5-2016

Anonymous identity-based broadcast encryption with chosen-ciphertext security

Kai HE

Jian WENG

Jia-Nan LIU

Joseph K. LIU

Wei LIU

See next page for additional authors

DOI: https://doi.org/10.1145/2897845.2897879

Anonymous Identity-Based Broadcast Encryption with Chosen-Ciphertext Security

Kai He
Department of Computer Science,Jinan University,Guangzhou 510632, China
Faculty of Information Technology,Monash University,Australia
hekai1214@yahoo.com

Jian Weng*
Department of Computer Science
Jinan University,Guangzhou 510632, China
cryptjweng@gmail.com

Jia-Nan Liu
Department of Computer Science
Jinan University
Guangzhou 510632, China
j.n.liu@foxmail.com

Joseph K. Liu
Faculty of Information Technology
Monash University
Australia
ksliu9@gmail.com

Wei Liu
Department of Computer Science
Jinan University
Guangzhou 510632, China
WeiLiuscholar@gmail.com

Robert H. Deng
School of Information Systems
Singapore Management University
Singapore 178902
robertdeng@smu.edu.sg

ABSTRACT

In this paper, we propose the first identity-based broadcast encryption scheme, which can simultaneously achieves confidentiality and full anonymity against adaptive chosen-ciphertext attacks under a standard assumption. In addition, two further desirable features are also provided: one is fully-collusion resistant which means that even if all users outside of receivers S collude they cannot obtain any information about the plaintext. The other one is stateless which means that the users in the system do not need to update their private keys when the other users join or leave the system. In particular, our scheme is highly efficient, where the public parameters size, the private key size and the decryption cost are all independent to the number of the receivers.

Keywords

anonymous; identity-based broadcast encryption; adaptive chosen-ciphertext security; weakly robust; random oracle model

1. INTRODUCTION

Broadcast encryption (BE) was first introduced by Fiat and Naor [17]. In a BE system, a sender encrypts a message to a set of receivers S over an insecure channel, only the users in the set S can decrypt, while the other users outside of S cannot decrypt. In particular, BE can save computational cost and communication load relatively to repeatedly utilize point-to-point traditional encryption. Thus, BE brings many practical applications, such as encrypted file sharing [25], satellite TV subscription services [13], digital right management [24], social network service [19].

Chosen-ciphertext security [27, 28, 5, 15] is a desirable security notion for public key encryption (PKE) schemes, where there exists some active attackers who may potentially modify the transmissive messages. It is a more stronger security notion than a chosen-plaintext security where the attacker can only obtain the ciphertexts for arbitrary plaintexts. A public-key BE [14] (hereinafter referred to as BE) is a specific type of PKE, in which any sender can create a ciphertext by using the public keys of receivers S. Specially, it is preferable security if the BE system is not only chosen-ciphertext security, but also fully collusion-resistance security [7], which captures the intuition that even if all users outside of S collude, they cannot obtain any information about the plaintext. In the aspect of function, stateless receivers is a desirable property for BE system [14, 26], where the users in the system do not (necessarily) update their private keys when the other users join or leave. In 2005, Boneh, Gentry, and Waters [6] proposed the first stateless and fully-collusion resistant BE scheme with chosen-ciphertext security. However, it was proven to be secure in the selective security model under q-type assumptions. The selective security requires an adversary to declare the attacked targets before it obtains the public parameters. Until 2009, Gentry and Waters [18] proposed a BE scheme with adaptive secure without random oracle. The adaptive secure allows an adversary to declare the attacked targets after it receives the public parameters. That is selective security model is weaker security model than adaptive security model.

*The Corresponding Author.

ASIA CCS'16 May 30-June 3, 2016, Xi'an, China

http://dx.doi.org/10.1145/2897845.2897879

Anonymity is another security requirement for encryption schemes, it means that anyone cannot obtain the identities of receivers from the ciphertexts. For example: when a customer orders some sensitive TV programs, the customer usually does not expect any other customers know him subscribe programs. In particular, the issue has received more and more attention in various fields of cryptography so far, such as key-privacy public key encryption scheme [4], anonymous identity-based encryption schemes [1, 9, 10], attribute-based encryption with hidden policy scheme [22], predicate encryption with hidden-vector scheme [20]. In particular, in 2006, Barth, Boneh and Waters [3] presented two fully anonymous BE constructions with chosen-ciphertext security. One is a generic construction, which is based on a chosen-ciphertext secure anonymous PKE schemes in standard model, but the decryption cost is linear with the number of receivers, and the other one is an improved construction which requires a constant number of decryption operations, whereas the security proof relies on the random oracle model. In 2012, Libert, Paterson and Quaglia [23] also presented some fully anonymous BE constructions with adaptive chosen-ciphertext security in the standard model and gave a formal security definition for anonymous BE schemes. At the same year, Fazio and Perera [16] proposed two outsider-anonymous BE constructions with sublinear ciphertexts and have proven their constructions against adaptive chosen-plaintext attack (CPA) and adaptive chosen-ciphertext attack (CCA) in standard model, respectively.

Identity-based broadcast encryption (IBBE) is a specific case of broadcast encryption [30], in which the users' public key can be an arbitrary string provided that the string can uniquely identify the user, such as passport number, email address. It has been drawn more and more attentions. In 2005, Baek, Safavi-Naini and Susilo [2] proposed the first efficient multi-receiver IBE scheme, which is a selectively CCA-secure in random oracle model. It is noteworthy that any multi-receiver IBE scheme can be transformed into a identity-based BE (IBBE) scheme. In 2007, Delerablee [12] proposed the first IBBE scheme with constant size ciphertexts and private keys, and it is also selectively CCA-secure in random oracle model. In 2009, Gentry and Waters [18] presented the first adaptively CPA-secure IBBE scheme in standard model. In 2014, Boneh and Waters [8] gave the first selectively CCA-secure IBBE from multilinear maps with constant size ciphertexts. In 2015, Kim, Susilo, Au and Seberry presented an adaptively CCA-secure IBBE scheme [21] in standard model through employing dual system encryption technique. However, all of these schemes cannot obtain anonymity. As the receivers' identities are transmitted as a part of the ciphertext. It completely leaks the identities of receivers.

In order to issue this problem, in the literature, there exists some anonymous IBBE schemes. Here we discuss some of the state-of-the-art ones. In 2013, Zhang and Takagi [34] proposed two fully anonymous multi-receiver IBE schemes with adaptive CCA security in the random oracle. However, insider-anonymous in their first scheme was attacked by Zhang and Mao [32] and the security proof for their second scheme was not provided. Additionally, Zhang and Mao [32] gave a new anonymous multi-receiver IBBE scheme, and they declared that their scheme can obtain CCA security. However, we found that there exists a flaw in their proof, that is they confused the hash function with the hash oracle. At the same year, Zhang, Wu and Mu [33] presented a fully anonymous IBBE schemes with adaptive CPA security in a composite group. In 2014, Ren, Niu and Zhang [29] proposed a fully anonymous IBBE scheme with adaptive CPA security in standard model. At the same year, Xie and Ren [31] proposed an outsider-anonymous IBBE with adaptive CPA security in standard model. However, none of these schemes can achieve confidentiality and anonymity simultaneously with adaptive CCA security.

Our Contributions To address the challenge mentioned above, in this paper, we propose a secure anonymous IBBE scheme under a standard (DBDH) assumption. Firstly, our scheme is the first IBBE scheme that can simultaneously satisfy confidentiality and anonymity with adaptive CCA security. Secondly, our scheme has some desirable features which are fully collusion resistant and stateless. Thirdly, our scheme is highly efficient, and it has constant public parameters size, private key size and decryption time. Finally, we define a new security notion for IBBE scheme which is named weakly robust under chosen-ciphertext attacks (WROB-CCA).

The remainder of the paper is organized as follows. In Section 2, we review some fundamental backgrounds necessary to understand our paper, which includes Bilinear Groups, DBDH assumption and Target Collision Resistant (TCR) hash function. Next, we give the formal definition and security notions of IBBE scheme in Section 3. In Section 4, we present our anonymous IBBE scheme and prove its security. In Section 5, we compare the performance and the simulation results between our scheme and the other schemes (BE schemes and IBBE schemes). Finally, we draw conclusions in Section 6.

2. PRELIMINARIES

2.1 Bilinear Groups

We briefly review the concept of Bilinear groups which is the underlying algebraic structure of many IBBE including ours. G is an algorithm, which takes as input a security parameter λ and outputs a tuple $(p, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are multiplicative cyclic groups of prime order p, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a map, which has the following properties: **Bilinearity:** $e(u^a, v^b) = e(u, v)^{ab}$ for all $u, v \in \mathbb{G}$ and $\forall a, b \in \mathcal{Z}_p$. **Non-degeneracy:** $e(g, g) \neq 1_{\mathbb{G}}$, where g is a generator of $\mathbb{G}$. **Computability:** There exists an efficient algorithm to compute $e(u, v)$ for $\forall u, v \in \mathbb{G}$.

2.2 Decisional Bilinear Diffie-Hellman (DBDH) Assumption

The decisional BDH problem in a bilinear group $(p, \mathbb{G}, \mathbb{G}_T, e)$ is as follows: Given a tuple (g, g^a, g^b, g^c, Z) for $a, b, c \leftarrow_R \mathcal{Z}_p$ as input, output 1 if $Z = e(g, g)^{abc}$ and 0 otherwise. For a probabilistic algorithm $\mathcal{A}$, we define its advantage in solving the DBDH problem as:

$$Adv_{\mathcal{A}}^{\text{DBDH}} = |\Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[\mathcal{A}(g, g^a, g^b, g^c, Z) = 1]|$$

where g is a random generator in $\mathbb{G}$ and $Z \leftarrow_R \mathbb{G}_T$.

We say that the decisional BDH assumption holds in the bilinear map $(p, \mathbb{G}, \mathbb{G}_T, e)$ if all probabilistic polynomial-time (PPT) algorithms have a negligible advantage in solving the DBDH problem.

2.3 Target Collision Resistant hash function

In a TCR hash function family $\mathcal{H}$, choose a hash function $H \in_R \mathcal{H}$ and a random value x from the definition domain of the hash function H. For any PPT adversary $\mathcal{A}$, it is infeasible to succeed in finding a collision such that $H(y) = H(x)$ with $y \neq x$.

Informally, we define $\mathcal{A}$'s advantage in attacking the target collision resistance of hash function H as $Adv^{\text{TCR}}_{H,\mathcal{A}} = \Pr[\mathcal{A}$ succeeds in finding collisions]. For any PPT adversary $\mathcal{A}$ and any hash function $H \in_R \mathcal{H}$, if the advantage function $Adv^{\text{TCR}}_{H,\mathcal{A}}$ is negligible, we say the TCR hash function family $\mathcal{H}$ is a target collision resistant.

3. IDENTITY-BASED BROADCAST ENCRYPTION

We present the definition and security notions for IBBE scheme in the following [12, 23].

DEFINITION 1. *An identity-based broadcast encryption scheme, associated with message space $\mathcal{M}$, consists of a tuple of four algorithms* (Setup, Extract, Encrypt, Decrypt)*:*

- **Setup**(1^λ): On input a security parameter λ, output the public parameters $params$ and a master secret key msk.
- **Extract**(msk, ID): On input a master secret key msk and an identity ID, output a private key sk_{ID} for the identity ID.
- **Encrypt**$(params, S, M)$: On input the public parameters $params$, a receiver set S and a message $M \in \mathcal{M}$, output a ciphertext CT.
- **Decrypt**$(params, sk_{ID}, CT)$: On input the public parameters $params$, a private key sk_{ID} and a ciphertext CT, output either a message M or the error symbol $\perp$.

The correctness property requires that, for all $ID \in S$, if $(params, msk) \leftarrow \mathsf{Setup}\ (1^\lambda)$, $sk_{ID} \leftarrow \mathsf{Extract}\ (msk, ID)$ and $CT \leftarrow \mathsf{Encrypt}\ (params, S, M)$, then $\mathsf{Decrypt}\ (params, sk_{ID}, CT) = M$ with overwhelming probability.

Remark: Identity-based encryption is a special case of identity-based broadcast encryption, when the size of the receiver set is only one.

Next, we shall define the security notions for IBBE scheme. First, we review the notion of indistinguishability under chosen-ciphertext attacks (IND-CCA), which means that the ciphertext does not leak any information of the message. Then, we review the security notion of anonymity under chosen-ciphertext attacks (ANO-CCA), which means that the ciphertext does not leak the identities in the receiver set. Last, we define a new security notion named weakly robust against chosen-ciphertext attacks (WROB-CCA). It guarantees that decryption attempts fail with high probability if the "wrong" private key is used.

We define the IND-CCA security game for IBBE as follows. Let $\mathcal{A}$ be a PPT adversary, $\mathcal{A}$ interacts with challenger $\mathcal{C}$ in the following games.

The IND-CCA Game:

- **Setup:** Challenger $\mathcal{C}$ runs $(params, msk) \leftarrow \mathsf{Setup}(1^\lambda)$, and then sends $params$ to adversary $\mathcal{A}$ and keeps the master secret key msk itself.
- **Phase 1:** Adversary $\mathcal{A}$ adaptively issues the following queries:
  - Extraction Query: On input an identity ID, challenger $\mathcal{C}$ returns $sk_{ID} \leftarrow \mathsf{Extract}(msk, ID)$ to adversary $\mathcal{A}$.
  - Decryption Query: On input an identity ID and a ciphertext CT, challenger $\mathcal{C}$ returns $m \leftarrow \mathsf{Decrypt}$ $(params, sk_{ID}, CT)$ to adversary $\mathcal{A}$, where $sk_{ID} \leftarrow \mathsf{Extract}(msk, ID)$.
- **Challenge:** Adversary $\mathcal{A}$ submits two distinct equal-length messages $M_0, M_1 \in \mathcal{M}$ and a receiver set S^* to challenger $\mathcal{C}$. It is required that $\mathcal{A}$ has not issued Extraction Query on $ID \in S^*$. Challenger $\mathcal{C}$ flips a random coin $\beta \in \{0, 1\}$ and returns the challenge ciphertext $CT^* \leftarrow \mathsf{Encrypt}\ (params, S^*, M_\beta)$ to adversary $\mathcal{A}$.
- **Phase 2:** Adversary $\mathcal{A}$ continues to adaptively issue queries as in Phase 1 subject to the following restrictions: (i) $\mathcal{A}$ cannot issue *Extraction Query* on ID, where $ID \in S^*$; (ii) $\mathcal{A}$ cannot issue Decryption Query on (ID, C^*), where $ID \in S^*$.
- **Guess:** Adversary $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$.

DEFINITION 2. *We define adversary $\mathcal{A}$'s advantage in* IND-CCA Game *as $Adv^{\text{IND-CCA}}_{\mathcal{A},IBBE} = |\Pr[\beta' = \beta] - 1/2|$. We say that an* IBBE *scheme is* IND-CCA secure*, if for any* PPT *adversary $\mathcal{A}$, the advantage $Adv^{\text{IND-CCA}}_{\mathcal{A},IBBE}$ is negligible in* IND-CCA Game*.*

We define the ANO-CCA security game for IBBE as follows.

The ANO-CCA Game:

- **Setup:** It is the same as in the IND-CCA Game.
- **Phase 1:** It is the same as in the IND-CCA Game.
- **Challenge:** $\mathcal{A}$ submits a message M^* and two distinct sets S_0, S_1 to $\mathcal{C}$. It is required that $|S_0| = |S_1|$ and $\mathcal{A}$ has not issued *Extraction Query* on $ID \in S_0 \triangle S_1$, where $S_0 \triangle S_1$ denotes $S_0 \cup S_1 - S_0 \cap S_1$. $\mathcal{C}$ flips a random coin $\beta \in \{0, 1\}$ and returns the challenge ciphertext $CT^* \leftarrow \mathsf{Encrypt}(params, S_\beta, M^*)$ to $\mathcal{A}$.
- **Phase 2:** $\mathcal{A}$ continues to adaptively issue queries as in Phase 1 with the restrictions as follows: (i) $\mathcal{A}$ cannot issue *Extraction Query* on ID, where $ID \in S_0 \triangle S_1$; (ii) $\mathcal{A}$ cannot issue *Decryption Query* on (ID, C^*), where $ID \in S_0 \triangle S_1$.
- **Guess:** $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$.

DEFINITION 3. *We define adversary $\mathcal{A}$'s advantage in the above* ANO-CCA Game *as $Adv^{\text{ANO-CCA}}_{\mathcal{A},IBBE} = |\Pr[\beta' = \beta] - 1/2|$. We say that an* IBBE *scheme is* ANO-CCA secure*, if for any* PPT *adversary $\mathcal{A}$, the advantage $Adv^{\text{ANO-CCA}}_{\mathcal{A},IBBE}$ is negligible in the above* ANO-CCA Game*.*

Remark: Note that the definition captures not only outsider attacks but also insider attacks. In other words, even when an identity $ID \in S_0 \cap S_1$ is corrupted, the anonymity of any non-corrupted $ID \in S_0 \triangle S_1$ is still preserved.

We define the WROB-CCA security game for IBBE as follows.

The WROB-CCA Game:

- **Setup:** It is the same as in the IND-CCA Game.
- **Query Phase:** It is the same as Phase 1 in the IND-CCA Game.
- **Output:** Adversary $\mathcal{A}$ outputs a message M, a receiver set $S^* = \{ID_1, ID_2, \cdots, ID_t\}$, where $|S^*| = t$. $\mathcal{C}$ outputs the challenge ciphertext $CT^* \leftarrow$ Encrypt $(params, S^*, M)$.

We say that $\mathcal{A}$ wins the WROB-CCA Game if Decrypt $(params, sk_{ID^*}, CT^*) \neq \perp$, where $ID^* \notin S^*$ and sk_{ID^*} = Extract (msk, ID^*). It is required that $\mathcal{A}$ has not issued *Extraction Query* on ID^* in Query Phase.

We define adversary $\mathcal{A}$'s advantage as the probability of that $\mathcal{A}$ wins.

Definition 4. *We say that an* IBBE *scheme is* WROB-CCA secure*, if for all* PPT *adversaries $\mathcal{A}$, the advantage of winning the above* WROB-CCA Game *is negligible.*

Remark: The above security notions of IND-CCA, ANO-CCA and WROB-CCA can be naturally defined for an identity-based encryption (IBE) scheme by limiting the size of the receiver set to be only one.

4. AN EFFICIENT ANONYMOUS IBBE CONSTRUCTION

In this section, we present a highly efficient anonymous IBBE construction. Hereon, we simply introduce some notations throughout this construction. For two strings x, y, let $[x]_\ell$ denote the first ℓ bits of x, $[x]^\ell$ denote the last ℓ bits of x, and $x||y$ denote that x connects with y.

4.1 Construction

- **Setup**(1^λ): On input a security parameter λ, it first generates a bilinear group $(p, \mathbb{G}, \mathbb{G}_T, e)$, where p is a λ-bit prime, $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups with prime order p, e is a bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, and then it picks generators $g, u, v, w \in_R \mathbb{G}$, chooses $\alpha \in_R \mathbb{Z}_p$ as a master secret key, computes $g_1 = g^\alpha$, and chooses cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}, H_2 : \mathbb{G}_T \rightarrow \mathbb{Z}_p$, $H_3 : \mathbb{Z}_p \times \mathbb{G} \rightarrow \{0,1\}^l$ and a target collision-resistant hash function $H_4 : \mathbb{G} \times \{0,1\}^\ell \times {\mathbb{Z}_p}^t \rightarrow \mathbb{Z}_p$. The public parameters are $params = (p, \mathbb{G}, \mathbb{G}_T, e, g, g_1, u, v, w, H_1, H_2, H_3, H_4)$ and the master secret key is $msk = \alpha$.
- **Extract**(msk, ID): On input master secret key msk and identity $ID \in \{0,1\}^*$, it first computes $Q_{ID} = H_1(ID)$, and then outputs the private key $sk_{ID} = Q_{ID}^\alpha$ for identity ID.
- **Encrypt**$(params, S, m)$: On input public parameters $params$, receiver set $S = \{ID_1, ID_2, \cdots, ID_t\}$ and message $m \in \{0,1\}^{\ell_1}$, it picks r, k, $\tau \in_R \mathbb{Z}_p$ and computes $C_0 = g^r$. For each $ID_i \in S$, it sets $V_{ID_i} = H_2(e(Q_{ID_i}, g_1)^r)$, $f(x) = \prod_{i=1}^{t}(x - V_{ID_i}) + k = \sum_{j=0}^{t-1} a_j x^j + x^t \pmod p$, which a_j is the coefficient correspond to x^j. $C_1 = [H_3(k||C_0)]_{\ell-\ell_1} || ([H_3(k||C_0)]^{\ell_1} \oplus m)$, $h = H_4(C_0, C_1, a_0, \cdots, a_{t-1})$, $C_2 = (u^h v^\tau w)^r$. The ciphertext is $CT = (\tau, C_0, C_1, C_2, a_0, a_1, \cdots, a_{t-1})$.
- **Decrypt**$(params, sk_{ID}, CT)$: On input public parameters $params$, private key sk_{ID} and ciphertext $CT = (\tau, C_0, C_1, C_2, a_0, a_1, \cdots, a_{t-1})$, it computes $h = H_4(C_0, C_1, a_0, a_1, \cdots, a_{t-1})$, and then checks whether $e(C_0, u^h v^\tau w) = e(g, C_2)$ holds. If not, it outputs $\perp$. Otherwise, it computes $V_{ID} = H_2(e(sk_{ID}, C_0))$ and $k = f(V_{ID}) = \sum_{j=0}^{t-1} a_j (V_{ID})^j + {V_{ID}}^t \pmod p$. If $[C_1]_{\ell-\ell_1} \neq [H_3(k||C_0)]_{\ell-\ell_1}$, it outputs $\perp$. Otherwise, it outputs $m = [H_3(k \,||\, C_0)]^{\ell_1} \oplus [C_1]^{\ell_1}$.

4.2 Security Analysis

We shall prove that the above IBBE construction is WROB-CCA secure, IND-CCA secure and ANO-CCA seucre.

First, we shall prove the IBBE construction is WROB-CCA security. As the property of WROB-CCA security is needed when we prove the above construction to be IND-CCA security and ANO-CCA security.

The following theorem states the above IBBE construction is WROB-CCA security.

Theorem 1. *Suppose H_1, H_2, H_3 are random oracles, then the above* IBBE *construction is* WROB-CCA *secure.*

Proof. Suppose there exists a WROB-CCA adversary $\mathcal{A}$ against the above IBBE construction, it is easy to construct a PPT algorithm $\mathcal{B}$ that makes use of $\mathcal{A}$ to break the randomness of H_1, H_2, H_3 oracles's outputs. $\mathcal{B}$ runs $\mathcal{A}$ as follows.

- **Setup.** $\mathcal{B}$ chooses bilinear groups $(p, \mathbb{G}, \mathbb{G}_T, e)$ of prime order p, picks generators $g, u, v, w \in_R \mathbb{G}$, chooses $\alpha \in_R \mathbb{Z}_p$ as the master secret key, and sets $g_1 = g^\alpha$. $\mathcal{A}$ is given the public parameters $params = (p, \mathbb{G}, \mathbb{G}_T, e, g, g_1, u, v, w, H_1, H_2, H_3, H_4)$, where H_1, H_2, H_3 are random oracles controlled by $\mathcal{B}$ and H_4 is collision-resistant hash function. $\mathcal{B}$ keeps the master private key α itself.
- **Query Phase.** $\mathcal{A}$ adaptively issues queries as follows:
  - *$Hash_1$ Query*: On input ID, $\mathcal{B}$ does the following: If there exists a record $\langle ID, Q, q\rangle$ in the H_1-list, which the list is initialized empty, it returns Q; else it selects $q \in_R \mathbb{Z}_p$, computes $Q = g^q \in \mathbb{G}$, and adds $\langle ID, Q, q\rangle$ into the H_1-list, it returns Q to $\mathcal{A}$.
  - *$Hash_2$ Query*: On input X, $\mathcal{B}$ does the following: If there exists a record $\langle X, v\rangle$ in the H_2-list, which the list is initialized empty, it returns v to $\mathcal{A}$; else, it selects $v \in_R Z_q^*$, adds $\langle X, v\rangle$ into the H_2-list, returns v to $\mathcal{A}$.
  - *$Hash_3$ Query*: On input $\langle k, C_0\rangle$, $\mathcal{B}$ does the following: If there exists a record $\langle k, C_0, K\rangle$ in the H_3-list, which the list is initialized empty, it returns K; else, it selects $K \in_R \{0,1\}^\ell$, and adds $\langle k, C_0, K\rangle$ into H_3-list, it returns K to $\mathcal{A}$.
  - *Extraction Query*: On input ID, $\mathcal{B}$ first queries $Hash_1$ Query on ID, suppose that $\langle ID, Q, q\rangle$ be the corresponding tuple in the H_1-list. Then $\mathcal{B}$ computes $sk_{ID} = Q^\alpha = g^{\alpha q}$ and sends sk_{ID} to $\mathcal{A}$.
  - *Decryption Query*: $\mathcal{A}$ inputs $\langle ID, CT\rangle$, $\mathcal{B}$ can use master private key α to answer any *Decryption Query* to $\mathcal{A}$.

- **Output.** $\mathcal{A}$ outputs message $M \in \{0,1\}^{\ell_1}$ and receiver set $S^* = (ID_1^*, ID_2^*, \cdots, ID_t^*)$, where $|S^*| = t$. $\mathcal{B}$ runs $CT \leftarrow \mathsf{Encrypt}(params, S^*, M)$ as follows: Pick $r, k^*, \tau^* \in_R \mathbb{Z}_p$, for all $ID_i^* \in S^*$, compute $C_0^* = g^r$, $V_{ID_i^*}^* = H_2(e(g_1, H_1(ID_i^*))^r)$, $f(x) = \prod_{i=1}^{t}(x - V_{ID_i^*}^*) + k^* = \sum_{j=0}^{t-1} a_j^* x^j + x^t \pmod p$, output $\{a_0^*, \cdots, a_{t-1}^*\}$, which a_j^* is the coefficient correspond to x^j. $C_1^* = [H_3(k^*||C_0^*)]_{\ell-\ell_1} ||([H_3(k^*||C_0^*)]^{\ell_1} \oplus M)$, $h^* = H_4(C_0^*, C_1^*, a_0^*, \cdots, a_{t-1}^*)$, $C_2^* = (u^{h^*} v^{\tau^*} w)^r$. The challenge ciphertext: $CT^* = (\tau^*, C_0^*, C_1^*, C_2^*, a_0^*, a_1^*, \cdots, a_{t-1}^*)$. If $\mathsf{Decrypt}(params, sk_{ID^*}, CT^*) \neq \perp$, where $ID^* \notin S^*$ and $sk_{ID^*} \leftarrow \mathsf{Extract}(msk, ID^*)$. It is required that $\mathcal{A}$ has not issued *Extraction Query* on ID^* in Query Phase. Then $\mathcal{A}$ wins.

Analysis: If $\mathcal{A}$ wins the WROB-CCA game, then there exists some $M' \neq \perp$, such that $\mathsf{Decrypt}(params, sk_{ID^*}, CT^*) = M'$ and $ID^* \notin S^*$, it implies that there exists a k', such that $C_1^* = [H_3(k'||C_0^*)]_{\ell-\ell_1}||([H_3(k'||C_0^*)]^{\ell_1} \oplus M')$, where $k' = f(V'_{ID^*})$, $V'_{ID^*} = H_2(e(sk_{ID^*}, C_0^*))$. However, for $ID_i^* \in S$, $C_1^* = [H_3(k^*||C_0^*)]_{\ell-\ell_1}||([H_3(k^*||C_0^*)]^{\ell_1} \oplus M)$, where $k^* = f(V_{ID_i^*}^*)$, $V_{ID_i^*}^* = H_2(e(sk_{ID_i^*}, C_0^*))$.

However, the advantage of $\mathcal{A}$ winning the game is negligible.

1. If $k' = k^*$, namely $f(V'_{ID^*}) = f(V_{ID_i^*}^*)$, since $f(x) = \prod_{i=1}^{t}(x - V_{ID_i^*}^*) + k^*$ for $ID_i^* \in S^*$, then we get $\prod_{i=1}^{t}(V'_{ID^*} - V_{ID_i^*}^*) = 0$. It means that these exists some $V_{ID_i^*}^*$, such that $V'_{ID^*} = V_{ID_i^*}^*$, that is $H_2(X'_{ID^*}) = H_2(X_{ID_i^*}^*)$. As H_2 is a random oracle, so $X'_{ID^*} = X_{ID_i^*}^*$. As $X'_{ID^*} = e(H_1(ID^*), g_1)^r$ and $X_{ID_i^*}^* = e(H_1(ID_i^*), g_1)^r$, it implies $H_1(ID^*) = H_1(ID_i^*)$, As H_1 is a random oracle, then $ID^* = ID_i^*$, but it is contradictory with $ID^* \notin S^*$. So we know $k' = k^*$ is not correct.

2. If $k' \neq k^*$, as H_3 is a random oracle, then $[H_3(k' \,||\, C_0^*)]_{\ell-\ell_1} \neq [H_3(k^*||C_0^*)]_{\ell-\ell_1}$. However, $[H_3(k^*||C_0^*)]_{\ell-\ell_1} = [C_1^*]_{\ell-\ell_1}$, then $[H_3(k'||C_0^*)]_{\ell-\ell_1} \neq [C_1^*]_{\ell-\ell_1}$.

So $\mathcal{A}$ can only get $\perp$, it is contradictory with $M' \neq \perp$. So the advantage of $\mathcal{A}$ winning the game is negligible. □

Next, we shall prove the above IBBE construction is IND-CCA security.

THEOREM 2. *Suppose that H_1, H_2, H_3 are random oracles, the above* IBBE *construction is* WROB-CCA *secure and the* DBDH *assumption holds, then the above* IBBE *construction is* IND-CCA *secure.*

PROOF. Suppose there exists an IND-CCA adversary $\mathcal{A}$ against the above IBBE scheme. It is easy to construct a PPT algorithm $\mathcal{B}$ that makes use of $\mathcal{A}$ to solve the DBDH problem or break the IBBE construction's WROB-CCA security. Algorithm $\mathcal{B}$ is given a random tuple (g, g^a, g^b, g^c, Z), that is either sampled from $\mathcal{P}_{\mathcal{BDH}}$ (where $Z = e(g,g)^{abc}$) or from $\mathcal{R}_{\mathcal{BDH}}$ (where Z is uniform and independent in G_T). $\mathcal{B}$ runs $\mathcal{A}$ to execute the following steps.

- **Setup.** $\mathcal{B}$ sets $g_1 = g^a, u = g^{bx_1} g^{x_2}, v = g^{by_1} g^{y_2}, w = g^{bz_1} g^{z_2}$, where $x_1, x_2, y_1, y_2, z_1, z_2 \in_R \mathbb{Z}_p$, $\mathcal{A}$ is given the public parameters $params = (p, \mathbb{G}, \mathbb{G}_T, g, g_1, u, v, w, H_1, H_2, H_3, H_4)$, where H_1, H_2, H_3 are random oracles controlled by $\mathcal{B}$ and H_4 is target collision-resistant hash function. The master secret key a is unknown to $\mathcal{B}$.

- **Phase 1.** $\mathcal{A}$ adaptively issues queries as follows:

  - *$Hash_1$ Query*: On input ID, $\mathcal{B}$ does the following: If there exists a record $\langle ID, Q, q, \varpi \rangle$ in H_1-list, which the list is initially empty, it returns Q; else it generates $\varpi \in_R \{0,1\}$ and selects $q \in_R \mathbb{Z}_p$. If $\varpi = 0$, it computes $Q = g^q$; else it computes $Q = g^{bq}$ and adds $\langle ID, Q, q, \varpi \rangle$ into H_1-list. It returns Q to $\mathcal{A}$.
  - *$Hash_2$ Query*: It is the same as the above WROB-CCA game.
  - *$Hash_3$ Query*: It is the same as the above WROB-CCA game.
  - *Extraction Query*: On input ID, $\mathcal{B}$ first issues $Hash_1$ Query on ID to obtain $\langle ID, Q, q, \varpi \rangle$, if $\varpi = 1$, $\mathcal{B}$ outputs $\perp$ and aborts; else it computes $sk_{ID} = g_1^q$ and returns sk_{ID} to $\mathcal{A}$. (Note that $sk_{ID} = g_1^q = g^{aq} = Q^a = H_1(ID)^\alpha$, so this is a proper private key for ID).
  - *Decryption Query*: On input $\langle ID, CT \rangle$, where $CT = (\tau, C_0, C_1, C_2, a_0, a_1, \cdots, a_{t-1})$, $\mathcal{B}$ first issues $Hash_1$ Query on ID to obtain $\langle ID, Q, q, \varpi \rangle$, if $\varpi = 0$, it computes $sk_{ID} = g_1^q$, and then uses this private key to respond the *Decryption Query*; else it does as follows: compute $h = H_4(C_0, C_1, a_0, a_1, \cdots, a_{t-1})$ and check whether $e(C_0, u^h v^\tau w) = e(g, C_2)$ holds. If not, output $\perp$, which indicates an invalid ciphertext; else check whether $x_1 h + y_1 \tau + z_1 = 0$ holds. If so, abort and randomly output a bit; else continue to execute the rest steps: As $C_2 = (u^h v^\tau w)^r = (g^{b(x_1 h + y_1 \tau + z_1)})^r (g^{(x_2 h + y_2 \tau + z_2)})^r = C_0^{b(x_1 h + y_1 \tau + z_1)} C_0^{(x_2 h + y_2 \tau + z_2)}$, and compute $C_0^b = (\frac{C_2}{C_0^{(x_2 h + y_2 \tau + z_2)}})^{\frac{1}{(x_1 h + y_1 \tau + z_1)}}$. So $X_{ID} = e(Q_{ID}, g_1)^r = e(g^{bq}, g_1)^r = e(C_0^b, g_1)^q$. $\mathcal{B}$ issues $Hash_2$ Query on X_{ID} to get V_{ID}, where $V_{ID} = H_2(X_{ID})$, and computes $k = f(V_{ID}) = \sum_{i=0}^{t-1} a_i (V_{ID})^i + (V_{ID})^t$, and then issues $Hash_3$ Query on $\langle k, C_0 \rangle$ to get K, where $K = H_3(k||C_0)$. If $[C_1]_{\ell-\ell_1} \neq [K]_{\ell-\ell_1}$, it outputs $\perp$ which indicates an invalid ciphertext; else it outputs $m = [K]^{\ell_1} \oplus [C_1]^{\ell_1}$.

    Recall that, the public parameters $u = g^{bx_1} g^{x_2}$, $v = g^{by_1} g^{y_2}$, $w = g^{bz_1} g^{z_2}$ for random x_1, x_2, y_1, y_2, z_1, $z_2 \in Z_q^*$, x_1, (y_1, z_1. resp.) is blinded by x_2, (y_2, z_2. resp.), and hence no information about x_1, y_1 and z_1 is leaked to $\mathcal{A}$, and the equality $x_1 h + y_1 \tau + z_1 = 0 \pmod p$ information-theoretically holds with probability at most $\frac{1}{p}$.

- **Challenge.** $\mathcal{A}$ outputs two distinct equal-length messages M_0, M_1 and a receiver set S^*. It required that $\mathcal{A}$ has not issued *Extraction Query* on any ID, where $ID \in S^*$ in Phase 1. For all $ID_i \in S^*$, $\mathcal{B}$ first issues $Hash_1$ Query on ID_i to obtain (ID_i, Q_{ID_i}, q_i, ϖ_i). If there exists some $ID_i \in S^*$ and $\varpi_i = 0$, $\mathcal{B}$ aborts; else for each $ID_i \in S^*$, $\mathcal{B}$ lets $X_{ID_i}^* = Z^{q_i}$ and issues $Hash_2$ Query on $X_{ID_i}^*$ to obtain $V_{ID_i}^*$ from H_2-list, where

$V^*_{ID_i} = H_2(X^*_{ID_i})$. Next, $\mathcal{B}$ randomly chooses $k^* \in \mathbb{Z}_p$, computes $f(x) = \prod_{i=1}^{t}(x - V^*_{ID_i}) + k^* = \sum_{i=0}^{t-1} a_i^* x^i + x^t \pmod p$ and outputs $(a_0^*, a_1^*, \cdots, a_{t-1}^*)$. Let $C_0^* = g^c$, $\mathcal{B}$ issues $Hash_3$ Query on (k^*, C_0^*) to obtain K^*, where $K^* = H_3(k^* || C_0^*)$, $\mathcal{B}$ randomly chooses $\beta \in \{0,1\}$, computes $C_1^* = [K^*]_{\ell-\ell_1} \,||\, ([K^*]^{\ell_1} \oplus M_\beta)$, $h^* = H_4(C_0^*, C_1^*, a_0^*, \cdots, a_{t-1}^*)$, defines $\tau^* = -\frac{x_1 h^* + z_1}{y_1} \in \mathbb{Z}_p$ and compute $C_2^* = (g^c)^{x_2 h^* + y_2 \tau^* + z_2}$. Last, $\mathcal{B}$ outputs the challenge ciphertext: $CT^* = (\tau^*, C_0^*, C_1^*, C_2^*, a_0^*, a_1^*, \cdots, a_{t-1}^*)$.

- **Phase 2.** $\mathcal{A}$ continues to adaptively issue queries as following:
  - *Extraction Query*: $\mathcal{A}$ inputs ID, where $ID \notin S^*$, $\mathcal{B}$ handles them as in Phase 1.
  - *Decryption Query*: $\mathcal{A}$ inputs $\langle ID, CT \rangle$, where $CT = (\tau, C_0, C_1, C_2, a_0, a_1, \cdots, a_{t-1})$.
    - If $CT \neq CT^*$, $\mathcal{B}$ checks if $H_4(C_0, C_1, a_0, \cdots, a_{t-1}) = H_4(C_0^*, C_1^*, a_0^*, \cdots, a_{t-1}^*)$. If so, $\mathcal{B}$ aborts and randomly outputs a bit; else responds as in Phase 1. (Note that, $\mathcal{A}$ can produce such a ciphertext, this would imply a collision in the hash function H_4, but the probability that this event occurs is negligible).
    - If $CT = CT^*$ and $ID \in S^*$, $\mathcal{B}$ outputs $\perp$.
    - If $CT = CT^*$ and $ID \notin S^*$, $\mathcal{B}$ outputs $\perp$ with non-negligible advantage. As the IBBE scheme is WROB-CCA secure, $CT^* \leftarrow$ Encrypt $(params, S^*, M_\beta)$ and Decrypt $(params, sk_{ID}, CT^*) \neq \perp$ is negligible for $ID \notin S^*$.
- **Guess.** $\mathcal{A}$ outputs a bit b'.

  If $b' = b$ then $\mathcal{B}$ outputs 1 meaning $Z = e(g,g)^{abc}$; else it outputs 0 meaning $Z \neq e(g,g)^{abc}$.

Ananysis: When $Z = e(g,g)^{abc}$, assume $r^* = c$, challenge ciphertext issued by $\mathcal{A}$ comes from a distribution identical to that in the actual construction; When Z is uniform and independent in G_T, the ciphtertext $C_1^* = [K^*]_{\ell-\ell_1} \,||\, ([K^*]^{\ell_1} \oplus M_\beta)$, where $K^* = H_3(k^* || C_0^*)$ is uniform and random, so M_β is independent of the adversary $\mathcal{A}$'s view. □

Finally, we shall prove the above IBBE construction is ANO-CCA secure.

THEOREM 3. *Suppose that H_1, H_2, H_3 are random oracles and* DBDH *assumption holds, then the above* IBBE *construction is* ANO-CCA *secure.*

PROOF. Suppose that there exists an ANO-CCA adversary $\mathcal{A}$ against the above IBBE construction. It is easy to construct a PPT algorithm $\mathcal{B}$ makes use of $\mathcal{A}$ to solve the DBDH problem. $\mathcal{B}$ is given as input a random tuple (g, g^a, g^b, g^c, Z), that is either sampled from $\mathcal{P}_{BDH}$ (where $Z = e(g,g)^{abc}$) or from $\mathcal{R}_{BDH}$ (where Z is uniform and independent in G_T). Algorithm $\mathcal{B}$'s goal is to output 1 if $Z = e(g,g)^{abc}$ and 0 otherwise. $\mathcal{B}$ runs $\mathcal{A}$ as follows.

- **Setup.** It is the same as in the Setup of Theorem 2.
- **Phase 1.** It is the same as in the Phase 1 of Theorem 2.
- **Challenge.** $\mathcal{A}$ outputs a message $M \in \{0,1\}^{\ell_1}$ and two distinct receiver sets S_0^*, S_1^*, where there is at least one different user in the two sets. There is no loss generality, assuming that $S_0^* = \{ID_0^*, ID_2, \cdots, ID_t\}$ and $S_1^* = \{ID_1^*, ID_2, \cdots, ID_t\}$. It required that $\mathcal{A}$ has not issued *Extraction Query* on ID such that $ID \in \{ID_0^*, ID_1^*\}$ in Phase 1. Then, $\mathcal{B}$ responds as follows: Let $C_0^* = g^c$, choose a random bit $\beta \in \{0,1\}$, where $S_\beta^* = \{ID_\beta^*, ID_2, \cdots, ID_t\}$. Issue $Hash_1$ Query on ID_β^* to obtain $(ID_\beta^*, Q_\beta^*, q_\beta, \varpi_\beta)$, if $\varpi_\beta = 0$, output $\perp$ and abort; else $Q_{ID_\beta^*} = g^{bq_\beta}$ and $X^*_{ID_\beta^*} = Z^{q_\beta}$, and then issue $Hash_2$ Query on $X^*_{ID_\beta^*}$ to get $V^*_{ID_\beta^*}$, where $V^*_{ID_\beta^*} = H_2(X^*_{ID_\beta^*})$. For the other identities $ID_i \in S_\beta^* \setminus ID_\beta^*$, first issue $Hash_1$ Query on ID_i to obtain $(ID_i, Q_i, q_i, \varpi_i)$, if there exists some $\varpi_i = 1$, output $\perp$ and abort; else compute $Q_{ID_i} = g^{q_i}$ and $X^*_{ID_i} = e(g^{cq_i}, g^a)$. Then, issues $Hash_2$ Query on $X^*_{ID_i}$ to get $V^*_{ID_i}$, where $V^*_{ID_i} = H_2(X^*_{ID_i})$. Next, choose $k^* \in_R \mathbb{Z}_p$, compute $f(x) = (x - V^*_{ID_\beta^*}) \prod_{i=2}^{t}(x - V^*_{ID_i}) + k^* = \sum_{i=0}^{t-1} a_i^* x^i + x^t \pmod p$, output $(a_0^*, a_1^*, \cdots, a_{t-1}^*)$ and issue $Hash_3$ Query on $\langle k^*, C_0^* \rangle$ to get K^*, where $K^* = H_3(k^* || C_0^*)$. Last, compute $C_1^* = [K^*]_{\ell-\ell_1} || ([K^*]^{\ell_1} \oplus M)$, $h^* = H_4(C_0^*, C_1^*, a_0^*, \cdots, a_{t-1}^*)$, set $\tau^* = -\frac{x_1 h^* + z_1}{y_1}$ and $C_2^* = (g^c)^{x_2 h^* + y_2 \tau^* + z_2}$. Output the challenge ciphertext: $CT^* = (\tau^*, C_0^*, C_1^*, C_2^*, a_0^*, a_1^*, \cdots, a_{t-1}^*)$.
- **Phase 2.** $\mathcal{A}$ continues to adaptively issue queries as follows:
  - *Extraction Query*: $\mathcal{A}$ issues *Extraction Query* on ID such that $ID \notin \{ID_0^*, ID_1^*\}$, $\mathcal{B}$ handles them as in Phase 1.
  - *Decryption Query*: $\mathcal{A}$ inputs $\langle ID, CT \rangle$, where $CT = (\tau, C_0, C_1, C_2, a_0, a_1, \cdots, a_{t-1})$, $\mathcal{B}$ performs the following steps:
    - If $CT \neq CT^*$, $\mathcal{B}$ checks if $H_4(C_0, C_1, a_0, \cdots, a_{t-1}) = H_4(C_0^*, C_1^*, a_0^*, \cdots, a_{t-1}^*)$. If so, it aborts, and randomly outputs a bit; else responds as in Phase 1. (Note that $\mathcal{A}$ can produce such a ciphertext, this would represent a target collision in the hash function H_4, and so the probability that this event occurs is negligible).
    - If $CT = CT^*$, for $ID \in \{ID_0^*, ID_1^*\}$, $\mathcal{B}$ outputs $\perp$. For $ID \in S_0^* \cap S_1^*$, $\mathcal{B}$ outputs M. For $ID \notin S_0^* \cup S_1^*$, $\mathcal{B}$ outputs $\perp$ with non-negligible advantage. As the IBBE scheme is WROB-CCA security. That is $CT^* \leftarrow$ Encrypt $(params, S_\beta^*, M)$, and Decrypt$(params, sk_{ID}, CT^*) \neq \perp$ is negligible, for $ID \notin S_0^* \cup S_1^*$.
- **Guess.** $\mathcal{A}$ outputs a bit b'.

  If $b' = b$ then $\mathcal{B}$ outputs 1 meaning $Z = e(g,g)^{abc}$; otherwise, it outputs 0 meaning $Z \neq e(g,g)^{abc}$.

Ananysis: When $Z = e(g,g)^{abc}$, assume $r^* = c$, challenge ciphertext issued by $\mathcal{A}$ comes from a distribution identical to that in the actual construction; When Z is uniform and independent in G_T, the ciphtertext $C_1^* = [K^*]_{\ell-\ell_1} || ([K^*]^{\ell_1} \oplus M_\beta)$, where $K^* = H_3(k^* || C_0^*)$ is uniform and random, so M_β is independent of the adversary $\mathcal{A}$'s view. □

Table 1: Performance Comparisons between IBBE schemes and ours

	PPs Size	Sk Size	CT Size	Dec Time	Security Model	Order	Assumption	Random Oracle	Stateless	Anonymous
[2]	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	sID-CCA	Prime	Gap-BDH	✓	✓	×
[12]	$\mathcal{O}(\ell)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	sID-CPA	Prime	GDDHE	✓	×	×
[18]	$\mathcal{O}(\ell)$	$\mathcal{O}(1)$	$\mathcal{O}(\sqrt{\ell})$	$\mathcal{O}(\sqrt{\ell})$	ID-CPA	Prime	q-type	×	✓	×
[8]	$\mathcal{O}(\log \ell)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	sID-CPA	Prime	l-BDHE	×	×	×
[21]	$\mathcal{O}(\ell)$	$\mathcal{O}(\ell)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	ID-CCA	Composite	GSD	×	✓	×
Ours	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	ID-CCA	Prime	DBDH	✓	✓	✓

Table 2: Performance Comparisons between Anonymous BE schemes and ours

	Anonymity	Security Model	Pk Size	Sk Size	CT Size	Decryption time	Random Oracle	Identity-based
[3]	Fully	sID-CCA	$\mathcal{O}(\ell)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	✓	×
[23]	Fully	ID-CCA	$\mathcal{O}(\ell)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	×	×
[16]	Outsider	ID-CCA	$\mathcal{O}(\ell \log \ell)$	$\mathcal{O}(\ell)$	$\mathcal{O}(r)$	$\mathcal{O}(1)$	×	×
[34]	Outsider	ID-CCA	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	✓	✓
[29]	Fully	ID-CPA	$\mathcal{O}(n)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	×	✓
[33]	fully	ID-CPA	$\mathcal{O}(\ell)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	×	✓
[31]	Outsider	ID-CPA	$\mathcal{O}(\ell)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	×	✓
Ours	Fully	ID-CCA	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	✓	✓

5. PERFORMANCE ANALYSES

In this section, we first compare our scheme with the other IBBE schemes proposed in the literature [2, 12, 18, 8, 21]. The comparisons are summarized in Table 1. Then, we compare our scheme with the other anonymous BE schemes proposed in the literature [3, 23, 16, 34, 33, 29, 31]. The comparisons are summarized in Table 2. Finally, we compare the running time of encryption and decryption between ours and the scheme [34] which achieves low computation cost and light communication load. It is depicted in Figure 1.

Now, let us explain some notations used in Table 1 and Table 2. Here "ℓ" denotes the total number of the system users. "k" denotes the number of receivers. "r" denotes the number of revocation users. "n" denotes the bit length of an identity. "sID" and "ID" denote selective security and adaptive security, respectively.

From Table 1, it's not hard to see that only our scheme is anonymous. The public parameters size, private key size and decryption time are constant just in the scheme [2] and ours. However, the scheme [2] achieves only selective security which is weaker than adaptive security. Although the ciphertext size of ours is linear with the number of receivers and the ciphertext size of schemes [12, 8, 21] are constant, but in those schemes [12, 8, 21] the public parameter size are related with the total number of users and the decryption time are linear with the number of receivers. Meanwhile, the scheme [12] is only selectively secure under GDDHE assumption and has no stateless property. The scheme [8] employed $(\log \ell)$-way multilinear map and also has no stateless property. The scheme [21] employed dual system encryption technique and the private key size are linear with the number of the total users. The public parameters size, ciphertext size and decryption time of scheme [18] are not constant. And it was proved adaptive CPA-security under the decisional Bilinear Diffie-Hellman Exponent (BDHE) assumption. However, our scheme is proved adaptive CCA-security under DBDH assumption and with stateless property.

From Table 2, the schemes [16, 34, 31] are all outside anonymous IBBE schemes. Although the schemes [3, 23, 29, 33] are fully anonymity. But the schemes [3, 23] are not identity-based BE schemes. The schemes [29, 33] are only adaptively CPA-secure, and the decryption cost of the scheme [29] is linear with the number of receivers. However, our scheme is full anonymous scheme with adaptive CCA-secure.

The comparison results indicate that our scheme has a better overall performance and security.

Finally, we evaluate the performance of our anonymous IBBE construction. All the programs were executed on a Win7 PC with Inter(R) Core(TM) i5-3470 CPU @ 3.20GHz processor and 4G DDR3-RAM. We use jPBC libery [11] and JDK 1.7 to implement our construction in software. In order to achieve the practical function, we choose a pairing-friendly type-A 160-bit elliptic cure group. It's worth pointing out that our running setting is the same as in [34] scheme which only achieves outsider anonymity. The running time of encryption and decryption about Zhang et al. scheme [34] and ours are showed in Figure 1. In the aspect of encryption, Zhang et al. scheme [34] has similar computation efficiency with ours. However, in the aspect of decryption, the running time of their scheme is linear with the number of receivers. But the running time of our scheme is almost constant, which is independent of the number of receivers.

6. CONCLUSIONS

In this paper, we construct an IBBE scheme which is the first of its kind that simultaneously achieves confidentiality and anonymity with adaptive CCA-secure under DBDH assumption. Additionally, our scheme permits stateless receivers and supports fully collusion-resistant. In particular, our scheme is highly efficient, and it has constant public parameters size, private key size and decryption time. However, the ciphertext size is linear with the number of the receivers. In our future work, we shall try to construct an anonymous IBBE scheme with constant size ciphertext.

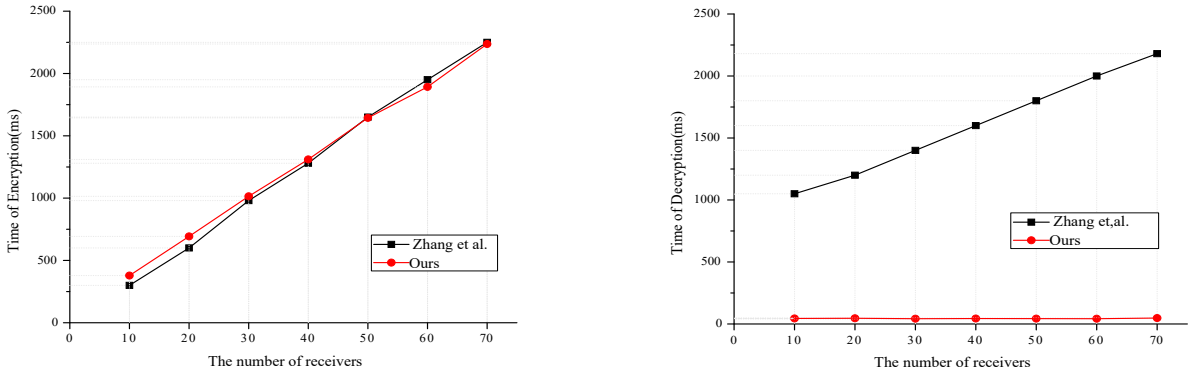

Figure 1: The running time of Encryption and Decryption about Zhang et al. scheme and ours

7. ACKNOWLEDGMENTS

This work was supported by National Science Foundation of China (Grant Nos. 61272413, 61133014, 61272415 and 61472165), Program for New Century Excellent Talents in University (Grant No. NCET-12-0680), Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20134401110011), Foundation for Distinguished Young Talents in Higher Education of Guangdong (Grant No. 2012LYM 0027), the Fundamental Research Funds for the Central Universities (Grant No. 11613106), and this work is also supported by China Scholarship Council.

8. REFERENCES

[1] 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: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, pages 205–222, 2005.

[2] J. Baek, R. Safavi-Naini, and W. Susilo. Efficient multi-receiver identity-based encryption and its application to broadcast encryption. In *Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005, Proceedings*, pages 380–397, 2005.

[3] A. Barth, D. Boneh, and B. Waters. Privacy in encrypted content distribution using private broadcast encryption. In *Financial Cryptography and Data Security, 10th International Conference, FC 2006, Anguilla, British West Indies, February 27-March 2, 2006, Revised Selected Papers*, pages 52–64, 2006.

[4] M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval. Key-privacy in public-key encryption. In *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, pages 566–582, 2001.

[5] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, pages 26–45, 1998.

[6] D. Boneh, X. Boyen, and E. Goh. Hierarchical identity based encryption with constant size ciphertext. *IACR Cryptology ePrint Archive*, 2005:15, 2005. http://eprint.iacr.org/2005/015.

[7] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, pages 258–275, 2005.

[8] D. Boneh, B. Waters, and M. Zhandry. Low overhead broadcast encryption from multilinear maps. In *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, pages 206–223, 2014.

[9] X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption (without random oracles). In *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, pages 290–307, 2006.

[10] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy. Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data. In *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings*, pages 196–214, 2009.

[11] A. De Caro and V. Iovino. jpbc: Java pairing based cryptography. In *Proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC 2011*, pages 850–855, Kerkyra, Corfu, Greece, June 28 - July 1, 2011.

[12] C. Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings*, pages 200–215, 2007.

[13] C. Delerablée, P. Paillier, and D. Pointcheval. Fully collusion secure dynamic broadcast encryption with

constant-size ciphertexts or decryption keys. In *Pairing-Based Cryptography - Pairing 2007, First International Conference, Tokyo, Japan, July 2-4, 2007, Proceedings*, pages 39–59, 2007.

[14] Y. Dodis and N. Fazio. Public key broadcast encryption for stateless receivers. In *Security and Privacy in Digital Rights Management, ACM CCS-9 Workshop, DRM 2002, Washington, DC, USA, November 18, 2002, Revised Papers*, pages 61–80, 2002.

[15] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography (extended abstract). In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 542–552, 1991.

[16] N. Fazio and I. M. Perera. Outsider-anonymous broadcast encryption with sublinear ciphertexts. In *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*, pages 225–242, 2012.

[17] A. Fiat and M. Naor. Broadcast encryption. In *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, pages 480–491, 1993.

[18] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, pages 171–188, 2009.

[19] Y. Jung, Y. Nam, J. Kim, W. Jeon, H. Lee, and D. Won. Key management scheme using dynamic identity-based broadcast encryption for social network services. *Advances in Computer Science and its Applications*, 279:435–443, 2014.

[20] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, pages 146–162, 2008.

[21] J. Kim, W. Susilo, M. H. Au, and J. Seberry. Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. *IEEE Transactions on Information Forensics and Security*, 10(3):679–693, 2015.

[22] X. Li, D. Gu, Y. Ren, N. Ding, and K. Yuan. Efficient ciphertext-policy attribute based encryption with hidden policy. In *Internet and Distributed Computing Systems - 5th International Conference, IDCS 2012, Wuyishan, Fujian, China, November 21-23, 2012. Proceedings*, pages 146–159, 2012.

[23] B. Libert, K. G. Paterson, and E. A. Quaglia. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*, pages 206–224, 2012.

[24] X. Lin, X. Sun, P. Ho, and X. Shen. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE T. Vehicular Technology*, 56(6):3442–3456, 2007.

[25] B. Malek and A. Miri. Adaptively secure broadcast encryption with short ciphertexts. *I. J. Network Security*, 14(2):71–79, 2012.

[26] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 41–62, 2001.

[27] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, pages 427–437, 1990.

[28] C. Rackoff and D. R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, pages 433–444, 1991.

[29] Y. Ren, Z. Niu, and X. Zhang. Fully anonymous identity-based broadcast encryption without random oracles. *I. J. Network Security*, 16(4):256–264, 2014.

[30] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, pages 47–53, 1984.

[31] L. Xie and Y. Ren. Efficient anonymous identity-based broadcast encryption without random oracles. *IJDCF*, 6(2):40–51, 2014.

[32] J. Zhang, Y. Xu, and J. Zou. Comment on wang et al.'s anonymous multi-receiver id-based encryption scheme and its improved schemes. *IJIIDS*, 7(5):400–413, 2013.

[33] L. Zhang, Q. Wu, and Y. Mu. Anonymous identity-based broadcast encryption with adaptive security. In *Cyberspace Safety and Security - 5th International Symposium, CSS 2013, Zhangjiajie, China, November 13-15, 2013, Proceedings*, pages 258–271, 2013.

[34] M. Zhang and T. Takagi. Efficient constructions of anonymous multireceiver encryption protocol and their deployment in group e-mail systems with privacy preservation. *IEEE Systems Journal*, 7(3):410–419, 2013.