Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2013, Article ID 217480, 9 pages
http://dx.doi.org/10.1155/2013/217480

Research Article

On the Anonymity of Identity-Based Encryption

Song Luo[1] and Ning Hu[2]

[1] *College of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400054, China*
[2] *Kai Feng Culture And Arts College, Kaifeng 475000, China*

Correspondence should be addressed to Song Luo; ratiopku@126.com

Received 23 April 2013; Revised 17 October 2013; Accepted 19 October 2013

Academic Editor: Mina Abd-El-Malek

Anonymity of identity-based encryption (IBE) means that given a ciphertext, one cannot distinguish the target identity from a random identity. In this paper, we thoroughly discuss the anonymity of IBE systems. We found that the current definition of anonymity is obscure to describe some IBE systems, such as Gentry IBE system. Furthermore, current definition cannot express the degree of anonymity. So we divide the degree of anonymity into weak anonymity and strong anonymity based on indistinguishability between different games. For weakly anonymous IBE systems, the target identity in a ciphertext cannot be distinguished from a random identity. For strongly anonymous IBE systems, the whole ciphertext cannot be distinguished from a random tuple. We also discuss the type of anonymity and divide it into two types. Type 1 means that a random tuple can be seen as a valid ciphertext, while type 2 cannot. Based on our new definitions, we show that three famous IBE systems, Gentry IBE system, Boyen-Waters IBE system, and Lewko IBE system, have strong but different types of anonymity.

1. Introduction

Shamir [1] proposed the concept of identity-based encryption (IBE) in 1984 to simplify the public key infrastructure. In an IBE system, public keys for users can be formed from arbitrary strings such as e-mail addresses, IP addresses, or other meaningful strings. Anyone can encrypt messages using the identity, and only the owner of the corresponding secret key can decrypt the messages. But Shamir did not give a concrete construction of IBE until Boneh and Franklin [2] presented the first practical IBE system based on groups with efficiently computable bilinear maps. Another but less efficient IBE system using quadratic residues was proposed by Cocks [3]. After that, many new IBE systems are proposed [4–11].

Anonymous IBE was first noticed by Boyen [12] and later formalized by Abdalla et al. [13, 14]. Roughly speaking, an IBE system is said to be *recipient anonymous* or simply *anonymous* if the ciphertext leaks no information about the recipient's identity. In other words, an attack cannot distinguish the target identity from a random identity for a ciphertext. Recently, people found that the anonymity of IBE can help to construct public key encryption with keyword search (PEKS) systems [13, 15–17].

The first anonymous IBE system is Boneh-Franklin IBE system [2]. In fact, this system has intrinsic anonymity; that is, its semantic security equals anonymity. But Boneh-Franklin IBE system is proposed in the random oracle model [18]. Boyen and Waters [8] gave the first construction of anonymous IBE in the standard model under the decisional bilinear Diffie-Hellman (BDH) and decisional linear assumptions. Another efficient construction of anonymous IBE in the standard model was proposed by Gentry [9], but it is proven secure under a dynamic and complicates assumption. After that, many new anonymous IBE systems in the standard model are proposed [19–21]. An extension of anonymous IBE, named committed blind anonymous IBE, was proposed by Camenisch et al. [22] in which a user can request the decryption key for a given identity without the key generation entity learning the identity.

When studying how to construct anonymous IBE systems, researchers have found if asymmetric bilinear maps are used in previous IBE systems [4–7]; these systems seem anonymous. But how to prove anonymous security of these

systems from simple assumptions was unknown until Ducas [23] gave a positive answer. He showed that an IBE system can be proven anonymous with some minor modification. Another anonymous IBE system using asymmetric bilinear map is proposed by Chen et al. [24]. Recently, Herranz et al. [25] discussed the relations between semantic security and anonymity for IBE systems.

When an "anonymous" IBE system is constructed, we should prove its anonymity. It seems to prove anonymity for IBE systems, we only need to prove that we cannot distinguish the target identity from the challenge ciphertext in the security game for anonymity. However, current anonymous IBE systems, except Gentry IBE system [9], all use a stronger game called $\text{Game}_{\text{Random}}$ than the standard game for anonymity where the challenge ciphertext is composed of independently random group elements to prove anonymity. Obviously, if a valid ciphertext is indistinguishable from a random tuple, it is definitely anonymous. However, the game $\text{Game}_{\text{Random}}$ is overqualified for anonymity, because anonymity only requires that an attacker cannot distinguish the target identity for a ciphertext. Hence, current definition of anonymity is not complete enough to describe the anonymity of current IBE systems.

Our Results. We make a concrete analysis of the anonymity of identity-based encryption systems. We found that current definition of anonymity is obscure to describe some IBE systems, such as Gentry IBE system [9]. Furthermore, current definition cannot express the degree of anonymity. By using the indistinguishability of some related security games, we divide anonymity into two degrees: weak anonymity and strong anonymity. Weak anonymity equals current definition of anonymity, in which the target identity for a ciphertext cannot be distinguished from a random identity. For strongly anonymous IBE systems, the whole ciphertext cannot be distinguished from a random tuple. We also discuss the type of anonymity and divide it into two types. Type 1 means that a random tuple can be seen as a valid ciphertext for some identity, while type 2 cannot. Based on our discussion, we analyse some IBE systems. We show that three famous IBE systems, Gentry IBE System [9], Boyen-Waters IBE system [8], and Lewko IBE System [26], have strong but different types of anonymity.

Organization. The paper is organized as follows. We give necessary background information and definitions of security in Section 2. We then analyse the anonymity and define different degrees and types of anonymity in Section 3. In Section 4, we discuss the anonymity of some current IBE systems. At last we conclude the paper with Section 5.

2. Background

In this section, we briefly review the concepts of the bilinear maps, identity-based encryption, and its security models for semantic security and anonymity.

2.1. Bilinear Maps

Definition 1. Let $\mathbb{G}$, $\mathbb{G}_T$ be two cyclic multiplicative groups with prime order p. Let g be a generator of $\mathbb{G}$ and $e : \mathbb{G}\times\mathbb{G} \to \mathbb{G}_T$ a bilinear map with the following properties:

(1) bilinearity: for all $u, v \in \mathbb{G}$ and for all $a, b \in \mathbb{Z}$, one has $e(u^a, v^b) = e(u, v)^{ab}$;

(2) nondegeneracy: the map does not send all pairs in $\mathbb{G} \times \mathbb{G}$ to the identity in $\mathbb{G}_T$. Observe that since $\mathbb{G}, \mathbb{G}_T$ are groups of prime order, this implies that if g is a generator of $\mathbb{G}$ then $e(g, g)$ is a generator of $\mathbb{G}_T$.

We say that $\mathbb{G}$ is a bilinear group if the group operation in $\mathbb{G}$ and the bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ are both efficiently computable.

Bilinear maps are also called pairings. We assume that there is an efficient algorithm $\mathcal{G}$ for generating bilinear groups. The algorithm $\mathcal{G}$, on input a security parameter λ, outputs a tuple $G = [p, \mathbb{G}, \mathbb{G}_1, g \in \mathbb{G}, e]$, where g is a generator and $\log(p) = \Theta(\lambda)$.

2.2. Algorithms. An IBE system consists of the following four algorithms: Setup, KeyGen, Encrypt, and Decrypt.

Setup(1^λ). This algorithm takes as input the security parameter λ and outputs a public key PK and a master secret key MK. The public key implies also a key space $\mathcal{K}(\text{PK})$ and an identity space $\mathcal{ID}(\text{PK})$.

KeyGen(MK, $\mathcal{I}$). This algorithm takes as input the master secret key MK and an identity $\mathcal{I} \in \mathcal{ID}(\text{PK})$ and outputs a secret key $\text{SK}_{\mathcal{I}}$ associated with $\mathcal{I}$.

Encrypt(PK, $\mathcal{I}$, M). This algorithm takes as input the public key PK, an identity $\mathcal{I}$, and a message M and outputs a ciphertext CT.

Decrypt($\text{SK}_{\mathcal{I}}$, CT). This algorithm takes as input a secret key $\text{SK}_{\mathcal{I}}$ and the ciphertext CT. If the ciphertext is an encryption to $\mathcal{I}$, then the algorithm outputs the encrypted message M.

2.3. Security Models. The chosen plaintext security (semantic security) and anonymity of an IBE system are defined according to the following IND-ID-CPA (indistinguishability against full identity and chosen plaintext attacks) game and ANON-ID-CPA (anonymity against full identity and chosen plaintext attacks) game, respectively.

IND-ID-CPA Game

Setup. The challenger $\mathcal{B}$ runs the Setup algorithm and gives PK to the adversary $\mathcal{A}$.

Phase 1. The adversary $\mathcal{A}$ submits an identity $\mathcal{I}$. The challenger creates a secret key $\text{SK}_{\mathcal{I}}$ for that identity and gives it to the adversary.

Challenge. $\mathcal{A}$ submits a challenge identity $\mathcal{I}^*$ and two equal length messages M_0, M_1 to $\mathcal{B}$ with the restriction that each identity $\mathcal{I}$ given out in the key phase must not be $\mathcal{I}^*$. Then

$\mathcal{B}$ flips a random coin $\beta \in \{0,1\}$ and passes the ciphertext $\mathrm{CT}^* = \mathrm{Encrypt}(\mathrm{PK}, M_\beta, \mathcal{I}^*)$ to $\mathcal{A}$.

Phase 2. Phase 1 is repeated with the restriction that any queried identity $\mathcal{I}$ is not $\mathcal{I}^*$.

Guess. $\mathcal{A}$ outputs its guess β' of β.

The advantage of $\mathcal{A}$ in this game is defined as $\mathrm{Adv}_{\mathcal{A}} = |\Pr[\beta' = \beta] - (1/2)|$.

Definition 2. One says that an IBE system is IND-ID-CPA secure, if no probabilistic polynomial time adversary $\mathcal{A}$ has a nonnegligible advantage in winning the IND-ID-CPA game.

ANON-ID-CPA Game

Setup. The challenger $\mathcal{B}$ runs the Setup algorithm and gives PK to the adversary $\mathcal{A}$.

Phase 1. The adversary $\mathcal{A}$ submits an identity $\mathcal{I}$. The challenger creates a secret key $\mathrm{SK}_{\mathcal{I}}$ for that identity and gives it to the adversary.

Challenge. $\mathcal{A}$ submits two challenge identities $\mathcal{I}_0^*, \mathcal{I}_1^*$ and a message M to $\mathcal{B}$ with the restriction that each identity $\mathcal{I}$ given out in the key phase must not be $\mathcal{I}_0^*$ or $\mathcal{I}_1^*$. Then $\mathcal{B}$ flips a random coin $\mu \in \{0,1\}$ and passes the ciphertext $\mathrm{CT}^* = \mathrm{Encrypt}(\mathrm{PK}, M, \mathcal{I}_\mu^*)$ to $\mathcal{A}$.

Phase 2. Phase 1 is repeated with the restriction that any queried identity $\mathcal{I}$ is not $\mathcal{I}_0^*$ or $\mathcal{I}_1^*$.

Guess. $\mathcal{A}$ outputs its guess μ' of μ.

The advantage of $\mathcal{A}$ in this game is defined as $\mathrm{Adv}_{\mathcal{A}} = |\Pr[\mu' = \mu] - (1/2)|$.

Definition 3. One says that an IBE system is ANON-ID-CPA secure, if no probabilistic polynomial time adversary $\mathcal{A}$ has a nonnegligible advantage in winning the ANON-ID-CPA game.

Some systems such as [8, 27] use weaker notions called IND-sID-CPA (indistinguishability against selective identity and chosen plaintext attacks) security and ANON-sID-CPA (anonymity against selective identity and chosen plaintext attacks) security, which are against selective identity. In the selective identity models, the adversary submits the target identity $\mathcal{I}^*$ (or $\mathcal{I}_1^*$, $\mathcal{I}_2^*$) before public parameters are generated.

3. Analysis of Anonymity

Most IBE systems are constructed on bilinear maps. However, it is hard to construct anonymous IBE systems due to the bilinearity of bilinear maps, that is, for all $u, v \in \mathbb{G}$ and for all $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u^b, v^a)$. For pairing-based IBE systems, it is easy for us to test the target identity if an IBE system is not anonymous. Roughly speaking, if an IBE system is not anonymous, supposing that $C_1, \ldots, C_k \in \mathbb{G}$ are components of a ciphertext of such a system, we can construct elements $a_1, \ldots, a_k \in \widehat{\mathbb{G}}$ from the public parameters and some identity $\mathcal{I}$ to check whether $e(C_1, a_1) \cdots e(C_k, a_k) = 1$, where $e : \mathbb{G} \times \widehat{\mathbb{G}} \to \mathbb{G}_T$ denotes the bilinear map used in the system. If the equation is true, the target identity is $\mathcal{I}$. Using this method, we can easily see that some previous IBE systems are not anonymous, such as [4–7, 10, 11].

Gentry proposed the concept of ANON-IND-ID-CPA (anonymity and indistinguishability against full identity and chosen plaintext attacks) security in [9] which is the conjunction of IND-ID-CPA security and ANON-ID-CPA security. It seems that Gentry's definition is equivalent to IND-ID-CPA security and ANON-ID-CPA security, but there is a flaw which makes them not equivalent. To make up this flaw in Gentry's definition, we first review Gentry's definition and rewrite these definitions using the indistinguishability between some similar security games.

ANON-IND-ID-CPA Game

Setup. The challenger $\mathcal{B}$ runs the Setup algorithm and gives PK to the adversary $\mathcal{A}$.

Phase 1. The adversary $\mathcal{A}$ submits an identity $\mathcal{I}$. The challenger creates a secret key $\mathrm{SK}_{\mathcal{I}}$ for that identity and gives it to the adversary.

Challenge. $\mathcal{A}$ submits two challenge identities $\mathcal{I}_0^*, \mathcal{I}_1^*$ and two equal length message M_0, M_1 to $\mathcal{B}$ with the restriction that each identity $\mathcal{I}$ given out in the key phase must not be $\mathcal{I}_0^*$ or $\mathcal{I}_1^*$. Then $\mathcal{B}$ picks two random bits $\beta, \mu \in \{0,1\}$ and passes the ciphertext $\mathrm{CT}^* = \mathrm{Encrypt}(\mathrm{PK}, M_\beta, \mathcal{I}_\mu^*)$ to $\mathcal{A}$.

Phase 2. Phase 1 is repeated with the restriction that any queried identity $\mathcal{I}$ is not $\mathcal{I}_0^*$ or $\mathcal{I}_1^*$.

Guess. $\mathcal{A}$ outputs its guess β' of β and μ' of μ.

The advantage of $\mathcal{A}$ in this game is defined as $\mathrm{Adv}_{\mathcal{A}} = |\Pr[\beta' = \beta \wedge \mu' = \mu] - (1/4)|$.

Definition 4. One says that an IBE system is ANON-IND-ID-CPA secure, if no probabilistic polynomial time adversary $\mathcal{A}$ has a nonnegligible advantage in winning the ANON-IND-ID-CPA game.

Though the ANON-IND-ID-CPA game is the conjunction of the IND-ID-CPA game and the ANON-ID-CPA game, they are not always equivalent. If the assumption used in the IND-ID-CPA game is different from the assumption used in the ANON-ID-CPA game, these two games cannot be combined to be the ANON-IND-ID-CPA game. In Gentry's definition, they are equivalent because only one assumption called the Decision q-ABDHE assumption is used in these games.

To cover the difference caused by different assumptions and full or selective security, we focus on the core of these games. In the IND-ID-CPA game, the adversary needs to distinguish an encryption of the chosen message from an encryption of a random message both for the challenge identity, while in the ANON-ID-CPA game, the adversary

needs to distinguish an encryption for the challenge identity from an encryption for a random identity both of the chosen message. And in the combined ANON-IND-ID-CPA game, the adversary needs to distinguish an encryption of the chosen message for the challenge identity from an encryption of a random message for a random identity. Hence, we can redefine these concepts using the indistinguishability between different challenge ciphertexts.

Let M be a message and $\mathcal{I}^*$ a challenge identity both chosen by the adversary. Let M_R be a random message and $\mathcal{I}_R$ a random identity. We define the following games which differ on what challenge ciphertext is given by the simulator to the adversary.

(i) $\text{Game}_{M,\mathcal{I}^*}$: it is the basic game. The challenger runs the Setup algorithm and gives the public key to the adversary. The adversary can make a secret key query for $\mathcal{I}$, where $\mathcal{I}$ is not equal to the target identity $\mathcal{I}^*$. The challenge ciphertext is Encrypt(PK, M, $\mathcal{I}^*$).

(ii) $\text{Game}_{M_R,\mathcal{I}^*}$: this is like $\text{Game}_{M,\mathcal{I}^*}$ except that the challenge ciphertext is Encrypt(PK, M_R, $\mathcal{I}^*$).

(iii) $\text{Game}_{M,\mathcal{I}_R}$: this is like $\text{Game}_{M,\mathcal{I}^*}$ except that the challenge ciphertext is Encrypt(PK, M, $\mathcal{I}_R$).

(iv) $\text{Game}_{M_R,\mathcal{I}_R}$: this is like $\text{Game}_{M,\mathcal{I}^*}$ except that the challenge ciphertext is Encrypt(PK, M_R, $\mathcal{I}_R$).

Using the indistinguishability between these games, we rewrite the definitions of ANON-IND-ID-CPA, IND-ID-CPA, and ANON-ID-CPA securities as follows.

Definition 5. One says that an IBE system is ANON-IND-ID-CPA secure, if no probabilistic polynomial time adversary $\mathcal{A}$ has a nonnegligible advantage in distinguishing between $\text{Game}_{M,\mathcal{I}^*}$ and $\text{Game}_{M_R,\mathcal{I}_R}$.

Definition 6. One says that an IBE system is IND-ID-CPA secure, if no probabilistic polynomial time adversary $\mathcal{A}$ has a nonnegligible advantage in distinguishing between $\text{Game}_{M,\mathcal{I}^*}$ and $\text{Game}_{M_R,\mathcal{I}^*}$.

Definition 7. One says that an IBE system is ANON-ID-CPA secure, if no probabilistic polynomial time adversary $\mathcal{A}$ has a nonnegligible advantage in distinguishing between $\text{Game}_{M,\mathcal{I}^*}$ and $\text{Game}_{M,\mathcal{I}_R}$.

Definitions for selective identity are similar except that in all the games the adversary should submit the target identity $\mathcal{I}^*$ before public parameters are generated. Note that $\text{Game}_{M_R,\mathcal{I}^*}$, $\text{Game}_{M,\mathcal{I}_R}$, and $\text{Game}_{M_R,\mathcal{I}_R}$ are three different games. We have the following result for the relation between ANON-IND-ID-CPA security, IND-ID-CPA security, and ANON-ID-CPA security.

Lemma 8. *If an IBE system $\mathcal{E}$ is IND-ID-CPA secure and ANON-ID-CPA secure, then $\mathcal{E}$ is ANON-IND-ID-CPA secure.*

Proof. We have

$$\left|\text{Game}_{M,\mathcal{I}^*}\text{Adv}_{\mathcal{A}} - \text{Game}_{M_R,\mathcal{I}^*}\text{Adv}_{\mathcal{A}}\right| \le \epsilon_1, \quad (1)$$

$$\left|\text{Game}_{M_R,\mathcal{I}^*}\text{Adv}_{\mathcal{A}} - \text{Game}_{M_R,\mathcal{I}_R}\text{Adv}_{\mathcal{A}}\right| \le \epsilon_2, \quad (2)$$

where ϵ_1, ϵ_2 are both negligible. Equation (1) holds because $\mathcal{E}$ is IND-ID-CPA secure and (2) holds because $\mathcal{E}$ is ANON-ID-CPA secure. So

$$\left|\text{Game}_{M,\mathcal{I}^*}\text{Adv}_{\mathcal{A}} - \text{Game}_{M_R,\mathcal{I}_R}\text{Adv}_{\mathcal{A}}\right| \le \epsilon_1 + \epsilon_2, \quad (3)$$

which means that $\mathcal{E}$ is ANON-IND-ID-CPA secure. □

However, it is still unknown whether ANON-IND-ID-CPA security is equivalent to IND-ID-CPA security and ANON-ID-CPA security. The following lemma is an efficient method to prove the anonymity, which is used for some previous systems, such as Caro-Iovino-Persiano HIBE system [28], Seo-Cheon HIBE system [29].

Lemma 9. *If an IBE system $\mathcal{E}$ is IND-ID-CPA secure, and there is no polynomial time adversary who can distinguish between $\text{Game}_{M_R,\mathcal{I}^*}$ and $\text{Game}_{M_R,\mathcal{I}_R}$ with nonnegligible advantage, then $\mathcal{E}$ is ANON-ID-CPA secure.*

Proof. We have

$$\left|\text{Game}_{M,\mathcal{I}^*}\text{Adv}_{\mathcal{A}} - \text{Game}_{M_R,\mathcal{I}^*}\text{Adv}_{\mathcal{A}}\right| \le \epsilon_1, \quad (4)$$

$$\left|\text{Game}_{M,\mathcal{I}_R}\text{Adv}_{\mathcal{A}} - \text{Game}_{M_R,\mathcal{I}_R}\text{Adv}_{\mathcal{A}}\right| \le \epsilon_2, \quad (5)$$

$$\left|\text{Game}_{M_R,\mathcal{I}^*}\text{Adv}_{\mathcal{A}} - \text{Game}_{M_R,\mathcal{I}_R}\text{Adv}_{\mathcal{A}}\right| \le \epsilon_3, \quad (6)$$

where $\epsilon_1, \epsilon_2, \epsilon_3$ are all negligible. Equations (4) and (5) hold because $\mathcal{E}$ is IND-ID-CPA secure and (6) holds according to the hypothesis. So

$$\left|\text{Game}_{M,\mathcal{I}^*}\text{Adv}_{\mathcal{A}} - \text{Game}_{M,\mathcal{I}_R}\text{Adv}_{\mathcal{A}}\right| \le \epsilon_1 + \epsilon_2 + \epsilon_3, \quad (7)$$

which means that $\mathcal{E}$ is ANON-ID-CPA secure. □

In some anonymous IBE systems, such as Boyen-Waters anonymous IBE system, they use a new game called $\text{Game}_{\text{Random}}$. We define it as follows.

(i) $\text{Game}_{\text{Random}}$: this is like $\text{Game}_{M,\mathcal{I}^*}$ except that the challenge ciphertext consists of independent random group elements.

Note that $\text{Game}_{\text{Random}}$ is different from $\text{Game}_{M_R,\mathcal{I}_R}$. Though they are similar concepts, they are not always equivalent. $\text{Game}_{\text{Random}}$ is a special game in which the challenge ciphertext is composed of independent random group elements, while the challenge ciphertext of $\text{Game}_{M_R,\mathcal{I}_R}$ is still a valid ciphertext. Since every element is random, the ciphertext leaks no information about the identity. So if the transition from $\text{Game}_{M,\mathcal{I}^*}$ to $\text{Game}_{\text{Random}}$ is computationally indistinguishable, the IBE system is no doubt anonymous. This proof method was used in Boyen-Waters anonymous IBE system and later anonymous IBE systems. Obviously, the

transition from $\text{Game}_{M,\mathcal{I}^*}$ to $\text{Game}_{M,\mathcal{I}_R}$ is different from the transition from $\text{Game}_{M,\mathcal{I}^*}$ to $\text{Game}_{\text{Random}}$. The difference leads to the following classification of anonymous IBE systems.

Definition 10 (weak anonymity). One says that an IBE system has weak anonymity, if no probabilistic polynomial time adversary $\mathcal{A}$ has a nonnegligible advantage in distinguishing between $\text{Game}_{M,\mathcal{I}^*}$ and $\text{Game}_{M,\mathcal{I}_R}$ or distinguishing between $\text{Game}_{M,\mathcal{I}^*}$ and $\text{Game}_{M_R,\mathcal{I}_R}$.

Definition 11 (strong anonymity). One says that an IBE system has strong anonymity, if no probabilistic polynomial time adversary $\mathcal{A}$ has a nonnegligible advantage in distinguishing between $\text{Game}_{M,\mathcal{I}^*}$ and $\text{Game}_{\text{Random}}$.

Obviously, weak anonymity is the standard definition shown in previous articles where the target identity is indistinguishable from a random identity. It is easy to see that weak anonymity is required for all anonymous IBE systems and strong anonymity implies weak anonymity. So weak anonymity is also called standard anonymity, while strong anonymity is called superstandard anonymity. In the next section, we will analyse some IBE systems based on our definitions of anonymity. We will see that these IBE systems all have strong anonymity. To further clarify the anonymity of IBE systems, we use the difference between $\text{Game}_{M_R,\mathcal{I}_R}$ and $\text{Game}_{\text{Random}}$ to define two types of anonymity, named type 1 anonymity and type 2 anonymity. First we define the equivalence of two games. Let Game_A, Game_B be two games. If any ciphertext output by Game_A can seem as a properly distributed ciphertext output by Game_B and vice versa, we say that Game_A equals Game_B or $\text{Game}_A = \text{Game}_B$. Obviously, $\text{Game}_A = \text{Game}_B$ means that Game_A is indistinguishable from Game_B. However, if two games are indistinguishable, they are not always equivalent. For example, for any IND-IND-CPA secure IBE system, $\text{Game}_{M,\mathcal{I}^*} \neq \text{Game}_{M_R,\mathcal{I}^*}$, but they are indistinguishable according to the definition of IND-ID-CPA security.

Definition 12. For an anonymous IBE system $\mathcal{E}$, if $\text{Game}_{M_R,\mathcal{I}_R} = \text{Game}_{\text{Random}}$, one says that $\mathcal{E}$ has type 1 anonymity, or else $\mathcal{E}$ has type 2 anonymity.

If an IBE system $\mathcal{E}$ has only weak anonymity, it is obvious that $\text{Game}_{M_R,\mathcal{I}_R} \neq \text{Game}_{\text{Random}}$; that is, $\mathcal{E}$ has type 2 anonymity. So there is no type 1 anonymous IBE system with only weak anonymity. For a strongly anonymous IBE system, type 1 anonymity always means that it only needs to prove $\mathcal{E}$'s anonymity in the ANON-IND-ID-CPA game or in the ANON-ID-CPA game, while type 2 anonymity always means that $\mathcal{E}$ needs additional steps to prove strong anonymity, for example, proving the indistinguishability of transition from $\text{Game}_{M_R,\mathcal{I}_R}$ to $\text{Game}_{\text{Random}}$.

Note that there is some IBE system which has the property $\text{Game}_{M_R,\mathcal{I}_R} = \text{Game}_{\text{Random}}$, such as Boneh-Boyen IBE system. In Boneh-Boyen IBE system, a ciphertext is like $Me(g,g)^{\alpha s}$, $(u^{\mathcal{I}}h)^s$, g^s. It is easy to see that a random tuple is still a valid ciphertext for some identity and message. But as we know, Boneh-Boyen IBE system is not anonymous because there is a gap between $\text{Game}_{M,\mathcal{I}}$ and $\text{Game}_{M,\mathcal{I}_R}$.

4. Anonymity of Some IBE Systems

In this section, we analyse some IBE systems based on our definitions of anonymity. We discuss three famous anonymous IBE systems: Gentry IBE System [9], Boyen-Waters IBE system [8], and Lewko IBE System [26]. We show that these three IBE systems are all strongly anonymous but have different types.

4.1. Gentry IBE System [9]. We show that Gentry's anonymous IBE system has type 1 strong anonymity. We first briefly describe Gentry IBE system as follows.

Setup(1^λ). Given the security parameter λ, the setup algorithm first gets $(p, \mathbb{G}, \mathbb{G}_T, g, e) \leftarrow \mathcal{G}(\lambda)$. Next it chooses another random generator $h \in \mathbb{G}$ and random integer $\alpha \in \mathbb{Z}_p$. Then the setup algorithm sets $g_1 = g^\alpha$. The public key PK is published as

$$\text{PK} = (g, g_1, h), \tag{8}$$

and the master key MK is

$$\text{MK} = (\alpha). \tag{9}$$

KeyGen(MK, $\mathcal{I}$). To generate the secret key $\text{SK}_{\mathcal{I}}$ for an identity $\mathcal{I} \in \mathbb{Z}_p$, the key extract algorithm chooses random $r_{\mathcal{I}} \in \mathbb{Z}_p$ and outputs $\text{SK}_{\mathcal{I}}$ as

$$\text{SK}_{\mathcal{I}} = \left(r_{\mathcal{I}}, \left(hg^{-r_{\mathcal{I}}}\right)^{1/(\alpha-\mathcal{I})}\right). \tag{10}$$

The constraints are that $\mathcal{I} \neq \alpha$ and the PKG always uses the same random value $r_{\mathcal{I}}$ for $\mathcal{I}$.

Encrypt(PK, $\mathcal{I}$, M). To encrypt a message $M \in \mathbb{G}_T$ for an identity $\mathcal{I}$, the algorithm chooses random integers $s \in \mathbb{Z}_p$ and outputs the ciphertext CT as

$$\text{CT} = \left(M \cdot e(g,h)^{-s}, g_1^s g^{-s\cdot\mathcal{I}}, e(g,g)^s\right). \tag{11}$$

Decrypt($\text{SK}_{\mathcal{I}}$, CT). To decrypt a ciphertext $\text{CT} = (C, C_1, C_2)$ for an identity $\mathcal{I}$, using the corresponding secret key $\text{SK}_{\mathcal{I}} = (r_{\mathcal{I}}, h_{\mathcal{I}})$ outputs

$$M = C \cdot e\left(h_{\mathcal{I}}, C_1\right) \cdot C_2^{r_{\mathcal{I}}}. \tag{12}$$

Lemma 13 (see [9, Theorem 1]). *Gentry IBE system is ANON-IND-ID-CPA secure.*

Lemma 14. *For Gentry IBE system, $\text{Game}_{M_R,\mathcal{I}_R} = \text{Game}_{Random}$.*

Proof. Let $\mathcal{C}_1$ be the set of all the possible ciphertext output by $\text{Game}_{M_R,\mathcal{I}_R}$ and $\mathcal{C}_2$ the set of all the possible ciphertext outputs by $\text{Game}_{\text{Random}}$. We will show that $\mathcal{C}_1 = \mathcal{C}_2$.

Obviously, we have $\mathcal{C}_1 \subset \mathcal{C}_2$. Note that this claim is true for all IBE systems.

Next, for a random tuple (C, C_1, C_2), where $C_1 \in \mathbb{G}$ and $C, C_2 \in \mathbb{G}_T$, we say that it is a valid ciphertext of Gentry-AIBE system. At first we can set $C_2 = e(g,g)^s$ for some s and then we can set $C_1 = g_1^s g^{-s\cdot\mathcal{I}}$ for some identity $\mathcal{I}$ and $C = M \cdot e(g, h)^{-s}$ for some message M. So we have $\mathscr{C}_2 \subset \mathscr{C}_1$.

As a result, $\mathscr{C}_1 = \mathscr{C}_2$. This means that the challenge ciphertext output by Game_{M_R,I_R} can seem as a challenge ciphertext by $\text{Game}_{\text{Random}}$ and vice versa. Then for Gentry-AIBE system, $\text{Game}_{M_R,I_R} = \text{Game}_{\text{Random}}$. □

From Lemmas 13 and 14, we get the following result.

Theorem 15. *Gentry IBE system has type 1 strong anonymity.*

4.2. Boyen-Waters IBE System [8]. For an anonymous IBE system, equation $\text{Game}_{M_R,\mathcal{I}_R} = \text{Game}_{\text{Random}}$ means that it is intrinsically strongly anonymous, just as we showed for Gentry IBE system in the previous section. The equation also holds for some previous systems, for example, Boneh-Franklin IBE system. But for some strongly anonymous IBE systems, it does not hold; that is, $\text{Game}_{M_R,I_R} \neq \text{Game}_{\text{Random}}$. In fact, these two games are *computationally* indistinguishable under some assumption, for example, the decisional linear assumption.

As an example, we will show that Boyen-Waters anonymous IBE system is a type 2 anonymous IBE system; that is, it does not satisfy the equation. We first briefly describe Boyen-Waters IBE system as follows.

Setup(1^λ). Given the security parameter λ, the setup algorithm first gets $(p, \mathbb{G}, \mathbb{G}_T, g, e) \leftarrow \mathcal{G}(\lambda)$. Next it chooses another two random group elements $g_0, g_1 \in \mathbb{G}$ and five random integers $\omega, t_1, t_2, t_3, t_4 \in \mathbb{Z}_p$. Then the setup algorithm sets $\Omega = e(g,g)^{t_1 t_2 \omega}$, $v_1 = g^{t_1}$, $v_2 = g^{t_2}$, $v_3 = g^{t_3}$, $v_4 = g^{t_4}$. The public key PK is published as

$$\text{PK} = \left(\Omega, g, g_0, g_1, v_1, v_2, v_3, v_4\right), \tag{13}$$

and the master key MK is

$$\text{MK} = \left(\omega, t_1, t_2, t_3, t_4\right). \tag{14}$$

KeyGen(MK, $\mathcal{I}$). To generate the secret key $\text{SK}_{\mathcal{I}}$ for an identity $\mathcal{I} \in \mathbb{Z}_p$, the key extract algorithm chooses random $r_1, r_2 \in \mathbb{Z}_p$ and outputs $\text{SK}_{\mathcal{I}}$ as

$$\begin{aligned}\text{SK}_{\mathcal{I}} = \Big(&g^{r_1 t_1 t_2 + r_2 t_3 t_4}, g^{-\omega t_2}\left(g_0 g_1^{\mathcal{I}}\right)^{-r_1 t_2}, g^{-\omega t_1}\left(g_0 g_1^{\mathcal{I}}\right)^{-r_1 t_1},\\ &\left(g_0 g_1^{\mathcal{I}}\right)^{-r_2 t_4}, \left(g_0 g_1^{\mathcal{I}}\right)^{-r_2 t_3}\Big).\end{aligned} \tag{15}$$

Encrypt(PK, $\mathcal{I}$, M). To encrypt a message $M \in \mathbb{G}_T$ for an identity $\mathcal{I}$, the algorithm chooses random integers $s, s_1, s_2 \in \mathbb{Z}_p$ and outputs the ciphertext CT as

$$\text{CT} = \left(M\Omega^s, \left(g_0 g_1^{\mathcal{I}}\right)^s, v_1^{s-s_1}, v_2^{s_1}, v_3^{s-s_2}, v_4^{s_2}\right). \tag{16}$$

Decrypt($\text{SK}_{\mathcal{I}}$, CT). To decrypt a ciphertext $\text{CT} = (C, C_1, C_2, C_3, C_4, C_5)$ for an identity $\mathcal{I}$, using the corresponding secret key $\text{SK}_{\mathcal{I}} = (d_1, d_2, d_3, d_4, d_5)$ outputs

$$\begin{aligned}M = C &\cdot e\left(d_1, C_1\right) \cdot e\left(d_2, C_2\right) \cdot e\left(d_3, C_3\right)\\ &\cdot e\left(d_4, C_4\right) \cdot e\left(d_5, C_5\right).\end{aligned} \tag{17}$$

Using the conjunction of Lemmas 1, 2, and 3 in [8], we have the following result for Boyen-Waters IBE system.

Lemma 16. *For Boyen-Waters IBE system, $\text{Game}_{M,\mathcal{I}^*}$ and Game_{Random} are computationally indistinguishable under the decisional BDH and decisional linear assumptions.*

Now we show that Boyen-Waters IBE system has type 2 anonymity.

Lemma 17. *For Boyen-Waters IBE system, $\text{Game}_{M_R,\mathcal{I}_R} \neq \text{Game}_{Random}$.*

Proof. Given a random tuple $(R, R_1, R_2, R_3, R_4, R_5)$ where $R \in \mathbb{G}_T$ and $R_1, \ldots, R_5 \in \mathbb{G}$, we say that it has at most $1/p$ probability to be a valid ciphertext of BW-AIBE system. At first we set $R_3 = v_2^{s_1}$ and $R_5 = v_4^{s_2}$ for some s_1 and s_2, respectively, and then we can set $R_2 = v_1^{s-s_1}$ for some s, but a valid ciphertext requires that $R_4 = v_3^{s-s_2}$. Since R_4 is a random element of $\mathbb{G}$, so R_4 has only $1/p$ probability to be $v_3^{s-s_2}$. When $R_4 \neq v_3^{s-s_2}$, the random tuple cannot be a valid ciphertext which means that $\text{Game}_{M_R,I_R} \neq \text{Game}_{\text{Random}}$. □

From Lemmas 16 and 17, we can easily get the following result.

Theorem 18. *Boyen-Waters IBE system has type 2 strong anonymity.*

4.3. Lewko IBE System [26]. Boyen-Waters IBE system only has selective security. We now show that a fully secure IBE system, Lewko IBE system, has type 2 full anonymity. Lewko IBE system is constructed from dual orthonormal bases and can seem as a translation of Lewko-Waters IBE system [11] in prime order groups. In Lewko's original description, she only gave a proof for chosen plaintext security.

Lewko IBE system is constructed on dual orthonormal bases of dual pairing vector spaces. We first review vectors of group elements. Given a group element $g \in \mathbb{G}$ and a vector $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}_p^n$, we write $g^{\mathbf{v}}$ to denote a n-tuple of elements of $\mathbb{G}$: $g^{\mathbf{v}} := (g^{v_1}, \ldots, g^{v_n})$. For any $a \in \mathbb{Z}_p$ and $\mathbf{v}, \mathbf{w} \in \mathbb{Z}_p^n$, we have $(g^{\mathbf{v}})^a = g^{a\mathbf{v}} = (g^{av_1}, \ldots, g^{av_n})$ and $g^{\mathbf{v}+\mathbf{w}} = (g^{v_1+w_1}, \ldots, g^{v_n+w_n})$. We also use e_n to denote the pairing of vectors:

$$e_n\left(g^{\mathbf{v}}, g^{\mathbf{w}}\right) := \prod_{i=1}^{n} e\left(g^{v_i}, g^{w_i}\right) = e(g,g)^{\mathbf{v}\cdot\mathbf{w}}. \tag{18}$$

For a fixed (constant) dimension n, we choose two random bases $\mathbb{B} := (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ and $\mathbb{B}^* := (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of $\mathbb{Z}_p^{n\times n}$, subject to the constraint that

$$\mathbf{b}_i \cdot \mathbf{b}_j^* = \begin{cases} 0, & i \neq j \\ \psi, & i = j \end{cases} \pmod p. \tag{19}$$

$(\mathbb{B}, \mathbb{B}^*)$ are called *dual orthonormal bases* and $\mathrm{Dual}(\mathbb{Z}_p^n)$ denotes the set of dual orthonormal bases. We then describe Lewko IBE system as follows.

Setup(1^λ). Given the security parameter λ, the setup algorithm first gets $(p, \mathbb{G}, \mathbb{G}_T, g, e) \leftarrow \mathcal{G}(\lambda)$. Next it chooses random dual orthonormal bases $(\mathbb{D}, \mathbb{D}^*)$ from $\mathrm{Dual}(\mathbb{Z}_p^6)$. Let $\mathbb{D} = (\mathbf{d}_1, \ldots, \mathbf{d}_6)$ and $\mathbb{D} = (\mathbf{d}_1^*, \ldots, \mathbf{d}_6^*)$. It also chooses random values $\alpha, \theta, \sigma \in \mathbb{Z}_p$. The public key is published as

$$\mathrm{PK} = \left(p, \mathbb{G}, \Omega = e(g,g)^{\alpha\theta\mathbf{d}_1\cdot\mathbf{d}_1^*}, g^{\mathbf{d}_1}, \ldots, g^{\mathbf{d}_4}\right), \tag{20}$$

and the master key is

$$\mathrm{MK} = \left(g^{\theta\mathbf{d}_1^*}, g^{\alpha\theta\mathbf{d}_1^*}, g^{\theta\mathbf{d}_2^*}, g^{\sigma\mathbf{d}_3^*}, g^{\sigma\mathbf{d}_4^*}\right). \tag{21}$$

KeyGen(MK, $\mathcal{I}$). The key generation algorithm chooses random $r_1, r_2 \in \mathbb{Z}_p$ and outputs the secret key as

$$\mathrm{SK}_{\mathcal{I}} := g^{(\alpha + r_1\mathcal{I})\theta\mathbf{d}_1^* - r_1\theta\mathbf{d}_2^* + r_2\mathcal{I}\sigma\mathbf{d}_3^* - r_2\sigma\mathbf{d}_4^*}. \tag{22}$$

Encrypt(PK, $\mathcal{I}$, M). To encrypt a message $M \in \mathbb{G}_T$ for an identity $\mathcal{I}$, the algorithm chooses random integers $s_1, s_2 \in \mathbb{Z}_p$ and outputs the ciphertext as

$$\mathrm{CT} = \left(C_1 := M\Omega^{s_1}, C_2 := g^{s_1\mathbf{d}_1 + s_1\cdot\mathcal{I}\mathbf{d}_2 + s_2\mathbf{d}_3 + s_2\cdot\mathcal{I}\mathbf{d}_4}\right). \tag{23}$$

Decrypt($\mathrm{SK}_{\mathcal{I}}$, CT). The decryption algorithm computes the message as

$$M = \frac{C_1}{e_n\left(\mathrm{SK}_{\mathcal{I}}, C_2\right)}. \tag{24}$$

Security proof of Lewko IBE system used the dual system encryption technique [10]. Its semifunctional keys are like $g^{(\alpha+r_1\mathcal{I})\theta\mathbf{d}_1^* - r_1\theta\mathbf{d}_2^* + r_2\mathcal{I}\sigma\mathbf{d}_3^* - r_2\sigma\mathbf{d}_4^* + t_5\mathbf{d}_5^* + t_6\mathbf{d}_6^*}$ and its semifunctional ciphertext is $(M\Omega^{s_1}, g^{s_1\mathbf{d}_1 + w\mathbf{d}_2 + s_2\mathbf{d}_3 + s_2\cdot\mathcal{I}\mathbf{d}_4 + s_5\mathbf{d}_5 + s_6\mathbf{d}_6})$ where $t_5, t_6, s_5, s_6 \overset{R}{\leftarrow} \mathbb{Z}_p$. Let $\mathrm{Game}_{\mathrm{Final}}$ be the game, where all returned keys are semifunctional and the challenge ciphertext is $(R, g^{s_1\mathbf{d}_1 + w\mathbf{d}_2 + s_2\mathbf{d}_3 + s_2\cdot\mathcal{I}\mathbf{d}_4 + s_5\mathbf{d}_5 + s_6\mathbf{d}_6})$, where $R \overset{R}{\leftarrow} \mathbb{G}_T$ and $w, s_5, s_6 \overset{R}{\leftarrow} \mathbb{Z}_p$. In [26], Lewko showed that $\mathrm{Game}_{M,\mathcal{I}}$ is indistinguishable from $\mathrm{Game}_{\mathrm{Final}'}$ under the subspace assumption. We continue her work and show that her IBE system has type 2 strong anonymity.

We first review the subspace assumption introduced by Lewko in [26].

Definition 19. Given a group generation $\mathcal{G}$, one defines the following distribution:

$$\begin{aligned}
&G := \left(p, \mathbb{G}, \mathbb{G}_T, g, e\right) \overset{R}{\longleftarrow} \mathcal{G},\\
&\left(\mathbb{B}, \mathbb{B}^*\right) \overset{R}{\longleftarrow} \mathrm{Dual}\left(\mathbb{Z}_p^n\right), \eta, \beta, \tau_1, \tau_2, \tau_3, \mu_1, \mu_2, \mu_3 \overset{R}{\longleftarrow} \mathbb{Z}_p,\\
&U_1 := g^{\mu_1\mathbf{b}_1 + \mu_2\mathbf{b}_{k+1} + \mu_3\mathbf{b}_{2k+1}},\\
&U_2 := g^{\mu_1\mathbf{b}_2 + \mu_2\mathbf{b}_{k+2} + \mu_3\mathbf{b}_{2k+2}}, \ldots,\\
&U_k := g^{\mu_1\mathbf{b}_k + \mu_2\mathbf{b}_{2k} + \mu_3\mathbf{b}_{3k}},\\
&V_1 := g^{\tau_1\eta\mathbf{b}_1^* + \tau_2\beta\mathbf{b}_{k+1}^*},\\
&V_2 := g^{\tau_1\eta\mathbf{b}_2^* + \tau_2\beta\mathbf{b}_{k+2}^*}, \ldots,\\
&V_k := g^{\tau_1\eta\mathbf{b}_k^* + \tau_2\beta\mathbf{b}_{2k}^*},\\
&W_1 := g^{\tau_1\eta\mathbf{b}_1^* + \tau_2\beta\mathbf{b}_{k+1}^* + \tau_3\mathbf{b}_{2k+1}^*},\\
&W_2 := g^{\tau_1\eta\mathbf{b}_2^* + \tau_2\beta\mathbf{b}_{k+2}^* + \tau_3\mathbf{b}_{2k+2}^*}, \ldots,\\
&W_k := g^{\tau_1\eta\mathbf{b}_k^* + \tau_2\beta\mathbf{b}_{2k}^* + \tau_3\mathbf{b}_{3k}^*},\\
&\vec{D} := \left(g^{\mathbf{b}_1}, g^{\mathbf{b}_2}, \ldots, g^{\mathbf{b}_{2k}}, g^{\mathbf{b}_{3k+1}}, \ldots, g^{\mathbf{b}_n}, g^{\eta\mathbf{b}_1^*}, \ldots,\right.\\
&g^{\eta\mathbf{b}_k^*}, g^{\beta\mathbf{b}_{k+1}^*}, \ldots, g^{\beta\mathbf{b}_{2k}^*}, g^{\mathbf{b}_{2k+1}^*}, \ldots,\\
&\left.g^{\mathbf{b}_n^*}, U_1, U_2, \ldots, U_k, \mu_3\right).
\end{aligned} \tag{25}$$

We define the advantage of an algorithm $\mathcal{A}$ in breaking the subspace assumption to be

$$\left|\Pr\left[\mathcal{A}\left(\vec{D}, V_1, \ldots, V_k\right) = 1\right] - \Pr\left[\mathcal{A}\left(\vec{D}, W_1, \ldots, W_k\right) = 1\right]\right|. \tag{26}$$

We say that the subspace assumption holds if no probabilistic polynomial time algorithm has a nonnegligible advantage in breaking the subspace assumption.

Lemma 20. *Let $\mathrm{Game}_{\mathrm{Final}'}$ be the game, where all returned keys are semifunctional and the challenge ciphertext is $(R, g^{s_1\mathbf{d}_1 + w_2\mathbf{d}_2 + s_2\mathbf{d}_3 + w_4\mathbf{d}_4 + s_5\mathbf{d}_5 + s_6\mathbf{d}_6})$, where $R \overset{R}{\leftarrow} \mathbb{G}_T$ and $w_2, w_4, s_5, s_6 \overset{R}{\leftarrow} \mathbb{Z}_p$. If there exists a polynomial time algorithm $\mathcal{A}$, where $\mathrm{Game}_{\mathrm{Final}}Adv_{\mathcal{A}} - \mathrm{Game}_{\mathrm{Final}'}Adv_{\mathcal{A}} = \epsilon$, then we can construct a polynomial time algorithm $\mathcal{B}$ with advantage ϵ to break the subspace assumption with $n = 6$ and $k = 1$.*

Proof. $\mathcal{B}$ is given $D := (g^{\mathbf{b}_1}, g^{\mathbf{b}_2}, g^{\mathbf{b}_4}, g^{\mathbf{b}_5}, g^{\mathbf{b}_6}, g^{\eta\mathbf{b}_1^*}, g^{\beta\mathbf{b}_2^*}, g^{\mathbf{b}_3^*}, g^{\mathbf{b}_4^*}, g^{\beta\mathbf{b}_5^*}, g^{\beta\mathbf{b}_6^*}, U_1, \mu_3)$ along with T_1. $\mathcal{B}$ should decide whether T_1 is distributed as $g^{\tau_1\eta\mathbf{b}_1^* + \tau_2\beta\mathbf{b}_2^*}$ or as $g^{\tau_1\eta\mathbf{b}_1^* + \tau_2\beta\mathbf{b}_2^* + \tau_3\mathbf{b}_3^*}$.

At first $\mathcal{B}$ implicitly sets $\mathbf{d}_1 = \mathbf{b}_6^*, \mathbf{d}_2 = \mathbf{b}_5^*, \mathbf{d}_3 = \mathbf{b}_4^*, \mathbf{d}_4 = \mathbf{b}_3^*, \mathbf{d}_5 = \mathbf{b}_2^*, \mathbf{d}_6 = \mathbf{b}_1^*$. Then $\mathcal{B}$ can produce $g^{\mathbf{d}_1}, \ldots, g^{\mathbf{d}_4}$ for the public parameters. Next $\mathcal{B}$ sets $\mathbf{d}_1^* = \mathbf{b}_6, \mathbf{d}_2^* = \mathbf{b}_5, \mathbf{d}_3^* = \mathbf{b}_4, \mathbf{d}_4^* = \mathbf{b}_3, \mathbf{d}_5^* = \mathbf{b}_2, \mathbf{d}_6^* = \mathbf{b}_1$. Note that $\mathcal{B}$ only does not know $g^{\mathbf{d}_4^*}$.

Table 1: Comparison.

System	Security	Anonymity degree	Anonymity type	Security model
Boneh and Franklin [2]	IND-ID-CPA ANON-ID-CPA	Strong	1	Random oracle
Boyen and Waters [8]	IND-sID-CPA ANON-sID-CPA	Strong	2	Standard
Gentry [9]	ANON-IND-ID-CPA	Strong	1	Standard
Ducas [23]	IND-sID-CPA ANON-sID-CPA	Strong	2	Standard
Lewko [26]	IND-ID-CPA ANON-ID-CPA	Strong	2	Standard
Chen et al. [24]	ANON-IND-ID-CPA	Strong	2	Standard

$\mathcal{B}$ chooses random values $\theta, \sigma, \alpha \in \mathbb{Z}_p$ for itself. It can compute $e(g,g)^{\alpha\theta \mathbf{d}_1 \cdot \mathbf{d}_1^*}$ as $(e_n(g^{\mathbf{b}_6^*}, g^{\mathbf{b}_6}))^{\alpha\theta}$. It gives $\mathcal{A}$ the public key

$$\mathrm{PK} := \mathbb{G}, p, e(g,g)^{\alpha\theta \mathbf{d}_1 \cdot \mathbf{d}_1^*}, g^{\mathbf{d}_1}, \ldots, g^{\mathbf{d}_4}. \quad (27)$$

To respond a key query for $\mathcal{I}$, $\mathcal{B}$ chooses random values $r_1, r_2', t_5', t_6' \in \mathbb{Z}_p$. It will set $r_2 = \mu_3 r_2'$. It forms the secret key as

$$\mathrm{SK}_{\mathcal{I}} := (U_1)^{\sigma r_2'} g^{(\alpha + r_1 \cdot \mathcal{I})\theta \mathbf{d}_1^* - r_1 \theta \mathbf{d}_2^* + \mu_3 r_2' \cdot \mathcal{I} \sigma \mathbf{d}_3^* + t_5' \mathbf{d}_5^* + t_6' \mathbf{d}_6^*}. \quad (28)$$

At the challenge phase, $\mathcal{B}$ receives two messages M_0, M_1 and a challenge identity $\mathcal{I}^*$. $\mathcal{B}$ chooses a random bit $b \in \{0, 1\}$, a random element $R \in \mathbb{G}_T$, and random values $w_2, s_1, s_2 \in \mathbb{Z}_p$ and sets

$$C_1 := R, \qquad C_2 := g^{s_1 \mathbf{d}_1 + w_2 \mathbf{d}_2 + s_2 \mathbf{d}_3 + s_2 \cdot \mathcal{I}^* \mathbf{d}_4} T_1. \quad (29)$$

If $T_1 = g^{\tau_1 \eta \mathbf{b}_1^* + \tau_2 \beta \mathbf{b}_2^*}$, then the exponent vector of T_1 is a random linear combination of $\mathbf{d}_5$ and $\mathbf{d}_6$, so it is in $\mathrm{Game}_{\mathrm{Final}}$. If the exponent of T_1 additionally has $\tau_3 \mathbf{b}_3^* = \tau_3 \mathbf{d}_4$, it is in $\mathrm{Game}_{\mathrm{Final}'}$. Therefore, $\mathcal{B}$ can use the output of $\mathcal{A}$ to break the subspace assumption. □

Theorem 21. *Lewko IBE system has type 2 strong anonymity.*

Proof. From Lemma 20 we know that the ciphertext of Lewko IBE system leaks no information about target identity, so it is anonymous.

Furthermore, note that $\mathbf{d}_1, \ldots, \mathbf{d}_6$ is a base of $\mathbb{Z}_p^{6\times 6}$, so $g^{s_1 \mathbf{d}_1 + w_2 \mathbf{d}_2 + s_2 \mathbf{d}_3 + w_4 \mathbf{d}_4 + s_5 \mathbf{d}_5 + s_6 \mathbf{d}_6}$ can seem a random element in $\mathbb{Z}_p^{6\times 6}$. In other words, $\mathrm{Game}_{\mathrm{Final}'} = \mathrm{Game}_{\mathrm{Random}}$. So Lewko IBE system has strong anonymity.

Obviously, the set of all possible C_2 is contained in $\mathrm{span}(g^{\mathbf{d}_1}, g^{\mathbf{d}_2}, g^{\mathbf{d}_3}, g^{\mathbf{d}_4})$. Note that any nonzero vectors in $\mathrm{span}(g^{\mathbf{d}_5}, g^{\mathbf{d}_6})$ are not included in $\mathrm{span}(g^{\mathbf{d}_1}, g^{\mathbf{d}_2}, g^{\mathbf{d}_3}, g^{\mathbf{d}_4})$, so $\mathrm{Game}_{M_R, \mathcal{I}_R} \neq \mathrm{Game}_{\mathrm{Random}}$ for Lewko IBE system which means that Lewko IBE system has type 2 anonymity. □

4.4. Comparison. Like previous analysis for Gentry IBE system, Boyen-Waters IBE system, and Lewko IBE system, we can analyse other anonymous IBE systems. A brief comparison for some anonymous IBE systems is given in Table 1. We would find that all listed IBE systems have strong anonymity, that is, superstandard anonymity. Though weak anonymity, that is, standard anonymity, is the current definition of anonymity, to the best of our knowledge, there is no IBE system having only weak anonymity. Hence we leave an open problem to construct an IBE system with only weak anonymity.

5. Conclusion

In this paper, we discuss the anonymity of identity-based encryption systems. Anonymity can be divided into two degrees: weak anonymity and strong anonymity. If an IBE system has weak anonymity, the target identity of its ciphertext cannot be distinguished from a random identity. For strongly anonymous IBE systems, the whole ciphertext cannot be distinguished from a random tuple. We also discuss the type of anonymity and divide it into two types: type 1 means that a random tuple can be seen as a valid ciphertext for some identity, while type 2 cannot. We show that some current anonymous IBE systems, such as Gentry IBE system, Boyen-Waters IBE system, and Lewko IBE system, have strong but different type of anonymity. We hope that our analysis of anonymity would help to construct more anonymous IBE and related systems.

Acknowledgments

This work was supported by Chongqing Natural Science Foundation (no. cstc2013jcyjA40019) and the authors would like to thank the anonymous referees for helpful suggestions.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, vol. 196 of *Lecture Notes in Computer Science (LNCS)*, pp. 47–53, Springer, Berlin, Germany, 1984.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology*, J. Kilian, Ed., vol. 2139 of *Lecture Notes in Computer Science (LNCS)*, pp. 213–229, Springer, Berlin, Germany, 2001.

[3] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Cryptography and Coding*, B. Honary, Ed., vol. 2260 of *Lecture Notes in Computer Science (LNCS)*, pp. 360–363, Springer, Berlin, Germany, 2001.

[4] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in *Advances in Cryptology*, E. Biham, Ed., vol. 2656 of *Lecture Notes in Computer Science (LNCS)*, pp. 255–271, Springer, Berlin, Germany, 2003.

[5] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in *Advances in Cryptology*, C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Computer Science (LNCS)*, pp. 223–238, Springer, Berlin, Germany, 2004.

[6] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in *Advances in Cryptology*, M. Franklin, Ed., vol. 3152 of *Lecture Notes in Computer Science (LNCS)*, pp. 443–459, Springer, Berlin, Germany, 2004.

[7] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology*, R. Cramer, Ed., vol. 3494 of *Lecture Notes in Computer Science (LNCS)*, pp. 114–127, Springer, Berlin, Germany, 2005.

[8] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," in *Advances in Cryptology*, C. Dwork, Ed., vol. 4117 of *Lecture Notes in Computer Science (LNCS)*, pp. 290–307, Springer, Berlin, Germany, 2006.

[9] C. Gentry, "Practical identity-based encryption without random oracles," in *Advances in Cryptology*, S. Vaudenay, Ed., vol. 4004 of *Lecture Notes in Computer Science (LNCS)*, pp. 445–464, Springer, Berlin, Germany, 2006.

[10] B. Waters, "Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology*, vol. 5677 of *Lecture Notes in Computer Science (LNCS)*, pp. 619–636, Springer, Berlin, Germany, 2009.

[11] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure hibe with short ciphertexts," in *Theory of Cryptography*, D. Micciancio, Ed., vol. 5978 of *Lecture Notes in Computer Science (LNCS)*, pp. 455–479, Springer, 2010.

[12] X. Boyen, "Multipurpose identity-based signcryption: a Swiss Army knife for identity-based cryptography," in *Advances in Cryptology*, D. Boneh, Ed., vol. 2729 of *Lecture Notes in Computer Science (LNCS)*, pp. 383–399, Springer, Berlin, Germany, 2003.

[13] M. Abdalla, M. Bellare, D. Catalano et al., "Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions," in *Advances in Cryptology*, V. shoup, Ed., vol. 3621 of *Lecture Notes in Computer Science (LNCS)*, pp. 205–222, Springer, Berlin, Germany, 2005.

[14] M. Abdalla, M. Bellare, D. Catalano et al., "Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions," *Journal of Cryptology*, vol. 21, no. 3, pp. 350–391, 2008.

[15] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology*, C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Computer Science (LNCS)*, pp. 506–522, Springer, Berlin, Germany, 2004.

[16] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Theory of cryptography*, S. Vadhan, Ed., vol. 4392 of *Lecture Notes in Computer Science (LNCS)*, pp. 535–554, Springer, Berlin, Germany, 2007.

[17] E. Shi, J. Bethencourt, T. H. H. Chan, D. Song, and A. Perrig, "Multi-dimensional range query over encrypted data," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 350–364, 2007.

[18] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *Journal of the ACM*, vol. 51, no. 4, pp. 557–594, 2004.

[19] E. Shi and B. Waters, "Delegating capabilities in predicate encryption systems," in *Automata, languages and programming. Part II*, L. Aceto, Ed., vol. 5126 of *Lecture Notes in Computer Science (LNCS)*, pp. 560–578, Springer, Berlin, Germany, 2008.

[20] K. G. Paterson and S. Srinivasan, "Security and anonymity of identity-based encryption with multiple trusted authorities," in *Pairing-Based Cryptography*, S. D. Galbraith and K. G. Paterson, Eds., vol. 5209 of *Lecture Notes in Computer Science (LNCS)*, pp. 354–375, Springer, Berlin, Germany, 2008.

[21] V. Iovino and G. Persiano, "Hidden-vector encryption with groups of prime order," in *Pairing-Based Cryptography*, S. D. Galbraith and K. G. Paterson, Eds., vol. 5209 of *Lecture Notes in Computer Science (LNCS)*, pp. 75–88, Springer, Berlin, Germany, 2008.

[22] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in *Public Key Cryptography*, vol. 5443 of *Lecture Notes in Computer Science (LNCS)*, pp. 196–214, Springer, Berlin, 2009.

[23] L. Ducas, "Anonymity from asymmetry: new constructions for anonymous HIBE," in *Topics in Cryptology*, J. Pieprzyk, Ed., vol. 5985 of *Lecture Notes in Computer Science (LNCS)*, pp. 148–164, Springer, Berlin, Germany, 2010.

[24] J. Chen, H. W. Lim, S. Ling, H. Wang, and H. Wee, "Shorter ibe and signatures via asymmetric pairings.," in *Pairing-Based Cryptography*, vol. 7708 of *Lecture Notes in Computer Science*, pp. 122–140, 2013.

[25] J. Herranz, F. Laguillaumie, and C. Rfols, "Relations between semantic security and anonymity in identitybased encryption," *Information Processing Letters*, vol. 111, no. 10, pp. 453–460, 2011.

[26] A. Lewko, "Tools for simulating features of composite order bilinear groups in the prime order setting," in *Advances in Cryptology*, vol. 7237 of *Lecture Notes in Computer Science*, pp. 318–335, 2012.

[27] J. H. Seo, T. Kobayashi, M. Ohkubo, and K. Suzuki, "Anonymous hierarchical identity-based encryption with constant size ciphertexts," in *Public key Cryptography*, S. Jarecki and G. Tsudik, Eds., vol. 5443 of *Lecture Notes in Computer Science (LNCS)*, pp. 215–234, Springer, Berlin, Germany, 2009.

[28] A. D. Caro, V. Iovino, and G. Persiano, "Fully secure anonymous hibe and secret-key anonymous ibe with short ciphertexts," in *Pairing-Based Cryptography*, vol. 6487 of *Lecture Notes in Computer Science*, pp. 347–366, 2010.

[29] J. H. Seo and J. H. Cheon, "Fully secure anonymous hierarchical identity-based encryption with constant size ciphertexts," Cryptology EPrint Archive: Report 2011/021, http://eprint.iacr.org/2011/021.