding plaintext. Hence this notion can be regarded as a computational version of the perfect secrecy introduced in [11]. In considering provable security of practical encryption schemes (e.g. [2, 4, 12]), however, it is usually convenient to employ, as the security goal of the systems, another security notion called indistinguishability, which is rather artificial but equivalent to semantic security[6, 8, 13].

To formalize semantic security, as well as the other security notions, two different definitions can be used: namely, the simulator-based and comparison-based definitions (see [3]). The simulator-based definition requests that, for any adversary given a ciphertext, there exists a polynomial-time algorithm, called a simulator, which succeeds in the attack (i.e. can extract non-negligible information) without the ciphertext essentially as well as the adversary. The comparison-based definition requests that any adversary in possession of the ciphertext obtains no advantage over one which performs only random guesses. Since random guesses can be regarded as a special case of the simulation, the simulator-based notion may seem stronger than the comparison-based one. On the other hand, in the simulator-based definition,

* Research supported by the Special Postdoctoral Researchers Program of RIKEN (The Institute of Physical and Chemical Research).

there is no restriction on the computability of partial information which an adversary wishes to extract (see [6, 8] for such definitions), while in the comparison-based one, the partial information has to be generated from a polynomial-time algorithm. This may seem to show that the former is stronger than the latter. Regarding the notion of non-malleability[5], it has been shown that the simulator-based one is equivalent to the comparison-based one[3]. This paper concerns the case of semantic security in a more general framework where an adversary may take side information of a plaintext and the computability of partial information which an adversary wishes to extract is not restricted in the simulator-based case.

In this paper, we obtain the following results. If any side information of a plaintext is not accessible to an adversary, then these two notions are equivalent. Otherwise, the comparison-based notion is strictly stronger than the simulator-based one. The rest of this paper is organized as follows. In section 2, we provide the simulator-based and comparison-based definitions of semantic security. In section 3, we show that the comparison-based semantic security implies the simulator-based one. However, the converse does not hold in general. In section 4, we show that, when any side information of a plaintext is not accessible, the simulator-based semantic security implies the comparison-based one, but otherwise, the former does not imply the latter

2 Preliminaries

In this section, we provide two definitions of semantic security; one is based on simulator, and the other is based on comparison.

We begin with providing some definitions which will be used later.

Definition 1 (Public key encryption scheme). A public key encryption scheme is a triplet of algorithms, $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, such that

- the key generation algorithm \mathcal{K} is a probabilistic polynomial-time algorithm which takes a security parameter $k \in \mathbb{N}$ and outputs a pair (pk, sk) of matching public and secret keys,
- the encryption algorithm \mathcal{E} is a probabilistic polynomial-time algorithm which takes a public key pk and a plaintext x and outputs a ciphertext y ,
- the decryption algorithm \mathcal{D} is a deterministic polynomial-time algorithm which takes a secret key sk and a ciphertext y and outputs either a plaintext x or a special symbol \perp to indicate that the ciphertext is invalid,

where $\mathcal{D}_{sk}(\mathcal{E}_{pk}(x)) = x$ for all x and (pk, sk) .

Definition 2 (Negligible function). A function $\epsilon : \mathbb{N} \rightarrow \mathbb{R}$, $k \mapsto \epsilon(k)$, is called negligible if for every constant $c \geq 0$ there exists $k_c \in \mathbb{N}$ such that $|\epsilon(k)| < k^{-c}$ for all $k > k_c$.

The notion of semantic security was first introduced in [8], and later refined in [6]. The definitions formalize the intuition of privacy that whatever can be efficiently computed about a plaintext from its ciphertext can also be computed without the ciphertext. The following definition is slightly modified from the original definition[6] for the chosen plaintext attack (CPA) model so that it can be applied to the attacking model including the chosen ciphertext attacks (CCAs)[9,10]. Another version of the definition and related results can be found in [6]. See also [7] for a more general attacking model.

Definition 3 (Simulator-based semantic security). *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let A be a polynomial-time adversary and A' be a polynomial-time algorithm which simulates A (A' is called a simulator of A). Let f be a function (which may not be computable in polynomial-time). For $atk \in \{cpa, cca1, cca2\}$ and $k \in \mathbb{N}$, consider*

Experiment $\text{Exp}_{\mathcal{PE}, A, f}^{ss-atk}(k)$

$(pk, sk) \leftarrow \mathcal{K}(k); (X, s, h) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk); x \leftarrow X; y \leftarrow \mathcal{E}_{pk}(x); t \leftarrow \{s, h(x)\};$
 $(v, u) \leftarrow A_2^{\mathcal{O}_2(\cdot)}(t, y); \text{if } v = f(x, u, X) \text{ then } d \leftarrow 1 \text{ else } d \leftarrow 0;$
return d

Experiment $\text{Exp}_{\mathcal{PE}, A', f}^{ss-atk}(k)$

$(X, s, h) \leftarrow A'_1(k); x' \leftarrow X; t \leftarrow \{s, h(x')\}; (v, u) \leftarrow A'_2(t);$
if $v = f(x', u, X)$ **then** $d \leftarrow 1$ **else** $d \leftarrow 0;$
return d

where

$$\begin{aligned} \mathcal{O}_1(\cdot) &= \epsilon & \text{and } \mathcal{O}_2(\cdot) &= \epsilon & \text{for } atk = cpa \\ \mathcal{O}_1(\cdot) &= \mathcal{D}_{sk}(\cdot) & \text{and } \mathcal{O}_2(\cdot) &= \epsilon & \text{for } atk = cca1 \\ \mathcal{O}_1(\cdot) &= \mathcal{D}_{sk}(\cdot) & \text{and } \mathcal{O}_2(\cdot) &= \mathcal{D}_{sk}(\cdot) & \text{for } atk = cca2 \end{aligned}$$

with ϵ being the function which, on any input, returns the empty string. In the case of CCA2, A_2 is prohibited from asking its oracle to decrypt y . Let

$$\text{Adv}_{\mathcal{PE}, A, A', f}^{ss-atk}(k) = \Pr[\text{Exp}_{\mathcal{PE}, A, f}^{ss-atk}(k) = 1] - \Pr[\text{Exp}_{\mathcal{PE}, A', f}^{ss-atk}(k) = 1],$$

where the probability is taken over the internal coin tosses of all the algorithms. Then \mathcal{PE} is said to be secure in the sense of SSS-ATK if for any A there exists A' such that $\text{Adv}_{\mathcal{PE}, A, A', f}^{ss-atk}(k)$ is negligible for any f .

We now give the definition of the comparison-based semantic security according to the framework in [1].

Definition 4 (Comparison-based semantic security). Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and let $A = (A_1, A_2)$ be a polynomial-time adversary. For $atk \in \{cpa, cca1, cca2\}$, $b \in \{0, 1\}$ and $k \in \mathbb{N}$, consider

Experiment $\text{Exp}_{\mathcal{PE}, A}^{css-atk-b}(k)$

```

(pk, sk) ← K(k); (M, s, h) ← A1O1(·)(pk); x0, x1 ← M; y ← Epk(x1);
t ← {s, h(x1)}; (v, f) ← A2O2(·)(t, y); if v = f(xb) then d ← 1 else d ← 0;
return d

```

where

$$\begin{aligned}
\mathcal{O}_1(\cdot) &= \epsilon & \text{and } \mathcal{O}_2(\cdot) &= \epsilon & \text{for } atk = cpa \\
\mathcal{O}_1(\cdot) &= \mathcal{D}_{sk}(\cdot) & \text{and } \mathcal{O}_2(\cdot) &= \epsilon & \text{for } atk = cca1 \\
\mathcal{O}_1(\cdot) &= \mathcal{D}_{sk}(\cdot) & \text{and } \mathcal{O}_2(\cdot) &= \mathcal{D}_{sk}(\cdot) & \text{for } atk = cca2
\end{aligned}$$

with ϵ being the function which, on any input, returns the empty string. In the case of CCA2, A_2 is prohibited from asking its oracle to decrypt y . Let

$$\text{Adv}_{\mathcal{PE}, A}^{css-atk}(k) = \Pr[\text{Exp}_{\mathcal{PE}, A}^{css-atk-1}(k) = 1] - \Pr[\text{Exp}_{\mathcal{PE}, A}^{css-atk-0}(k) = 1],$$

where the probability is taken over the internal coin tosses of all the algorithms. Then \mathcal{PE} is said to be secure in the sense of CSS-ATK if $\text{Adv}_{\mathcal{PE}, A}^{css-atk}(k)$ is negligible for any A .

3 CSS-ATK implies SSS-ATK

In this and the next sections, we consider the relation between CSS-ATK and SSS-ATK. Remember that in definition 3 there is neither restriction to the computability of f nor need for the adversary to know f , while in definition 4 f has to be generated from a polynomial-time algorithm. Therefore it is not so trivial whether CSS-ATK implies SSS-ATK or not. However, as we will see below, it can be shown that CSS-ATK implies SSS-ATK.

Theorem 1. $\text{CSS-ATK} \Rightarrow \text{SSS-ATK}$.

Proof. Suppose that an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of CSS-ATK. Then \mathcal{PE} is shown to be secure in the sense of SSS-ATK as follows.

Let $B = (B_1, B_2)$ be an SSS-ATK adversary, i.e. an adversary which attacks \mathcal{PE} in the sense of SSS-ATK. We wish to show that for any B there exists a simulator $B' = (B'_1, B'_2)$ of B such that $\text{Adv}_{\mathcal{PE}, B', f}^{sss-atk}(k)$ is negligible for any f . So, for given

B , let us construct its simulator B' as

Algorithm $B'_1(k)$ $(pk', sk') \leftarrow \mathcal{K}(k);$ $(X, s, h) \leftarrow B_1^{\mathcal{O}'_1(\cdot)}(pk');$ $s' \leftarrow \{s, pk', sk', X\};$ return (X, s', h)	Algorithm $B'_2(t)$ $x \leftarrow X; y \leftarrow \mathcal{E}_{pk'}(x);$ $(v, u) \leftarrow B_2^{\mathcal{O}'_2(\cdot)}(t, y);$ return (v, u)
--	--

Note that the simulator B' can answer queries from B because it has the secret key sk' . To show that $\text{Adv}_{\mathcal{P}\mathcal{E}, B, B', f}^{ss-atk}(k)$ is negligible, we consider the CSS-ATK adversary $A = (A_1, A_2)$ constructed as

Algorithm $A_1^{\mathcal{O}_1(\cdot)}(pk)$ $(M, s, h) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk);$ return (M, s, h)	Algorithm $A_2^{\mathcal{O}_2(\cdot)}(t, y)$ $\hat{v} \leftarrow B_1^{\mathcal{O}_2(\cdot)}(t, y);$ $\hat{f} \leftarrow \hat{f}(x) := B_2^{\mathcal{O}_2(\cdot)}(t, \mathcal{E}_{pk}(x));$ return (\hat{v}, \hat{f})
--	---

It is now convenient to denote by E the experiment

Experiment E

$(pk, sk) \leftarrow \mathcal{K}(k); (X, s, h) \leftarrow B_1^{\mathcal{O}'_1(\cdot)}(pk); x_0, x_1 \leftarrow X;$
 $y_0 \leftarrow \mathcal{E}_{pk}(x_0); y_1, y'_1 \leftarrow \mathcal{E}_{pk}(x_1); t_0 \leftarrow \{s, h(x_0)\}; t_1 \leftarrow \{s, h(x_1)\};$
 $(v_0, u_0) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t_0, y_0); (v_1, u_1) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t_1, y_1); (v'_1, u'_1) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t_1, y'_1);$

Then the advantages $\text{Adv}_{\mathcal{P}\mathcal{E}, A}^{css-atk}(k)$ and $\text{Adv}_{\mathcal{P}\mathcal{E}, B, B', f}^{ss-atk}(k)$ can be written as

$$\begin{aligned} \text{Adv}_{\mathcal{P}\mathcal{E}, A}^{css-atk}(k) &= \Pr[E : v_1 = v'_1] - \Pr[E : v_1 = v_0], \\ \text{Adv}_{\mathcal{P}\mathcal{E}, B, B', f}^{ss-atk}(k) &= \Pr[E : v_1 = f(x_1, u_1, X)] - \Pr[E : v_1 = f(x_0, u_0, X)], \end{aligned}$$

respectively. Now let us introduce the random variable R to denote the coin tosses commonly used for computing v and u . Furthermore, let \mathcal{X} and \mathcal{R} be the set of all possible assignments of X and R respectively, and let $\Omega = \mathcal{X} \times \mathcal{X} \times \mathcal{R}$. Here, if we define the mapping of Ω into \mathbb{R} , $\mu : \Omega \rightarrow \mathbb{R}$, by

$$m_0 \times m_1 \times r \mapsto \Pr[x_0 = m_0, x_1 = m_1, R = r],$$

then the triplet $\mathcal{P} = (\Omega, 2^\Omega, \mu)$ constitutes a discrete probability space. Let \mathcal{A} be the set of all possible outputs from B . For $a \in \mathcal{A}$, we define the random variables on \mathcal{P} , X_a and Y_a , by writing

$$\begin{aligned} X_a &= p_1(a|m_0, m_1, r) - p_0(a|m_0, m_1, r), \\ Y_a &= q_1(a|m_0, m_1, r) - q_0(a|m_0, m_1, r), \end{aligned}$$

where we have introduced the notations

$$\begin{aligned} p_b(a|m_0, m_1, r) &= \Pr[E : v_b = a | x_0 = m_0, x_1 = m_1, R = r], \\ q_b(a|m_0, m_1, r) &= \Pr[E : f(x_b, u_b) = a | x_0 = m_0, x_1 = m_1, R = r]. \end{aligned}$$

Then the advantages $\text{Adv}_{\mathcal{PE},A}^{\text{css-atk}}(k)$ and $\text{Adv}_{\mathcal{PE},B,B',f}^{\text{sss-atk}}(k)$ are now expressed, in terms of X_a and Y_a , as

$$\begin{aligned} \text{Adv}_{\mathcal{PE},A}^{\text{css-atk}}(k) &= \frac{1}{2} \sum_{a \in \mathcal{A}} E_\mu[X_a^2], \\ \text{Adv}_{\mathcal{PE},B,B',f}^{\text{sss-atk}}(k) &= \frac{1}{2} \sum_{a \in \mathcal{A}} E_\mu[X_a Y_a], \end{aligned}$$

where $E_\mu[\cdot]$ denotes the expectation with respect to the probability measure μ . The above expressions may facilitate the comparison between the advantages. In fact it is easy to see that

$$E_\mu[X_a^2]E_\mu[Y_b^2] + E_\mu[X_b^2]E_\mu[Y_a^2] \geq 2E_\mu[X_a Y_a]E_\mu[X_b Y_b].$$

Furthermore, since q_0 and q_1 are conditional probabilities, it can be shown that

$$\sum_{a \in \mathcal{A}} E_\mu[Y_a^2] \leq 2.$$

Collecting these inequalities, we obtain

$$\text{Adv}_{\mathcal{PE},A}^{\text{css-atk}}(k) = p(1) - p(0) \geq (p'(1) - p'(0))^2 = (\text{Adv}_{\mathcal{PE},B,B',f}^{\text{sss-atk}}(k))^2.$$

Therefore, if \mathcal{PE} is secure in the sense of CSS-ATK, then $\text{Adv}_{\mathcal{PE},A}^{\text{css-atk}}(k)$ is negligible, and so $\text{Adv}_{\mathcal{PE},B,B',f}^{\text{sss-atk}}(k)$ is also negligible. This completes the proof. \square

We note that, in the above proof, it is essential that the function f may depend on the distribution X . On the other hand, it is not essential that f can depend on the output u , and so removing u from the definition does not reduce the strength of security of SSS-ATK.

4 Does SSS-ATK imply CSS-ATK?

In this section, we consider whether SSS-ATK implies CSS-ATK or not. Regarding the notion of non-malleability, it has been shown that the simulator-based one is equivalent to the comparison-based one provided the function h in our formulation is empty (see [3]). The same result also holds for the case of semantic security. That is, we can show the following theorem.

Theorem 2. *If h (in the definitions 3 and 4) is empty, then $SSS\text{-}ATK \Rightarrow CSS\text{-}ATK$.*

Proof. Suppose that an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of SSS-ATK. Then \mathcal{PE} is shown to be secure in the sense of CSS-ATK as follows.

Let $B = (B_1, B_2)$ be an CSS-ATK adversary. For given B , let us consider the SSS-ATK adversary constructed as

<p>Algorithm $A_1^{\mathcal{O}_1(\cdot)}(pk)$</p> <p>$(M, s, \emptyset) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk);$ $x_0, x_1 \leftarrow M; X \leftarrow \{x_0, x_1\}_U;$ $s' \leftarrow \{s, x_0, x_1\};$ return (X, s, \emptyset)</p>	<p>Algorithm $A_2^{\mathcal{O}_2(\cdot)}(t, y)$</p> <p>$(\hat{v}, \hat{f}) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t, y);$ if $(\hat{v} = \hat{f}(x_1) \wedge \hat{v} \neq \hat{f}(x_0))$ then $v \leftarrow 1;$ if $(\hat{v} = \hat{f}(x_0) \wedge \hat{v} \neq \hat{f}(x_1))$ then $v \leftarrow 0;$ else $v \leftarrow \{x_0, x_1\}_U;$ return $(v, 0)$</p>
---	---

where $\{x_0, x_1\}_U$ denotes the uniform distribution over $\{x_0, x_1\}$. Let \mathcal{S} be the set of all possible values of s , the second output from B_1 . For $\hat{s} \in \mathcal{S}$ and $b \in \{0, 1\}$, let us introduce $p(\hat{s})$ and $p(b|\hat{s})$ by writing

$$\begin{aligned}
 p(\hat{s}) &= \Pr[(pk, sk) \leftarrow \mathcal{K}(k); (M, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk) : s = \hat{s}], \\
 p(b|\hat{s}) &= \Pr[(pk, sk) \leftarrow \mathcal{K}(k); (M, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk); x_0, x_1 \leftarrow M; y \leftarrow \mathcal{E}_{pk}(x_b); \\
 &\quad (\hat{v}, \hat{f}) \leftarrow A_2^{\mathcal{O}_2(\cdot)}(s, y) : \hat{v} = \hat{f}(x_b) | s = \hat{s}],
 \end{aligned}$$

respectively. In the sequent discussion, we will assume that

$$\text{Adv}_{\mathcal{PE}, B}^{css-atk}(k) = \sum_{s \in \mathcal{S}} p(s) (p(1|s) - p(0|s)) \geq 0.$$

We can obtain the same result as below for the case where $\text{Adv}_{\mathcal{PE}, B}^{css-atk}(k) \leq 0$ only by changing the output $(v, 0)$ to $(\bar{v}, 0)$. Now, for the function f defined by

$$f(x, u, X) = f(x, X) = \begin{cases} 1 & \text{if } X = \{x_0, x_1\}_U \text{ and } x = x_1, \\ 0 & \text{if } X = \{x_0, x_1\}_U \text{ and } x = x_0, \end{cases}$$

the probability that A succeeds in the attack is written as

$$\begin{aligned}
 &\Pr[\text{Exp}_{\mathcal{PE}, A, f}^{sss-atk}(k) = 1] \\
 &= \Pr[(pk, sk) \leftarrow \mathcal{K}(k); (X, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk); x \leftarrow X; y \leftarrow \mathcal{E}_{pk}(x); \\
 &\quad (v, u) \leftarrow A_2^{\mathcal{O}_2(\cdot)}(s, y) : v = f(x, u, X)] \\
 &= \sum_{s \in \mathcal{S}} p(s) \left(p(1|s)(1 - p(0|s)) + \frac{1}{2} \{ p(1|s)p(0|s) + (1 - p(0|s))(1 - p(1|s)) \} \right) \\
 &= \frac{1}{2} + \frac{1}{2} \sum_{s \in \mathcal{S}} p(s) (p(1|s) - p(0|s)) = \frac{1}{2} + \frac{1}{2} \text{Adv}_{\mathcal{PE}, B}^{css-atk}(k).
 \end{aligned}$$

On the other hand, for the above f , the probability that A' succeeds in the attack is written as

$$\begin{aligned}
& \Pr[\text{Exp}_{\mathcal{P}\mathcal{E}, A', f}^{\text{sss-atk}}(k) = 1] \\
&= \Pr[(X, s) \leftarrow A'_1(k); x \leftarrow X; (v, u) \leftarrow A'_2(s) : v = f(x, u, X)] \\
&\leq \Pr[(\{x_0, x_1\}_U, s) \leftarrow A'_1(k); x \leftarrow \{x_0, x_1\}_U; (v, u) \leftarrow A'_2(s) : \\
&\quad v = f(x, u, \{x_0, x_1\}_U)] \\
&= \Pr[(\{x_0, x_1\}_U, s) \leftarrow A'_1(k); b \leftarrow \{0, 1\}_U; (v, u) \leftarrow A'_2(s) : \\
&\quad (b = 1 \wedge v = 1) \vee (b = 0 \wedge v = 0)] \\
&= \frac{1}{2} \Pr[(\{x_0, x_1\}_U, s) \leftarrow A'_1(k); (v, u) \leftarrow A'_2(s) : (v = 1) \vee (v = 0)] \leq \frac{1}{2}.
\end{aligned}$$

Hence, we obtain

$$\begin{aligned}
\text{Adv}_{\mathcal{P}\mathcal{E}, A, A', f}^{\text{sss-atk}}(k) &= \Pr[\text{Exp}_{\mathcal{P}\mathcal{E}, A, f}^{\text{sss-atk}}(k) = 1] - \Pr[\text{Exp}_{\mathcal{P}\mathcal{E}, A', f}^{\text{sss-atk}}(k) = 1] \\
&\geq \frac{1}{2} \text{Adv}_{\mathcal{P}\mathcal{E}, B}^{\text{css-atk}}(k).
\end{aligned}$$

Therefore, if $\mathcal{P}\mathcal{E}$ is secure in the sense of SSS-ATK, then $\text{Adv}_{\mathcal{P}\mathcal{E}, A, A', f}^{\text{sss-atk}}(k)$ is negligible, and so $\text{Adv}_{\mathcal{P}\mathcal{E}, B}^{\text{css-atk}}(k)$ is also negligible. This completes the proof. \square

We note that, in the above proof, it is essential that h is empty. Indeed, if h is not empty, then the inequality for $\Pr[\text{Exp}_{\mathcal{P}\mathcal{E}, A', f}^{\text{sss-atk}}(k) = 1]$ does not hold in general, because v and x (or b) are no longer independent. Hence it would be of interest to consider the case when h may not be empty. From the following theorem, we can see that it is crucial for the equivalence between SSS-ATK and CSS-ATK whether h is empty or not.

Theorem 3. *If h (in the definitions 3 and 4) may not be empty, then SSS-ATK $\not\equiv$ CSS-ATK.*

Proof. Suppose that an encryption scheme $\mathcal{P}\mathcal{E} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of SSS-ATK. We wish to show that there exists an encryption scheme $\mathcal{P}\mathcal{E}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is secure in the sense of SSS-ATK, but not secure in the sense of CSS-ATK.

Let $g(x)$ be a function of x computable in polynomial-time, and $\mathcal{P}\mathcal{E}'$ be the modification of $\mathcal{P}\mathcal{E}$ given by

Algorithm $\mathcal{K}'(k)$ $(pk, sk) \leftarrow \mathcal{K}(k);$ return (pk, sk)	Algorithm $\mathcal{E}'_{pk}(x)$ $y \leftarrow \mathcal{E}_{pk}(x); w \leftarrow g(x);$ $y' \leftarrow \{y, w\};$ return y'	Algorithm $\mathcal{D}'_{sk}(y')$ $\hat{x} \leftarrow \mathcal{D}_{sk}(y);$ return \hat{x}
--	---	---

Then, we first show that $\mathcal{P}\mathcal{E}'$ is secure in the sense of SSS-ATK. For this purpose, it suffices to show the following lemma.

Lemma 1. \mathcal{PE} is SSS-ATK $\Leftrightarrow \mathcal{PE}'$ is SSS-ATK.

Proof. The converse part is trivial. Hence we show the direct part. Suppose that $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of SSS-ATK. Then \mathcal{PE}' is shown to be secure in the sense of SSS-ATK as follows.

Let $B = (B_1, B_2)$ be an SSS-ATK adversary attacking \mathcal{PE}' . For given B , let us consider the SSS-ATK adversary $A = (A_1, A_2)$ attacking \mathcal{PE} constructed as

$$\begin{array}{l|l} \text{Algorithm } A_1^{\mathcal{O}_1(\cdot)}(pk) & \text{Algorithm } A_2^{\mathcal{O}_2(\cdot)}(t', y) \\ (X, s, h) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk); & (v, u) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t', y, w); \\ h' \leftarrow \{h, g\}; & \text{return } (v, u) \\ \text{return } (X, s, h') & \end{array}$$

where we have defined t' by $t' = \{t, w\} = \{\{s, h(x)\}, g(x)\}$. Remember that \mathcal{PE} is supposed to be secure in the sense of SSS-ATK. Thus there exists a simulator $A' = (A'_1, A'_2)$ of the adversary A such that $\text{Adv}_{\mathcal{PE}, A, A', f}^{\text{sss-atk}}(k)$ is negligible for any f . By using such A' , we can construct the simulator $B' = (B'_1, B'_2)$ of B as

$$\begin{array}{l|l} \text{Algorithm } B'_1(k) & \text{Algorithm } B'_2(t) \\ (X, s, h) \leftarrow A'_1(k); & (v, u) \leftarrow A'_2(t); \\ \text{return } (X, s, h) & \text{return } (v, u) \end{array}$$

It is clear from the above constructions that

$$\text{Adv}_{\mathcal{PE}, A, A', f}^{\text{sss-atk}}(k) = \text{Adv}_{\mathcal{PE}, B, B', f}^{\text{sss-atk}}(k)$$

for any f . Since $\text{Adv}_{\mathcal{PE}, A, A', f}^{\text{sss-atk}}(k)$ is negligible for any f , so is $\text{Adv}_{\mathcal{PE}, B, B', f}^{\text{sss-atk}}(k)$. This completes the proof. \square

Next, we show that \mathcal{PE}' is not secure in the sense of CSS-ATK.

Lemma 2. \mathcal{PE}' is not CSS-ATK.

Proof. We show that there exists an CSS-ATK adversary $A = (A_1, A_2)$ attacking \mathcal{PE}' such that $\text{Adv}_{\mathcal{PE}', A}^{\text{css-atk}}(k)$ is not negligible. For this purpose, we now define the function g by

$$g(x) := \text{msb}(x),$$

where $\text{msb}(x)$ denotes the most significant bit of x . Here let us construct the adversary A by

$$\begin{array}{l|l} \text{Algorithm } A_1^{\mathcal{O}_1(\cdot)}(pk) & \text{Algorithm } A_2^{\mathcal{O}_2(\cdot)}(t, y') \\ X \leftarrow \{0, 1\}_U^k; s \leftarrow \emptyset; h \leftarrow \emptyset; & f \leftarrow f(x) := \text{msb}(x); \\ \text{return } (X, s, h) & \text{return } (w, f) \end{array}$$

where $y' = \{y, w\}$ as above, and $\{0, 1\}_U^k$ is the uniform distribution over $\{0, 1\}^k$. Then it is clear from the above construction that

$$\text{Adv}_{\mathcal{PE}, A}^{\text{css-atk}}(k) = 1 - \frac{1}{2} = \frac{1}{2},$$

which is not negligible. This completes the proof. \square

These lemmas at once give that there exists an encryption scheme \mathcal{PE}' which is SSS-ATK but not CSS-ATK, so the theorem follows. \square

Note that, in the above proof, it is essential that h may not be empty. Indeed, if h is empty, then lemma 1 would not hold in general.

References

1. M. BELLARE, A. DESAI, D. POINTCHEVAL AND P. ROGAWAY, *Relations among notions of security for public-key encryption schemes*, In Proceedings of Advances in Cryptology – Crypto’98, Lecture Notes in Computer Science Vol. 1462, H. Krawczyk ed., Springer-Verlag, Berlin, 1998, pp. 26–45. The latest version is available from <http://www-cse.ucsd.edu/users/mihir/>
2. M. BELLARE AND P. ROGAWAY, *Optimal asymmetric encryption*, In Proceedings of Advances in Cryptology – Eurocrypt’94, Lecture Notes in Computer Science Vol. 950, A. De Santis ed., Springer-Verlag, Berlin, 1994, pp. 92–111.
3. M. BELLARE AND A. SAHAI, *Non-Malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization*, In Proceedings of Advances in Cryptology – Crypto’99, Lecture Notes in Computer Science Vol. 1666, M. Wiener ed., Springer-Verlag, Berlin, 1999, pp. 519–536.
4. R. CRAMER AND V. SHOUP, *A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack*, In Proceedings of Advances in Cryptology – Crypto’98, Lecture Notes in Computer Science Vol. 1462, H. Krawczyk, ed., Springer-Verlag, Berlin, 1998, pp. 13–25.
5. D. DOLEV, D. DWORK AND M. NAOR, *Non-malleable cryptography*, In Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, ACM, New York, 1991, pp. 542–552; D. DOLEV, D. DWORK AND M. NAOR, *Non-malleable cryptography*, SIAM Journal on Computing, 30 (2000), pp. 391–437.
6. O. Goldreich, Foundations of cryptography, Volume II, 2002.
available from <http://www.wisdom.weizmann.ac.il/~oded/foc.html>
7. O. Goldreich, Y. Lustig and M. Naor, On Chosen Ciphertext Security of Multiple Encryptions, available from <http://eprint.iacr.org/2002/089/>
8. S. Goldwasser and S. Micali, Probabilistic encryption. *Journal of Computer and System Sciences* **28**, pp. 270–299, 1984.
9. M. Naor and M. Yung, Public-key cryptosystems provably secure against chosen ciphertext attacks, In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pp. 427–437, 1990.
10. C. Rackoff and D. Simon, Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack, In *Proceedings of Advances in Cryptology – Crypto’91*, Lecture Notes in Computer Science Vol. 576, J. Feigenbaum ed., pp. 433–444, Springer-Verlag, 1991.
11. C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal* **28**, pp. 656–715, 1949.
12. V. Shoup, OAEP Reconsidered, In *Proceedings of Advances in Cryptology – Crypto 2001*, Lecture Notes in Computer Science Vol. 2139, J. Kilian ed., pp. 239–259, Springer-Verlag, 2001.

13. Y. Watanabe, J. Shikata and H. Imai, Equivalence between semantic security and indistinguishability against chosen ciphertext attacks, In *Proceedings of International Workshop on Practice and Theory in Public Key Cryptosystems - PKC 2003*, Lecture Notes in Computer Science Vol. 2567, Y. Desmedt ed., pp. 71–84, Springer-Verlag, 2003.