A Variant of Boyen-Waters Anonymous IBE Scheme*

Song Luo[1,3,4], Qingni Shen[2,**], Yongming Jin[3,4],
Yu Chen[5], Zhong Chen[2,3,4], and Sihan Qing[2,6]

[1] College of Computer Science and Engineering,
Chongqing University of Technology, China
[2] School of Software and Microelectronics & MoE Key Lab of Network and Software Assurance, Peking University, Beijing, China
[3] Institute of Software, School of Electronics Engineering and Computer Science, Peking University
[4] Key Laboratory of High Confidence Software Technologies (Peking University), Ministry of Education
[5] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[6] Institute of Software, Chinese Academy of Sciences, Beijing, China
{luosong,shenqn,jinym,chenyu,chen}@infosec.pku.edu.cn,
qsihan@ercist.iscas.ac.cn

Abstract. An identity-based encryption (IBE) scheme is called anonymous if the ciphertext leaks no information about the recipient's identity. In this paper, we present a novel anonymous identity-based encryption scheme. Our scheme comes from the analysis of Boyen-Waters anonymous IBE Scheme in which we find a method to construct anonymous IBE schemes. We show that Boyen-Waters anonymous IBE scheme can be transformed from BB_1-IBE scheme. Our scheme is also transformed from BB_1-IBE scheme and can be seemed as a variant of Boyen-Waters anonymous IBE scheme. The security proof shows the transformed scheme has the same semantic security as the original scheme and has anonymous security. We prove anonymity under the Decision Linear assumption.

Keywords: Identity-Based Encryption, Anonymity, Transformation.

1 Introduction

The notion of Identity-Based encryption (IBE) was first introduced by Shamir [25] to simplify the public-key infrastructure in public key encryption. Users can use arbitrary strings such as e-mail addresses, IP addresses or phone numbers to form public keys directly. All private keys are generated by private key generator (PKG). Anyone can encrypt messages using the identity, and only the owner of the corresponding secret key can decrypt the messages. But a concrete construction of IBE was not given by Shamir until Boneh and Franklin [8] presented

* Supported by National Natural Science Foundation of China (No.60873238, 61073156, 60970135, 60821003).
** Corresponding author.

S. Qing et al. (Eds.): ICICS 2011, LNCS 7043, pp. 42–56, 2011.
© Springer-Verlag Berlin Heidelberg 2011

the first practical IBE scheme using efficiently computable bilinear maps. At the same year, Cocks proposed another but less efficient IBE scheme using quadratic residues [16].

Hierarchical identity-based encryption (HIBE) [21] is a generalization of IBE that mirrors an organizational hierarchy. In HIBE systems, a parent identity of the hierarchy tree can issue secret keys to its child identities, but cannot decrypt messages intended for other identities. The first HIBE scheme was proposed by Gentry and Silverberg [20] which can be seemed as an extension of Boneh-Franklin IBE scheme. Their scheme was proved to be secure in the random oracle model. Up to now, many new secure IBE or HIBE schemes are proposed without random oracles [12, 3, 4, 5, 10, 18, 15, 14, 28, 24, 19, 22, 13].

Recently, people found the anonymity of IBE and HIBE can help to construct Public Key Encryption with Keyword Search (PEKS) schemes [7, 2, 9, 26]. Roughly speaking, an IBE or HIBE is said to be *recipient anonymous* or simply *anonymous* if the ciphertext leaks no information about the recipient's identity. Generally speaking, for pairing-based IBE schemes, we can use some equation to check whether one identity is the target identity. For example, let us see an instantiation of BB_1-IBE scheme. Let $C = M \cdot e(g_1, g_2)^s, C_1 = g^s, C_2 = (g_1^{\mathrm{ID}} h)^s$ where s is the random integer chosen by the encryptor and g, g_1, h come from the public parameter. For such an instantiation C, C_1, C_2, we can easily construct $h_1 = g_1^{\mathrm{ID}'} h$ and $h_2 = g^{-1}$ and check whether $e(C_1, h_1)e(C_2, h_2) = 1$, where $e : \mathbb{G} \times \hat{\mathbb{G}} \to \mathbb{G}_T$ denotes the bilinear map (or called "pairing") used in the scheme. If yes, then the target identity is ID'.

Generally but roughly speaking, if an IBE or HIBE scheme is *not* anonymous, supposing that $C_1, \cdots, C_k$ be components of a ciphertext of such a scheme, we can construct elements $h_1, \cdots, h_k$ from the public parameters and some identity ID to check whether $e(C_1, h_1) \cdots e(C_k, h_k) = 1$. If the equation is true, the target identity is ID. It is hard to construct anonymous IBE schemes, even more difficult for anonymous HIBE schemes. The difficulty or the feasibility of equation check roots in the bilinearity of bilinear maps, i.e., $\forall u \in \mathbb{G}, v \in \mathbb{G}_T$ and $\forall a, b \in \mathbb{Z}$, we have $e(u^a, v^b) = e(u^b, v^a)$. This is the key point why we can test whether some previous IBE or HIBE schemes are anonymous.

1.1 Our Contribution

We present a novel anonymous IBE scheme from the analysis of Boyen-Waters anonymous IBE Scheme. We find that in an IBE scheme, if the target identity in the original IBE scheme is *only* judged by the equation $e(C_1, h_1) \cdots e(C_k, h_k) = 1$ where $C_1, \cdots, C_k$ come from ciphertext and $h_1, \cdots, h_k$ are constructed from the public parameters and some identity. Then we can use the linear splitting technique in [10, 26] to make it hard to distinguish the identity from the ciphertext. Simply speaking, we divide nearly every component of the ciphertext C_i into four blind pieces $C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4}$ which makes it hard to construct corresponding elements for equation test.

Using the proposed method, we show that Boyen-Waters anonymous IBE scheme [10] can be transformed from BB_1-IBE scheme. Our scheme is also

transformed from BB_1-IBE scheme and can be considered as a variant of Boyen-Waters anonymous IBE scheme. The security proof shows the transformed scheme has the same semantic security as the original scheme and has anonymous security. And we prove anonymity under the Decision Linear assumption.

1.2 Related Works

Anonymous IBE was first noticed by Boneh et al. [7] and later formalized by Abdalla et al. [2, 1]. While there are several approaches to constructing an IBE scheme using bilinear maps, most constructions in the standard model are not recipient anonymous [12, 3, 4, 27]. BF-IBE [8] is intrinsically anonymous, but its HIBE version [20] is not anonymous. Gentry [18] proposed a concrete construction of anonymous IBE in the standard model and Boyen and Waters (BW-HIBE) [10] also proposed another anonymous IBE scheme and an anonymous HIBE scheme. Gentry's version is fully secure under a complicated and dynamic assumption and Boyen-Waters' constructions are selectively secure under the Decision BDH and the Decision Linear assumptions.

Seo et al. [24] proposed the first constant size ciphertext anonymous HIBE scheme in composite order groups. An extension of anonymous IBE, named committed blind anonymous IBE, was proposed by Camenisch et al. [11] in which a user can request the decryption key for a given identity without the key generation entity learning the identity. Recently, Caro et al. [13], Seo and Cheon [23] independently presented a new fully secure anonymous HIBE scheme with short ciphertexts in composite order groups. All of these schemes were proposed in the standard model without random oracles. Ducas [17] shows that if asymmetric bilinear maps are used in previous IBE and HIBE schemes with minor modification, anonymity can also be achieved.

1.3 Organization

The paper is organized as follows. We give necessary background information and definitions of security in Section 2. We first review Boyen-Waters anonymous IBE scheme and give an analysis in Section 3. Next we get a variant of Boyen-Waters anonymous IBE scheme in Section 4 and discuss some extensions in Section 5. Finally, we conclude the paper with Section 6.

2 Preliminaries

In this section, we briefly summarize the bilinear maps, and review the Decision Linear (D-Linear) assumption. Then we describe the concepts of IBE and its security models.

2.1 Bilinear Maps

Definition 1. *Let $\mathbb{G}$, $\mathbb{G}_1$ be two cyclic multiplicative groups with prime order p. Let g be be a generator of $\mathbb{G}$ and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ be a bilinear map with the following properties:*

1. Bilinearity: $\forall u, v \in \mathbb{G}$ *and* $\forall a, b \in \mathbb{Z}$*, we have* $e(u^a, v^b) = e(u, v)^{ab}$.

2. Non-degeneracy: The map does not send all pairs in $\mathbb{G} \times \mathbb{G}$ *to the identity in* $\mathbb{G}_1$*. Observe that since* $\mathbb{G}, \mathbb{G}_1$ *are groups of prime order this implies that if* g *is a generator of* $\mathbb{G}$ *then* $e(g, g)$ *is a generator of* $\mathbb{G}_1$.

We say that $\mathbb{G}$ *is a bilinear group if the group operation in* $\mathbb{G}$ *and the bilinear map* $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ *are both efficiently computable.*

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 Complexity Assumption

The Decision Linear (D-Linear) assumption was first proposed in [6] by Boneh, Boyen, and Shacham for group signatures. In anonymous IBE schemes, the D-Linear assumption is always used to prove anonymity.

Definition 2. *Let* $c_1, c_2 \in \mathbb{Z}_p^*$ *be chosen at random and* $g, f, \nu \in \mathbb{G}$ *be random generators. Let* Z *be a random element in* $\mathbb{G}$*. We define the advantage of an algorithm* $\mathcal{A}$ *in breaking the D-Linear assumption to be*

$$\left|\Pr[\mathcal{A}(g, f, \nu, g^{c_1}, f^{c_2}, \nu^{c_1+c_2}) = 1] - \Pr[\mathcal{A}(g, f, \nu, g^{c_1}, f^{c_2}, Z) = 1]\right|.$$

We say that the D-Linear assumption holds if no probabilistic polynomial-time algorithm has a non-negligible advantage in breaking the D-Linear assumption.

2.3 Algorithms

An IBE scheme consists of the following five algorithms: **Setup**, **KeyGen**, **Encrypt**, and **Decrypt**.

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

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

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

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

2.4 Security Models

The chosen-plaintext security (semantic security) and anonymity of an IBE scheme are defined according to the following IND-ID-CPA game and ANON-ID-CPA game, respectively.

IND-ID-CPA Game

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

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

Challenge. $\mathcal{A}$ submits a challenge identity ID^* and two equal length messages M_0, M_1 to $\mathcal{B}$ with the restriction that each identity ID given out in the key phase must not be ID^*. Then $\mathcal{C}$ flips a random coin μ and passes the ciphertext $\mathrm{CT}^* = \mathbf{Encrypt}(\mathrm{PK}, M_\mu, \mathrm{ID}^*)$ to $\mathcal{A}$.

Phase 2. Phase 1 is repeated with the restriction that any queried identity vector ID is not ID^*.

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

The advantage of $\mathcal{A}$ in this game is defined as $Adv_{\mathcal{A}} = |\Pr[\mu' = \mu] - \frac{1}{2}|$.

Definition 3. *We say that an IBE scheme is* IND-ID-CPA *secure, if no probabilistic polynomial time adversary $\mathcal{A}$ has a non-negligible advantage in winning the* IND-ID-CPA *game.*

ANON-ID-CPA Game

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

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

Challenge. $\mathcal{A}$ submits two challenge identity vectors $\mathrm{ID}_0^*, \mathrm{ID}_1^*$ and a message M to $\mathcal{B}$ with the restriction that each identity ID given out in the key phase must not be ID_0^* or ID_1^*. Then $\mathcal{C}$ flips a random coin μ and passes the ciphertext $\mathrm{CT}^* = \mathbf{Encrypt}(\mathrm{PK}, M, \mathrm{ID}_\mu^*)$ to $\mathcal{A}$.

Phase 2. Phase 1 is repeated with the restriction that any queried identity ID is not ID_0^* or ID_1^*.

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

The advantage of $\mathcal{A}$ in this game is defined as $Adv_{\mathcal{A}} = |\Pr[\mu' = \mu] - \frac{1}{2}|$.

Definition 4. *We say that an IBE scheme is* ANON-ID-CPA *secure, if no probabilistic polynomial time adversary $\mathcal{A}$ has a non-negligible advantage in winning the* ANON-ID-CPA *game.*

Some schemes such as [10, 24] use weaker notions called IND-sID-CPA secure and ANON-sID-CPA secure, which are against selective identity. In the selective identity models, the adversary submits the target identity ID^* before public parameters are generated.

3 BW-AIBE Review and Analysis

3.1 Scheme Description

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

$$\mathrm{PK} = (\Omega, g, g_0, g_1, v_1, v_2, v_3, v_4),$$

and the master key MK is

$$\mathrm{MK} = (\omega, t_1, t_2, t_3, t_4).$$

KeyGen(MK, ID). To generate the secret key $\mathrm{SK_{ID}}$ for an identity $\mathrm{ID} \in \mathbb{Z}_p$, the key extract algorithm chooses random $r_1, r_2 \in \mathbb{Z}_p$ and outputs $\mathrm{SK_{ID}}$ as

$$\mathrm{SK_{ID}} = \begin{pmatrix} g^{r_1 t_1 t_2 + r_2 t_3 t_4}, g^{-\omega t_2}(g_0 g_1^{\mathrm{ID}})^{-r_1 t_2}, g^{-\omega t_1}(g_0 g_1^{\mathrm{ID}})^{-r_1 t_1}, \\ (g_0 g_1^{\mathrm{ID}})^{-r_2 t_4}, (g_0 g_1^{\mathrm{ID}})^{-r_2 t_3} \end{pmatrix}.$$

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

$$\mathrm{CT} = (M\Omega^s, (g_0 g_1^{\mathrm{ID}})^s, v_1^{s-s_1}, v_2^{s_1}, v_3^{s-s_2}, v_4^{s_2}).$$

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

$$M = C \cdot e(d_1, C_1) \cdot e(d_2, C_2) \cdot e(d_3, C_3) \cdot e(d_4, C_4) \cdot e(d_5, C_5).$$

3.2 Analysis

As the analysis of $\mathrm{BB_1}$ scheme, for a ciphertext instance $C = M\Omega^s, C_1 = (g_0 g_1^{\mathrm{ID}})^s$, $C_2 = v_1^{s-s_1}, C_3 = v_2^{s_1}, C_4 = v_3^{s-s_2}, C_5 = v_4^{s_2}$, we need to find h_1, h_2, h_3, h_4, h_5 such that $e(C_1, h_1)\ e(C_2, h_2)\ e(C_3, h_3)\ e(C_4, h_4)\ e(C_5, h_5) = 1$ where h_1, h_2, h_3, h_4, h_5 are constructed from public parameters and the target identity ID.

However, it is not easy to find such elements. As shown in the secret key, a direct construction is that $h_1 = g^{-t_1 t_2}$, $h_2 = (g_0 g_1^{\mathrm{ID}})^{t_2}$,$h_3 = (g_0 g_1^{\mathrm{ID}})^{t_1}$, ,$h_4 = (g_0 g_1^{\mathrm{ID}})^{t_4}$,$h_5 = (g_0 g_1^{\mathrm{ID}})^{t_3}$. Unfortunately, these elements cannot be provided due to the loss of $g_0^{t_1}, g_1^{t_1}, \cdots, g_1^{t_4}, g_1^{t_4}$.

This technique is called "linear splitting", because an important element g^s (corresponding to $\mathrm{BB_1}$) is split into four parts: $v_1^{s-s_1}$, $v_2^{s_1}$, $v_3^{s-s_2}$, $v_4^{s_2}$. To make things appear clearer, we can rewrite these four elements as $g^{t_1 s} v_1^{-s_1}$, $v_2^{s_1}$, $g^{t_3 s} v_3^{-s_2}$, $v_4^{s_2}$. We can find that g^s is blinded by two elements $v_1^{-s_1}$ and $v_3^{-s_2}$. To remove the blindness factor in decryption, two extra elements $v_2^{s_1}, v_4^{s_2}$ are

provided. In the security proof of BW-AIBE, we can see that all these elements are proved "random" at the view of adversary. So if we want hide the identity in ciphertext, we can blind the related elements to be "random". In BW-AIBE, g^s is blinded. In fact, we can change the target of blinded target, for example, blinding $(g_0 g_1^{\mathrm{ID}})^s$. These analyses result in our generic construction in the next section.

3.3 Generic Construction

Let $\mathcal{E}$ be an IBE scheme and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is the bilinear map used in $\mathcal{E}$. Suppose a message $M \in \mathbb{G}_T$ is randomized as MY^s in the encryption process, where $Y \in \mathbb{G}_T$ comes from public key and $s \in \mathbb{Z}_p^*$ is randomly chosen by the encryptor. Then $\mathcal{E}$ is constructed as follows:

Setup. It outputs public key PK and master secret key MK.

KeyGen. For an identity ID, it outputs the corresponding secret key $\mathrm{SK}_{\mathrm{ID}} = (d_1, \cdots, d_n)$ where $d_1, \cdots, d_n \in \mathbb{G}$.

Encrypt. For a message $M \in \mathbb{G}_T$ and an identity ID, it outputs ciphertext $\mathrm{CT} = (C = MY^s, C_1, \cdots, C_n)$ where $C \in \mathbb{G}_T$ and $C_1, \cdots, C_n \in \mathbb{G}$.

Decrypt. $M = C \cdot e(d_1, C_1) \cdots e(d_n, C_n)$.

As stated before, we require that the target identity in the IBE scheme can be *only* judged by the equation $e(C_1, h_1) \cdots e(C_n, h_n) = 1$ where $C_1, \cdots, C_n$ come from ciphertext and $h_1, \cdots, h_n$ are constructed from the public parameters and some identity. And we also require that every $h_i \neq 1, i = 1, \cdots, n$.

Let A be a non-empty set, $t \in \mathbb{Z}_p^*$, we define $A^t := \{x^t | x \in A\}$. This notation is the same as the definition of product of sets, but can be easily distinguished from its context. Let $A \backslash B$ be the difference of A and B, i.e., $A \backslash B = \{x | x \in A \wedge x \notin B\}$. Let g be a generator of $\mathbb{G}$. We transform the above scheme to an anonymous IBE scheme as follows:

Setup. This algorithm chooses two random integers $t_1, t_2, t_3, t_4 \in \mathbb{Z}_p^*$, computes $v_1 = g^{t_1}, v_2 = g^{t_2}$, $v_3 = g^{t_3}$, $v_4 = g^{t_4}$ and outputs the public key $\{Y^{t_1 t_2}, v_1, v_2, v_3, v_4\} \cup \mathrm{PK}^{t_1} \cup \mathrm{PK}^{t_3} \backslash \{Y^{t_1}, Y^{t_3}\}$ and the master secret key $\mathrm{MK} \cup \{t_1, t_2, t_3, t_4\}$.

KeyGen. Let $h_1, \cdots, h_n$ be the elements constructed to judge the identity in the ciphertext, i.e., $e(h_1, C_1) \cdots e(h_n, C_n) = 1$ where $C_1, \cdots, C_n$ are the elements of ciphertext. Then we split the transformation into two parts. For $i = 1, \cdots, n-1$, the algorithm chooses random integer $r \in \mathbb{Z}_p^*$ and computes $d_{i,1} = d_i^{t_1}, d_{i,2} = d_i^{t_2}$, $d_{i,3} = h_i^{t_3 \cdot r}$, $d_{i,4} = h_i^{t_4 \cdot r}$. For $i = n$, it computes $d'_n = d_n^{t_1 t_2} \cdot h_n^{t_3 t_4 r}$. Then the secret key is

$$(\langle d_{i,1}, d_{i,2}, d_{i,3}, d_{i,4} \rangle_{i=1,\cdots,n-1}, d'_n).$$

Encrypt. Like **KeyGen**, we also split the transformation into two parts. For $i = 1, \cdots, n-1$, this algorithm chooses $2(n-1)$ random integers $s_{1,1}$, $s_{1,2}$, $\cdots$, $s_{n-1,1}$, $s_{n-1,2} \in \mathbb{Z}_p^*$, computes $C_{i,1} = v_2^{s_{i,1}}, C_{i,2} = v_1^{-s_{i,1}} C_i^{t_1}, C_{i,3} =$

$v_4^{s_{i,2}}, C_{i,2} = v_3^{-s_{i,2}} C_i^{t_3}$. For $i = n$, it sets $C'_n = C_n$, leaving this element unchanged. Then the ciphertext is

$$(C' = MY^{t_1 t_2 s}, \langle C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4} \rangle_{i=1,\cdots,n-1}, C'_n).$$

Decrypt. This algorithm outputs

$$M = C' \cdot \left(\prod_{i=1}^{n-1} e(d_{i,1}, C_{i,1}) \cdot e(d_{i,2}, C_{i,2}) \cdot e(d_{i,3}, C_{i,3}) \cdot e(d_{i,4}, C_{i,4}) \right) \cdot e(d'_n, C'_n).$$

Correctness: The correctness of new decryption can be easily seen as follows. Note that in the original decryption process, we have $M = C \cdot e(d_1, C_1) \cdots e(d_n, C_n)$ which implies $Y^s \cdot e(d_1, C_1) \cdots e(d_n, C_n) = 1$. For $i = 1, \cdots, n-1$, we have

$$\begin{aligned} & e(d_{i,1}, C_{i,1}) \cdot e(d_{i,2}, C_{i,2}) \cdot e(d_{i,3}, C_{i,3}) \cdot e(d_{i,4}, C_{i,4}) \\ &= e(d_i^{t_1}, v_2^{s_{i,1}}) e(d_i^{t_2}, v_1^{-s_{i,1}} C_i^{t_1}) e(h_i^{t_3 \cdot r}, v_4^{s_{i,2}}) e(h_i^{t_4 \cdot r}, v_3^{-s_{i,2}} C_i^{t_3}) \\ &= e(d_i, C_i)^{t_1 t_2} e(h_i, C_i)^{t_3 t_4 r} \end{aligned}$$

For $i = n$, we have $e(d'_n, C'_n) = e(d_n^{t_1 t_2} \cdot h_n^{t_3 t_4 r}, C_n) = e(d_n, C_n)^{t_1 t_2} \cdot e(h_n, C_n)^{t_3 t_4 r}$.

Note that $\prod_{i=1}^{n} e(h_i, C_i)^{t_3 t_4 r} = (\prod_{i=1}^{n} e(h_i, C_i))^{t_3 t_4 r} = 1$. So

$$\begin{aligned} & C' \cdot \left(\prod_{i=1}^{n-1} e(d_{i,1}, C_{i,1}) \cdot e(d_{i,2}, C_{i,2}) \cdot e(d_{i,3}, C_{i,3}) \cdot e(d_{i,4}, C_{i,4}) \right) \cdot e(d'_n, C'_n) \\ &= MY^{t_1 t_2 s} \cdot \prod_{i=1}^{n} e(d_i, C_i)^{t_1 t_2} \cdot \prod_{i=1}^{n} e(h_i, C_i)^{t_3 t_4 r} \\ &= MY^{t_1 t_2 s} \cdot e(d_1, C_1)^{t_1 t_2} \cdots e(d_n, C_n)^{t_1 t_2} \\ &= M(Y^s \cdot e(d_1, C_1) \cdots e(d_n, C_n))^{t_1 t_2} \\ &= M \end{aligned}$$

Observe that if the **Decrypt** algorithm is $M = C \cdot e(a_1, C_1) \cdots \frac{1}{e(a_k, C_k)} \cdots e(a_n, C_n)$, we don't need to modify the **Encrypt** and **Decrypt** algorithms. The **Encrypt** algorithm remains the same and the **Decrypt** algorithm is

$$\begin{aligned} & M = C \cdot e(a_{1,1}, C_{1,1}) \cdot e(a_{1,2}, C_{1,2}) \cdot e(a_{1,3}, C_{1,3}) \cdot e(a_{1,4}, C_{1,4}) \cdots \\ & \cdot \frac{1}{e(a_{k,1}, C_{k,1}) \cdot e(a_{k,2}, C_{k,2}) \cdot e(a_{k,3}, C_{k,3}) \cdot e(a_{k,4}, C_{k,4})} \cdot \\ & \cdots e(a_{n,1}, C_{n,1}) \cdot e(a_{n,2}, C_{n,2}) \cdot e(a_{n,3}, C_{n,3}) \cdot e(a_{n,4}, C_{n,4}). \end{aligned}$$

4 A Variant of BW-AIBE

We now transform the first Boneh-Boyen scheme (BB_1) [3] to an anonymous scheme. Note that BB_1 was proposed as an HIBE scheme but can be regarded as an IBE scheme with the hierarchy depth = 1. For ease of presentation, we denote the IBE and HIBE version by BB_1-IBE, BB_1-HIBE. Given an instance of BB_1-IBE ciphertext $M \cdot e(g_1, g_2)^s, g^s, (g_1^{\mathrm{ID}} h)^s$, if we leave $(g_1^{\mathrm{ID}} h)^s$ unchanged, then we can get Boyen-Waters anonymous IBE scheme (BW-AIBE). If we leave g^s unchanged, we can get a variant of BW-AIBE scheme. We denote this transformed scheme by BB_1-AIBE.

4.1 Construction

For an instance of ciphertext $C = M \cdot e(g_1, g_2)^s, C_1 = g^s, C_2 = (g_1^{\mathrm{ID}} h)^s$, we choose $h_1 = (g_1^{\mathrm{ID}} h)^{-1}$ and $h_2 = g$. It is easy to see that $e(C_1, h_1)e(C_2, h_2) = 1$. Then scheme BB_1-AIBE is constructed 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 generator $g_2, h \in \mathbb{G}$ and five random integers $\alpha, t_1, t_2, t_3, t_4 \in \mathbb{Z}_p^*$. Then the setup algorithm sets $g_1 = g^\alpha, Y = e(g_1, g_2)^{t_1 t_2}, v_1 = g^{t_1}, v_2 = g^{t_2}, v_3 = g^{t_3}, v_4 = g^{t_4}$. The public key PK is published as

$$\mathrm{PK} = (Y, g, v_1, v_2, v_3, v_4, g_1^{t_1}, h^{t_1}, g_1^{t_3}, h^{t_3}),$$

and the master key MK is

$$\mathrm{MK} = (g_2^\alpha, t_1, t_2, t_3, t_4).$$

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

$$\mathrm{SK}_{\mathrm{ID}} = (g_2^{-\alpha t_1 t_2} (g_1^{\mathrm{ID}} h)^{-r_1 t_1 t_2 - r_2 t_3 t_4}, v_1^{r_1}, v_2^{r_1}, v_3^{r_2}, v_4^{r_2}).$$

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

$$\mathrm{CT} = (MY^s, g^s, v_2^{s_1}, (g_1^{t_1 \mathrm{ID}} h^{t_1})^s v_1^{-s_1}, v_4^{s_2}, (g_1^{t_3 \mathrm{ID}} h^{t_3})^s v_3^{-s_2}).$$

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

$$M = C \cdot e(d_1, C_1) \cdot e(d_2, C_2) \cdot e(d_3, C_3) \cdot e(d_4, C_4) \cdot e(d_5, C_5).$$

4.2 Security

We have the following result for the transformed scheme.

Theorem 1. *If the Decision BDH and D-Linear assumptions hold, scheme* BB_1-AIBE *is* IND-sID-CPA *secure and* ANON-sID-CPA *secure.*

The security (semantic security and anonymity) of the transformed scheme can be proved by hybrid experiments similar to that of [10]. We define the following hybrid games which differ on what challenge ciphertext is given by the simulator to the adversary:

- Game_1: $\mathrm{CT}_1 = (C, C_1, C_2, C_3, C_4, C_5)$
- Game_2: $\mathrm{CT}_2 = (R, C_1, C_2, C_3, C_4, C_5)$

– Game_3: $\text{CT}_3 = (R, C_1, C_2, R_1, C_4, C_5)$
– Game_4: $\text{CT}_4 = (R, C_1, C_2, R_1, C_4, R_2)$

Here $(C, C_1, C_2, C_3, C_4, C_5)$ denotes the challenge ciphertext given to the adversary during a real attack, R is a randomly chosen element from $\mathbb{G}_1$ and R_1, R_2 are randomly chosen elements from $\mathbb{G}$. Since every element of the challenge ciphertext in Game_4 is random group element, so it does not leak any information about the message or the identity. Therefore indistinguishability between games proves semantic security and anonymity.

Indistinguishability between Game_1 and Game_2

To prove the indistinguishability between Game_1 and Game_2, we can directly prove the transformed scheme is IND-sID-CPA secure. Here we prove this by an indirect way which is based on the semantic security of the original scheme, that is, if one can break the transformed scheme, the original scheme can also be broken.

Lemma 1 (Semantic Security). *If there is an adversary who can distinguish between* Game_1 *and* Game_2 *with advantage* ϵ*, a simulator can take the adversary as oracle and break* BB_1-IBE *in the* IND-sID-CPA *game with advantage* ϵ*.*

Proof. We show how to construct a simulator $\mathcal{B}$ which can take the adversary $\mathcal{A}$ as oracle to play the IND-sID-CPA game with the challenger $\mathcal{C}$ to break BB_1-IBE.

Init. The simulator $\mathcal{B}$ runs $\mathcal{A}$. $\mathcal{A}$ gives $\mathcal{B}$ a challenge identity ID^*. Then $\mathcal{B}$ submits the challenge identity ID^* to $\mathcal{C}$.

Setup. The challenger $\mathcal{C}$ generates the master public parameters $\text{PK}' = \{Y, g, g_1, h\}$ and gives them to $\mathcal{B}$. $\mathcal{B}$ chooses random integers $t_1, t_2, t_3, t_4 \in \mathbb{Z}_p^*$, computes $v_1 = g^{t_1}, v_2 = g^{t_2}, v_3 = g^{t_3}, v_4 = g^{t_4}$ and outputs the new public key $\text{PK} = \{Y^{t_1 t_2}, g, v_1, v_2, v_3, v_4, g_1^{t_1}, h^{t_1}, g_1^{t_3}, h^{t_3}\}$ and keeps $\{t_1, t_2, t_3, t_4\}$ secret. Then $\mathcal{B}$ gives PK to the adversary $\mathcal{A}$.

Phase 1. $\mathcal{A}$ submits ID to $\mathcal{B}$ with the restriction that $\mathcal{A}$ cannot request the secret key for ID^*. Then $\mathcal{B}$ sends the same ID to $\mathcal{C}$. $\mathcal{C}$ gives $\mathcal{B}$ the secret key $\text{SK}'_{\text{ID}} = (d'_1, d'_2)$. Then $\mathcal{B}$ chooses a random integer $r \in \mathbb{Z}_p^*$, computes $d_1 = d_1'^{t_1 t_2}(g_1^{\text{ID}} h)^{-r t_3 t_4}$, $d_2 = d_2'^{t_1}$,$d_3 = d_2'^{t_2}$, $d_4 = v_3^r$, $d_5 = v_4^r$ and sets $\text{SK}_{\text{ID}} = (d_1, d_2, d_3, d_4, d_5)$. Finally $\mathcal{B}$ gives the new secret key to $\mathcal{A}$.

Challenge. $\mathcal{A}$ submits a message M to $\mathcal{B}$. $\mathcal{B}$ chooses a random element $R_0 \in \mathbb{G}_T$, sets $M_0 = R_0^{t_1^{-1} t_2^{-1}}, M_1 = M^{t_1^{-1} t_2^{-1}}$ and submits ID^*, M_0, M_1 to $\mathcal{C}$. Here we suppose that M_0 has the same length as M_1. $\mathcal{C}$ flips a random coin b and passes the ciphertext $\text{CT}'^* = \textbf{Encrypt}(\text{PK}, M_b, \text{ID}^*) = (C', C'_1, C'_2)$ to $\mathcal{B}$. Then $\mathcal{B}$ chooses random integers $s_1, s_2 \in \mathbb{Z}_p^*$, sets $C = C'^{t_1 t_2}, C_1 = C'_1$, computes $C_2 = v_2^{s_1}, C_3 = C_2'^{t_1} v_1^{-s_1}, C_4 = v_4^{s_2}, C_5 = C_2'^{t_3} v_3^{-s_2}$, and gives the new ciphertext $\text{CT}^* = (C, C_1, C_2, C_3, C_4, C_5)$ to $\mathcal{A}$.

Phase 2. Phase 1 is repeated.

Guess. $\mathcal{B}$ outputs its guess b' of b as follows: if $\mathcal{A}$ outputs 1 (Game_1), then $\mathcal{B}$ outputs its guess $b' = 1$; if $\mathcal{A}$ outputs 2 (Game_2), then $\mathcal{B}$ outputs its guess $b' = 0$. Note that $M = M_1^{t_1 t_2}$ and $MY^{t_1 t_2 s} = (M^{t_1^{-1} t_2^{-1}} Y^s)^{t_1 t_2}$, so if $b = 1$, CT^* is the right ciphertext for message M. If $b = 0$, $C = R_0 Y^{t_1 t_2 s} = (R_0^{t_1^{-1} t_2^{-1}} Y^s)^{t_1 t_2}$ is a random element in $\mathbb{G}_1$.

Since the simulator plays Game_1 if and only if the given ciphertext CT^* is encrypted for message M_1, the simulator's advantage in the IND-sID-CPA game is exactly ϵ. □

According to [3, Theorem 1], we have the following result for BB_1-AIBE's semantic security:

Corollary 1. *If the Decision BDH assumption holds, scheme* BB_1-AIBE *is* IND-sID-CPA *secure.*

Indistinguishability between Game_2 **and** Game_3

Lemma 2 (Anonymity, Part 1). *If there is an adversary who can distinguish between* Game_2 *and* Game_3 *with advantage* ϵ*, a simulator can take the adversary as oracle and win the D-Linear game with advantage* ϵ*.*

Proof. We assume that there exists an adversary $\mathcal{A}$ who can distinguish between Game_2 and Game_3 with advantage ϵ. We show that the simulator $\mathcal{B}$ can win the D-Linear game with advantage ϵ by taking $\mathcal{A}$ as oracle.

Given a D-Linear instance $[g, f, \nu, g^{c_1}, f^{c_2}, Z]$ where Z is either $\nu^{c_1+c_2}$ or random in $\mathbb{G}$ with equal probability. The simulator plays the game in the following stages.

Init. The simulator $\mathcal{B}$ runs $\mathcal{A}$. $\mathcal{A}$ gives $\mathcal{B}$ a challenge identity ID^*.

Setup. $\mathcal{B}$ first chooses random exponents $\alpha, \omega, y, t_3, t_4 \in \mathbb{Z}_p$. It lets g in the simulation be as in the instance and sets $v_1 = \nu, v_2 = f$ which implies t_1, t_2 are unknown to the simulator. Next it sets $g_1 = g^\alpha, g_2 = g^\omega, h = g^y, v_3 = g^{t_3}, v_4 = g^{t_4}$. Then $Y = e(g_1, g_2)^{t_1 t_2} = e(f, \nu)^{\alpha\omega}$. The public key is published as:

$$\text{PK} = (Y, g, v_1, v_2, v_3, v_4, g_1^{t_1} = \nu^\alpha, h^{t_1} = \nu^y, g_1^{t_3}, h^{t_3}).$$

Phase 1. $\mathcal{A}$ submits ID to $\mathcal{B}$ with the restriction that $\mathcal{A}$ cannot request the secret key for ID^*. Then $\mathcal{B}$ chooses random $r \in \mathbb{Z}_p$, computes $d_1 = g^{-r(\alpha\text{ID}+y)t_3 t_4}$, $d_2 = \nu^{-\frac{\alpha\omega}{\alpha\text{ID}+y}}, d_3 = f^{-\frac{\alpha\omega}{\alpha\text{ID}+y}}, d_4 = v_3^r, d_5 = v_4^r$ and sets $\text{SK}_{\text{ID}} = (d_1, d_2, d_3, d_4, d_5)$. We say this is a well formed secret key if we set $r_1 = -\frac{\alpha\omega}{\alpha\text{ID}+y}, r_2 = r$, then $d_1 = g_2^{-\alpha t_1 t_2}(g_1^{\text{ID}} h)^{-r_1 t_1 t_2 - r_2 t_3 t_4}$, $d_2 = v_1^{r_1}$, $d_3 = v_2^{r_1}$, $d_4 = v_3^{r_2}$ and $d_5 = v_4^{r_2}$. Finally $\mathcal{B}$ gives the secret key to $\mathcal{A}$.

Challenge. $\mathcal{A}$ submits a message M to $\mathcal{B}$ and $\mathcal{B}$ discard this message. $\mathcal{B}$ picks a random element $R \in \mathbb{G}_1$, a random integer $s_2 \in \mathbb{Z}_p$ and outputs the ciphertext as:

$$\text{CT}^* = (R, g^{c_1}, (f^{c_2})^{-(\alpha\text{ID}^*+y)}, Z^{\alpha\text{ID}^*+y}, v_4^{s_2}, (g^{c_1})^{(\alpha\text{ID}^*+y)t_3} v_3^{-s_2}).$$

If $Z = \nu^{c_1+c_2}$, then $C_1 = g^{c_1}$, $C_2 = (f^{c_2})^{-(\alpha \mathrm{ID}^*+y)} = v_2^{s_1}$, $C_3 = \nu^{(c_1+c_2)(\alpha \mathrm{ID}^*+y)} = (g_1^{t_1 \mathrm{ID}^*} h^{t_1})^s v_1^{-s_1}$, $C_4 = v_4^{s_2}$, $C_5 = (g_1^{t_3 \mathrm{ID}^*} h^{t_3})^s v_3^{-k_2}$ where $s = c_1, s_1 = -(\alpha \mathrm{ID}^* + y)c_2$; all parts of the challenge but C are thus well formed, and the simulator behaved as in Game_2. If instead, when Z is random, then C_3 are random elements from the adversarial viewpoint, i.e., the simulator responded as in Game_3.

Phase 2. Phase 1 is repeated.

Guess. $\mathcal{B}$ outputs its guess as follows: if $\mathcal{A}$ outputs 2 (Game_2), then $\mathcal{B}$ outputs its guess 1 ($Z = \nu^{c_1+c_2}$); if $\mathcal{A}$ outputs 3 (Game_3), then $\mathcal{B}$ outputs its guess 0 ($Z \neq \nu^{c_1+c_2}$).

By the simulation setup, the simulator's advantage in the D-Linear game is exactly ϵ. □

Indistinguishability between Game_3 and Game_4

Lemma 3 (Anonymity, Part 2). *If there is an adversary who can distinguish between* Game_3 *and* Game_4 *with advantage* ϵ*, a simulator can take the adversary as oracle and win the D-Linear game with advantage* ϵ*.*

Proof. We assume that there exists an adversary $\mathcal{A}$ who can distinguish between Game_3 and Game_4 with advantage ϵ. We show that the simulator $\mathcal{B}$ can win the D-Linear game with advantage ϵ by taking $\mathcal{A}$ as oracle.

Given a D-Linear instance $[g, f, \nu, g^{c_1}, f^{c_2}, Z]$ where Z is either $\nu^{c_1+c_2}$ or random in $\mathbb{G}$ with equal probability. The simulator plays the game in the following stages.

Init. The simulator $\mathcal{B}$ runs $\mathcal{A}$. $\mathcal{A}$ gives $\mathcal{B}$ a challenge identity ID^*.

Setup. $\mathcal{B}$ first chooses random exponents $\alpha, \omega, y, t_1, t_2 \in \mathbb{Z}_p$. It lets g in the simulation be as in the instance and sets $v_3 = \nu, v_4 = f$ which implies t_3, t_4 are unknown to the simulator. Next it sets $g_1 = g^\alpha, h = g^y, v_1 = g^{t_1}, v_2 = g^{t_2}$. Finally it sets $Y = e(f, \nu)^{\alpha\omega t_1 t_2}$. Note that it means $g_2 = g^{\omega t_3 t_4}$. The public key is published as:

$$\mathrm{PK} = (Y, g, v_1, v_2, v_3, v_4, g_1^{t_1}, h^{t_1}, g_1^{t_3} = \nu^\alpha, h^{t_3} = \nu^y).$$

Phase 1. $\mathcal{A}$ submits ID to $\mathcal{B}$ with the restriction that $\mathcal{A}$ cannot request the secret key for ID^*. Then $\mathcal{B}$ chooses random $r \in \mathbb{Z}_p$, computes $d_1 = g^{-r(\alpha \mathrm{ID}+y)t_1 t_2}$, $d_2 = v_1^r, d_3 = v_2^r, d_4 = \nu^{-\frac{\alpha\omega t_1 t_2}{\alpha \mathrm{ID}+y}}, d_5 = f^{-\frac{\alpha\omega t_1 t_2}{\alpha \mathrm{ID}+y}}$ and sets $\mathrm{SK}_{\mathrm{ID}} = (d_1, d_2, d_3, d_4, d_5)$. We say this is a well formed secret key if we set $r_1 = r$, $r_2 = -\frac{\alpha\omega t_1 t_2}{\alpha \mathrm{ID}+y}$, then $d_1 = g_2^{-\alpha t_1 t_2} (g_1^{\mathrm{ID}} h)^{-r_1 t_1 t_2 - r_2 t_3 t_4}$, $d_2 = v_1^{r_1}$, $d_3 = v_2^{r_1}$, $d_4 = v_3^{r_2}$ and $d_5 = v_4^{r_2}$. Finally $\mathcal{B}$ gives the secret key to $\mathcal{A}$.

Challenge. $\mathcal{A}$ submits a message M to $\mathcal{B}$ and $\mathcal{B}$ discard this message. $\mathcal{B}$ picks a random element $R \in \mathbb{G}_1$, a random element $R_1 \in \mathbb{G}$, a random integer $s_1 \in \mathbb{Z}_p$ and outputs the ciphertext as:

$$\mathrm{CT}^* = (R, g^{c_1}, v_2^{s_1}, R_1, (f^{c_2})^{-(\alpha \mathrm{ID}+y)}, Z^{\alpha \mathrm{ID}+y}).$$

If $Z = \nu^{c_1+c_2}$, then $C_1 = g^{c_1}$, $C_4 = (f^{c_2})^{-(\alpha \mathrm{ID}+y)} = v_4^{s_2}$, $C_5 = \nu^{(c_1+c_2)(\alpha \mathrm{ID}+y)} = (g_1^{t_3 \mathrm{ID}} h^{t_3})^s v_3^{-s_2}$, where $s = c_1, s_2 = -(\alpha \mathrm{ID}+y)c_2$; all parts of the challenge but C are thus well formed, and the simulator behaved as in Game_2. If instead, when Z is random, then C_3 are random elements from the adversarial viewpoint, i.e., the simulator responded as in Game_3.

Phase 2. Phase 1 is repeated.

Guess. $\mathcal{B}$ outputs its guess as follows: if $\mathcal{A}$ outputs 3 (Game_3), then $\mathcal{B}$ outputs its guess 1 ($Z = \nu^{c_1+c_2}$); if $\mathcal{A}$ outputs 4 (Game_4), then $\mathcal{B}$ outputs its guess 0 ($Z \neq \nu^{c_1+c_2}$).

By the simulation setup, the simulator's advantage in the D-Linear game is exactly ϵ. □

Proof of Theorem 1. It is obvious from Corollary 1, Lemma 2 and Lemma 3. □

5 Discussion

5.1 Other Transformation

Note that the transformed scheme BB_1-AIBE is IND-sID-CPA secure and ANON-sID-CPA secure. To get fully secure anonymous schemes, we can transform fully secure schemes by using our method, such as another Boneh-Boyen IBE scheme [4], or Waters IBE scheme [27], or Waters dual system encryption IBE scheme [28], and these transformed schemes will be IND-ID-CPA secure and ANON-ID-CPA secure.

5.2 Anonymous HIBE

Another natural extension for our method is that whether our method can be used to transform an HIBE scheme to an anonymous HIBE scheme. There are two problems. One is that our framework is present for IBE not HIBE, so we should prove security under the security model of HIBE. Another obstacle is that we should consider the key derivation, i.e., an identity ID's secret key can be derived from another identity ID^*'s secret key if ID^* is a prefix of ID. Unfortunately, our method cannot be applied in previous HIBE schemes, such as BB_1-HIBE, BBG-HIBE, due to the key delegation of hierarchical identities. A possible approach would be to use the parallel technique introduced in [10] which re-randomizes the keys between all siblings and all children. We leave it an open problem to construct secure anonymous HIBE schemes by extending our method.

6 Conclusion

We analyse the construction of Boyen-Waters anonymous IBE Scheme and find a method to construct anonymous IBE schemes. We show that Boyen-Waters anonymous IBE scheme can be transformed from BB_1-IBE scheme. We give a

new anonymous IBE scheme which is also transformed from BB_1-IBE scheme and can be seemed as a variant of Boyen-Waters anonymous IBE scheme. The security proof shows the transformed scheme has the same semantic security as the original BB_1-IBE scheme and has anonymous security. And we prove anonymity under the Decision Linear assumption.

References

1. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. Journal of Cryptology 21(3), 350–391 (2008)
2. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (2005)
3. Boneh, D., Boyen, X.: Efficient Selective-id Secure Identity-based Encryption without Random Oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
4. Boneh, D., Boyen, X.: Secure Identity Based Encryption without Random Oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004)
5. Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical Identity Based Encryption with Constant Size Ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005)
6. Boneh, D., Boyen, X., Shacham, H.: Short Group Signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
7. Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public Key Encryption with Keyword Search. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506–522. Springer, Heidelberg (2004)
8. Boneh, D., Franklin, M.: Identity-based Encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
9. Boneh, D., Waters, B.: Conjunctive, Subset, and Range Queries on Encrypted Data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer, Heidelberg (2007)
10. Boyen, X., Waters, B.: Anonymous Hierarchical Identity-based Encryption (without Random Oracles). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290–307. Springer, Heidelberg (2006)
11. Camenisch, J., Kohlweiss, M., Rial, A., Sheedy, C.: Blind and Anonymous Identity-based Encryption and Authorised Private Searches on Public Key Encrypted Data. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 196–214. Springer, Heidelberg (2009)
12. Canetti, R., Halevi, S., Katz, J.: A Forward-secure Public-key Encryption Scheme. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 255–271. Springer, Heidelberg (2003)
13. Caro, A.D., Iovino, V., Persiano, G.: Fully secure anonymous hibe and secret-key anonymous ibe with short ciphertexts. Cryptology ePrint Archive, Report 2010/197 (2010), `http://eprint.iacr.org/`

14. Chatterjee, S., Sarkar, P.: Hibe with Short Public Parameters without Random Oracle. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 145–160. Springer, Heidelberg (2006)
15. Chatterjee, S., Sarkar, P.: New Constructions of Constant Size Ciphertext Hibe without Random Oracle. In: Rhee, M.S., Lee, B. (eds.) ICISC 2006. LNCS, vol. 4296, pp. 310–327. Springer, Heidelberg (2006)
16. Cocks, C.: An Identity Based Encryption Scheme Based on Quadratic Residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001)
17. Ducas, L.: Anonymity from Asymmetry: New Constructions for Anonymous Hibe. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 148–164. Springer, Heidelberg (2010)
18. Gentry, C.: Practical Identity-based Encryption without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
19. Gentry, C., Halevi, S.: Hierarchical Identity Based Encryption with Polynomially Many Levels. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 437–456. Springer, Heidelberg (2009)
20. Gentry, C., Silverberg, A.: Hierarchical ID-based Cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002)
21. Horwitz, J., Lynn, B.: Toward Hierarchical Identity-based Encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466–481. Springer, Heidelberg (2002)
22. Lewko, A., Waters, B.: New Techniques for Dual System Encryption and Fully Secure Hibe with Short Ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (2010)
23. Seo, J.H., Cheon, J.H.: Fully secure anonymous hierarchical identity-based encryption with constant size ciphertexts. Cryptology ePrint Archive, Report 2011/021 (2011), `http://eprint.iacr.org/`
24. Seo, J.H., Kobayashi, T., Ohkubo, M., Suzuki, K.: Anonymous Hierarchical Identity-based Encryption with Constant Size Ciphertexts. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 215–234. Springer, Heidelberg (2009)
25. Shamir, A.: Identity-based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
26. Shi, E., Bethencourt, J., Chan, T.H.H., Song, D., Perrig, A.: Multi-dimensional range query over encrypted data. In: SP 2007: IEEE Symposium on Security and Privacy, pp. 350–364 (2007)
27. Waters, B.: Efficient Identity-based Encryption without Random Oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
28. Waters, B.: Dual System Encryption: Realizing Fully Secure Ibe and Hibe under Simple Assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)