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

Yodai Watanabe[1⋆] and Junji Shikata[2]

[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).

Abstract. This paper studies the relation among simulator-based and comparison-based definitions of semantic security. The definitions are considered in a more general framework than the ordinal one; namely, an adversary is assumed to have access to prior information of a plaintext. If the framework is restricted to the ordinal one, then all the security notions considered in this paper, including indistinguishability, are shown to be equivalent. On the other hand, the equivalence is not necessarily valid in the general framework. In fact, it is shown that no encryption scheme is secure in the sense of comparison-based semantic security in the strongest forms. Furthermore, a sufficient condition for the equivalence between semantic security and indistinguishability is derived.

Key words: Semantic security, Simulator-based definition, Comparison-based definition, Indistinguishability, Relation among security notions

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 (in the ordinary framework)[6, 8, 13].

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

To formalize semantic security, 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 comparison-based notion may seem stronger than the simulator-based one. On the other hand, in the simulator-based definition, there is no restriction on the computability of partial information which an adversary wishes to extract[6, 8], while in the comparison-based one, the partial information has to be efficiently generated and evaluated by 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 prior information of a plaintext is available to an adversary. The significance of adopting this framework stems from the following facts. First, from the practical point of view, in most applications the plaintext may not be uniformly distributed and its prior information may be accessible to an adversary (see [6]). Second, from the theoretical point of view, investigating security notions in the general framework may reveal more detailed and novel relation among them.

The results of this paper are as follows. If the framework is restricted to the ordinal one, then all the security notions considered in this paper, including indistinguishability, are shown to be equivalent. This can be seen as evidence that our definitions in the general framework are consistent with the ordinary ones. On the other hand, the equivalence is not necessarily valid in the general framework. In fact, it is shown that there exists no encryption scheme which is secure in the sense of comparison-based semantic security in the strongest forms. However, that in weaker forms is shown to be equivalent to indistinguishability, which gives a sufficient condition for the equivalence between semantic security and indistinguishability.

2 Semantic security

In this section, we provide several definitions of semantic security; some are based on simulator, and the others are 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* $\epsilon : \mathbb{N} \to \mathbb{R}$*,* $k \mapsto \epsilon(k)$*, is called* negligible *if*

$$\forall c \geq 0 \exists k_c \big(k > k_c \Rightarrow 0 \leq \epsilon(k) < k^c\big).$$

Suppose here that we obtain partial information about a plaintext, and consider the posterior distribution of the plaintext. The following definition is a formalization of the sets of algorithms which sample the plaintext according to the posterior distribution. As we will see in the next section, the computational complexity of such sampling algorithms plays an important role in considering the equivalence between semantic security and indistinguishability.

Definition 3. *Let* A *and* M^* *be algorithms and let* ϵ *be a function of* $\mathbb{N}$ *into* $\mathbb{R}$*,* $k \mapsto \epsilon(k) \geq 0$*. For* $k \in \mathbb{N}$*, consider*

`Experiment` $E(k)$
$(M, g) \leftarrow A(k);\ x_1 \leftarrow M;\ w \leftarrow g(x_1);\ x_0 \leftarrow M^*(M, g, w);$

Then M^* *is called an* ϵ-conditional algorithm for A *if*

$$\sum_x \big|\Pr[E(k) : x_0 = x | M = M', g = g', w = w'] \\ - \Pr[E(k) : x_1 = x | M = M', g = g', w = w']\big| \leq \epsilon$$

for any M'*,* g' *and* w'*. For given* A *as above,*

$$\begin{aligned}
\mathcal{M}^*(A;\epsilon) &= \{M^* | M^* \text{ is an } \epsilon\text{-conditional algorithm for } A\},\\
\mathcal{M}^*(A) &= \{M^* | \exists \epsilon (M^* \in \mathcal{M}^*(A;\epsilon) \wedge \epsilon \text{ is negligible})\},\\
\mathcal{M}^*_P(A;\epsilon) &= \{M^* | M^* \in \mathcal{M}^*(A;\epsilon) \wedge M^* \text{ is computable in polynomial-time}\},\\
\mathcal{M}^*_P(A) &= \{M^* | \exists \epsilon (M^* \in \mathcal{M}^*_P(A;\epsilon) \wedge \epsilon \text{ is negligible})\}.
\end{aligned}$$

We now provide several results related to this definition.

Proposition 1. *Let* A *be as in definition 3.*

1. *If* $g = \varepsilon$*, then* $M \in \mathcal{M}^*(A; 0)$*.*
2. *If* g *is a bijective function such that both* g *and* g^{-1} *are computable in polynomial-time, then* $M^*(M, g, w) := g^{-1}(w) \in \mathcal{M}^*(A; 0)$*.*
3. *If* $\#\{x | x \leftarrow M\}$ *is finite and* g *is deterministic, then there exists an algorithm* $M^* \in \mathcal{M}^*_P(A; 0)$*.*

Proof. The proof is clear from the definition. □

Lemma 1. *Let A and ϵ be as in definition 3, and suppose that $M^* \in \mathcal{M}^*(A;\epsilon)$. Then*

$$\sum_{x,x'} \left|\Pr[E(k) : x_1 = x \wedge x_0 = x'] - \Pr[E(k) : x_1 = x' \wedge x_0 = x]\right| \leq 2\epsilon.$$

Proof. For given M', g' and w', let p' and p_b denote

$$p' = \Pr[E(k) : M = M', g = g', w = w'],$$
$$p_b(x) = \Pr[E(k) : x_b = x | M = M', g = g', w = w'],$$

respectively. It is straightforward to verify that

$$\begin{aligned}
&\sum_{x,x'} \left|\Pr[E(k) : x_1 = x \wedge x_0 = x'] - \Pr[E(k) : x_1 = x' \wedge x_0 = x]\right| \\
=&\sum_{M',h',s'} \sum_{x,x'} p' \left|p_1(x)p_0(x') - p_1(x')p_0(x)\right| \\
=&\sum_{M',h',s'} \sum_{x,x'} p' \left|p_1(x)p_0(x') - p_0(x)p_0(x') + p_0(x)p_0(x') - p_1(x')p_0(x)\right| \\
\leq&\sum_{x,x'} \left(\Pr[E(k) : x_0 = x']\left|p_1(x) - p_0(x)\right| + \Pr[E(k) : x_0 = x]\left|p_1(x') - p_0(x')\right|\right) \\
\leq&2\epsilon \sum_{x} \Pr[E(k) : x_0 = x] = 2\epsilon,
\end{aligned}$$

where the last inequality follows from that in definition 3. This completes the proof. □

Proposition 2. *Let A be as in definition 3. If there exists a one-way function, then there exists a polynomial-time algorithm A such that $\mathcal{M}^*_P(A) = \emptyset$.*

Proof. Let g be a (deterministic) one-way function, and A be an algorithm which takes k and outputs $(\{0,1\}^k_U, g)$, where X_U denotes the uniform distribution over the set X. Suppose that $\mathcal{M}^*_P(A)$ is not empty. Let M^* be an element of $\mathcal{M}^*_P(A)$, and ϵ be a negligible function such that $M^* \in \mathcal{M}^*_P(A;\epsilon)$. For $k \in \mathbb{N}$, consider

`Experiment` $E(k)$

$\Pr[(\{0,1\}^k_U, g) \leftarrow A(k);\ x_1 \leftarrow \{0,1\}^k_U;\ w \leftarrow g(x_1);\ x_0 \leftarrow M^*(\{0,1\}^k_U, g, w);$

Then

$$\begin{aligned}
&\Pr[E(k) : x_0 \in g^{-1}(w)] = \Pr[E(k) : g(x_0) = w] \\
=&\sum_{x,x'} \Pr[E(k) : x_1 = x \wedge x_0 = x']\Pr[E(k) : g(x') = w | x_1 = x \wedge x_0 = x'] \\
\geq&\Pr[E(k) : g(x_1) = w] - 2\epsilon = 1 - 2\epsilon,
\end{aligned}$$

where the inequality follows from lemma 1. This contradicts the one-wayness of g, so the proposition follows. □

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]. Another version of the definition and related results can be found in [6]. See also [7] for a more general attacking model.

Definition 4 (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 probabilistic function. For $atk \in \{cpa, cca1, cca2\}$ and $k \in \mathbb{N}$, consider*

$\texttt{Experiment}\ \mathrm{Exp}^{sss-atk}_{\mathcal{PE},A,F}(k)$
$\quad (pk, sk) \leftarrow \mathcal{K}(k);\ (M, h, s_0, s_1) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk);\ x \leftarrow M;$
$\quad y \leftarrow \mathcal{E}_{pk}(x);\ z \leftarrow h(x);\ t \leftarrow (s_0, s_1, z);\ v \leftarrow A_2^{\mathcal{O}_2(\cdot)}(t, y);$
$\quad \texttt{if}\ (F(v, x, M, h, s_0) = 1 \wedge v \neq \varepsilon)\ \texttt{then}\ d \leftarrow 1\ \texttt{else}\ d \leftarrow 0;$
$\quad \texttt{return}\ d$
$\texttt{Experiment}\ \mathrm{Exp}^{sss-atk}_{\mathcal{PE},A',F}(k)$
$\quad (M, h, s_0, s_1) \leftarrow A'_1(k);\ x \leftarrow M;\ z \leftarrow h(x);\ t \leftarrow (s_0, s_1, z);\ v \leftarrow A'_2(t);$
$\quad \texttt{if}\ (F(v, x, M, h, s_0) = 1 \wedge v \neq \varepsilon)\ \texttt{then}\ d \leftarrow 1\ \texttt{else}\ d \leftarrow 0;$
$\quad \texttt{return}\ d$

Here ε is the empty string, $|x| = |x'|$ for any $x, x' \leftarrow M$, and A is assumed to have access to the oracles $\mathcal{O}_1(\cdot)$ and $\mathcal{O}_2(\cdot)$ as follows:

$$\begin{array}{lll} \mathcal{O}_1(\cdot) = \varepsilon(\cdot) & \textit{and}\ \mathcal{O}_2(\cdot) = \varepsilon(\cdot) & \textit{for}\ atk = cpa \\ \mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot) & \textit{and}\ \mathcal{O}_2(\cdot) = \varepsilon(\cdot) & \textit{for}\ atk = cca1 \\ \mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot) & \textit{and}\ \mathcal{O}_2(\cdot) = \mathcal{D}_{sk}(\cdot) & \textit{for}\ atk = cca2 \end{array}$$

where $\varepsilon(\cdot)$ is the function which, on any input, returns ε. In the case of CCA2, A_2 is prohibited from asking its oracle to decrypt y. Let

$$\mathrm{Adv}^{sss-atk}_{\mathcal{PE},A,A',F}(k) = \left|\Pr[\mathrm{Exp}^{sss-atk}_{\mathcal{PE},A,F}(k) = 1] - \Pr[\mathrm{Exp}^{sss-atk}_{\mathcal{PE},A',F}(k) = 1]\right|,$$

where the probability is taken over the internal coin tosses of all the algorithms and function. Then $\mathcal{PE}$ is said to be secure in the sense of *SSS-ATK if*

$$\forall A \exists A' \forall F \left(\mathrm{Adv}^{sss-atk}_{\mathcal{PE},A,A',F}(k)\ \textit{is negligible}\right). \tag{1}$$

We note that the function F in the above definition is implicit, and so the definition gives a stronger notion than the conventional one. However, as long as we consider the ordinal framework, these definitions are shown to be equivalent. The following lemma, whose proof is essentially based on the implicitness, plays an important role in the reduction from simulator-based definitions to comparison-based ones.

Lemma 2. *Let A and A' be algorithms, and F be a function. For $k \in \mathbb{N}$, consider*

$$\begin{array}{l}\texttt{Experiment } E(k) \\ \quad a \leftarrow A(k);\ a' \leftarrow A'(k);\end{array}$$

Define $\mathrm{Adv}_{A,A',F}$ *and* $\mathrm{Adv}_{A,A'}$ *by*

$$\mathrm{Adv}_{A,A',F} = \left|\Pr[E(k) : F(a) = 1] - \Pr[E(k) : F(a') = 1]\right|,$$
$$\mathrm{Adv}_{A,A'} = \sum_{\hat{a}} \left|\Pr[E(k) : a = \hat{a}] - \Pr[E(k) : a' = \hat{a}]\right|,$$

respectively. Suppose that for any F, $\mathrm{Adv}_{A,A',F}$ is negligible. Then $\mathrm{Adv}_{A,A'}$ is also negligible (i.e. the distribution of a is statistically indistinguishable from that of a').

Proof. Let $\mathcal{A}_+$ be

$$\mathcal{A}_+ = \{\hat{a} | \Pr[E(k) : a = \hat{a}] \geq \Pr[E(k) : a' = \hat{a}]\}.$$

From the assumption, it follows that for the function F defined by

$$F(a) = \begin{cases} 1 & a \in \mathcal{A}_+, \\ 0 & \text{otherwise}, \end{cases}$$

there exists a negligible function ϵ such that

$$\mathrm{Adv}_{A,A',F} = \sum_{\hat{a} \in \mathcal{A}_+} \left|\Pr[E(k) : a = \hat{a}] - \Pr[E(k) : a' = \hat{a}]\right| \leq \epsilon.$$

Similarly, it can be shown that there exists a negligible function ϵ' such that

$$\sum_{\hat{a} \notin \mathcal{A}_+} \left|\Pr[E(k) : a = \hat{a}] - \Pr[E(k) : a' = \hat{a}]\right| \leq \epsilon'.$$

The lemma readily follows from the above inequalities. □

Next we give a comparison-based definition of semantic security and that of indistinguishability.

Definition 5 (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. Let $\hat{M}_A$ be a plaintext-sampling algorithm. For $atk \in \{cpa, cca1, cca2\}$, $b \in \{0, 1\}$ and $k \in \mathbb{N}$, consider*

$$\begin{array}{l}\texttt{Experiment } \mathrm{Exp}^{css-atk-b}_{\mathcal{PE},A,\hat{M}_A}(k) \\ \quad (pk, sk) \leftarrow \mathcal{K}(k);\ (M, h, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk);\ x_1 \leftarrow M;\ z \leftarrow h(x_1); \\ \quad t \leftarrow (s, z);\ y \leftarrow \mathcal{E}_{pk}(x_1);\ (v, f) \leftarrow A_2^{\mathcal{O}_2(\cdot)}(t, y);\ x_0 \leftarrow \hat{M}_A(M, h, t); \\ \quad \texttt{if } v = f(x_b) \texttt{ then } d \leftarrow 1 \texttt{ else } d \leftarrow 0; \\ \quad \texttt{return } d\end{array}$$

Here $|x| = |x'|$ for any $x, x' \leftarrow M$, and A is assumed to have oracle access as in definition 4. Let

$$\mathrm{Adv}^{css-atk}_{\mathcal{PE},A,\hat{M}_A}(k) = \left|\Pr[\mathrm{Exp}^{css-atk-1}_{\mathcal{PE},A,\hat{M}_A}(k) = 1] - \Pr[\mathrm{Exp}^{css-atk-0}_{\mathcal{PE},A,\hat{M}_A}(k) = 1]\right|,$$

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*

$$\forall A \exists \hat{M}_A \big(\mathrm{Adv}^{css-atk}_{\mathcal{PE},A,\hat{M}_A}(k) \text{ is negligible}\big). \tag{2}$$

Definition 6 (Indistinguishability). *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. Let $\hat{M}_A$ be a plaintext-sampling algorithm. For $atk \in \{cpa, cca1, cca2\}$, $b \in \{0,1\}$ and $k \in \mathbb{N}$, consider*

`Experiment` $\mathrm{Exp}^{ind-atk-b}_{\mathcal{PE},A,\hat{M}_A}(k)$
  $(pk, sk) \leftarrow \mathcal{K}(k)$; $(x_0, x_1, h, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk)$; $a \leftarrow \{0,1\}_U$; $z \leftarrow h(x_a)$;
  $t \leftarrow (s, z)$; $y \leftarrow \mathcal{E}_{pk}(x_a)$; $v_1 \leftarrow A_2^{\mathcal{O}_2(\cdot)}(t, y)$; $v_0 \leftarrow \hat{M}_A(x_0, x_1, h, t)$;
  `if` $v_b = a$ `then` $d \leftarrow 1$ `else` $d \leftarrow 0$;
  `return` d

Here $|x_0| = |x_1|$, and A is assumed to have oracle access as in definition 4. Let

$$\mathrm{Adv}^{ind-atk}_{\mathcal{PE},A,\hat{M}_A}(k) = \Pr[\mathrm{Exp}^{ind-atk-1}_{\mathcal{PE},A,\hat{M}_A}(k) = 1] - \Pr[\mathrm{Exp}^{ind-atk-0}_{\mathcal{PE},A,\hat{M}_A}(k) = 1],$$

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 *IND-ATK if*

$$\forall A \exists \hat{M}_A \big(\mathrm{Adv}^{ind-atk}_{\mathcal{PE},A,\hat{M}_A}(k) \text{ is negligible}\big). \tag{3}$$

We note that the above definitions are weaker than the conventional ones (see e.g. [1]), because a plaintext-sampling algorithm is used instead of the random guessing algorithm (i.e. the algorithm M itself). However, as long as we consider the ordinal framework, the above definitions turn out to be equivalent to the conventional ones.

As we will see in the next section, the above comparison-based definition of semantic security is too strong to be considered in the general framework, because there exists no encryption scheme secure in that sense. Hence, we provide several weaker definitions.

Definition 7. *Let the security notion GOAL-ATK be defined in the same way as definition 4. Then*

1. *$\mathcal{PE}$ is called* secure in the sense of *$GOAL_M$-ATK if M is restricted to $\{x_0, x_1\}_U$ with $|x_0| = |x_1|$,*
2. *$\mathcal{PE}$ is called* secure in the sense of *$GOAL_S$-ATK if formula (1) is replaced by*

$$\forall A \forall F \exists A' \big(\mathrm{Adv}^{sss-atk}_{\mathcal{PE},A,A',F}(k) \text{ is negligible}\big), \tag{4}$$

3. $\mathcal{PE}$ *is called* secure in the sense of *$GOAL_F$-ATK if F is restricted to such that*

$$\exists \hat{F} \forall v \forall x \forall M \forall h \big(F(v, x, M, h, s_0) = 1 \Leftrightarrow v = \hat{F}(x, M, h, s_0) \wedge \mathcal{M}_P^*(A_F) \neq \emptyset \big),$$

where A_F is defined by

$$\begin{array}{l} \texttt{Algorithm } A_F^{\mathcal{O}_1(\cdot),\mathcal{O}_2(\cdot)}(k; \mathcal{K}, A, \hat{F}) \\ \quad (pk, sk) \leftarrow \mathcal{K}(k);\ (M, h, s_0, s_1) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk); \\ \quad \hat{F}^* \leftarrow \hat{F}^*(x) := \hat{F}(x, M, h, s_0); \\ \quad \texttt{return } (M, \hat{F}^*) \end{array}$$

Definition 8. *Let the security notion $GOAL$-ATK be defined in the same way as definition 5. Then*

1. $\mathcal{PE}$ *is called* secure in the sense of *$GOAL_M$-ATK if M is restricted to $\{x_0, x_1\}_U$ with $|x_0| = |x_1|$,*
2. $\mathcal{PE}$ *is called* secure in the sense of *$GOAL_S$-ATK if* $\mathrm{Exp}_{\mathcal{PE},A,\hat{M}_A}^{css-atk-b}$ *is replaced by*

$$\begin{array}{l} \texttt{Experiment } \mathrm{Exp}_{\mathcal{PE},A,\hat{M}_A}^{css-atk-b}(k) \\ \quad (pk, sk) \leftarrow \mathcal{K}(k);\ (M, f, h, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk);\ x_1 \leftarrow M;\ z \leftarrow h(x_1); \\ \quad t \leftarrow (s, z);\ y \leftarrow \mathcal{E}_{pk}(x_1);\ v \leftarrow A_2^{\mathcal{O}_2(\cdot)}(t, y);\ x_0 \leftarrow \hat{M}_A(M, h, t); \\ \quad \texttt{if } v = f(x_b) \texttt{ then } d \leftarrow 1 \texttt{ else } d \leftarrow 0; \\ \quad \texttt{return } d \end{array}$$

3. $\mathcal{PE}$ *is called* secure in the sense of *$GOAL_F$-ATK if f is restricted to such that $\mathcal{M}_P^*(A_f) \neq \emptyset$, where A_f is defined by one of the followings:*

$$\begin{array}{l} \texttt{Algorithm } A_f^{\mathcal{O}_1(\cdot),\mathcal{O}_2(\cdot)}(k; \mathcal{K}, A) \\ \quad (pk, sk) \leftarrow \mathcal{K}(k);\ (M, h, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk);\ x \leftarrow M;\ z \leftarrow h(x); \\ \quad t \leftarrow (s, z);\ y \leftarrow \mathcal{E}_{pk}(x);\ (v, f) \leftarrow A_2^{\mathcal{O}_2(\cdot)}(t, y); \\ \quad \texttt{return } (M, f) \\ \texttt{Algorithm } A_f^{\mathcal{O}_1(\cdot)}(k; \mathcal{K}, A) \\ \quad (pk, sk) \leftarrow \mathcal{K}(k);\ (M, f, h, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk); \\ \quad \texttt{return } (M, f) \end{array}$$

Definition 9. *Let the security notion $GOAL$-ATK be defined in the same way as above. Then $\mathcal{PE}$ is called* secure in the sense of *$GOAL'$-ATK if h is restricted to such that $\mathcal{M}_P^*(A_h) \neq \emptyset$, where A_h is defined as*

$$\begin{array}{l} \texttt{Algorithm } A_h^{\mathcal{O}_1(\cdot)}(k; \mathcal{K}, A) \\ \quad (pk, sk) \leftarrow \mathcal{K}(k);\ (M, h, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk); \\ \quad \texttt{return } (M, h) \end{array}$$

We note that, if h is empty (i.e. if the framework is ordinary), then $M \in \mathcal{M}_P^*(A_h)$ (proposition 1(i)), and so $\mathcal{M}_P^*(A_h) \neq \emptyset$.

3 Relation among the definitions

In this section, we investigate the relation among the definitions given in the previous section. Before we turn to the general framework, we first confirm that these definitions are proper; for this purpose, we show that all the definitions given in the previous section are equivalent in the ordinary framework.

Theorem 1. *(i) SSS'-$ATK \Rightarrow SSS'_{MSF}$-$ATK$, (ii) SSS'_{MSF}-$ATK \Rightarrow CSS'$-ATK, (iii) CSS'-$ATK \Rightarrow CSS'_{MSF}$-$ATK$, (iv) CSS'_{MSF}-$ATK \Rightarrow SSS'$-ATK.*

Proof. (i), (iii) The proof is trivial from the definitions.

(ii) Suppose that an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of SSS'_{MSF}-ATK. Let $B = (B_1, B_2)$ be a CSS'-ATK adversary. Let M^* be an element of $\mathcal{M}^*_P(A_h(k; \mathcal{K}, B))$, and ϵ be a negligible function such that $M^* \in \mathcal{M}^*_P(A_h(k; \mathcal{K}, B), \epsilon)$. By using B and M^*, let us construct the SSS'_{MSF}-ATK adversary $A = (A_1, A_2)$ as

`Algorithm` $A_1^{\mathcal{O}_1(\cdot)}(pk)$	`Algorithm` $A_2^{\mathcal{O}_2(\cdot)}(t, y)$
$(M, h, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$;	$(v, f) \leftarrow B_2^{\mathcal{O}_2(\cdot)}((s, z), y)$;
$x_1 \leftarrow M$; $z \leftarrow h(x_1)$;	`if` $v = f(x_1)$ `then` $d \leftarrow 1$ `else` $d \leftarrow 0$;
$x_0 \leftarrow M^*(M, h, z)$;	`return` d
$s_1 \leftarrow (s, x_1, z)$;	
`return` $(\{x_0, x_1\}_U, \varepsilon(\cdot), \varepsilon, s_1)$	

Note that we can assume without loss of generality that $\mathrm{Adv}^{css-atk}_{\mathcal{PE},B}(k) \geq 0$. In fact, for the case when $\mathrm{Adv}^{css-atk}_{\mathcal{PE},B}(k) < 0$, we may change the output d to $\bar{d}$, the inversion of d, in the construction of the algorithm A_2. Now it is convenient to denote by $E(k)$ the experiment

`Experiment` $E(k)$

$(pk, sk) \leftarrow \mathcal{K}(k)$; $(M, h, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$; $x_1 \leftarrow M$; $z \leftarrow h(x_1)$;
$t \leftarrow (s, z)$; $x_0 \leftarrow M^*(M, h, z)$; $y_1 \leftarrow \mathcal{E}_{pk}(x_1)$; $y_0 \leftarrow \mathcal{E}_{pk}(x_0)$;
$(v_1, f_1) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t, y_1)$; $(v_0, f_0) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t, y_0)$;

We will show that the advantage

$$\mathrm{Adv}^{css-atk}_{\mathcal{PE},B,M^*}(k) = \Pr[E(k) : v_1 = f_1(x_1)] - \Pr[E(k) : v_1 = f_1(x_0)]$$

is negligible. For this purpose, we consider the function $\hat{F}$ given by

$$\hat{F}(x, M, h, s_0) = \begin{cases} 1 & \text{for } M = \{x_0, x_1\}_U, h = \varepsilon(\cdot), s_0 = \varepsilon \text{ and } x = x_1, \\ 0 & \text{for } M = \{x_0, x_1\}_U, h = \varepsilon(\cdot), s_0 = \varepsilon \text{ and } x = x_0, \\ \varepsilon & \text{otherwise.} \end{cases}$$

Then the probability that A succeeds in the attack is written as

$$
\begin{aligned}
&\Pr[\mathrm{Exp}^{sss-atk}_{\mathcal{PE},A,\hat{F}}(k)=1] \\
&= \frac{1}{2}\Big(\frac{1}{2}\big(\Pr[E(k):v_1=f_1(x_1)]+(1-\Pr[E(k):v_1=f_1(x_0)])\big) \\
&\qquad \frac{1}{2}\big(\Pr[E(k):v_0=f_1(x_0)]+(1-\Pr[E(k):v_0=f_0(x_1)])\big)\Big) \\
&\geq \frac{1}{2}\big(\Pr[E(k):v_1=f_1(x_1)]+(1-\Pr[E(k):v_1=f_1(x_0)])-\epsilon\big) \\
&= \frac{1}{2}+\frac{1}{2}\mathrm{Adv}^{css-atk}_{\mathcal{PE},B,M^*}(k)-\frac{1}{2}\epsilon,
\end{aligned}
$$

where the inequality follows from lemma 1. On the other hand, for the above $\hat{F}$, the probability that A' succeeds in the attack is written as

$$
\begin{aligned}
&\Pr[\mathrm{Exp}^{sss-atk}_{\mathcal{PE},A',\hat{F}}(k)=1] \\
&= \Pr[(M,h,s_0,s_1)\leftarrow A'_1(k);\ x\leftarrow M;\ v\leftarrow A'_2((s_0,s_1,h(x))): \\
&\qquad v=\hat{F}(x,M,h,s_0)\wedge v\neq\varepsilon] \\
&\leq \Pr[(\{x_0,x_1\}_U,\varepsilon(\cdot),\varepsilon,s_1)\leftarrow A'_1(k);\ x\leftarrow\{x_0,x_1\}_U;\ v\leftarrow A'_2((\varepsilon,s_1,\varepsilon)): \\
&\qquad v=\hat{F}(x,\{x_0,x_1\}_U,\varepsilon(\cdot),\varepsilon)] \\
&= \Pr[(\{x_0,x_1\}_U,\varepsilon(\cdot),\varepsilon,s_1)\leftarrow A'_1(k);\ b\leftarrow\{0,1\}_U;\ v\leftarrow A'_2((\varepsilon,s_1,\varepsilon)): \\
&\qquad (b=1\wedge v=1)\vee(b=0\wedge v=0)] \\
&= \frac{1}{2}\Pr[(\{x_0,x_1\}_U,\varepsilon,s_0,s_1)\leftarrow A'_1(k);\ v\leftarrow A'_2((\varepsilon,s_1,\varepsilon)):v=1\vee v=0]\leq\frac{1}{2}.
\end{aligned}
$$

Hence, we obtain

$$
\mathrm{Adv}^{sss-atk}_{\mathcal{PE},A,A',F}(k)+\frac{1}{2}\epsilon\geq\frac{1}{2}\mathrm{Adv}^{css-atk}_{\mathcal{PE},B,M^*}(k)\ (\geq 0)
$$

for any A'. Since $\mathcal{PE}$ is supposed to be secure in the sense of SSS'_{MSF}-ATK, the advantage $\mathrm{Adv}^{sss-atk}_{\mathcal{PE},A,A',F}(k)$ is negligible for some A', and so $\mathrm{Adv}^{css-atk}_{\mathcal{PE},B,M^*_\epsilon}(k)$ is also negligible. This shows that, for any CSS'-ATK adversary B, there exists $\hat{M}_B(M,h,t)=M^*(M,h,z)$ such that $\mathrm{Adv}^{css-atk}_{\mathcal{PE},B,\hat{M}_B}(k)$ is negligible. Thus the assertion (ii) follows.

(iv) Suppose that an encryption scheme $\mathcal{PE}=(\mathcal{K},\mathcal{E},\mathcal{D})$ is secure in the sense of CSS'_{MSF}-ATK. Let $B=(B_1,B_2)$ be an SSS'-ATK adversary. Let M^* be an element of $\mathcal{M}^*_P(A_h(k;\mathcal{K},B))$, and ϵ be a negligible function such that $M^*\in\mathcal{M}^*_P(A_h(k;\mathcal{K},B),\epsilon)$. By using B and M^*, let us construct the CSS'_{MSF}-

ATK adversary $A = (A_1, A_2)$ as

`Algorithm` $A_1^{\mathcal{O}_1(\cdot)}(pk)$	`Algorithm` $A_2^{\mathcal{O}_2(\cdot)}(t, y)$
$(M, h, s_0, s_1) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$;	$v' \leftarrow B_2^{\mathcal{O}_2(\cdot)}((s, z), y)$; $b \leftarrow \{0, 1\}_U$;
$x_1 \leftarrow M$; $z \leftarrow h(x_1)$;	$v_b \leftarrow B_2^{\mathcal{O}_2(\cdot)}((s, z), \mathcal{E}_{pk}(x_b))$;
$x_0 \leftarrow M^*(M, h, z)$;	`if` $v' = v_b$ `then` $v \leftarrow b$ `else` $v \leftarrow \bar{b}$;
$s \leftarrow (s_0, s_1, x_0, x_1, z)$;	`return` v
$f \leftarrow f(x) := \begin{cases} 1 & \text{for } x = x_1, \\ 0 & \text{for } x = x_0; \end{cases}$	
`return` $(\{x_0, x_1\}_U, f, \varepsilon(\cdot), s)$	

Furthermore, let $\hat{M}_A$ be a plaintext-sampling algorithm for A, and, by using B and M^*, let us construct $B' = (B'_1, B'_2)$ as

`Algorithm` $B'_1(k)$	`Algorithm` $B'_2(t)$
$(pk', sk') \leftarrow \mathcal{K}(k)$;	$x \leftarrow M^*(M, h, z)$; $y \leftarrow \mathcal{E}_{pk'}(x)$;
$(M, h, s_0, s_1) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk')$;	$t' \leftarrow (s, z)$; $v \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t', y)$;
$s'_1 \leftarrow (s_1, pk', sk', M, h)$;	`return` v
`return` (M, h, s_0, s'_1)	

Note that B' can answer queries from B because it has the secret key sk'. It is now convenient to denote by $E(k)$ the experiment

`Experiment` $E(k)$

$$
\begin{aligned}
&(pk, sk) \leftarrow \mathcal{K}(k);\ (M, h, s_0, s_1) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk);\ x_1 \leftarrow M;\ z \leftarrow h(x_1); \\
&t \leftarrow (s_0, s_1, z);\ x_0 \leftarrow M^*(M, h, z);\ y_1, y'_1 \leftarrow \mathcal{E}_{pk}(x_1);\ y_0 \leftarrow \mathcal{E}_{pk}(x_0); \\
&v_1 \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t, y_1);\ v'_1 \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t, y'_1);\ v_0 \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t, y_0);
\end{aligned}
$$

Here we introduce the random variable R to denote the triplet of the random variables M, h and t (i.e. $R = (M, h, t)$). 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 $\mathbb{R}$, $\mu : \Omega \to \mathbb{R}$, by

$$\mu : (m_0, m_1, r) \mapsto \Pr[x_0 = m_0, x_1 = m_1, R = r],$$

then the triplet $\mathcal{P} = (\Omega, 2^\Omega, \mu)$ constitutes a discrete probability space. Let $\mathcal{V}$ be the set of all possible values of v, the output from B_2. For $v \in \mathcal{V}$, we define the random variables on $\mathcal{P}$, X_v and Y_v, by writing

$$
\begin{aligned}
X_v &= p_1(v|m_0, m_1, r) - p_0(v|m_0, m_1, r), \\
Y_v &= q_1(v|m_0, m_1, r) - q_0(v|m_0, m_1, r),
\end{aligned}
$$

where

$$
\begin{aligned}
p_b(v|m_0, m_1, r) &= \Pr[E(k) : v_b = v | x_0 = m_0, x_1 = m_1, R = r], \\
q_b(v|m_0, m_1, r) &= \Pr[E(k) : F(v, x_b, M, h) = 1 | x_0 = m_0, x_1 = m_1, R = r].
\end{aligned}
$$

Then $\Pr[\mathrm{Exp}^{css-atk-1}_{\mathcal{PE},A,\hat{M}_A}(k)=1]$ and $\mathrm{Adv}^{sss-atk}_{\mathcal{PE},B,B',F}(k)$ are now expressed, in terms of X_v and Y_v, as

$$\Pr[\mathrm{Exp}^{css-atk-1}_{\mathcal{PE},A,\hat{M}_A}(k)=1] \geq \frac{1}{2}+\frac{1}{4}\sum_{v\in\mathcal{V}} E_\mu[X_v^2]-\frac{1}{2}\epsilon,$$
$$\mathrm{Adv}^{sss-atk}_{\mathcal{PE},B,B',F}(k) \leq \frac{1}{2}\sum_{v\in\mathcal{V}} E_\mu[X_vY_v]+\epsilon,$$

where $E_\mu[\cdot]$ denotes the expectation with respect to the probability measure μ, and the inequalities follow from lemma 1 as before. The above expressions may facilitate the comparison between the advantages. In fact it is easy to see that

$$E_\mu[X_v^2]E_\mu[Y_w^2]+E_\mu[X_w^2]E_\mu[Y_v^2] \geq 2E_\mu[X_vY_v]E_\mu[X_wY_w].$$

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

$$\sum_{v\in\mathcal{V}} E_\mu[Y_v^2] \leq 2.$$

On the other hand, since the output from M_A is independent of that from A_2, we obtain

$$\Pr[\mathrm{Exp}^{css-atk-0}_{\mathcal{PE},A,\hat{M}_A}(k)=1] \leq \frac{1}{2}$$

as in the proof of (ii). These inequalities give that

$$2\mathrm{Adv}^{css-atk}_{\mathcal{PE},A,\hat{M}_A}(k)+2\epsilon \geq \left(\mathrm{Adv}^{sss-atk}_{\mathcal{PE},B,B',F}(k)\right)^2.$$

Since $\mathcal{PE}$ is supposed to be secure in the sense of CSS'_{MSF}-ATK, the advantage $\mathrm{Adv}^{sss-atk}_{\mathcal{PE},A,\hat{M}_A}(k)$ is negligible for some $\hat{M}_A$, and so $\mathrm{Adv}^{css-atk}_{\mathcal{PE},B,B',F}(k)$ is also negligible. Hence the theorem follows. □

Corollary 1. *All the security notions with prime are equivalent.*

Proof. The proof readily follows from the above theorem, together with theorem 2, which shows the equivalence between comparison-based semantic security (in weaker forms) and indistinguishability. □

Having observed the relation among the definitions in the ordinary framework, we now examine the relation in the general framework. The results are summarized in figure 1. We first show that comparison-based semantic security in some weaker forms is equivalent to indistinguishability.

Theorem 2. *(i) CSS_{MF}-$ATK \Rightarrow CSS_{MSF}$-$ATK$. (ii) CSS_{MSF}-$ATK \Rightarrow$ IND-ATK, (iii) IND-$ATK \Rightarrow CSS_{MF}$-ATK.*

Proof. (i) The proof is trivial from the definitions.

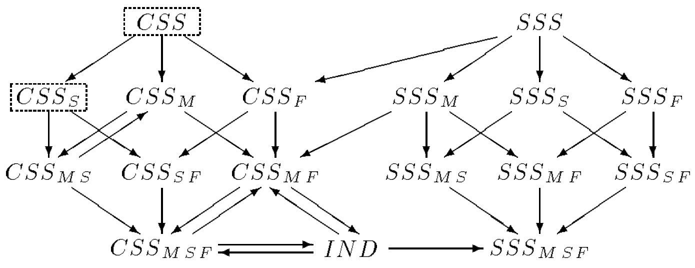

Fig. 1. Relations among security notions in the general framework. The arrow from X to Y, $X \to Y$, shows that the security notion X-ATK implies the security notion Y-ATK. No encryption scheme is secure in the sense of the boxed notions.

(ii) Suppose that an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of CSS_{MSF}-ATK. Let $B = (B_1, B_2)$ be an IND-ATK adversary. By using B, let us construct the CSS_{MSF}-ATK adversary $A = (A_1, A_2)$ as

`Algorithm` $A_1^{\mathcal{O}_1(\cdot)}(pk)$	`Algorithm` $A_2^{\mathcal{O}_2(\cdot)}(t, y)$
$(x_0, x_1, h, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$;	$v \leftarrow B_2^{\mathcal{O}_2(\cdot)}((s, z), y)$;
$s' \leftarrow (s, x_0, x_1)$;	`return` v
$f \leftarrow f(x) := \begin{cases} 1 & \text{for } x = x_1, \\ 0 & \text{for } x = x_0; \end{cases}$	
`return` $(\{x_0, x_1\}_U, f, h, s')$	

Let $\hat{M}_A(\{x_0, x_1\}_U, h, t)$ be a plaintext-sampling algorithm for A. Consider the plaintext-sampling algorithm for B given by

$$\hat{M}_B(x_0, x_1, h, t) := \hat{M}_A(\{x_0, x_1\}_U, h, (s, z)).$$

It then follows that

$$\mathrm{Adv}^{css-atk}_{\mathcal{PE}, A, \hat{M}_A}(k) = \frac{1}{2} \mathrm{Adv}^{ind-atk}_{\mathcal{PE}, B, \hat{M}_B}(k).$$

Since $\mathcal{PE}$ is supposed to be secure in the sense of CSS_{MSF}-ATK, the left-hand side is negligible for some $\hat{M}_A$, and so the right-hand side is also negligible. Thus the assertion (ii) follows.

(iii) Suppose that an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of IND-ATK. Let $B = (B_1, B_2)$ be an SSS_{MF}-ATK adversary. Let M^* be an element of $\mathcal{M}^*_P(A_f(k; \mathcal{K}, B))$, and ϵ be a negligible function such that $M^* \in \mathcal{M}^*_P(A_f(k; \mathcal{K}, B), \epsilon)$. By using B and M^*, let us construct the IND-ATK adversary $A = (A_1, A_2)$ as

`Algorithm` $A_1^{\mathcal{O}_1(\cdot)}(pk)$	`Algorithm` $A_2^{\mathcal{O}_2(\cdot)}(t, y)$
$(\{x_0, x_1\}_U, h, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$;	$(v, f) \leftarrow B_2^{\mathcal{O}_2(\cdot)}((s, z), y)$;
$s' \leftarrow (s, x_0, x_1)$;	$x \leftarrow M^*(\{x_0, x_1\}_U, f, v)$;
`return` $(\{x_0, x_1\}_U, h, s')$	`if` $x = x_1$ `then` $d \leftarrow 1$ `else` $d \leftarrow 0$;
	`return` d

Let $\hat{M}_A(x_0, x_1, h, t)$ be a plaintext-sampling algorithm for A. Consider the plaintext-sampling algorithm for B given by

$$\hat{M}_B(\{x_0, x_1\}_U, h, t) := \hat{M}_A(x_0, x_1, h, (s, z)).$$

It then follows that

$$\mathrm{Adv}^{ind-atk}_{\mathcal{PE},A,\hat{M}_A}(k) + \epsilon \geq \frac{1}{2}\mathrm{Adv}^{css-atk}_{\mathcal{PE},B,\hat{M}_B}(k).$$

Since $\mathcal{PE}$ is supposed to be secure in the sense of *IND-ATK*, the left-hand side is negligible for some $\hat{M}_A$, and so the right-hand side is also negligible. Hence the theorem follows. □

The following theorem can be shown in the same way as above.

Theorem 3. *CSS_{SF}-ATK $\Rightarrow$ CSS_F-ATK,*

Proof. Suppose that an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of CSS_{SF}-ATK. Let $B = (B_1, B_2)$ be a CSS_F-ATK adversary. Let M^* be an element of $\mathcal{M}^*_P(A_f(k; \mathcal{K}, B))$, and ϵ be a negligible function such that $M^* \in \mathcal{M}^*_P(A_f(k; \mathcal{K}, B), \epsilon)$. By using B and M^*, let us construct the CSS_{SF}-ATK adversary $A = (A_1, A_2)$ as

Algorithm $A_1^{\mathcal{O}_1(\cdot)}(pk)$	Algorithm $A_2^{\mathcal{O}_2(\cdot)}(t, y)$
$(M, h, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$;	$(v, f) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(t, y)$;
$f' \leftarrow f'(x) := x$;	$x \leftarrow M^*(M, f, v)$;
return (M, f', h, s)	return x

Let $\hat{M}_A(M, h, t)$ be a plaintext-sampling algorithm for A. Consider the plaintext-sampling algorithm for B given by

$$\hat{M}_B(M, h, t) := \hat{M}_A(M, h, t).$$

It then follows that

$$\mathrm{Adv}^{css-atk}_{\mathcal{PE},A,\hat{M}_A}(k) + \epsilon \geq \frac{1}{2}\mathrm{Adv}^{css-atk}_{\mathcal{PE},B,\hat{M}_B}(k).$$

Since $\mathcal{PE}$ is supposed to be secure in the sense of CSS_{SF}-ATK, the left-hand side is negligible for some $\hat{M}_A$, and so the right-hand side is also negligible. This completes the proof. □

Next we consider the relation between simulator-based and comparison-based definitions of semantic security.

Theorem 4. *(i) SSS-ATK $\Rightarrow$ CSS_F-ATK, (ii) SSS_M-ATK $\Rightarrow$ CSS_{MF}-ATK.*

Proof. (i) Suppose that an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of *SSS-ATK*. Let $B = (B_1, B_2)$ be a CSS_F-*ATK* adversary. Let M^* be an element of $\mathcal{M}^*_P(A_f(k; \mathcal{K}, B))$, and ϵ be a negligible function such that $M^* \in \mathcal{M}^*_P(A_f(k; \mathcal{K}, B), \epsilon)$. By using B and M^*, let us construct the *SSS-ATK* adversary $A = (A_1, A_2)$ as

```
Algorithm A_1^{O_1(·)}(pk)              | Algorithm A_2^{O_2(·)}(t, y)
    (M, h, s) ← B_1^{O_1(·)}(pk);       |     (v, f) ← B_2^{O_2(·)}((s, z), y);
    s_0 ← s; s_1 ← M;                   |     x ← M*(M, f, v);
    return (M, h, s_0, s_1)             |     return x
```

Let $A' = (A'_1, A'_2)$ be a simulator of A. Consider the plaintext-sampling algorithm for B given by

```
Algorithm M̂_B(M, h, t)
    x ← A'_2(t);
    return x
```

Since $\mathcal{PE}$ is supposed to be secure in the sense of *SSS-ATK*, it follows from lemma 2 that the distribution of the output from A is statistically indistinguishable from that from A'. Therefore there exists a negligible function ϵ' such that

$$\epsilon' + 2\epsilon \geq \mathrm{Adv}^{css-atk}_{\mathcal{PE},B,\hat{M}_B}(k),$$

where the inequality in lemma 1 has been used. This shows that $\mathrm{Adv}^{css-atk}_{\mathcal{PE},B,\hat{M}_B}(k)$ is negligible.

(ii) It is clear that the above proof is applicable only by replacing M by $\{x_0, x_1\}_U$. Hence the theorem follows. $\square$

Theorem 5. CSS_{MF}-*ATK* $\Rightarrow$ $SSS_{M\,SF}$-*ATK*,

Proof. Suppose that an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of CSS_{MF}-*ATK*. Let $B = (B_1, B_2)$ be an $SSS_{M\,SF}$-*ATK* adversary, and $\hat{F}$ be a function such that $\mathcal{M}^*_P(A_f(k; \mathcal{K}, B, \hat{F})) \neq \emptyset$. Let M^* be an element of $\mathcal{M}^*_P(A_f(k; \mathcal{K}, B, \hat{F}))$, and ϵ be a negligible function such that $M^* \in \mathcal{M}^*_P(A_f(k; \mathcal{K}, B, \hat{F}), \epsilon)$. By using B, $\hat{F}$ and M^*, let us construct the CSS_{MF}-*ATK* adversary $A = (A_1, A_2)$ as

```
Algorithm A_1^{O_1(·)}(pk)                          | Algorithm A_2^{O_2(·)}(t, y)
    ({x_0, x_1}_U, h, s_0, s_1) ← B_1^{O_1(·)}(pk); |     v ← B_2^{O_2(·)}(t, y);
    s ← (s_0, s_1);                                 |     f ← f(x):=F̂(x, {x_0, x_1}_U, h, s_0);
    return ({x_0, x_1}_U, h, s)                     |     return (v, f)
```

Let $\hat{M}_A(x_0, x_1, h, t)$ be a plaintext-sampling algorithm for A. Consider the simulator of B given by

```
Algorithm B'_1(k)                                    | Algorithm B'_2(t)
    (pk', sk') ← K(k);                               |     x ← M̂_A({x_0, x_1}_U, h, (s_0, s_1, z));
    ({x_0, x_1}_U, h, s_0, s_1) ← B_1^{O_1(·)}(pk'); |     v ← F̂(x, {x_0, x_1}_U, h, s_0);
    s'_1 ← (s_1, pk', sk', {x_0, x_1}_U, h);         |     return v
    return ({x_0, x_1}_U, h, s_0, s'_1)              |
```

It then follows that

$$\mathrm{Adv}^{css-atk}_{\mathcal{PE},A,\hat{M}_A}(k) = \mathrm{Adv}^{sss-atk}_{\mathcal{PE},B,B',\hat{F}}(k).$$

Since $\mathcal{PE}$ is supposed to be secure in the sense of CSS_{MF}-ATK, the left-hand side is negligible for some $\hat{M}_A$, and so the right-hand side is also negligible. □

Finally, we show that no encryption scheme is secure in the sense of comparison-based semantic security in the strongest forms. This shows that there exist (trivial) separations among the security notions considered in this paper.

Theorem 6. *No encryption scheme is secure in the sense of CSS_S-ATK and also CSS-ATK.*

Proof. The existence of a secure encryption scheme implies that of a trapdoor one-way function. Thus the theorem follows from the following lemma. □

Lemma 3. *If there exists a one-way function, then no encryption scheme secure in the sense of CSS_S-ATK exists.*

Proof. Let g be a (deterministic) one-way function. Consider the CSS_S-ATK adversary given by

Algorithm $A_1^{\mathcal{O}_1(\cdot)}(pk)$	Algorithm $A_2^{\mathcal{O}_2(\cdot)}(t, y)$
$M \leftarrow M{:=}\{0,1\}^k$;	$v \leftarrow z$;
$f \leftarrow g$; $h \leftarrow g$; $s \leftarrow g$;	return v
return (M, f, h, s)	

Let $\hat{M}_A(M, h, t)$ be a plaintext-sampling algorithm for A. It follows from the above construction that

$$\begin{aligned}\Pr[\mathrm{Exp}^{css-atk-0}_{\mathcal{PE},A,\hat{M}_A}(k) = 1] &= \Pr[\mathrm{Exp}^{css-atk-1}_{\mathcal{PE},A,\hat{M}_A}(k) = 1] - \mathrm{Adv}^{css-atk}_{\mathcal{PE},A,\hat{M}_A}(k)\\ &= 1 - \mathrm{Adv}^{css-atk}_{\mathcal{PE},A,\hat{M}_A}(k).\end{aligned}$$

Thus, if $\mathrm{Adv}^{css-atk}_{\mathcal{PE},A,\hat{M}_A}(k)$ is negligible, then $\hat{M}_A$ outputs $x \in g^{-1}(z)$ with non-negligible probability. This contradicts the one-wayness of g, so the lemma follows. □

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 Yrok, 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.