Fully Anonymous Identity-based Broadcast Encryption without Random Oracles

Yanli Ren[1], Zhihua Niu[2], and Xinpeng Zhang[1]
(Corresponding author: Yanli Ren)

School of Communication and Information Engineering, Shanghai University[1]
99 Shangda Road, BaoShan District, Shanghai 200444, China
School of Computer Engineering and Science, Shanghai University[2]
99 Shangda Road, BaoShan District, Shanghai 200444, China
(Email: ryl1982@shu.edu.cn)

(Received Aug. 1, 2013; revised and accepted Nov. 4, 2013)

Abstract

In a broadcast encryption (BE) scheme, a broadcaster can encrypt a message for a set S of users who are listening to a broadcast channel. Most identity-based broadcast encryption (IBBE) schemes are not anonymous, which means the attacker can obtain the identities of all receivers from the ciphertext. Currently, anonymous IBBE schemes are only provably secure in the random oracle model. In this paper, we propose a fully anonymous IBBE scheme based on asymmetric bilinear groups, which is adaptive-ID secure without random oracles. Any attacker cannot get the identities of the receivers from the ciphertext, and each receiver is anonymous for any other receiver, and only the broadcaster knows the identities of all receivers. The scheme can simultaneously realize semantic security and recipient anonymity.

Keywords: anonymous, broadcast encryption, identity-based, without random oracles

1 Introduction

The concept of broadcast encryption (BE) was proposed by Fiat and Naor [9] in 1993, which means a broadcaster can encrypt a message for a set S of users who are listening to a broadcast channel. Any user in S can use his private key to decrypt the ciphertext and the broadcaster can encrypt to any subset S of his choice. A BE system is said to be collusion resistant even if all users outside of S collude they can obtain no information about the contents of the plaintext [1]. Broadcast encryption has several applications including access control in encrypted file systems, satellite TV subscription services, and DVD content protection [14, 18].

To realize broadcast encryption in the identity-based setting [16], Sakai et al. proposed an identity-based broadcast encryption (IBBE) scheme with constant size ciphertext and private key [15]. The scheme is provably secure in the random oracle model. Delerablee proposed another IBBE scheme with constant size ciphertexts and private keys [5]. Their construction is a key encapsulation mechanism (KEM), thus long messages can be encrypted under a short symmetric key. In this scheme, the public key is of size linear in the maximal value of the set of receivers. The scheme only achieves selective-ID security in the random oracle model. In 2009, Gentry et al. proposed IBBE schemes that is adaptive-ID secure without random oracles [10, 11].

Most IBBE schemes are not anonymous (also called privacy-preserving), which means anyone can obtain the identities of the receivers from a broadcast ciphertext even if he cannot decrypt the ciphertext. Nevertheless, more and more users gradually pay attention to their privacy such that the issue of privacy protection is urgently desired to be addressed in cryptographic protocols, including IBBE schemes. Some examples: students would like to keep their identities private in the email that a teacher sent to all of the students who failed a class; In satellite TV subscription services, a customer usually expects that any other customer does not know his identity when ordering sensitive TV programs.

In 2010, Fan et al. presented an anonymous multi-receiver identity-based encryption scheme where any adversary cannot obtain the identities of the message receivers and every receiver is anonymous for any other receiver [7]. The scheme is only selective-ID secure in the random oracle model. Hur et al. [12] proposed a privacy-preserving IBBE scheme where the ciphertext size is linear in the number of all receivers. It is difficult for the receiver to find his own ciphertext from the whole ciphertext, since the scheme is anonymous and the ciphertext hides all receivers' identities. The scheme also achieves selective-ID security in the random oracle model. Recently, Libert et al. present fully anonymous BE schemes without random oracles where any outside or inside adversary cannot obtain the information of the receivers and only the broadcaster knows the information of all receivers, and the ciphertext is linear in the size of the target set [13]. However, the anonymous BE schemes in the identity-based setting were not discussed in this paper. Fazio et al. also propose anonymous BE schemes with sublinear ciphertext, but the schemes only provide outside-anonymity, which means illegal users cannot obtain the information of receivers from the ciphertext and one of legal receivers can get information of other receivers [8]. Therefore, the scheme is not fully anonymous though it reduces the length of the ciphertext. Currently, there is no fully anonymous IBBE scheme which is adaptive-ID secure without random oracles.

We discuss the problem of privacy-preserving in a broadcast encryption system, and propose a fully anonymous IBBE scheme based on decisional bilinear Diffie-Hellman (DBDH) assumption. Any attacker cannot get the identities of the receivers from the ciphertext, and each receiver is anonymous for any other receiver, and only the broadcaster knows the identities of all receivers. The proposed scheme uses asymmetric bilinear groups, and achieves adaptive-ID security without random oracles.

2 Definitions

Below, we review the definition of an asymmetric bilinear map and discuss the complexity assumption on which our system is based. We also review the syntax and security model for an anonymous IBBE system.

2.1 Asymmetric Bilinear Map

Let p be a large prime number, $G, \hat{G}$ be additive groups of order p, and G_T be multiplicative group of order p, and $P, \hat{P}$ be generators of G and $\hat{G}$ respectively. $e : G \times \hat{G} \rightarrow G_T$ is an asymmetric bilinear map, which has the following properties [6]:

1) Bilinearity: $\forall U \in G, \hat{V} \in \hat{G}$ and $a, b \in Z_p$, $e(aU, b\hat{V}) = e(U, \hat{V})^{ab}$.

2) Non-degeneracy: $e(P, \hat{P}) \neq 1$.

3) Computability: There exists an efficient algorithm to compute $e(U, \hat{V})$, $\forall U \in G, \hat{V} \in \hat{G}$.

2.2 Complexity Assumption

Our scheme is based on asymmetric decisional bilinear Diffie-Hellman (DBDH) assumption [6], which is defined as follows.

Definition 1 (Asymmetric DBDH assumption). *Let $a, b, c \in Z_p^*$ be chosen at random and $P, \hat{P}$ be generators of G and $\hat{G}$ respectively. The assumption is that no probability polynomial-time algorithm can distinguish the tuple $[P, bP, cP, \hat{P}, a\hat{P}, b\hat{P}, e(P, \hat{P})^{abc}]$ from $[P, bP, cP, \hat{P}, a\hat{P}, b\hat{P}, Z]$ with non-negligible advantage where Z is a random element in G_T.*

We say that the decision (t, ε)-DBDH assumption holds in $G, \hat{G}, G_T$ if no t-time algorithm has advantage at least ε in solving the decision DBDH problem in $G, \hat{G}, G_T$.

2.3 Syntax

An anonymous IBBE scheme is a tuple of algorithms described as follows:

Setup(λ). Take as input the security parameter λ, outputs a master secret key MSK and a public key PK. The PKG is given MSK, and PK is made public.

Extract(MSK, ID_i). Take as input the master secret key MSK and a user identity ID_i, outputs a private key d_i, which is sent to the user associated with ID_i securely.

Encrypt(PK, M, K, S). Take as input the public key PK, a message M, a symmetric key K and a set S, and output a pair (S, Hdr, C_M), where Hdr is called the header and C_M be the encryption of M under the symmetric key K. The pair (S, Hdr) is often called the full header and C_M the broadcast body.

Decrypt(ID_i, d_i, Hdr, PK). Take as input an identity ID_i and the corresponding private key d_i, a header Hdr, and the public key PK. If $ID_i \in S$, output the message key $K \in G_T$. The key K can be used to decrypt the broadcast body C_M and obtain the message M.

2.4 Security Model

In this section, we define adaptive-ID security against an chosen plaintext attack for an anonymous IBBE scheme.

Definition 2 (IND-ID-CPA)). *Semantic security for the proposed IBBE scheme can be defined by the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$.*

Setup. *The challenger runs Setup(λ) algorithm to obtain a public key PK and sends it to $\mathcal{A}$.*

Phase 1. *The adversary $\mathcal{A}$ adaptively issues queries. Extract query $\langle ID_i \rangle$: $\mathcal{A}$ sends ID_i to $\mathcal{B}$. The challenger runs Extract algorithm on ID_i and returns $\mathcal{A}$ a decryption key d_i.*

Challenge. *$\mathcal{A}$ sends (S, K_0, K_1) to $\mathcal{B}$, where S is a set of t users and K_0, K_1 are two keys of same length. The challenger randomly chooses $\mu \in \{0, 1\}$ and runs algorithm Encrypt to obtain (Hdr^*, S). It then gives Hdr^* to adversary $\mathcal{A}$.*

Phase 2. *$\mathcal{A}$ adaptively issues extract query (ID_i), where $ID_i \notin S$.*

Guess. *Finally, the adversary outputs a guess $\mu' \in \{0, 1\}$ and wins the game if $\mu' = \mu$.*

We call the adversary $\mathcal{A}$ in the above game an IND-ID-CPA adversary. The advantage of $\mathcal{A}$ is defined as $|Pr[\mu' = \mu] - \frac{1}{2}|$.

An anonymous IBBE system is (t, ε, q) IND-ID-CPA secure if all t-time IND-ID-CPA adversaries making at most q extract queries have advantage at most ε in winning the above game.

Definition 3 (ANON-ID-CPA). *Receiver anonymity for the proposed IBBE scheme can be defined by the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$.*

Setup. *The challenger runs $Setup(\lambda)$ algorithm to obtain a public key PK and sends it to $\mathcal{A}$.*

Phase 1. *The adversary $\mathcal{A}$ adaptively issues queries. Extract query $\langle ID_i \rangle$: $\mathcal{A}$ sends ID_i to $\mathcal{B}$. The challenger runs Extract algorithm on ID_i and returns $\mathcal{A}$ a decryption key d_i.*

Challenge. *$\mathcal{A}$ sends (S_0, S_1, K) to B, where S_0, S_1 are two sets of t users, and the identities of $(S_0 \cup S_1)$ excluding $(S_0 \cap S_1)$ have not been executed the extract query in Phase 1.*

The challenger randomly chooses $\nu \in \{0, 1\}$ and runs algorithm Encrypt to obtain (Hdr^*, S_ν, K). It then gives Hdr^* to adversary $\mathcal{A}$.

Phase 2. *$\mathcal{A}$ adaptively issues extract query $\langle ID_i \rangle$, where ID_i does not belong to the set $((S_0 \cup S_1) - (S_0 \cap S_1))$.*

Guess. *Finally, the adversary outputs a guess $\nu' \in \{0, 1\}$ and wins the game if $\nu' = \nu$.*

We call the adversary $\mathcal{A}$ in the above game an ANON-ID-CPA adversary. The advantage of $\mathcal{A}$ is defined as $|Pr[\nu' = \nu] - \frac{1}{2}|$.

An anonymous IBBE system is (t, ε, q) ANON-ID-CPA secure if all t-time ANON-ID-CPA adversaries making at most q extract queries have advantage at most ε in winning the above game.

3 The Proposed Anonymous IBBE Scheme

We present a fully anonymous IBBE scheme which is adaptive-ID secure without random oracles based on Waters' IBE scheme [17]. A detailed description of the scheme follows.

3.1 Setup

Given security parameter λ, three groups $G, \hat{G}, G_T$ of order p are constructed as described in Section 2.1. $e : G \times \hat{G} \to G_T$ is an asymmetric bilinear map and $P, \hat{P}$ are generators of $G, \hat{G}$ respectively. Assume an identity is a bit string of length n, and H is a collision-resistant hash function from $\{0, 1\}^n$ to Z_p^*. The PKG randomly chooses $\alpha, \beta, \gamma, \gamma_i \in Z_p^*$, and computes

$$\begin{aligned} A &= e(P, \hat{P})^{\alpha\beta}, \\ \hat{B} &= \beta\hat{P}, \\ u' &= \gamma P, \\ \hat{u}' &= \gamma\hat{P}, \\ u_i &= \gamma_i P, \\ \hat{u}_i &= \gamma_i \hat{P}, \quad i \in \{1, 2, \ldots, n\}. \end{aligned}$$

Finally, the public parameters $PK = (P, \hat{P}, A, u', u_i, i \in \{1, 2, \ldots, n\})$ and $(\alpha\hat{B}, \hat{u}', \hat{u}_i, i \in \{1, 2, \ldots, n\})$ are the master secret keys of PKG.

3.2 Extraction

To user i with $ID_i = (ID_{i,1}, ID_{i,2}, \ldots, ID_{i,n}) \in \{0, 1\}^n$, the PKG randomly chooses $r \in Z_p^*$, and computes

$$\begin{aligned} d_{i,1} &= \alpha\hat{B} + r(\hat{u}' + \sum_{ID_{i,k}=1} \hat{u_k}), \\ d_{i,2} &= r\hat{P}, \end{aligned}$$

so the private key of i is $d_i = (d_{i,1}, d_{i,2})$.

3.3 Encryption

For a set $S = (ID_1, ID_2, \ldots, ID_L)$, do as follows:

1) Compute

$$\begin{aligned} x_i &= H(ID_i), i \in \{1, 2, \ldots, L\}; \\ f_i(x) &= \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} \\ &= a_{i,1} + a_{i,2}x + \ldots + a_{i,t}x^{t-1}, \\ &\qquad j \in \{1, 2, \ldots, L\}. \end{aligned}$$

So $f_i(x_i) = 1, f_i(x_j) = 0 (i, j \in \{1, 2, \ldots, L\}, j \neq i)$.

2) Randomly choose $s \in Z_p^*, K \in G_T$, and compute

$$\begin{aligned} R_i &= \sum_{j=1}^{L} a_{j,i} s(u' + \sum_{ID_{j,k}=1} u_k), \\ V &= sP, \\ W &= K \cdot A^s. \end{aligned}$$

The ciphertext is $Hdr = (R_1, \ldots, R_L, V, W)$. Then K is used to encrypt a message.

3.4 Decryption

If $ID_i \in S$, the receiver associated with ID_i sets:

1) $x_i = H(ID_i)$,
$\delta = R_1 + \ldots + (x_i^{i-1})R_i + \ldots + (x_i^{L-1} \bmod p)R_L$.

2) $W \frac{e(\delta, d_{i,2})}{e(V, d_{i,1})} = K$.

Thus, the receiver can decrypt the ciphertext correctly without knowing the identities of other receivers and the proposed scheme achieves full anonymity from the decrypt algorithm.

Notice: The proposed scheme is not the trivial solution in which one encrypts the session key to each user individually using an anonymous IBE scheme though the ciphertext size is linear in the size of receiver set. Assume there are t receivers for one encryption. There are two cases:

Case 1. The sender encrypts a session key and sends the corresponding ciphertext to each user respectively. In this case, the sender needs to execute encryption and communication operations for t times, but it only executes one encryption and communication with users in our scheme.

Case 2. The broadcaster generates the partial ciphertext for each user respectively by one encryption and broadcasts total ciphertext to all users. In this case, each receiver cannot find its corresponding one from the total ciphertext since the scheme achieves receiver anonymity. Each receiver maybe need to decrypt all ciphertexts to get the session key where it can obtain the correct session key by only one decryption in our scheme.

In addition, the ciphertext size is linear in the receiver set in all of fully anonymous BE or IBBE schemes until now such as [7, 12, 13], and the BE scheme with sublinear ciphertext is only outside-anonymous [8].

3.5 Correctness

The correctness of the proposed scheme is as follows.

$$
\begin{aligned}
\delta &= R_1 + \ldots + (x_i^{i-1})R_i + \ldots + (x_i^{L-1} \bmod p)R_L \\
&= (a_{1,1}s(u' + \sum_{ID_{1,k}=1} u_k) + \ldots \\
&\quad + a_{L,1}s(u' + \sum_{ID_{L,k}=1} u_k)) + \ldots \\
&\quad + (x_i^{i-1}a_{1,i}s(u' + \sum_{ID_{1,k}=1} u_k) + \ldots \\
&\quad + x_i^{i-1}a_{L,i}s(u' + \sum_{ID_{L,k}=1} u_k)) + \ldots \\
&\quad + (x_i^{L-1}a_{1,L}s(u' + \sum_{ID_{1,k}=1} u_k) + \ldots \\
&\quad + x_i^{L-1}a_{L,L}s(u' + \sum_{ID_{L,k}=1} u_k)) \\
&= s(\sum_{j=1}^{L} a_{1,j}x_i^{j-1})(u' + \sum_{ID_{1,k}=1} u_k) + \ldots \\
&\quad + s(\sum_{j=1}^{L} a_{i,j}x_i^{j-1})(u' + \sum_{ID_{i,k}=1} u_k) + \ldots \\
&\quad + s(\sum_{j=1}^{L} a_{L,j}x_i^{j-1})(u' + \sum_{ID_{L,k}=1} u_k) \\
&= sf_1(x_i)(u' + \sum_{ID_{1,k}=1} u_k) + \ldots \\
&\quad + sf_i(x_i)(u' + \sum_{ID_{i,k}=1} u_k) + \ldots \\
&\quad + sf_L(x_i)(u' + \sum_{ID_{L,k}=1} u_k) \\
&= s(u' + \sum_{ID_{i,k}=1} u_k).
\end{aligned}
$$

Note that $\delta = s(u' + \sum_{ID_{i,k}=1} u_k)$ since $f_i(x_i) = 1, f_j(x_i) = 0 (j \neq i)$ as described in Section 3.3.

$$
\begin{aligned}
e(V, d_{i,1}) &= e(sP, \alpha\hat{B} + r(\hat{u}' + \sum_{ID_{i,k}=1} \hat{u}_k)) \\
&= A^s e(sP, r(\gamma + \sum_{ID_{i,k}=1} \gamma_k)\hat{P}) \\
&= A^s e(s(\gamma + \sum_{ID_{i,k}=1} \gamma_k)P, r\hat{P}) \\
&= A^s e(s(u' + \sum_{ID_{i,k}=1} u_k), d_{i,2}) \\
&= A^s e(\delta, d_{i,2}).
\end{aligned}
$$

Note: The proposed scheme is anonymous based on asymmetric bilinear groups because the tuple $(\hat{u}', \hat{u}_i, i \in \{1, 2, \ldots, n\})$ is secret and the adversary cannot verify the identity of the receiver through the equation $e(\delta, \hat{P}) = e(sP, \hat{u}' + \sum_{ID_{i,k}=1} \hat{u}_k)$.

4 Analysis of the Anonymous IBBE Scheme

In this section, we analyze semantic security and receiver anonymity of the proposed IBBE scheme and compare security and efficiency with that of the previous work.

4.1 Ciphertext Confidentiality

We prove that the proposed anonymous IBBE scheme achieves IND-ID-CPA security under the DBDH assumption without random oracles. In this game, the adversary cannot obtain any information of a plaintext from the corresponding ciphertext.

Theorem 1. *Assume that the (t', ε')-DBDH assumption holds in $G, \hat{G}, G_T$, then the proposed scheme is (t, ε, q) IND-ID-CPA secure for*

$$t' = t + O(\varepsilon^{-2}\ln(\varepsilon^{-1})\eta^{-1}\ln(\eta^{-1})), \varepsilon' = \tfrac{\varepsilon}{32q(n+1)^L},$$

where $\eta = \frac{1}{8q(n+1)^L}$.

Proof. Assume $\mathcal{A}$ is an IND-ID-CPA adversary as described in Section 2.4, then we can construct an algorithm $\mathcal{B}$ that solves the DBDH problem. At the beginning of the game, $\mathcal{B}$ is given a tuple $(P, bP, cP, \hat{P}, a\hat{P}, b\hat{P}, Z) \in G^3 \times \hat{G}^3 \times G_T$ to decide whether $T = e(P, \hat{P})^{abc}$.

Setup. $\mathcal{B}$ sets $m = 4q$, and randomly chooses an integer l between 0 and n. It then chooses random elements x', y', x_i, y_i between 0 and $m - 1$, where $i \in \{1, 2, \ldots, n\}$.

For an identity $ID_i \in Z_p^*$, B defines:

$$\begin{aligned} F(ID_i) &= (p - lm) + x' + \sum_{ID_{i,k}=1} x_k, \\ J(ID_i) &= y' + \sum_{ID_{i,k}=1} y_k, \\ Q(ID_i) &= \left\{ \begin{array}{l} 0 \ x' + \sum_{ID_{i,k}=1} x_k \equiv 0(mod\mathrm{m}) \\ 1 \text{ otherwise} \end{array} \right\} \end{aligned} \quad (1)$$

$\mathcal{B}$ sets:

$$\begin{aligned} A &= e(bP, a\hat{P}) = e(P, \hat{P})^{ab}, \\ \hat{B} &= b\hat{P}, \\ u' &= (p - lm + x')(bP) + y'P, \\ \hat{u}' &= (p - lm + x')(b\hat{P}) + y'\hat{P}, \\ u_i &= x_i(bP) + y_iP, \\ \hat{u}_i &= x_i(b\hat{P}) + y_i\hat{P}, \quad i \in \{1, 2, \ldots, n\}. \end{aligned}$$

$\mathcal{B}$ sends the public keys $PK = (P, \hat{P}, A, u', u_i, i \in \{1, 2, \ldots, n\})$ to the adversary $\mathcal{A}$.

Phase 1. The adversary $\mathcal{A}$ adaptively issues queries.

Extract query $\langle ID_i \rangle$: $\mathcal{A}$ sends ID_i to B. If $Q(ID_i) = 0$, $\mathcal{B}$ aborts and randomly chooses $\omega' \in \{0, 1\}$ to solve the DBDH problem. Otherwise, $\mathcal{B}$ randomly chooses $r \in Z_p$ and sets:

$$\begin{aligned} d_{i,1} &= -\frac{J(ID_i)}{F(ID_i)}(a\hat{P}) + r(\hat{u}' + \sum_{ID_{i,k}=1} \hat{u}_k), \\ d_{i,2} &= -\frac{1}{F(ID_i)}(a\hat{P}) + r\hat{P}. \end{aligned}$$

It is a valid private key. Let $\widetilde{r} = r - \frac{a}{F(ID_i)}$, $d_{i,2} = (r - \frac{a}{F(ID_i)})\hat{P} = \widetilde{r}\hat{P}$, and

$$\begin{aligned} d_{i,1} &= -\frac{J(ID_i)}{F(ID_i)}(a\hat{P}) + r[(p - lm + x')B \hat{+} y'\hat{P} \\ &\quad + \sum_{ID_{i,k}=1} (x_k\hat{B} + y_k\hat{P})] \\ &= -\frac{J(ID_i)}{F(ID_i)}(a\hat{P}) + r[(y' + \sum_{ID_{i,k}=1} y_k)\hat{P} \\ &\quad +(p - lm + x' + \sum_{ID_{i,k}=1} x_k)\hat{B}] \\ &= -\frac{J(ID_i)}{F(ID_i)}(a\hat{P}) + r[F(ID_i)\hat{B} + J(ID_i)\hat{P}] \\ &= a\hat{B} + (-\frac{a}{F(ID_i)})(F(ID_i)\hat{B} + J(ID_i)\hat{P}) \\ &\quad +r[F(ID_i)\hat{B} + J(ID_i)\hat{P}] \\ &= a\hat{B} + (r - \frac{a}{F(ID_i)})(F(ID_i)\hat{B} + J(ID_i)\hat{P}) \\ &= a\hat{B} + \widetilde{r}(F(ID_i)\hat{B} + J(ID_i)\hat{P}) \\ &= a\hat{B} + \widetilde{r}(\hat{u}' + \sum_{ID_{i,k}=1} \hat{u}_k). \end{aligned}$$

$\mathcal{B}$ could perform the simulation if and only if $F(ID_i) \neq 0 \pmod p$.

Challenge. $\mathcal{A}$ submits a set S of L users and two same length keys (K_0, K_1) to $\mathcal{B}$, where the identities of S have not been executed the extract query in Phase 1.

Let $S = (ID_1, ID_2, \ldots, ID_L)$. For any identity $ID_i \in S$, $\mathcal{B}$ aborts and chooses a random $\omega' \in \{0, 1\}$ as a solution for the DBDH problem if $x' + \sum_{ID_{i,k}=1} x_k \neq lm$. Otherwise, $F(ID_i) \equiv 0$ (mod p) for any identity $ID_i \in S$. $\mathcal{B}$ randomly chooses $\mu \in \{0, 1\}$, and does as follows:

1) Compute $x_i = H(ID_i), i \in \{1, 2, \ldots, L\}$.

$$\begin{aligned} f_i(x) &= \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} \\ &= a_{i,1} + a_{i,2}x + \ldots + a_{i,L}x^{L-1}, \\ &\qquad\qquad j \in \{1, 2, \ldots, L\}. \end{aligned}$$

So $f_i(x_i) = 1$, $f_i(x_j) = 0$ $(i, j \in \{1, 2, \ldots, L\}, j \neq i)$.

2) Set the ciphertext as below:

$$\begin{aligned} R_1 &= \sum_{j=1}^{L} a_{j1} \cdot J(ID_j) \cdot (cP), \ldots, \\ R_L &= \sum_{j=1}^{L} a_{jL} \cdot J(ID_j) \cdot (cP), \\ V &= cP, \\ W &= K_\mu \cdot Z, \\ Hdr^* &= (R_1, R_2, \ldots, R_L, V, W). \end{aligned}$$

Let $s^* = c$. If $Z = e(P, \hat{P})^{abc}$, $V = cP = s^*P$, and

$$\begin{aligned} R_1 &= \sum_{j=1}^{L} a_{j1} \cdot (y' + \sum_{ID_{j,k}=1} y_k) \cdot (cP) \\ &= \sum_{j=1}^{L} a_{j1} \cdot s^*[F(ID_j)(bP) \\ &\quad +(y' + \sum_{ID_{j,k}=1} y_k)P] \end{aligned}$$

$$\begin{aligned}
&= \sum_{j=1}^{L} a_{j1}\cdot s^*[(p-lm+x')(bP)+y'P \\
&\quad + \sum_{ID_{j,k}=1}(x_k(bP)+y_kP)] \\
&= \sum_{j=1}^{L} a_{j1}\cdot s^*(u'+\sum_{ID_{j,k}=1}u_k), \\
&\quad\vdots \\
R_L &= \sum_{j=1}^{L} a_{jL}\cdot s^*(u'+\sum_{ID_{j,k}=1}u_k), \\
W &= K_\mu \cdot Z \\
&= K_\mu \cdot e(P,\hat{P})^{abc} \\
&= K_\mu \cdot A^{s^*}.
\end{aligned}$$

Since $c = s^*$ is uniformly random, Hdr^* is a valid ciphertext of K_μ for the set S and an appropriately-distributed challenge to A.

Phase 2. $\mathcal{A}$ adaptively issues extract query ID_i, where $ID_i \notin S$.

Guess. $\mathcal{A}$ submits a guess $\mu' \in \{0,1\}$. If $\mu' = \mu$, B outputs 0 (indicating that $Z = e(P,\hat{P})^{abc}$); otherwise, it outputs 1.

□

Probability analysis: It is same to [17] except any identity ID_i of a set S need to satisfy the condition $F(ID_i) \equiv 0 \pmod p$. As we described above, there are L identities in S. Thus the probability of the simulation not aborting by the guess phase is at least $\eta = \frac{1}{8q}(\frac{1}{n+1})^L$, and B can solve the DBDH problem with probability $\varepsilon' > \frac{3}{4}\eta\varepsilon > \frac{\varepsilon}{32q}(\frac{1}{n+1})^L$.

Time complexity: It is same to [17].

Remark 1. In this game, the adversary can query the private key of all identities excluding those of S. Otherwise, $\mathcal{A}$ always decrypts the challenge ciphertext correctly if Hdr^* is a valid ciphertext, and the game cannot prove semantic security of the proposed scheme.

$\mathcal{A}$ output $\mu' = \mu$ with probability greater than 1/2 if Hdr^* is a valid ciphertext and $\mathcal{A}$ has the ability of distinguishing the ciphertexts of two different plaintexts. Then $\mathcal{B}$ may solve the DBDH problem using the output of $\mathcal{A}$. In fact, there is no probability polynomial-time (PPT) algorithm to solve the DBDH problem currently, so we have a contradiction. Thus, it is impossible for $\mathcal{A}$ to distinguish the ciphertexts of two different plaintexts, and the proposed IBBE scheme achieves semantic security against a CPA adversary.

4.2 Receiver Anonymity

We now prove that the proposed IBBE scheme achieves ANON-ID-CPA security under the DBDH assumption without random oracles. In this scheme, the adversary cannot obtain the identities of all receivers if it is not included the receiver set, and one of the receivers cannot get the identities of the other receivers.

Theorem 2. *Assume that the (t',ε')-DBDH assumption holds in $G, \hat{G}, G_T$, then the proposed scheme is (t,ε,q)-ANON-ID-CPA secure for*

$$t' = t + O(\varepsilon^{-2}\ln(\varepsilon^{-1})\eta^{-1}\ln(\eta^{-1})), \varepsilon' = \tfrac{\varepsilon}{32q(n+1)^{2L}},$$

where $\eta = \frac{1}{8q(n+1)^{2L}}$.

Proof. Assume $\mathcal{A}$ is an ANON-ID-CPA adversary as described in Section 2.4, then we can construct an algorithm $\mathcal{B}$ that solves the DBDH problem as follows. At first, $\mathcal{B}$ is given a tuple $(P, bP, cP, \hat{P}, a\hat{P}, b\hat{P}, Z) \in G^3 \times \hat{G}^3 \times G_T$ to decide whether $Z = e(P,\hat{P})^{abc}$.

Setup, Phase 1. As Theorem 1.

Challenge. $\mathcal{A}$ submits two sets (S_0, S_1) of L users and a key K to $\mathcal{B}$, where the identities of $(S_0 \cup S_1)$ excluding $(S_0 \cap S_1)$ have not been executed the extract query in Phase 1.

For any identity $ID_i \in S_0$ or S_1, $\mathcal{B}$ aborts and chooses a random $\omega' \in \{0,1\}$ as a solution for the DBDH problem if $x' + \sum_{ID_{i,k}=1} x_k \neq lm$. Otherwise, $F(ID_i) \equiv 0 \pmod p$ for any identity $ID_i \in S_0$ or S_1. $\mathcal{B}$ randomly chooses $\nu \in \{0,1\}$, and does as follows:

1) Set $x_i = H(ID_i), ID_i \in S_\nu, i \in \{1,2,\ldots,L\}$.

$$\begin{aligned}
f_i(x) &= \prod_{j\neq i}\frac{x-x_j}{x_i-x_j} \\
&= a_{i,1}+a_{i,2}x+\ldots+a_{i,L}x^{L-1}, \\
&\qquad\qquad j\in\{1,2,\ldots,L\}.
\end{aligned}$$

So $f_i(x_i) = 1$, $f_i(x_j) = 0$ $(i,j \in \{1,2,\ldots,L\}$, $j \neq i)$.

2) Compute the challenge ciphertext as below:

$$\begin{aligned}
R_1 &= \sum_{j=1}^{L} a_{j1}\cdot J(ID_j)\cdot(cP),\ldots, \\
R_L &= \sum_{j=1}^{L} a_{jL}\cdot J(ID_j)\cdot(cP), \\
V &= cP, \\
W &= K\cdot Z, \\
Hdr^* &= (R_1,R_2,\ldots,R_L,V,W).
\end{aligned}$$

Let $s^* = c$. If $Z = e(P,\hat{P})^{abc}$, $V = cP = s^*P$, and

$$\begin{aligned}
R_1 &= \sum_{j=1}^{L} a_{j1} \cdot (y' + \sum_{ID_{j,k}=1} y_k) \cdot (cP) \\
&= \sum_{j=1}^{L} a_{j1} \cdot s^*[F(ID_j)(bP) \\
&\qquad +(y' + \sum_{ID_{j,k}=1} y_k)P] \\
&= \sum_{j=1}^{L} a_{j1} \cdot s^*[(p - lm + x')(bP) + y'P \\
&\qquad + \sum_{ID_{j,k}=1} (x_k(bP) + y_kP)] \\
&= \sum_{j=1}^{L} a_{j1} \cdot s^*(u' + \sum_{ID_{j,k}=1} u_k), \\
&\vdots \\
R_L &= \sum_{j=1}^{L} a_{jL} \cdot s^* \cdot (u' + \sum_{ID_{j,k}=1} u_k), \\
W &= K \cdot Z \\
&= K \cdot e(P, \hat{P})^{abc} \\
&= K \cdot A^{s^*}.
\end{aligned}$$

Since $c = s^*$ is uniformly random, Hdr^* is a valid ciphertext of K for the set S_ν and an appropriately-distributed challenge to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ adaptively issues extract query ID_i, where ID_i does not belong to the set $((S_0 \cup S_1) - (S_0 \cap S_1))$.

As we noted in the phase of Challenge, $F(ID_i) \equiv 0 \pmod p$ for any identity $ID_i \in S_0$ or S_1. However, $\mathcal{B}$ could perform the extract simulation for an identity ID_i if and only if $F(ID_i) \not\equiv 0 (\bmod\ p)$ as described in Theorem 1. So, $\mathcal{B}$ aborts and chooses a random $\omega' \in \{0,1\}$ if $\mathcal{A}$ issues extract query for $ID_i \in (S_0 \cap S_1)$. Otherwise, $\mathcal{B}$ answers these queries as Phase 1.

Guess. $\mathcal{A}$ submits a guess $\nu' \in \{0,1\}$. If $\nu' = \nu$, $\mathcal{B}$ outputs 0 (indicating that $Z = e(P, \hat{P})^{abc}$); otherwise, it outputs 1.

□

Probability analysis: It is same to Theorem 1 except any identity ID_i of two sets S_0 and S_1 need to satisfy the condition $F(ID_i) \equiv 0 \pmod p$. As we described above, there are $2L$ identities in S_0 and S_1. Thus the probability of the simulation not aborting by the guess phase is at least $\eta = \frac{1}{8q}(\frac{1}{n+1})^{2L}$, and $\mathcal{B}$ can solve the DBDH problem with probability $\varepsilon' > \frac{3}{4}\eta\varepsilon > \frac{\varepsilon}{32q}(\frac{1}{n+1})^{2L}$.

Time complexity: It is same to [17].

Remark 2. In this game, $\mathcal{A}$ cannot query the private keys of identities in $((S_0 \cup S_1) - (S_0 \cap S_1))$. Otherwise, $\mathcal{A}$ always decrypts the challenge ciphertext and decide whether S_0 or S_1 is the receiver set correctly if Hdr^* is a valid ciphertext, and the game cannot prove receiver anonymity of the proposed scheme.

$\mathcal{A}$ output $\nu' = \nu$ with probability greater than 1/2 if Hdr^* is a valid ciphertext and $\mathcal{A}$ has the ability of distinguishing the ciphertexts of two receiver sets. Then $\mathcal{B}$ may solve the DBDH problem using the output of $\mathcal{A}$. In fact, there is no PPT algorithm to solve the DBDH problem currently, so we have a contradiction. Therefore, it is impossible for a PPT adversary to get the identities of the receiver sets, and the proposed IBBE scheme achieves receiver anonymity against a CPA adversary.

Chosen-ciphertext security: The results of Canetti et al. [4], further improved by [2], show how to build a CCA-secure IBE scheme from a 2-level hierarchical IBE (HIBE) scheme [3]. Similarly to Waters' IBE scheme, we can also transform the proposed scheme into a hybrid 2-level HIBE scheme, and then get an ANON-IND-ID-CCA secure IBBE scheme.

4.3 Comparison

In this section, we compare the proposed anonymous BE schemes recently in Table 1 and the known IBBE schemes in Table 2.

In Table 1 and Table 2, "sID, ID" denote "selective-ID" and "adaptive-ID" security model respectively. m, L represent the number of total users and the maximal receivers for one encryption, and n is the length of an identity in the scheme.

From Table 1, we know that the schemes in [8] only provide outside-anonymity and the anonymous BE schemes in the identity-based setting were not discussed in [8, 13].

From Table 2, we conclude that the receiver is not anonymous in the schemes of [5, 10, 11, 15]. The anonymous IBBE schemes in [7] and [12] are only selective-ID secure in the random oracle model, and our IBBE scheme is anonymous and achieves adaptive-ID security without random oracles. It is well known that the schemes proven in the random oracle model may not be secure in the real world. Thus, the proposed anonymous IBBE scheme has better security than that of [7] and [12], though the public key size is not constant and linear in the length of an identity.

5 Conclusion

We present a fully anonymous IBBE scheme in this paper. It is impossible for any attacker to get the identities of the receivers, and one of receivers is anonymous for any other receiver. The scheme achieves adaptive-ID security without random oracles based on asymmetric DBDH assumption.

There is still a gap between the sizes of ciphertexts in state-of-the-art IBBE schemes and our proposed scheme.

Table 1: Comparison among anonymous BE schemes

Scheme	Identity based	Fully anonymous	Random oracles	Security model	Public key size	Ciphertext size	Decrypt time
[8]	no	no	no	ID	$O(1)$	$O(\log L)$	$O(\log L)$
[13]	no	yes	no	ID	$O(m)$	$O(L)$	$O(L)$
Ours	yes	yes	no	ID	$O(n)$	$O(L)$	$O(L)$

Table 2: Comparison among IBBE schemes

Scheme	Anonymous	Random oracles	Security model	Public key size	Ciphertext size	Decrypt time
[5]	no	yes	sID	$O(m)$	$O(1)$	$O(L)$
[10]	no	no	ID	$O(m)$	$O(1)$	$O(1)$
[11]	no	no	ID	$O(n)$	$O(L)$	$O(n)$
[15]	no	yes	ID	$O(m)$	$O(1)$	$O(L)$
[7]	yes	yes	sID	$O(1)$	$O(L)$	$O(L)$
[12]	yes	yes	sID	$O(1)$	$O(L)$	$O(1)$
Ours	yes	no	ID	$O(n)$	$O(L)$	$O(L)$

Currently, the ciphertext size is not constant in all of fully anonymous BE or IBBE schemes, we expect to reduce the length of the ciphertext while maintaining its full anonymity properties in the future research.

Acknowledgments

This work described in this paper was supported by the Natural Science Foundation of China (61202367), Natural Science Foundation of Shanghai (12ZR1443700), and the Innovation Program of Shanghai Municipal Education Commission (14YZ020). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] D. Boneh, C. Gentry, B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys", *Proc. of 25th Annual International Cryptology Conference (Crypto'05)*, pp. 258-275, Santa Barbara, USA, 2005.

[2] D. Boneh, J. Katz, "Improved efficiency for CCA-secure cryptosystems built using identity-based encryption", *Proc. of 5th Cryptographers' Track at the RSA Conference (CT-RSA'05)*, pp. 87-103, San Francisco, USA, 2005.

[3] D. Boneh, X. Boyen, E.J. Goh, "Hierarchical identity based encryption with constant size ciphertext", *Proc. of 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05)*, pp. 440-456, Aarhus, Denmark, 2005.

[4] R. Canetti, S. Halevi, J. Katz, "Chosen-ciphertext security from identity-based encryption", *Proc. of 23th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'04)*, pp. 207-222, Interlaken, Switzerland, 2004.

[5] C. Delerablee, "Identity-based broadcast encryption with constant size ciphertexts and private keys", *Proc. of 13th Annual International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT'07)*, pp. 200-215, Kuching, Malaysia, 2007.

[6] L. Ducas, "Anonymity from asymmetry: new constructions for anonymous HIBE", *Proc. of 10th Cryptographers' Track at the RSA Conference (CT-RSA'10)*, pp. 148-164, San Francisco, USA, 2010.

[7] C. Fan, L. Hwang, P. Ho, "Anonymous multireceiver identity-based encryption", *IEEE Transactions on Computers*, vol. 59, no. 9, pp. 1239-1249, 2010.

[8] N. Fazio, I. Perera, "Outsider-anonymous broadcast encryption with sublinear ciphertexts", *Proc. of 15th Annual International Conference on Practice and Theory in Public Key Cryptography (PKC'12)*, pp. 225-242, Darmstadt, Germany, 2012.

[9] A. Fiat, M. Naor, "Broadcast encryption", *Proc. of 13th Annual International Cryptology Conference (Crypto'93)*, pp. 480-491, Santa Barbara, USA, 1993.

[10] C. Gentry, B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)", *Proc. of 28th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'09)*, pp. 171-188, Cologne, Germany, 2009.

[11] C. Gentry, S. Halevi, "Hierarchical identity based encryption with polynomially many levels", *Proc. of 6th*

Theory of Cryptography Conference (TCC'09), pp. 437-456, San Francisco, USA, 2009.

[12] J. Hur, C. Park, S. Hwang, "Privacy-preserving identity-based broadcast encryption", *Information Fusion*, vol. 13, no. 4, pp. 296-303, 2012.

[13] B. Libert, G. Paterson, A. Quaglia, "Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model", *Proc. of 15th Annual International Conference on Practice and Theory in Public Key Cryptography (PKC'12)*, pp. 206-224, Darmstadt, Germany, 2012.

[14] B. Malek, A. Miri, "Adaptively Secure Broadcast Encryption with Short Ciphertexts", *International Journal of Network Security*, vol. 14, no. 2, pp. 71-79, 2012.

[15] R. Sakai, J. Furukawa, "Identity-based broadcast encryption", http://eprint.iacr.org/2007/217.

[16] A. Shamir, "Identity-based cryptosystems and signature schemes", *Proc. of 4th Annual International Cryptology Conference (Crypto'84)*, pp. 47-53, Santa Barbara, USA, 1984.

[17] B. Waters, "Efficient identity-based encryption without random oracles", *Proc. of 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05)*, pp. 114-127, Aarhus, Denmark, 2005.

[18] X. Zhao, "Amendment to Trace and Revoke Systems with Short Ciphertexts", *International Journal of Network Security*, vol. 14, no. 5, pp. 251-256, 2012.

Yanli Ren is an associate professor in School of Communication and Information Engineering at Shanghai University. She was awarded a MS degree in applied mathematics in 2005 from Shaanxi Normal University, China, and a PhD degree in computer science and technology in 2009 from Shanghai Jiao Tong University, China. Her research interests include applied cryptography, secure computing, and network security.

Zhihua Niu received her B.S degree in Mathematics Education at Huaibei Normal University, China, in 1998. She received her M.S. degree in Computational Mathematics at Xi'an Jiaotong University, China, in 2002. And she received her Ph.D. degree in Cryptography at Xidian University, China, in 2005. Now she is an associate professor at Shanghai University, China. Her research interests are mainly at Cryptography and Information security.

Xinpeng Zhang received the BS degree in computational mathematics from Jilin University, China, in 1995, and the ME and PhD degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University, where he is currently a professor. His research interests include multimedia security, image processing and digital forensics.