New Techniques for Anonymous HIBE with Short Ciphertexts in Prime Order Groups

Kwangsu Lee and Dong Hoon Lee
Graduate School of Information Management and Security, Korea University,
Anam-dong, Seungbuk-gu, Seoul, Korea
[e-mail: {guspin, donghlee}@korea.ac.kr]
*Corresponding author: Dong Hoon Lee

Received June 11, 2010; revised May 27, 2010; accepted September 11, 2010; published October 30, 2010

Abstract

Anonymous hierarchical identity based encryption (HIBE) is an extension of identity based encryption (IBE) that can use an arbitrary string like an e-mail address for a public key, and it additionally provide the anonymity of identity in ciphertexts. Using the anonymous HIBE schemes, it is possible to construct anonymous communication systems and public key encryption with keyword search. This paper presents an anonymous HIBE scheme with constant size ciphertexts under prime order symmetric bilinear groups, and shows that it is secure under the selective security model. Previous anonymous HIBE schemes were constructed to have linear size ciphertexts, to use composite order bilinear groups, or to use asymmetric bilinear groups that is a special type of bilinear groups. Our construction is the first efficient anonymous HIBE scheme that has constant size ciphertexts and that uses prime order symmetric bilinear groups. Compared to the previous scheme of composite order bilinear groups, ours is ten times faster. To achieve our construction, we first devise a novel cancelable random blinding technique. The random blinding property of our technique provides the anonymity of our construction, and the cancellation property of our technique enables decryption.

Keywords: Cryptography, provable security, identity based encryption, hierarchical identity based encryption, anonymity, bilinear pairing

This work was supported by the IT R&D program of MKE/KEIT [KI002113, Development of Security Technology for Car-Healthcare], the Korean government.

DOI: 10.3837/tiis.2010.10.016

1. Introduction

A public key encryption system is one of the essential components of efficient and secure digital communication systems. Identity based encryption (IBE) is public key encryption where an arbitrary identity string like an e-mail address can be used as a public key. Therefore, IBE is a new paradigm of public key encryption that can solve the public key distribution and management problems in public key encryption. Hierarchical IBE (HIBE) is a generalization of IBE such that the identity is represented as a hierarchical structure and a private key can be delegated from a higher level user to a lower level user. The concept of IBE was suggested by Shamir in 1984. However, the first efficient and secure construction of IBE was proposed by Boneh and Franklin using bilinear groups in [1][2]. The construction of HIBE was presented by Gentry and Silverberg in [3]. After that, other constructions of IBE and HIBE were presented in [4][5][6][7][8][9][10].

The security notion of IBE and HIBE is defined as indistinguishability of messages. That is, the ciphertext of IBE and HIBE provides a *message hiding* property (semantic security). This property of security is enough for the traditional digital communication systems since they only require the privacy of messages that they transfer. However, as users' concern about privacy increases, the need for providing the privacy of additional data in the ciphertext also increases. Anonymous IBE and HIBE provide not only the *message hiding* property but also the *identity hiding* property (anonymity) that gives the privacy of identity information in ciphertexts [11]. Because of the identity hiding property, it is not easy to construct anonymous IBE and HIBE schemes. Furthermore, it is very hard to construct anonymous HIBE schemes because HIBE allows the delegation of private keys and the delegation components of private keys hinder the anonymity of ciphertexts. Boyen and Waters proposed the first anonymous HIBE scheme [12]. After their realization, many other constructions were proposed by extending the techniques of Boyen and Waters [13][14][15][16].

1.1 Applications

The main application of anonymous HIBE is anonymous communication systems [17]. An anonymous communication system provides anonymity between sent messages and true recipients (recipient anonymity), and anonymity between received messages and true senders (sender anonymity). Bellare et al. showed that public key encryption with key-privacy (anonymous public key encryption) can be used for anonymous communication systems in [18]. For example, consider a system that consists of n users and has a broadcast channel. All n users of the system periodically broadcast messages with equal length at a fixed time interval t. If a user A want to send a message to a user B, then A creates a ciphertext for B using the anonymous public key encryption. If a user does not want to send a message, then he creates a random string. Thus, the semantic security, the recipient anonymity, and the sender anonymity are provided by the properties of anonymous public key encryption. However, in public key encryption, a user should retrieve the public key of the recipient from a public key infrastructure. Therefore, an adversary that performs traffic analysis can easily gather the information of recipient. In contrast to public key encryption, the process of retrieving a public key is not required in IBE and HIBE. Thus, anonymous HIBE is an ideal solution for the anonymous communication systems [12].

Another important application of anonymous HIBE is public key encryption with keyword search (PEKS) [19]. In PEKS, a ciphertext is associated with a keyword x and a token is

associated with a keyword *w*. Additionally, the ciphertext does not reveal any information of the keyword *x*. If the keyword *w* is equal with the keyword *x*, then we can decrypt the ciphertext using the token. For example, a user *A* creates a ciphertext with a keyword *x* using the public key of a user *B*, and stores it in a public database server. If the user *B* wants to search ciphertexts that have a keyword *w*, then he generates a token of the keyword *w* and gives the token to the public database server. Then the server tests ciphertexts using the token, and returns the ciphertexts if *x*=*w*. Boneh et al. constructed the first efficient and secure PEKS scheme using the IBE scheme of Boneh and Franklin [19]. Abdalla et al. defined anonymous IBE and HIBE, and showed that PEKS and IBE with keyword search (IBEKS) can be constructed from anonymous IBE and anonymous HIBE respectively in [11]. Shi et al. constructed multi-dimensional range query over encrypted data using anonymous IBE [20].

1.2 Previous Methods

As pointed out previously, the construction of anonymous IBE and HIBE is not easy because of the anonymity. The main reason of this difficulty is that the bilinear pairing that enables the realization of IBE and HIBE can be a powerful tool for attacking the anonymity of IBE and HIBE. That is, if we can re-organize ciphertext elements as the decision Diffie-Hellman (DDH) problem using a public key and delegation components of a private key, then we can break the anonymity since the bilinear pairing solves the DDH problem easily. After the first realization of anonymous HIBE by Boyen and Waters, many anonymous HIBE schemes were proposed in [12][13][14][15][16]. The previous strategies of designing anonymous HIBE schemes are classified into four methods.

The first method is a *linear splitting* technique that was devised by Boyen and Waters [12]. This method divides the random exponent of a ciphertext as two different random values. In Boneh and Boyen's IBE [4], an adversary can easily break the anonymity since it can create a bilinear pairing equation like $e(g^t,(hu^{ID}))=e(g,(hu^{ID})^t)$ where g^t and (hu^{ID}) are ciphertext components with a random *t*. The linear splitting technique prevents the creation of bilinear pairing equation by splitting the random *t* to t_1, t_2 where $t=t_1+t_2$. Intuitively speaking, this technique represents a ciphertext as a random point on a 2-dimensional plane using two random scalars t_1, t_2. The anonymity of ciphertexts is easily obtained because a distinguishing problem whether a random point is on a 2-dimensional plane or 3-dimensional space is equivalent to the decisional Linear (DLIN) assumption. Though, this technique enables the construction of anonymous IBE, it is not sufficient for the construction of anonymous HIBE. To achieve anonymous HIBE, Boyen and Waters additionally devised a *private re-randomization* technique. In this technique, additional re-randomization components are included in a private key instead of a public key, and the re-randomization components can not be used to attack the anonymity by making the re-randomization process to be private. Boyen and Waters constructed the first anonymous HIBE scheme with linear size ciphertexts under prime order symmetric bilinear groups using the two techniques, and proved its security under the decisional Bilinear Diffie-Hellman and DLIN assumptions.

The second method is to use *composite order bilinear groups*. A composite order bilinear group consists of prime order bilinear subgroups where each subgroup is orthogonal to other subgroups. In the construction of ciphertexts, we use one subgroup $\mathbb{G}_{p_1}$ to implement a scheme and use another subgroup $\mathbb{G}_{p_2}$ to randomize the ciphertext (random blinding). In the construction of private keys, we use $\mathbb{G}_{p_1}$ only since it is orthogonal to $\mathbb{G}_{p_2}$. The random blinding elements in ciphertexts provide the anonymity of ciphertexts, and the orthogonal

property of subgroups enables the cancellation of random blinding in decryption process. Shi and Waters constructed a delegatable hidden vector encryption (dHVE) scheme under composite order bilinear groups, and they showed that it imply an anonymous HIBE scheme [13]. Seo et al. constructed an anonymous HIBE scheme with constant size ciphertexts under composite order bilinear groups [14]. However, the disadvantage of composite order bilinear groups is that the group order n should be larger than 1024 bits to defeat the integer factorization attacks. Therefore, using composite order bilinear groups is inefficient from point of view of ciphertext size and pairing operations when it is compared to prime order bilinear groups since prime order bilinear groups only requires 160 bits size of group order.

The third method is to use *asymmetric bilinear groups*. The asymmetric bilinear group is a prime order bilinear groups with an asymmetric bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ where $\mathbb{G}_1, \mathbb{G}_2$ are different and there are no efficiently computable homomorphisms between them. In asymmetric bilinear groups, the decision Diffie-Hellman (DDH) assumption holds in two groups $\mathbb{G}_1$ and $\mathbb{G}_2$. Thus, the previous IBE schemes that do not provide the anonymity are easily converted to anonymous IBE schemes on asymmetric bilinear groups. If we apply the private re-randomization techniques of Boyen and Waters to previous HIBE schemes that are not anonymous, then anonymous HIBE schemes are easily obtained [12][16]. Additionally, anonymous HIBE schemes under composite order bilinear groups are also converted to anonymous HIBE schemes under asymmetric prime order bilinear groups [16][21]. However, asymmetric bilinear groups have disadvantages such that it is a special kind of prime order bilinear groups and it requires strong assumptions for the proof of security.

The fourth method is to use *dual pairing vector space* that was devised by Okamoto and Takashima in [15]. The dual pairing vector space is higher dimensional vector space of bilinear groups with two important properties, namely, the hardness of decomposability and the existence of dual orthogonal basis. The hardness of decomposability says that is is hard to decompose basis vectors from the ciphertext vector, and this property provides the anonymity of ciphertexts. The existence of dual orthogonal basis says that it is possible to compute inner product of a ciphertext vector and a private key vector, and this property enables the decryption of ciphertexts. Okamoto and Takashima constructed a hierarchical predicate encryption (HPE) scheme using the dual pairing vector space, and showed that $2l+6$ dimensional HPE imply l-level anonymous HIBE [15]. However, the disadvantage of this approach is that it is hard to construct an anonymous HIBE scheme with constant size ciphertexts.

1.3 Our Contributions

For the efficiency of anonymous HIBE, it is better to use prime order bilinear groups and have constant size ciphertexts than to use composite order bilinear groups and have linear size ciphertexts. For the generality of anonymous HIBE, it is preferable to use symmetric bilinear groups than to use asymmetric bilinear groups. However, it is currently an unsolved problem to construct an anonymous HIBE scheme with constant size ciphertexts under prime order symmetric bilinear groups.

In this paper, we construct an anonymous HIBE scheme with constant size ciphertexts under prime order symmetric bilinear groups and prove its security without random oracles. To achieve our construction, we first devise a novel *cancelable random blinding* technique that enables the construction of anonymous HIBE under prime order symmetric groups. In this technique, the ciphertext components are multiplied by random blinding elements, and the random blinding elements are cancellated by a private key in decryption process. Thus, the

random blinding property provides the anonymity of ciphertexts and the cancellation property provides successful decryption.

We construct an anonymous HIBE scheme with constant size ciphertexts under prime order symmetric bilinear groups and prove its selective security under the decisional *l*-weak Bilinear Diffie-Hellman Inversion (*l*-wBDHI) and *l*-Parallel 3-party Diffie-Hellman (*l*-P3DH) assumptions. Compared to the previous scheme of Seo et al. [22], ours is ten times faster. The comparison of previous HIBE schemes, anonymous HIBE schemes, and our anonymous HIBE scheme are summarized in **Table 1**.

Table 1. Comparison between previous HIBE scheme and ours

Scheme	Group Order	Anonymity	Ciphertext Size	Assumption
GS-HIBE [3]	p	No	$l\|G\|+\|G_T\|$	RO, BDH
BB-HIBE [4]	p	No	$(l+1)\|G\|+\|G_T\|$	BDH
BBG-HIBE [5]	p	No	$2\|G\|+\|G_T\|$	l-wBDHI
Wat-HIBE [9]	p	No	$(l+8)\|G\|+\|G_T\|+\|Z_p\|$	BDH, DLIN
LW-HIBE [10]	p, asym	No	$6\|G_1\|+\|G_T\|$	Static
BW-HIBE [12]	p	Yes	$(2l+5)\|G\|+\|G_T\|$	BDH, DLIN
SW-dHVE [13]	$p_1p_2p_3$	Yes	$(l+3)\|G\|+\|G_T\|$	BDH, C3DH
SKOS-HIBE [14]	p_1p_2	Yes	$3\|G\|+\|G_T\|$	l-wBDHI, l-cDH
OT-HPE [15]	p	Yes	$(2l+6)\|G\|+\|G_T\|$	RDSP, IDSP
Duc-HIBE [16]	p, asym	Yes	$3\|G_1\|+\|G_T\|$	l-wBDHI, P^l-DH
Ours	p	Yes	$6\|G\|+\|G_T\|$	l-wBDHI, l-P3DH

p = prime value, l = hierarchical depth, asym = asymmetric group

1.4 Related Works

Boneh and Franklin constructed the first efficient and secure IBE scheme using bilinear groups and proved its security under the random oracle model [1][2]. Boneh and Boyen constructed two efficient IBE schemes without random oracles and proved that they are secure under a weaker selective-ID security model [4]. Waters proposed a fully secure IBE scheme without random oracles [6], and Gentry proposed a fully secure IBE scheme with tight security reduction using a strong assumption [7]. The IBE schemes of Boneh and Franklin, and Gentry provide the anonymity of ciphertexts. IBE is not only a new paradigm of public key encryption but also a new solution that provides new methodologies for public key encryption research. That is, IBE can be used to construct public key signature [6][9][24][25], chosen ciphertext secure public key encryption [24], and public key encryption with keyword search[11][19].

IBE can be extended to hierarchical IBE (HIBE) [3][4][5][8][9][10][12][14][26], attribute based encryption (ABE) [22][27], and predicate encryption (PE) [11][13][15][19][28][29] depends on the structure of identity.

In HIBE, the identities of users are represented as a hierarchical structure, and the private key of a higher level user can be delegated to a lower level user. The concept of HIBE was introduced by Horwitz and Lynn, but the first efficient and secure construction was proposed by Gentry and Silverberg [3]. Boneh and Boyen constructed an efficient HIBE scheme without random oracles [4], and Boneh et al. constructed an efficient HIBE scheme with constant size ciphertexts [5]. Boyen and Waters constructed the first anonymous HIBE scheme [12]. In contrast to IBE, it is hard to prove the security of HIBE under full model security with efficient

reduction because of its hierarchical structure of identity. Recently, Gentry and Halevi constructed fully secure HIBE scheme using a strong assumption [8], and Waters also constructed fully secure HIBE scheme by introducing dual system encryption [9][10]. The main applications of HIBE are forward secure public key encryption [30] and public key broadcast encryption [31].

In ABE, a private key is associated with an access structure *A* and a ciphertext is associated with a set *S* of attributes. If $S \subseteq A$, then the user of a private key *A* can decrypt the ciphertext of *S*. The concept of ABE was introduced by Sahai and Waters, and they proposed a fuzzy IBE that is a special kind of ABE [27]. Goyal et al. constructed an ABE scheme that supports general access structures [22]. If an ABE scheme supports the delegation capability of private keys, then it can be converted to an HIBE scheme [22]. However, there is no ABE scheme that supports the anonymity of attributes in contrast to HIBE schemes.

In PE, a ciphertext is associated with a vector *x* and a private key is associated with a predicate *f* where the ciphertext provides the anonymity of the vector *x*. If *f*(*x*)=1, then the user of a private key *f* can decrypt the ciphertext, but the ciphertext gives no information except *f*(*x*)=1. The concept of PE was proposed by Boneh et al., and they proposed a public key encryption with keyword search (PEKS) scheme that is a special kind of PE [19]. Abdalla et al. introduced anonymous IBE and anonymous HIBE, and they showed that PEKS can be constructed from anonymous IBE [11]. Boneh and Waters constructed a hidden vector encryption (HVE) scheme that support conjunctive equality, conjunctive comparison, and subset queries on encrypted data [28]. Katz et al. constructed the most expressive PE scheme that supports inner product, and they showed that it can support anonymous IBE, HVE, disjunctive operation, evaluation of polynomials, and CNF & DNF queries [29]. Recently, delegatable PE was introduced and it can support anonymous HIBE [13][15].

2. Background

We define anonymous HIBE and give the formal definition of its selective security model. Next, we review bilinear groups of prime order, and introduce complexity assumptions for our constructions.

2.1 Anonymous Hierarchical Identity Based Encryption

Let IS be an identity space and MS be a message space. A hierarchical identity ID of depth c is defined as an identity vector $(I_1, \cdots, I_c) \in IS^c$. A hierarchical identity $ID = (I_1, \cdots, I_c)$ of depth c is a prefix of a hierarchical identity $ID' = (I'_1, \cdots, I'_d)$ of depth d if $c \le d$ and for all $i \in \{1, \cdots, c\}$, $I_i = I'_i$.

An anonymous HIBE scheme consists of five algorithms (*Setup, KeyGen, Delegate, Encrypt, Decrypt*). Formally it is defined as:

$Setup(1^\lambda, l)$. The setup algorithm takes as input a security parameter 1^λ and a hierarchical depth l. It outputs a public key PK and a master key MK.

$KeyGen(ID, MK, PK)$. The key generation algorithm takes as input a hierarchical identity $ID \in IS^c$, the master key MK, and the public key PK. It outputs a private key SK_{ID}.

$Delegate(ID', SK_{ID}, PK)$. The delegation algorithm takes as input a hierarchical identity $ID' \in IS^d$, a private key SK_{ID} for a hierarchical identity $ID \in IS^c$, and the public key PK. If ID is a prefix of ID', then it outputs a delegated private key $SK_{ID'}$ for ID'.

$Encrypt(ID, M, PK)$. The encryption algorithm takes as input a hierarchical identity $ID \in IS^d$, a message $M \in MS$, and the public key PK. It outputs a ciphertext CT for ID and M.

$Decrypt(CT, SK_{ID}, PK)$. The decryption algorithm takes as input a ciphertext CT for ID', a private key SK_{ID} for a hierarchical identity ID, and the public key PK. It outputs an encrypted message M.

The scheme should satisfy the following correctness property: for all $ID, ID' \in IS^d$, $M \in MS$, let $(PK, MK) \leftarrow Setup(1^\lambda, l)$, $SK_{ID} \leftarrow KeyGen(ID, MK, PK)$, and $CT \leftarrow Encrypt(ID', M, PK)$.

- If $ID = ID'$, then $Decrypt(CT, SK_{ID}, PK) = M$.

We define the selective security model of anonymous HIBE as the following game between a challenger C and an adversary A:

Init: A submits two hierarchical identities $ID_0^*, ID_1^* \in IS^l$.

Setup: C runs the setup algorithm $Setup(1^\lambda, l)$ to generate a master key MK and a public key PK. It keeps MK to itself and gives PK to A.

Query 1: A adaptively requests private keys for hierarchical identities $ID_1, \cdots, ID_{q_1}$ subject to the restriction that ID_i is not a prefix of ID_0^* and ID_1^*. In responses, C gives the corresponding private keys SK_{ID_i} to A by running the key generation algorithm $KeyGen(ID_i, MK, PK)$.

Challenge: A submits two message M_0^*, M_1^* with equal length. C flips a random coin $\gamma \in \{0,1\}$ and gives the challenge ciphertext CT^* to A by running the encryption algorithm $Encrypt(ID_\gamma^*, M_\gamma^*, PK)$.

Query 2: A continue to request private keys for hierarchical identities $ID_{q_1+1}, \cdots, ID_q$ subject to the restriction as before.

Guess: A outputs a guess $\gamma' \in \{0,1\}$ of γ, and wins the game if $\gamma' = \gamma$.

The advantage of A is defined as $Adv_A^{AHIBE} = \left|\Pr[\gamma = \gamma'] - 1/2\right|$ where the probability is taken over the coin tosses made by A and C.

Definition 1. *We say that an anonymous HIBE scheme is selectively secure if all probabilistic polynomial-time adversaries have at most a negligible advantage in the above game.*

2.2 Bilinear Groups of Prime Order

Let $\mathbb{G}$ and $\mathbb{G}_T$ be multiplicative cyclic groups of prime p order. Let g be a generator of $\mathbb{G}$. The bilinear map $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ has the following properties:

1. Bilinearity: $\forall u, v \in \mathbb{G}$ and $\forall a, b \in Z_p$, $e(u^a, v^b) = e(u, v)^{ab}$.
2. Non-degeneracy: $\exists g$ such that $e(g, g) \neq 1$, that is, $e(g, g)$ is a generator of $\mathbb{G}_T$.

We say that $\mathbb{G}, \mathbb{G}_T$ are bilinear groups if the group operations in $\mathbb{G}$ and $\mathbb{G}_T$ as well as the bilinear map e are all efficiently computable.

2.3 Complexity Assumptions

We introduce two assumptions under prime order bilinear groups. The decisional *l*-weak Bilinear Diffie-Hellman Inversion (*l*-wBDHI) assumption was used in [5]. The decisional *l*-Parallel 3-party Diffie-Hellman (*l*-P3DH) assumption is newly introduced for our construction.

***l*-weak Bilinear Diffie-Hellman Inversion (*l*-wBDHI) Assumption** Let $(p, \mathbb{G}, \mathbb{G}_T, e)$ be a description of the bilinear group of prime order p. The decisional *l*-wBDHI problem is stated as follows: given a challenge tuple

$$D = ((p, \mathbb{G}, \mathbb{G}_T, e), g, g^a, g^{a^2}, \cdots, g^{a^l} g^c) \text{ and } T,$$

decides whether $T = e(g, g)^{a^{l+1} c}$ or $T = R$ with random choices of $a, c \in Z_p, R \in \mathbb{G}_T$. The advantage of A in solving the decisional *l*-wBDHI problem is defined as

$$Adv_A^{l-wBDHI} = \left| \Pr[A(D, T = e(g, g)^{a^{l+1} c}) = 1] - \Pr[A(D, T = R) = 1] \right|$$

where the probability is taken over the random choices of D, T and the random used by A.

Definition 4. *We say that the decisional l-wBDHI assumption holds if no probabilistic polynomial-time algorithm has a non-negligible advantage in solving the decisional l-wBDHI problem.*

***l*-Parallel 3-party Diffie-Hellman (*l*-P3DH) Assumption** Let $(p, \mathbb{G}, \mathbb{G}_T, e)$ be a description of the bilinear group of prime order p. The decisional *l*-P3DH problem is stated as follows: given a challenge tuple

$$D = ((p, \mathbb{G}, \mathbb{G}_T, e), g, g^a, g^{a^2}, \cdots, g^{a^l}, g^{a^{l+1}} f^{z_1}, g^c f^{z_2},$$
$$f, f^a, f^{a^2}, \cdots, f^{a^l}, f^{a^{l+1}} g^{-z_1}, f^c g^{-z_2}) \text{ and } T,$$

decides whether $T = Q = (g^{a^{l+1} c} f^{z_3}, f^{a^{l+1} c} g^{-z_3})$ or $T = R = (g^d f^{z_3}, f^d g^{-z_3})$ with random choices of $a, c, d \in Z_p$, and $z_1, z_2, z_3 \in Z_p$. The advantage of A in solving the decisional *l*-P3DH problem is defined as

$$Adv_A^{l-P3DH} = \left| \Pr[A(D, T = Q) = 1] - \Pr[A(D, T = R) = 1] \right|$$

where the probability is taken over the random choices of D, T and the random used by A.

Definition 5. *We say that the decisional l-P3DH assumption holds if no probabilistic polynomial-time algorithm has a non-negligible advantage in solving the decisional l-P3DH problem.*

3. Anonymous HIBE

We define anonymous HIBE and give the formal definition of its selective security model. Next, we review bilinear groups of prime order, and introduce complexity assumptions for our constructions.

3.1 Design Principle

To provide the anonymity of ciphertexts under prime order symmetric bilinear groups, we first devise a new cancelable random blinding technique. In this technique, ciphertext components are multiplied by random blinding elements to provide the anonymity of ciphertexts. Additionally, the multiplied random blinding elements are cancellated by pairing operations with the private key of a user. To use this new technique, we use two instances of HIBE schemes in parallel. The first instance of HIBE is multiplied by random blinding elements, and the second instance of HIBE is also multiplied by blinding elements to cancellate the random blinding of the first instance. Though the random blinding of two instances are the same, an adversary can not attack the anonymity of ciphertexts.

For the construction of anonymous HIBE, additional technique is required since anonymous HIBE allows the delegation of private keys and the delegated private keys can be used to attack the anonymity of ciphertexts. To overcome this problem, we use the private re-randomization technique of Boyen and Waters [12]. In this technique, the re-randomization components of a private key are included in the private key instead of a public key, and the re-randomization components of a user A is only used for the user A. That is, this technique can prevent an adversary from attacking the anonymity of ciphertexts using the re-randomization components of other users.

3.2 Construction

$Setup(1^\lambda, l)$: The setup algorithm first generates the bilinear group $\mathbb{G}$ of prime order p of bit size $\Theta(\lambda)$. Next, it chooses random elements $g, v, h, u_1, \cdots, u_l, w \in \mathbb{G}$, random exponents $x, \alpha \in Z_p$, and random blinding values $z_v, z_h, z_{u,1}, \cdots, z_{u,l}, z_w \in Z_p$. It keeps $v, h, u_1, \cdots, u_l, w, g^\alpha, x$ as a master key MK, and then it publishes a public key PK as follows

$$PK = (g, V^1 = vg^{xz_v}, H^1 = hg^{xz_h}, U_1^1 = u_1 g^{xz_{u,1}}, \cdots, U_l^1 = u_l g^{xz_{u,l}}, W^1 = wg^{xz_w},$$
$$g^x, V^2 = v^x g^{-z_v}, H^2 = h^x g^{-z_h}, U_1^2 = u_1^x g^{-z_{u,1}}, \cdots, U_l^2 = u_l^x g^{-z_{u,l}}, W^2 = w^x g^{-z_w},$$
$$\Omega = e(v, g)^{(1+x^2)\alpha})$$

$KeyGen(ID, MK, PK)$: The key generation algorithm takes as input a hierarchical identity $ID = (I_1, \cdots, I_c) \in Z_p^c$ and the master key MK. It selects random exponents $r_1, r_2 \in Z_p$ and computes decryption components of a private key as

$$K_1^1 = g^{\alpha}(h\prod_{i=1}^{c} u_i^{I_i})^{r_1} w^{r_2}, K_2^1 = v^{-r_1}, K_3^1 = v^{-r_2}, K_{4,c+1}^1 = u_{c+1}^{r_1}, \cdots, K_{4,l}^1 = u_l^{r_1},$$
$$K_1^2 = (K_1^1)^x, K_2^2 = (K_2^1)^x, K_3^2 = (K_3^1)^x, K_{4,c+1}^2 = (K_{4,c+1}^1)^x, \cdots, K_{4,l}^2 = (K_{4,l}^1)^x.$$

Next, it selects random exponents $r_3, r_4, r_5, r_6 \in Z_p$ and computes randomization components of a private key as

$$L_1^{1,1} = (h\prod_{i=1}^{c} u_i^{I_i})^{r_3} w^{r_4}, L_2^{1,1} = v^{-r_3}, L_3^{1,1} = v^{-r_4}, L_{4,c+1}^{1,1} = u_{c+1}^{r_3}, \cdots, L_{4,l}^{1,1} = u_l^{r_3},$$
$$L_1^{1,2} = (h\prod_{i=1}^{c} u_i^{I_i})^{r_5} w^{r_6}, L_2^{1,2} = v^{-r_5}, L_3^{1,2} = v^{-r_6}, L_{4,c+1}^{1,2} = u_{c+1}^{r_5}, \cdots, L_{4,l}^{1,2} = u_l^{r_5},$$
$$L_1^{2,1} = (L_1^{1,1})^x, L_2^{2,1} = (L_2^{1,1})^x, L_3^{2,1} = (L_3^{1,1})^x, L_{4,c+1}^{2,1} = (L_{4,c+1}^{1,1})^x, \cdots, L_{4,l}^{2,1} = (L_{4,l}^{1,1})^x,$$
$$L_1^{2,2} = (L_1^{1,2})^x, L_2^{2,2} = (L_2^{1,2})^x, L_3^{2,2} = (L_3^{1,2})^x, L_{4,c+1}^{2,2} = (L_{4,c+1}^{1,2})^x, \cdots, L_{4,l}^{2,2} = (L_{4,l}^{1,2})^x.$$

Finally, it outputs a private key as

$$SK_{ID} = (K_1^1, K_2^1, K_3^1, K_{4,c+1}^1, \cdots, K_{4,l}^1, \{(L_1^{1,k}, L_2^{1,k}, L_3^{1,k}, L_{4,c+1}^{1,k}, \cdots, L_{4,l}^{1,k})\}_{k=1}^2,$$
$$K_1^2, K_2^2, K_3^2, K_{4,c+1}^2, \cdots, K_{4,l}^2, \{(L_1^{2,k}, L_2^{2,k}, L_3^{2,k}, L_{4,c+1}^{2,k}, \cdots, L_{4,l}^{2,k})\}_{k=1}^2).$$

$Delegate(ID', SK_{ID}, PK)$: The delegation algorithm takes as input a hierarchical identity $ID' = (I_1, \cdots, I_d) \in Z_p^d$ and a private key SK_{ID} for a hierarchical identity $ID = (I_1, \cdots, I_c) \in Z_p^c$ where ID is a prefix of ID'. It first selects random exponents $\delta_1, \delta_2 \in Z_p$. For all $j \in \{1, 2\}$, it computes decryption components of a private key as

$$\tilde{K}_1^j = K_1^j \prod_{i=c+1}^{d} (K_{4,i}^j)^{I_i} \cdot (L_1^{j,1} \prod_{i=c+1}^{d} (L_{4,i}^{j,1})^{I_i})^{\delta_1} (L_1^{j,2} \prod_{i=c+1}^{d} (L_{4,i}^{j,2})^{I_i})^{\delta_2},$$
$$\tilde{K}_2^j = K_2^j \cdot (L_2^{j,1})^{\delta_1} (L_2^{j,2})^{\delta_2}, \tilde{K}_3^j = K_3^j \cdot (L_3^{j,1})^{\delta_1} (L_3^{j,2})^{\delta_2},$$
$$\tilde{K}_{4,d+1}^j = K_{4,d+1}^j \cdot (L_{4,d+1}^{j,1})^{\delta_1} (L_{4,d+1}^{j,2})^{\delta_2}, \cdots, \tilde{K}_{4,l}^j = K_{4,l}^j \cdot (L_{4,l}^{j,1})^{\delta_1} (L_{4,l}^{j,2})^{\delta_2}.$$

Next, it selects random exponents $\delta_3, \delta_4, \delta_5, \delta_6 \in Z_p$. For all $j \in \{1, 2\}$, it computes randomization components of a private key as

$$\tilde{L}_1^{j,1} = (L_1^{j,1} \prod_{i=c+1}^{d} (L_{4,i}^{j,1})^{I_i})^{\delta_3} (L_1^{j,2} \prod_{i=c+1}^{d} (L_{4,i}^{j,2})^{I_i})^{\delta_4}, \tilde{L}_2^{j,1} = (L_2^{j,1})^{\delta_3} (L_2^{j,2})^{\delta_4},$$
$$\tilde{L}_3^{j,1} = (L_3^{j,1})^{\delta_3} (L_3^{j,2})^{\delta_4}, \tilde{L}_{4,d+1}^{j,1} = (L_{4,d+1}^{j,1})^{\delta_3} (L_{4,d+1}^{j,2})^{\delta_4}, \cdots, \tilde{L}_{4,l}^{j,1} = (L_{4,l}^{j,1})^{\delta_3} (L_{4,l}^{j,2})^{\delta_4},$$
$$\tilde{L}_1^{j,2} = (L_1^{j,1} \prod_{i=c+1}^{d} (L_{4,i}^{j,1})^{I_i})^{\delta_5} (L_1^{j,2} \prod_{i=c+1}^{d} (L_{4,i}^{j,2})^{I_i})^{\delta_6}, \tilde{L}_2^{j,2} = (L_2^{j,1})^{\delta_5} (L_2^{j,2})^{\delta_6},$$
$$\tilde{L}_3^{j,2} = (L_3^{j,1})^{\delta_5} (L_3^{j,2})^{\delta_6}, \tilde{L}_{4,d+1}^{j,2} = (L_{4,d+1}^{j,1})^{\delta_5} (L_{4,d+1}^{j,2})^{\delta_6}, \cdots, \tilde{L}_{4,l}^{j,2} = (L_{4,l}^{j,1})^{\delta_5} (L_{4,l}^{j,2})^{\delta_6}.$$

Finally, it outputs a delegated private key as

$$SK_{ID'} = (\tilde{K}_1^1, \tilde{K}_2^1, \tilde{K}_3^1, \tilde{K}_{4,d+1}^1, \cdots, \tilde{K}_{4,l}^1, \{(\tilde{L}_1^{1,k}, \tilde{L}_2^{1,k}, \tilde{L}_3^{1,k}, \tilde{L}_{4,c+1}^{1,k}, \cdots, \tilde{L}_{4,l}^{1,k})\}_{k=1}^2,$$
$$\tilde{K}_1^2, \tilde{K}_2^2, \tilde{K}_3^2, \tilde{K}_{4,d+1}^2, \cdots, \tilde{K}_{4,l}^2, \{(\tilde{L}_1^{2,k}, \tilde{L}_2^{2,k}, \tilde{L}_3^{2,k}, \tilde{L}_{4,c+1}^{2,k}, \cdots, \tilde{L}_{4,l}^{2,k})\}_{k=1}^2).$$

$Encrypt(ID, M, PK)$: The encryption algorithm takes as input a hierarchical identity $ID = (I_1, \cdots, I_d) \in Z_p^d$, a message $M \in G_T$, and the public key PK. It chooses a random exponent $t \in Z_p$ and random blinding values $z_1, z_2, z_3 \in Z_p$. Then it outputs a ciphertext as

$$CT = (C_0 = \Omega^t M, C_1^1 = (V^1)^t g^{xz_1}, C_2^1 = (H^1 \prod_{i=1}^d (U_i^1)^{I_i})^t g^{xz_2}, C_3^1 = (W^1)^t g^{xz_3},$$
$$C_1^2 = (V^2)^t g^{-z_1}, C_2^2 = (H^2 \prod_{i=1}^d (U_i^2)^{I_i})^t g^{-z_2}, C_3^2 = (W^2)^t g^{-z_3}).$$

$Decrypt(CT, SK_{ID}, PK)$: The decryption algorithm takes as input a ciphertext CT and a private key SK_{ID} for a hierarchical identity $ID = (I_1, \cdots, I_d) \in Z_p^d$. It outputs an encrypted message as

$$M \leftarrow C_0 \cdot (\prod_{i=1}^3 e(C_i^1, K_i^1) \cdot e(C_i^2, K_i^2))^{-1}.$$

3.3 Correctness

To show that the above anonymous HIBE scheme satisfy the correctness property, we should prove that private keys from the key generation and delegation algorithms are identically distributed, and that a ciphertext from the encryption algorithm is correctly decrypted by the decryption algorithm using a private key that is generated by the key generation or delegation algorithm.

We first show that private keys from the key generation and delegation algorithms are identically distributed. A private key consists of decryption components and re-randomization components. The decryption components of a private key are re-randomized as follows in the delegation algorithm. If $r_3 r_6 - r_5 r_4 \neq 0 \bmod p$, then new values $\tilde{r}_1, \tilde{r}_2$ are uniformly distributed in Z_p since δ_1, δ_2 are uniformly chosen in Z_p. Note that the probability of $r_3 r_6 - r_5 r_4 \neq 0 \bmod p$ is $1/p$, that is, negligible since r_3, r_4, r_5, r_6 are random values in Z_p.

$$\begin{bmatrix} \tilde{r}_1 \\ \tilde{r}_2 \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} + \begin{bmatrix} r_3 & r_5 \\ r_4 & r_6 \end{bmatrix} \cdot \begin{bmatrix} \delta_1 \\ \delta_2 \end{bmatrix}$$

The re-randomization components of a private key are re-randomized as follows in the delegation algorithm. In this case, new values $\tilde{r}_3, \tilde{r}_4, \tilde{r}_5, \tilde{r}_6$ are uniformly distributed in Z_p since $r_3 r_6 - r_5 r_4 \neq 0 \bmod p$ and $\delta_3, \delta_4, \delta_5, \delta_6$ are uniformly chosen in Z_p.

$$\begin{bmatrix} \tilde{r}_3 & \tilde{r}_5 \\ \tilde{r}_4 & \tilde{r}_6 \end{bmatrix} = \begin{bmatrix} r_3 & r_5 \\ r_4 & r_6 \end{bmatrix} \cdot \begin{bmatrix} \delta_3 & \delta_5 \\ \delta_4 & \delta_6 \end{bmatrix}$$

Next, we show that a ciphertext from the encryption algorithm is correctly decrypted by the decryption algorithm using a private key from the key generation algorithm since the distribution of private keys from the key generation and delegation algorithms are identical. The following simple calculation shows that a session key is correctly recovered from the decryption algorithm.

$$\begin{aligned}
&\prod_{i=1}^{3} e(C_i^1, K_i^1)\cdot e(C_i^2, K_i^2)\\
&= e(v^t g^{x(z_v t+z_1)}, K_1^1)\cdot e(v^{xt} g^{-(z_v t+z_1)}, (K_1^1)^x)\cdot\\
&\quad e((h\prod_{i=1}^{d} u_i^{I_i})^t g^{x((z_h+\sum_{i=1}^{d} z_{u,i} I_i)t+z_2)}, K_1^1)\cdot e((h^x \prod_{i=1}^{d} u_i^{xI_i})^t g^{-((z_h+\sum_{i=1}^{d} z_{u,i} I_i)t+z_2)}, (K_2^1)^x)\cdot\\
&\quad e(w^t g^{x(z_w t+z_3)}, K_3^1)\cdot e(w^{xt} g^{-(z_w t+z_3)}, (K_3^1)^x)\\
&= e(v, g)^{\alpha t} e(v^x, g^x)^{\alpha t}
\end{aligned}$$

3.4 Security

We show that our construction is secure in the selective security model under the decisional *l*-wBDHI and *l*-P3DH assumptions. We later show that our construction can be proven to be secure in chosen ciphertext security and full model security.

Theorem 1. *The above anonymous HIBE construction is selectively secure under the decisional l-wBDHI and l-P3DH assumptions.*

Proof. The proof uses a sequence of games. The first game will be the original security game and the last one will be a game such that the adversary has no advantage. We define the games as follows.

Game_0. This game is the original selective security game in Section 2.1.

Game_1. We define the Game_1 as follows. This game is almost identical to Game_0 except in the way that the challenge ciphertext component C_0 is generated. If $M_0^* \neq M_1^*$, then the simulator generates the challenge ciphertext component C_0 by multiplying a random elements in $\mathbb{G}_T$, and it generates the rest of the ciphertext components as usual. Otherwise, it is created as normal.

Game_2. We modify Game_1 into a new game Game_2. This game is the same with the Game_1 except that the challenge ciphertext components C_2^j, C_3^j are generated. The simulator creates C_1^j as normal for all *j*. However, it creates C_2^j, C_3^j using a new random exponent *s*. That is, the challenge ciphertext components are distributed as follows

$$\begin{aligned}
&C_1^1 = (V^1)^t g^{xz_1}, C_2^1 = (H^1 \prod_{i=1}^{d} (U_i^1)^{I_i})^s g^{xz_2}, C_3^1 = (W^1)^s g^{xz_3},\\
&C_1^2 = (V^2)^t g^{-z_1}, C_2^2 = (H^2 \prod_{i=1}^{d} (U_i^2)^{I_i})^s g^{-z_2}, C_3^2 = (W^2)^s g^{-z_3}.
\end{aligned}$$

Additionally, if $M_0^* \neq M_1^*$, then C_0 is replaced by a random elements from $\mathbb{G}_T$. Otherwise, it is created as normal.

Game_3. Finally, we define a game Game_3. In this game, the simulator creates the challenge ciphertext components C_1^j as normal for all *j*. However, it creates C_2^j, C_3^j as completely random elements in $\mathbb{G}$. Additionally, if $M_0^* \neq M_1^*$, then C_0 is replaced by a completely random elements from $\mathbb{G}_T$. Otherwise, it is created as normal. Note that in Game_3, the challenge ciphertext gives no information about ID_γ^* and M_γ^*. Therefore, the adversary's advantage in this game is zero.

Through the following three lemmas, we prove that it is hard to distinguish Game_{i-1} from Game_i under the given assumptions. Thus, the proof is easily obtained by the following three lemmas. This completes our proof.

Lemma 1. *If the decisional l-wBDHI assumption holds, then no polynomial-time adversary can distinguish between Game_0 and Game_1 with a non-negligible advantage.*

Proof. Suppose there exists an adversary *A* that distinguishes between Game_0 and Game_1 with a non-negligible advantage. A simulator *B* that solves the decisional *l*-wBDHI assumption using *A* is given: a challenge tuple $D=((p,\mathbb{G},\mathbb{G}_T,e),g,g^a,g^{a^2},\cdots,g^{a^l}g^c)$ and T where $T=e(g,g)^{a^{l+1}c}$ or $T=R\in\mathbb{G}_T$. Then *B* that interacts with *A* is described as follows.

Init: *A* gives two hierarchical identities $ID_0^*=(I_{0,1}^*,\cdots,I_{0,l}^*)$ and $ID_1^*=(I_{1,1}^*,\cdots,I_{1,l}^*)$. *B* then flips a random coin $\gamma\in\{0,1\}$ internally.

Setup: *B* first chooses random exponents $v',h',u_1',\cdots,u_l',w',x\in Z_p$. It keeps these as a master key and computes $v=g^{v'}, h=g^{h'}\prod_{i=1}^{l}(g^{a^{l+1-i}})^{-u_i'I_{\gamma,i}^*}$, $u_1=(g^{a^l})^{u_1'},\cdots,u_l=(g^a)^{u_l'}$, $w=g^{w'}$. Next, it implicitly sets $g^\alpha=g^{a^{l+1}}$ and publishes a public key using random blinding values $z_v,z_h,z_{u,1},\cdots,z_{u,l},z_w\in Z_p$ as

$$g,V^1=vg^{xz_v},H^1=hg^{xz_h},U_1^1=u_1g^{xz_{u,1}},\cdots,U_l^1=u_lg^{xz_{u,l}},W^1=wg^{xz_w},$$
$$g^x,V^2=v^xg^{-z_v},H^2=h^xg^{-z_h},U_1^2=u_1^xg^{-z_{u,1}},\cdots,U_l^2=u_l^xg^{-z_{u,l}},W^2=w^xg^{-z_w},$$
$$\Omega=e(g^a,g^{a^l})^{(1+x^2)}.$$

Query 1: *A* adaptively requests a private key for $ID=(I_1,\cdots,I_c)$. Let $\Delta I_i=(I_i-I_{\gamma,i}^*)$. There exists a smallest index *k* such that $\Delta I_k\neq 0$ and $1\le k\le c$ since *A* can not request a private key for ID that is a prefix of ID_γ^*. *B* chooses random exponents $r_1',r_2\in Z_p$ and creates decryption components of the private key as

$$K_1^1=((g^{a^k})^{h'}\prod_{i=c+1}^{l}(g^{a^{l+1-i+k}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k+1}^{c}(g^{a^{l+1-i+k}})^{u_i'\Delta I_i})^{-1/u_k'\Delta I_k}$$
$$(g^{h'}\prod_{i=c+1}^{l}(g^{a^{l+1-i}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k}^{c}(g^{a^{l+1-i}})^{u_i'\Delta I_i})^{r_1'}w^{r_2},$$
$$K_2^1=g^{-v'r_1'}(g^{a^k})^{v'/u_k'\Delta I_k},K_3^1=v^{-r_2},\{K_{4,i}^1=(g^{a^{l+1-i+k}})^{u_i'r_1'}(g^{a^{l+1-i+k}})^{-u_i'/u_k'\Delta I_k}\}_{i=c+1}^{l},$$
$$K_1^2=(K_1^1)^x,K_2^2=(K_2^1)^x,K_3^2=(K_3^1)^x,\{K_{4,i}^2=(K_{4,i}^1)^x\}_{i=c+1}^{l}.$$

Next, it chooses random exponents $r_3,r_4,r_5,r_6\in Z_p$ and creates randomization components of the private key since it knows $v,h,u_1,\cdots,u_l,w$ and x.

If we define the randomness of the private key as $r_1=r_1'-a^k/u_k'\Delta I_k \bmod p$, then the distribution of the private key is correct as follows

$$K_1^1 = g^{a^{l+1}}(g^{h'}\prod_{i=c+1}^{l}(g^{a^{l+1-i}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k}^{c}(g^{a^{l+1-i}})^{u_i'\Delta I_i})^{r_1'-a^k/u_k'\Delta I_k} w^{r_2}$$
$$= ((g^{a^k})^{h'}\prod_{i=c+1}^{l}(g^{a^{l+1-i+k}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k+1}^{c}(g^{a^{l+1-i+k}})^{u_i'\Delta I_i})^{-1/u_k'\Delta I_k}$$
$$(g^{h'}\prod_{i=c+1}^{l}(g^{a^{l+1-i}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k}^{c}(g^{a^{l+1-i}})^{u_i'\Delta I_i})^{r_1'} w^{r_2}.$$

Challenge: *A* submits two messages M_0^*, M_1^*. If $M_0^* = M_1^*$, then *B* aborts and takes a random guess. Otherwise, it chooses random blinding values $z_1, z_2, z_3 \in Z_p$ and outputs a challenge ciphertext as

$$C_0 = (T)^{v'(1+x^2)} M_\gamma^*, C_1^1 = (g^c)^{v'} g^{xz_1}, C_2^1 = (g^c)^{h'} g^{xz_2}, C_3^1 = (g^c)^{w'} g^{xz_3},$$
$$C_1^2 = (g^c)^{v'x} g^{-z_1}, C_2^2 = (g^c)^{h'x} g^{-z_2}, C_3^2 = (g^c)^{w'x} g^{-z_3}.$$

If $T = e(g,g)^{a^{l+1}c}$, then *B* is playing Game$_0$. Otherwise, it is playing Game$_1$.

Query 2: Same as Query Phase 1.

Guess: *A* outputs a guess γ'. If $\gamma = \gamma'$, it outputs 0. Otherwise, it outputs 1.

This completes our proof.

Lemma 2. *If the decisional l-P3DH assumption holds, then no polynomial-time adversary can distinguish between Game$_1$ and Game$_2$ with a non-negligible advantage.*

Proof. Suppose there exists an adversary *A* that distinguishes between Game$_1$ and Game$_2$ with a non-negligible advantage. A simulator *B* that solves the decisional *l*-P3DH assumption using *A* is given: a challenge tuple $D = ((p, \mathrm{G}, \mathrm{G}_T, e), g, g^a, g^{a^2}, \cdots, g^{a^l}, g^{a^{l+1}} f^{z_1}, g^c f^{z_2}, f, f^a, f^{a^2}, \cdots, f^{a^l}, f^{a^{l+1}} g^{-z_1}, f^c g^{-z_2})$ and $T = (T_1, T_2)$ where $T = (g^{a^{l+1}c} f^{z_3}, f^{a^{l+1}c} g^{-z_3})$ or $T = (g^d f^{z_3}, f^d g^{-z_3})$. Then *B* that interacts with *A* is described as follows.

Init: *A* gives two hierarchical identities $ID_0^* = (I_{0,1}^*, \cdots, I_{0,l}^*)$ and $ID_1^* = (I_{1,1}^*, \cdots, I_{1,l}^*)$. *B* then flips a random coin $\gamma \in \{0,1\}$ internally.

Setup: *B* first chooses random exponents $v', h', u_1', \cdots, u_l', w', \alpha \in Z_p$. It keeps these as a master key and implicitly sets $v = g^{v'}, h = g^{a^{l+1}h'}\prod_{i=1}^{l}(g^{a^{l+1-i}})^{-u_i'I_{\gamma,i}^*}, u_1 = g^{a^l u_1'}, \cdots, u_l = g^{a u_l'}, w = g^{a^{l+1}w'}, g^x = f$. Next, it publishes a public key using random blinding values $z_v, z_h, z_{u,1}, \cdots, z_{u,l}, z_w \in Z_p$ as

$$g, V^1 = g^{v'} f^{z_v}, H^1 = (g^{a^{l+1}} f^{z_1})^{h'}\prod_{i=1}^{l}(g^{a^{l+1-i}})^{-u_i'I_{\gamma,i}^*} f^{z_h}, U_1^1 = (g^{a^l})^{u_1'} f^{z_{u,1}}, \cdots,$$
$$U_l^1 = (g^a)^{u_l'} f^{z_{u,l}}, W^1 = (g^{a^{l+1}} f^{z_1})^{w'} f^{z_w},$$
$$f, V^2 = f^{v'} g^{-z_v}, H^2 = (f^{a^{l+1}} g^{-z_1})^{h'}\prod_{i=1}^{l}(f^{a^{l+1-i}})^{-u_i'I_{\gamma,i}^*} g^{-z_h}, U_1^2 = (f^{a^l})^{u_1'} g^{-z_{u,1}}, \cdots,$$
$$U_l^2 = (f^a)^{u_l'} g^{-z_{u,l}}, W^2 = (f^{a^{l+1}} g^{-z_1})^{w'} g^{-z_w}, \Omega = e(g,g)^{v'\alpha} e(f,f)^{v'\alpha}.$$

Query 1: *A* adaptively requests a private key for $ID=(I_1,\cdots,I_c)$. Let $\Delta I_i=(I_i-I^*_{\gamma,i})$. There exists a smallest index *k* such that $\Delta I_k\neq 0$ and $1\le k\le c$ since *A* can not request a private key for *ID* that is a prefix of ID^*_γ. *B* chooses random exponents $r_1',r_2'\in Z_p$ and creates decryption components of the private key as

$$K_1^1=g^\alpha(\prod_{i=c+1}^{l}(g^{a^{l+1-i}})^{-u_i'I^*_{\gamma,i}}\prod_{i=k}^{c}(g^{a^{l+1-i}})^{u_i'\Delta I_i})^{r_1'}(\prod_{i=c+1}^{l}(g^{a^{l+1-i+k}})^{-u_i'I^*_{\gamma,i}}\prod_{i=k+1}^{c}(g^{a^{l+1-i+k}})^{u_i'\Delta I_i})^{r_2'},$$
$$K_2^1=g^{-v'r_1'}(g^{a^k})^{-v'r_2'},K_3^1=g^{v'(h'r_1'+u_k'\Delta I_k r_2')/w'}(g^{a^k})^{v'(h'r_1')/w'},K_{4,i}^1=(g^{a^{l+1-i}})^{u_i'r_1'}(g^{a^{l+1-i+k}})^{u_i'r_2'},$$
$$K_1^2=f^\alpha(\prod_{i=c+1}^{l}(f^{a^{l+1-i}})^{-u_i'I^*_{\gamma,i}}\prod_{i=k}^{c}(f^{a^{l+1-i}})^{u_i'\Delta I_i})^{r_1'}(\prod_{i=c+1}^{l}(f^{a^{l+1-i+k}})^{-u_i'I^*_{\gamma,i}}\prod_{i=k+1}^{c}(f^{a^{l+1-i+k}})^{u_i'\Delta I_i})^{r_2'},$$
$$K_2^2=f^{-v'r_1'}(f^{a^k})^{-v'r_2'},K_3^2=f^{v'(h'r_1'+u_k'\Delta I_k r_2')/w'}(f^{a^k})^{v'(h'r_1')/w'},K_{4,i}^2=(f^{a^{l+1-i}})^{u_i'r_1'}(f^{a^{l+1-i+k}})^{u_i'r_2'}.$$

To show that the above components are the same as the one in the original game, we define the randomness of the private key as

$$r_1=r_1'+r_2'a^k \bmod p,\ r_2=-(h'r_1'+u_k'\Delta I_k r_2')/w'-(h'r_2')a^k/w' \bmod p$$

It is not hard to see that r_1,r_2 are independent random values since $\Delta I_k\neq 0$. Thus the distribution of the above components are correct as follows

$$K_1^1=g^\alpha(g^{a^{l+1}h'}\prod_{i=c+1}^{l}(g^{a^{l+1-i}})^{-u_i'I^*_{\gamma,i}}\prod_{i=k}^{c}(g^{a^{l+1-i}})^{u_i'\Delta I_i})^{r_1'+r_2'a^k}(g^{a^{l+1}w'})^{-(h'r_1'+u_k'\Delta I_k r_2')/w'-(h'r_2')a^k/w'}$$
$$=g^\alpha(\prod_{i=c+1}^{l}(g^{a^{l+1-i}})^{-u_i'I^*_{\gamma,i}}\prod_{i=k}^{c}(g^{a^{l+1-i}})^{u_i'\Delta I_i})^{r_1'}(\prod_{i=c+1}^{l}(g^{a^{l+1-i+k}})^{-u_i'I^*_{\gamma,i}}\prod_{i=k+1}^{c}(g^{a^{l+1-i+k}})^{u_i'\Delta I_i})^{r_2'},$$
$$K_2^1=g^{-v'(r_1'+r_2'a^k)}=g^{-v'r_1'}(g^{a^k})^{-v'r_2'},$$
$$K_3^1=g^{-v'(-(h'r_1'+u_k'\Delta I_k r_2')/w'-(h'r_2')a^k/w')}=g^{v'(h'r_1'+u_k'\Delta I_k r_2')/w'}(g^{a^k})^{v'(h'r_1')/w'},$$
$$K_{4,i}^1=(g^{a^{l+1-i}})^{u_i'(r_1'+r_2'a^k)}=(g^{a^{l+1-i}})^{u_i'r_1'}(g^{a^{l+1-i+k}})^{u_i'r_2'}.$$

The randomization components of the private key is similar to the decryption components of the private key except g^α. Since *B* selects α itself, it can generate the randomization components using random exponents $r_3',r_4',r_5',r_6'\in Z_p$ similar to the above. Therefore, we omit the generation of the randomization components of the private key.

Challenge: *A* submits two messages M_0^*,M_1^*. If $M_0^*=M_1^*$, then *B* computes $C_0=(e(g^c f^{z_2},g)\cdot e(f^c g^{-z_2},f))^{v'\alpha}\cdot M_\gamma^*$. Otherwise, it chooses a random elements in G_T for C_0. Next, it chooses random blinding values $z_{c,1},z_{c,2},z_{c,3}\in Z_p$ and outputs a challenge ciphertext as

$$C_1^1=(g^c f^{z_2})^{v'}f^{z_{c,1}},C_2^1=(T_1)^{h'}f^{z_{c,2}},C_3^1=(T_1)^{w'}f^{z_{c,3}},$$
$$C_1^2=(f^c g^{-z_2})^{v'}g^{-z_{c,1}},C_2^2=(T_2)^{h'}g^{-z_{c,2}},C_3^2=(T_2)^{w'}g^{-z_{c,3}}.$$

If $T=(g^{a^{l+1}c}f^{z_3},f^{a^{l+1}c}g^{-z_3})$, then *B* is playing Game_1. Otherwise, it is playing Game_2 as follows

$$C_1^1 = (g^{v'} f^{z_v})^c f^{v'z_2 + z_{c,1} - cz_v} = (g^c f^{z_2})^{v'} f^{z_{c,1}},$$

$$C_2^1 = ((g^{a^{l+1}} f^{z_1})^{h'} f^{z_h} \prod_{i=1}^{l} (f^{z_{u,i}})^{I^*_{\gamma,i}})^{d/a^{l+1}} f^{h'z_3 + z_{c,2} - (h'z_1 + z_h + \sum_{i=1}^{l} z_{u,i} I^*_{\gamma,i})d/a^{l+1}}$$

$$= (g^{a^{l+1} \cdot d/a^{l+1}} f^{z_3})^{h'} f^{z_{c,2}},$$

$$C_3^1 = ((g^{a^{l+1}} f^{z_1})^{w'} f^{z_w})^{d/a^{l+1}} f^{w'z_3 + z_{c,3} - (w'z_1 + z_w)d/a^{l+1}} = (g^{a^{l+1} \cdot d/a^{l+1}} f^{z_3})^{w'} f^{z_{c,3}}.$$

where c and d/a^{l+1} are independent random values.

Query 2: Same as Query Phase 1.

Guess: *A* outputs a guess γ'. If $\gamma = \gamma'$, it outputs 0. Otherwise, it outputs 1.

This completes our proof.

Lemma 3. *If the decisional l-P3DH assumption holds, then no polynomial-time adversary can distinguish between Game$_2$ and Game$_3$ with a non-negligible advantage.*

Proof. Suppose there exists an adversary *A* that distinguishes between Game$_2$ and Game$_3$ with a non-negligible advantage. A simulator *B* that solves the decisional *l*-P3DH assumption using *A* is given: a challenge tuple $D = ((p, \mathrm{G}, \mathrm{G}_T, e), g, g^a, g^{a^2}, \cdots, g^{a^l}, g^{a^{l+1}} f^{z_1}, g^c f^{z_2}, f, f^a, f^{a^2}, \cdots, f^{a^l}, f^{a^{l+1}} g^{-z_1}, f^c g^{-z_2})$ and $T = (T_1, T_2)$ where $T = (g^{a^{l+1}c} f^{z_3}, f^{a^{l+1}c} g^{-z_3})$ or $T = (g^d f^{z_3}, f^d g^{-z_3})$. Then *B* that interacts with *A* is described as follows.

Init: *A* gives two hierarchical identities $ID_0^* = (I_{0,1}^*, \cdots, I_{0,l}^*)$ and $ID_1^* = (I_{1,1}^*, \cdots, I_{1,l}^*)$. *B* then flips a random coin $\gamma \in \{0,1\}$ internally.

Setup: *B* first chooses random exponents $v', h', u_1', \cdots, u_l', w', \alpha \in Z_p$. It keeps these as a master key and implicitly sets $v = g^{a^{l+1}v'}, h = g^{a^{l+1}h'} \prod_{i=1}^{l} (g^{a^i})^{-u_i' I^*_{\gamma,i}}, u_1 = g^{a u_1'}, \cdots,$ $u_l = g^{a^l u_l'}, w = g^{w'}, g^x = f$. Next, it publishes a public key using random blinding values $z_v, z_h, z_{u,1}, \cdots, z_{u,l}, z_w \in Z_p$ as

$$g, V^1 = (g^{a^{l+1}} f^{z_1})^{v'} f^{z_v}, H^1 = (g^{a^{l+1}} f^{z_1})^{h'} \prod_{i=1}^{l} (g^{a^i})^{-u_i' I^*_{\gamma,i}} f^{z_h}, U_1^1 = (g^a)^{u_1'} f^{z_{u,1}}, \cdots,$$

$$U_l^1 = (g^{a^l})^{u_l'} f^{z_{u,l}}, W^1 = g^{w'} f^{z_w},$$

$$f, V^2 = (f^{a^{l+1}} g^{-z_1})^{v'} g^{-z_v}, H^2 = (f^{a^{l+1}} g^{-z_1})^{h'} \prod_{i=1}^{l} (f^{a^i})^{-u_i' I^*_{\gamma,i}} g^{-z_h}, U_1^2 = (f^a)^{u_1'} g^{-z_{u,1}}, \cdots,$$

$$U_l^2 = (f^{a^l})^{u_l'} g^{-z_{u,l}}, W^2 = f^{w'} g^{-z_w}, \Omega = e(g^a, g^{a^l})^{v'\alpha} e(f^a, f^{a^l})^{v'\alpha}.$$

Query 1: *A* adaptively requests a private key for $ID = (I_1, \cdots, I_c)$. Let $\Delta I_i = (I_i - I^*_{\gamma,i})$. There exists a smallest index *k* such that $\Delta I_k \neq 0$ and $1 \leq k \leq c$ since *A* can not request a private key for ID that is a prefix of ID^*_γ. *B* chooses random exponents $r_1', r_2' \in Z_p$ and creates a private key as

$$K_1^1 = g^{\alpha}(g^{a^{l-k}h'}\prod_{i=c+1}^{l}(g^{a^{i-k-1}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k+1}^{c}(g^{a^{i-k-1}})^{u_i'\Delta I_i})^{r_1'}(g^{a^l h'}\prod_{i=c+1}^{l}(g^{a^{i-1}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k}^{c}(g^{a^{i-1}})^{u_i'\Delta I_i})^{r_2'},$$
$$K_2^1 = (g^{a^{l-k}})^{-v'r_1'}(g^{a^l})^{-v'r_2'}, K_3^1 = (g^{a^l})^{v'u_k'\Delta I_k r_1'/w'}, K_{4,i}^1 = (g^{a^{i-k-1}})^{u_i'r_1'}(g^{a^{i-1}})^{u_i'r_2'},$$
$$K_1^2 = f^{\alpha}(f^{a^{l-k}h'}\prod_{i=c+1}^{l}(f^{a^{i-k-1}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k+1}^{c}(f^{a^{i-k-1}})^{u_i'\Delta I_i})^{r_1'}(f^{a^l h'}\prod_{i=c+1}^{l}(f^{a^{i-1}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k}^{c}(f^{a^{i-1}})^{u_i'\Delta I_i})^{r_2'},$$
$$K_2^2 = (f^{a^{l-k}})^{-v'r_1'}(f^{a^l})^{-v'r_2'}, K_3^2 = (f^{a^l})^{v'u_k'\Delta I_k r_1'/w'}, K_{4,i}^2 = (f^{a^{i-k-1}})^{u_i'r_1'}(f^{a^{i-1}})^{u_i'r_2'}.$$

To show that the above private key is the same as the one in the original game, we define the randomness of the private key as

$$r_1 = r_1'/a^{k+1} + r_2'/a \bmod p,\ r_2 = -(u_k'\Delta I_k r_1')/w'a \bmod p$$

It is not hard to see that r_1, r_2 are independent random values since $\Delta I_k \neq 0$. Thus the distribution of the above private key is correct as follows

$$\begin{aligned}K_1^1 &= g^{\alpha}(g^{a^{l+1}h'}\prod_{i=c+1}^{l}(g^{a^i})^{-u_i'I_{\gamma,i}^*}\prod_{i=k}^{c}(g^{a^i})^{u_i'\Delta I_i})^{r_1'/a^{k+1}+r_2'/a}(g^{w'})^{-(u_k'\Delta I_k r_1')/w'a}\\ &= g^{\alpha}(g^{a^{l-k}h'}\prod_{i=c+1}^{l}(g^{a^{i-k-1}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k+1}^{c}(g^{a^{i-k-1}})^{u_i'\Delta I_i})^{r_1'}\\ &\quad (g^{a^l h'}\prod_{i=c+1}^{l}(g^{a^{i-1}})^{-u_i'I_{\gamma,i}^*}\prod_{i=k}^{c}(g^{a^{i-1}})^{u_i'\Delta I_i})^{r_2'},\end{aligned}$$
$$K_2^1 = g^{-a^{l+1}v'(r_1'/a^{k+1}+r_2'/a)} = (g^{a^{l-k}})^{-v'r_1'}(g^{a^l})^{-v'r_2'}, K_3^1 = g^{-a^{l+1}v'(-(u_k'\Delta I_k r_1')/w'a)} = (g^{a^l})^{v'u_k'\Delta I_k r_1'/w'},$$
$$K_{4,i}^1 = (g^{a^i})^{u_i'(r_1'/a^{k+1}+r_2'/a)} = (g^{a^{i-k-1}})^{u_i'r_1'}(g^{a^{i-1}})^{u_i'r_2'}.$$

The randomization components of the private key is similar to the decryption components of the private key except g^{α}. Since *B* selects α itself, it can generate the randomization components using random exponents $r_3', r_4', r_5', r_6' \in Z_p$ similar to the above. Therefore, we omit the generation of the randomization components of the private key.

Challenge: *A* submits two messages M_0^*, M_1^*. If $M_0^* = M_1^*$, then *B* selects a random exponent $t \in Z_p$ and computes $C_0 = \Omega^t M_{\gamma}^*$. Otherwise, it chooses a random elements in G_T for C_0. Next, it chooses random blinding values $z_{c,1}, z_{c,2}, z_{c,3} \in Z_p$ and outputs a challenge ciphertext as

$$C_1^1 = (g^{a^{l+1}}f^{z_1})^{v't}f^{z_{c,1}}, C_2^1 = (T_1)^{h'}f^{z_{c,2}}, C_3^1 = (g^c f^{z_2})^{w'}f^{z_{c,3}},$$
$$C_1^2 = (f^{a^{l+1}}g^{-z_1})^{v't}g^{-z_{c,1}}, C_2^2 = (T_2)^{h'}g^{-z_{c,2}}, C_3^2 = (f^c g^{-z_2})^{w'}g^{-z_{c,3}}.$$

If $T = (g^{a^{l+1}c}f^{z_3}, f^{a^{l+1}c}g^{-z_3})$, then *B* is playing Game_2. Otherwise, it is playing Game_3 as follows

$$C_1^1 = ((g^{a^{l+1}}f^{z_1})^{v'}f^{z_v})^t f^{v'tz_1+z_{c,1}-(v'z_v+z_v)t} = (g^{a^{l+1}}f^{z_1})^{v't}f^{z_{c,1}},$$
$$\begin{aligned}C_2^1 &= ((g^{a^{l+1}}f^{z_1})^{h'}f^{z_h}\prod_{i=1}^{l}(f^{z_{u,i}})^{I_{\gamma,i}^*})^{d/a^{l+1}}f^{h'z_3+z_{c,2}-(h'z_1+z_h+\sum_{i=1}^{l}z_{u,i}I_{\gamma,i}^*)d/a^{l+1}}\\ &= (g^{a^{l+1}\cdot d/a^{l+1}}f^{z_3})^{h'}f^{z_{c,2}},\end{aligned}$$
$$C_3^1 = (g^{w'}f^{z_w})^c f^{w'z_2+z_{c,3}-cz_w} = (g^c f^{z_2})^{w'}f^{z_{c,3}}.$$

where t, d/a^{l+1}, and c are independent random values.

Query 2: Same as Query Phase 1.

Guess: A outputs a guess γ'. If $\gamma = \gamma'$, it outputs 0. Otherwise, it outputs 1.

This completes our proof.

3.4 Extensions

Full Model Security. In the full model security, an adversary selects a target identity at the challenge phase of the security model in contrast to the selective model security where the adversary select the target identity at the initialization phase. Boneh et al. showed that a selectively secure HIBE scheme can be converted to a fully secure HIBE scheme with exponential loss of security reduction [4][5]. Our construction of the selective model security also can be made to provide the full model security with exponential loss of security reduction.

Chosen Ciphertext Security. In the chosen ciphertext security, an adversary can access to additional decryption oracles of the scheme. Canettie et al. showed that a chosen ciphertext secure l-level HIBE scheme can be constructed from a chosen plaintext secure l+1-level HIBE scheme [24]. If we adapt the method of Canettie et al., then our construction of this paper also can provide the chosen ciphertext security.

Asymmetric Bilinear Groups. The bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ of asymmetric bilinear groups is defined as $\mathbb{G}_1, \mathbb{G}_2$ are different and there are no efficiently computable homomorphisms between two groups. In asymmetric bilinear groups, the decision Diffie-Hellman (DDH) assumption still holds in $\mathbb{G}_1$ and $\mathbb{G}_2$. Therefore, the anonymity of ciphertexts is easily obtained. Our construction also can be converted to use asymmetric bilinear groups. In this case, the cancelable random blinding technique is not required. Thus, our construction under asymmetric bilinear groups is the same as the construction of Seo et al. [14] under asymmetric bilinear groups.

4. Performance Analysis

For the comparison of performance, we compare our construction under prime order bilinear groups with the construction of Seo et al. [14] under composite order bilinear groups.

Table 2. The detailed information of bilinear groups

Bilinear Group	Security	Group Order	$\lvert\mathbb{G}\rvert$	$\lvert\mathbb{G}\rvert$	T_{exp}	T_{pair}
Composite Order	80 bits	1024 bits	1024 bits	2048 bits	$O(rb^2)$	757 ms
Prime Order	80 bits	160 bits	512 bits	1024 bits	$O(rb^2)$	25 ms

T_{exp} = exponentiation time, T_{exp} = pairing time, r = the size of group, b = the size of $\mathbb{G}$

The detailed information of composite order bilinear groups and prime order symmetric bilinear groups is summarized in **Table 2**. In composite order bilinear groups, the order of groups should be larger than 1024 bits to defeat the integer factorization attacks. Thus, the size of group elements in $\mathbb{G}$ is 1024 bits and the size of group elements in $\mathbb{G}_T$ is 2048 bits. In contrast, the order of prime order bilinear groups is only 160 bits to provide 80 bits security

level. Thus the size of group elements in $\mathbb{G}$ is 512 bits and the size of groups elements in $\mathbb{G}_T$ is 1024 bits. For the comparison of pairing time in each groups, we use the data in PBC library.

Table 3. Comparison of two anonymous HIBE schemes

Scheme	|PK|	|SK|	|CT|	KeyGen	Encrypt	Decrypt
SKOS-HIBE	1024l bits	3072(l-d) bits	5120 bits	$3lT_{exp}$	dT_{exp}	2271 ms
Ours	1024l bits	3072(l-d) bits	4096 bits	$6lT_{exp}$	$2dT_{exp}$	150 ms
Ratio	1/1	1/1	1.25/1	12.8/1	12.8/1	15.1/1

l = hierarchical depth, d = identity depth

The comparison between two constructions is summarized in **Table 3**. The public key size and private key size of two constructions is the same. However, the ciphertext size of ours is 20% shorter. If the operation time of two schemes is compared, there is big difference. The main operation of the key generation and encryption algorithms is an exponentiation operation. One exponentiation in prime order symmetric bilinear groups is approximately $1024^3/(160\cdot 512^2)\approx 25.6$ times faster than the one in composite order groups. Thus the key generation and encryption algorithms of ours is 12.8 times faster. The main operation of the decryption algorithm is a pairing operation. One pairing in prime order symmetric bilinear groups is approximately 30.2 times faster than the one in composite order bilinear groups. Therefore, the decryption algorithm of ours is 15.1 times faster.

5. Conclusions

In this paper, we presented a new cancelable random blinding technique for the construction of anonymous HIBE, and this technique is different from the previous known techniques. Using our technique, we constructed an anonymous HIBE scheme with constant size ciphertexts under prime order symmetric bilinear groups, and proved its selective model security. Our technique has an independent interest, and it may be possible to use this technique for the construction of other encryption schemes in prime order bilinear groups.

An interesting open problem is to construct an anonymous HIBE scheme with constant size ciphertexts under prime order symmetric bilinear groups that can be prove to be fully secure with reasonable loss of reduction. One idea for this construction is to use the dual system encryption method by Waters [9][10]. However, the simple combination of these methods does not solve the problem because the dual encryption system of [9][10] does not work for an HIBE scheme with constant size ciphertexts under prime order symmetric bilinear groups.

References

[1] D. Boneh and M.K. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology - CRYPTO 2001. Lecture Notes in Computer Science*, vol. 2139, pp. 213-229, 2001.

[2] D. Boneh and M.K. Franklin, "Identity-based encryption from the weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586-615, 2003.

[3] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in *Advances in Cryptology-ASIACRYPT 2002, Lecture Notes in Computer Science*, vol. 2501, pp. 548-566, 2002.

[4] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," in *Advances in Cryptology - EUROCRYPT 2004. Lecture Notes in Computer Science*, vol. 3027, pp. 223-238, 2004.
[5] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Advances in Cryptology - EUROCRYPT 2005. Lecture Notes in Computer Science*, vol. 3493, pp. 440-456, 2005.
[6] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology - EUROCRYPT 2005. Lecture Notes in Computer Science*, vol. 3494, pp. 114-127, 2005.
[7] C. Gentry, "Practical identity-based encryption without random oracles," in *Advances in Cryptology - EUROCRYPT 2006, Lecture Notes in Computer Science*, vol. 4004, pp. 445-464, 2006.
[8] C. Gentry and S. Halevi, "Hierarchical identity based encryption with polynomially many levels," in *TCC 2009, Lecture Notes in Computer Science*, vol. 5444, pp. 437-456, 2009.
[9] B. Waters, "Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology - CRYPTO 2009. Lecture Notes in Computer Science*, vol. 5677, pp. 619-636, 2009.
[10] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in *TCC 2010, Lecture Notes in Computer Science*, vol. 5978, pp. 455-479, 2010.
[11] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions," in *Advances in Cryptology - CRYPTO 2005. Lecture Notes in Computer Science*, vol. 3621, pp. 205-222, 2005.
[12] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," in *Advances in Cryptology – CRYPTO 2006. Lecture Notes in Computer Science*, vol. 4117, pp. 290-307, 2006.
[13] E. Shi and B. Waters, "Delegating capabilities in predicate encryption systems," in *ICALP 2008. Lecture Notes in Computer Science*, vol. 5126, pp. 560-578, 2008.
[14] J.H. Seo, T. Kobayashi, M. Ohkubo, and K. Suzuki, "Anonymous hierarchical identity-based encryption with constant size ciphertexts," in *PKC 2009. Lecture Notes in Computer Science*, vol. 5443, pp. 215-234, 2009.
[15] T. Okamoto and K. Takashima, "Hierarchical predicate encryption for inner-products," in *Advances in Cryptology - ASIACRYPT 2009. Lecture Notes in Computer Science*, vol. 5912, pp. 214-231, 2009.
[16] L. Ducas, "Anonymity from asymmetry: New constructions for anonymous HIBE," in *CT-RSA 2010, Lecture Notes in Computer Science*, vol. 5985, pp. 148-164, 2010.
[17] M. Edman and B. Yener, "On anonymity in an electronic society: A survey of anonymous communication systems," *ACM Computing Surveys*, vol. 42, no. 1, article 5, 2009.
[18] M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval, "Key-privacy in public-key encryption," in *Advances in Cryptology – ASIACRYPT 2001. Lecture Notes in Computer Science*, vol. 2248, pp. 566-582, 2001.
[19] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public-key encryption with keyword search," in *Advances in Cryptology - EUROCRYPT 2004. Lecture Notes in Computer Science*, vol. 3027, pp. 506-522, 2004.
[20] E. Shi, J. Bethencourt, T.H. Chan, D. Song, and A. Perrig, "Multi-dimensional range query over encrypted data," in *IEEE Symposium on Security and Privacy 2007*, pp. 350-364, 2007.
[21] D.M. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in *Advances in Cryptology - EUROCRYPT 2010, Lecture Notes in Computer Science*, vol. 6110, pp. 44-61, 2010.
[22] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute based encryption for fine-graned access control of encrypted data," in *ACM Conference on Computer and Communications Security 2006*, pp. 89-98, 2006.

[23] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Advances in Cryptology - Asiacrypt 2001. Lecture Notes in Computer Science*, vol. 2248, pp. 514-532, 2001.
[24] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Advances in Cryptology - EUROCRYPT 2004. Lecture Notes in Computer Science*, vol. 3027, pp. 56-73, 2004.
[25] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *Advances in Cryptology - EUROCRYPT 2004. Lecture Notes in Computer Science*, vol. 3027, pp. 207-222, 2004.
[26] X. Boyen, "General ad hoc encryption from exponent inversion IBE," in *Advances in Cryptology - EUROCRYPT 2007, Lecture Notes in Computer Science*, vol. 4515, pp. 394-411, 2007.
[27] A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Advances in Cryptology - EUROCRYPT 2005. Lecture Notes in Computer Science*, vol. 3494, pp. 457-473, 2005.
[28] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *TCC 2007. Lecture Notes in Computer Science*, vol. 4392, pp. 535-554, 2007.
[29] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Advances in Cryptology - EUROCRYPT 2008. Lecture Notes in Computer Science*, vol. 4965, pp. 146-162, 2008.
[30] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in *Advances in Cryptology - EUROCRYPT 2003. Lecture Notes in Computer Science*, vol. 2656, pp. 255-271, 2003.
[31] Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers," in *Digital Rights Management Wrokshop, Lecture Notes in Computer Science*, vol. 2696, pp. 61-80, 2002.

Kwangsu Lee received his B.Sc. degree in Computer Science from the Yonsei University in Korea and M.Sc. degree in Computer Science from the Korea Advanced Institute of Science and Technology (KAIST) in Korea in 1998 and 2000, respectively. From 2000 to 2006, he worked for SoftForum Co. and Samsung Networks Co. He is currently a Ph.D. student of Graduate School of Information Management and Security in the Korea University. His research interests include cryptography, provable security, and pairing-based cryptography.

Dong Hoon Lee is a professor of Graduate School of Information Management and Security of the Korea University in Korea. He received his B.S (1985) of Economics from the Korea University, M.Sc. (1988) from the University of Oklahoma, and Ph.D. (1992) from the University of Oklahoma. He was a faculty member at the University of Dankook of Korea from 1992 to 1993 before he joined the Korea University in 1993. He was an Editor-in-Chief at Korea Institute of Information Security and Cryptology (KIISC, 2002), Program Co-Chair of ICISC (International Conference on Information Security and Cryptology) Program Committee. He has been a chairman at Electronics Election Research (EER) and Mobile Payment Standard Association (MPSA). He is the leading researcher on Information Security, Cryptology, and Ubiquitous Security Study.