SCIS 2006 The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

Universally Composable Identity-Based Encryption

Ryo Nishimaki * Yoshifumi Manabe * † Tatsuaki Okamoto * †

Abstract— The identity-based encryption (IBE) is one of the most important primitives in cryptography, and various security notions of IBE (e.g., IND-ID-CCA2, NM-ID-CCA2, IND-sID-CPA etc.) have been introduced and the relations among them have been clarified recently. This paper, for the first time, investigate the security of IBE in the universally composable (UC) framework. This paper first defines the UC-security of IBE, i.e., we define the ideal functionality of IBE, $\mathcal{F}_{\mathrm{IBE}}$. We then show that UC-secure IBE is equivalent to conventionally-secure (IND-ID-CCA2-secure) IBE. This paper also introduces the UC-security of weaker security notions of IBE, which correspond to IND-ID-CPA IBE and IND-sID-CCA2. We finally prove that Boneh-Franklin's suggestion on the construction of a secure signatures from an IND-ID-CPA IBE scheme is true in the UC framework.

Keywords: identity-based encryption, IND-ID-CCA2, universal composition, digital signatures

1 Introduction

1.1 Background

The concept of identity-based encryption (IBE) was introduced by Shamir [12], and is a variant of public-key encryption (PKE), where the identity of a user is employed in place of the user's public-key.

Boneh and Franklin [2] defined the security, IND-ID-CCA2 (indistinguishable against adaptively chosen-ciphertext attacks under chosen identity attacks), as the desirable security of IBE schemes. Canetti, Halevi, and Katz [6, 7] defined a weaker notion of security in which the adversary commits ahead of time to the challenge identity it will attack. We refer to this notion as *selective identity* (sID) adaptively chosen-ciphertext secure IBE (IND-sID-CCA2). In addition, they also define a weaker security notion of IBE, selective-identity *chosen-plaintext* (CPA) secure IBE (IND-sID-CPA). Attrapadung et. al. [1], and Galindo and Hasuo [10] introduced the *non-malleability* (NM) in the security notion of IBE. Thus, the security definitions considered up to now in the literature are: G-A1-A2, where G $\in$ {IND, NM}, A1 $\in$ {ID, sID}, ID denotes full-identity attacks, and A2 $\in$ {CPA, CCA1, CCA2}.

Attrapadung et. al. [1], and Galindo and Hasuo [10] have clarified the relationship among these notions, and shown that IND-ID-CCA2 is equivalent to the strongest security notion, NM-ID-CCA2, among them.

Since Canetti introduced universal composability (UC) as a new framework for analyzing the security of cryptographic primitives/protocols [3], investing the relation between UC-secure primitives/protocols and conventionally-secure primitives/protocols has been one of the significant topics in cryptography [4, 5, 8, 9, 11]. Since UC represents stronger security requirements, a lot of conventionally-secure protocols fail to meet UC security requirements. For example, we cannot design secure two party protocols in the UC framework with no setup assumption, while there are conventionally-secure two party protocols (e.g., commitment and zero-knowledge proofs) with no setup assumption.

However, we know that the conventional security notions are equivalent to UC security notions for a few cryptographic primitives. For example, UC-secure PKE is equivalent to conventionally-secure (IND-CCA2-secure) PKE [3] and UC-secure signatures are equivalent to conventionally-secure (existentially unforgeable against chosen message attacks: EUF-CMA-secure) signatures [4].

IBE is a more complex cryptographic primitive than PKE and signatures, so it is not clear whether conventionally-secure (i.e., IND-ID-CCA2-secure) IBE is equivalent to UC-secure IBE or not. Since IBE is one of the most significant primitives like PKE and signatures in cryptography, it is important to clarify the relationship between the UC security and conventional security notions of IBE. The UC security of IBE, however, has not been investigated.

That is, we have the following problems:

1. What is the security definition of IBE in the UC framework (i.e., how to define an ideal functionality of IBE)?
2. Is UC-secure IBE equivalent to IND-ID-CCA2-secure IBE?

Some weaker security notions of IBE than IND-ID-CCA2 are also useful to construct a secure (IND-CCA2) PKE scheme and a secure (EUF-CMA) signatures. For example, Canetti, Halevi and Katz [7] have shown how

* Department of Social Informatics, Graduate School of Informatics, Kyoto University, Yoshidahonmachi, Sakyo-ku, Kyoto-shi, Japan, nisimaki@lab7.kuis.kyoto-u.ac.jp
† NTT Laboratories, 1-1 Hikari-no-oka, Yokosuka-shi, Japan, manabe.yoshifumi@lab.ntt.co.jp, okamoto.tatsuaki@lab.ntt.co.jp

to construct a secure PKE scheme from a selective-ID-secure (IND-sID-CPA-secure) IBE scheme. Boneh and Franklin [2] suggested a construction of a secure signatures from an IND-ID-CPA IBE scheme.

The UC security treatment of such weaker security notions of IBE may provide insight into a new relationship between IBE and other primitives and also offer a simpler and more clear proof of the relations than the conventional proofs. Therefore, it should be significant to define the weaker security notions of IBE in the UC framework.

That is, we have the following problem:

1. What are the UC security definitions of the weaker security notions of IBE?
2. How to prove the constructibility of secure PKE/ signatures from the weaker security notions of IBE in the UC framework?

1.2 Our Results

This paper answers the above-mentioned problems:

1. This paper defines the UC-security of IBE, i.e., we define the ideal functionality of IBE, $\mathcal{F}_{\mathrm{IBE}}$.
2. We show that UC-secure IBE is equivalent to conventionally-secure (IND-ID-CCA2-secure) IBE.
3. We define the ideal functionalities of weaker security notions of IBE, $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{ND}}$ and $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$. We then show that UC-secure IBE with $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{ND}}$ is equivalent to IND-ID-CPA IBE, and that UC-secure IBE with $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$ is equivalent to IND-sID-CCA2 IBE.
4. We prove that Boneh-Franklin's suggestion [2] on the construction of a secure signatures from an IND-ID-CPA IBE scheme is true in the UC framework. That is, we present a protocol which UC-realizes ideal functionality $\mathcal{F}_{\mathrm{SIG_W}}$ in the $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{ND}}$-hybrid model, where $\mathcal{F}_{\mathrm{SIG_W}}$ is an ideal functionality with (normal) unforgeability, while $\mathcal{F}_{\mathrm{SIG}}$ defined by Canetti [4] represents *strong* unforgeability.

2 Preliminaries

2.1 Conventions

Notations We describe probabilistic algorithms and experiments with standard notations and conventions. For probabilistic algorithm A, $A(x_1, x_2, ...; r)$ is the result of running A that takes as inputs $x_1, x_2, ...$ and coins r. We let $y \leftarrow A(x_1, x_2, ...)$ denote the experiment of picking r at random and letting y equal the output of $A(x_1, x_2, ...; r)$. If S is a finite set, then $x \leftarrow S$ denotes the experiment of assigning to x an element uniformly chosen from S. If α is neither an algorithm nor a set, then $x \leftarrow \alpha$ indicates that we assign α to x. We say that y can be output by $A(x_1, x_2, ...)$ if there is some r such that $A(x_1, x_2, ...; r) = y$. $\hat{\mathcal{M}}$ 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.

We say that a function $g : \Re \to \Re$ is negligible if for any $d > 0$ we have $|g(k)| < \frac{1}{k^d}$ for sufficiently large k.

2.2 Identity-Based Encryption

Identity-Based Encryption scheme Identity-based encryption scheme Σ is specified by four algorithms: $\mathcal{S}$, $\mathcal{X}$, $\mathcal{E}$, $\mathcal{D}$:

Setup: $\mathcal{S}$ takes security parameter k and returns $params$ (system parameters) and mk (master-key). The system parameters include a description of a finite message space $\mathcal{M}$, and a description of a finite ciphertext space $\mathcal{C}$.

Extract: $\mathcal{X}$ takes as input $params$, mk, and an arbitrary $ID \in \{0,1\}^*$, and returns private key d. Here ID is an arbitrary string that will be used as a public key, and d is the corresponding private decryption key.

Encrypt: $\mathcal{E}$ takes as input $params$, ID, and $M \in \mathcal{M}$. It returns a ciphertext $C \in \mathcal{C}$.

Decrypt: $\mathcal{D}$ takes as input $params$, $C \in \mathcal{C}$, and a private key d. It returns $M \in \mathcal{M}$.

These algorithms must satisfy the standard consistency constraint, namely,

$\forall M \in \mathcal{M} : \mathcal{D}(params, C, d) = M$ where $C = \mathcal{E}(params, ID, M)$, $d = \mathcal{X}(params, mk, ID)$

2.3 Definitions of security notions for IBE schemes

Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary; we say $\mathcal{A}$ is polynomial time if both probabilistic algorithm $\mathcal{A}_1$ and $\mathcal{A}_2$ are polynomial time. At the first stage, given the system parameters, the adversary computes and outputs challenge template τ. $\mathcal{A}_1$ can output some information s which will be transferred to $\mathcal{A}_2$. At the second stage, the adversary is challenged with ciphertext y^* generated from τ by a probabilistic function, in a manner depending on the goal. We say adversary $\mathcal{A}$ successfully breaks the scheme if she achieves her goal. We consider a security goal, IND [1, 10], and three attack models, ID-CPA, ID-CCA, ID-CCA2, listed in order of increasing strength. The difference among the models is whether or not $\mathcal{A}_1$ or $\mathcal{A}_2$ is granted access to decryption oracles. We describe in Table 1 the ability with which the adversary can, in the different attack models, access the Extraction Oracle $\mathcal{X}(params, mk, \cdot)$, the Encryption Oracle $\mathcal{E}(params, ID, \cdot)$ and the Decryption Oracle $\mathcal{D}(params, d, \cdot)$ (We omit parameters in Table 1). When we say $\mathcal{O}_i = \{\mathcal{EO}_i, \mathcal{XO}_i, \mathcal{DO}_i\} = \{\mathcal{X}(params, mk, \cdot), \mathcal{E}(params, ID, \cdot), \epsilon\}$, where $i \in \{1, 2\}$, we mean $\mathcal{DO}_i$ is a function that returns a empty string ϵ on any input.

Indistinguishability Let $\mathcal{IBE} = (\mathcal{S}, \mathcal{X}, \mathcal{E}, \mathcal{D})$ be an identity based encryption scheme and let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For atk $\in$ {id-cpa, id-cca, id-cca2} and $k \in N$ let,

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

where for $b, d \in \{0,1\}$ and $|m_0| = |m_1|$,

$$\begin{gathered}\text{Experiment } \mathbf{Exp}^{\text{ind-atk-b}}_{\text{IBE},\mathcal{A}}(k)\\ (params, mk) \leftarrow \mathcal{S}(k);\\ (m_0, m_1, s, ID) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(params);\\ c^* \leftarrow \mathcal{E}(params, ID, m_b);\\ d \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(m_0, m_1, s, c^*, ID);\\ \text{return } d\end{gathered}$$

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

Table 1: Oracle Set $\mathcal{O}_1, \mathcal{O}_2$

	$\mathcal{O}_1$	$\mathcal{O}_2$
ID-CPA	$\{\mathcal{X}, \mathcal{E}, \epsilon\}$	$\{\mathcal{X}, \mathcal{E}, \epsilon\}$
ID-CCA	$\{\mathcal{X}, \mathcal{E}, \mathcal{D}\}$	$\{\mathcal{X}, \mathcal{E}, \epsilon\}$
ID-CCA2	$\{\mathcal{X}, \mathcal{E}, \mathcal{D}\}$	$\{\mathcal{X}, \mathcal{E}, \mathcal{D}\}$

selective-ID Canetti, Halevi, and Katz considered selective node attack [6]. Under this definition, the identity for which the challenge ciphertext is encrypted is selected by the adversary in advance (i.e., non-adaptively) before the public key is generated.

2.4 Universal Composability

Ideal functionality of secure channel, $\mathcal{F}_{\text{SC}}$ To realize identity-based encryption functionality, $\mathcal{F}_{\text{IBE}}$, we use $\mathcal{F}_{\text{SC}}$ [8]. To understand UC framework, see more details in [3].

3 UC-secure IBE is equivalent to IND-ID-CCA2-secure IBE

3.1 The Identity-Based Encryption Functionality $\mathcal{F}_{\text{IBE}}$

We define IBE functionality $\mathcal{F}_{\text{IBE}}$ in Fig.1. $\mathcal{F}_{\text{IBE}}$ is a functionality of IBE-setup, IBE-extraction, IBE-encryption and IBE-decryption.

3.2 UC-secure IBE is equivalent to IND-ID-CCA2-secure IBE

Next, we present a protocol that securely realizes $\mathcal{F}_{\text{IBE}}$.

Let $\Sigma = (\mathcal{S}, \mathcal{X}, \mathcal{E}, \mathcal{D})$ be an identity based encryption scheme. Consider the following transformation from IBE scheme Σ to protocol π_{IBE} that is geared towards realizing $\mathcal{F}_{\text{IBE}}$ in the $\mathcal{F}_{\text{SC}}$-hybrid model:

1. Upon input $(\texttt{Setup}, sid, P_i)$ within some party P_i, P_i obtains the system parameters PK_i and master-key SK_i by running algorithm $\mathcal{S}()$, then outputs $(\texttt{Set}, sid, PK_i)$ and sends $(\texttt{Establish-session}, sid, P, \textit{initiator})$ to $\mathcal{F}_{\text{SC}}$ for all parties.
2. Upon input $(\texttt{Extract}, sid, ID, PK'_i)$ within some party P_k, P_k sends $(\texttt{Establish-session}, sid, P_i, \textit{responder})$ to $\mathcal{F}_{\text{SC}}$ and sends message $(\texttt{Extract}, sid, ID, PK'_i)$ to P_i.

Functionality $\mathcal{F}_{\text{IBE}}$

$\mathcal{F}_{\text{IBE}}$ proceeds as follows, running with parties P_1,...,P_n and adversary $\mathcal{S}$.

Setup

In the first activation, expect to receive a value $(\texttt{Setup}, sid, P_i)$ from some party P_i. Then do:

1. Hand $(\texttt{Setup}, sid, P_i)$ to adversary $\mathcal{S}$.
2. Receive value $(\texttt{Set}, sid, PK_i)$ from adversary $\mathcal{S}$, and hand $(\texttt{Set}, sid, PK_i)$ to P_i.
3. Record the pair (P_i, PK_i).

Extract

Upon receiving value $(\texttt{Extract}, sid, ID, PK'_i)$ from some party P_k, proceed as follows:

1. If PK'_i is recorded and ID is P_k's, record (ID, P_k) in ID-Reg. Else do not record.
2. Hand $(\texttt{Extract}, sid, ID, PK'_i)$ to adversary $\mathcal{S}$, and receive $(\texttt{Received}, sid)$ from adversary $\mathcal{S}$.
3. Hand $(\texttt{Extracted}, sid, P_k, PK'_i)$ to P_k and P_i (If PK'_i is not recorded or ID is not P_k's, do not hand.)

Encrypt

Upon receiving value $(\texttt{Encrypt}, sid, m, ID, PK'_i)$ from some party P_j, proceed as follows:

1. Hand $(\texttt{Encrypt}, sid, |m|, ID, PK'_i)$ to adversary $\mathcal{S}$, where $|m|$ the length of m.(If PK'_i is not recorded hand $(\texttt{Encrypt}, sid, m, ID, PK'_i)$.)
2. Receive $(\texttt{Encrypted}, sid, c, ID, PK'_i)$ from adversary $\mathcal{S}$ and hand $(\texttt{Encrypted}, sid, c, ID, PK'_i)$ to P_j.
3. Store (m, c, ID) in Plain-Cipher.

Decrypt

Upon receiving value $(\texttt{Decrypt}, sid, c, ID, PK'_i)$ from P_k, proceed as follows:

1. If the following four conditions are satisfied then hand $(\texttt{Decrypted}, sid, m, ID, PK'_i)$ to P_k.
   (a) (ID, P_k) is recorded in ID-Reg.
   (b) P_i(Setup party) is not corrupted or P_i is corrupted after ID is extracted.
   (c) P_k is not corrupted.
   (d) (m, c, ID) is stored in Plain-Cipher.
2. If (ID, P_k) is not recorded in ID-Reg then hand value $(\texttt{Decrypt}, sid, c, ID, PK'_i)$ to adversary $\mathcal{S}$ and hand `not-recorded` to P_k.
3. Otherwise, hand value $(\texttt{Decrypt}, sid, c, ID, PK'_i)$ to adversary $\mathcal{S}$, receive value $(\texttt{Decrypted}, sid, m', PK'_i)$ from adversary $\mathcal{S}$, and hand $(\texttt{Decrypted}, sid, m', ID, PK'_i)$ to P_k.

Figure 1: The identity-based encryption functionality

sid, ID, PK_i') to P_i. Upon receiving this message, P_i obtains private key d_k by running algorithm $\mathcal{X}(PK_i', SK_i', ID)$. If PK_i' is already defined and ID is P_k's, P_i sends ($\texttt{Send}, sid, d_k$) to $\mathcal{F}_{\text{SC}}$. Upon receiving ($\texttt{Received}, sid, d_k$) from $\mathcal{F}_{\text{SC}}$, P_k outputs ($\texttt{Extracted}, sid, P_k, PK_i'$). If PK_i' is not yet defined or ID is not P_k's, P_i ignores the request.

3. Upon input ($\texttt{Encrypt}, sid, m, ID, PK_i'$) within some party P_j, P_j obtains ciphertext c by running algorithm $\mathcal{E}(PK_i', ID, m)$ and outputs ($\texttt{Encrypted}, sid, c, ID, PK_i'$). (Note that it does not necessarily hold that ID is P_j's)

4. Upon input ($\texttt{Decrypt}, sid, c, ID, PK_i'$) within P_k, if PK_i' is already defined and ID is P_k's, P_k obtains $m = \mathcal{D}(PK_i', c, d_k)$ and outputs ($\texttt{Decrypted}, sid, m, P_k, PK_i'$). If P_k has not extracted private key d_k yet, P_k outputs `not-recorded`.

Theorem 1 π_{IBE} securely realizes $\mathcal{F}_{\text{IBE}}$ in the $\mathcal{F}_{\text{SC}}$-hybrid model with respect to non-adaptive adversaries if and only if IBE scheme Σ is IND-ID-CCA2-secure.

Proof sketch. (only if part): Assuming that there exists adversary $\mathcal{A}^*$ that can guess bit b correctly with probability $\frac{1}{2}+\epsilon$, in an IND-ID-CCA2 game with scheme Σ, we prove that we can construct environment $\mathcal{Z}$ and real life adversary $\mathcal{A}$ such that for any ideal process adversary (simulator) $\mathcal{S}$, $\mathcal{Z}$ can tell with probability ϵ whether it is interacting with $\mathcal{A}$ and π_{IBE} or with $\mathcal{S}$ in the ideal process for $\mathcal{F}_{\text{IBE}}$ by using adversary $\mathcal{A}^*$ that breaks IND-ID-CCA2 security.

$\mathcal{Z}$ proceeds as follows:

1. Activates party P_i with ($\texttt{Setup}, sid, P_i$) and obtains PK_i.

2. Hands PK_i to $\mathcal{A}^*$ and plays the role of an oracle for adversary $\mathcal{A}^*$ in the IND-ID-CCA2 game.

3. Obtains (ID_k, M_0, M_1) from $\mathcal{A}^*$. ID_k (party P_k's ID) is the ID $\mathcal{A}^*$ attacks.

4. Activates P_k with ($\texttt{Extract}, sid, ID_k, PK_i$), obtains ($\texttt{Extracted}, sid, ID_k, PK_i$).

5. Chooses random bit $b \in \{0,1\}$, selects an arbitrary party $P_j \neq P_k$ and activates P_j with ($\texttt{Encrypt}, sid, M_b, ID_k, PK_i$) and obtains C^*.

6. Hands C^* to $\mathcal{A}^*$ as the test ciphertext.

7. Plays the role of an oracle for adversary $\mathcal{A}^*$ in the IND-ID-CCA2 game, and obtains guess $b' \in \{0,1\}$.

8. Outputs 1 if $b = b'$, otherwise outputs 0 and halts.

In step 2, the adversary issues queries $q_1, ..., q_m$ where query q_l is one of:

1. Extraction query $\langle ID_l \rangle$. $\mathcal{Z}$ asks $\mathcal{A}$ to corrupt P_l and responds by activating P_l with ($\texttt{Extract}, sid, ID_l, PK_i$) to obtain private key d_l corresponding to public key $\langle ID_l \rangle$. It sends d_l to the adversary.

2. Decryption query $\langle ID_l, C_l \rangle$. $\mathcal{Z}$ asks $\mathcal{A}$ to corrupt P_l, obtains private key d_l corresponding to ID_l and responds by running algorithm $\mathcal{D}(PK_i, C_l, d_l)$ to decrypt ciphertext C_l using private key d_l. It sends the resulting plaintext to the adversary.

These queries may be asked adaptively, that is, each query q_l may depend on the replies to $q_1, ..., q_{l-1}$.

In step 7, the adversary issues more queries $q_{m+1}, ..., q_n$ where query q_l is one of:

1. Extraction query $\langle ID_l \rangle$ where $ID_l \neq ID_k$. $\mathcal{Z}$ responds as in step 2.

2. Decryption query $\langle ID_l, C_l \rangle \neq \langle ID_k, C^* \rangle$. If $ID_l \neq ID_k$ $\mathcal{Z}$ responds as in step 2, else if $ID_l = ID_k, C_l \neq C^*$, $\mathcal{Z}$ activates P_k with ($\texttt{Decrypt}, sid, C_l, P_k, PK_i$) and sends the resulting plaintext to the adversary (if ID_k is not extracted then activates P_k with ($\texttt{Extract}, sid, ID_k, PK_i$) before activating P_k with ($\texttt{Decrypt}, sid, C_l, P_k, PK_i$)).

These queries may be asked adaptively as in step 2.

We omit details, see the full paper version.

(if part): We show that if π_{IBE} does not securely realize $\mathcal{F}_{\text{IBE}}$, then π_{IBE} is not IND-ID-CCA2-secure. We then prove that π_{IBE} is not IND-ID-CCA2 secure by using distinguishable environment $\mathcal{Z}$.

We omit how simulator $\mathcal{S}$ proceeds, see the full paper version.

For some value of the security parameter z for $\mathcal{Z}$, we assume that there is environment $\mathcal{Z}$ such that $IDEAL_{\mathcal{F},\mathcal{S},\mathcal{Z}}(z) - REAL_{\pi_{\text{IBE}},\mathcal{A},\mathcal{Z}}(z) > \sigma$, then we show that there exists $\mathcal{A}_h^*$ which correctly guesses bit b with probability $\frac{1}{2} + \frac{\sigma}{2l}$ in the IND-ID-CCA2 game, where l is the total number of messages that were encrypted throughout the running of the system and $h \in \{1, ..., l\}$. $\mathcal{A}_h^*$ runs $\mathcal{Z}$ on the following simulated interaction with a system running π_{IBE}. Let m_j denotes the jth message that $\mathcal{Z}$ asks to encrypt in this simulation and ID_j denotes the jth ID that $\mathcal{Z}$ uses to encrypt in this simulation.

1. When $\mathcal{Z}$ activates some party P_i with input ($\texttt{Setup}, sid, P_i$), $\mathcal{A}_h^*$ lets P_i output the value PK_i from $\mathcal{A}_h^*$'s input.

2. When $\mathcal{Z}$ activates some party P_k with input ($\texttt{Extract}, sid, ID_k, PK_i$), $\mathcal{A}_h^*$ lets P_k output message ($\texttt{Extracted}, sid, ID_k, PK_i$) from $\mathcal{A}_h^*$'s input. If P_k is corrupted then $\mathcal{A}_h^*$ queries its extraction oracle on ID_k, obtains value u, and lets P_k return u to $\mathcal{Z}$.

3. For the first $h-1$ times that $\mathcal{Z}$ asks to encrypt some message, m_j, $\mathcal{A}_h^*$ lets the encrypting party return $c_j = \mathcal{E}(PK_i, ID_j, m_j)$.

4. The h-th time that $\mathcal{Z}$ asks to encrypt message, m_h by ID^*, $\mathcal{A}_h^*$ queries its encryption oracle with the pair of messages $(m_h, 0^{|m_h|})$, and obtains test ciphertext c_h. It then hands c_h to $\mathcal{Z}$ as the encryption of m_h. That is, $c_h = \mathcal{E}(PK_i, ID^*, m_h)$ or $c_h = \mathcal{E}(PK_i, ID^*, 0^{|m_h|})$.

5. For the remaining $l - h$ times that $\mathcal{Z}$ asks to encrypt some message, m_j, $\mathcal{A}_h^*$ lets the encrypting party return $c_j = \mathcal{E}(PK_i, ID'_j, 0^{|m_j|})$.

6. Whenever decryptor P_j is activated with input $(\texttt{Decrypt}, sid, c, ID_j, PK_i)$ where $c = c_j$ for some j, $\mathcal{A}_h^*$ lets P_j return the corresponding plaintext m_j. If c is different from all c_j's and ID_j is extracted then $\mathcal{A}_h^*$ queries its decryption oracle on (ID_j, c), obtains value u, and lets P_j return u to $\mathcal{Z}$. If c is different from all c_j's and ID_j is not extracted then $\mathcal{A}_h^*$ lets P_j output `not-recorded`.

7. When $\mathcal{Z}$ halts, $\mathcal{A}_h^*$ outputs whatever $\mathcal{Z}$ outputs and halts.

We apply a standard hybrid argument for analyzing the success probability of $\mathcal{A}_h^*$. We omit the details, see the full paper version.

□

4 UC-secure IBE with ND is equivalent to IND-ID-CPA-secure IBE

4.1 The Identity-Based Encryption with ND Functionality $\mathcal{F}_{\text{IBE}}^{\text{ND}}$

We define an IBE functionality with no decryption (ND), $\mathcal{F}_{\text{IBE}}^{\text{ND}}$ in Fig.2.

The main difference from $\mathcal{F}_{\text{IBE}}$ is **Decrypt** stage. $\mathcal{F}_{\text{IBE}}^{\text{ND}}$ does not hand results of decryption.

Functionality $\mathcal{F}_{\text{IBE}}^{\text{ND}}$

$\mathcal{F}_{\text{IBE}}^{\text{ND}}$ proceeds as follows, running with parties P_1,...,P_n and adversary $\mathcal{S}$.

Setup, **Extract**, **Encrypt**: See Figure 1.

Decrypt

Upon receiving value $(\texttt{Decrypt}, sid, c, ID, PK'_i)$ from P_k, proceed as follows:

1. If P_k is not corrupted,
   (a) If (ID, P_k) is recorded in ID-Reg, then hand $(\texttt{Decrypted}, sid, 1, ID, PK'_i)$ to P_k.
   (b) Otherwise, hand $(\texttt{Decrypted}, sid, 0, ID, PK'_i)$ to P_k.
2. If P_k is corrupted, hand value $(\texttt{Decrypt}, sid, c, ID, PK'_i)$ to adversary $\mathcal{S}$, receive the answer from adversary $\mathcal{S}$, and hand the answer to P_k.

Figure 2: The identity-based encryption functionality with ND

4.2 UC-secure IBE with ND is equivalent to IND-ID-CPA-secure IBE

We omit protocol $\pi_{\text{IBE}}^{\text{ND}}$ that securely realizes $\mathcal{F}_{\text{IBE}}^{\text{ND}}$, see the full paper version.

Theorem 2 $\pi_{\text{IBE}}^{\text{ND}}$ securely realizes $\mathcal{F}_{\text{IBE}}^{\text{ND}}$ in the $\mathcal{F}_{\text{SC}}$-hybrid model with respect to non-adaptive adversaries if and only if IBE scheme Σ is IND-ID-CPA-secure.

We omit the proof of Theorem 2, see the full paper version.

4.3 A Universally Composable Signature Based on the IBE Scheme

Functionality $\mathcal{F}_{\text{SIG}_\text{W}}$

Key Generation:

Upon receiving value $(\texttt{KeyGen}, sid)$ from some party S (signer), verify that $sid = (S, sid')$ for some sid'. If not, then ignore the request. Else, hand $(\texttt{KeyGen}, sid)$ to the adversary. Upon receiving $(\texttt{Verification Key}, sid, v)$ from the adversary, output $(\texttt{Verification Key}, sid, v)$ to S, and record the pair (S, v).

Signature Generation:

Upon receiving value $(\texttt{Sign}, sid, m)$ from S, verify that $sid = (S, sid')$ for some sid'. If not, then ignore the request. Else, send $(\texttt{Sign}, sid, m)$ to the adversary. Upon receiving $(\texttt{Signature}, sid, m, \sigma)$ from the adversary, verify that no entry $(m, v, 0)$ is recorded. If it is, then output an error message to S and halt. Else, output $(\texttt{Signature}, sid, m, \sigma)$ to S, and record the entry $(m, v, 1)$.

Signature Verification:

Upon receiving value $(\texttt{Verify}, sid, m, \sigma, v')$ from some party P, hand $(\texttt{Verify}, sid, m, \sigma, v')$ to the adversary. Upon receiving $(\texttt{Verified}, sid, m, \phi)$ from the adversary do:

1. If $v = v'$ and the entry $(m, v, 1)$ is recorded, then set $f = 1$.
2. Else if $v = v'$, the signer is not corrupted, and no entry $(m, v, 1)$ is recorded, then set $f = 0$ and record the entry $(m, v, 0)$.
3. Else, if there is an entry (m, v', f') recorded, then let $f = f'$.
4. Else, let $f = \phi$ and record the entry (m, v', ϕ)

Output $(\texttt{Verified}, sid, m, f)$ to P.

Figure 3: The digital signatures functionality

Canetti defined ideal functionality of digital signatures, $\mathcal{F}_{\text{SIG}}$, and showed that UC-secure signatures are equivalent to EUF-CMA-secure signatures [4]. $\mathcal{F}_{\text{SIG}}$ represents strong unforgeability. We define an ideal functionality of digital signatures with (normal) unforgeability, $\mathcal{F}_{\text{SIG}_\text{W}}$ in Fig.3. An IND-ID-CPA-secure

IBE scheme can be converted into a signature scheme that is existentially unforgeable against chosen message attack (EUF-CMA).

Theorem 3 $\pi_{\mathrm{SIG_W}}$ UC-realizes $\mathcal{F}_{\mathrm{SIG_W}}$ in the $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{ND}}$-hybrid model.

We omit protocol $\pi_{\mathrm{SIG_W}}$ and the proof of the Theorem 3, see the full paper version.

5 UC IBE with sID is equivalent to IND-sID-CCA2-secure IBE

Canetti, Halevi, and Katz have shown how to construct a secure PKE scheme from a selective-ID-secure IBE scheme [7].

We define IBE functionality $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$ in Fig.4. The main difference from $\mathcal{F}_{\mathrm{IBE}}$ are **Setup**, **Encrypt** and **Decrypt** stages. $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$ receives target ID, ID^* at **Setup** stage. If $ID = ID^*$, then $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$ excutes encryption (resp. decryption) at **Encrypt** (resp. **Decrypt**) stage.

We can present protocol $\pi_{\mathrm{IBE}}^{\mathrm{sID}}$ that securely realizes $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$ as in Section 3.

Theorem 4 $\pi_{\mathrm{IBE}}^{\mathrm{sID}}$ securely realizes $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$ in the $\mathcal{F}_{\mathrm{SC}}$-hybrid model with respect to non-adaptive adversaries if and only if IBE scheme Σ is IND-sID-CCA2 secure.

We omit the proof of the Theorem 4, see the full paper version.

6 Conclusion

We defined $\mathcal{F}_{\mathrm{IBE}}$ and showed that UC-secure IBE is equivalent to IND-ID-CCA2-secure IBE. We also defined the ideal functionalities of weaker security notions of IBE, $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{ND}}$ and $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$. We then showed that UC-secure IBE with $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{ND}}$ is equivalent to IND-ID-CPA-secure IBE, and that UC-secure IBE with $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$ is equivalent to IND-sID-CCA2-secure IBE. We presented a protocol which UC-realizes ideal functionality $\mathcal{F}_{\mathrm{SIG_W}}$ in the $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{ND}}$-hybrid model.

Functionality $\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$

$\mathcal{F}_{\mathrm{IBE}}^{\mathrm{sID}}$ proceeds as follows, running with parties P_1,...,P_n and adversary $\mathcal{S}$.

Setup

In the first activation, expect to receive value $(\mathtt{Setup}, sid, P_i, ID^*)$ from some party P_i. Then do:

1. Record target ID, ID^*.
2. 3. 4. See Figure 1.

Extract: See Figure 1.

Encrypt

Upon receiving value $(\mathtt{Encrypt}, sid, m, ID, PK_i')$ from some party P_j, if $ID \neq ID^*$, then ignore the request. Else, proceed as $\mathcal{F}_{\mathrm{IBE}}$ in Figure 1.

Decrypt

Upon receiving value $(\mathtt{Decrypt}, sid, c, ID, PK_i')$ from P_k, if $ID \neq ID^*$, then ignore the request. Else, proceed as $\mathcal{F}_{\mathrm{IBE}}$ in Figure 1.

Figure 4: The identity-based encryption functionality with sID

References

[1] Nuttapong Attrapadung, Yang Cui, Goishiro Hanaoka, Hideki Imai, Kanta Matsuura, Peng Yang, and Rui Zhang. Relations among notions of security for identity based encryption schemes. Cryptology ePrint Archive, Report 2005/258, 2005. http://eprint.iacr.org/.

[2] Dan Boneh and Matthew Franklin. Identity-based encryption from the weil pairing. *In proceedings of CRYPTO'01*, 2001.

[3] Ran Canetti. Universally composable security:a new paradigm for cryptograpic protocols. *In proceedings of FOCS'01*, 2001.

[4] Ran Canetti. Universally composable signatures, certification, and authenticated communication. *In proceedings of 17th Computer Security Foundations Workshop*, 2004.

[5] Ran Canetti and Marc Fischlin. Universally composable commitments. *In proceedings of CRYPTO'01*, 2001.

[6] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. *In proceedings of EUROCRYPT'03*, 2003.

[7] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. *In proceedings of EUROCRYPT'04*, 2004.

[8] Ran Canetti and Hugo Krawczyk. Universally composable key exchange and secure channels. *In proceedings of EUROCRYPT'02*, 2002.

[9] Ran Canetti and Tale Rabin. Universal composition with joint state. *In proceedings of CRYPTO'03*, 2003.

[10] David Galindo and Ichiro Hasuo. Security notions of for identity based encryption. Cryptology ePrint Archive, Report 2005/253, 2005. http://eprint.iacr.org/.

[11] Waka Nagao, Yoshihumi Manabe, and Tatsuaki Okamoto. A universally composable secure channel based on the kem-dem framework. *In proceedings of TCC'05*, 2005.

[12] Adi Shamir. Identity-based cryptosystems and signature schemes. *In proceedings of CRYPTO'84*, 1984.