*Regular Paper*

# Relations among Notions of Security for Identity Based Encryption Schemes

Peng Yang,[†] Goichiro Hanaoka,[††] Yang Cui,[†] Rui Zhang,[†] Nuttapong Attrapadung,[†] Kanta Matsuura[†] and Hideki Imai[†]

Identity based encryption ($\mathcal{IBE}$) schemes have been flourishing since the very beginning of this century. In $\mathcal{IBE}$, proving the security of a scheme in the sense of IND-ID-CCA2 is widely believed to be sufficient to claim that the scheme is also secure in the senses of both SS-ID-CCA2 and NM-ID-CCA2. The justification for this belief is the relations among indistinguishability (IND), semantic security (SS) and non-malleability (NM). However these relations have been proved *only* for conventional public key encryption ($\mathcal{PKE}$) schemes in previous works. The fact is that $\mathcal{IBE}$ and $\mathcal{PKE}$ have a difference of special importance, i.e., only in $\mathcal{IBE}$ can the adversaries perform a particular attack, namely, the *chosen identity attack*. In this paper we have shown that security proved in the sense of IND-ID-CCA2 is validly sufficient for implying security in any other sense in $\mathcal{IBE}$. This is to say that the security notion, IND-ID-CCA2, captures the essence of security for all $\mathcal{IBE}$ schemes. To show this, we first formally defined the notions of security for $\mathcal{IBE}$, and then determined the relations among IND, SS and NM in $\mathcal{IBE}$, along with rigorous proofs. All of these results take the chosen identity attack into consideration.

## 1. Introduction

Identity based encryption ($\mathcal{IBE}$) is a public key encryption mechanism where an arbitrary string, such as the recipient's identity, can serve as a public key. This convenience eliminates the need to distribute public key certificates. On the other hand, in conventional public key encryption ($\mathcal{PKE}$) schemes, it is unavoidable to access the online public key directory in order to obtain the public keys. $\mathcal{IBE}$ schemes are largely motivated by many applications such as encrypting emails with the recipient's e-mail address.

Although the basic concept of $\mathcal{IBE}$ was proposed by Shamir[15] more than two decades ago, only very recently was the first fully functional scheme proposed[7]. In 2001, Boneh and Franklin defined a security model and gave the first fully functional solution provably secure in the random oracle model. The notions of security proposed in their work are natural extensions to the standard ones for $\mathcal{PKE}$, namely indistinguishability-based ones.

### 1.1 Motivation

So far in the literature, the security notion IND-ID-CCA2 is widely considered to be the "right" one that captures the essence of security for $\mathcal{IBE}$[4)~7),17)]. However, this issue has not been investigated rigorously, *yet*. In this work we aim to establish such an affirmative justification. Before discussing how to define the "right" security notion for $\mathcal{IBE}$, we first review the case of $\mathcal{PKE}$.

#### 1.1.1 Notions of Security for $\mathcal{PKE}$

A convenient way to formalize notions of security for cryptographic schemes is to consider combinations of various *security goals* and possible *attack models*. Three essential security goals being considered in the case of $\mathcal{PKE}$ are *indistinguishability* (IND), *semantic security* (SS)[13], and *non-malleability* (NM)[9], i.e. $\mathsf{G}_i \in$ {IND,SS,NM}. The attack models are the *chosen plaintext attack* (CPA)[13], the *non-adaptive chosen ciphertext attack* (CCA1)[9] and the *adaptive chosen ciphertext attack* (CCA2)[14], i.e., $\mathsf{A}_j \in$ {CPA,CCA1,CCA2}. (The details of these attack models are given in Appendix A.1.) Their combinations give nine security notions for $\mathcal{PKE}$, e.g. IND-CCA2.

SS is widely accepted as the natural goal of encryption scheme because it formalizes an adversary's inability to obtain any information about the plaintext from a given ciphertext. The equivalence of SS-CPA and IND-CPA has been proved[13]; and the equivalences between SS-CCA1,2 and IND-CCA1,2 have been proven only recently[12),16)]. On the other hand, NM formalizes an adversary's inability, given a chal-

[†] Institute of Industrial Science, The University of Tokyo
[††] Research Center for Information Security, National Institute of Advanced Industrial Science and Technology

$$\begin{tikzcd}
\mathsf{NM\text{-}ID\text{-}CPA} \arrow[d, "5"'] & \mathsf{NM\text{-}ID\text{-}CCA1} \arrow[l, dotted] \arrow[d, "5"'] & \mathsf{NM\text{-}ID\text{-}CCA2} \arrow[l, dotted] \arrow[d, shift right, "5"'] \\
\mathsf{IND\text{-}ID\text{-}CPA} \arrow[d, shift right, "2"'] & \mathsf{IND\text{-}ID\text{-}CCA1} \arrow[l, dotted] \arrow[d, shift right, "2"'] & \mathsf{IND\text{-}ID\text{-}CCA2} \arrow[l, dotted] \arrow[u, shift right, "4"'] \arrow[d, shift right, "2"'] \\
\mathsf{SS\text{-}ID\text{-}CPA} \arrow[u, shift right, "3"'] & \mathsf{SS\text{-}ID\text{-}CCA1} \arrow[l, dotted] \arrow[u, shift right, "3"'] & \mathsf{SS\text{-}ID\text{-}CCA2} \arrow[l, dotted] \arrow[u, shift right, "3"']
\end{tikzcd}$$

**Fig. 1** Relations among notions of security for $\mathcal{IBE}$.

lenge ciphertext $y^*$, to output a different ciphertext $y'$ in such a way that the plaintexts $x$ and $x'$ underlying these two ciphertexts are meaningfully related, e.g., $x' = x + 1$. The implications from $\mathsf{IND\text{-}CCA2}$ to $\mathsf{NM}$ under any attack have been proved[3]. For these reasons, along with the convenience of proving security in the sense of $\mathsf{IND}$, in almost all concrete schemes, $\mathsf{IND\text{-}CCA2}$ is considered to be the "right" standard security notion for $\mathcal{PKE}$.

### 1.1.2 Towards Defining Notions of Security for $\mathcal{IBE}$

Due to a particular mechanism, the adversaries are granted more power in $\mathcal{IBE}$ than in $\mathcal{PKE}$. Essentially, the adversaries can access the *key extraction oracle*, which answers the private key of any queried public key (identity). Including this particular *adaptive chosen identity attack*[☆], we formalize the security notions for $\mathcal{IBE}$, e.g., $\mathsf{IND\text{-}ID\text{-}CCA2}$, in this way: $\mathsf{G}_i$-$\mathsf{ID}$-$\mathsf{A}_j$, where $\mathsf{G}_i \in \{\mathsf{IND,SS,NM}\}$, $\mathsf{ID}$ denotes the particular attack mentioned above, and $\mathsf{A}_j \in \{\mathsf{CPA,CCA1,CCA2}\}$. Boneh and Franklin were the first to define the security notion for $\mathcal{IBE}$, by naturally extending $\mathsf{IND\text{-}CCA2}$ to $\mathsf{IND\text{-}ID\text{-}CCA2}$.

Let us rigorously investigate whether $\mathsf{IND\text{-}ID\text{-}CCA2}$ could be considered the "right" notion for $\mathcal{IBE}$, besides the intuitive reason that it is analogous to $\mathsf{IND\text{-}CCA2}$. The natural approach to justify the appropriateness for $\mathcal{IBE}$ is, analogously to the case of $\mathcal{PKE}$, to (i) first define $\mathsf{SS}$- and $\mathsf{NM}$- based security notions for $\mathcal{IBE}$ (ii) and then establish the relations among the above security notions. To be more specific, we establish implications from $\mathsf{IND\text{-}ID\text{-}CCA2}$ to all the other notions; i.e., $\mathsf{IND\text{-}ID\text{-}CCA2}$ is the *strongest* notion of security for $\mathcal{IBE}$.

Intuition tells us that task (i) can be simply achieved by considering the analogy to the case of shifting $\mathsf{IND\text{-}CCA}$ to $\mathsf{IND\text{-}ID\text{-}CCA}$ as done in Ref. 7), and that task (ii) immediately follows from the relations among the notions as in the case of $\mathcal{PKE}$ because we shift all the notions with the same additional attack power (namely, the accessibility to the key extraction oracle). However, we emphasize that the tasks will not follow simply and immediately until rigorous definitions for task (i) and rigorous proofs for task (ii) are presented. We accomplish both tasks in this paper.

## 1.2 Our Contributions

Our contributions are twofold. First, we formally present the definitions of the notions of security for $\mathcal{IBE}$ schemes. The overall definitions are built upon previous work[3],[7],[12].

Second, we rigorously prove the relations among these notions and conclude that, $\mathsf{IND\text{-}ID\text{-}CCA2}$ is the "right" notion of security for $\mathcal{IBE}$. Our intuition about those relations turns out to be right: the implication $\mathsf{G}_1$-$\mathsf{ID}$-$\mathsf{A}_1 \Rightarrow \mathsf{G}_2$-$\mathsf{ID}$-$\mathsf{A}_2$ holds in $\mathcal{IBE}$ if and only if $\mathsf{G}_1$-$\mathsf{A}_1 \Rightarrow \mathsf{G}_2$-$\mathsf{A}_2$ holds in $\mathcal{PKE}$, where the corresponding security goals $\mathsf{G}_i$ and attack models $\mathsf{A}_j$ are as mentioned above.

The results of our second contribution are illustrated in **Fig. 1**. The vertical *line arrows* represent implications that are explicitly proven, and the horizontal *dot arrows* represent implications that are self-evident. In both cases, an arrow from notion **A** to notion **B** denotes that if an identity based encryption scheme is secure in the sense of **A**, then it is also secure in the sense of **B**. The scripted numbers beside the arrows denote the theorem or lemma in which the implication is proved.

Our results could be considered to have the same flavor as some historical results, to name just one, the equivalence between $\mathsf{IND\text{-}CCA2}$ and $\mathsf{SS\text{-}CCA2}$ for $\mathcal{PKE}$. There, although $\mathsf{IND\text{-}CPA}$ and $\mathsf{SS\text{-}CPA}$ were defined and proved

[☆] Actually, in $\mathcal{IBE}$, there exists the other attack against identity, called the *selective chosen identity attack*. We omit formal definitions of the security notions in this selective-ID secure sense because these notions are weak. More details about the selective chosen identity attack are given in Appendix A.2.

equivalent in 1984[13)], the equivalence between IND-CCA2 and SS-CCA2 was not proved rigorously until 2003[16)]. During this long period of time, people simply believed that shifting the attack power from CPA to CCA2 did not affect the equivalence.

A preliminary version of this paper was presented as a part of Ref. 1), which is merged from two independent studies[2),10)].

### 1.3 Organization

The rest of the paper is organized as follows: in Section 2, we review the formal definitions of $\mathcal{IBE}$ schemes and several other basic terms. In Section 3, we formally define notions of security for $\mathcal{IBE}$ schemes. In Section 4, we rigorously prove important relations among these notions.

## 2. Preliminary

In this section, we review the model of $\mathcal{IBE}$ and define some notations.

### 2.1 Identity Based Encryption

Formally, an identity based encryption scheme consists of four algorithms, i.e., $\mathcal{IBE} = (\mathcal{S}, \mathcal{X}, \mathcal{E}, \mathcal{D})$, where

- $\mathcal{S}$, the setup algorithm, takes a security parameter $k$ and outputs system parameters $param$ and a master-key, $mk$. The system parameters include a description of a message space $\mathcal{M}$ and a description of a ciphertext space $\mathcal{C}$. The system parameters should be publicly known, while the $mk$ should be known only by the "private key generator" (PKG).
- $\mathcal{X}$, the extract algorithm, takes three inputs, $param, mk$, and an arbitrary string $id \in \{0,1\}^*$, and outputs a private key, $sk = \mathcal{X}(param, mk, id)$. Here, $id$ will be used as the public encryption key, and $sk$ is the corresponding private decryption key. Intuitively, this algorithm extracts the private key from a given public key.
- $\mathcal{E}$, the encrypt algorithm, takes three inputs, $param$, $id \in \{0,1\}^*$, and a plaintext $x \in \mathcal{M}$. It outputs the corresponding ciphertext $y \in \mathcal{C}$.
- $\mathcal{D}$, the decrypt algorithm, takes three inputs, $param$, $y \in \mathcal{C}$, and the corresponding private key $sk$. It outputs $x \in \mathcal{M}$.

The four algorithms must satisfy the standard consistency constraint; i.e., if $sk$ is the private key generated by the extract algorithm with the given $id$ as the public key, then $\forall x \in \mathcal{M} : \mathcal{D}(param, sk, y) = x$, where $y = \mathcal{E}(param, id, x)$.

### 2.2 Conventions

**Notations.**

We use $\vec{x} \leftarrow \mathcal{D}(param, sk, \vec{y})$ to denote that the vector $\vec{x}$ is made up of the plaintexts corresponding to every ciphertext in the vector $\vec{y}$. The term $\hat{\mathcal{M}}$ denotes a subset of message space $\mathcal{M}$, where the elements of $\hat{\mathcal{M}}$ are distributed according to the distribution designated by some algorithm. The function $h : \hat{\mathcal{M}} \rightarrow \{0,1\}^*$ denotes the a-priori partial information about the plaintext, and the function $f : \hat{\mathcal{M}} \rightarrow \{0,1\}^*$ denotes the a-posteriori partial information.

**Negligible Function.**

We say that a function $\epsilon : \mathbb{N} \rightarrow \mathbb{R}$ is *negligible* if for every constant $c \geq 0$, an integer $k_c$ exists such that $\epsilon(k) < k^{-c}$ for all $k > k_c$.

**$R$-related Relation.**

We consider the $R$-related relation of arity $t$, where $t$ is polynomial in the security parameter $k$. Rather than writing $R(x_1, x_2, \ldots, x_t)$, we write $R(x, \vec{x})$, denoting that the first argument is special and bunching the others into a vector $\vec{x}$ where $|\vec{x}| = t - 1$ and for every $x_i \in \vec{x},\ R(x, x_i)$ holds.

**Experiments.**

Let $A$ be a probabilistic algorithm, and let $A(x_1, \ldots, x_n; r)$ be the result of running $A$ on inputs $(x_1, \ldots, x_n)$ and coins $r$. Let $y \leftarrow A(x_1, \ldots, x_n)$ denote the experiment of picking $r$ at random, and let $y$ be $A(x_1, \ldots, x_n; r)$. If $S$ is a finite set, then let $x \leftarrow S$ denote the operation of picking an element randomly and uniformly from $S$. If $\alpha$ is neither an algorithm nor a set, then let $x \leftarrow \alpha$ denote a simple assignment statement. We say that $y$ can be output by $A(x_1, \ldots, x_n)$ if there is some $r$ such that $A(x_1, \ldots, x_n; r) = y$.

## 3. Definitions of Security Notions for $\mathcal{IBE}$ Schemes

Let $A = (A_1, A_2)$ be an adversary. We say that $A$ is polynomial time if both probabilistic algorithms $A_1$ and $A_2$ are polynomial time. In the first stage, given the system parameters, the adversary computes and outputs a challenge template $\tau$. The algorithm $A_1$ can output some state information $s$, which will be transferred to $A_2$. In the second stage, the adversary is issued a challenge ciphertext $y^*$ generated from $\tau$ by a probabilistic function, in a manner depending on the goal. We say that the adversary $A$ breaks the scheme if she achieves her goal.

We consider three security goals, IND, SS and

**Table 1** Oracle set $\mathcal{O}_1$ in the definitions of the notions for $\mathcal{IBE}$.

| | $\mathcal{O}_1 = \{\mathcal{XO}_1, \mathcal{EO}_1, \mathcal{DO}_1\}$ |
|---|---|
| ID-CPA | $\{\mathcal{X}(param, mk, \cdot), \mathcal{E}(param, id, \cdot), \varepsilon\}$ |
| ID-CCA1 | $\{\mathcal{X}(param, mk, \cdot), \mathcal{E}(param, id, \cdot), \mathcal{D}(param, sk, \cdot)\}$ |
| ID-CCA2 | $\{\mathcal{X}(param, mk, \cdot), \mathcal{E}(param, id, \cdot), \mathcal{D}(param, sk, \cdot)\}$ |

**Table 2** Oracle set $\mathcal{O}_2$ in the definitions of the notions for $\mathcal{IBE}$.

| | $\mathcal{O}_2 = \{\mathcal{XO}_2, \mathcal{EO}_2, \mathcal{DO}_2\}$ |
|---|---|
| ID-CPA | $\{\mathcal{X}(param, mk, \cdot), \mathcal{E}(param, id, \cdot), \varepsilon\}$ |
| ID-CCA1 | $\{\mathcal{X}(param, mk, \cdot), \mathcal{E}(param, id, \cdot), \varepsilon\}$ |
| ID-CCA2 | $\{\mathcal{X}(param, mk, \cdot), \mathcal{E}(param, id, \cdot), \mathcal{D}(param, sk, \cdot)\}$ |

NM, and we consider three attack models, ID-CPA,ID-CCA1 and ID-CCA2, in order of increasing strength. The difference among the models is whether $A_1$ or $A_2$ is granted access to decryption oracles[☆].

We describe in **Table 1** and **Table 2** the ability with which the adversary in different attack models accesses the *Extraction Oracle* $\mathcal{X}(param, mk, \cdot)$, the *Encryption Oracle* $\mathcal{E}(param, id, \cdot)$ and the *Decryption Oracle* $\mathcal{D}(param, sk, \cdot)$. The only restriction is that in ID-CCA2, $A_2$ must not ask the decryption oracle for the decryption of the challenge $y^*$.

When we say $\mathcal{O}_i = \{\mathcal{XO}_i, \mathcal{EO}_i, \mathcal{DO}_i\} = \{\mathcal{X}(param, mk, \cdot), \mathcal{E}(param, id, \cdot), \varepsilon\}$, where $i \in \{1, 2\}$, we mean that $\mathcal{DO}_i$ is a function that returns an empty string $\varepsilon$ for any input.

*Remark 1.*To have meaningful definitions, we insist that the target public key *id* should not be previously queried on; i.e., the definitions are completely meaningless if the adversary already knows the corresponding private key of *id*.

### 3.1 Indistinguishability

This important notion of security was first introduced by Goldwasser and Micali [13] for $\mathcal{PKE}$ and then described by Boneh and Franklin [7] for $\mathcal{IBE}$. Here, we define indistinguishability through a two-stage experiment. The algorithm $A_1$ is run on the system parameters *param* as input. At the end of executing $A_1$, the adversary outputs $(x_0, x_1, s, id)$ such that $x_0$ and $x_1$ are plaintexts with the same length, $s$ is state information (possibly including *param*) that she wants to preserve, and *id* is the public key that she wants to attack. One of $x_0$ and $x_1$ is *randomly* selected, say $x_b$, beyond the adversary's view. A challenge $y^*$ is computed by encrypting $x_b$ with the public key *id*. The algorithm $A_2$ tries to distinguish whether $y^*$ was the encryption of $x_0$ or $x_1$.

**Definition 1 (IND-ID-CPA, IND-ID-CCA1, IND-ID-CCA2).** Let $\mathcal{IBE} = (\mathcal{S}, \mathcal{X}, \mathcal{E}, \mathcal{D})$ be an identity based encryption scheme and let $A = (A_1, A_2)$ be an adversary. For $\texttt{atk} \in \{\texttt{id-cpa}, \texttt{id-cca1}, \texttt{id-cca2}\}$ and $k \in \mathbb{N}$, let

$$\begin{aligned}\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},A}(k) = \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},A}(k) = 1] \\ -\Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},A}(k) = 1]\end{aligned} \quad (1)$$

where for $b, d \in \{0, 1\}$ and $|x_0| = |x_1|$,

```
Experiment $\mathbf{Exp}^{\texttt{ind-atk-b}}_{\mathcal{IBE},A}(k)$
    $(param, mk) \leftarrow \mathcal{S}(k)$;
    $(x_0, x_1, s, id) \leftarrow A_1^{\mathcal{O}_1}(param)$;
    $y^* \leftarrow \mathcal{E}(param, id, x_b)$;
    $d \leftarrow A_2^{\mathcal{O}_2}(x_0, x_1, s, y^*, id)$;
    return $d$
```

We say that $\mathcal{IBE}$ is secure in the sense of IND-ATK, if $\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},A}(k)$ is negligible for any $A$.

### 3.2 Semantic Security

Semantic security (for $\mathcal{PKE}$) was introduced by Goldwasser and Micali [13] and later refined by Goldreich [11]. It captures the security requirement that intercepting the ciphertext gives an adversary no partial information. We can naturally extend it to the case of $\mathcal{IBE}$. $A_1$ is given *param* and outputs $(\hat{\mathcal{M}}, h, f, s, id)$. Here, the distribution of $\hat{\mathcal{M}}$ is designated by $A_1$, and $(\hat{\mathcal{M}}, h, f)$ is the challenge template $\tau$. $A_2$ receives an encryption $y^*$ of a random message

[☆] Inspecting the similarity between the adaptive chosen identity attack and the selective chosen identity attack, we only discuss in details the former case (full-ID security). The results can be extended to the latter case (selective-ID security), because the strategies are similar. Roughly speaking, the target public key *id* should be decided by the adversary in advance, before the challenger runs the setup algorithm. The restriction is that the extraction query on *id* is prohibited.

$x^*$ drawn from $\hat{\mathcal{M}}$. The adversary then outputs a value $v$. She hopes that $v = f(x^*)$. The adversary is successful if she can do this with a probability significantly higher than any *simulator* does. The simulator tries to do as well as the adversary without knowing the challenge ciphertext $y^*$ or accessing any oracle.

**Definition 2 (SS-ID-CPA, SS-ID-CCA1, SS-ID-CCA2).** Let $\mathcal{IBE} = (\mathcal{S}, \mathcal{X}, \mathcal{E}, \mathcal{D})$ be an identity based encryption scheme, let $A = (A_1, A_2)$ be an adversary, and let $A' = (A'_1, A'_2)$ be the simulator. For $\texttt{atk} \in \{\texttt{id-cpa}, \texttt{id-cca1}, \texttt{id-cca2}\}$ and $k \in \mathbb{N}$, let

$$\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},A,A'}(k) = \Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A'}(k) = 1] \quad (2)$$

where for $b \in \{0, 1\}$,

```
Experiment $\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A}(k)$
    $(param, mk) \leftarrow \mathcal{S}(k)$;
    $(\hat{\mathcal{M}}, h, f, s, id) \leftarrow A_1^{\mathcal{O}_1}(param)$;
    $x^* \leftarrow \hat{\mathcal{M}}$;
    $y^* \leftarrow \mathcal{E}(param, id, x^*)$;
    $v \leftarrow A_2^{\mathcal{O}_2}(s, y^*, h(x^*), id)$;
    if $v = f(x^*)$
        then $d \leftarrow 1$ else $d \leftarrow 0$;
    return $d$
```

```
Experiment $\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A'}(k)$
    $(\hat{\mathcal{M}}, h, f, s, id) \leftarrow A'_1(k)$;
    $x^* \leftarrow \hat{\mathcal{M}}$;
    $v \leftarrow A'_2(s, |x^*|, h(x^*), id)$;
    if $v = f(x^*)$
        then $d \leftarrow 1$ else $d \leftarrow 0$;
    return $d$
```

We say that $\mathcal{IBE}$ is secure in the sense of SS-ATK if for any adversary $A$ a simulator exists such that $\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},A,A'}(k)$ is negligible.

We comment here that in the two cases, $\tau$ must be distributed identically because both $A$ and $A'$ generate target public key $id$ by themselves, i.e., $\tau$ is output individually by $A$ and $A'$.

### 3.3 Non-malleability

Non-malleability was introduced by Dolev et al.[9]. It roughly requires that an adversary, given a challenge ciphertext, cannot modify it into another, different ciphertext in such a way that the plaintexts underlying the two ciphertexts are meaningfully related. $A_1$ is given *param* and outputs a triple $(\hat{\mathcal{M}}, s, id)$. $A_2$ receives an encryption $y^*$ of a random message $x_1$ drawn from $\hat{\mathcal{M}}$. The adversary then outputs a description of a relation $R$ and a vector $\vec{y}$ of ciphertexts. We insist that $y \notin \vec{y}$[☆]. The adversary hopes that $R(x_1, \vec{x})$ holds. We say that she is successful if she can do this with a probability significantly greater than that with which $R(x_0, \vec{x})$ holds. Here, $x_0$ is also a plaintext chosen uniformly from $\hat{\mathcal{M}}$, independently of $x_1$.

**Definition 3 (NM-ID-CPA, NM-ID-CCA1, NM-ID-CCA2).** Let $\mathcal{IBE} = (\mathcal{S}, \mathcal{X}, \mathcal{E}, \mathcal{D})$ be an identity based encryption scheme and let $A = (A_1, A_2)$ be an adversary. For $\texttt{atk} \in \{\texttt{id-cpa}, \texttt{id-cca1}, \texttt{id-cca2}\}$ and $k \in \mathbb{N}$, let

$$\mathbf{Adv}^{\texttt{nm-atk}}_{\mathcal{IBE},A}(k) = \Pr[\mathbf{Exp}^{\texttt{nm-atk-1}}_{\mathcal{IBE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\texttt{nm-atk-0}}_{\mathcal{IBE},A}(k) = 1] \quad (3)$$

where for $b \in \{0, 1\}$ and $|x_0| = |x_1|$,

```
Experiment $\mathbf{Exp}^{\texttt{nm-atk-b}}_{\mathcal{IBE},A}(k)$
    $(param, mk) \leftarrow \mathcal{S}(k)$;
    $(\hat{\mathcal{M}}, s, id) \leftarrow A_1^{\mathcal{O}_1}(param)$;
    $x_0, x_1 \leftarrow \hat{\mathcal{M}}$;
    $y^* \leftarrow \mathcal{E}(param, id, x_1)$;
    $(R, \vec{y}) \leftarrow A_2^{\mathcal{O}_2}(s, y^*, id)$;
    $\vec{x} \leftarrow \mathcal{D}(param, id, \vec{y})$;
    if $y^* \notin \vec{y} \wedge \perp \notin \vec{x} \wedge R(x_b, \vec{x})$
        then $d \leftarrow 1$ else $d \leftarrow 0$;
    return $d$
```

We say that $\mathcal{IBE}$ is secure in the sense of NM-ATK, if $\mathbf{Adv}^{\texttt{nm-atk}}_{\mathcal{IBE},A}(k)$ is negligible for any $A$.

## 4. Relations among the Notions of Security for $\mathcal{IBE}$ Schemes

In this section, we show that security proved in the sense of IND-ID-CCA2 is validly sufficient for implying security in any other sense in $\mathcal{IBE}$. We first extend the relation (equivalence) between IND-ATK and SS-ATK into the $\mathcal{IBE}$ environment and then extend the relation between IND-ATK and NM-ATK into the $\mathcal{IBE}$ environment. Because of these relations, the research on identity based encryption schemes has been blossoming over the past several years; thus, we say that these relations are significant.

### 4.1 Equivalence of IND and SS

**Theorem 1 (IND-ATK ⇔ SS-ATK).** *A scheme $\mathcal{IBE}$ is secure in the sense of* IND-ATK *if and only if $\mathcal{IBE}$ is secure in the sense of*

[☆] The adversary is prohibited from copying the challenge ciphertext $y^*$. Otherwise, she could output the equality relation $R$, where $R(a, b)$ holds if and only if $a = b$, output $\vec{y} = \{y^*\}$, and *always* be successful.

SS-ATK*, for any attack* ATK $\in$ {ID-CPA,ID-CCA1,ID-CCA2}*.*

We prove this theorem by proving two directions, i.e., that IND-ATK implies SS-ATK and that SS-ATK implies IND-ATK.

**Lemma 2 (IND-ATK $\Rightarrow$ SS-ATK).** *If a scheme $\mathcal{IBE}$ is secure in the sense of* IND-ATK *then $\mathcal{IBE}$ is secure in the sense of* SS-ATK*, for any attack* ATK $\in$ {ID-CPA,ID-CCA1,ID-CCA2}*.*

*Main Idea of Proof.* To clearly show the proof strategy, we describe our main idea as follows. First, according to the definition of SS, to prove that the scheme is secure in the sense of SS-ATK, we show that for any SS-ATK adversary $B$, a corresponding simulator $B'$ can be constructed with oracle access to $B$ such that $B'$ can do as well as $B$ in an SS-ATK game. To calculate how well the constructed simulator $B'$ can do, we first construct an IND-ATK adversary $A$ with oracle access to $B$ and show that $\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},B,B'}(k)$ is equal to $\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},A}(k)$. Because the scheme is secure in the IND-ATK sense, no matter which $B$ is accessed as an oracle, the advantage, $\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},A}(k)$, of $A$ to break the scheme is *always* negligible. Thus, we claim that the advantage, $\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},B,B'}(k)$, of $B$ to break the scheme is also negligible; i.e., $B'$ can do as well as $B$. This is to say that the scheme is secure in the SS-ATK sense. The point is how to prove that the advantage of $A$ in IND-ATK game is equal to the advantage of $B$ in SS-ATK game.

**Proof** Let $B' = (B'_1, B'_2)$, $B = (B_1, B_2)$ and $A = (A_1, A_2)$ be SS-ATK simulator, SS-ATK adversary and IND-ATK adversary, respectively. In our construction, both adversaries $B$ and $A$ have access to an oracle set $\mathcal{O}_1$ at their first stage and an oracle set $\mathcal{O}_2$ in their second stages, while the simulator $B'$ has no access to any oracle. The compositions of these oracle sets are represented in Section 3.

The SS-ATK simulator $B'$ is constructed as follows:

```
Algorithm $B'_1(k)$
    $(param, mk) \leftarrow \mathcal{S}(k)$;
    $(\hat{\mathcal{M}}, h, f, s, id) \leftarrow B_1^{\mathcal{O}_1}(param)$;
    return $(\hat{\mathcal{M}}, h, f, s, id)$

Algorithm $B'_2(s, |x^*|, h(x^*), id)$
    $x' \leftarrow \hat{\mathcal{M}}$ where $|x'| = |x^*|$;
    $y' \leftarrow \mathcal{E}(param, id, x')$;
    $v \leftarrow B_2^{\mathcal{O}_2}(s, y', h(x^*), id)$;
    return $v$
```

The point that must be emphasized is that because the challenge template $\tau = (\hat{\mathcal{M}}, h, f)$ is chosen by $B$ and $B'$ themselves, $\tau$ is distributed identically in the two cases. Thus, $B'_1$ is likely to start by generating $(mk, param) \leftarrow \mathcal{S}(k)$, where *param* is the same as the system parameters given to $B_1$.

We comment that the generated master-key *mk* allows $B'$ not only to *simulate* the extraction oracle, but also to extract the secret key *sk* corresponding to the target public key *id*. In this way, $B'$ is able to *simulate* the encryption oracle and decryption oracle.

To calculate how well the simulator $B'$ does, we construct an IND-ATK adversary $A$ and show that $\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},B,B'}(k)$ is equal to $\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},A}(k)$.

```
Algorithm $A_1^{\mathcal{O}_1}(param)$
    $(\hat{\mathcal{M}}, h, f, s, id) \leftarrow B_1^{\mathcal{O}_1}(param)$;
    $x_0, x_1 \leftarrow \hat{\mathcal{M}}$;
    $s' \leftarrow (s, h)$;
    return $(x_0, x_1, s', id)$

Algorithm $A_2^{\mathcal{O}_2}(x_0, x_1, s', y^*, id)$
                              where $s' = (s, h)$
    $v \leftarrow B_2^{\mathcal{O}_2}(s, y^*, h(x_1), id)$;
    if $v = f(x_1)$ then $d \leftarrow 1$ else $d \leftarrow 0$;
    return $d$
```

Note that in the experiment $\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},B'}(k)$, the simulator $B'$ invokes the SS-ATK adversary $B$ with a *dummy* encryption $y'$. This experiment finally outputs 1 only when $B$ captures a-posteriori partial information from this *dummy* encryption. On the other hand, in the experiment $\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},A}(k)$, the adversary IND-ATK $A$ is challenged with the ciphertext $y^*$ corresponding to $x_0$, invokes $B$ with the a-priori partial information $h(x_1)$, and finally outputs 1 only when the SS-ATK adversary $B$ captures the a-posteriori partial information $f(x_1)$ of $x_1$. Thus we say in this situation that the encryption $y^*$ is also a *dummy* for $B$. Hence,

$$\Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},A}(k) = 1] = \Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},B'}(k) = 1] \tag{4}$$

In contrast, in the experiment $\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},A}(k)$, the IND-ATK adversary $A$ is challenged with the ciphertext $y^*$ corresponding to $x_1$. Focusing on our construction of $A$, we can see that this experiment obviously outputs 1 only when $B$ captures a-posteriori partial information from this *useful* (no longer *dummy*) encryption; i.e., at the end of $B$'s second stage $B$ outputs $v$ and $v = f(x_1)$. Hence,

$$\Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},A}(k)=1]=\Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},B}(k)=1] \qquad (5)$$

We obtain

$$\begin{aligned}\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},A}(k) &\overset{(1)}{=} \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},A}(k)=1]\\ &\quad -\Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},A}(k)=1]\\ &\overset{(2)}{=} \Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},B}(k)=1]\\ &\quad -\Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},B'}(k)=1]\\ &\overset{(3)}{=} \mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},B,B'}(k)\end{aligned}$$

Equations $\overset{(1)}{=}$ and $\overset{(3)}{=}$ are according to the definitions of advantages in IND (1) and SS (2), respectively. Equation $\overset{(2)}{=}$ holds according to Eqs. (4) and (5).

Because $\mathcal{IBE}$ is secure in the IND-ATK sense we know that for the adversary $A$ constructed by any $B$ $\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},A}(k)$ is negligible, and hence for any $B$, $\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},B,B'}(k)$ is negligible too. Thus we say the constructed simulator $B'$ does as well as *any* adversary $B$. This concludes the proof of Lemma 2. □

**Lemma 3 (SS-ATK ⇒ IND-ATK).** *If a scheme $\mathcal{IBE}$ is secure in the sense of* SS-ATK *then $\mathcal{IBE}$ is secure in the sense of* IND-ATK*, for any attack* ATK $\in$ {ID-CPA,ID-CCA1,ID-CCA2}*.*

*Main Idea of Proof.* Our strategy is as follows. Towards contradiction, we prove that if a scheme is *not* secure in the IND-ATK sense, then it is *not* secure in the SS-ATK as well. So we first assume there exists an IND-ATK adversary $B$ who can successfully break IND-ATK with an advantage that is not negligible, and then we show that we can construct an SS-ATK adversary $A$ who can successfully break SS-ATK with an advantage that is not negligible; i.e., no SS-ATK simulator exists that can do as well as $A$. We do this by allowing $A$ to call $B$ as an oracle.

**Proof** Let $A = (A_1, A_2)$ and $B = (B_1, B_2)$ be SS-ATK adversary and IND-ATK adversary respectively.

$A$ is constructed as follows:

```
Algorithm $A_1^{\mathcal{O}_1}(param)$
    $(x_0, x_1, s, id) \leftarrow B_1^{\mathcal{O}_1}(param)$;
    $\hat{\mathcal{M}} \leftarrow \{x_0, x_1\}_U$;
    choose $f$ satisfies $f(x_0) = 0$ and $f(x_1) = 1$;
    choose $h$ satisfies $h(x_0) = h(x_1)$;
    return $(\hat{\mathcal{M}}, h, f, s, id)$
```

```
Algorithm $A_2^{\mathcal{O}_2}(s, y^*, h(x^*), id)$
    $d' \leftarrow B_2^{\mathcal{O}_2}(x_0, x_1, s, y^*, id)$;
    $v \leftarrow d'$;
    return $v$
```

Because either $x_0$ or $x_1$ is chosen at a probability of 1/2, we obtain

$$\Pr[b=0] = \Pr[b=1] = \frac{1}{2} \qquad (6)$$

Recalling the definition of advantages in IND-ATK (1), we obtain

$$\begin{aligned}&\Pr[\mathbf{Exp}^{\texttt{ind-atk-b}}_{\mathcal{IBE},B}(k)=0]\\ &\quad +\Pr[\mathbf{Exp}^{\texttt{ind-atk-b}}_{\mathcal{IBE},B}(k)=1]=1 \qquad (7)\end{aligned}$$

for $b \in \{0,1\}$. Furthermore, focusing on our construction, we obtain

$$\begin{aligned}&\Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A}(k)=1]\\ &\quad = \Pr[b=0]\cdot\Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},B}(k)=0]\\ &\qquad + \Pr[b=1]\cdot\Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k)=1]\\ &\quad \overset{(1)}{=} \frac{1}{2}\cdot(1-\Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},B}(k)=1])\\ &\qquad + \frac{1}{2}\cdot\Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k)=1]\\ &\quad \overset{(2)}{=} \frac{1}{2}+\frac{1}{2}\cdot\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},B}(k) \qquad (8)\end{aligned}$$

Here, equation $\overset{(1)}{=}$ holds according to Eqs. (6) and (7). Equation $\overset{(2)}{=}$ holds according to Eq. (1).

On the other hand, recall the definition of SS-ATK (on Page 2421). Because the challenge template $\tau$ should be distributed identically in the two cases, we observe that in the second stage of the simulator, the input values $\big(s, |x^*|, h(x^*), id\big)$ are independent of the event $x^* = x_b$, where $b$ is chosen randomly and uniformly in $\{0,1\}$. Hence for any simulator,

$$\Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A'}(k)=1] \le \frac{1}{2} \qquad (9)$$

This means that $A'$ cannot be successful at a probability more than 1/2. In this inequality, the equality holds in case $A'$ always outputs a value in $\{0,1\}$.

According to the definition of advantage in SS-ATK (2) and Eq. (8) and inequality (9), we obtain

$$\begin{aligned}\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},A,A'}(k) &= \Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A}(k)=1]\\ &\quad -\Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A'}(k)=1]\\ &\ge \frac{1}{2}\cdot\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},B}(k)\end{aligned}$$

We have assumed that $\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},B}(k)$ is not negligible; thus, $\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},A,A'}(k)$ is also not negligible. We have reached a contradiction to the hypothesis that $\mathcal{IBE}$ is secure in the SS-ATK sense. Thus, $\mathcal{IBE}$ is also secure in the IND-ATK sense. This concludes the proof of Lemma 3. □

**Proof of Theorem 1** From Lemma 2 and 3, Theorem 1 is proven immediately. ■

### 4.2 Relations between IND and NM

**Theorem 4 (IND-ID-CCA2 ⇒ NM-ID-CCA2).** *If a scheme $\mathcal{IBE}$ is secure in the sense of* IND-ID-CCA2 *then $\mathcal{IBE}$ is secure in the sense of* NM-ID-CCA2*.*

*Main Idea of Proof.* Towards contradiction, we prove that if a scheme is *not* secure in the NM-ID-CCA2 sense, then it is *not* secure in the IND-ID-CCA2 either. We first assume that an NM-ID-CCA2 adversary $B$ exists who can break NM-ID-CCA2 with an advantage that is not negligible, then we show that we can construct an IND-ID-CCA2 adversary $A$ who can break IND-ID-CCA2 with an advantage that is not negligible. We do this by allowing $A$ to call $B$ as an oracle.

**Proof** Let $A = (A_1, A_2)$ and $B = (B_1, B_2)$ be IND-ID-CCA2 adversary and NM-ID-CCA2 adversary respectively.

$A$ is constructed as follows:

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

Algorithm $A_2^{\mathcal{O}_2}(x_0, x_1, s', id, y^*)$
                          where $s' = (\hat{\mathcal{M}}, s)$
    $(R, \vec{y}) \leftarrow B_2^{\mathcal{O}_2}(s, y^*, id)$;
    $\vec{x} \leftarrow \mathcal{D}(param, id, \vec{y})$;
    if $R(x_0, \vec{x}) \wedge \neg R(x_1, \vec{x})$ then $d \leftarrow 0$;
      else if $\neg R(x_0, \vec{x}) \wedge R(x_1, \vec{x})$
        then $d \leftarrow 1$;
        else $d \leftarrow \{0,1\}_U$;
    return $d$
```

Focusing on our construction we observe that,

$$\begin{aligned}
&\mathbf{Adv}^{\texttt{ind-id-cca2}}_{\mathcal{IBE},A}(k)\\
&\overset{(1)}{=}\Pr[\mathbf{Exp}^{\texttt{ind-id-cca2-1}}_{\mathcal{IBE},A}(k)=1]\\
&\qquad -\Pr[\mathbf{Exp}^{\texttt{ind-id-cca2-0}}_{\mathcal{IBE},A}(k)=1]\\
&\overset{(2)}{=}\Big[p(0,1)+\frac{1}{2}\cdot\big(\ p(0,0)+p(1,1)\ \big)\Big]\\
&\qquad -\Big[p(1,0)+\frac{1}{2}\cdot\big(\ p(0,0)+p(1,1)\ \big)\Big]\\
&= p(0,1)-p(1,0)
\end{aligned}$$

**Table 3** Definitions of $p(i,j)$ for $i, j \in \{0,1\}$.

| | $R(x_0,\vec{x})$ | $R(x_1,\vec{x})$ | Probability |
|---|---|---|---|
| whether | false | false | $p(0,0)$ |
| $R(x_b,\vec{x})$ | true | false | $p(1,0)$ |
| holds | false | true | $p(0,1)$ |
| or not | true | true | $p(1,1)$ |

$$\begin{aligned}
&\mathbf{Adv}^{\texttt{nm-id-cca2}}_{\mathcal{IBE},B}(k)\\
&\overset{(3)}{=}\Pr[\mathbf{Exp}^{\texttt{nm-id-cca2-1}}_{\mathcal{IBE},B}(k)=1]\\
&\qquad -\Pr[\mathbf{Exp}^{\texttt{nm-id-cca2-0}}_{\mathcal{IBE},B}(k)=1]\\
&\overset{(4)}{=}\big(\ p(0,1)+p(1,1)\ \big)\\
&\qquad -\big(\ p(1,0)+p(1,1)\ \big)\\
&= p(0,1)-p(1,0)
\end{aligned}$$

The notations $p(i,j)$, where $i, j \in \{0,1\}$, are defined in **Table 3**. In this way we obtain equations $\overset{(2)}{=}$ and $\overset{(4)}{=}$. Equations $\overset{(1)}{=}$ and $\overset{(3)}{=}$ are according to the definitions of advantages in IND (1) and NM (3), respectively. Hence,

$$\mathbf{Adv}^{\texttt{ind-id-cca2}}_{\mathcal{IBE},A}(k)=\mathbf{Adv}^{\texttt{nm-id-cca2}}_{\mathcal{IBE},B}(k)$$

Under the assumption that $\mathbf{Adv}^{\texttt{nm-id-cca2}}_{\mathcal{IBE},B}(k)$ is not negligible, $\mathbf{Adv}^{\texttt{ind-id-cca2}}_{\mathcal{IBE},A}(k)$ is also not negligible. We reach a contradiction to the hypothesis that $\mathcal{IBE}$ is secure in the IND-ID-CCA2 sense. Thus $\mathcal{IBE}$ is also secure in the NM-ID-CCA2 sense. This concludes the proof of Theorem 4. □

**Theorem 5 (NM-ATK ⇒ IND-ATK).** *If a scheme $\mathcal{IBE}$ is secure in the sense of* NM-ATK *then $\mathcal{IBE}$ is secure in the sense of* IND-ATK*, for any attack* ATK $\in$ {ID-CPA,ID-CCA1,ID-CCA2}*.*

*Main Idea of Proof.* Towards contradiction, we prove that if a scheme is *not* secure in the IND-ATK sense, then it is *not* secure in the NM-ATK as well. We first assume that an IND-ATK adversary $B$ exists who can break IND-ATK with an advantage that is not negligible, then we show that we can construct an NM-ATK adversary $A$ who can break NM-ATK with an advantage that is not negligible. We do this by allowing $A$ to call $B$ as an oracle.

**Proof** Let $A = (A_1, A_2)$ and $B = (B_1, B_2)$ be an NM-ATK adversary and an IND-ATK adversary.

$A$ is constructed as follows:

```
Algorithm $A_1^{\mathcal{O}_1}(param)$
    $(x_0, x_1, s, id) \leftarrow B_1^{\mathcal{O}_1}(param)$;
    $\hat{\mathcal{M}} \leftarrow \{x_0, x_1\}_U$;
    $s' \leftarrow (x_0, x_1, s)$;
    return $(\hat{\mathcal{M}}, s', id)$
```

```
Algorithm $A_2^{\mathcal{O}_2}(\hat{\mathcal{M}}, s', y^*, id)$
                              where $s' = (x_0, x_1, s)$
    $d \leftarrow B_2^{\mathcal{O}_2}(x_0, x_1, s, id, y^*)$;
    $y' \leftarrow \mathcal{E}(param, id, (x_d + 1))$;
    $\vec{y} \leftarrow \{y'\}$;
    return $(R, \vec{y})$
        where $R(a, b) = 1$ iff $a + 1 = b$
```

In $A_1$ the notation $\hat{\mathcal{M}} \leftarrow \{x_0, x_1\}_U$ denotes that $\hat{\mathcal{M}}$ is being assigned the probability space that assigns to each of $x_0$ and $x_1$ a probability of 1/2.

Inspecting either $x_0$ or $x_1$ was randomly chosen with a probability of 1/2, and recalling the definitions of advantages in $\mathsf{IND}$ (1) and $\mathsf{NM}$ (3), we obtain

$$\Pr[b = 0] = \Pr[b = 1] = \frac{1}{2} \qquad (10)$$

$$\Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-b}}(k) = 0] + \Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-b}}(k) = 1] = 1 \qquad (11)$$

for $b \in \{0, 1\}$. Furthermore, focusing on our construction, we obtain

$$\begin{aligned}\Pr[\mathbf{Exp}_{\mathcal{IBE},A}^{\texttt{nm-atk-1}}(k) = 1] &= \Pr[b{=}0] \cdot \Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-0}}(k) = 0] \\ &\quad + \Pr[b{=}1] \cdot \Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-1}}(k){=}1] \qquad (12)\end{aligned}$$

$$\begin{aligned}\Pr[\mathbf{Exp}_{\mathcal{IBE},A}^{\texttt{nm-atk-0}}(k){=}1] &= \Pr[b{=}0] \cdot \Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-0}}(k){=}1] \\ &\quad + \Pr[b{=}1] \cdot \Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-1}}(k){=}0] \qquad (13)\end{aligned}$$

The event $b = i$, where $i \in \{0, 1\}$, denotes that the challenger chose $x_b$, encrypted $x_b$ and sent the corresponding ciphertext $y^*$ as a challenge to the $\mathsf{NM\text{-}ATK}$ adversary $A$. Hence,

$$\begin{aligned}&\mathbf{Adv}_{\mathcal{IBE},A}^{\texttt{nm-atk}}(k) \\ &\overset{\textcircled{1}}{=} \Pr[\mathbf{Exp}_{\mathcal{IBE},A}^{\texttt{nm-atk-1}}(k) = 1] - \Pr[\mathbf{Exp}_{\mathcal{IBE},A}^{\texttt{nm-atk-0}}(k) = 1] \\ &\overset{\textcircled{2}}{=} \frac{1}{2} \cdot \Big\{ (\Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-0}}(k) = 0] + \Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-1}}(k) = 1]) \\ &\qquad - (\Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-0}}(k) = 1] + \Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-1}}(k) = 0]) \Big\} \\ &\overset{\textcircled{3}}{=} \Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-1}}(k) = 1] - \Pr[\mathbf{Exp}_{\mathcal{IBE},B}^{\texttt{ind-atk-0}}(k) = 1] \\ &\overset{\textcircled{4}}{=} \mathbf{Adv}_{\mathcal{IBE},B}^{\texttt{ind-atk}}(k)\end{aligned}$$

Equations $\overset{\textcircled{1}}{=}$ and $\overset{\textcircled{4}}{=}$ hold according to the definitions of advantages in $\mathsf{NM}$ (3) and $\mathsf{IND}$ (1), respectively. Equation $\overset{\textcircled{2}}{=}$ holds according to Eqs. (10) (12) (13). Equation $\overset{\textcircled{3}}{=}$ holds according to Eq. (11).

Under the assumption that $\mathbf{Adv}_{\mathcal{IBE},B}^{\texttt{ind-atk}}(k)$ is not negligible, $\mathbf{Adv}_{\mathcal{IBE},A}^{\texttt{nm-atk}}(k)$ is also not negligible. We reach a contradiction to the hypothesis that $\mathcal{IBE}$ is secure in the $\mathsf{NM\text{-}ATK}$ sense. Thus $\mathcal{IBE}$ is also secure in the $\mathsf{IND\text{-}ATK}$ sense. This concludes the proof of Theorem 5. □

## References

1) Attrapadung, N., Cui, Y., Galindo, D., Hanaoka, G., Hasuo, I., Imai, H., Matsuura, K., Yang, P. and Zhang, R.: Relations Among Notions of Security for Identity Based Encryption Schemes, *Latin American Theoretical Informatics* (*LATIN '06*), LNCS, Vol.3887, Springer, pp.130–141 (2006).

2) Attrapadung, N., Cui, Y., Hanaoka, G., Imai, H., Matsuura, K., Yang, P. and Zhang, R.: Relations Among Notions of Security for Identity Based Encryption Schemes, Cryptology ePrint Archive, Report 2005/258 (2005). http://eprint.iacr.org/2005/258

3) Bellare, M., Desai, A., Pointcheval, D. and Rogaway, P.: Relations among notions of security for public-key encryption schemes, *Proc. CRYPTO '98*, LNCS, Vol.1462, pp.26–45, Springer (1998).

4) Boneh, D. and Boyen, X.: Chosen-ciphertext security from identity-based encryption, *Proc. EUROCRYPT '98*, LNCS, Vol.3027, pp.223–238, Springer (2004).

5) Boneh, D. and Boyen, X.: Secure identity based encryption without random oracles, *Proc. CRYPTO '04*, LNCS, Vol.3152, pp.443–459, Springer (2004).

6) Boneh, D., Boyen, X. and Goh, E.: Hierarchical identity based encryption with constant size ciphertext, *Proc. EUROCRYPT '05*, LNCS, Vol.3494, pp.440–456, Springer (2005).

7) Boneh, D. and Franklin, M.: Identity-based encryption from the Weil pairing, *Proc. CRYPTO '01*, LNCS, Vol.2139, pp.213–229, Springer (2001).

8) Canetti, R., Halevi, S. and Katz, J.: A forward-secure public-key encryption scheme, *Proc. EUROCRYPT '03*, LNCS, Vol.2656, pp.255–271, Springer (2003).

9) Dolev, D., Dwork, C. and Naor, M.: Non-malleable cryptography (Extended Abstract), *Proc. STOC '91*, pp.542–552 (1991).

10) Galindo, D. and Hasuo, I.: Security Notions for Identity Based Encryption, Cryptol-

ogy ePrint Archive, Report 2005/253 (2005). http://eprint.iacr.org/2005/253

11) Goldreich, O.: *Foundations of cryptography, Volumn II Basic Applications*, Cambridge University Press (2003).

12) Goldreich, O., Lustig, Y. and Naor, M.: On chosen ciphertext security of multiple encryptions, Cryptology ePrint Archive, Report 2002/89 (2002). http://eprint.iacr.org/

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

14) Rackoff, C. and Simon, D.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack, *Proc. of CRYPTO '91*, LNCS, Vol.576, pp.433–444, Springer (1991).

15) Shamir, A.: Identity-based cryptosystems and signature schemes, *Proc. CRYPTO '84*, LNCS, Vol.196, pp.47–53, Springer (1985).

16) Watanabe, Y., Shikata, J. and Imai, H.: Equivalence between semantic security and indistinguishability against chosen ciphertext attacks, *Public Key Cryptography – PKC '03*, LNCS, Vol.2567, pp.71–84, Springer (2003).

17) Waters, B.: Efficient identity-based encryption without random oracles, *Proc. EUROCRYPT '05*, LNCS, Vol.3494, pp.114–127, Springer (2005).

## Appendix

### A.1 CPA, CCA1, CCA2 Attack Models

Under CPA the adversary can obtain ciphertexts of plaintexts of her choice. In public key cryptographic schemes, this attack is unavoidable because the adversary always gets access to the encryption function, a.k.a., the encryption oracle. Under CCA1, in addition to the public key, the adversary is granted access to an oracle for the decryption function, a.k.a., the decryption oracle. The adversary may use this decryption function only for the period of time before she is given the challenge ciphertext $y^*$. (This non-adaptive attack is also called a "lunchtime attack".) Under CCA2, in addition to the public key, the adversary again gets access to the decryption oracle, but this time she is permitted to use this decryption oracle even on ciphertexts that are chosen after the challenge ciphertext $y^*$ is issued. The only restriction is that the adversary may not ask for the decryption of $y^*$.

### A.2 Particular Attack Models in $\mathcal{IBE}$

In the $\mathcal{IBE}$ environment, the adversary could be granted more power than the adaptive chosen ciphertext attack, which has been thoroughly considered in $\mathcal{PKE}$. The adversary is allowed to attack an arbitrary public key $id^*$ of her choice. Thus, in addition to the adaptive chosen ciphertext attack on $id^*$, the adversary could obtain the private keys for any public key of her choice, other than the private key for $id^*$. She can do this by performing a series of extraction queries to a private key generator. The adversary should still have a negligible advantage in breaking the scheme, even with such power.

In this section, we describe two different secure levels of *indistinguishability* for identity based encryption schemes. They are adaptive chosen ciphertext security against adaptive chosen identity attack (IND-ID-CCA2)[7] and adaptive chosen ciphertext security against selective identity attack (IND-sID-CCA2)[8].

#### A.2.1 Adaptive Chosen ID Security

To achieve adaptive chosen identity security, the scheme should remain secure under adaptive chosen identity attacks. The reason is that when an adversary attacks a public key $id^*$ in $\mathcal{IBE}$, she might already possess the series of private keys of other public keys $id_1, id_2, \ldots id_n$. In this situation, we must formalize such power into the definition of conventional chosen ciphertext security, which is defined for $\mathcal{PKE}$. Such queries are called private key extraction queries. We say an identity based encryption scheme $\mathcal{IBE}$ is full-ID secure (IND-ID-CCA2) against adaptive chosen identity attack and adaptive chosen ciphertext attack if no polynomial adversary $A$ has a non-negligible advantage to break the scheme in the following IND-ID-CCA2 game:

**Setup**: The challenger takes a security parameter $k$ and runs the Setup algorithm. It gives the adversary the resulting system parameters *param*. It keeps the master-key $mk$ to itself as secret.

**Phase 1**: The adversary issues queries $q_1, \ldots q_m$ where query $q_i$ is one of

- Extraction query $< id_i >$. The challenger responds by running the Extract algorithm to generate the private key $sk_i$ corresponding to the public key $id_i$. It sends $sk_i$ to the adversary.
- Decryption query $< id_i, y_i >$. The challenger responds by running the Extract algorithm to generate the private key $sk_i$ corresponding to $id_i$. It then runs the Decrypt algorithm to decrypt the ciphertext $y_i$ using the private key $sk_i$. It sends the resulting plaintext $x_i$ to the adversary.

These queries may be asked adaptively; that is, each query $q_i$ may depend on the replies to $q_1, \dots q_{i-1}$.

**Challenge**: Once the adversary decides that Phase 1 is over, it outputs two equal-length plaintexts $x_0, x_1 \in \mathcal{M}$ and an identity $id^*$ with which it wishes to be challenged. The only constraint is that $id^*$ did not appear in any private key extraction query in Phase 1. The challenger picks a random bit $b^* \in \{0,1\}$ and sets $y^* = \mathcal{E}(param, id^*, x_{b^*})$. It sends $y^*$ as the challenge to the adversary.

**Phase 2**: The adversary issues more queries $q_{m+1}$ where query $q_i$ is one of

- Extraction query $< id_i >$, where $id_i \neq id^*$. The challenger responds as in Phase 1.
- Decryption query $< id_i, y_i >$, where $(id_i, y_i) \neq (id^*, y^*)$. The challenger responds as in Phase 1.

These queries may be asked adaptively as in Phase 1.

**Guess**: Finally, the adversary outputs a guess $b' \in \{0,1\}$ and wins the game if $b' = b^*$.

An adversary such as $A$ is referred to as an IND-ID-CCA2 adversary. We say $A$ breaks the scheme in the sense of IND-ID-CCA2 if she can distinguish which plaintext was encrypted with a probability significantly more than that of a random guess.

### A.2.2 Selective Chosen ID Security

Besides the adaptive identity attack model, a weaker definition of security was introduced by Canetti, Halevi and Katz [8]. Here, the identity for which the challenge ciphertext is encrypted is *selected* by the adversary in advance (say, "selectively") before the public key is generated. We say that an identity based encryption scheme $\mathcal{IBE}$ is *selectively* semantically secure against an adaptive chosen ciphertext attack (IND-sID-CCA2) if no polynomially bounded adversary $A$ has a non-negligible advantage against the challenger in the following IND-sID-CCA2 game:

**Select**: The adversary $A$ selects a target identity $id^* \in \{0,1\}^*$.

**Setup**: The challenger takes $k$ and runs the Setup algorithm. It gives the adversary $param$ and keeps $mk$ to itself.

**Phase 1**: The adversary issues queries $q_1, \dots q_m$, where query $q_i$ is one of

- Extraction query $< id_i >$, where $id_i \neq id^*$. The challenger responds by running the Extract algorithm to generate the private key $sk_i$ corresponding to the public key $id_i$. It sends $sk_i$ to the adversary.
- Decryption query $< id_i, y_i >$, where $(id_i, y_i) \neq (id^*, y^*)$. The challenger responds by running the Extract algorithm to generate the private key $sk_i$ corresponding to $id_i$. It then runs the Decrypt algorithm to decrypt the ciphertext $y_i$ using the private key $sk_i$. It sends the resulting plaintext $x_i$ to the adversary.

These queries may be asked adaptively; that is, each query $q_i$ may depend on the replies to $q_1, \dots q_{i-1}$.

**Challenge**: Once the adversary decides that Phase 1 is over it outputs two equal-length plaintexts $x_0, x_1 \in \mathcal{M}$. The challenger picks a random bit $b^* \in \{0,1\}$ and sets $y^* = \mathcal{E}(param, id^*, x_{b^*})$. It sends $y^*$ as the challenge to the adversary.

**Phase 2**: The adversary issues more queries $q_{m+1}$, where query $q_i$ is one of:

- Extraction query $< id_i >$, where $id_i \neq id^*$. The challenger responds as in Phase 1.
- Decryption query $< id_i, y_i >$, where $(id_i, y_i) \neq (id^*, y^*)$. The challenger responds as in Phase 1.

These queries may be asked adaptively as in Phase 1.

**Guess**: Finally, the adversary outputs a guess $b' \in \{0,1\}$ and wins the game if $b' = b^*$.

An adversary such as $A$ is referred to as an IND-sID-CCA2 adversary. We say $A$ breaks the scheme in the sense of IND-sID-CCA2 if she can distinguish which plaintext was encrypted with a probability significantly more than random guess.

(Received November 28, 2005)
(Accepted June 1, 2006)

(Online version of this article can be found in the IPSJ Digital Courier, Vol.2, pp.465–477.)

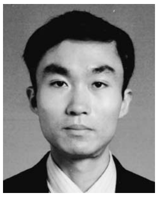
**Peng Yang** was born in the city of Shenyang, China in 1981. He received his B.E. degree in computer science in 2003 from Beihang University (a.k.a., Beijing University of Aeronautics and Astronautics, or BUAA for short). As a student, he was awarded the Heshi Study Scholarship, Outstanding Freshman Scholarship and People Scholarship in 1998, 1999 and 2000. In 2002, he was certified by Microsoft as MCP, MCDBA, MCSE and MCSA. He is currently a grantee of the Japanese Government (Monbukagakusho) Scholarship. His research interests include information security, cryptography theory, E-government and E-business.

**Goichiro Hanaoka** received his B.E. degree in electronic engineering from the University of Tokyo in 1997 and received his M.E. and Ph.D. degrees in information and communication engineering from the University of Tokyo in 1999 and 2002, respectively. From 2002 to 2005 he was a Research Fellow of Japan Society for the Promotion of Science (JSPS). Since 2005 he has been with the National Institute of Advanced Industrial Science and Technology, Japan.

**Yang Cui** received the B.E. degree in electronic and communication engineering from Harbin Institute of Technology, P.R. China in 2000 and the M.E. degree in information science and technology from the University of Tokyo, Japan in 2004. He is currently a Ph.D. student in the Department of Information and Communication Engineering, the University of Tokyo. His research interests include cryptography and information security.

**Rui Zhang** received his B.E. degree in electronic engineering from Tsinghua University in 1999 and received his M.E. and Ph.D. degrees in information and communication engineering from the School of Information Science and Technology, the University of Tokyo in 2002 and 2005. From 2005 to 2006, he was a Research Fellow of the Japan Society for the Promotion of Science (JSPS). Since 2006, he has been with the National Institute of Advanced Industrial Science and Technology, Japan.

**Nuttapong Attrapadung** received his B.E. degree in electrical engineering from Chulalongkorn University in Thailand in 2001 and received his M.E. degree in information and communication engineering from the University of Tokyo in 2004. Currently, he is pursuing the Ph.D. degree at the same place and expected to graduate in 2007.



**Kanta Matsuura** was born in Osaka, Japan, in 1969. He received the B.E. degree in electrical engineering in 1992, the M.E. degree in electronics in 1994, and the Ph.D. degree in electronics in 1997, all from the University of Tokyo, Japan. He is currently an associate professor of the Institute of Industrial Science at the University of Tokyo. His research interests include network and system security, applied cryptography, and risk management. He is a member of IEEE, ACM, IACR, IEICE, and IPSJ.

**Hideki Imai** received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Tokyo in 1966, 1968, and 1971, and Honor Doctor Degree from Soonchunhyang University, Korea in 1999. From 1992 to 2006 he was a professor at the IIS, the University of Tokyo. Currently he is a professor of Chuo University and is also the director of the Research Center for Information Security, National Institute of Advanced Industrial Science and Technology. He is the chair of CRYPTREC and a Junior Past President of IEEE Information Theory Society. He is a member of the Science Council of Japan and a fellow of IEEE and IEICE.