Equivalence between Semantic Security and Indistinguishability against Chosen Ciphertext Attacks

Yodai Watanabe[1], Junji Shikata[2], and Hideki Imai[3]

[1] 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
[3] Institute of Industrial Science, University of Tokyo
4-6-1 Komaba, Meguro-ku, Tokyo 153-8505, Japan
imai@iis.u-tokyo.ac.jp

Abstract. The aim of this work is to examine the relation between the notions of semantic security and indistinguishability against chosen ciphertext attacks. For this purpose, a new security notion called non-dividability is introduced independent of attack models, and is shown to be equivalent to each of the previous two notions. This implies the equivalence between semantic security and indistinguishability under any form of attack.

1 Introduction

The security of public key cryptosystems is usually classified from the point of view of their goals and attack models. The (currently known) standard goals of public key cryptosystems are as follows. (i)Semantic security (SS)[10]: In this security notion, any adversary (probabilistic polynomial-time Turing machine) cannot obtain any partial information about the plaintext of a given ciphertext. This notion corresponds to a computational version of the "perfect secrecy" introduced by Shannon[14]. (ii)Indistinguishability (IND)[10]: Here, given a ciphertext of one of two plaintexts any adversary cannot distinguish which one is encrypted. This notion is rather artificial, but in considering provable security of a public key cryptosystem it is usually convenient to employ this notion as the goal of the system. (iii)Non-malleability (NM)[6]: Given a ciphertext of a plaintext any adversary cannot construct another ciphertext whose plaintext is meaningfully related to the initial one.

On the other hand, the (currently known) standard attack models of public key cryptosystems are as follows. (a)Chosen plaintext attacks (CPA): In this model, an adversary has access to an encryption oracle. That is, she can choose

Y.G. Desmedt (Ed.): PKC 2003, LNCS 2567, pp. 71–84, 2003.

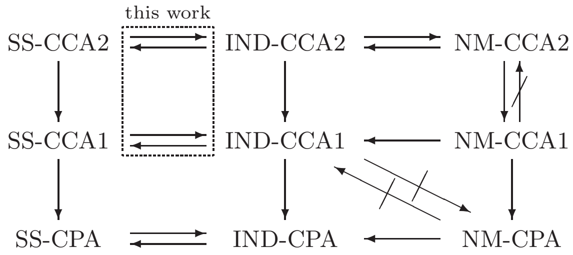

Fig. 1. Relations among security notions

a set of plaintexts and obtain the corresponding ciphertexts. (b)(Non-adaptive) chosen ciphertext attacks (CCA1)[12]: In this model, an adversary has, in addition to the ability of the CPA adversary, access to a decryption oracle before she obtains a challenge ciphertext. That is, she can choose a set of ciphertexts and obtain the corresponding plaintexts during this period. (c)Adaptive chosen ciphertext attacks (CCA2)[13]: In this model, an adversary has, in addition to the ability of the CCA1 adversary, access to a decryption oracle even after she obtains a challenge ciphertext. However, she is prohibited from asking the oracle to decrypt the challenge ciphertext itself.

Several security notions can be constructed by combining these goals and attack models, and, of course, there are relations between some of these notions. In fact, the following facts on such relations have been known so far (figure 1). First, regarding the attack models, the power of the adversaries gets stronger in the order CPA, CCA1 and CCA2, so does the strength of the security notions. Next, regarding the goals, it has been shown that NM implies IND in general, but, in CCA2 model, IND also implies NM[2]. On the other hand, SS is equivalent to IND in CPA model[7, 10], but, in CCA models, the equivalence has not been strictly verified so far (see [2]). Observe that, in proposing a public key cryptosystem, it is conventional to claim, based on the fact IND-CCA2$\Leftrightarrow$NM-CCA2 mentioned above, that the system has the strongest security by showing that it is secure in the sense of IND-CCA2 (see, e.g. [3, 5, 15]). However, in the background of this claim, it seems to be implicitly assumed that the equivalence between SS and IND holds under CCA models as well. Hence, formalizing and proving this equivalence under this stronger attack model (CCA) is of importance. In this paper, we show that this assumption is true, that is, SS and IND are equivalent under any attack model.[1]

The rest of this paper is organized as follows. We first extend the definition of semantic security to CCA models in section 2. In section 3, we introduce a new security notion called *non-dividability* which is equivalent to semantic security

[1] After the work of this paper had been completed, the authors were informed that Goldreich had independently shown the same result in a chapter of his book recently revised[8], which deals with wide-ranging subjects of encryption and contains several new results.

under any form of attack. In section 4, we show that this notion is equivalent to indistinguishability, which yields that semantic security is equivalent to indistinguishability under any form of attack. We devote section 5 to the conclusion of this paper.

2 Preliminaries

In this section, we consider two security notions, semantic security and indistinguishability. First, we provide the definition of indistinguishability according to Bellare et al.[2], and then that of semantic security according to Goldreich[7]. Note that the former is independent of attack models, while the latter supposes CPA model. Thus we next give an extended version of the definition of semantic security which is based on the framework by Bellare et al.[2], and so is independent of attack models. Finally, we show that the extended version of semantic security implies the original one (in CPA model), which ensures the validity of the extension.

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

Definition 1. *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 message* 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 message* 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. *A function* $\epsilon : \mathbb{N} \to \mathbb{R}$*,* $\epsilon(n) \geq 0$ *for* $n \in \mathbb{N}$*, is called* negligible *if for every constant* $c \geq 0$ *there exists an integer* k_c *such that* $\epsilon(k) < k^{-c}$ *for all* $k > k_c$*.*

Now we consider the notion of indistinguishability. This notion was first introduced by Goldwasser and Micali[10], and later a version of this notion was provided by Bellare et al.[2]. We now describe the definition of this notion according to Bellare et al.[2]. Let $A = (A_1, A_2)$ be an adversary attacking an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. In the first stage of the attack by the adversary, algorithm A_1, given the public key pk, outputs a triplet (x_0, x_1, s), where the first two components are messages of the same length, and the last one is state information. A random one of x_0 and x_1, say x_b, is selected, and then x_b is encrypted to give a challenge ciphertext y. In the second stage of the attack by the adversary, algorithm A_2, given (x_0, x_1, s, y), guesses the bit b, i.e. which of the two messages is encrypted. If any adversary can guess the bit essentially no more than random guess, then $\mathcal{PE}$ is called secure in the sense of IND-ATK, where ATK represents the attack model of A, i.e. CPA, CCA1, or CCA2. The formal definition is as follows.

Definition 3 (Indistinguishability[2]). *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 $\mathrm{Exp}^{ind-atk-b}_{\mathcal{PE},A}(k)$
    $(pk, sk) \xleftarrow{R} \mathcal{K}(k)$; $(x_0, x_1, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk)$; $y \leftarrow \mathcal{E}_{pk}(x_b)$;
    $d \leftarrow A_2^{\mathcal{O}_2(\cdot)}(x_0, x_1, s, y)$;
    return $d$
```

where $|x_0| = |x_1|$ and

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

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

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

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 $\mathrm{Adv}^{ind-atk}_{\mathcal{PE},A}(k)$ is negligible for any A.*

The notion of semantic security was first introduced by Goldwasser and Micali[10], and later refined by Goldreich[7]. The definitions formalize the intuition of privacy that whatever can be efficiently computed about a message from its ciphertext can also be computed without the ciphertext. This is a polynomially bounded version of "perfect secrecy" introduced by Shannon in the context of information theoretic security[14]. Now we describe the definition of this notion according to Goldreich[7]. Let A be an adversary attacking an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. First, a random message x is generated from a message space X_k samplable in polynomial time, and then x is encrypted to give a challenge ciphertext y. Given the public key pk, the length $|x|$ of the messages, a priori information $h(x)$ of x, and a challenge ciphertext y, the adversary A tries to extract partial information $f(x)$ of the message x. If for every A there exists its simulator A' which can guess $f(x)$ only from $(pk, |x|, h(x))$ (i.e. without y) essentially as well as A, then $\mathcal{PE}$ is called secure in the sense of $\mathrm{SS_G}$-ATK. The formal definition is as follows.

Definition 4 (Semantic security under CPA model[7]). *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). For $k \in \mathbb{N}$, a polynomial-time samplable message space X_k, a polynomial-time computable function h of X_k into $\{0,1\}^*$ and a function f of X_k into $\{0,1\}^*$, consider*

```
Experiment $\mathrm{Exp}^{ss_g-cpa-1}_{\mathcal{PE},A}(k, X_k, f, h)$
    $(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k)$; $x \leftarrow X_k$; $y \leftarrow \mathcal{E}_{pk}(x)$; $v \leftarrow A(k, pk, |x|, h(x), y)$;
    if $v = f(x)$ then $d \leftarrow 1$ else $d \leftarrow 0$;
    return $d$
Experiment $\mathrm{Exp}^{ss_g-cpa-0}_{\mathcal{PE},A'}(k, X_k, f, h)$
    $x \leftarrow X_k$; $v \leftarrow A'(k, |x|, h(x))$; if $v = f(x)$ then $d \leftarrow 1$ else $d \leftarrow 0$;
    return $d$
```

where $|x| = |x'|$ for every $x, x' \in X_k$. Let

$$\begin{aligned}\mathrm{Adv}^{ss_g-cpa}_{\mathcal{PE},A,A'}(k, X_k, f, h) =&\Pr[\mathrm{Exp}^{ss_g-cpa-1}_{\mathcal{PE},A}(k, X_k, f, h) = 1]\\ &- \Pr[\mathrm{Exp}^{ss_g-cpa-0}_{\mathcal{PE},A'}(k, X_k, f, h) = 1].\end{aligned}$$

Then $\mathcal{PE}$ is said to be secure in the sense of SS$_G$-CPA *if for every A there exists A' such that $\mathrm{Adv}^{ss_g-cpa}_{\mathcal{PE},A,A'}(k, X_k, f, h)$ is negligible for every X_k, f and h.*

Note that, in the above definition, there is neither restriction to the computability of f nor need for the adversary to know f.

The above definition of semantic security implicitly supposes CPA model. Thus, for our purpose, it is necessary first to extend the definition to CCA models. Now we give a definition of semantic security under any attack models based on the framework of of Bellare et al.[2]. Let $A = (A_1, A_2)$ be an adversary attacking an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. In the first stage of the attack by the adversary, algorithm A_1, given the public key pk, outputs a pair (M, s), where the first component is a message space samplable in polynomial time and the second one is state information. A random message x is generated from M and then encrypted to give a challenge ciphertext y. In the second stage of the attack by the adversary, algorithm A_2, given (M, s, y), tries to find a pair (v, f) such that $v = f(x)$. If for every A there exists a simulator A' which can find such a pair only from (M, s) (i.e. without y) essentially as well as A, then $\mathcal{PE}$ is called secure in the sense of SS-ATK. The formal definition is as follows.

Definition 5 (Semantic security under any attack models). *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let A be a polynomial-time adversary and A' a polynomial-time simulator of A. For $k \in \mathbb{N}$, consider*

```
Experiment $\mathrm{Exp}^{ss-atk-1}_{\mathcal{PE},A}(k)$
    $(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k)$; $(M, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk)$; $x \leftarrow M$; $y \leftarrow \mathcal{E}_{pk}(x)$;
    $(v, f) \leftarrow A_2^{\mathcal{O}_2(\cdot)}(M, s, y)$; if $v = f(x)$ then $d \leftarrow 1$ else $d \leftarrow 0$;
    return $d$
```

```
Experiment $\mathrm{Exp}^{ss-atk-0}_{\mathcal{PE},A'}(k)$
    $(pk, sk) \xleftarrow{R} \mathcal{K}(k)$; $(M, s) \leftarrow A'_1(pk)$; $x \leftarrow M$; $(v, f) \leftarrow A'_2(M, s)$;
    if $v = f(x)$ then $d \leftarrow 1$ else $d \leftarrow 0$;
    return $d$
```

where $|x| = |x'|$ for every $x, x' \in M$, f is a polynomial-time computable function (or a polynomial-time algorithm) of M into $\{0,1\}^*$, $v \in f(M)$, and $\mathcal{O}_1(\cdot)$ and $\mathcal{O}_2(\cdot)$ are as in definition 3. In the case of CCA2, A_2 is prohibited from asking its oracle to decrypt y. Let

$$\mathrm{Adv}^{ss-atk}_{\mathcal{PE},A,A'}(k) = \Pr[\mathrm{Exp}^{ss-atk-1}_{\mathcal{PE},A}(k) = 1] - \Pr[\mathrm{Exp}^{ss-atk-0}_{\mathcal{PE},A'}(k) = 1].$$

Then $\mathcal{PE}$ is said to be secure in the sense of SS-CPA *if for every A there exists A' such that $\mathrm{Adv}^{ss-atk}_{\mathcal{PE},A,A'}(k)$ is negligible.*

To see the validity of the above formulation for CCA models, we show that, in CPA model, this one implies the original one, that is, this one provides a stronger security notion than the original one.

Theorem 1. *SS-CPA⇒SS$_G$-CPA*

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

Let B be an SS$_\mathrm{G}$-CPA adversary, and let B' be a simulator of B defined as

```
Algorithm $B'(k, |x|, h(x))$
    $(pk', sk') \leftarrow \mathcal{K}(k)$; $x_1 \leftarrow X_k$; $y \leftarrow \mathcal{E}_{pk'}(x_1)$; $v \leftarrow B(k, pk', |x_1|, h(x_1), y)$;
    return $v$
```

Now we show that $\mathrm{Adv}^{ss_g-cpa}_{\mathcal{PE},B,B'}(k, X_k, f, h)$ is negligible for any B, X_k, f and h. For this purpose, we assume, towards contradiction, that there exists B such that $\mathrm{Adv}^{ss_g-cpa}_{\mathcal{PE},B,B'}(k, X_k, f, h)$ is not negligible. By using such B, X_k, f and h, let us construct an SS-CPA adversary $A = (A_1, A_2)$ and its simulator $A' = (A'_1, A'_2)$ as follows.

```
Algorithm $A_1(pk)$
    $M \leftarrow X_k$; $s \leftarrow \{pk\}$;
    return $(M, s)$

Algorithm $A_2(M, s, y)$
    $v \leftarrow B(k, pk, |x|, h(x), y)$;
    $\tilde{f}(x) \leftarrow B(k, pk, |x|, h(x), \mathcal{E}_{pk}(x))$;
    return $(v, \tilde{f})$

Algorithm $A'_1(pk)$
    $M \leftarrow X_k$; $s \leftarrow \{pk\}$;
    return $(M, s)$

Algorithm $A'_2(M, s)$
    $(pk', sk') \leftarrow \mathcal{K}(k)$; $x_1 \leftarrow M$; $y \leftarrow \mathcal{E}_{pk'}(x_1)$;
    $v \leftarrow B(k, pk', |x_1|, h(x_1), y)$;
    $\tilde{f}(x) \leftarrow B(k, pk', |x|, h(x), \mathcal{E}_{pk'}(x))$;
    return $(v, \tilde{f})$
```

It is clear from this construction that A and A' are polynomial-time. Now let us define $p(1)$, $p(0)$, $p'(1)$ and $p'(0)$ by

$$\begin{aligned}
p(1) &= \Pr[(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (M, s) \leftarrow A_1(pk);\ x_1 \leftarrow M;\ y \leftarrow \mathcal{E}_{pk}(x_1);\\
&\qquad\quad (v, \tilde{f}) \leftarrow A_2(M, s, y) :\ v = \tilde{f}(x_1)]\\
p(0) &= \Pr[(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (M, s) \leftarrow A_1(pk);\ x_0 \leftarrow M;\\
&\qquad\quad (v, \tilde{f}) \leftarrow A'_2(M, s) :\ v = \tilde{f}(x_0)]\\
p'(1) &= \Pr[(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ x_1 \leftarrow X_k;\ y \leftarrow \mathcal{E}_{pk}(x_1);\\
&\qquad\quad v \leftarrow B(k, pk, |x_1|, h(x_1), y) :\ v = f(x_1)]\\
p'(0) &= \Pr[x_0 \leftarrow X_k;\ v \leftarrow B'(k, |x_0|, h(x_0)) :\ v = f(x_0)]
\end{aligned}$$

respectively. It is now convenient to denote by E the experiment

`Experiment` E

$$\begin{aligned}
&(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ x_0, x_1 \leftarrow X_k;\ y_0 \leftarrow \mathcal{E}_{pk}(x_0);\ y_1, y'_1 \leftarrow \mathcal{E}_{pk}(x_1);\\
&v_0 \leftarrow B(s_0, y_0);\ v_1 \leftarrow B(s_1, y_1);\ v'_1 \leftarrow B(s_1, y'_1);
\end{aligned}$$

where $s_b = \{k, pk, |x_b|, h(x_b)\}$ for $b \in \{0, 1\}$. Then it is straightforward to verify that

$$\begin{aligned}
p'(1) &= \Pr[E : v_0 = f(x_0)] = \Pr[E : v_1 = f(x_1)] = \Pr[E : v'_1 = f(x_1)],\\
p'(0) &= \Pr[E : v_0 = f(x_1)] = \Pr[E : v_1 = f(x_0)] = \Pr[E : v'_1 = f(x_0)],
\end{aligned}$$

and

$$\begin{aligned}
p(1) &= \Pr[E : v_1 = v'_1]\\
&\quad = \Pr[E : v_1 = f(x_1) \wedge v'_1 = f(x_1)] + \Pr[E : v_1 = f(x_0) \wedge v'_1 = f(x_0)]\\
&\qquad + \Pr[E : v_1 = v'_1 \wedge v_1 \neq f(x_0) \wedge v_1 \neq f(x_1)]\\
&\quad \geq \Pr[E : v_1 = f(x_1) \wedge v_0 = f(x_0)] + \Pr[E : v_1 = f(x_0) \wedge v_0 = f(x_1)]\\
&\qquad + \Pr[E : v_1 = v_0 \wedge v_1 \neq f(x_0) \wedge v_1 \neq f(x_1)]\\
&\quad = p'(1)p'(1) + p'(0)p'(0) + \Pr[E : v_1 = v_0 \wedge v_1 \neq f(x_0) \wedge v_1 \neq f(x_1)],\\
p(0) &= \Pr[E : v_1 = v_0]\\
&\quad = \Pr[E : v_1 = f(x_1) \wedge v_0 = f(x_1)] + \Pr[E : v_1 = f(x_0) \wedge v_0 = f(x_0)]\\
&\qquad + \Pr[E : v_1 = v_0 \wedge v_1 \neq f(x_0) \wedge v_1 \neq f(x_1)]\\
&\quad = p'(1)p'(0) + p'(0)p'(1) + \Pr[E : v_1 = v_0 \wedge v_1 \neq f(x_0) \wedge v_1 \neq f(x_1)].
\end{aligned}$$

It follows from the above equations that

$$\mathrm{Adv}^{ss-cpa}_{\mathcal{PE},A,A'}(k) = p(1) - p(0) \geq \big(p'(1) - p'(0)\big)^2 = \big(\mathrm{Adv}^{ss_g-cpa}_{\mathcal{PE},B,B'}(k)\big)^2.$$

Therefore, if $\mathrm{Adv}^{ss_g-cpa}_{\mathcal{PE},B,B'}(k, X_k, f, h)$ is non-negligible, then $\mathrm{Adv}^{ss-cpa}_{\mathcal{PE},A,A'}(k)$ is also non-negligible. This contradicts our supposition that $\mathcal{PE}$ is secure in the sense of SS-ATK, thus the theorem follows. □

It should be mentioned that the SS-CPA adversary can choose f at her will, while the $\mathrm{SS_G}$-CPA adversary cannot. This indicates that the former has potentially stronger power of attack than the latter. In order that the converse of the above proposition holds as well, it would be necessary to modify f so that it is computable in polynomial time and also dependent on the outputs of an SS-CPA adversary $A = (A_1, A_2)$ (see [4]).

3 A New Security Notion: Non-dividability

In the previous section, we have provided the definitions of semantic security and indistinguishability. So far the equivalence between these two notions has been shown in CPA model[7, 10], but the equivalence is less clear at least by a direct comparison of their definitions. One obstacle to a clear understanding would be that semantic security is defined by use of an auxiliary function f. Thus, in this section, we introduce a new security notion called non-dividability which is equivalent to semantic security but is described only in terms of the message space.

Before describing the security notion non-dividability, we first prepare the following definition and proposition:

Definition 6. *Let M be a message space samplable in polynomial time. The* membership problem *of a subset $Z \subset M$ is a problem to test whether $x \in Z$ or not for a given $x \in M$. Let $\mathfrak{B}_p(M)$ denote the set of subsets of M whose membership problem is computable in polynomial time.*

Proposition 1. *Let M be a message space samplable in polynomial time, and f be a function defined on M computable in polynomial time. Then, for $v \in f(M)$, $f^{-1}(v) \in \mathfrak{B}_p(M)$.*

Proof. It is obvious that, for given $v \in f(M)$, $x \in f^{-1}(v)$ if and only if $f(x) = v$. It is thus clear that the membership problem of $f^{-1}(v)$ is computable in polynomial time by testing, for given $x \in M$, whether $f(x) = v$ or not. □

The notion of non-dividability captures an adversary's inability to divide the message space into two parts in such a way that she can guess which part contains the message of a given ciphertext. We now describe the definition more precisely. Let $A = (A_1, A_2)$ be an adversary attacking an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. In the first stage of the attack by the adversary, algorithm A_1, given the public key pk, outputs a pair (M, s), where the first component is a message space samplable in polynomial time and the second one is state information. A random message x is generated from M and then encrypted to give a challenge ciphertext y. In the second stage of the attack by the adversary, algorithm A_2, given (M, s, y), tries to find a subset of M which contains the message x. If any adversary can find such a subset essentially no more than random guess, then $\mathcal{PE}$ is called secure in the sense of ND-ATK. The formal definition is as follows.

Definition 7 (Non-dividability). *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 $\mathrm{Exp}^{nd-atk-b}_{\mathcal{PE},A}(k)$
    $(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k)$; $(M, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk)$; $x_0, x_1 \leftarrow M$; $y \leftarrow \mathcal{E}_{pk}(x_1)$;
    $Z \leftarrow A_2^{\mathcal{O}_2(\cdot)}(M, s, y)$; if $x_b \in Z$ then $d \leftarrow 1$ else $d \leftarrow 0$;
    return $d$
```

where $|x| = |x'|$ for every $x, x' \in M$, $Z \in \mathfrak{B}_p(M)$, and $\mathcal{O}_1(\cdot)$ and $\mathcal{O}_2(\cdot)$ are as in definition 3. In the case of CCA2, A_2 is prohibited from asking its oracle to decrypt y. Let

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

Then $\mathcal{PE}$ is said to be secure in the sense of ND-ATK *if $\mathrm{Adv}^{nd-atk}_{\mathcal{PE},A}(k)$ is negligible for any A.*

Next we show that this notion is indeed equivalent to semantic security. The following proof may seem more complicated than expected. This is mostly because the definitions of these notions are based on different frameworks; the former is based on comparison, while the latter is based on simulator (see [4] for details of these frameworks). The essential point of the proof is merely that $v = f(x)$ if and only if $x \in f^{-1}(v)$ for given v and f; that is, what is leaked from the information $v = f(x)$ is that $x \in f^{-1}(v)$.

Theorem 2. *ND-ATK⇔SS-ATK*

Proof. (i) ND-ATK⇒SS-ATK

Suppose that an encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is secure in the sense of ND-ATK. Then $\mathcal{PE}$ is shown to be secure in the sense of SS-ATK as follows. Let $B = (B_1, B_2)$ be an SS-ATK adversary, and let $B' = (B'_1, B'_2)$ be a simulator of B defined as

```
Algorithm $B'_1(pk)$
    $(pk', sk') \leftarrow \mathcal{K}(k)$; $(M, s) \leftarrow B_1^{\mathcal{O}'_1(\cdot)}(pk')$;
    $s' \leftarrow \{s, pk', sk'\}$;
    return $(M, s')$

Algorithm $B'_2(M, s')$
    $x_1 \leftarrow M$; $y \leftarrow \mathcal{E}_{pk'}(x_1)$;
    $(v, f) \leftarrow B_2^{\mathcal{O}'_2(\cdot)}(M, s, y)$;
    return $(v, f)$
```

Note that B' can answer queries from B because she knows the secret key sk'. Now we show that $\mathrm{Adv}^{ss-atk}_{\mathcal{PE},B,B'}(k)$ is negligible for any B. For this purpose, we assume, towards contradiction, that there exists B such that $\mathrm{Adv}^{ss-atk}_{\mathcal{PE},B,B'}(k)$ is non-negligible. By using such B, let us construct an ND-ATK adversary $A = (A_1, A_2)$ as follows.

```
Algorithm $A_1^{\mathcal{O}_1(\cdot)}(pk)$
    $(M, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$;
    return $(M, s)$

Algorithm $A_2^{\mathcal{O}_2(\cdot)}(M, s, y)$
    $(v, f) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(M, s, y)$; $Z \leftarrow f^{-1}(v)$;
    return $Z$
```

Here, it is easy to see, on remembering proposition 1, that both A and B' are polynomial-time. Now, for $b \in \{0,1\}$, let us introduce $p(b)$, $p'(1)$ and $p'(0)$ by writing

$$\begin{aligned}
p(b) = \Pr[&(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (M, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk);\ x_0, x_1 \leftarrow M; \\
&y \leftarrow \mathcal{E}_{pk}(x_1);\ Z \leftarrow A_2^{\mathcal{O}_2(\cdot)}(M, s, y) :\ x_b \in Z] \\
p'(1) = \Pr[&(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (M, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk);\ x_1 \leftarrow M; \\
&y \leftarrow \mathcal{E}_{pk}(x_1);\ (v, f) \leftarrow B_2^{\mathcal{O}_2(\cdot)}(M, s, y) :\ v = f(x_1)] \\
p'(0) = \Pr[&(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (M, s) \leftarrow B'_1(pk);\ x_0 \leftarrow M; \\
&(v, f) \leftarrow B'_2(M, s) :\ v = f(x_0)]
\end{aligned}$$

respectively. From these definitions, it is straightforward to verify that

$$p(1) = p'(1) \text{ and } p(0) = p'(0),$$

and so

$$\mathrm{Adv}_{\mathcal{PE},A}^{nd-atk}(k) = p(1) - p(0) = p'(1) - p'(0) = \mathrm{Adv}_{\mathcal{PE},B,B'}^{ss-atk}(k).$$

Since we have assumed that $\mathrm{Adv}_{\mathcal{PE},B,B'}^{ss-atk}(k)$ is non-negligible, $\mathrm{Adv}_{\mathcal{PE},A}^{nd-atk}(k)$ is also non-negligible. This contradicts our supposition that $\mathcal{PE}$ is secure in the sense of ND-ATK. Thus we have ND-ATK⇒SS-ATK.

(ii) ND-ATK⇐SS-ATK

Let $B = (B_1, B_2)$ be an ND-ATK adversary. By using B, let us construct an SS-ATK adversary $A = (A_1, A_2)$ and its simulator $A' = (A'_1, A'_2)$ in the same way as above:

```
Algorithm $A_1^{\mathcal{O}_1(\cdot)}(pk)$
    $(M, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$;
    return $(M, s)$
```

```
Algorithm $A_2^{\mathcal{O}_2(\cdot)}(M, s, y)$
    $Z \leftarrow B_2^{\mathcal{O}_2(\cdot)}(M, s, y)$;
    $f \leftarrow f(x) = \begin{cases} 1 & \text{for } x \in Z, \\ 0 & \text{for } x \notin Z; \end{cases}$
    return $(1, f)$
```

```
Algorithm $A'_1(pk)$
    $(pk', sk') \leftarrow \mathcal{K}(k)$;
    $(M, s) \leftarrow A_1^{\mathcal{O}'_1(\cdot)}(pk')$;
    $s' \leftarrow \{s, pk', sk'\}$;
    return $(M, s')$
```

```
Algorithm $A'_2(M, s')$
    $x_1 \leftarrow M$; $y \leftarrow \mathcal{E}_{pk'}(x_1)$;
    $(v, f) \leftarrow A_2^{\mathcal{O}'_2(\cdot)}(M, s, y)$;
    return $(v, f)$
```

Then we again obtain

$$\mathrm{Adv}_{\mathcal{PE},A,A'}^{ss-atk}(k) = \mathrm{Adv}_{\mathcal{PE},B}^{nd-atk}(k).$$

Therefore, if $\mathrm{Adv}_{\mathcal{PE},B}^{nd-atk}(k)$ is non-negligible, then $\mathrm{Adv}_{\mathcal{PE},A,A'}^{ss-atk}(k)$ is also non-negligible. This completes the presentation that ND-ATK⇐SS-ATK, so the theorem follows. □

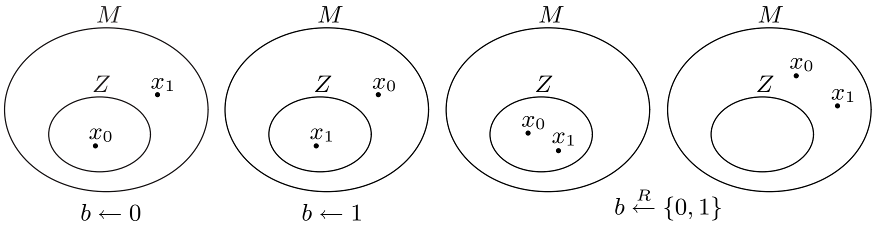

Fig. 2. Reduction of an ND-ATK adversary to an IND-ATK adversary

4 Equivalence among ND-ATK, SS-ATK and IND-ATK

In this section, we show that non-dividability is equivalent to indistinguishability under any attack model. The proof of the direct part is easy to show. Thus we now outline the proof of the converse part. Let x_0 and x_1 be two messages randomly generated from a message space M. A random one of x_0 and x_1, say x_b, is selected and then encrypted to give a challenge ciphertext y. Suppose that given y an ND-ATK adversary divides M into two parts. We wish, by using this adversary, to construct an IND-ATK adversary to guess the bit b. Observe that, if x_0 is in one of the two parts and x_1 is in the other, then the ND-ATK adversary can guess the bit b only by checking which part contains the message of y, i.e. x_b (see figure 2). Since this situation occurs with non-negligible probability, it follows that we can construct a required IND-ATK adversary. Below we describe this more precisely.

Theorem 3. *ND-ATK⇔IND-ATK*

Proof. (i) ND-ATK⇒IND-ATK

Let $B = (B_1, B_2)$ be an IND-ATK adversary. By using B, let us construct an ND-ATK adversary $A = (A_1, A_2)$ as follows.

```
Algorithm $A_1^{\mathcal{O}_1(\cdot)}(pk)$
    $(x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$;
    $M \leftarrow \{x_0, x_1\}$; $s' \leftarrow \{x_0, x_1, s\}$;
    return $(M, s')$
```

```
Algorithm $A_2^{\mathcal{O}_2(\cdot)}(M, s', y)$
    $b \leftarrow B_2^{\mathcal{O}_2(\cdot)}(x_0, x_1, s, y)$; $Z \leftarrow x_b$;
    return $Z$
```

It is clear that A is polynomial-time. Here, for $b \in \{0,1\}$, let us define $p(b)$ and $p'(b)$ as

$$\begin{aligned}
p(b) &= \Pr[(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (M, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk);\ x_0, x_1 \leftarrow M; \\
&\qquad y \leftarrow \mathcal{E}_{pk}(x_1);\ Z \leftarrow A_2^{\mathcal{O}_2(\cdot)}(M, s, y) : x_b \in Z] \\
&= \Pr[(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (M, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk);\ x_0, x_1 \leftarrow M; \\
&\qquad y \leftarrow \mathcal{E}_{pk}(x_b);\ Z \leftarrow A_2^{\mathcal{O}_2(\cdot)}(M, s, y) : x_1 \in Z] \\
p'(b) &= \Pr[(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk); \\
&\qquad y \leftarrow \mathcal{E}_{pk}(x_b);\ d \leftarrow B_2^{\mathcal{O}_2(\cdot)}(x_0, x_1, s, y) : d = 1]
\end{aligned}$$

respectively. Then it is clear from the construction of A that $p(b) = p'(b)$ for $b \in \{0,1\}$, and so

$$\mathrm{Adv}^{nd-atk}_{\mathcal{PE},A}(k) = p(1) - p(0) = p'(1) - p'(0) = \mathrm{Adv}^{ind-atk}_{\mathcal{PE},B}(k).$$

Therefore, if $\mathrm{Adv}^{ind-atk}_{\mathcal{PE},B}(k)$ is non-negligible, then $\mathrm{Adv}^{nd-atk}_{\mathcal{PE},A}(k)$ is also non-negligible. This completes the presentation that ND-ATK⇒IND-ATK.

(ii) ND-ATK⇐IND-ATK

Let $B = (B_1, B_2)$ be an ND-ATK adversary. By using B, let us construct an IND-ATK adversary $A = (A_1, A_2)$ as follows.

```
Algorithm $A_1^{\mathcal{O}_1(\cdot)}(pk)$
    $(M, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk)$;
    $x_0, x_1 \leftarrow M$; $s' \leftarrow \{M, s\}$
    return $(x_0, x_1, s')$
```

```
Algorithm $A_2^{\mathcal{O}_2(\cdot)}(x_0, x_1, s', y)$
    $Z \leftarrow B_2^{\mathcal{O}_2(\cdot)}(M, s, y)$;
    if $(x_0 \in Z \wedge x_1 \notin Z)$ then $d \leftarrow 0$;
    if $(x_1 \in Z \wedge x_0 \notin Z)$ then $d \leftarrow 1$;
     else $d \overset{R}{\leftarrow} \{0,1\}$;
    return $d$
```

It is clear that A is polynomial-time. Now, for $b \in \{0,1\}$, let us define $p(b)$ and $p'(b)$ as

$$\begin{aligned}
p(b) &= \Pr[(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (x_0, x_1, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk);\ y \leftarrow \mathcal{E}_{pk}(x_b); \\
&\qquad d \leftarrow A_2^{\mathcal{O}_2(\cdot)}(x_0, x_1, s, y) :\ d = 1] \\
p'(b) &= \Pr[(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (M, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk);\ x_0, x_1 \leftarrow M;\ y \leftarrow \mathcal{E}_{pk}(x_1); \\
&\qquad Z \leftarrow B_2^{\mathcal{O}_2(\cdot)}(M, s, y) :\ x_b \in Z] \\
&= \Pr[(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(k);\ (M, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(pk);\ x_0, x_1 \leftarrow M;\ y \leftarrow \mathcal{E}_{pk}(x_b); \\
&\qquad Z \leftarrow B_2^{\mathcal{O}_2(\cdot)}(M, s, y) :\ x_1 \in Z]
\end{aligned}$$

respectively. Here observe that A_2 outputs 1 not only when $x_1 \in Z \wedge x_0 \notin Z$ but also as a result of the coin flip $d \overset{R}{\leftarrow} \{0,1\}$. With this observation in mind, we obtain

$$\begin{aligned}
p(1) &= p'(1)\bigl(1 - p'(0)\bigr) + \frac{1}{2}\bigl\{p'(1)p'(0) + \bigl(1 - p'(1)\bigr)\bigl(1 - p'(0)\bigr)\bigr\} \\
&= \frac{1}{2} + \frac{1}{2}\bigl(p'(1) - p'(0)\bigr).
\end{aligned}$$

It thus follows that

$$\mathrm{Adv}^{ind-atk}_{\mathcal{PE},A}(k) = p(1) - p(0) = 2p(1) - 1 = p'(1) - p'(0) = \mathrm{Adv}^{nd-atk}_{\mathcal{PE},B}(k).$$

Therefore, if $\mathrm{Adv}^{nd-atk}_{\mathcal{PE},B}(k)$ is non-negligible, then $\mathrm{Adv}^{ind-atk}_{\mathcal{PE},A}(k)$ is also non-negligible. This completes the presentation that ND-ATK⇐IND-ATK, so the theorem follows. □

This, together with the theorem in the previous section, at once yields the equivalence between semantic security and indistinguishability.[2]

Theorem 4. *SS-ATK⇔IND-ATK*

5 Conclusion

In this paper, we studied the relation between semantic security and indistinguishability against chosen ciphertext attacks. First, we extended the definition of semantic security to CCA models and confirmed that this extension is valid. Next, we introduced a new security notion called non-dividability which is independent of the attack model and is described only in terms of the message space. This notion is shown to be equivalent to both of the two notions, and hence we got that semantic security and indistinguishability are equivalent under any form of attack.

Acknowledgement

The first author acknowledges support from the Special Postdoctoral Researchers Program administered by RIKEN (The Institute of Physical and Chemical Research).

References

[1] J. H. An, Y. Dodis and T. Rabin, On the security of joint signature and encryption, In *Proceedings of Advances in Cryptology – Eurocrypt 2002*, Lecture Notes in Computer Science Vol. 2332, L. Knudsen ed., pp. 83–107, Springer-Verlag, 2002. 83

[2] 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., pp. 26–45, Springer-Verlag, 1998. The latest version is available from http://www-cse.ucsd.edu/users/mihir/ 72, 73, 74, 75

[3] 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., pp. 92–111, Springer-Verlag, 1994. 72

[4] 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., pp. 519–536, Springer-Verlag, 1999. 78, 79

[5] 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., pp. 13–25, Springer-Verlag 1998. 72

[2] We note that the result holds independent of attack models and the equivalence is also valid for generalized CCA, a slight relaxation of chosen ciphertext attacks (see, e.g., [1]).

[6] D. Dolev, D. Dwork and M. Naor, Non-malleable cryptography, In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pp. 542–552, 1991; 71

D. Dolev, D. Dwork and M. Naor, Non-malleable cryptography, *SIAM Journal on Computing* **30**, pp. 391–437, 2000.

[7] O. Goldreich, Foundations of cryptography: basic tools, Cambridge: New York, Cambridge University Press, 2001. The Volume II of this book is available from http://www.wisdom.weizmann.ac.il/~oded/PSBookFrag/enc2.ps 72, 73, 74, 78

[8] O. Goldreich, Foundations of cryptography, Volume II (third posted version), 2002.
available from http://www.wisdom.weizmann.ac.il/~oded/PSBookFrag/enc.ps 72

[9] O. Goldreich, A uniform complexity treatment of encryption and zero-knowledge, Journal of Cryptology, Vol. 6, pp. 21–53, 1993.

[10] S. Goldwasser and S. Micali, Probabilistic encryption. *Journal of Computer and System Sciences* **28**, pp. 270–299, 1984. 71, 72, 73, 74, 78

[11] S. Micali, C. Rackoff and R. Sloan, The notion of security for probabilistic cryptosystems, *SIAM Journal on Computing* **17**, pp. 412–426, 1988.

[12] 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. 72

[13] 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. 72

[14] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal* **28**, pp. 656–715, 1949. 71, 74

[15] 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. 72

[16] A. Yao, Theory and applications of trapdoor functions, In *Proceedings of the 23rd Symposium on Foundations of Computer Science*, pp. 80–91, IEEE, 1982.