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

Follow this and additional works at: http://ink.library.smu.edu.sg/sis_research
Part of the Information Security Commons

Citation
Available at: http://ink.library.smu.edu.sg/sis_research/3350

This Conference Proceeding Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.
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 achieve 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 \( S \). Specialy, 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.
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 an 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 systems 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, G, GT, e), where G and GT are multiplicative cyclic groups of prime order p, and e : G × G → GT is a map, which has the following properties: Bilinearity: e(u,v) = e(u,v), Non-degeneracy: e(g,g) ̸= 1GT, where g is a generator of G. Computability: There exists an efficient algorithm to compute e(u,v) for ∀u, v ∈ G.

2.2 Decisional Bilinear Diffie-Hellman (DBDH) Assumption

The decisional BDH problem in a bilinear group (p, G, GT, e) is as follows: Given a tuple (g, g^a, g^b, g^c, Z) for a, b, c ∈ R Zp as input, output 1 if Z = e(g,g)^abc and 0 otherwise. For a probabilistic algorithm A, we define its advantage in solving the DBDH problem as:

AdvDBDH = PPr[A(g, g^a, g^b, g^c, e(g,g)^abc) = 1] - PPr[A(g, g^a, g^b, g^c, Z) = 1]

where g is a random generator in G and Z ← GT.
2.3 Target Collision Resistant hash function

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

Informally, we define $A$’s advantage in attacking the target collision resistance of hash function $H$ as $Adv^{TCR}_{H,A} = Pr[A \text{ succeeds in finding collisions}]$. For any PPT adversary $A$ and any hash function $H \in \mathcal{H}$, if the advantage function $Adv^{TCR}_{H,A}$ 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 $M$, consists of a tuple of four algorithms (Setup, Extract, Encrypt, Decrypt):

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

The correctness property requires that, for all $ID \in S$, if $(\text{params}, \text{msk}) \leftarrow \text{Setup}(1^\lambda), sk_{ID} \leftarrow \text{Extract}(\text{msk}, ID)$ and $CT \leftarrow \text{Encrypt}(\text{params}, S, M)$, then $\text{Decrypt}(\text{params}, sk_{ID}, CT) = M$ 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 $A$ be a PPT adversary, $A$ interacts with challenger $C$ in the following games.

The IND-CCA Game:

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

Definition 2. We define adversary $A$’s advantage in IND-CCA Game as $Adv_{A,\text{IBBE}}^{\text{IND-CCA}} = Pr[\beta' = \beta] - 1/2$. We say that an IBBE scheme is IND-CCA secure, if for any PPT adversary $A$, the advantage $Adv_{A,\text{IBBE}}^{\text{IND-CCA}}$ is negligible in the 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**: $A$ submits a message $M^*$ and two distinct sets $S_0, S_1$ to $C$. It is required that $|S_0| = |S_1|$ and $A$ has not issued Extraction Query on $ID \in S_0 \triangle S_1$, where $S_0 \triangle S_1$ denotes $S_0 \cup S_1 - S_0 \cap S_1$. Challenger $C$ flips a random coin $\beta \in \{0, 1\}$ and returns the challenge ciphertext $CT^* \leftarrow \text{Encrypt}(\text{params}, S_{\beta}, M^*)$ to $A$.
- **Phase 2**: $A$ continues to adaptively issue queries as in Phase 1 with the restrictions as follows: (i) $A$ cannot issue Extraction Query on $ID$, where $ID \in S_0 \triangle S_1$; (ii) $A$ cannot issue Decryption Query on $(ID, C^*)$, where $ID \in S_0 \triangle S_1$.
- **Guess**: $A$ outputs a guess $\beta' \in \{0, 1\}$.

Definition 3. We define adversary $A$’s advantage in the above ANO-CCA Game as $Adv_{A,\text{IBBE}}^{\text{ANO-CCA}} = Pr[\beta' = \beta] - 1/2$. We say that an IBBE scheme is ANO-CCA secure, if for any PPT adversary $A$, the advantage $Adv_{A,\text{IBBE}}^{\text{ANO-CCA}}$ 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 \( A \) outputs a message \( M \), a receiver set \( S' = \{ID_1, ID_2, \cdots, ID_t\} \), where \( |S'| = t \). \( C \) outputs the challenge ciphertext \( CT^* \leftarrow \text{Encrypt} \left( \text{params}, S', M \right) \).

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

We define adversary \( A \)’s advantage as the probability of that \( A \) wins.

**Definition 4.** We say that an IBBE scheme is WROB-CCA secure, if for all PPT adversaries \( A \), 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 \( \ell \) bits of \( x \), \( [x]_\ell^r \) denote the last \( \ell \) bits of \( x \), and \( x|y \) denote that \( x \) connects with \( y \).

#### 4.1 Construction

- **Setup\((1^\lambda)\)**: On input a security parameter \( \lambda \), it first generates a bilinear group \((p, \mathbb{G}, \mathbb{G}_T, e)\), where \( p \) is a \( \lambda \)-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 \( g, u, v, w \in \mathbb{G} \), chooses \( \alpha \in \mathbb{Z}_p \) as a master secret key, computes \( g_1 = g^\alpha \), and chooses cryptographic hash functions \( H_1 : \{0,1\}^* \rightarrow \mathbb{G}, H_2 : \mathbb{G}_T \rightarrow \mathbb{G}_p, H_3 : Z_p \times \mathbb{G}_T \rightarrow \{0,1\}^t \) and a target collision-resistant hash function \( H_4 : \mathbb{G} \times \{0,1\}^t \rightarrow \mathbb{Z}_p \). The public parameters are \( \text{params} = (p, \mathbb{G}, \mathbb{G}_T, e, g, g_1, u, v, w, H_1, H_2, H_3, H_4) \) and the master secret key is \( \text{msk} = \alpha \).

- **Extract\((\text{msk}, ID)\)**: On input master secret key \( \text{msk} \) 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\((\text{params}, S, m)\)**: On input public parameters \( \text{params} \), receiver set \( S = \{ID_1, ID_2, \cdots, ID_t\} \) and message \( m \in \{0,1\}^{k_1} \), it picks \( r, k, \tau \in \mathbb{Z}_p \) and computes \( C_0 = g^r \). For each \( ID_i \in S \), it sets \( V_{ID_i} = H_2(e(Q_{ID_i}, g_1)^\tau) \). \( f(x) = \prod_{i=1}^{t} (x - V_{ID_i}) + k \sum_{i=1}^{t} a_i x^i \pmod{p} \), where \( a_i \) is the coefficient correspond to \( x^i \). \( C_1 = [H_2(k||C_0)]_{\tau^t_i} \left((H_2(k||C_0)^{t_1} || m) \right) \), \( h = H_3(C_0, C_1, a_0, \cdots, a_{t-1}) \). \( C_2 = (u^v w^v)^r \). The ciphertext is \( CT = (\tau, C_0, C_1, C_2, a_0, a_1, \cdots, a_{t-1}) \).

- **Decrypt\((\text{params}, sk_{ID}, CT)\)**: On input public parameters \( \text{params} \), private key \( sk_{ID} \) and ciphertext \( CT = (\tau, C_0, C_1, C_2, a_0, a_1, \cdots, a_{t-1}) \), it computes \( h = H_3(C_0, C_1, a_0, \cdots, a_{t-1}) \), and then checks whether \( e(C_0, u^v w^v) = e(g, C_2) \) holds. If not, it outputs \( \bot \). Otherwise, it computes \( V_{ID} = H_2(e(sk_{ID}, C_0)) \) and \( k = \sum_{i=0}^{t-1} a_i (V_{ID})^i + V_{ID} \pmod{p} \). If \( |C_1|_{\tau^t_i} \neq |H_2(k||C_0)|_{\tau^t_i} \), it outputs \( \bot \). Otherwise, it outputs \( m = |H_3(k||C_0)|^{t_1} \mp |C_1|^{t_1} \).

### 4.2 Security Analysis

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

First, we shall prove the IBBE construction is WROB-CCA secure. 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 secure.

**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 \( A \) against the above IBBE construction, it is easy to construct a PPT algorithm \( B \) that makes use of \( A \) to break the randomness of \( H_1, H_2, H_3 \) oracle’s outputs. \( B \) runs \( A \) as follows.

- **Setup.** \( B \) chooses bilinear groups \((p, \mathbb{G}, \mathbb{G}_T, e)\) of prime order \( p \), picks generators \( g, u, v, w \in \mathbb{G} \), chooses \( \alpha \in \mathbb{Z}_p \) as the master secret key, and sets \( g_1 = g^\alpha \). \( A \) is given the public parameters \( \text{params} = (p, \mathbb{G}, \mathbb{G}_T, e, g, g_1, u, v, w, H_1, H_2, H_3) \), where \( H_1, H_2, H_3 \) are random oracles controlled by \( B \) and \( H_1 \) is collision-resistant hash function. \( B \) keeps the master private key \( \alpha \) itself.

- **Query Phase.** \( A \) adaptively issues queries as follows:
  - **Hash1 Query.** On input \( ID, B \) does the following:
    - If there exists a record \( (ID, Q, q) \) in the \( H_1 \)-list, which the list is initialized empty, it returns \( Q \); else it selects \( q \in \mathbb{Z}_p \), computes \( Q = q^r \in \mathbb{G} \), and adds \( (ID, Q, q) \) into the \( H_1 \)-list, it returns \( Q \) to \( A \).
  - **Hash2 Query.** On input \( X, B \) does the following:
    - If there exists a record \( (X, v) \) in the \( H_2 \)-list, which the list is initialized empty, it returns \( v \) to \( A \); else, it selects \( v \in \mathbb{Z}_p \), adds \( (X, v) \) into the \( H_2 \)-list, returns \( v \) to \( A \).
  - **Hash3 Query.** On input \( (k, C_0), B \) does the following:
    - If there exists a record \( (k, C_0, K) \) in the \( H_3 \)-list, which the list is initialized empty, it returns \( K \); else, it selects \( K \in \{0,1\}^t \), and adds \( (k, C_0, K) \) into the \( H_3 \)-list, it returns \( K \) to \( A \).

- **Extraction Query.** On input \( ID, B \) first queries \( \text{Hash1} \) on \( ID \), suppose that \( (ID, Q, q) \) be the corresponding tuple in the \( H_1 \)-list. Then \( B \) computes \( sk_{ID} = Q^\alpha = g^\alpha q^{-r} \) and sends \( sk_{ID} \) to \( A \).

- **Decryption Query.** \( A \) inputs \((ID, CT), B \) can use master private key \( \alpha \) to answer any Decryption Query to \( A \).
• Output. A outputs message $M \in \{0, 1\}^{t_1}$ and receiver set $S^* = (ID_1^*, ID_2^*, \ldots, ID_2)$, where $|S^*| = t$. B runs $CT \leftarrow \text{Encrypt}(\text{params}, S^*, M)$ as follows: Pick $r, k^*, \tau^* \in \mathbb{Z}_p$, for all $ID_i^* \in S^*$, compute $C_{0i}^* = g^{r_i}$, $V_{ID_i^*} = H_2(e(g_1, H_1(ID_i^*)^{e_1})), f(x) = \prod_{i=1}^{n}(x - V_{ID_i^*}) + k^* = \sum_{j=0}^{n-1}a_j x^j + x^t \pmod{p}$, output $\{a_0^*, \ldots, a_{t-1}^*\}$, which $a_j^*$ is the coefficient correspond to $x^j$. $C_{t-1}^* = [H_2(k^* \| C_{0i}^*)]_{e_{t-1}} = (H_2(k^* \| C_{0i}^*))^{\tau_{t-1}} \cdot M$, $h^* = H_3(C_{0i}^*, C_{t-1}^*, a_0^*, \ldots, a_{t-1}^*)$. If $\text{Decrypt}(\text{params}, sk_{ID^*}, CT^*) \neq 1$, where $ID^* \notin S^*$ and $sk_{ID^*} \leftarrow \text{Extract}(\text{msg}, ID^*)$. It is required that $A$ has not issued Extraction Query on $ID^*$ in Query Phase. Then $A$ wins.

Analysis: If $A$ wins the WROB-CCA game, then there exists some $M' \neq \perp$ such that $\text{Decrypt}(\text{params}, sk_{ID^*}, CT^*) = M'$ and $ID^* \notin S^*$, it implies that there exists a $k^*$, such that $C_{t-1}^* = [H_2(k^* \| C_{0i}^*)]_{e_{t-1}} = (H_2(k^* \| C_{0i}^*))^{\tau_{t-1}} \cdot M$, where $k^* = f(V_{ID_1^*}, V_{ID_2^*} = H_2(e(r, C_{0i}^*) \cdot M))$. However, for $ID_1^* \in S$, $C_{t-1}^* = [H_2(k^* \| C_{0i}^*)]_{e_{t-1}} = (H_2(k^* \| C_{0i}^*))^{\tau_{t-1}} \cdot M$, where $k^* = f(V_{ID_1^*}, V_{ID_2^*} = H_2(e(r, C_{0i}^*) \cdot M))$. However, the advantage of $A$ winning the game is negligible.

1. If $k' = k^*$, namely $f(V_{ID_1^*}) = f(V_{ID_2^*})$, since $f(x) = \prod_{i=1}^{n}(x - V_{ID_i^*}) + k^*$ for $ID_i^* \in S$, then we get $\prod_{i=1}^{n}(V_{ID_1^*} - V_{ID_2^*}) = 0$. It means that there exists some $V_{ID_2^*}^*$, such that $V_{ID_1^*} = V_{ID_2^*}$, that is $H_2(X_{ID_1}) = H_2(X_{ID_2})$. As $H_2$ is a random oracle, so $X_{ID_1} = X_{ID_2}$. As $X_{ID_1} = e(H_1(ID_1^*), g_1)^{\tau_{t-1}}$ and $X_{ID_2} = e(H_1(ID_2^*), g_1)^{\tau_{t-1}}$, it implies $H_1(ID_1^*) = H_1(ID_2^*)$. As $H_1$ is a random oracle, then $ID_1^* = ID_2^*$, but it is contradictory with $ID_1^* \notin S^*$. So we know $k' = k^*$ is not correct.

2. If $k' \neq k^*$, as $H_3$ is a random oracle, then $[H_2(k^* \| C_{0i}^*])_{e_{t-1}} \neq [H_2(k^* \| C_{0i}^*)]_{e_{t-1}}$. However, $[H_2(k^* \| C_{0i}^*)]_{e_{t-1}} = [C_{t-1}^*]_{e_{t-1}}$, then $[H_2(k^* \| C_{0i}^*)]_{e_{t-1}} \neq [C_{t-1}^*]_{e_{t-1}}$. So $A$ can only get $\perp$, it is contradictory with $M' \neq \perp$. So the advantage of $A$ winning the game is negligible.

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

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 $A$ against the above IBBE scheme. It is easy to construct a PPT algorithm $B$ that makes use of $A$ to solve the DBDH problem or break the IBBE construction’s WROB-CCA security. Algorithm $B$ is given a random tuple $(g^{r_0}, g_a, g_b, Z)$, that is either sampled from $P_{DBDH}$ (where $Z = e(g, g)^{\tau_{2n}}$) or from $R_{DBDH}$ (where $Z$ is uniform and independent in $G_2$). $B$ runs $A$ to execute the following steps.

• Setup. $B$ sets $g_1 = g^u, u = g^{x_1}g^{x_2}, v = g^{y_1}g^{y_2}, w = g^{z_1}g^{z_2}$, where $x_1, x_2, y_1, y_2, z_1, z_2 \in \mathbb{Z}_p$. $A$ is given the public parameters $\text{params} = (p, G, G_T, g, g_1, u, v, w, H_1, H_2, H_3, H_4)$, where $H_1, H_2, H_3$ are random oracles controlled by $B$ and $H_4$ is target collision-resistant hash function. The master secret key $a$ is chosen at random in $\mathbb{Z}_p$.

• Phase 1. $A$ adaptively issues queries as follows:

$\text{Hash}_2$ Query: On input $ID, B$ does the following:
If there exists a record $(ID, Q, q, \tau)$ in $H_1$-list, which the list is initially empty, it returns $Q$; else it generates $\tau \in \{0, 1\}$ and selects $q \in \mathbb{Z}_p$. If $\tau = 0$, it computes $Q = g^{\tau}$; else it computes $Q = g^{q\tau}$ and adds $(ID, Q, q, \tau)$ into $H_1$-list. It returns $Q$ to $A$.

$\text{Hash}_2$ Query: It is the same as the above WROB-CCA game.

$\text{Hash}_3$ Query: It is the same as the above WROB-CCA game.

$\text{Extraction}$ Query: On input $1D, B$ first issues $\text{Hash}_1$ Query on $1D$ to obtain $(ID, Q, q, \tau)$, if $\tau = 0$, it computes $sk_{ID} = g^\tau$, and then uses this private key to respond the $\text{Decryption}$ Query; else it does as follows: compute $h = H_3(C_0, C_1, a_0, a_1, a_2, \ldots, a_{t-1})$ and check whether $e(C_0, u_{w}v_{w}) = e(g, C_2)$ holds. If not, output $\perp$, which indicates an invalid ciphertext; else check whether $x_1h + y_1\tau + z_1 = 0$ holds. If so, abort and randomly output a bit; else continue to execute the rest steps: As $C_2 = (u_{w}v_{w})^{e_1} = (g^{b_1 \cdot x_1 + y_1 \cdot \tau + z_1})^{e_2} = C_0^{e_1} = C_0^{e_1}$ and computes $C_0^\tau = (g^{b_1 \cdot x_1 + y_1 \cdot \tau + z_1})^{\tau_{2n}}$. So $X_{ID} = e(Q_{ID}, g_1)^\tau = e(g^{x_2}g^{2\tau_{2n}})^\tau = e(C_0^\tau, g_1)^\tau$. $B$ issues $\text{Hash}_2$ Query on $X_{ID}$ to get $V_{ID}$, where $\prod_{i=1}^{n}(x - V_{ID_i^*}) + k^* = \sum_{i=1}^{n}a_i(V_{ID_i^*}) + (V_{ID})^t$, and then issues $\text{Hash}_3$ Query on $(k, C_0)$ to get $K$, where $K = H_3(k')$. If $[C_1]_{e_{t-1}} \neq [K]_{e_{t-1}}$, it outputs $\perp$, which indicates an invalid ciphertext; else outputs $m = [K]_{e_{t-1}}$ and $[C_1]_{e_{t-1}}$. Recall that, the public parameters $u = g^{b_1}g^{2\tau_{2n}}$, $v = g^{y_1}g^{2\tau_{2n}}$, $w = g^{z_1}g^{2\tau_{2n}}$ for random $x_1, x_2, y_1, y_2, z_1, z_2 \in \mathbb{Z}_p$, $x_1, y_1, z_1$ is blinded by $x_2$, $(y_2, z_2, \text{resp})$, and hence no information about $x_1, y_1$ and $z_1$ is leaked to $A$, and the equality $x_1h + y_1\tau + z_1 = 0 \pmod{p}$ information-theoretically holds with probability at most $\frac{1}{p}$.

• Challenge. $A$ outputs two distinct equal-length messages $M_0, M_1$ and a receiver set $S^*$. It required that $A$ has not issued Extraction Query on any $1D$, where $ID \in S^*$ in Phase 1. For all $ID, S^*$, $B$ first issues $\text{Hash}_1$ Query on $1D$, to obtain $(ID, Q_{ID}, q, \tau)$. If there exists some $1D \in S^*$ and $\tau = 0$, $B$ aborts; else for each $ID_i \in S^*$, $B$ lets $X_{ID_i^*} = Z^{\tau_{2n}}$ and issues $\text{Hash}_2$ Query on $X_{ID_i^*}$ to obtain $V_{ID_i^*}$ from $H_2$-list, where
$V_{1D_i} = H_2(X_{1D_i})$. Next, $B$ randomly chooses $k^* \in \mathbb{Z}_p$, computes $f(x) = \prod_{i=0}^{l-1}(x - V_{1D_i}) + k^* = \sum_{i=0}^{l-1} a_i x^i + x^l (\text{mod} \ p)$ and outputs $(a_0^*, a_1^*, \ldots, a_{l-1}^*)$. Let $C_0^* = g^{a_0^*}$. $B$ issues Hash Query on $(k^*, C_0^*)$ to obtain $k^*$, where $K^* = H_2(k^*[C_0^*])$. $B$ randomly chooses $\beta \in \{0, 1\}$, computes $C_i^* = [K^*]_{\cdot - \ell_i} \otimes ([K^*]_{\cdot}^f \oplus M_i)$. $h^* = H_2(C_0^*, C_1^*, a^*_0, \ldots, a^*_{l-1})$, defines $\tau^* = -\frac{E \cdot k^* + E_1}{g^2}$, $\in \mathbb{Z}_p$ and compute $C_2^* = (g^{a_2})^{2h^* + 2\tau^* + 12}_1$. Last, $B$ outputs the challenge ciphertext: $C_{\text{Challenge}}^* = (\tau^*, C_0^*, C_1^*, C_2^*, a_0^*, a_1^*, \ldots, a_{l-1}^*)$.

**Phase 2.** $A$ continues to adaptively issue queries as follows:

- **Extraction Query.** $A$ inputs $ID$, where $ID \notin S^*$, $B$ handles them as in Phase 1.

- **Decryption Query.** $A$ inputs $(ID, CT)$, where $CT = (\tau, C_0, C_1, C_2, a_0, a_1, \ldots, a_{l-1})$.
  
  - If $CT \neq CT^*$, $B$ checks if $H_4(C_0, C_1, a_0, \ldots, a_{l-1}) = H_4(C_0^*, C_1^*, a_0^*, \ldots, a_{l-1}^*)$. If so, $B$ aborts and randomly outputs a bit; else responds as in Phase 1. (Note that $A$ cannot 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 $ID \in S^*$, $B$ outputs $\perp$.

- **Decryption Query.** $A$ inputs $(ID, CT)$, where $CT = (\tau, C_0, C_1, C_2, a_0, a_1, \ldots, a_{l-1})$. $B$ outputs $\perp$ with non-negligible advantage. As the IBBE scheme is WROB-CCA secure, $CT^* \leftarrow \text{Encrypt}(\text{params}, S^*, M_\beta)$ and $\text{Decrypt}(\text{params}, sk_{ID}, CT^*) \neq \perp$ is negligible for $ID \notin S^*$.

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

**Analysis:** When $Z = e(g,g)^{abc}$, assume $r^* = c$, challenge ciphertext issued by $A$ comes from a distribution identical to that in the actual construction; when $Z$ is uniform and independent in $G_T$, the ciphertext $C_{\text{Challenge}}^* = [K^*]_{\cdot - \ell_i}[([K^*]_{\cdot}^f \oplus M_i)]$, where $K^* = H_2(k^*[C_0^*])$ is uniform and random, so $M_\beta$ is independent of the adversary $A$’s view.

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

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

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

- **Phase 2.** $A$ outputs a message $M \in \{0,1\}^f$ and two distinct receiver sets $S_R^1, S_R^2$, where there is at least one different user in the two sets. There is no loss generality, assuming that $S_R^1 = \{ID_R^1, ID_R^2, \ldots, ID_R\}$ and $S_R^2 = \{ID_R^1, ID_R^2, \ldots, ID_R\}$. It required that $A$ has not issued Extraction Query on $ID$ such that $ID \in \{ID_R^1, ID_R^2\}$ in Phase 1. Then, $B$ responds as follows: Let $C_0^* = g^{a_0}$, choose a random bit $\beta \in \{0, 1\}$, where $S_R^1 = \{ID_R^1, ID_R^2, \ldots, ID_R\}$. Issue Hash Query on $ID_R^2$ to obtain $(ID_R^2, Q_3, q_3, \varpi_3)$, if $\varpi_3 = 0$, output $\perp$ and abort; else $Q_{ID_R^2} = g^q$ and $X_{1D_R^2} = Z_{1D_R^2}$, and then issue Hash Query on $X_{1D_R^2}$ to get $V_{1D_R^2}$, where $V_{1D_R^2} = H_2(X_{1D_R^2})$. For the other identities $ID_i \in S_R^2 \setminus ID_R^2$, first issue Hash 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 $Q_{ID} = g^q$ and $X_{ID} = e(g^q, g^q)$. Then, issues $A$ with non-negligible advantage. As the IBBE scheme is WROB-CCA secure, $CT^* \leftarrow \text{Encrypt}(\text{params}, S^*, M_\beta)$ and $\text{Decrypt}(\text{params}, sk_{ID}, CT^*) \neq \perp$ is negligible for $ID \notin S^*$.

- **Guess.** $A$ outputs a bit $b'$. If $b' = b$ then $B$ outputs 1 meaning $Z = e(g,g)^{abc}$; otherwise, it outputs 0 meaning $Z \neq e(g,g)^{abc}$.

**Analysis:** When $Z = e(g,g)^{abc}$, assume $r^* = c$, challenge ciphertext issued by $A$ comes from a distribution identical to that in the actual construction; when $Z$ is uniform and independent in $G_T$, the ciphertext $C_{\text{Challenge}}^* = [K^*]_{\cdot - \ell_i}([([K^*]_{\cdot}^f \oplus M_i)]$, where $K^* = H_2(k^*[C_0^*])$ is uniform and random, so $M_\beta$ is independent of the adversary $A$’s view.
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 library [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 curve 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.
REFERENCES


