On a zero-knowledge property of arguments of knowledge based on secure public key encryption schemes

Yodai Watanabe[1]*

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

Abstract. This paper considers a weak variant on the notion of zero-knowledge. The weak notion is compatible with the chosen ciphertext security. In fact, arguments of knowledge based on *IND-CCA* encryption schemes are shown to be statistical zero-knowledge in that sense.

Key words: Arguments of knowledge, Chosen ciphertext security, Ciphertext indistinguishability, Public key encryption schemes, Statistical zero-knowledge

1 Introduction

The notion of ciphertext indistinguishability against chosen ciphertext attacks is one of the most important and fundamental notions in public key cryptography. In fact, the security of the notion is commonly considered as the strongest[1, 10, 19], and so in proposing a provably secure encryption schemes, the notion is usually employed as the security goal of the scheme[3, 5, 18]. The aim of this paper is to characterize the security of ciphertext indistinguishability in the light of the notion of zero-knowledge. Here, one obstacle to relate the security of encryption schemes and the zero-knowledge property is that in the public key scenario, instances of a language of interest (pairs of public and secret keys) are usually distributed according to a prescribed distribution induced by key generation algorithm; in particular in considering the chosen ciphertext security, it is essential that the advantage of an adversary is estimated by taking the expectation over the instance distribution. Thus, for the compatibility with the chosen ciphertext security, this paper formalizes a weak variant on the notion of zero-knowledge which takes the instance distribution into account. Further, this paper introduces a novel security notion called statistical simulatability as an extension of semantic security, and then shows the equivalence with ciphertext indistinguishability. This equivalence implies that for any adversary in the sense of ciphertext indistinguishability, there exists a simulator whose output is statistically indistinguishable from that of the adversary. This simulatability leads

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

to a general result: arguments of knowledge based on IND-CCA encryption schemes are statistical zero-knowledge in the weak sense.

The rest of this paper is organized as follows. In section 2, we provide some basic definitions, and then formalize a weak variant on the notion of zero-knowledge. In section 3, we introduce a novel security notion called statistical simulatability as an extension of semantic security. This security notion is shown to be equivalent to ciphertext indistinguishability in section 4. Section 5 is devoted to showing a general result which relates ciphertext indistinguishability with the weak notion of zero-knowledge.

2 A variant on the notion of zero-knowledge

In this section, we introduce a weak variant on the notion of zero-knowledge. We first recall the ordinary notions of arguments of knowledge and zero-knowledge in order to make the difference clear, and then give the definitions of the corresponding weak notions.

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). *Let* L *be a language. A function* $\epsilon : L \to \mathbb{R}$*,* $x \mapsto \epsilon(x)$*, is called* negligible *if*

$$\forall c \geq 0 \exists k_c \forall x \in L\big(|x| > k_c \Rightarrow 0 \leq \epsilon(x) < k^{-c}\big).$$

Also, a function from $\mathbb{N}$ *to* $\mathbb{R}$ *is called* negligible *if it is negligible as a function from* L *to* $\mathbb{R}$ *with* $L = \{1^k\}_{k \in \mathbb{N}}$*.*

Definition 3 (Statistical indistinguishability). *Let* L *be a language, and let* $\{X_x\}_{x \in L}$ *and* $\{Y_x\}_{x \in L}$ *be families of random variables. Denote by* $d_V(X, Y)$ *the variation distance between the probability distributions of* X *and* Y*, i.e.*

$$d_V(X, Y) = \frac{1}{2} \sum_z \big|\Pr[X = z] - \Pr[Y = z]\big|,$$

where the summation is taken over all possible assignments of X *(and* Y*). Then* $\{X_x\}_{x \in L}$ *and* $\{Y_x\}_{x \in L}$ *are said to be* statistically indistinguishable *if* $d_V(X_x, Y_x)$ *is negligible.*

The notion of proofs of knowledge, introduced in [13], formalizes the following requirements for interactive proof systems: one party (called the prover) with some specific information can convince the other party (called the verifier), but any prover without the information cannot convince the verifier. Here, the first requirement is called the non-triviality, and the second one is called the validity. The verifier is assumed to be polynomial-time, while in general, the prover is assumed to be computationally unbounded. The notion of arguments of knowledge is a relaxed variant of proofs of knowledge where the prover is also assumed to be polynomial-time. We now give the basic (but less general) definition of arguments of knowledge. The reader may wish to consult e.g. [2, 9] for the definition of proofs of knowledge satisfactory in the general scenario.

Definition 4 (System for arguments of knowledge). *Let R be a binary relation, and $L_R = \{x | \exists y((x, y) \in R)\}$. A pair of interactive machines (P, V) is called* a system for arguments of knowledge for R *if they are polynomial-time and the following two conditions hold:*

1. *Non-triviality: For every $(x, y) \in R$, V accepts the interaction with P on common input x and auxiliary input y with probability 1, i.e.*
$$\Pr[\langle P(y), V\rangle(x) = 1] = 1,$$
2. *Validity: For every $x \in L_R$ and every polynomial-time interactive machine P^*, V accepts the interaction with P on common input x with negligible probability, i.e.*
$$\Pr[\langle P^*, V\rangle(x) = 1] \leq \epsilon(x)$$
for some negligible function $\epsilon : L \to \mathbb{R}$,

where the probability is taken over all the internal coin tosses of the algorithms.

The notion of zero-knowledge, introduced in [13], formalizes the following requirement for interactive proof systems: whatever can be efficiently computed from the interaction with the prover can also be computed efficiently without the interaction in a sufficiently indistinguishable manner. There are three types of the indistinguishability commonly considered in the literature, and they yield different notions of zero-knowledge, namely perfect, statistical and computational zero-knowledge. The formal definition of statistical zero-knowledge are described below. An alternative but equivalent definition can be made by considering the verifier's view of the interaction with the prover. See e.g. [9] for these related definitions.

Definition 5 (Statistical zero-knowledge). *Let (P, V) be a system for arguments of knowledge for a binary relation R. Let $L_R = \{x | \exists y((x, y) \in R)\}$ and $R(x) = \{y | (x, y) \in R\}$. Then (P, V) is said to be* statistical zero-knowledge for R *if for every probabilistic polynomial-time interactive machine V^*, there exists a probabilistic polynomial-time algorithm M such that the families of random variables, $\{\langle P(y_x), V^*\rangle(x)\}_{x \in L_R}$ and $\{M(x)\}_{x \in L_R}$, are statistically indistinguishable for all possible $y_x \in R(x)$, where $\langle P(y_x), V^*\rangle(x)$ represents the output of V^* after it interacts with P on common input $x \in L_R$ and auxiliary input $y_x \in R(x)$.*

We have provided the definitions concerning the notion of zero-knowledge. The definitions are, of course, satisfactory for the ordinary purpose; however, for the present purpose, more relaxed definitions are desirable because instances of a language are assumed to be distributed according to a prescribed distribution. Hence, to describe such a situation, we now consider the definition of an probabilistic polynomial-time algorithm which samples the instances of a language.

Definition 6 (Instance generation algorithm). *Let R be a binary relation, and $L_R = \{x | \exists y((x, y) \in R)\}$. A probabilistic polynomial-time algorithm G is called an* instance generation algorithm for R *if G takes $x \in L_R$ and outputs $(x', y') \in R$. For an instance generation algorithm G and $i \in \{1, 2\}$, the random variable corresponding to the i-th component of the output of G will be denoted by G_i.*

Based on this definition, one can straightforwardly extend definitions 4 and 5 to the situation where the security of a system of interest is formalized by taking the expectation over the instance distribution. The extended definitions are described below.

Definition 7 (System for expected arguments of knowledge). *Let R be a binary relation, and $L_R = \{x | \exists y((x, y) \in R)\}$. A pair of interactive machines (P, V) together with an instance generation algorithm G for R is called* a system for expected arguments of knowledge for R *if they are polynomial-time and the following two conditions hold:*

1. *Expected non-triviality: For every $x \in L_R$, V accepts the interaction with P on common input G_1 and auxiliary input G_2 with probability 1, i.e.*

$$\Pr[\langle P(G_2(x)), V\rangle(G_1(x)) = 1] = 1,$$

2. *Expected validity: For every polynomial-time interactive machine P^*, V accepts the interaction with P^* on common input G_1 with negligible probability, i.e.*

$$\Pr[\langle P^*, V\rangle(G_1(x)) = 1] \leq \epsilon(x)$$

for some negligible function $\epsilon : L_R \to \mathbb{R}$,

where the probability is taken over all the internal coin tosses of the algorithms.

Definition 8 (Expected statistical zero-knowledge). *Let $((P, V), G)$ be a system for expected arguments of knowledge for a binary relation R. Let $L_R = \{x | \exists y((x, y) \in R)\}$. Then $((P, V), G)$ is said to be* expected statistical zero-knowledge for R *if for every probabilistic polynomial-time interactive machine V^*, there exists a probabilistic polynomial-time algorithm M such that the families of random variables,*

$$\{\langle P(G_2(x)), V^*\rangle(G_1(x))\}_{x \in L_R} \text{ and } \{M(G_1(x))\}_{x \in L_R},$$

are statistically indistinguishable, where $\langle P(G_2), V^*\rangle(G_1)$ represents the output of V^* after it interacts with P on common input G_1 and auxiliary input G_2.

These notions are weaker than the original ones in the following sense.

Proposition 1. *(i) Let (P, V) be a system for arguments of knowledge for a binary relation R. Then for every instance generation algorithm G, $((P, V), G)$ is expected arguments of knowledge for R. (ii) Let (P, V) be a system for arguments of knowledge for a binary relation R. Suppose that (P, V) is statistical zero-knowledge for R. Then for every instance generation algorithm G, $((P, V), G)$ is expected statistical zero-knowledge for R.*

Proof. The proof readily follows from the following lemma. □

Lemma 1. *Let $((P, V), G)$ be a system for expected arguments of knowledge for a binary relation R, and $L_R = \{x | \exists y((x, y) \in R)\}$. Then there exists a constant $c > 0$ such that*

$$\Pr\left[x' \leftarrow G_1(x) : |x'| \leq |x|^c\right] \leq \epsilon(x)$$

for some negligible function $\epsilon : L_R \to \mathbb{R}$.

Proof. Let $q_z(x) = \Pr[x' = z | x' \leftarrow G_1(x)]$. Note that, for each $x \in L_R$,

$$\sum_{z \in \{0,1\}^*} q_z(x) = 1 \text{ and } q_z(x) \geq 0 \text{ for all } z \in \{0, 1\}^*.$$

Hence there exists $z_x \in \{0, 1\}^*$ such that $q_{z_x}(x) \geq q_z(x)$ for all $z \in \{0, 1\}^*$. Consider now the prover P^* which runs G to generate (x', y') and calls P on common input x' and auxiliary input y'. Here, if $q_{z_x}(x)$ is non-negligible, then

$$\Pr[\langle P^*, V\rangle(G_1(x)) = 1] \geq \left(q_{z_x}(x)\right)^2$$

is also non-negligible. This contradicts the expected validity of the system, and so $q_{z_x}(x)$ must be negligible. Thus there exists a constant $c > 0$ and an integer k such that

$$|x| > k \Rightarrow |x|^{2c} < -\log\left(q_{z_x}(x)\right).$$

Define now

$$n_{x;c} = \#\left\{x' \middle| \Pr\left[x' \leftarrow G_1(x) : |x'| < |x|^c\right] > 0\right\}.$$

It readily follows that

$$n_{x;c} < \left(q_{z_x}(x)\right)^{-\frac{1}{2}}.$$

As a consequence, we obtain

$$|x| > k \Rightarrow \Pr\left[x' \leftarrow G_1(x) : |x'| < |x|^c\right] \leq n_{x;c} q_{z_x}(x) < \left(q_{z_x}(x)\right)^{\frac{1}{2}},$$

so the lemma follows.

3 A novel security notion: statistical simulatability

One purpose of this paper is to characterize the security of ciphertext indistinguishability in a more detail than the literature. Note that the strength of security notions is usually investigated by reduction methodology, or in other words, by comparing their relative strength. Thus, for use of comparison, we introduce a novel security notion called statistical simulatability as an extension of semantic security, and then provide an intuitive explanation of the notion.

We begin with recalling the two fundamental security notions mentioned above, i.e. ciphertext indistinguishability and semantic security. The notion of ciphertext indistinguishability, introduced in [12], formalizes the following requirement for encryption schemes: given a ciphertext of one of two plaintexts any adversary cannot distinguish which one is encrypted. Since ciphertext indistinguishability is easy to use, it is conventional to employ the notion in analyzing the security of practical encryption schemes (e.g. [3, 5, 18]). The formal definition is described below.

Definition 9 (Ciphertext indistinguishability). *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let $A = (A_1, A_2)$ be a polynomial-time adversary. For $atk \in \{cpa, cca1, cca2\}$ and $k \in \mathbb{N}$, consider*

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

Here $|x_0| = |x_1|$, and A is assumed to have access to the oracles $\mathcal{O}_1(\cdot)$ and $\mathcal{O}_2(\cdot)$ as follows:

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

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

$$\mathrm{Adv}_{\mathcal{PE},A}^{ind-atk}(k) = \Pr[\mathrm{Exp}_{\mathcal{PE},A}^{ind-atk}(k) = 1] - \frac{1}{2},$$

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

$$\forall A \big(\mathrm{Adv}_{\mathcal{PE},A}^{ind-atk}(k) \textit{ is negligible}\big).$$

The formulation of ciphertext indistinguishability is simple but rather artificial, and so it is less clear that it indeed captures a strong notion of privacy.

However it has been shown that the notion is equivalent to another notion called semantic security, which is a direct formalization of the intuition of privacy. Indeed, the notion of semantic security, introduced in [12], formalizes the following requirement for encryption schemes: whatever can be efficiently computed about a plaintext from its ciphertext can also be computed efficiently without the ciphertext. We now describe the formal definition based on the framework given by [4] for convenience of later extension. Other versions of the definition and related results can be found in [6, 10, 14] etc. See also [11] for a more general attacking model.

Definition 10 (Semantic security). *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let $A = (A_1, A_2)$ be a polynomial-time adversary and $A' = (A'_1, A'_2)$ be a polynomial-time algorithm which simulates A (A' is called a simulator of A). Let F be a deterministic function computable in polynomial-time. For $atk \in \{cpa, cca1, cca2\}$ and $k \in \mathbb{N}$, consider*

$$
\begin{array}{l}
\texttt{Experiment } \mathrm{Exp}^{ss-atk}_{\mathcal{PE},A,F}(k) \\
\quad (pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, h, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(1^k, pk); \\
\quad x \leftarrow M;\ z \leftarrow h(x);\ y \leftarrow \mathcal{E}_{pk}(x);\ v \leftarrow A_2^{\mathcal{O}_2(\cdot)}(s, z, y); \\
\quad \texttt{if } v = F(x, M, h, s, z) \texttt{ then } d \leftarrow 1 \texttt{ else } d \leftarrow 0; \\
\quad \texttt{return } d \\
\texttt{Experiment } \mathrm{Exp}^{ss-atk}_{\mathcal{PE},A',F}(k) \\
\quad (M, h, s) \leftarrow A'_1(1^k);\ x \leftarrow M;\ z \leftarrow h(x);\ v \leftarrow A'_2(s, z); \\
\quad \texttt{if } v = F(x, M, h, s, z) \texttt{ then } d \leftarrow 1 \texttt{ else } d \leftarrow 0; \\
\quad \texttt{return } d
\end{array}
$$

where $|x| = |x'|$ for every $x, x' \leftarrow M$, and A is assumed to have oracle access as in definition 9. Let

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

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

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

We mention that in the definition the adversary is allowed to have access to prior information of the plaintext (see [10] for the motivation of this situation).

In the above definition of semantic security, there are some factors which make the notion weaker and are removable as well (at least formally). By eliminating such factors, we now introduce a novel security notion called statistical simulatability. The formal definition is as follows.

Definition 11 (Statistical simulatability). *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. Let $A = (A_1, A_2)$ be a polynomial-time adversary and $A' = (A'_1, A'_2)$ be a polynomial-time simulator of A. Let F be a probabilistic function.*

For $atk \in \{cpa, cca1, cca2\}$ and $k \in \mathbb{N}$, consider

$$
\begin{array}{l}
\texttt{Experiment } \mathrm{Exp}^{ssm-atk}_{\mathcal{PE},A,F}(k) \\
\quad (pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, h, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(1^k, pk); \\
\quad x \leftarrow M;\ y \leftarrow \mathcal{E}_{pk}(x);\ z \leftarrow h(x);\ v \leftarrow A_2^{\mathcal{O}_2(\cdot)}(s, z, y); \\
\quad \texttt{if } F(v, x, M, h, s, z) = 1 \texttt{ then } d \leftarrow 1 \texttt{ else } d \leftarrow 0; \\
\quad \texttt{return } d \\
\texttt{Experiment } \mathrm{Exp}^{ssm-atk}_{\mathcal{PE},A',F}(k) \\
\quad (M, h, s) \leftarrow A'_1(1^k);\ x \leftarrow M;\ z \leftarrow h(x);\ v \leftarrow A'_2(s, z); \\
\quad \texttt{if } F(v, x, M, h, s, z) = 1 \texttt{ then } d \leftarrow 1 \texttt{ else } d \leftarrow 0; \\
\quad \texttt{return } d
\end{array}
$$

where $|x| = |x'|$ for every $x, x' \leftarrow M$, and A is assumed to have access to the oracles $\mathcal{O}_1(\cdot)$ and $\mathcal{O}_2(\cdot)$ as in definition 10. Let

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

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

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

Note that the definition is stronger than definition 10 in the following sense:

1. F has implicit form (or in other words, F is a relation),
2. there is no restriction on the computability of F,
3. the simulator is supposed to exist independently of F.

These modifications may seem merely technical at first sight; however, they endow a remarkable property with encryption schemes. To see this, we now show the following lemma.

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

$$
\begin{array}{l}
\texttt{Experiment } E(k) \\
\quad a \leftarrow A(1^k);\ a' \leftarrow A'(1^k);
\end{array}
$$

Let

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

Suppose that

$$\forall F (\mathrm{Adv}_{A,A',F}(k) \text{ is negligible}).$$

Then a and a' are statistically indistinguishable.

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

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

Define F_+ and F_- by

$$F_+(a) = \begin{cases} 1 & a \in \mathcal{A}_+, \\ 0 & \text{otherwise}, \end{cases} \quad \text{and} \quad F_-(a) = \begin{cases} 1 & a \notin \mathcal{A}_+, \\ 0 & \text{otherwise}, \end{cases}$$

respectively. It then follows that

$$d_V(a, a') = \frac{1}{2}\bigl(\mathrm{Adv}_{A,A',F_+}(k) + \mathrm{Adv}_{A,A',F_-}(k)\bigr).$$

Note that by the assumption, both $\mathrm{Adv}_{A,A',F_+}(k)$ and $\mathrm{Adv}_{A,A',F_-}(k)$ are negligible, so is $d_V(a, a')$. This completes the proof. □

We note that in general, the functions F_+ and F_- in the proof are not computable in polynomial-time.

The lemma at once gives the following proposition.

Proposition 2. *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. If $\mathcal{PE}$ is secure in the sense of SSM-ATK, then for every adversary there exists a simulator whose output is statistically indistinguishable from that of the adversary.*

Proof. The proof is a direct consequence of the lemma. □

As a consequence, we can see that the notion of statistical simulatability captures the following property of encryption schemes: whatever can be efficiently computed about a plaintext from its ciphertext can be efficiently reconstructed without the ciphertext in the statistically indistinguishable manner. (The name "statistical simulatability" comes from this property.) Thus this notion may seem much stronger than semantic security (and so ciphertext indistinguishability). However, as we will see in the next section, the strength of statistical simulatability coincides with that of ciphertext indistinguishability.

4 Equivalence among the security notions

In this section, we show the equivalence among the the security notions considered in the previous section.

Theorem 1. *SSM-ATK $\Leftrightarrow$ SS-ATK $\Leftrightarrow$ IND-ATK.*

Proof. We show (i) *SSM-ATK* $\Rightarrow$ *SS-ATK*, (ii) *SS-ATK* $\Rightarrow$ *IND-ATK* and (iii) *IND-ATK* $\Rightarrow$ *SSM-ATK*.

(i) 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 *SS-ATK*. Let $B = (B_1, B_2)$ be a *IND-ATK* adversary. By using B, let us construct the *SS-ATK* adversary $A = (A_1, A_2)$ and its simulator $A' = (A'_1, A'_2)$

as

`Algorithm` $A_1^{\mathcal{O}_1(\cdot)}(1^k, pk)$	`Algorithm` $A_2^{\mathcal{O}_2(\cdot)}(s, z, y)$
$(x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(1^k, pk)$;	$v \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, y)$;
$M{:=}\{x_0, x_1\}_U$; $h{:=}\varepsilon(\cdot)$;	`return` v
`return` (M, h, s)	
`Algorithm` $A_1'(1^k)$	`Algorithm` $A_2'(s', z)$
$(pk', sk') \leftarrow \mathcal{K}(1^k)$;	$y \leftarrow \mathcal{E}_{pk'}(x_1)$;
$(x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(1^k, pk')$;	$d \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, y)$;
$M{:=}\{x_0, x_1\}_U$; $h{:=}\varepsilon(\cdot)$;	`if` $d = 1$ `then` $v \leftarrow 1$ `else` $v \leftarrow 0$:
$s'{:=}(s, pk', sk', x_1)$;	`return` v
`return` (M, h, s')	

Consider the function F given by

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

Note that A' can answer queries from B because she knows the secret key sk'. Now it is convenient to denote by $E(k)$ the experiment

`Experiment` $E(k)$

$(pk, sk) \leftarrow \mathcal{K}(1^k)$; $(x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(1^k, pk)$;

$y_1 \leftarrow \mathcal{E}_{pk}(x_1)$; $y_0 \leftarrow \mathcal{E}_{pk}(x_0)$; $v_1 \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, y_1)$; $v_0 \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, y_0)$;

Then it is straightforward to show that

$$\begin{aligned} \mathrm{Adv}_{\mathcal{PE},B}^{ind-atk}(k) &= \frac{1}{2}\big|\Pr[v_0 = 0|E(k)] + \Pr[v_1 = 1|E(k)] - 1\big| \\ &= \frac{1}{2}\big|\Pr[v_0 = 0|E(k)] - \Pr[v_1 = 0|E(k)]\big| \\ &= \mathrm{Adv}_{\mathcal{PE},A,A',F}^{ss-atk}(k). \end{aligned}$$

Since $\mathcal{PE}$ is supposed to be secure in the sense of IND-ATK, the advantage $\mathrm{Adv}_{\mathcal{PE},B}^{ind-atk}(k)$ is negligible, so is $\mathrm{Adv}_{\mathcal{PE},A,A'F}^{ss-atk}(k)$. 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 SSM-ATK adversary. By using B, let us construct the IND-ATK adversary $A = (A_1, A_2)$ as

`Algorithm` $A_1^{\mathcal{O}_1(\cdot)}(1^k, pk)$	`Algorithm` $A_2^{\mathcal{O}_2(\cdot)}(s', y)$
$(M, h, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(1^k, pk)$;	$v \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, z, y)$;
$x \leftarrow M$; $z \leftarrow h(x)$;	$y' \leftarrow \mathcal{E}_{pk}(x)$; $v' \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, z, y')$;
$s' \leftarrow (s, z, x)$;	`if` $v = v'$ `then` $d \leftarrow 1$ `else` $d \leftarrow 0$;
`return` $(x, 1^{\lvert x\rvert}, s')$	`return` d

Also consider the simulator $B' = (B_1', B_2')$ of B constructed as

`Algorithm` $B_1'(1^k)$	`Algorithm` $B_2'(s', z)$
$(pk', sk') \leftarrow \mathcal{K}(1^k);$	$x \leftarrow M;$
$(M, h, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(1^k, pk');$	$y \leftarrow \mathcal{E}_{pk'}(1^{\lvert x \rvert});$
$s' \leftarrow (s, pk', sk', M);$	$v \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, z, y);$
`return` (M, h, s')	`return` v

It is now convenient to denote by $E(k)$ the experiment

`Experiment` $E(k)$

$$(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, h, s) \leftarrow B_1^{\mathcal{O}_1(\cdot)}(1^k, pk);\ x_1 \leftarrow M;\ x_0 {:=} 1^{\lvert x_1 \rvert};$$
$$z \leftarrow h(x_1);\ y_1 \leftarrow \mathcal{E}_{pk}(x_1);\ y_1' \leftarrow \mathcal{E}_{pk}(x_1);\ y_0 \leftarrow \mathcal{E}_{pk}(x_0);$$
$$v_1 \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, z, y_1);\ v_1' \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, z, y_1');\ v_0 \leftarrow B_2^{\mathcal{O}_2(\cdot)}(s, z, y_0);$$

Let us now introduce the random variable T to denote the quartet of the random variables M, h, s and z (i.e. $T = (M, h, s, z)$). Further, let $\mathcal{M}$ and $\mathcal{T}$ be the set of all possible assignments of x_1 and T respectively, and let $\Omega = \mathcal{M} \times \mathcal{T}$. Here, if we define the mapping from Ω to $[0, 1]$, $\mu : \Omega \to [0, 1]$, by

$$\mu : (m, t) \mapsto \Pr[x_1 = m, T = t],$$

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

$$X_v = p_1(v|m, t) - p_0(v|m, t),$$
$$Y_v = q_1(v|m, t) - q_0(v|m, t),$$

where

$$p_b(v|m, t) = \Pr[v_b = v|E(k), x_1 = m, T = t],$$
$$q_b(v|m, t) = \Pr[F(v, x_b, T) = 1|E(k), x_1 = m, T = t],$$

with F being an arbitrary function. Then the advantage $\mathrm{Adv}_{\mathcal{PE},A}^{ind-atk}(k)$ is now expressed, in terms of X_v and Y_v, as

$$\begin{aligned}
\mathrm{Adv}_{\mathcal{PE},A}^{ind-atk}(k) &= \frac{1}{2}\big(\Pr[v_1 = v_1'] + \Pr[v_1 \neq v_0]\big) - \frac{1}{2} \\
&= \frac{1}{2}\big(\Pr[v_1 = v_1'] - \Pr[v_1 = v_0]\big) = \frac{1}{2}\sum_{v \in \mathcal{V}} E_\mu[p_1 p_1 - p_1 p_0] \\
&= \frac{1}{4}\sum_{v \in \mathcal{V}} E_\mu[p_1 p_1 - p_1 p_0 - p_0 p_1 + p_0 p_0] = \frac{1}{4}\sum_{v \in \mathcal{V}} E_\mu[X_v^2],
\end{aligned}$$

where $p_0 = p_0(v|m, t)$ and $p_1 = p_1(v|m, t)$ for short, and $E_\mu[\cdot]$ denotes the expectation with respect to the probability measure μ. Note that the third equality follows from the conditional independence among the random variables. Similarly, the advantage $\mathrm{Adv}^{ssm-atk}_{\mathcal{PE},B,B',F}(k)$ is expressed as

$$\begin{aligned}\mathrm{Adv}^{ssm-atk}_{\mathcal{PE},B,B',F}(k) &= \frac{1}{2}\big(\Pr[F(v_1,x_1,T)=1]+\Pr[F(v_0,x_0,T)=1] \\ &\qquad -\Pr[F(v_0,x_1,T)=1]-\Pr[F(v_0,x_0,T)=1]\big) \\ &= \frac{1}{4}\sum_{v\in\mathcal{V}} E_\mu[X_vY_v].\end{aligned}$$

These expressions may facilitate the comparison between the advantages. In fact it is easy to see that

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

for $v,w\in\mathcal{V}$. Further, since q_0 and q_1 are conditional probabilities, it can be shown that

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

These inequalities give that

$$\mathrm{Adv}^{ind-atk}_{\mathcal{PE},A}(k)\geq\big(\mathrm{Adv}^{ssm-atk}_{\mathcal{PE},B,B',F}(k)\big)^2.$$

Since $\mathcal{PE}$ is supposed to be secure in the sense of IND-ATK, the advantage $\mathrm{Adv}^{ind-atk}_{\mathcal{PE},A}(k)$ is negligible, so is $\mathrm{Adv}^{ssm-atk}_{\mathcal{PE},B,B',F}(k)$. Hence the theorem follows. □

We state that the proof of the assertion (ii) can be found in the literature (see e.g. [6, 10, 19]), and hence the essential contribution of this paper in the proof is to show the assertion (iii).

5 Arguments of knowledge based on secure public key encryption schemes

Public key encryption schemes can be used to construct a system for (expected) arguments of knowledge. The idea is based on the fact that the party with secret key can decrypt a ciphertext, while any party without the secret key cannot. We now give the definitions describing such a system.

Definition 12 (Relation and instance generation algorithm induced by an encryption scheme). *Let $\mathcal{PE}=(\mathcal{K},\mathcal{E},\mathcal{D})$ be an public key encryption scheme. A binary relation R is said to be* induced by $\mathcal{PE}$ *if*

$$R(x,y)=1\Leftrightarrow\exists k\in\mathbb{N}(\Pr[x=pk,y=sk|(pk,sk)\leftarrow\mathcal{K}(1^k)]>0).$$

Also, an algorithm G is called the instance generation algorithm induced by $\mathcal{PE}$ *if it is given by $G(x)=\mathcal{K}(1^{|x|})$.*

Definition 13 (System for interactive protocol based on an encryption scheme). *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an public key encryption scheme. A pair of interactive machines (P, V) is called a* system for the interactive protocol based on $\mathcal{PE}$ *if it is constructed as follows:*

1. *Initialization: Set the security parameter k and runs the key generation algorithm $\mathcal{K}$ on input 1^k to generate a matching pair (pk, sk) of public and secret keys. Set the common and auxiliary inputs as follows:*
   - *Common input: 1^k and pk.*
   - *Auxiliary input (to the prover): sk.*
2. *Verifier's first step (V1): Compute $x \leftarrow \{0,1\}^k_U$; $y \leftarrow \mathcal{E}_{pk}(x)$ and send y to the prover.*
3. *Prover's first step (P1): Compute $x' \leftarrow \mathcal{D}_{sk}(y)$ and send x' to the verifier.*
4. *Verifier's second step (V2): Check whether or not $x' = x$ and output 1 iff the equality holds.*

It is plausible that if an encryption scheme is secure, then a system constructed as above has the expected non-triviality and expected validity. Moreover, if an encryption scheme is ciphertext indistinguishable against chosen ciphertext attacks, then a system constructed as above has the expected zero-knowledge property as well. We now show this in the following theorem.

Theorem 2. *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public key encryption scheme, and suppose that $\mathcal{PE}$ is secure in the sense of IND-CCA. Let R be the binary relation induced by $\mathcal{PE}$, and G be the instance generation algorithm induced by $\mathcal{PE}$. Further, let (P, V) be a system for the interactive protocol based on $\mathcal{PE}$. Then $((P, V), G)$ is an expected statistical zero-knowledge arguments of knowledge for R.*

Proof. (i) Expected non-triviality: The expected non-triviality follows from the condition $\mathcal{D}_{sk}(\mathcal{E}_{pk}(x)) = x$ for all x and (pk, sk).

(ii) Expected validity: Suppose that there exists a probabilistic polynomial-time interactive machine P^* such that $\Pr[\langle P^*, V\rangle(G_1(x)) = 1]$ is non-negligible as a function from L_R to $\mathbb{R}$. Then by using P^* we can construct an adversary which breaks $\mathcal{PE}$ with non-negligible probability. This contradicts ciphertext indistinguishability of $\mathcal{PE}$, so the expected validity follows.

(iii) Expected zero-knowledge: Let V^* be a probabilistic polynomial-time interactive machine interacting with P. By using V^*, let us construct the *SSM-CCA* adversary $A = (A_1, A_2)$ attacking $\mathcal{PE}$ as

$$
\begin{array}{l|l}
\texttt{Algorithm } A_1^{\mathcal{D}_{sk}(\cdot)}(1^k, pk) & \texttt{Algorithm } A_2^{\mathcal{O}_2(\cdot)}(r, y) \\
\quad (x, s) \leftarrow V_1^*(1^k, pk); & \quad \texttt{return } r \\
\quad y \leftarrow \mathcal{D}_{sk}(x);\ r \leftarrow V_2^*(s, y); & \\
\quad \texttt{return } (\{0,1\}^k_U, \varepsilon(\cdot), r) &
\end{array}
$$

where V_i^* $(i \in \{1, 2\})$ represents the machine V^* at the i-th step, and we have introduced state information s to explicitly indicate that V_1^* and V_2^* constitute one machine V^*. Note that, since chosen ciphertext attacks are allowed to A, A_1 has oracle access to $\mathcal{D}_{sk}(\cdot)$. Now, remember that $\mathcal{PE}$ is IND-CCA. It thus follows from theorem 1 that $\mathcal{PE}$ is also SSM-CCA. Therefore there exists a simulator A' whose output is statistically indistinguishable from that of A. By using A', let us define $M(1^k, pk) = [A'_1(1^k)]_3$, where $[A'_1]_3$ denotes the third component of the output of A'_1 (i.e. r). Then it is easy to see that

$$\left\{\langle P(G_2(x)), V^*\rangle(G_1(x))\right\}_{x\in L_R} \text{ and } \left\{M(G_1(x))\right\}_{x\in L_R}$$

are statistically indistinguishable, so the theorem follows. □

Acknowledgement

The author is grateful to Dr. Junji Shikata for discussions.

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.
2. M. Bellare and O. Goldreich, *On defining Proofs of Knowledge*, In Proceedings of Advances in Cryptology – Crypto'92, Lecture Notes in Computer Science Vol. 740, E. Brickell ed., Springer-Verlag, Berlin, 1992, pp. 390–420.
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., Springer-Verlag, Berlin, 1994, pp. 92–111.
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., Springer-Verlag, Berlin, 1999, pp. 519–536.
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., Springer-Verlag, Berlin, 1998, pp. 13–25.
6. Y. Dodis, *Introduction to Cryptography*, Lecture Notes at New York University, 2001.
7. 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.
8. U. Feige, A. Fiat and A. Shamir, *Zero knowledge proofs of identity*, Journal of Cryptology, Vol. 1, pp. 77–94, 1988.
9. O. Goldreich, *Foundations of cryptography: basic tools*, Cambridge University Press, Cambridge, 2001.
10. O. Goldreich, Foundations of cryptography, Volume II, 2002. available from http://www.wisdom.weizmann.ac.il/~oded/foc.html

11. O. Goldreich, Y. Lustig and M. Naor, On Chosen Ciphertext Security of Multiple Encryptions, available from http://eprint.iacr.org/2002/089/
12. S. Goldwasser and S. Micali, Probabilistic encryption, *Journal of Computer and System Sciences* **28**, pp. 270–299, 1984.
13. S. Goldwasser, S. Micali and C. Rackoff, *The Knowledge Complexity of Interactive Proof Systems*, SIAM Journal on Computing, Vol. 18, 1989, pp. 186–208.
14. S. Micali, C. Rackoff and R. Sloan, The notion of security for probabilistic cryptosystems, *SIAM Journal on Computing* **17**, pp. 412–426, 1988.
15. 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.
16. 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.
17. C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal* **28**, pp. 656–715, 1949.
18. 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.
19. 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.