数理解析研究所講究録
1148巻 2000年 112-117

A New Definition of Semantic Security for Public-Key Encryption Schemes

Hideaki Sakai(酒井 秀晃), Noriko Nakamura(中村 雅子), Yoshihide Igarashi(五十嵐 善英)

Department of Computer Science, Gunma University
1-5-1 Tenjin-cho, Kiryu 376-8515, Japan

We introduce a new definition of semantic security. The new definition is valid against not only chosen-plaintext attacks but also chosen-ciphertext attacks whereas the original one, due to Goldwasser and Micali, is defined against only chosen-plaintext attacks. We show that semantic security formalized by the new definition is equivalent to indistinguishability for each of chosen-plaintext attacks, non-adaptive chosen-ciphertext attacks, and adaptive chosen-ciphertext attacks.

1 Introduction

Various notions of security for public-key encryption have been discussed [1, 2, 3, 4, 5, 6, 8, 9]. A way to define a notion of secure encryption is by giving a pair of a possible goal and a particular attack model. The goals are indistinguishability (IND) of encryptions due to Goldwasser and Micali, referred as polynomial security [6], non-malleability (NM) due to Dolev, Dwork and Naor [4], plaintext awareness (PA) [2] and one-wayness (OW) [5]. Chosen-plaintext attack (CPA), non-adaptive chosen-ciphertext attack (CCA1) and adaptive chosen-ciphertext attack (CCA2) are popular different attack models. The notions of IND-CPA, IND-CCA1 and IND-CCA2 were given in [6], [8] and [9], respectively. The notions of NM-CPA, NM-CCA1 and NM-CCA2 were given in [4]. Relations among these notions of security were discussed in [1, 3, 4, 5].

Goldwasser and Micali [6] proposed two different definitions, polynomial security, referred to IND-CPA, and semantic security, and proved that the first notion implies the second. Micali, Rackoff and Sloan [7] proved that all of polynomial security, semantic security, and the definition by Yao [10] are equivalent.

In this paper we introduce a new definition of semantic security, which we believe a simple and clear formalization of security for public-key encryption schemes. The new definition is valid against not only CPA but also CCA1 and CCA2. We show that semantic security formalized by the new definition is equivalent to IND for any attack in {CPA, CCA1, CCA2}.

2 Preliminaries

We employ a number of definitions and notations for secure encryption from [1, 3, 4, 5]. Indistinguishability (IND) formalizes the inability of an adversary to learn any information about the plaintext underlying a challenge ciphertext. The notion of non-malleability (NM) was defined as an extension of semantic security [4]. It formalizes the inability of an adversary to output a ciphertext y' whose underlying plaintext x' is meaningfully related to the plaintext x underlying a challenge ciphertext y. Plaintext awareness (PA) formalizes an adversary's inability to create a ciphertext y without knowing its underlying plaintext x, and it has only been defined in the random-oracle [2]. One-wayness (OW) is defined by the adversary's inability, given a challenge ciphertext y, to decrypt y and get the whole plaintext x [5]. Under chosen plaintext attack (CPA) for the public-key encryption scheme, the adversary can obtain ciphertexts of chosen plaintexts by the public-key. Under non-adaptive chosen ciphertext attack (CCA1), the adversary can have

access to an oracle for the decryption function for a period before obtaining the challenge ciphertext. Under adaptive chosen-ciphertext attack (CCA2), the adversary can have access to an oracle for the decryption function even after obtaining the challenge ciphertext y, with only restriction that the adversary cannot ask for the decryption of y itself by the oracle.

- $\mathcal{K}$: a probabilistic algorithm, called the key generation algorithm, takes a security parameter $k \in \mathsf{N}$, provided in unary, and returns a pair of public and secret keys, (pk, sk), where N is the set of natural numbers. A valid message space $M^{(k)}$ consisting of strings with the same length is specified by a probabilistic algorithm with input pk. That is, $M^{(k)}$ is a probabilistic space induced by (pk, sk) such that for any pair of x and x' in $M^{(k)}$, $|x| = |x'|$. As a special case of the valid message space induced by (pk, sk), we may choose the set of all binary sequences with length k, denoted by M_k.
- $\mathcal{E}$: a probabilistic algorithm, called the encryption algorithm, that takes a public-key pk and a message $x \in \{0,1\}^*$, and then returns a ciphertext y. The encryption value y given by $\mathcal{E}$ on pk and x is denoted by $y \leftarrow \mathcal{E}_{pk}(x)$.
- $\mathcal{D}$: a deterministic algorithm, called the decryption algorithm, that takes a secret key sk and ciphertext y and returns either a message $x \in \{0,1\}^*$ or a special symbol $\perp$ indicating that the ciphertext is invalid. The decryption algorithm derived from the secret key sk is denoted by $\mathcal{D}_{sk}$, and its decryption value x on y is denoted by $x \leftarrow \mathcal{D}_{sk}(y)$.
- $A = (A_1, A_2)$: an adversary, a pair of probabilistic algorithms A_1 and A_2.

We require that $\mathcal{K}$, and $\mathcal{E}$ and $\mathcal{D}$ should be probabilistic polynomial time algorithms, and that $\mathcal{D}$ is a deterministic polynomial time algorithm. We say that an adversary $A = (A_1, A_2)$ is polynomial if both A_1 and A_2 are polynomial-time probabilistic algorithms. A function $f : \mathsf{N} \to \mathsf{R}$ is said to be *negligible* if for every constant $c \geq 0$ there exists an integer k_c such that $f(k) \leq k^{-c}$ for all $k \geq k_c$, where R is the set of non-negative real numbers. If S is a finite set then $x \leftarrow S$ means the assignment operation for picking an element from S by a sampling algorithm associated with S (i.e., the finite set S implicitly includes a description of a probabilistic algorithm for sampling an element from S). If B is a single value or the output by a deterministic algorithm, then $x \leftarrow B$ is a simple assignment statement. If algorithm α receives only one input we write $\alpha(\cdot)$, if it receives two inputs we write $\alpha(\cdot, \cdot)$, and so on. If $\alpha(\cdot)$ is a probabilistic algorithm, then any input i, $\alpha(i)$ refers to the probabilistic space which assigns to the string w the probability that α, on input i, outputs w.

We employ notations used in [1] or [7] to formalize semantic security. Using these notations we give the original definition of semantic security given by Goldwasser and Micali [6] or equivalently given by Micali, Rackoff and Sloan [7]. For the formalism of semantic security by Goldwasser and Micali [6], in the first stage of the attack by adversary A, algorithm A_1 runs on a given public-key, pk, and at the end of its execution it outputs a (f, s), where f is a function on $M_k = \{0,1\}^k$ and s is state information possibly including pk. The triple (M_k, f, s) and an encryption y of a message, say x, sampled from M_k are given to algorithm A_2 as its input. We restate the definition of semantic security [GMSS], with minor modifications, based on the formalism in [7].

Definition 1 (GMSS) *Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and let $A = (A_1, A_2)$ be an adversary. For $k \in \mathsf{N}$, any function $f : M_k \to V$, where $M_k = \{0,1\}^k$, define*

$$\mathsf{Adv}^{\mathrm{GMSS}}_{A,\Pi}(k) \stackrel{\mathrm{def}}{=} \mathsf{Succ}^{\mathrm{GMSS}}_{A,\Pi}(k) - p^{\max}_{M_k,f}$$

where

$$\mathsf{Succ}^{\mathrm{GMSS}}_{A,\Pi}(k) \stackrel{\mathrm{def}}{=} \Pr[(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M_k, f, s) \leftarrow A_1(pk);\ x \leftarrow M_k;\ y \leftarrow \mathcal{E}_{pk}(x);\ v \leftarrow A_2(M_k, f, s, y) : v = f(x)]$$

and

$$p^{\max}_{M_k,f} \stackrel{\text{def}}{=} \max_{v \in V}\{ \sum_{x \in f^{-1}(v)} \Pr[\, x \leftarrow M_k \,] \}.$$

We say that Π *is semantically secure in the sense of GMSS if* A *being a pair of polynomial-size probabilistic circuits implies that* $\mathsf{Adv}^{\text{GMSS}}_{A,\Pi}(\cdot)$ *is negligible.*

The following definition, quoted from [1], is a formalism of indistinguishability (IND) against CPA, CCA1 and CCA2. For this definition, in the first stage of the attack by $A = (A_1, A_2)$, A_1 runs on pk and it can access to an oracle function $\mathcal{O}_1$, and at the end of its execution it outputs a triple (x_0, x_1, s), where x_0 and x_1 are a pair of elements in the valid message space $M^{(k)}$, and s is state information possibly including pk. The triple and a chosen ciphertext, say y, are given to A_2 as its input. An oracle function $\mathcal{O}_2$ can be accessed by A_2. An algorithm A_i with its oracle function $\mathcal{O}_i$ is denoted by $A_i^{\mathcal{O}_i}$, where $i \in \{1,2\}$. When we write $\mathcal{O}_i(\cdot) = \epsilon$, we mean that $\mathcal{O}_i$ is the function returning the null string ϵ on any input.

Definition 2 (IND-CPA, IND-CCA1, IND-CCA2) *Let* $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *be an encryption scheme and let* $A = (A_1, A_2)$ *be an adversary. For* $ATK \in \{CPA, CCA1, CCA2\}$ *and* $k \in \mathsf{N}$, *let*

$$\mathsf{Adv}^{\text{IND-ATK}}_{A,\Pi}(k) \stackrel{\text{def}}{=} 2 \cdot Pr\Big[(pk, sk) \leftarrow \mathcal{K}(1^k);\ (x_0, x_1, s) \leftarrow A_1^{\mathcal{O}_1}(pk);\ b \leftarrow \{0,1\};\ y \leftarrow \mathcal{E}_{pk}(x_b);\ c \leftarrow A_2^{\mathcal{O}_2}(x_0, x_1, s, y) : c = b\Big] - 1$$

where

if $ATK = CPA$ *then* $\mathcal{O}_1(\cdot) = \epsilon$ *and* $\mathcal{O}_2(\cdot) = \epsilon$,
if $ATK = CCA1$ *then* $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ *and* $\mathcal{O}_2(\cdot) = \epsilon$, *and*
if $ATK = CCA2$ *then* $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ *and* $\mathcal{O}_2(\cdot) = \mathcal{D}_{sk}(\cdot)$.

We insist, above, that A_1 *outputs* x_0, x_1 *with* $|x_0| = |x_1|$. *In the case of CCA2, we further insist that* A_2 *does not ask its oracle to decrypt* y. *We say that* Π *is secure in the sense of IND-ATK if* A *being polynomial-time (i.e., a pair of polynomial-time probabilistic algorithms) implies that* $\mathsf{Adv}^{\text{IND-ATK}}_{A,\Pi}(\cdot)$ *is negligible.*

3 A new definition of semantic security

In this section we give a new formal definition of semantic security against any attack model of CPA, CCA1 and CCA2. The formalisms of semantic security against CPA, CCA1 and CCA2 by the new definition are denoted by NSS-CPA, NSS-CCA1 and NSS-CCA2, respectively. Informally speaking, an encryption scheme is semantically secure if any adversary cannot obtain any information about the plaintext x underlying a challenge ciphertext y in a polynomial time.

Definition 3 (NSS-CPA, NSS-CCA1, NSS-CCA2) *Let* $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *be an encryption scheme and let* $A = (A_1, A_2)$ *be an adversary. For* $ATK \in \{CPA, CCA1, CCA2\}$ *and* $k \in \mathsf{N}$, *define*

$$\mathsf{Adv}^{\text{NSS-ATK}}_{A,\Pi}(k) \stackrel{\text{def}}{=} \Big|\, \mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi}(k) - \mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi,\$}(k) \,\Big|$$

where

$$\mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi}(k) \stackrel{\text{def}}{=} \Pr\Big[(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M^{(k)}, s) \leftarrow A_1^{\mathcal{O}_1}(pk);\ x \leftarrow M^{(k)};\ y \leftarrow \mathcal{E}_{pk}(x);\ (f, v) \leftarrow A_2^{\mathcal{O}_2}(M^{(k)}, s, y) :\ v = f(x)\Big]$$

and

$$\mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi,\$}(k) \stackrel{\text{def}}{=} \Pr\left[(pk,sk) \leftarrow \mathcal{K}(1^k);\ (M^{(k)},s) \leftarrow A_1^{\mathcal{O}_1}(pk);\ x,\tilde{x} \leftarrow M^{(k)};\right.$$
$$\left. y \leftarrow \mathcal{E}_{pk}(x);\ (f,v) \leftarrow A_2^{\mathcal{O}_2}(M^{(k)},s,y) :\ \ v = f(\tilde{x})\right]$$

where

if ATK = CPA then $\mathcal{O}_1(\cdot) = \epsilon$ *and* $\mathcal{O}_2(\cdot) = \epsilon$,
if ATK = CCA1 then $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ *and* $\mathcal{O}_2(\cdot) = \epsilon$, *and*
if ATK = CCA2 then $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ *and* $\mathcal{O}_2(\cdot) = \mathcal{D}_{sk}(\cdot)$.

We say that Π *is secure in the sense of NSS-ATK if adversary* A *being polynomial and* f *of* (f,v), *one of the output of* A_2, *being deterministic polynomial-time imply that* $\mathsf{Adv}^{\text{NSS-ATK}}_{A,\Pi}(\cdot)$ *is negligible.*

4 Equivalence of IND and NSS

Theorem 1 (IND-ATK ⇒ NSS-ATK) *For any ATK in* {CPA, CCA1, CCA2}, *if encryption scheme* Π *is secure in the sense of* IND-ATK *then* Π *is secure in the sense of* NSS-ATK.

Proof: We prove the contrapositive proposition of the theorem. Let Π be an encryption scheme that is not secure in the NSS-ATK sense. We shall show that Π is not secure in the IND-ATK sense.

Since Π is not secure in the sense of NSS-ATK, there is an adversary $B = (B_1, B_2)$ such that B is polynomial and it makes $\mathsf{Adv}^{\text{NSS-ATK}}_{B,\Pi}(\cdot)$ not negligible. We construct an adversary $A = (A_1, A_2)$ incorporating B as follows:

Algorithm $A_1^{\mathcal{O}_1}(pk)$	**Algorithm** $A_2^{\mathcal{O}_2}(x_0,x_1,s',y)$ where $s' = (M^{(k)},s)$
$(M^{(k)},s) \leftarrow B_1^{\mathcal{O}_1}(pk)$	$(f,v) \leftarrow B_2^{\mathcal{O}_2}(M^{(k)},s,y)$
$x_0,x_1 \leftarrow M^{(k)}$	**if** $v = f(x_0)$ **then** $d \leftarrow 0$
$s' \leftarrow (M^{(k)},s)$	**else** $d \leftarrow \{0,1\}$
return (x_0,x_1,s')	**return** d

Since B_1 , B_2 and all sampling algorithms incorporated into A are polynomial-time probabilistic algorithms in k, $A = (A_1, A_2)$ constructed above is also a pair of probabilistic polynomial algorithms in k.

For each $b \in \{0,1\}$ we define probability $p^{(k)}(b)$ as follows:

$$p^{(k)}(b) = \Pr\left[(pk,sk) \leftarrow \mathcal{K}(1^k);\ (M^{(k)},s) \leftarrow B_1^{\mathcal{O}_1}(pk);\ x_0,x_1 \leftarrow M^{(k)};\right.$$
$$\left. y \leftarrow \mathcal{E}_{pk}(x_b);\ (f,v) \leftarrow B_2^{\mathcal{O}_2}(M^{(k)},s,y) :\ \ v = f(x_0)\right].$$

Then $p^{(k)}(0)$ is the probability that in the execution by A_2, (f,v) is chosen by $B_2^{\mathcal{O}_2}$, y is the encryption of x_0 and $v = f(x_0)$, and $p^{(k)}(1)$ is the probability that in the execution by A_2, (f,v) is chosen by $B_2^{\mathcal{O}_2}$, y is the encryption of x_1 and $v = f(x_0)$.

Then for the adversary A we have

$$\begin{aligned}\mathsf{Adv}^{\text{IND-ATK}}_{A,\Pi}(k) &= 2\left[\frac{1}{2}\left[p^{(k)}(0) + \{1-p^{(k)}(0)\}\frac{1}{2}\right] + \frac{1}{2}\{1-p^{(k)}(1)\}\frac{1}{2}\right] - 1\\ &= \frac{1}{2}\{p^{(k)}(0) - p^{(k)}(1)\}.\end{aligned}$$

Observe that the execution by B_2 for a given ciphertext y being equal to the encryption of x_0 tries to compute $f(x_0)$. This situation is explicitly reflected in the definition of $\mathsf{Succ}^{\text{NSS-ATK}}_{B,\Pi}(k)$. On the other hand, in the execution by B_2, it may be possible that for a given ciphertext y is equal not only to the encryption of x_0 but also to the encryption of x_1 may be possible. This situation is explicitly reflected in the definition of $\mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi,\$}(k)$. Thus we have

$$\mathsf{Adv}^{\text{SS-ATK}}_{B,\Pi}(k) = p^{(k)}(0) - p^{(k)}(1) = 2\mathsf{Adv}^{\text{IND-ATK}}_{A,\Pi}(k).$$

Since $\mathsf{Adv}^{\text{NSS-ATK}}_{B,\Pi}(\cdot)$ is not negligible from the assumption that Π is not secure in the sense of NSS-ATK, $\mathsf{Adv}^{\text{IND-ATK}}_{A,\Pi}(\cdot)$ is also not negligible, as desired. □

Theorem 2 (NSS-ATK ⇒ IND-ATK) *If encryption scheme* Π *is secure in the sense of* NSS-ATK *then* Π *is secure in the sense of* IND-ATK, *for any* ATK $\in$ {CPA, CCA1, CCA2}.

Proof: We prove the contrapositive proposition of the theorem. Let Π be an encryption scheme that is not secure in the sense of IND-ATK. We shall show that Π is also not secure in the sense of NSS-ATK.

Since Π is not secure in the IND-ATK sense, there is an adversary $B = (B_1, B_2)$ such that B is polynomial and it makes $\mathsf{Adv}^{\text{IND-ATK}}_{B,\Pi}(\cdot)$ not negligible. We construct an adversary $A = (A_1, A_2)$ incorporating B as follows:

Algorithm $A_1^{\mathcal{O}_1}(pk)$ $(x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$ $M^{(k)} := \{x_0, x_1\}$ $s' \leftarrow (x_0, x_1, pk, s)$ **return** $(M^{(k)}, s')$	**Algorithm** $A_2^{\mathcal{O}_2}(M^{(k)}, s', y)$ where $s' = (x_0, x_1, pk, s)$ $c \leftarrow B_2^{\mathcal{O}_2}(x_0, x_1, s, y)$ $f : f(x) = x$ for all $x \in M^{(k)}$ $v \leftarrow x_c$ **return** (f, v)

We may regard $M^{(k)} := \{x_0, x_1\}$ as the probabilistic space such that the sampling probability of each $\{x_0, x_1\}$ is $1/2$.

We can evaluate $\mathsf{Adv}^{\text{IND-ATK}}_{B,\Pi}(k)$ as follows:

$$\mathsf{Adv}^{\text{IND-ATK}}_{B,\Pi}(k) = 2p^{(k)} - 1$$

where

$$p^{(k)} = \Pr\left[(pk, sk) \leftarrow \mathcal{K}(1^k);\ (x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1}(pk);\ b \leftarrow \{0,1\};\ y \leftarrow \mathcal{E}_{pk}(x_b);\ c \leftarrow B_2^{\mathcal{O}_2}(x_0, x_1, s, y) :\ c = b\right].$$

We may assume here, without loss of generality, $x_0 \neq x_1$. The next claim is immediate

Claim 4.1 $\mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi}(k) = p^{(k)}$

Claim 4.2 $\mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi,\$}(k) = \frac{1}{2}$

Proof: This follows from an information theoretic fact, namely that A has no information about the message $\tilde{x}$. □

Now we can apply the two claims given above to show the following equalities and inequality.

$$\begin{aligned}
\mathsf{Adv}^{\text{NSS-ATK}}_{A,\Pi}(k) &= \left|\mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi}(k) - \mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi}(k)\right| \\
&\geq \mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi}(k) - \mathsf{Succ}^{\text{NSS-ATK}}_{A,\Pi,\$}(k) \\
&= p^{(k)} - \frac{1}{2} \\
&= \frac{1}{2}\mathsf{Adv}^{\text{IND-ATK}}_{B,\Pi}(k).
\end{aligned}$$

Since $\mathsf{Adv}^{\text{IND-ATK}}_{B,\Pi}(\cdot)$ is not negligible, the above implies $\mathsf{Adv}^{\text{NSS-ATK}}_{A,\Pi}(\cdot)$ is not negligible too. □

5 Concluding remarks

We showed that NSS-ATK is equivalent to IND-ATK for any ATK in {CPA, CCA1, CCA2 }. The definition of NSS resembles NM, but these two definition are not equivalent from the results in [1] and in this paper. We assume that the adversary is a pair of polynomial-time probabilistic algorithms. It might be interesting to study the case where the adversary belongs to a different computational complexity class.

References

[1] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among Notions of security for public-key encryption schemes", *Advances in Cryptology–Crypto'98, Lecture Notes in Computer Science*, vol. 1462, Springer-Verlag, Berlin, pp. 24–45, 1998.

[2] M. Bellare and P. Rogaway, "Optimal asymmetric encryption", *Advances in Cryptology - Eurocrypt'94, Perugia, Italy, Lecture Notes in Computer Science*, vol. 950, Springer-Verlag, Berlin, pp. 92–111, 1994.

[3] M. Bellare and A. Sahai, "Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization", to appear in *Cryptology - Crypto'99, Lecture Notes in Computer Science*, Springer-Verlag, Berlin, 1999.

[4] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography", *23rd Annual Symposium on Theory of Computing*, ACM, pp. 542–552, 1991.

[5] E. Fujisaki and T. Okamoto, "How to enhance the security of public-key encryption at minimum cost", *2nd International Workshop on Practice and Theory in Public-Key Cryptography, Lecture Notes in Computer Science*, vol. 1560, Springer-Verlag, pp.53–68, 1999.

[6] S. Goldwasser and S. Micali, "Probabilistic encryption", *J. of Computer and System Sciences*, vol. 28, pp. 270–199, 1984.

[7] S. Micali, C. Rackoff, and R. Sloan, "The notion of security for probabilistic cryptosystems", *SIAM J. of Computing*, vol. 17, pp.270–299, 1988.

[8] M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks", *22nd Annual Symposium on Theory of Computing*, ACM, pp. 427–437, 1990.

[9] C. Rackoff and D. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack", *Advances in Cryptology - Crypto 91, Lecture Notes in Computer Science*, vol. 576, Springer-Verlag, pp. 433–444, 1991.

[10] A. C. Yao, "Theory and applications of trapdoor functions", *23rd Annual IEEE Symposium on the Foundations of Computer Science*, pp. 80–91, 1982.