数理解析研究所講究録 1268 巻 2002 年 17-28

# On Public-Key Cryptosystems against Chosen Cipertext Attack

富士通研究所 (Fujitsu Laboratories Ltd.) 小柴健史 (Takeshi Koshiba)

## 1 Introduction

One of the important goals in computational cryptography is to provide a public-key encryption (PKE) scheme that achieves a security level as strong as possible under various circumstances. To this end, we have to carefully define "security" of the PKE schemes. Satisfactory definitions of security of PKE schemes were presented by Goldwasser and Micali [13]. One is called *semantic security* and the other is called *polynomial security* (a.k.a. indistinguishability (of ciphertext)). Yet another security goal *non-malleability* was introduced by Dolev, Dwork and Naor [8]. Attack models besides security goals were invented in the literature [18, 19, 10]. Nowadays, each security notion is defined in terms of a particular security goal and a particular attack model. Relations among security notions are being organized well [13, 16, 1, 3].

The major three attack models are *chosen plaintext attack* (CPA), *non-adaptive chosen ciphertext attack* (CCA1), and *adaptive chosen ciphertext attack* (CCA2). The adversary under CPA can obtain ciphertexts of plaintext of his choice. Since, in the public-key setting, giving the adversary the public key suffices to capture the attack, CPA is considered *passive attack*. On the other hand, the other attack models are called *active attack*. Under CCA1, due to Naor and Yung [18], the adversary gets, in addition to the public key, access to an oracle for the decryption function. The adversary may invoke this oracle before being given the challenge ciphertext $c$. Under CCA2, due to Rackoff and Simon [19], the adversary gets, in addition to the public key, access to the decryption oracle, but this time he may invoke the decryption oracle even on ciphertexts chosen after obtaining the challenge ciphertext $c$, the only restriction being that the adversary may not ask for the decryption of $c$ itself.

While non-malleability against CCA2 (NM-CCA2) is considered the most secure notion of PKE schemes, some PKE schemes actually achieve the security of NM-CCA2. Most of them are proved to have the security of NM-CCA2 in the random oracle model due to Bellare and Rogaway [2]. As the results in [6] say, the use of the random oracle model is controversial, though it brings a nice methodology to design PKE schemes. On the other hand, Cramer and Shoup [7] proposed an efficient PKE scheme with the security of NM-CCA2. They proved it not on the random oracle model but on the assumption the existence of a family of universal one-way hash functions (UOWHF) and the hardness of the Decision Diffie-Hellman problem. Furthermore, in the sense that no PKE schemes without the random oracle model or UOWHF is known so far, the security notion of NM-CCA2 is an exceedingly strong notion.

As we call both CCA1 and CCA2 "active" attacks, they are quite powerful. Before Bleichenbacher [4] showed a way to utilize active attacks to crack PKCS#1, active attacks had been considered impractical. However, the attack by Bleichenbacher is realized by a fraction of the power of chosen ciphertext attack. Moreover, though some separation results between security notions with respect to chosen ciphertext attack were shown [1], the separation results were caused by the abuse of a bad implementation of the decryption function in the PKE scheme. In the practical setting, it is hard to consider the existence of the bad implementation (of the decryption function) that, given an unexpected input, outputs the secret key. We can say that the current definitions of chosen ciphertext attack are somewhat unfit for the practical discussion.

In this paper, we introduce finer definitions of chosen ciphertext attack. We consider three types of chosen ciphertext attack: (1) Type $\alpha$ oracle answers whether a given string is a legitimate ciphertext or not. (2) Type $\beta$ oracle, given a legitimate ciphertext, answers the corresponding plaintext; If he is asked for a string that is not a legitimate ciphertext then he replies with "$\perp$"

that means undefined. (3) Type $\gamma$ oracle, given a legitimate ciphertext, answers the corresponding plaintext; If he is asked for a string that is not a legitimate ciphertext then he modifies the return value from the decryption algorithm and replies with the modified return value. We note that chosen ciphertext attack of type $\alpha$ is enough to express the Bleichenbacher's attack in [4]. We also note that the original chosen ciphertext attack is similar to the chosen ciphertext attack of type $\gamma$ and the oracle of type $\gamma$ may reply with the secret key.

Moreover, we refine relations among security notions and consider what properties of chosen ciphertext attack is essential for the separation and the implication of security notions with respect to chosen ciphertext attack. Though complexity theoretic research for PKE schemes so far has been focused mainly on security notions under CPA (e.g., [5, 9, 22, 14, 12]), we also consider security notions against chosen ciphertext attack from the viewpoint of computational complexity theory.

## 2 Preliminaries

This section provides formal definitions of security notions for public-key encryption (PKE) schemes. We use standard notations and conventions for writing probabilistic algorithms and experiments. If $A$ is a probabilistic algorithm, then $A(x_1, x_2, ...; r)$ is the result of running $A$ on inputs $x_1, x_2, ...$ and coins $r$. We let $y \leftarrow A(x_1, x_2, ...)$ denote the experiment of choosing $r$ randomly and uniformly and letting $y$ be $A(x_1, x_2, ...; r)$. We let $supp(A(x_1, x_2, ...)) = \{y : \Pr[y \leftarrow A(x_1, x_2, ...)] \gtrsim 0\}$. If $S$ is a finite set then $x \leftarrow S$ is the operation of choosing an element uniformly from $S$. If $a$ is neither an algorithm nor a set then $x \leftarrow a$ is a simple assignment statement.

A public-key encryption scheme $\mathcal{PKE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of three algorithms $\mathcal{K}$, $\mathcal{E}$ and $\mathcal{D}$, where

- $\mathcal{K}$, the *key generation algorithm,* is a probabilistic algorithm that inputs the unary expression of a security parameter $k \in \mathbb{N}$ and outputs a pair $(pk, sk)$ of the public key and the secret key.

- $\mathcal{E}$, the *encryption algorithm*, is a probabilistic algorithm that, given a public key $pk$ and a plaintext $m \in M_k$, outputs a ciphertext $c$, where $M_k$ is a message space. Without loss of generality we assume that $M_k \subseteq \{0, 1\}^k$.

- $\mathcal{D}$, the *decryption algorithm*, is a deterministic algorithm that, given a secret key $sk$ and a ciphertext $c$, outputs a plaintext $m \in M_k$.

We require that for all $(pk, sk)$ which can be output by $\mathcal{K}(1^k)$ and, for all $c$ such that $c = \mathcal{E}_{pk}(m)$ for some $m$, we have that $\mathcal{D}_{sk}(c) = m$. We also require that $\mathcal{K}$, $\mathcal{E}$ and $\mathcal{D}$ can be computed in polynomial time. We sometimes an additional property on PKE schemes as follows.

- The decryption algorithm $\mathcal{D}$, given a secret key and a non-ciphertext, outputs a special symbol "$\perp$" to indicate that the ciphertext is invalid.

We call the above property *invalidity checkable property.* Acutally, many PKE schemes of the NM-CCA2 security satisfy the "invalidity checkable (IC)" property. We note that, in general, the IC property is not requisite for PKE schemes. However, we will show that the IC property affects the security of PKE schemes through this paper.

A function $\epsilon : \mathbb{N} \rightarrow \mathbb{R}$ is said to be *negligible* if for every constant $c \geq 0$ there exists an integer $k_c$ such that $\epsilon(k) \leq k^{-c}$ for all $k \geq k_c$. We let $C$ (w.r.t. $\mathcal{PKE}$) denote the set $\{(pk, c) : c = \mathcal{E}_{pk}(m)$ for some $m \in M_k$, $pk \in supp(\mathcal{K}(1^k))$ (and some coins $r$)$\}$. We call the set $C$ *ciphertext space* (w.r.t. $\mathcal{PKE}$).

## 2.1 Attack Models

In this paper, we refine definitions of chosen ciphertext attack. Before giving them, we review attack models so far. We regard an adversary $A$ as a pair of probabilistic algorithms $A = (A_1, A_2)$. This corresponds to $A$ running in two stages. In the first stage, the adversary, given the public key, seeks and output some "test instance" and some additional information. In the second stage, the adversary is handed a challenge ciphertext $c$ that is generated as a function of the test instance and tries to achieve the goal.

First, we consider basic three types of attack models.

- In *chosen plaintext attack* (CPA), the adversary can encrypt plaintexts of his choice. CPA is passive attack in a sense that he also knows the public key and can compute a ciphertext for any plaintext he desires.
- In *non-adaptive chosen ciphertext attack* (CCA1), $A_1$ can access to the public key and a decryption oracle, but $A_2$ is not allowed to access to a decryption oracle.
- In *adaptive chosen ciphertext attack* (CCA2), $A_1$ can access to the public key and a decryption oracle, but also $A_2$ can access to the same decryption oracle, with the only restriction that he cannot ask the oracle for the challenge ciphertext $c$.

Now, we consider what we mean by "decryption oracle". It is literally an oracle that, given a ciphertext, lets us know the corresponding plaintext. Literalism itself for decryption oracle does not tell us the action of the oracle when the oracle is given a non-ciphertext. Most common interpretation is that the oracle, given a non-ciphertext, can reply with any string that can be output by the decryption algorithm. We note that the decryption oracle may reply with "secret key"! This is one of the broadest interpretation and brings us the strongest attack model. Here, we stress that we use "decryption oracle" and "decryption algorithm" in different terminologies. When we say "decryption algorithm", we mean that it is just a polynomial-time algorithm to decrypt ciphertexts. On the other hand, when we say "decryption oracle", me mean that it is exploited by the adversary. Thus, "decryption oracle" also exploits "decryption algorithm" as the need arises. Moreover, we may assume that "decryption oracle" has super-polynomially computational power.

A decryption algorithm (without the IC property) is an implementation of the decryption function, which may be a partial function. Any partial function has its domain and the functional value of some element not in the domain is usually "undefined". However, any functionally honest implementation (algorithm) of the decryption function should not let the secret key out carelessly even when any non-ciphertext is given to the algorithm. In some practical setting, a decryption algorithm may have a side effect such as "debug mode." Some decryption algorithm with debug mode may be functionally dishonest. On the other hand, any decryption algorithm of a PKE scheme with the IC property must be functionally honest.

Now, we are ready to prescribe the action of decryption oracle. We consider three types of decryption oracle as follows:

New chosen ciphertext attacks are defined in terms of the decryption oracle of the above types. We describe the chosen ciphertext attacks more precisely.

- In *adaptive chosen ciphertext attack of type* $\alpha$ ($\alpha$-CCA2), $A_1$ can access to the public key and a decryption oracle of type $\alpha$, but also $A_2$ can access to the same decryption oracle, with only restriction that he cannot ask the oracle for the challenge ciphertext $c$. Only information that both $A_1$ and $A_2$ can obtain from the decryption oracle is whether query strings are ciphertexts or not. We note that the restriction on $A_2$'s oracle queries actually does not influence on the security, because the membership information of the challenge

| | when a ciphertext is asked | when a non-ciphertext is asked |
|---|---|---|
| Type $\alpha$ | yes | no |
| Type $\beta$ | its plaintext | $\perp$ (undefined) |
| Type $\gamma$ | its plaintext | modification of the return value from the decryption algorithm |

Table 1: What decryption oracle replies with?

ciphertext is supposed. We also note that deciding whether given strings are ciphertext or not may be beyond the polynomial computation. Nevertheless, we assume that, in this model, the decryption oracle of type $\alpha$ can compute the membership exactly. In case of PKE schemes with the IC property, the membership is decidable in polynomial time, since the decryption algorithm (with the IC property) also can compute the membership in polynomial time. As long as we consider the PKE schemes with the IC property, the existence of the decryption oracle of type $\alpha$ is naturally assumed.

- In *adaptive chosen ciphertext attack of type* $\beta$ ($\beta$-CCA2), $A_1$ can access to the public key and a decryption oracle of type $\beta$, but also $A_2$ can access to the same decryption oracle, with only restriction that he cannot ask the oracle for the challenge ciphertext $c$. Whenever $A_1$ and $A_2$ query the decryption oracle of type $\beta$ with ciphertext, they can obtain the corresponding plaintext. On the other hand, whenever $A_1$ and $A_2$ query the decryption oracle of type $\beta$ with non-ciphertext, only information that they can obtain is the fact that the query string is just a non-ciphertext. In case of $\beta$-CCA2, the restriction on $A_2$'s oracle queries are essential. Moreover, deciding whether given strings are ciphertext or not may be beyond the polynomial computation. Nevertheless, we also assume that, in this model, the decryption oracle of type $\beta$ can compute the membership exactly. In addition, we assume that the decryption oracle, given a ciphertext, can reply with the corresponding plaintext. In case of PKE schemes with the IC property, computation that the decryption oracle of type $\beta$ performs is of polynomial-time, since the decryption algorithm (with the IC property) also can compute it in polynomial time. As long as we consider the PKE schemes with the IC property, the existence of the decryption oracle of type $\beta$ is naturally assumed.

- In *adaptive chosen ciphertext attack of type* $\gamma$ ($\gamma$-CCA2), $A_1$ can access to the public key and a decryption oracle of type $\gamma$, but also $A_2$ can access to the same decryption oracle, with only restriction that he cannot ask the oracle for the challenge ciphertext $c$. Whenever $A_1$ and $A_2$ query the decryption oracle of type $\gamma$ with ciphertext, they can obtain the corresponding plaintext. On the other hand, whenever $A_1$ and $A_2$ query the decryption oracle of type $\gamma$ with non-ciphertext, the oracle exploits the decryption algorithm. Namely, the oracle uses the decryption algorithm and obtains some information from the decryption algorithm. After that, the oracle modifies the information and replies with the modified information. So, if the decryption algorithm returns, given an unexpected input, some information, which may be the secret key, then the decryption oracle may reply with the information. In case of PKE schemes with the IC property, computation that the decryption oracle of type $\gamma$ performs is of polynomial-time, since the decryption algorithm (with the IC property) also can compute it in polynomial time. As long as we consider the PKE schemes with the IC property, the existence of the decryption oracle of type $\gamma$ is naturally assumed.

We may interpret the action of CCA2 of each type as follows. In CCA2 of any type, the decryption oracle can access to the membership oracle $\mathcal{L}$ that can answer whether given strings are ciphertexts or not. Here, the power of $\mathcal{L}$ may be beyond the polynomial computation even if the secret key is known. (We note that if we consider the PKE schemes with the IC property then $\mathcal{L}$ can be simulated in polynomial time by using the decryption algorithm.) The decryption oracle of each type first invokes the membership oracle $\mathcal{L}$ and then acts accordingly. Now, we assume that $w$ is a string given to the decryption oracle. The decryption oracle of type $\alpha$ replies with just the return value from the membership oracle $\mathcal{L}$. The decryption oracle of type $\beta$ invokes the decryption "algorithm" if $\mathcal{L}(w) = yes$, and replies with the return value from the decryption algorithm. The decryption oracle of type $\beta$ replies with "$\perp$" if $\mathcal{L}(w) = no$. The decryption oracle of type $\gamma$ invokes the decryption "algorithm" if $\mathcal{L}(w) = yes$, and replies with the return value from the decryption algorithm. The decryption oracle of type $\gamma$ replies with $f(\mathcal{D}(w))$ if $\mathcal{L}(w) = no$, where $f$ is a polynomial-time modification. We note that $\gamma$-CCA2 whose polynomial modification $f$ is an identical function coincides with the traditional CCA2 regardless of the computational power of $\mathcal{L}$, because the decryption oracle can be simulated by the decryption algorithm without the membership oracle $\mathcal{L}$. We also note that $\gamma$-CCA2 whose polynomial modification $f$ is a constant function (i.e., "$\perp$") coincides with $\beta$-CCA2.

We call answer by decryption oracle of type $\gamma$ that is asked for a non-ciphertext *dishonest answer.*

We note that the first practical chosen ciphertext attack by Bleichenbacher [4] is of type $\alpha$. Although Bellare *et al* [1] worked out the relations among security notions, some separation results (i.e., NM-CPA $\not\Rightarrow$ IND-CCA1 and NM-CCA1 $\not\Rightarrow$ NM-CCA2) were shown by using dishonest answers by decryption oracle of type $\gamma$.

We have given the definitions of adaptive chosen ciphertext attack (CCA2) of each type. It is easy to consider the corresponding definitions to non-adaptive chosen ciphertext attack (CCA1) of each type. Although we omit their description, we let $\alpha$-CCA1 denote non-adaptive chosen ciphertext attack where decryption oracle of type $\alpha$ is available to the adversary. Similarly, we use notations such that $\beta$-CCA1 and $\gamma$-CCA1.

For simplicity, the adversary $A = (A_1, A_2)$ for CCA2 consist of the probabilistic algorithms that invoke decryption oracle of the same type. It is not hard to consider the adversary $A = (A_1, A_2)$ for CCA2 where the type of $A_1$ is different from the type of $A_2$. In this paper, we do not consider the adversary of mixture types.

## 2.2 Security Goals

### 2.2.1 Indistinguishability of ciphertext

The notion of indistinguishability of ciphertext (IND) was originally introduced by Goldwasser and Micali [13]. Here we adopt a version of this notion by Bellare *et al* [1].

Algorithm $A_1$ is run on input the public key $pk$ and outputs a triple $(m_0, m_1, s)$, where $s$ is possible including $pk$. Let $m_b$ is randomly selected from $\{m_0, m_1\}$. A challenge $c$ is computed by encrypting $m_b$ using $pk$. Algorithm $A_2$ tries to guess if $c$ was selected as the ciphertext of $m_0$ or $m_1$. To this end, $A_2$ is given the additional information $s$ and the challenge ciphertext $c$.

**Definition 1** Let $\mathcal{PKE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a PKE scheme and $C$ be the ciphertext space with respect to $\mathcal{PKE}$ and let $A = (A_1, A_2)$ be an adversary. For atk $\in$ {cpa, $\alpha$-cca1, $\beta$-cca1, $\gamma$-cca1, $\alpha$-cca2, $\beta$-cca
$\gamma$-cca2} and $k \in \mathbb{N}$, we let

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

where, for $b \in \{0,1\}$, $\mathrm{Exp}^{\mathrm{ind-atk-b}}(k)$ is computed as follows.

$$(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(1^k); \quad (m_0, m_1, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk); \quad c \leftarrow \mathcal{E}_{pk}(m_b);$$
$$d \leftarrow A_2^{\mathcal{O}_2(\cdot)}(m_0, m_1, s, c); \quad \textsf{output } d,$$

and

$$\begin{array}{llllll} \text{if} & \mathrm{atk} = \mathrm{cpa} & \text{then} & \mathcal{O}_1(\cdot) = \epsilon & \text{and} & \mathcal{O}_2(\cdot) = \epsilon \\ \text{if} & \mathrm{atk} = t\text{-cca1, where } t \in \{\alpha, \beta, \gamma\} & \text{then} & \mathcal{O}_1(\cdot) = \mathcal{D}^t_{sk}(\cdot) & \text{and} & \mathcal{O}_2(\cdot) = \epsilon \\ \text{if} & \mathrm{atk} = t\text{-cca2, where } t \in \{\alpha, \beta, \gamma\} & \text{then} & \mathcal{O}_1(\cdot) = \mathcal{D}^t_{sk}(\cdot) & \text{and} & \mathcal{O}_2(\cdot) = \mathcal{D}^t_{sk}(\cdot), \end{array}$$

where $\mathcal{D}^{\alpha}_{sk}(w)$ replies with either $w \in C$ or $w \notin C$; $\mathcal{D}^{\beta}_{sk}(w) = \mathcal{D}_{sk}(w)$ only if $w \in C$ and $\mathcal{D}^{\beta}_{sk}(w) = \perp$ otherwise; $\mathcal{D}^{\gamma}_{sk}(w) = \mathcal{D}_{sk}(w)$ only if $w \in C$ and $\mathcal{D}^{\gamma}_{sk}(w) = f(\mathcal{D}_{sk}(w))$ otherwise, where $f$ is a polynomial-time modification.

Above it is mandatory that $|m_0| = |m_1|$. In the case of CCA2, we insist that $A_2$ does not invoke its oracle with the challenge ciphertext $c$. We say that $\mathcal{PKE}$ is secure in the sense of IND-ATK if $A$ being polynomial-time implies that $\mathrm{Adv}^{\mathrm{ind-atk}}(\cdot)$ is negligible.

### 2.2.2 Non-Malleability

The notion of non-malleability (NM) was originally introduced by Dolev, Dwork and Naor [8]. Here we adopt a version of this notion by Bellare *et al* [1].

Let $A = (A_1, A_2)$ be an adversary. Algorithm $A_1$, given the public key $pk$, outputs a description of a message space, described by a sampling algorithm $M$. The message space must be *valid*. Algorithm $A_2$ receives a ciphertext of a message $m_1$ drawn from $M$. $A_2$ then tries to output a description of a relation $R$ and a vector $\vec{c}$ (no component of which is $c$) such that $R(m, \vec{m})$ holds, where $\vec{m} \leftarrow \mathcal{D}_{sk}(\vec{c})$.

**Definition 2** Let $\mathcal{PKE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a PKE scheme and $C$ be the ciphertext space with respect to $\mathcal{PKE}$ and let $A = (A_1, A_2)$ be an adversary. For atk $\in$ {cpa, $\alpha$-cca1, $\beta$-cca1, $\gamma$-cca1, $\alpha$-cca2, $\beta$-cca2, $\gamma$-cca2} and $k \in \mathbb{N}$, we let

$$\mathrm{Adv}^{\mathrm{nm-atk}}(k) = \Pr[\mathrm{Exp}^{\mathrm{nm-atk-1}}(k) = 1] - \Pr[\mathrm{Exp}^{\mathrm{nm-atk-0}}(k) = 1]$$

where, for $b \in \{0,1\}$, $\mathrm{Exp}^{\mathrm{nm-atk-b}}(k)$ is computed as follows.

$$(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(1^k); \quad (M, s) \leftarrow A_1^{\mathcal{O}_1(\cdot)}(pk); \quad m_0, m_1 \leftarrow M; \quad c \leftarrow \mathcal{E}_{pk}(m_1);$$
$$(R, \vec{c}) \leftarrow A_2^{\mathcal{O}_2(\cdot)}(M, s, c); \quad \vec{m} \leftarrow \mathcal{D}_{sk}(\vec{c});$$
$$\textsf{if } c \notin \vec{c} \wedge \perp \notin \vec{m} \wedge R(m_b, \vec{m}) \textsf{ then } d \leftarrow 1 \textsf{ else } d \leftarrow 0; \quad \textsf{output } d,$$

and

$$\begin{array}{llllll} \text{if} & \mathrm{atk} = \mathrm{cpa} & \text{then} & \mathcal{O}_1(\cdot) = \epsilon & \text{and} & \mathcal{O}_2(\cdot) = \epsilon \\ \text{if} & \mathrm{atk} = t\text{-cca1, where } t \in \{\alpha, \beta, \gamma\} & \text{then} & \mathcal{O}_1(\cdot) = \mathcal{D}^t_{sk}(\cdot) & \text{and} & \mathcal{O}_2(\cdot) = \epsilon \\ \text{if} & \mathrm{atk} = t\text{-cca2, where } t \in \{\alpha, \beta, \gamma\} & \text{then} & \mathcal{O}_1(\cdot) = \mathcal{D}^t_{sk}(\cdot) & \text{and} & \mathcal{O}_2(\cdot) = \mathcal{D}^t_{sk}(\cdot), \end{array}$$

where $\mathcal{D}^{\alpha}_{sk}(w)$ replies with either $w \in C$ or $w \notin C$; $\mathcal{D}^{\beta}_{sk}(w) = \mathcal{D}_{sk}(w)$ only if $w \in C$ and $\mathcal{D}^{\beta}_{sk}(w) = \perp$ otherwise; $\mathcal{D}^{\gamma}_{sk}(w) = \mathcal{D}_{sk}(w)$ only if $w \in C$ and $\mathcal{D}^{\gamma}_{sk}(w) = f(\mathcal{D}_{sk}(w))$ otherwise, where $f$ is a polynomial-time modification.

Above it is mandatory that $M$ is valid, namely, $|m| = |m'|$ for any $m$, $m'$ in $supp(M)$. In the case of CCA2, we insist that $A_2$ does not invoke its oracle with the challenge ciphertext $c$. We say that $\mathcal{PKE}$ is secure in the sense of NM-ATK if $A$ runs in polynomial time $p(k)$, outputs a valid message space $M$ samplable in time $p(k)$, and outputs a relation $R$ computable in time $p(k)$, then $\mathrm{Adv}^{\mathrm{nm-atk}}(\cdot)$ is negligible.

## 3 Complexity Theoretic Consideration of $\alpha$-CCA

Before considering the relation among security notions, we consider the power of $\alpha$-CCA2 from the viewpoint of computational complexity theory. In [5], Brassard showed that if the cracking of a PKE scheme in the sense of one-wayness whose ciphertext space $C$ belongs to **coNP** is **NP**-hard then **NP** = **coNP**. Though number theoretic PKE schemes such as the RSA scheme is prone to being **coNP**, his claim is not so serious for cryptographic research. After that, complexity theoretic issues in cryptography have been studied in the literature [9, 22, 14, 12]. Those research is mainly security under CPA. In this section, we consider security under CCA from the viewpoint of computational complexity theory. To this end, we introduce a deterministic variant of the problem for distinguishing ciphertexts. We let

$$\begin{aligned} D_0 = \{(pk, c_0, c_1) : {}& c_0 = \mathcal{E}_{pk}(m), c_1 = \mathcal{E}_{pk}(m) \\ & \text{for some } m \in M_k \text{ and for some } pk \in supp(\mathcal{K}(1^k))\}, \\ D_1 = \{(pk, c_0, c_1) : {}& c_0 = \mathcal{E}_{pk}(m_0), c_1 = \mathcal{E}_{pk}(m_1) \\ & \text{for some } m_0, m_1 \in M_k \text{ such that } m_0 \neq m_1 \text{ and } |m_0| = |m_1| \text{ and} \\ & \text{for some } pk \in supp(\mathcal{K}(1^k))\}. \end{aligned}$$

We denote $D_0 \cup D_1$ by $D$. A *distinguishing ciphertexts problem* is a promise problem[1] $(D, D_0)$. Then, it is easy to see that $D, D_0, D_1 \in$ **NP**.

Under CCA2, decryption oracle of type $\alpha$ replies with only the membership of $C$. The power of $\alpha$-CCA2 depends deeply on the computational complexity of the ciphertext space $C$. In the original setting of CCA2, there are two stages. The first stage is before a challenge ciphertext is given. The second stage is after the challenge ciphertext is given. Because of the restriction of the adversary in the second stage, the treatment of the adversary is not uniform. The non-uniformity precludes us from considering the PKE schemes secure against CCA2 from the complexity theoretic viewpoint. However, as we have seen, the definition of $\alpha$-CCA2 enables us to consider the adversary uniformly. So, we have some relations between the complexity class of the ciphertext space and security notions for PKE schemes.

**Theorem 3** *Suppose that $\Pi$ is a PKE scheme whose ciphertext space $C$ is in* **P**. *Then, the following statements are equivalent.*

1. *$\Pi$ is secure against CPA.*
2. *$\Pi$ is secure against $\alpha$-CCA1.*
3. *$\Pi$ is secure against $\alpha$-CCA2.*

**Proof:** The proof is straightforward, since if $C \in$ **P** then decryption oracle of type $\alpha$ can be easily simulated in polynomial time. □

The above theorem says that $\alpha$-CCA2 attack on any PKE scheme whose ciphertext space is in **P** is not so powerful. In other words, if the PKE scheme whose ciphertext space is in **P** is not secure against $\alpha$-CCA2, then the PKE scheme is not secure against CPA, either.

**Theorem 4** *Suppose that $\Pi$ is a PKE scheme whose ciphertext space $C$ is* **NP***-complete w.r.t. truth-table reduction. Then $\Pi$ cannot achieve the security of IND-$\alpha$-CCA2.*

[1] A promise problem $(A, B)$ is a problem to decide whether $x \in B$ or not when $x \in A$. If $x \notin A$ then we do not care the answer. We call $A$ the *promise* of the promise problem. (For details about promise problem, see, e.g.,

**Proof:** Since $D_0 \in \mathbf{NP}$, there exists a truth-table reduction from $D_0$ to $C$. Then decryption oracle of type $\alpha$ helps to solve $D_0$ efficiently. This implies that the existence of a successful adversary in the sense of IND-$\alpha$-CCA2. □

We note that NP-completeness is usually defined in terms of many-one reduction. On the other hand, truth-table reduction is weaker reduction than many-one reduction. So, if $A$ is NP-complete w.r.t. many-one reduction, then $A$ is also NP-complete w.r.t. truth-table reduction. (See, e.g., [20] for details about truth-table reduction.) We also note that it is not known whether, in **NP**, many-one reduction is properly stronger than truth-table reduction or not.

**Corollary 5** *Suppose that* $\Pi$ *is a PKE scheme whose ciphertext space* $C$ *is* **NP***-complete w.r.t. truth-table reduction. Then* $\Pi$ *cannot achieve the security of IND-*$\beta$*-CCA2.*

Suppose that $\Pi$ is a PKE scheme whose ciphertext space $C$ is **NP**-complete w.r.t. truth-table reduction. Then, $\Pi$ cannot have the IC property, because the IC property requires that $C \in \mathbf{NP} \cap \mathbf{coNP}$. Thus, Theorem 4 and Corollary 5 say nothing about the security of PKE schemes with the IC property.

Next, we assume that $C$ belongs to an intermediate complexity class $\mathbf{NP} \cap \mathbf{coNP}$. Let us review a complexity result concerned with security under $\alpha$-CCA for a PKE scheme whose ciphertext space belongs to $\mathbf{NP} \cap \mathbf{coNP}$.

**Proposition 6** [21] $\mathbf{NP} = \mathbf{NP}^{\mathbf{NP} \cap \mathbf{coNP}}$

Since $D_0 \in \mathbf{NP}$, the above proposition apparently says that if $C \in \mathbf{NP} \cap \mathbf{coNP}$ then $\alpha$-CCA is not so powerful. However, it depends on the difficulty of $D_0$ whether $\alpha$-CCA helps to solve $D_0$ or not.

## 4 Relations

In this section, we consider relations among security notions more finely.

First, we mention trivial relations with respect to newly introduced chosen ciphertext attack.

**Theorem 7** *Let* $\Pi$ *be a PKE scheme. For any GOAL in* $\{IND, NM\}$*, we have the following.*

- *If* $\Pi$ *is GOAL-*$\gamma$*-CCA1 secure then* $\Pi$ *is GOAL-CCA1 secure.*
  *If* $\Pi$ *is GOAL-*$\gamma$*-CCA1 secure then* $\Pi$ *is GOAL-*$\beta$*-CCA1 secure.*
  *If* $\Pi$ *is GOAL-*$\beta$*-CCA1 secure then* $\Pi$ *is GOAL-*$\alpha$*-CCA1 secure.*
  *If* $\Pi$ *is GOAL-*$\alpha$*-CCA1 secure then* $\Pi$ *is GOAL-CPA secure.*
- *If* $\Pi$ *is GOAL-*$\gamma$*-CCA2 secure then* $\Pi$ *is GOAL-CCA2 secure.*
  *If* $\Pi$ *is GOAL-*$\gamma$*-CCA2 secure then* $\Pi$ *is GOAL-*$\beta$*-CCA2 secure.*
  *If* $\Pi$ *is GOAL-*$\beta$*-CCA2 secure then* $\Pi$ *is GOAL-*$\alpha$*-CCA2 secure.*
  *If* $\Pi$ *is GOAL-*$\alpha$*-CCA2 secure then* $\Pi$ *is GOAL-CPA secure.*

**Theorem 8** *Let* $\Pi$ *be a PKE scheme with the IC property. For any GOAL in* $\{IND, NM\}$*, we have the following.*

- $\Pi$ *is GOAL-*$\beta$*-CCA1 secure if and only if* $\Pi$ *is GOAL-CCA1 secure.*
- $\Pi$ *is GOAL-*$\beta$*-CCA2 secure if and only if* $\Pi$ *is GOAL-CCA2 secure.*

The following theorem is shown as the proof in [1].

**Theorem 9** *Let* $\Pi$ *be a PKE scheme. If* $\Pi$ *is NM-ATK secure then* $\Pi$ *is also IND-ATK secure, for ATK* $\in \{\alpha\text{-CCA1}, \beta\text{-CCA1}, \gamma\text{-CCA1}, \alpha\text{-CCA2}, \beta\text{-CCA2}, \gamma\text{-CCA2}\}$.

Next, we show several separation results. We define some property on message space. Message space is said to be *simple* if there exists a function $\xi : \mathbb{N} \to M_k$ that is computable in polynomial time and $\xi^{-1}$ is also computable in polynomial time. We call such a function *ordering function.*

**Theorem 10** *Suppose that there exists an IND-CPA PKE scheme which has simple message space. Then, IND-CPA and IND-$\alpha$-CCA2 are separable.*

**Proof:** (*Sketch*) Assume that there exists some IND-CPA PKE scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ which has simple message space, since otherwise the theorem is vacuously true. We now modify $\Pi$ to a new PKE scheme $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also IND-CPA secure but not secure in the IND-$\alpha$-CCA2 sense. Let $M_k$ be a simple message space for $\Pi$. The new PKE scheme $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ and the new message space $M'_k$ for $\Pi'$ are defined as follows. Let $\leq$ be the total order defined naturally from the ordering function.

```
Algorithm $\mathcal{K}'(1^k)$:
        $(pk, sk) \leftarrow \mathcal{K}(1^k)$; output $(pk, sk)$.
Algorithm $\mathcal{E}'_{pk}(m_0||m_1)$, where $m_0 \leq m_1$:
        $c_0 \leftarrow \mathcal{E}_{pk}(m_0)$; $c_1 \leftarrow \mathcal{E}_{pk}(m_1)$; output $c_0||c_1$.
Algorithm $\mathcal{D}'_{sk}(c_0||c_1)$:
        $m_0 \leftarrow \mathcal{D}_{sk}(c_0)$; $m_1 \leftarrow \mathcal{D}_{sk}(c_1)$;
        if $m_0 \leq m_1$ then output $m_0$ else output $\perp$.
$M'_k \leftarrow \{m_0||m_1 : m_0, m_1 \in M_k, m_0 \leq m_1\}$.
```

First, we show that $\Pi'$ is not secure in the IND-$\alpha$-CCA2 sense. Given a ciphertext $c_0||c_1$, the adversary $A = (A_1, A_2)$ runs as follows: $A_2$ asks the decryption oracle of type $\alpha$ for $\mathcal{E}_{pk}(\xi(2^i))||c_1$, where $i = 0, 1, 2, \ldots$, until the oracle replies with "no". Using this "binary method", $A_2$ can efficiently find $m_0$ such that $m_0 = \mathcal{D}_{sk}(c_0)$. Similarly $A_2$ can also find $m_1$ such that $m_1 = \mathcal{D}_{sk}(c_1)$. Thus, it is not hard to see that the adversary $A$ can distinguish any ciphertexts.

Next, we show that $\Pi'$ is IND-CPA secure. We assume that $\Pi'$ is not IND-CPA secure. That is, there exists a distinguisher $B = (B_1, B_2)$ for $\Pi'$. Now, we consider the following algorithm $B' = (B'_1, B'_2)$. $B'_1$ invokes $B_1$ and gets $(m_0||m'_0, m_1||m'_1, s)$. $B'_1$ finally outputs $(m_0, m_1, m'_0||m'_1||s)$. Let $c = \mathcal{E}_{pk}(m_b)$ for randomly chosen $b \in \{0, 1\}$. $B'_2$ invokes $B_2$ with input $(m_0||m'_0, m_1||m'_1, s, c||c')$ where $c' = \mathcal{E}_{pk}(m'_d)$ for randomly chosen $d \in \{0, 1\}$. $B'_2$ obtains the reply from $B_2$ and outputs the reply. It is not hard to see that $B' = (B'_1, B'_2)$ is a distinguisher of $\Pi$. This is a contradiction. Thus we have that $\Pi'$ is IND-CPA secure. □

In case of PKE schemes with the IC property, we have still a similar result to Theorem 10.

**Theorem 11** *Suppose that there exists an IND-CPA PKE scheme with the IC property which has simple message space. Then, in PKE schemes with the IC property, IND-CPA and IND-$\alpha$-CCA2 are separable.*

Theorem 10 and Theorem 11 say that chosen ciphertext attack like Bleichenbacher's [4] is properly stronger than chosen plaintext attack.

**Theorem 12** *IND-$\alpha$-CCA2 and IND-$\beta$-CCA2 are separable.*

**Proof:** (*Sketch*) Assume that there exists some IND-$\alpha$-CCA2 PKE scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is vacuously true. We now modify $\Pi$ to a new PKE scheme $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also IND-$\alpha$-CCA2 secure but not secure in the IND-$\beta$-CCA2 sense. Let $M_k$ be a message space for $\Pi$. The new PKE scheme $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ and the new message space $M'_k$ for $\Pi'$ are defined as follows.

```
Algorithm $\mathcal{K}'(1^k)$:
        $(pk, sk) \leftarrow \mathcal{K}(1^k)$; output $(pk, sk)$.
Algorithm $\mathcal{E}'_{pk}(m_0||m_1)$:
        $c_0 \leftarrow \mathcal{E}_{pk}(m_0)$; $c_1 \leftarrow \mathcal{E}_{pk}(m_1)$; output $c_0||c_1$.
Algorithm $\mathcal{D}'_{sk}(c_0||c_1)$:
        $m_0 \leftarrow \mathcal{D}_{sk}(c_0)$; $m_1 \leftarrow \mathcal{D}_{sk}(c_1)$; output $m_0||m_1$.
$M'_k \leftarrow \{m_0||m_1 : m_0, m_1 \in M_k\}$.
```

First, we show that $\Pi'$ is not secure in the IND-$\beta$-CCA2 sense. Given a ciphertext $c_0||c_1$, the adversary $A = (A_1, A_2)$ runs as follows: $A_2$ asks the decryption oracle of type $\beta$ for $c_1||c_0$. Thus, it is not hard to see that the adversary $A$ can distinguish any ciphertexts.

Next, we show that $\Pi'$ is IND-$\alpha$-CCA2 secure. We assume that $\Pi'$ is not IND-$\alpha$-CCA2 secure. That is, there exists a distinguisher $B = (B_1, B_2)$ for $\Pi'$. Now, we consider the following algorithm $B' = (B'_1, B'_2)$. $B'_1$ invokes $B_1$ and gets $(m_0||m'_0, m_1||m'_1, s)$. We note that $B'_1$ can deal with oracle query from $B_1$ using his own oracle invocation. $B'_1$ finally outputs $(m_0, m_1, m'_0||m'_1||s)$. Let $c = \mathcal{E}_{pk}(m_b)$ for randomly chosen $b \in \{0, 1\}$. $B'_2$ invokes $B_2$ with input $(m_0||m'_0, m_1||m'_1, s, c||c')$ where $c' = \mathcal{E}_{pk}(m'_d)$ for randomly chosen $d \in \{0, 1\}$. $B'_2$ obtains the reply from $B_2$ and outputs the reply. Again $B'_2$ can deal with oracle query from $B_2$ using his own oracle invocation. It is not hard to see that $B' = (B'_1, B'_2)$ is a distinguisher of $\Pi$. This is a contradiction. Thus we have that $\Pi'$ is IND-$\alpha$-CCA2 secure. □

As in the case of separation between IND-CPA and IND-$\alpha$-CCA2, when we restrict on PKE schemes with the IC property, separation between IND-$\alpha$-CCA2 and IND-$\beta$-CCA2 still holds.

**Theorem 13** *In PKE schemes with the IC property, IND-$\alpha$-CCA2 and IND-$\beta$-CCA2 are separable.*

Although chosen ciphertext attack like Bleichenbacher's is properly stronger than chosen plaintext attack, Theorem 12 and Theorem 13 say that chosen ciphertext attack like Bleichenbacher's is properly weaker than general chosen ciphertext attack.

**Theorem 14** *Suppose that there exists an IND-$\beta$-CCA2 PKE scheme which has simple message space. Then IND-$\beta$-CCA2 and IND-CCA2 are separable.*

**Proof:** (*Sketch*) Assume that there exists some IND-$\beta$-CCA2 PKE scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ which has simple message space, since otherwise the theorem is vacuously true. We now modify $\Pi$ to a new PKE scheme $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also IND-$\beta$-CCA2 secure but not secure in the IND-CCA2 sense. Let $M_k$ be a simple message space for $\Pi$. We assume that $|M_k| \geq 3$ without loss of generality. The new PKE scheme $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ and the new message space $M'_k$ for $\Pi'$ are defined as follows.

```
Algorithm $\mathcal{K}'(1^k)$:
        $(pk, sk) \leftarrow \mathcal{K}(1^k)$; output $(pk, sk)$.
Algorithm $\mathcal{E}'_{pk}(m)$:
        $c_0 \leftarrow \mathcal{E}_{pk}(m)$; $c_1 \leftarrow \mathcal{E}_{pk}(\xi(1))$; output $c_0||c_1$ or $c_1||c_0$ randomly.
Algorithm $\mathcal{D}'_{sk}(c_0||c_1)$:
        $m_0 \leftarrow \mathcal{D}_{sk}(c_0)$; $m_1 \leftarrow \mathcal{D}_{sk}(c_1)$; output $\max\{m_0, m_1\}$.
$M'_k \leftarrow \{m : \xi^{-1}(m) \geq 2\}$.
```

First, we show that $\Pi'$ is not secure in the IND-CCA2 sense. Given a ciphertext $c_0||c_1$, the adversary $A = (A_1, A_2)$ runs as follows: $A_2$ asks the decryption "algorithm" for $c_0||\mathcal{E}_{pk}(\xi(2))$ and $\mathcal{E}_{pk}(\xi(2))||c_1$. Although either $c_0||\mathcal{E}_{pk}(\xi(2))$ or $\mathcal{E}_{pk}(\xi(2))||c_1$ is not a legitimate ciphertext, the decryption algorithm $\mathcal{D}'$ still works for the non-ciphertext. Since, for any plaintext $m$ for $\Pi'$, $\xi^{-1}(m) \geq 2$, the decryption algorithm $\mathcal{D}'$ can calculate the corresponding plaintext. Thus, the adversary $A$ can distinguish any ciphertexts.

Next, we show that $\Pi'$ is IND-$\beta$-CCA2 secure. We assume that $\Pi'$ is not IND-$\beta$-CCA2 secure. That is, there exists a distinguisher $B = (B_1, B_2)$ for $\Pi'$. Now, we consider the following algorithm $B' = (B'_1, B'_2)$. $B'_1$ invokes $B_1$ and gets $(m_0, m_1, s)$ such that $\xi^{-1}(m_0) \geq 2$ and $\xi^{-1}(m_1) \geq 2$. We note that $B'_1$ can deal with oracle query from $B_1$ using his own oracle invocation. $B'_1$ finally outputs $(m_0, m_1, s)$. Let $c = \mathcal{E}_{pk}(m_b)$ for randomly chosen $b \in \{0,1\}$. $B'_2$ invokes $B_2$ with input $(m_0, m_1, s, c)$. $B'_2$ obtains the reply from $B_2$ and outputs the reply. Again $B'_2$ can deal with oracle query from $B_2$ using his own oracle invocation. It is not hard to see that $B' = (B'_1, B'_2)$ is a distinguisher of $\Pi$. This is a contradiction. Thus we have that $\Pi'$ is IND-$\beta$-CCA2 secure. □

The following two theorems are similarly shown as the proofs in [1].

**Theorem 15** *If a PKE scheme* $\Pi$ *IND-$\beta$-CCA2 secure then* $\Pi$ *is also NM-$\beta$-CCA2 secure.*

**Theorem 16** *If a PKE scheme* $\Pi$ *IND-$\gamma$-CCA2 secure then* $\Pi$ *is also NM-$\gamma$-CCA2 secure.*

## 5 Conclusion

In this paper, we refined the definitions of chosen ciphertext attack and discussed the power of chosen ciphertext attack more precisely. Though Bellare *et al* [1] showed the relation among security notions for public-key encryption, we refined the relation according to newly defined chosen ciphertext attack. We also gave some characterization of chosen ciphertext attack from the viewpoint of computational complexity theory. These results contribute to the understanding of chosen ciphertext attack and security for PKE schemes under CCA. Especially, we showed that the "invalidity checkable" property of the decryption algorithm plays an important role to determine the security of PKE schemes.

Though we worked out some relations among security notions for PKE schemes, the whole relations among relations have not been accomplished yet. If relations to $\alpha$-CCA1, $\beta$-CCA1 and $\gamma$-CCA1 are clarified, the understanding of security for PKE schemes under CCA will be improved further.

## References

[1] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *Proc. CRYPTO'98*, *Lecture Notes in Computer Science 1462*, pages 26–45. Springer, 1998.

[2] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. the 1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM, 1993.

[3] M. Bellare and A. Sahai. Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. In *Proc. CRYPTO'99*, *Lecture Notes in Computer Science 1666*, pages 519–536. Springer, 1999.

[4] D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS#1. In *Proc. CRYPTO'98*, *Lecture Notes in Computer Science 1462*, pages 1–12. Springer, 1998.

[5] G. Brassard. A note on the complexity of cryptography. *IEEE Transactions on Information Theory*, IT-25(2):232–233, 1979.

[6] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *Proc. the 30th Annual ACM Symposium on Theory of Computing*, pages 209–218. ACM, 1998.

[7] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Proc. CRYPTO'98*, *Lecture Notes in Computer Science 1462*, pages 13–25. Springer, 1998.

[8] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. *SIAM Journal on Computing*, 30(2):391–437, 2000.

[9] S. Even, A. L. Selman, and Y. Yacobi. The complexity of promise problems with applications to public-key cryptography. *Information and Control*, 61(2):159–173, 1984.

[10] Z. Galil, S. Haber, and M. Yung. Security against replay chosen-ciphertext attack. In J. Feigenbaum and M. Merritt, editors, *Distributed Computing and Cryptography*, volume 2 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 183–189. AMS, 1991.

[11] O. Goldreich. A uniform-complexity treatment of encryption and zero-knowledge. *Journal of Cryptology*, 6(1):21–53, 1993.

[12] O. Goldreich and S. Goldwasser. On the possibility of basing cryptography on the assumption that **P** $\neq$ **NP**. In *Cryptology ePrint Archive, Report 1998/005*, 1998. Available from `http://eprint.iacr.org/`.

[13] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[14] J. Grollmann and A. L. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.

[15] R. M. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thacher, editors, *Complexity of Computer Computations*, The IBM Research Symposia Series, pages 85–103. Plenum Press, New York, 1972.

[16] S. Micali, C. Rackoff, and B. Sloan. The notion of security for probabilistic cryptosystems. *SIAM Journal on Computing*, 17(2):412–426, 1988.

[17] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In *Proc. the 21st Annual ACM Symposium on Theory of Computing*, pages 33–43. ACM, 1989.

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

[19] C. Rackoff and D. R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Proc. CRYPTO'91*, *Lecture Notes in Computer Science 576*, pages 433–444. Springer, 1992.

[20] H. Rogers Jr. *Theory of Recursive Functions and Effective Computability.* McGraw Hill, 1967.

[21] U. Schöning. A low and a high hierarchy within **NP**. *Journal of Computer and System Sciences*, 27(1):14–28, 1983.

[22] A. L. Selman. Complexity issues in cryptography. In J. Hartmanis, editor, *Computational Complexity Theory*, volume 38 of *Proceedings of Symposia in Applied Mathematics*, pages 92–107. American Mathematical Society, 1989.

[23] A. L. Selman and Y. Yacobi. The complexity of promise problems. In *Proc. ICALP'82*, *Lecture Notes in Computer Science 140*, pages 502–509. Springer, 1982.