Relations Among Notions of Security for Identity Based Encryption Schemes

Nuttapong Attrapadung[1], Yang Cui[1], Goichiro Hanaoka[2], Hideki Imai[1], Kanta Matsuura[1], Peng Yang[1], and Rui Zhang[1]

[1] Institute of Industrial Science, University of Tokyo.
{nuts,cuiyang,zhang}@imailab.iis.u-tokyo.ac.jp
{imai,kanta,pengyang}@iis.u-tokyo.ac.jp
[2] Research Center for Information Security,
National Institute of Advanced Industrial Science and Technology.
hanaoka-goichiro@aist.go.jp

Abstract. Identity based encryption ($\mathcal{IBE}$) schemes have been flourishing since the very beginning of this century. In $\mathcal{IBE}$ it is widely believed that proving the security of a scheme in the sense of IND-ID-CCA2 is sufficient to claim 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). But these relations are proved *only* for conventional public key encryption ($\mathcal{PKE}$) schemes in historical works. The fact is that between $\mathcal{IBE}$ and $\mathcal{PKE}$, there exists a difference of special importance, i.e. only in $\mathcal{IBE}$ the adversaries can perform a particular attack, namely the *chosen identity attack*.
This paper shows 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 the security notion, IND-ID-CCA2, captures the essence of security for all $\mathcal{IBE}$ schemes. To achieve this intention, we first describe formal definitions of the notions of security for $\mathcal{IBE}$, and then present the relations among IND, SS and NM in $\mathcal{IBE}$, along with rigorous proofs. All of these results are proposed with the consideration of the chosen identity attack.

Key words: notions of security, identity based encryption schemes, equivalences, implications, chosen identity attacks.

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 yields the avoidance of 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 to encrypt emails with the recipient's email address.

Although the basic concept of $\mathcal{IBE}$ was proposed by Shamir [14] about two decades ago, it is only very recent that the first fully functional scheme was proposed [5]. 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 which captures the essence of security for $\mathcal{IBE}$ [2–5, 13, 16]. However, such an issue has not been investigated rigorously, *yet*. This work aims to establish such an affirmative justification. Before discussing about how to define the "right" security notion for $\mathcal{IBE}$, we first glance back to the case of $\mathcal{PKE}$.

NOTIONS OF SECURITY FOR $\mathcal{PKE}$. A convenient way to formalize notions of security for cryptographic schemes is considering combinations of the 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) [11], and *non-malleability* (NM) [7], i.e. $\mathsf{G}_i \in \{\mathsf{IND},\mathsf{SS},\mathsf{NM}\}$. The attack models are *chosen plaintext attack* (CPA) [11], *non-adaptive chosen ciphertext attack* (CCA1) [7] and *adaptive chosen ciphertext attack* (CCA2) [12], i.e. $\mathsf{A}_j \in \{\mathsf{CPA},\mathsf{CCA1},\mathsf{CCA2}\}$. [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 the ciphertext. The equivalence between SS-CPA and IND-CPA has been given [11]; and the equivalences between SS-CCA1,2 and IND-CCA1,2 are given only recently [10,15]. On the other hand, NM formalizes an adversary's inability, given a challenge ciphertext y^*, to output a different ciphertext y' in such a way that the plaintexts x, x', underlying these two ciphertexts, are meaningfully related, e.g. $x' = x + 1$. The implications from IND-CCA2 to NM under any attack have been proved [1]. For these reasons, along with the convenience of proving security in sense of IND, in almost all concrete schemes, IND-CCA2 is considered to be the "right" standard security notion for $\mathcal{PKE}$.

TOWARDS DEFINING NOTIONS OF SECURITY FOR $\mathcal{IBE}$. Due to the particular mechanism, the adversaries are granted more power in $\mathcal{IBE}$ than in $\mathcal{PKE}$. Essentially, the adversaries can access to the *key extraction oracle*, which answers the private key of any queried public key (identity). Including this particular *adaptive chosen identity attack*, [2] we formalize the security notions for $\mathcal{IBE}$, e.g. IND-ID-CCA2, in such a way: G_i-ID-A_j, where $\mathsf{G}_i \in \{\mathsf{IND},\mathsf{SS},\mathsf{NM}\}$, ID denotes the particular attack mentioned above, and $\mathsf{A}_j \in \{\mathsf{CPA},\mathsf{CCA1},\mathsf{CCA2}\}$. Boneh and Franklin are the first to define the security notion for $\mathcal{IBE}$, by naturally extending IND-CCA2 to IND-ID-CCA2.

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

At the first place the intuition tells us that task (i) seems to be simply achievable by considering the analogy to the case of shifting IND-CCA to IND-ID-CCA as done in [5], and task (ii) could immediately follow from the relations among the notions as the case of $\mathcal{PKE}$, since we shift all the notions with the same additional attack power (namely, the accessability to key extraction oracle). However, we emphasize that it will not follow simply and immediately until rigorous definitions for task (i) and rigorous proofs for task (ii) are presented.

We managed to accomplish both tasks in this paper. This kind of result can be considered as having the same flavor as some historical results, to name just one, the equivalence between IND-CCA2 and SS-CCA2 for $\mathcal{PKE}$. There, although IND-CPA and SS-CPA were defined and proved equivalent in the year 1984 [11], the equivalence between IND-CCA2 and SS-CCA2 had not been proved rigorously until the year 2003 [15]. During this long period of time, people just simply believed that shifting the attack power from CPA to CCA2 will not affect the equivalence.

[1] We give the details of these attack models in Appendix A.

[2] Actually in $\mathcal{IBE}$ there exists the other attack against identity, named *selective chosen identity attack*. In this paper we omit presenting the formal definitions of the security notions in this selective-ID secure sense because these notions are too weak. More details about selective chosen identity attack are given in Appendix B.

$$
\begin{tikzcd}
\textsf{NM-ID-CPA} \arrow[d, "1"'] & \textsf{NM-ID-CCA1} \arrow[l, dotted] \arrow[d, "1"'] & \textsf{NM-ID-CCA2} \arrow[l, dotted] \arrow[d, shift right, "1"'] \\
\textsf{IND-ID-CPA} \arrow[d, shift right, "4"'] & \textsf{IND-ID-CCA1} \arrow[l, dotted] \arrow[d, shift right, "4"'] & \textsf{IND-ID-CCA2} \arrow[l, dotted] \arrow[u, shift right, "2"'] \arrow[d, shift right, "4"'] \\
\textsf{SS-ID-CPA} \arrow[u, shift right, "5"'] & \textsf{SS-ID-CCA1} \arrow[l, dotted] \arrow[u, shift right, "5"'] & \textsf{SS-ID-CCA2} \arrow[l, dotted] \arrow[u, shift right, "5"']
\end{tikzcd}
$$

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

1.2 Our Contributions

Our contributions are twofold. First, we formally presented the definitions of the notions of security for $\mathcal{IBE}$ schemes. The overall definitions are built upon historical works [1, 5, 10].

Second, we rigorously proved the relations among these notions and achieved our conclusion that, IND-ID-CCA2 is the "right" notion of security for $\mathcal{IBE}$. It turns out that our intuition about those relations were right: the implication G_1-ID-$\mathsf{A}_1 \Rightarrow \mathsf{G}_2$-ID-$\mathsf{A}_2$ will hold in $\mathcal{IBE}$ if and only if G_1-$\mathsf{A}_1 \Rightarrow \mathsf{G}_2$-$\mathsf{A}_2$ holds in $\mathcal{PKE}$, where the corresponding security goals G_i and attack models A_j are mentioned above.

The results of our second contribution is illustrated in Figure 1. The vertical *line arrows* represent implications which are explicitly proven, and the horizontal *dots arrows* represent s implication which are self-evident. No matter in which case, 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 number beside an arrow denotes that in which theorem or lemma this implication is proved.

Related Work. Independently of our work, Galindo and Hasuo have shown similar results in their manuscript [8]. The relation between these works is that, they have not publicly announced their result yet by the time when this version of our draft is finished, while a previous version of this work has been publicly announced in Technical Report of IEICE [17].

1.3 Organization

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

2 Preliminary

In this section, we review the model of $\mathcal{IBE}$ and 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 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 triple inputs as $param, mk$, and an arbitrary $id \in \{0,1\}^*$, and outputs a private key $sk = \mathcal{E}(param, mk, id)$. Here id is arbitrary and will be used as the public encryption key. 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 triple inputs as *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 triple inputs as *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 and only if *sk* is the private key generated by the extract algorithm with the given *id* as the public key, then,

$$\forall x \in \mathcal{M} : \mathcal{D}(param, sk, y) = x, \text{ where } y = \mathcal{E}(param, id, x)$$

2.2 Conventions

Notations. $\vec{\boldsymbol{x}} \leftarrow \mathcal{D}(param, sk, \vec{\boldsymbol{y}})$ denotes that the vector $\vec{\boldsymbol{x}}$ is made up of the plaintexts corresponding to every ciphertext in the vector $\vec{\boldsymbol{y}}$. $\hat{\mathcal{M}}$ 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. Function $h : \hat{\mathcal{M}} \rightarrow \{0,1\}^*$ denotes the a-priori partial information about the plaintext and function $f : \hat{\mathcal{M}} \rightarrow \{0,1\}^*$ denotes the a-posteriori partial information.

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

***R*-related Relation.** We consider R-related relation of arity t where t will be polynomial in the security parameter k. Rather than writing $R(x_1, x_2, \ldots, x_t)$ we write $R(x, \vec{\boldsymbol{x}})$, denoting the first argument is special and the rest are bunched into a vector $\vec{\boldsymbol{x}}$ where $\mid \vec{\boldsymbol{x}} \mid = t-1$, and for every $x_i \in \vec{\boldsymbol{x}}$, $R(x, x_i)$ 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 at random and uniformly from S. And sometimes we use $x \stackrel{R}{\leftarrow} S$ in order to stress this randomness. If α 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, and we say A is polynomial time if both probabilistic algorithm A_1 and probabilistic algorithm A_2 are polynomial time. At the first stage, given the system parameters, the adversary computes and outputs a challenge template τ. A_1 can output some state information s which will be transferred to A_2. At the second stage the adversary is issued a challenge ciphertext y^* generated from τ by a probabilistic function, in a manner depending on the goal. We say the adversary A successfully breaks the scheme if she achieves her goal.

We consider three security goals, IND, SS and NM. And we consider three attack models, ID-CPA,ID-CCA1,ID-CCA2, in order of increasing strength. The difference among the models is whether or not A_1 or A_2 is granted accesses to decryption oracles. [3]

We describe in Table 1 and 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* $\mathcal{D}(param, sk, \cdot)$.

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 $\mathcal{DO}_i$ is a function that returns a empty string ε on any input.

[3] Inspecting the similarity between adaptive chosen identity attack and selective chosen identity attack, we only discuss in details the former case (full-ID security), while the results can be extended to the latter case (selective-ID security), since 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.

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	$\{\mathcal{X}(param, mk, \cdot), \mathcal{E}(param, id, \cdot), \mathcal{D}(param, sk, \cdot)\}$

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

3.1 Indistinguishability

This significant notion of security for $\mathcal{IBE}$ is described by Boneh and Franklin [5] with a distinguishing game. Here we define indistinguishability through a two-stage experiment. A_1 is run on the system parameters $param$ as input. At the end of A_1's execution she 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 $param$) which she wants to preserve, and id is the public key which she wants to attack. One of x_0 and x_1 is *randomly* selected, say x_b, beyond adversary's view. A challenge y^* is computed by encrypting x_b with the public key id. A_2 tries to distinguish 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,

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

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

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

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 [11] and later refined by Goldreich [9]. It captures the security requirement such that intercepting the ciphertext gives an adversary no useful 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 τ. A_2 receives an encryption y^* of a random message 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 more than any *simulator* does. The simulator tries to do as well as the adversary without knowing the challenge ciphertext y^* nor accessing to 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 $\mathtt{atk} \in \{\mathtt{id\text{-}cpa}, \mathtt{id\text{-}cca1}, \mathtt{id\text{-}cca2}\}$ and $k \in \mathbb{N}$ let,

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

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

Experiment $\mathbf{Exp}^{\mathtt{ss\text{-}atk}}_{\mathcal{IBE},A}(k)$	Experiment $\mathbf{Exp}^{\mathtt{ss\text{-}atk}}_{\mathcal{IBE},A'}(k)$
$(param, mk) \leftarrow \mathcal{S}(k)$;	$(\hat{\mathcal{M}}, h, f, s, id) \leftarrow A'_1(k)$;
$(\hat{\mathcal{M}}, h, f, s, id) \leftarrow A_1^{\mathcal{O}_1}(param)$;	$x^* \xleftarrow{R} \hat{\mathcal{M}}$;
$x^* \xleftarrow{R} \hat{\mathcal{M}}$;	$v \leftarrow A'_2(s, \lvert x^* \rvert, h(x^*), id)$;
$y^* \leftarrow \mathcal{E}(param, id, x^*)$;	`if` $v = f(x^*)$
$v \leftarrow A_2^{\mathcal{O}_2}(s, y^*, h(x^*), id)$;	`then` $d \leftarrow 1$ `else` $d \leftarrow 0$;
`if` $v = f(x^*)$	`return` d
`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 there exists a simulator such that $\mathbf{Adv}^{\mathtt{ss\text{-}atk}}_{\mathcal{IBE},A}(k)$ is negligible .

We comment here that it is necessary to require in both cases τ is distributed identically, since both A and A' generate target public key id by themselves, i.e. τ is output by A and A' themselves.

3.3 Non-malleability

Non-malleability is introduced by Dolev et al. [7]. 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 $\vec{\boldsymbol{y}}$ of ciphertexts. We insist that $y \notin \vec{\boldsymbol{y}}$. [4] The adversary hopes that $R(x_1, \vec{\boldsymbol{x}})$ holds. We say she is successful if, she can do this with a probability significantly more than that, with which $R(x_0, \vec{\boldsymbol{x}})$ 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 $\mathtt{atk} \in \{\mathtt{id\text{-}cpa}, \mathtt{id\text{-}cca1}, \mathtt{id\text{-}cca2}\}$ and $k \in \mathbb{N}$ let,

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

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

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

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

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 relatoin (equivalence) between IND-ATK and SS-ATK into $\mathcal{IBE}$ environment, and then extend the relation between IND-ATK and NM-ATK into $\mathcal{IBE}$ environment. It relies on these relations that the researches on identity based encryption schemes are blossoming over past several years, thus we say these relations are significantly important.

4.1 Equivalence between IND and SS

Theorem 1 (IND-ATK $\Leftrightarrow$ 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* SS-ATK*, for any attack* ATK $\in$ {ID-CPA,ID-CCA1,ID-CCA2}.

We prove this theorem by proving two directions respectively, i.e. IND-ATK implies SS-ATK and 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. According to the definition of SS, in order to prove 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 SS-ATK game. In order 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 $\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},B,B'}(k)$ is equal to $\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},A}(k)$. Since the scheme is secure in the IND-ATK sense, no matter which B is accessed as 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 the scheme is secure in the SS-ATK sense. The point is how we prove 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 adversary B and adversary A have access to an oracle set $\mathcal{O}_1$ at their first stage and an oracle set $\mathcal{O}_2$ at their second stage, while simulator B' have 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:

$$
\begin{array}{l|l}
\texttt{Algorithm } B'_1(k) & \texttt{Algorithm } B'_2(s, |x^*|, h(x^*), id) \\
\quad (param, mk) \leftarrow \mathcal{S}(k); & \quad x' \xleftarrow{R} \hat{\mathcal{M}} \text{ where } |x'| = |x^*|; \\
\quad (\hat{\mathcal{M}}, h, f, s, id) \leftarrow B_1^{\mathcal{O}_1}(param); & \quad y' \leftarrow \mathcal{E}(param, id, x'); \\
\quad \texttt{return } (\hat{\mathcal{M}}, h, f, s, id) & \quad v \leftarrow B_2^{\mathcal{O}_2}(s, y', h(x^*), id); \\
 & \quad \texttt{return } v
\end{array}
$$

The point that must be emphasized is, since the challenge template $\tau = (\hat{\mathcal{M}}, h, f)$ is chosen by B and B' themselves, τ is distributed identically in both 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 orale, 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 as well.

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

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

Note 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 a-posteriori partial information $f(x_1)$ of x_1. So we say in this situation, the encryption y^* is also *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, it is obvious that, this experiment outputs 1 only when B captures a-posteriori partial information from this *useful* (not *dummy* any more) encryption, i.e. at the end of B's second stage B outputs v and $v = f(x_1)$. Hence,

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

We obtain

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

The equations $\overset{(1)}{=}$ and $\overset{(3)}{=}$ are according to the definitions of advantages in IND (1) and SS (2), respectively. And the equation $\overset{(2)}{=}$ holds according to Eq. (4) (5).

Since $\mathcal{IBE}$ 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. 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. We first assume there exists an IND-ATK adversary B who can successfully break IND-ATK with non-negligible advantage, then we show that we can construct an SS-ATK adversary A who can successfully break SS-ATK with non-negligible advantage, i.e. there does not exist any SS-ATK simulator who 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:

$$\begin{array}{l|l}
\texttt{Algorithm } A_1^{\mathcal{O}_1}(param) & \texttt{Algorithm } A_2^{\mathcal{O}_2}(s, y^*, h(x_1), id) \\
\quad (x_0, x_1, s, id) \leftarrow B_1^{\mathcal{O}_1}(param); & \quad d' \leftarrow B_2^{\mathcal{O}_2}(x_0, x_1, s, y^*, id); \\
\quad \hat{\mathcal{M}} \leftarrow \{x_0, x_1\}_U; & \quad v \leftarrow d'; \\
\quad \text{choose } f \text{ satisfies } f(x_0) = 0 \text{ and } f(x_1) = 1; & \quad \texttt{return } v \\
\quad \text{choose } h \text{ satisfies } h(x_0) = h(x_1) \ ; & \\
\quad \texttt{return } (\hat{\mathcal{M}}, h, f, s, id) &
\end{array}$$

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

$$\Pr[b = 0] = \Pr[b = 1] = \frac{1}{2} \tag{6}$$

$$\Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},B}(k) = 0] = \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k) = 1] \tag{7}$$

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

$$\begin{aligned}
\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},B}(k) &= \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k) = 1] - \Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},B}(k) = 1] \\
&= 2 \cdot \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k) = 1] - 1
\end{aligned} \tag{8}$$

Furthermore, focusing on our construction, we obtain

$$\begin{aligned}
\Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A}(k) = 1] &= \Pr[b = 0] \cdot \Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},B}(k) = 0] \\
&\quad + \Pr[b = 1] \cdot \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k) = 1] \\
&\overset{(1)}{=} \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k) = 1] \\
&\overset{(2)}{=} \frac{1}{2} + \frac{1}{2} \cdot \mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},B}(k)
\end{aligned} \tag{9}$$

Here the equation $\overset{(1)}{=}$ holds according to Eq. (6) (7). The equation $\overset{(2)}{=}$ holds according to Eq. (8).

On the other hand, recall the definition of SS-ATK (on Page 6). Since the challenge template τ should be distributed identically in both cases, we observe that at 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 at random and uniformly in $\{0, 1\}$. Hence for any simulator,

$$\Pr[\mathbf{Exp}^{\texttt{ss-atk}}_{\mathcal{IBE},A'}(k) = 1] \leq \frac{1}{2} \tag{10}$$

This means that A' cannot be successful at a probability more than $1/2$. In this inequation 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. (9) and inequality (10), we obtain

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

We have assumed that $\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},B}(k)$ is non-negligible, thus $\mathbf{Adv}^{\texttt{ss-atk}}_{\mathcal{IBE},A,A'}(k)$ is also non-negligible. We reach 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.

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

	$R(x_0, \overrightarrow{\boldsymbol{x}})$	$R(x_1, \overrightarrow{\boldsymbol{x}})$	Probability
whether	*false*	*false*	$p(0,0)$
$R(x_b, \overrightarrow{\boldsymbol{x}})$	*true*	*false*	$p(1,0)$
holds	*false*	*true*	$p(0,1)$
or not	*true*	*true*	$p(1,1)$

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 as well. We first assume there exists an NM-ID-CCA2 adversary B who can successfully break NM-ID-CCA2 with non-negligible advantage, then we show that we can construct an IND-ID-CCA2 adversary A who can successfully break IND-ID-CCA2 with non-negligible advantage. 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 $A_1^{\mathcal{O}_1}(param)$	Algorithm $A_2^{\mathcal{O}_2}(x_0, x_1, s', id, y^*)$
$(\hat{\mathcal{M}}, s, id) \leftarrow B_1^{\mathcal{O}_1}(param)$;	where $s' = (\hat{\mathcal{M}}, s)$
$x_0 \leftarrow \hat{\mathcal{M}}; x_1 \leftarrow \hat{\mathcal{M}}$;	$(R, \overrightarrow{\boldsymbol{y}}) \leftarrow B_2^{\mathcal{O}_2}(s, y^*, id)$;
$s' \leftarrow (\hat{\mathcal{M}}, s)$;	$\overrightarrow{\boldsymbol{x}} \leftarrow \mathcal{D}(param, id, \overrightarrow{\boldsymbol{y}})$;
return (x_0, x_1, s', id)	**if** $R(x_0, \overrightarrow{\boldsymbol{x}}) \wedge \neg R(x_1, \overrightarrow{\boldsymbol{x}})$ **then** $d \leftarrow 0$;
	else if $\neg R(x_0, \overrightarrow{\boldsymbol{x}}) \wedge R(x_1, \overrightarrow{\boldsymbol{x}})$ **then** $d \leftarrow 1$;
	else $d \overset{R}{\leftarrow} \{0, 1\}_U$;
	return d

Focusing on our construction we observe,

$$\begin{aligned}
\mathbf{Adv}^{\texttt{ind-id-cca2}}_{\mathcal{IBE},A}(k) &\overset{(1)}{=} \Pr[\mathbf{Exp}^{\texttt{ind-id-cca2-1}}_{\mathcal{IBE},A}(k) = 1] - \Pr[\mathbf{Exp}^{\texttt{ind-id-cca2-0}}_{\mathcal{IBE},A}(k) = 1] \\
&\overset{(2)}{=} \Big| \Big[\ p(0,1) + \frac{1}{2} \cdot \big(\ p(0,0) + p(1,1)\ \big)\Big] \\
&\quad - \Big[\ p(1,0) + \frac{1}{2} \cdot \big(\ p(0,0) + p(1,1)\ \big)\Big] \Big| \\
&= \Big|\ p(0,1) - p(1,0)\ \Big| \\
\mathbf{Adv}^{\texttt{nm-id-cca2}}_{\mathcal{IBE},B}(k) &\overset{(3)}{=} \Pr[\mathbf{Exp}^{\texttt{nm-id-cca2-1}}_{\mathcal{IBE},B}(k) = 1] - \Pr[\mathbf{Exp}^{\texttt{nm-id-cca2-0}}_{\mathcal{IBE},B}(k) = 1] \\
&\overset{(4)}{=} \Big|\ \big(\ p(0,1) + p(1,1)\ \big) - \big(\ p(1,0) + p(1,1)\ \big)\ \Big| \\
&= \Big|\ p(0,1) - p(1,0)\ \Big|
\end{aligned}$$

Here, the notations $p(i, j)$, where $i, j \in \{0, 1\}$, are defined in Table 3. In this way we obtain the equations $\overset{(2)}{=}$ and $\overset{(4)}{=}$. And the 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 non-negligible, $\mathbf{Adv}^{\texttt{ind-id-cca2}}_{\mathcal{IBE},A}(k)$ is also non-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. $\square$

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 exists an IND-ATK adversary B who can successfully break IND-ATK with non-negligible advantage, then we show that we can construct an NM-ATK adversary A who can successfully break NM-ATK with non-negligible advantage. 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 NM-ATK adversary and IND-ATK adversary respectively. A is constructed as follows:

Algorithm $A_1^{\mathcal{O}_1}(param)$	Algorithm $A_2^{\mathcal{O}_2}(\hat{\mathcal{M}}, s', y^*, id)$
$(x_0, x_1, s, id) \leftarrow B_1^{\mathcal{O}_1}(param)$;	where $s' = (x_0, x_1, s)$
$\hat{\mathcal{M}} \leftarrow \{x_0, x_1\}_U$;	$d \leftarrow B_2^{\mathcal{O}_2}(x_0, x_1, s, id, y^*)$;
$s' \leftarrow (x_0, x_1, s)$;	$y' \leftarrow \mathcal{E}(param, id, (x_d + 1))$;
return $(\hat{\mathcal{M}}, s', id)$	$\overrightarrow{\boldsymbol{y}} \leftarrow \{y'\}$;
	return $(R, \overrightarrow{\boldsymbol{y}})$
	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 which 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 IND (1) and NM (3), we obtain

$$\Pr[b = 0] = \Pr[b = 1] = \frac{1}{2} \tag{11}$$

$$\Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},B}(k) = 0] = \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k) = 1] \tag{12}$$

$$\Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},B}(k) = 1] = \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k) = 0] \tag{13}$$

Furthermore, focusing on our construction, we obtain

$$\begin{aligned}\Pr[\mathbf{Exp}^{\texttt{nm-atk-1}}_{\mathcal{IBE},A}(k) = 1] = {} & \Pr[b = 0] \cdot \Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},B}(k) = 0] \\ & + \Pr[b = 1] \cdot \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k) = 1]\end{aligned} \tag{14}$$

$$\begin{aligned}\Pr[\mathbf{Exp}^{\texttt{nm-atk-0}}_{\mathcal{IBE},A}(k) = 1] = {} & \Pr[b = 0] \cdot \Pr[\mathbf{Exp}^{\texttt{ind-atk-0}}_{\mathcal{IBE},B}(k) = 1] \\ & + \Pr[b = 1] \cdot \Pr[\mathbf{Exp}^{\texttt{ind-atk-1}}_{\mathcal{IBE},B}(k) = 0]\end{aligned} \tag{15}$$

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 NM-ATK adversary A. Hence,

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

The equations $\overset{(1)}{=}$ and $\overset{(4)}{=}$ hold according to the definitions of advantages in NM (3) and IND (1), respectively. The equation $\overset{(2)}{=}$ holds according to Eq. (11) (14) (15). And the equation $\overset{(3)}{=}$ holds according to Eq. (12) (13).

Under the assumption that $\mathbf{Adv}^{\texttt{ind-atk}}_{\mathcal{IBE},B}(k)$ is non-negligible, $\mathbf{Adv}^{\texttt{nm-atk}}_{\mathcal{IBE},A}(k)$ is also non-negligible. We reach a contradiction to the hypothesis that $\mathcal{IBE}$ is secure in the NM-ATK sense. Thus $\mathcal{IBE}$ is also secure in the IND-ATK sense. This concludes the proof of Theorem 5. □

Acknowledgements

Rui Zhang is supported by a JSPS Fellowship. We are grateful to Jun Furukawa for his constructive suggestions. We also appreciate the very helpful discussions from Takeshi Gomi.

References

1. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology - CRYPTO '98*, volume 1462 of *LNCS*, pages 26–45. Springer-Verlag, 1998.
2. D. Boneh and X. Boyen. Chosen-ciphertext security from identity-based encryption. In *Advances in Cryptology - EUROCRYPT '98*, volume 3027 of *LNCS*, pages 223–238. Springer-Verlag, 2004.
3. D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In *Advances in Cryptology - CRYPTO '04*, volume 3152 of *LNCS*, pages 443–459. Springer-Verlag, 2004.
4. D. Boneh, X. Boyen, and E. Goh. Hierarchical identity based encryption with constant size ciphertext. In *Advances in Cryptology - EUROCRYPT '05*, volume 3494 of *LNCS*, pages 440–456. Springer-Verlag, 2005.
5. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology - CRYPTO '01*, volume 2139 of *LNCS*, pages 213–229. Springer-Verlag, 2001.
6. R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. In *Advances in Cryptology - EUROCRYPT '03*, volume 2656 of *LNCS*, pages 255–271. Springer-Verlag, 2003.
7. D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography (extended abstract). In *STOC '91*, pages 542–552, 1991.
8. D. Galindo and I. Hasuo. *Security notions for identity based encryption.* Manuscript, 2005.
9. O. Goldreich. *Foundations of cryptography, Volumn II (revised, posted version Nr. 4.2).* 2003. http://www.wisdom.weizmann.ac.il/ oded/.
10. O. Goldreich, Y. Lustig, and M. Naor. On chosen ciphertext security of multiple encryptions. Cryptology ePrint Archive, Report 2002/89, 2002. http://eprint.iacr.org/.
11. S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.
12. C. Rackoff and D.R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Advances in Cryptology - CRYPTO '91*, volume 576 of *LNCS*, pages 433–444. Springer-Verlag, 1991.
13. A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Advances in Cryptology - EUROCRYPT '05*, volume 3494 of *LNCS*, pages 457–473. Springer-Verlag, 2005.
14. Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology - CRYPTO '84*, volume 196 of *LNCS*, pages 47–53. Springer-Verlag, 1985.
15. Y. Watanabe, J. Shikata, and H. Imai. Equivalence between semantic security and indistinguishability against chosen ciphertext attacks. In *Public Key Cryptography - PKC '03*, volume 2567 of *LNCS*, pages 71–84. Springer-Verlag, 2003.
16. B. Waters. Efficient identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT '05*, volume 3494 of *LNCS*, pages 114–127. Springer-Verlag, 2005.
17. Peng Yang, Goichiro Hanaoka, Yang Cui, Rui Zhang, Nuttapong Attrapadung, Kanta Matsuura, and Hideki Imai. Relations among notions of security for identity based encryption schemes. In *IEICE Technical Report, Vol.105, No.194*, pages 25–32, Jul. 2005.

Appendix A. CPA, CCA1 and 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. 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. 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 named "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 which are chosen after the challenge ciphertext y^* is issued. The only restriction is that the adversary may not ask for the decryption of y^*.

Appendix B. Particular Attack Models in $\mathcal{IBE}$

In $\mathcal{IBE}$ environment, the adversary could be granted more power than adaptive chosen ciphertext attack, which has been well considered in $\mathcal{PKE}$. The adversary is allowed to attack an arbitrary public key id^* of her choice. Thus in additional 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 extraction queries to PKG (Private Key generator). The adversary should still have 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) [5] and adaptive chosen ciphertext security against selective identity attack (IND-sID-CCA2) [6].

B.1 Adaptive Chosen Identity Security

To achieve adaptive chosen identity security, the scheme should still remain secure under such adaptive chosen identity attack. The reason is that when an adversary attacks a public key id^* in $\mathcal{IBE}$, she might already possess the series private keys of other public keys $id_1, id_2, \dots id_n$. 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 named 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 polynomially 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.
- **Phase 1**: The adversary issues queries $q_1, \dots q_m$ 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 $id_i \neq id^*$. Challenger responds as in Phase 1.
  - Decryption query $< id_i, y_i >$, where $(id_i, y_i) \neq (id^*, y^*)$. 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 $b' = b^*$.

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

B.2 Selective Chosen Identity Security

Besides the adaptive identity attack model defined by Boneh and Franklin, there is also a weaker definition of security proposed by Canetti, Halevi and Katz [6]. Under this definition, 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* semantic 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 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.
- **Phase 1**: The adversary issues queries $q_1, \ldots q_m$ 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 $q_1, \ldots q_{i-1}$.
- **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 $id_i \neq id^*$. Challenger responds as in Phase 1.
  - Decryption query $< id_i, y_i >$, where $(id_i, y_i) \neq (id^*, y^*)$. 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 $b' = b^*$.

Such an adversary A is referred as an IND-sID-CCA2 adversary. We say A successfully break the scheme in the sense of IND-sID-CCA2 if she can distinguish that which plaintext was encrypted with a probability significantly more than random guess.