Fully Secure Anonymous Identity Based Broadcast Encryption with Group of Prime Order

Yang Ming and Hongping Yuan

(Corresponding author: Yang Ming)

School of Information Engineering, Chang'an University
Middle-section of Nan'er Huan Road, Xi'an, Shaanxi 710064, China
(Email: yangming@chd.edu.cn)

(Received Aug. 31, 2017; revised and accepted Nov. 5, 2017)

Abstract

Anonymous identity based broadcast encryption (IBBE) is a cryptographic primitive, which allows a broadcaster to transmit encrypted data over a broadcast channel to a large number of users such that only a select subset of privileged users can decrypt it and any user cannot distinguish the encrypted message to which user. In this paper, based on the asymmetric bilinear pairing, a new anonymous IBBE scheme is proposed. Under the assumption of symmetric external Diffie-Hellman, we prove that the proposed scheme is fully secure (adaptive security) in the standard model using the dual system encryption method. This construction utilizes the dual pairing vector space technique in the group of prime order to realize the parameter hiding and cancelling properties of the group of composite order. The performance analysis depict that the proposed scheme achieves simultaneously the constant size system parameters, private keys and ciphertexts. In addition, the recipient anonymity can be captured.

Keywords: Dual System Encryption; Fully Secure; Group of Prime Order; Identity Based Broadcast Encryption

1 Introduction

In 1993, Fiat and Naor [6] first introduced the concept of broadcast encryption (BE). In a BE scheme, the broadcaster broadcasts encrypted message over a broadcast channel to some subset of users. Any user in the designated subset can decrypt the ciphertext using his private key. Broadcast encryption is widely used in many fields, such as multicast communication, pay TV, satellite based electronic commerce, *etc.*. Since the concept of broadcast encryption is proposed, many BE schemes [1,4,5,12,18,28] have been proposed.

In 1984, the concept of identity based encryption (IBE) was firstly proposed by Shamir [27]. The main idea of IBE is that a user can utilize the identity (Email address, IP address, *etc.*) of recipient as public key to encrypt a message. It simplifies the management of public key certificates and avoids the need to distribute certificates. Identity based broadcast encryption (IBBE) is a generalization of identity based encryption (IBE). A scenario of IBBE is shown in Figure 1.

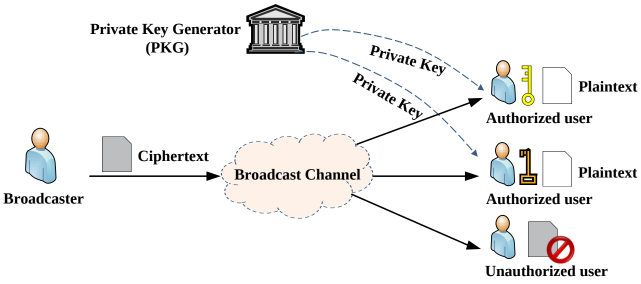

Figure 1: A typical structure of IBBE

In 2007, Delerable [3] proposed an IBBE scheme, which captures constant size ciphertexts and private keys. But the proposed scheme was only selective-identity secure (the adversary must declare at the beginning of its attack which identity it will target) in the random oracles model. In 2009, Gentry *et al.* [8] presented a provably secure BE scheme in the standard model, which achieved fully secure (the adversary may choose the target identity adaptively) with sublinear ciphertext. Ren *et al.* [25] proposed an IBBE scheme with constant size ciphertexts and public keys. The proposed scheme was fully secure in the standard model. Based on the dual system encryption idea, a BE scheme in the bilinear groups of composite order was presented by Waters [30]. However, this scheme is inefficient because of decryption cost depending on the user number. In 2010, Lewko *et al.* [20] presented an IBBE scheme in the groups of composite order and proved the security under the general subgroup decision assumption. The proposed scheme satisfied fully secure under the static assumption via the convenient properties of the bilinear groups of composite order. In 2012, Zhang *et al.* [33] presented a fully secure IBBE using dual system encryption technique in the subgroups, which achieved the constant size ciphertexts and private keys. In 2015, Kim *et al.* [13] proposed an IBBE scheme with constant size ciphertexts. This scheme was adaptively secure under the general decisional subgroup assumption in the standard model using the technique of dual system encryption. In 2016, Susilo *et al.* [29] given a recipient-revocable IBBE scheme, where ciphertext size is independent of the number of receivers.

In 2012, an anonymous BE scheme in the standard model was proposed by Libert *et al.* [21]. However, in which ciphertext size grows with the receiver numbers linearly. In 2013, Zhang *et al.* [35] presented an anonymous BE scheme with the group of composite order in the standard model, that was proved fully secure and the ciphertext size was constant at the same time. In 2014, Xie *et al.* [31] presented an anonymous IBBE scheme in the bilinear groups of prime order. The proposed scheme achieved adaptive secure under the asymmetric decisional bilinear Diffie-Hellman Exponent assumption without using the random oracles. However, the system parameter and private key size grows with the number of users and that of receivers linearly, respectively. Ren *et al.* [26] proposed a fully secure anonymous IBBE scheme based on asymmetric bilinear groups, which achieved adaptive secure in the standard model. But, system parameter, ciphertext and private key size grows with the number of users or that of receivers linearly, respectively. In 2015, Zhang *et al.* [34] proposed a leakage-resilient anonymous IBBE with constant size ciphertexts, which achieved fully secure in the standard model. However, the system parameter size is not constant and relies on the number of users. In 2016, Lai *et al.* [16] constructed an anonymous IBBE with ciphertext revocation. He *et al.* [9] proposed a generic IBBE construction in the random oracle model, which has constant size system parameters, the private keys and decryption cost. He *et al.* also [10] presented a secure IBBE scheme under the DBDH assumption. The new scheme was efficient and simultaneously achieved confidentiality and anonymity. Xu *et al.* [32] proposed an IBBE scheme with constant decryption complexity and strong anonymous. In 2017, He *et al.* [11] given a generic IBBE scheme that achieved confidentiality and anonymity. The proposed scheme was proven security in the random oracle model and satisfied constant size system parameters and private keys. Lai *et al.* [15, 17] proposed the fully revocable privacy-preserving IBBE schemes in the random oracle model.

To achieve the same security level, when the size of the elliptic curve group of composite order is 1024 bits, and that of prime order is only 160 bits [7]. Therefore, how to design the IBBE scheme in the group of prime order becomes a hot issue. In 2010, Freeman *et al.* [7] firstly showed that the group of composite order has two features: cancelling (orthogonality) and projecting and given a general technique to convert composite order schemes into prime order schemes relying on either cancelling or projecting. In 2016, Ming *et al.* [23] proposed a secure IBBE scheme using dual system encryption in the group of prime order. In this paper, based on the asymmetric bilinear pairing, we present an anonymous IBBE scheme using the dual pairing vector space and dual system encryption techniques. The proposed scheme captures fully secure (adaptive security) in the standard model assume that the symmetric external Diffie-Hellman problem is hard. The performance analysis shows that the proposed scheme has constant size system parameters, ciphertexts and private keys, and achieves the receiver's identity anonymity.

The rest of this paper is organized as follows. The preliminaries are presented in Section 2. Section 3 gives the formal model of anonymous IBBE. Our concrete construction is described in Section 4. Section 5 evaluates the performance. Finally, conclusions are provided in Section 6.

2 Preliminaries

2.1 Asymmetric Bilinear Groups

Assume $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be three cyclic groups with order of q, where q is a large prime. Let g_1 and g_2 be a generator of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. The bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ has the following properties [14, 22]:

Bilinearity: For all $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$ and $s, t \in \mathbb{Z}_q$, $e(g_1^s, g_2^t) = e(g_1, g_2)^{st}$.

Non-degeneracy: $e(g_1, g_2) \neq 1$.

Computability: There exists an efficient algorithm to compute $e(g_1, g_2)$ for all $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$.

2.2 Dual Pairing Vector Spaces

The asymmetric dual pairing vector spaces technique [24] will be utilized in the following proposed scheme. For $\mathrm{v} = (v_1, \cdots, v_n) \in \mathbb{Z}_q^n$ and $g_\beta \in \mathbb{G}_\beta$, g_β^{v} is defined as n elements of $\mathbb{G}_\beta$ for $\beta = 1, 2$:

$$g_\beta^{\mathrm{v}} = (g_\beta^{v_1}, \cdots, g_\beta^{v_n}).$$

For any $a \in \mathbb{Z}_q$ and $\mathrm{v}, \mathrm{w} \in \mathbb{Z}_q^n$, we have:

$$g_\beta^{a\mathrm{v}} = (g_\beta^{av_1}, \cdots, g_\beta^{av_n}),\ g_\beta^{\mathrm{v}+\mathrm{w}} = (g_\beta^{v_1+w_1}, \cdots, g_\beta^{v_n+w_n}).$$

Then we define

$$e(g_1^{\mathrm{v}}, g_2^{\mathrm{w}}) = \prod_{i=1}^{n} e(g_1^{v_i}, g_2^{w_i}) = e(g_1, g_2)^{\mathrm{v}\cdot\mathrm{w}}.$$

The two bases $\mathrm{B} = (b_1, \cdots, b_n)$ and $\mathrm{B}^* = (b_1^*, \cdots, b_n^*)$ of $\mathbb{Z}_q^n$ are randomly chosen to satisfy "dual orthonormal". This is to say that $b_r \cdot b_k^* = 0 (\mathrm{mod}\ q)$ for $r \neq k$, $b_k \cdot b_k^* = \psi (\mathrm{mod}\ q)$ for all k and a random element $\psi \in \mathbb{Z}_q$.

2.3 Security Assumptions

Decisional Diffie-Hellman problem in $\mathbb{G}_1$ (DDH1): Given $D = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, q, e, g_1^a, g_1^b)$, pick randomly $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, $a, b, c \in \mathbb{Z}_q$ and $T_1 = g_1^{ab}, T_2 = g_1^{ab+c}$, the DDH1 problem is to distinguish T_1 and T_2.

The advantage of an algorithm $\mathcal{B}$ solving the DDH1 problem is defined as:

$$Adv_{\mathcal{B}}^{DDH1} = |\Pr[\mathcal{B}(D, T_1)] - \Pr[\mathcal{B}(D, T_2)]|.$$

Decisional Diffie-Hellman problem in $\mathbb{G}_2$ (DDH2): Given $D = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, q, e, g_2^a, g_2^b)$, pick randomly $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, $a, b, c \in \mathbb{Z}_q$ and $T_1 = g_2^{ab}, T_2 = g_2^{ab+c}$, the DDH2 problem is to distinguish T_1 and T_2.

The advantage of an algorithm $\mathcal{B}$ solving the DDH2 problem is defined as:

$$Adv_{\mathcal{B}}^{DDH2} = |\Pr[\mathcal{B}(D, T_1)] - \Pr[\mathcal{B}(D, T_2)]|.$$

Symmetric external Diffie-Hellman assumption [2]: This assumption holds if both DDH 1 and DDH 2 problems are intractable.

Decisional subspace problem in $\mathbb{G}_1$ (DS1): Given $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e$, $\mathrm{B} = (b_1, \cdots, b_n)$, $\mathrm{B}^* = (b_1^*, \cdots, b_n^*)$, pick randomly $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, $\tau_1, \tau_2, \mu_1, \mu_2 \in \mathbb{Z}_q$ and

$$\begin{aligned}
U_1 &= g_2^{\mu_1 b_1^* + \mu_2 b_{K+1}^*}, \cdots, \\
U_K &= g_2^{\mu_1 b_K^* + \mu_2 b_{2K}^*}, \\
V_1 &= g_1^{\tau_1 b_1}, \cdots, \\
V_K &= g_1^{\tau_1 b_K}, \\
W_1 &= g_1^{\tau_1 b_1 + \tau_2 b_{K+1}}, \cdots, \\
W_K &= g_1^{\tau_1 b_K + \tau_2 b_{2K}}.
\end{aligned}$$

Let $D = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e, g_1, g_2, g_2^{b_1^*}, \cdots, g_2^{b_K^*}, g_2^{b_{2K+1}^*}, \cdots, g_2^{b_N^*}, g_1^{b_1}, \cdots, g_1^{b_N}, U_1, \cdots, U_K, \mu_2)$, where K, N are positive integers satisfying $2K \leq N$. The DS1 problem is to distinguish $V_1, \cdots, V_K$ and $W_1, \cdots, W_K$.

The advantage of an algorithm $\mathcal{B}$ solving the DS1 problem is defined as:

$$\begin{aligned}
Adv_{\mathcal{B}}^{DS1} = & \ |\Pr[\mathcal{B}(D, V_1, \cdots, V_K) = 1] \\
& - \Pr[\mathcal{B}(D, W_1, \cdots, W_K) = 1]|.
\end{aligned}$$

Decisional subspace problem in $\mathbb{G}_2$ (DS2): Given $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e$, $\mathrm{B} = (b_1, \cdots, b_n)$, $\mathrm{B}^* = (b_1^*, \cdots, b_n^*)$, pick randomly $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$, $\tau_1, \tau_2, \mu_1, \mu_2 \in \mathbb{Z}_q$ and

$$\begin{aligned}
U_1 &= g_1^{\mu_1 b_1^* + \mu_2 b_{K+1}^*}, \cdots, \\
U_K &= g_1^{\mu_1 b_K^* + \mu_2 b_{2K}^*}, \\
V_1 &= g_2^{\tau_1 b_1}, \cdots, \\
V_K &= g_2^{\tau_1 b_K}, \\
W_1 &= g_2^{\tau_1 b_1 + \tau_2 b_{K+1}}, \cdots, \\
W_K &= g_2^{\tau_1 b_K + \tau_2 b_{2K}}.
\end{aligned}$$

Let $D = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e, g_1, g_2, g_1^{b_1^*}, \cdots, g_1^{b_K^*}, g_1^{b_{2K+1}^*}, \cdots, g_1^{b_N^*}, g_2^{b_1}, \cdots, g_2^{b_N}, U_1, \cdots, U_K, \mu_2)$, where K, N are positive integers satisfying $2K \leq N$. The DS2 problem is to distinguish $V_1, \cdots, V_K$ and $W_1, \cdots, W_K$.

The advantage of an algorithm $\mathcal{B}$ solving the DS2 problem is defined as:

$$\begin{gathered}
Adv_{\mathcal{B}}^{DS2} = \\
|\Pr[\mathcal{B}(D, V_1, \cdots, V_K) = 1] - \Pr[\mathcal{B}(D, W_1, \cdots, W_K) = 1]|.
\end{gathered}$$

The DS1 problem is intractable if DDH1 problem is hard, the DS2 problem is intractable if DDH2 problem is hard [2].

3 Framework of Anonymous IBBE

3.1 Syntax

An IBBE scheme with security parameter λ consists of the following algorithms:

Setup: Given λ and m, the maximal size of the receiver set for one encryption, the Private Key Generator (PKG) generates the system parameter *params* and the master key *msk*. The *params* is made public while the *msk* is kept secret.

Extract: Given *params*, *msk* and a user's identity ID, this algorithm outputs the private key SK_{ID_i} and sends it to the user via a secure channel.

Encrypt: Given *params*, a set of identities $S = \{ID_1, \cdots, ID_n\}$ with $n \leq m$ and a message M, this algorithm outputs a ciphertext CT.

Decrypt: Given *params*, a subset $S = \{ID_1, \cdots, ID_n\}$ with $n \leq m$, a ciphertext CT, an identity ID_i and the private key SK_{ID_i}, if $ID_i \in S$, this algorithm outputs the plaintext M.

3.2 Security Model

We depict the fully secure (adaptive security) model for the anonymous IBBE scheme. The security is defined by the following interaction game played between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$. Let Ω the maximal size of the receivers set.

Setup: The challenger $\mathcal{C}$ runs the algorithm **Setup** to produce the master key msk and the system parameters $params$. Then $\mathcal{C}$ keeps master key msk secret and returns $params$ to $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ adaptively issues the private key queries and decryption queries.

Private key query: Given a private key query on ID_i, $\mathcal{C}$ runs the algorithm **Extract** to produce the private key SK_{ID_i} and return it to $\mathcal{A}$.

Decryption Query: Given a decryption query on (ID_i, S, CT) with $S \subseteq \Omega$ and $ID_i \in S$. $\mathcal{C}$ firstly runs the algorithm **Extract** to produce the private key SK_{ID_i}. Then it runs the algorithm **Decrypt** to obtain the message M and send it to $\mathcal{A}$.

Challenge: At the end of **Phase 1**, $\mathcal{A}$ outputs two same-length messages M_0^*, M_1^* and two user sets S_0^*, S_1^* on which it wants to be challenged. The challenger $\mathcal{C}$ selects a random value $\theta \in \{0,1\}$ and denotes the challenge ciphertext $CT^* = Encrypt(params, M_\theta^*, S_\theta^*)$. At last, $\mathcal{C}$ sends CT^* to $\mathcal{A}$ as its challenge ciphertext.

Phase 2: The adversary $\mathcal{A}$ issues queries adaptively again as in **Phase 1**. The challenger $\mathcal{C}$ responses these queries as **Phase 1** except that $\mathcal{A}$ is not permitted to issue a private key query on any $ID_i \in S_0^*, S_1^*$ and a decryption query on (CT^*, S_0^*) and (CT^*, S_1^*).

Guess: Eventually, the adversary $\mathcal{A}$ outputs its guess $\theta' \in \{0,1\}$. $\mathcal{A}$ wins the game if $\theta' = \theta$.

The advantage of $\mathcal{A}$ wins the game is defined as

$$Adv_{\mathcal{A}} = |2\Pr[\beta' = \beta] - 1|.$$

Definition 1. *An anonymous IBBE scheme is said to be $(q_k, q_d, t, \varepsilon)$-ANONY-IND-ID-CCA secure if for any adversary making at most q_k private key queries and q_d decryption queries in time t has advantage ε, we have $Adv_{\mathcal{A}} \leq \varepsilon$.*

Definition 2. *An anonymous IBBE scheme is said to be (q_k, t, ε)-ANONY-IND-ID-CPA secure if it is $(q_k, 0, t, \varepsilon)$-ANONY-IND-ID-CCA secure.*

4 The Proposed Scheme

This section describes an anonymous IBBE scheme with group of prime order. Let m denote the maximum size of the user set. The concrete construction includes the following phases:

Setup: Given the security parameter λ and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, the PKG randomly picks $\alpha \in \mathbb{Z}_q$ and samples random dual orthonormal bases (D,D*). Let $d_1, \cdots, d_4$ be the elements of D and $d_1^*, \cdots, d_4^*$ be the elements of D*. The master key is $msk = \{\alpha, g_2^{d_1^*}, g_2^{d_2^*}\}$. The public system parameters are $params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, q, e(g_1, g_2)^{\alpha d_1 d_1^*}, g_1^{d_1}, g_1^{d_2}\}$.

Extract: Given the identity $ID_i \in S$, where $S = \{ID_1, \cdots, ID_n\}$ for $n \leq m$, the PKG randomly chooses $r_1^1, \cdots, r_1^n \in \mathbb{Z}_q$ and computes $SK_{ID_i} = \{k_1, k_2\}$ as follows:

$$\begin{aligned} k_1 &= g_2^{(\alpha + r_1^i ID_i)d_1^* - r_1^i d_2^*}, \\ k_2 &= g_2^{(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)(ID_1 + \cdots + ID_n)d_1^*} \\ &\cdot g_2^{r_1^i (ID_1 + ID_2 + \cdots + ID_{i-1} + ID_{i+1} + \cdots + ID_n)d_1^*} \\ &\cdot g_2^{-(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)d_2^*}. \end{aligned}$$

Encrypt: Given the massage M, a broadcaster randomly chooses $z \in \mathbb{Z}_q$ and computes the ciphertext:

$$\begin{aligned} CT &= \{C_1, C_2\} \\ &= \{M \cdot e(g_1, g_2)^{\alpha z d_1 d_1^*}, g_1^{z d_1 + z(ID_1 + \cdots + ID_n) d_2}\} \end{aligned}$$

Decrypt: Given the ciphertext $CT = \{C_1, C_2\}$, any user $ID_i \in S$ can compute

$$M = \frac{C_1}{e(C_2, k_1 k_2)}.$$

5 Analysis

5.1 Correctness

$$\begin{aligned} & \frac{C_1}{e(C_2, k_1 k_2)} \\ &= \frac{M \cdot e(g_1, g_2)^{\alpha z d_1 d_1^*}}{e(g_1^{z d_1 + z(ID) d_2}, g_2^{[\alpha + R(ID)]d_1^* - R d_2^*})} \\ &= \frac{M \cdot e(g_1, g_2)^{\alpha z d_1 d_1^*}}{e(g_1, g_2)^{\alpha z d_1 d_1^* + zR(ID) d_1 d_1^* - zR(ID) d_2 d_2^*}} \\ &= \frac{M \cdot e(g_1, g_2)^{\alpha z d_1 d_1^*}}{e(g_1, g_2)^{\alpha z d_1 d_1^* + [zR(ID) - zR(ID)]\psi}} \\ &= M. \\ ID &= ID_1 + ID_2 + \cdots + ID_n \\ R &= r_1^1 + r_1^2 + \cdots + r_1^n \\ k_1 \cdot k_2 &= g_2^{(\alpha + r_1^i ID_i)d_1^* - r_1^i d_2^*} \\ &\cdot g_2^{(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)(ID_1 + \cdots + ID_n)d_1^*} \\ &\cdot g_2^{r_1^i (ID_1 + ID_2 + \cdots + ID_{i-1} + ID_{i+1} + \cdots + ID_n)d_1^*} \\ &\cdot g_2^{-(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)d_2^*} \\ &= g_2^{[\alpha + (r_1^1 + \cdots + r_1^n)(ID_1 + \cdots + ID_n)]d_1^* - (r_1^1 + \cdots + r_1^n)d_2^*} \end{aligned}$$

5.2 Security Proof

To prove the security of the proposed scheme using the dual system encryption technique [30], we need to define the semi-functional keys and semi-functional ciphertexts, which are only provided for definitional purpose, and are not part of the scheme.

Semi-functional keys: A normal key $SK'_{ID_i} = \{k'_1, k'_2\}$ is generated using the algorithm **Extract** and $v_1, v_2, \dot{v}_1, \dot{v}_2 \in \mathbb{Z}_q$ are randomly selected. The semi-functional keys are defined as

$$SK^{(SF)}_{ID_i} = \{k_1, k_2\} = \{k'_1 \cdot g_2^{v_1 d_3^* + v_2 d_4^*}, k'_2 \cdot g_2^{\dot{v}_1 d_3^* + \dot{v}_2 d_4^*}\}.$$

Semi-functional ciphertexts: A normal ciphertext $CT' = \{C'_1, C'_2\}$ is generated using the algorithm **Encrypt** and $\chi_1, \chi_2 \in \mathbb{Z}_q$ are randomly selected. The semi-functional ciphertexts are defined as

$$CT^{(SF)} = \{C_1, C_2\} = \{C'_1, C'_2 \cdot g_1^{\chi_1 d_3 + \chi_2 d_4}\}.$$

A hybrid argument over a sequence of games is used in proof. The first game is the real security game. The adversary has no advantage unconditionally in the last game and makes q_n private keys queries. We show that each game is indistinguishable from the next. These games are described as follows:

$Game_{real}$**:** This game is a real security game.

$Game_k$**:** For $k = 1, \cdots, q_n$, $Game_k$ is the same as $Game_{real}$ with the limitations:

1) The challenge ciphertext on the challenge set is a semi-functional ciphertext.
2) The first k private keys are semi-functional, and the remaining private keys are normal.

The challenge ciphertext is semi-functional, all the private keys are normal in $Game_0$, the challenge ciphertext, and all the private keys are semi-functional in $Game_{q_n}$.

$Game_{Final}$**:** This game is the same as $Game_{q_n}$ except that the challenge ciphertext is a semi-functional encryption of a random message, instead of one of the two challenge messages.

In the following four lemmas, we prove that these games are indistinguishable. Let $Adv_{\mathcal{A}}^{Game_{real}}$ be the advantage in $Game_{real}$, $Adv_{\mathcal{A}}^{Game_k}$ be advantage in $Game_k$, and $Adv_{\mathcal{A}}^{Game_{final}}$ be advantage in $Game_{final}$.

Lemma 1. Assume that there exists an adversary $\mathcal{A}$ such that $Adv_{\mathcal{A}}^{Game_{real}} - Adv_{\mathcal{A}}^{Game_0} = \varepsilon$, then there exists an algorithm B_0 with advantage $Adv_{B_0}^{DS1} = \varepsilon$ in solving the DS1 problem with $(K, N) = (2, 4)$.

Proof. The algorithm B_0 is given $D = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, q, g_1, g_2, g_2^{b_1^*}, g_2^{b_2^*}, g_1^{b_1}, \cdots, g_1^{b_4}, U_1, U_2, \mu_2\}$ along with T_1, T_2. The goal of B_0 is to decide whether T_1, T_2 are distributed as $g_1^{\tau_1 b_1}, g_1^{\tau_1 b_2}$ or $g_1^{\tau_1 b_1 + \tau_2 b_3}, g_1^{\tau_1 b_2 + \tau_2 b_4}$.

Setup: B_0 randomly selects an invertible matrix $\mathrm{A} \in \mathbb{Z}_q^{2\times 2}$ and implicitly defines dual orthonormal bases $\mathrm{D} = (d_1, d_2, d_3, d_4)$, $\mathrm{D}^* = (d_1^*, d_2^*, d_3^*, d_4^*)$ as follows:

$$\begin{aligned} d_1 &= b_1, d_2 = b_2, (d_3, d_4) = (b_3, b_4)\mathrm{A}, \\ d_1^* &= b_1^*, d_2^* = b_2^*, (d_3^*, d_4^*) = (b_3^*, b_4^*)(\mathrm{A}^{-1})^{\mathrm{T}}. \end{aligned}$$

B_0 randomly chooses a value $\alpha \in \mathbb{Z}_q$ and sends the public parameters $params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, q, g_1, g_2, e(g_1, g_2)^{\alpha d_1 d_1^*}, g_1^{d_1}, g_1^{d_2}\}$ to the adversary $\mathcal{A}$ and keeps the master key $msk = \{\alpha, g_2^{d_1^*}, g_2^{d_2^*}\}$ secret.

Query 1: $\mathcal{A}$ adaptively makes the private key queries on the identity $ID_i \in S$, where $S = \{ID_1, \cdots, ID_n\}$. B_0 runs the algorithm **Extract** using the master key to respond to all of $\mathcal{A}$'s queries.

Challenge: $\mathcal{A}$ outputs two challenge messages M_0^*, M_1^* and two challenge sets $S_0^* = \{ID_{01}^*, \cdots, ID_{0n}^*\}$, $S_1^* = \{ID_{11}^*, \cdots ID_{1n}^*\}$. B_0 randomly picks a bit $\theta \in \{0, 1\}$ and defines the ciphertext as follows:

$$C_1 = M_\theta^* \cdot e(T_1, g_2^{b_1^*})^\alpha,\ C_2 = T_1 \cdot (T_2)^{ID_{\theta 1}^* + \cdots + ID_{\theta n}^*}.$$

Query 2: $\mathcal{A}$ continues to make the private key queries on ID_i where $ID_i \notin S_0^*, S_1^*$.

Guess: Eventually, $\mathcal{A}$ outputs a guess $\theta' \in \{0, 1\}$. $\mathcal{A}$ wins the game if $\theta' = \theta$.

Let $\tau_1 = z$. If T_1, T_2 are equal to $g_1^{\tau_1 b_1}$, $g_1^{\tau_1 b_2}$, then $CT = \{C_1, C_2\}$ is a properly distributed normal ciphertext. Hence, B_0 has properly simulated $Game_{real}$.

If T_1, T_2 are equal to $g_1^{\tau_1 b_1 + \tau_2 b_3}$, $g_1^{\tau_1 b_2 + \tau_2 b_4}$, then $CT = \{C_1, C_2\}$ is a properly distributed semi-functional ciphertext. There is an additional term of $\tau_2[b_3 + b_4(ID_{\beta 1}^* + \cdots + ID_{\beta n}^*)]$ in the exponent of C_2. To compute the coefficients in the basis d_3, d_4, we multiply the matrix A^{-1} by the transpose of this vector and obtain $\tau_2 \mathrm{A}^{-1}[1 + (ID_{\beta 1}^* + \cdots + ID_{\beta n}^*)]^{\mathrm{T}}$. Since the matrix A is random, these coefficients are uniformly random according to statistical indistinguishability lemma [19]. Hence, B_0 has properly simulated $Game_0$.

B_0 can leverage $\mathcal{A}$'s advantage between $Game_{real}$ and $Game_0$ to achieve an advantage $Adv_{B_0}^{DS1} = \varepsilon$ in solving DS1 problem. □

Lemma 2. Assume that an adversary $\mathcal{A}$ makes at most q_n private key queries and such that $Adv_{\mathcal{A}}^{Game_{k-1}} - Adv_{\mathcal{A}}^{Game_k} = \varepsilon$. Then there exists an algorithm B_k with advantage $Adv_{B_k}^{DS2} = \varepsilon - 1/q$ in solving the DS2 problem with $(K, N) = (2, 4)$.

Proof. The algorithm B_k is given $D = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, q, g_1, g_2, g_1^{b_1}, g_1^{b_2}, g_2^{b_1^*}, \cdots, g_2^{b_4^*}, U_1, U_2, \mu_2\}$ along with T_1, T_2. The goal of B_k is to decide whether T_1, T_2 are distributed as $g_2^{\tau_1 b_1^*}$, $g_2^{\tau_1 b_2^*}$ or $g_2^{\tau_1 b_1^* + \tau_2 b_3^*}$, $g_2^{\tau_1 b_2^* + \tau_2 b_4^*}$.

Setup: B_k randomly picks an invertible matrix $\mathrm{A} \in \mathbb{Z}_q^{2\times 2}$ and implicitly defines dual orthonormal bases $\mathrm{D} = (d_1, d_2, d_3, d_4)$, $\mathrm{D}^* = (d_1^*, d_2^*, d_3^*, d_4^*)$ as follows:

$$\begin{aligned} d_1 &= b_1, d_2 = b_2, (d_3, d_4) = (b_3, b_4)\mathrm{A}, \\ d_1^* &= b_1^*, d_2^* = b_2^*, (d_3^*, d_4^*) = (b_3^*, b_4^*)(\mathrm{A}^{-1})^{\mathrm{T}}. \end{aligned}$$

B_k randomly chooses a value $\alpha \in \mathbb{Z}_q$ and sends the public parameters $params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, q, g_1, g_2, e(g_1, g_2)^{\alpha d_1 d_1^*}, g_1^{d_1}, g_1^{d_2}\}$ to the adversary $\mathcal{A}$ and keeps the master key $msk = \{\alpha, g_2^{d_1^*}, g_2^{d_2^*}\}$ secret.

Query 1: $\mathcal{A}$ adaptively makes the private key queries on the identity $ID_i \in S$, where $S = \{ID_1, \cdots, ID_n\}$. B_k answers as follows:

1) $i < k$, B_k firstly runs the algorithm **Extract** using the master key to produce the normal private keys. Since B_k knows $g_2^{d_3^*}, g_2^{d_4^*}$, it can easily produce the semi-functional private keys.

2) $i > k$, B_k runs the algorithm **Extract** using the master key to produce the normal private keys.

3) $i = k$, B_k randomly chooses $r_1^1, \cdots, r_1^{i-1}, r_1^{i+1}, \cdots, r_1^n \in \mathbb{Z}_q$ and implicitly sets $r_1^i = \tau_1$ and computes $SK_{ID_i} = \{k_1, k_2\}$ as follows:

$$\begin{aligned} k_1 &= g_2^{\alpha b_1^*} \cdot T_1^{ID_i} \cdot T_2^{-1}, \\ k_2 &= g_2^{(r_1^1+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)(ID_1+\cdots+ID_n)]b_1^*} \\ &\quad \cdot g_2^{-(r_1^1+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)b_2^*} \\ &\quad \cdot T_1^{(ID_1+\cdots+ID_{i-1}+ID_{i+1}+\cdots+ID_n)} \end{aligned}$$

If T_1, T_2 are equal to $g_2^{\tau_1 b_1^*}$, $g_2^{\tau_1 b_2^*}$, $SK_{ID_i} = \{k_1, k_2\}$ is a properly distributed normal key.

If T_1, T_2 are equal to $g_2^{\tau_1 b_1^* + \tau_2 b_3^*}$, $g_2^{\tau_1 b_2^* + \tau_2 b_4^*}$, $SK_{ID_i} = \{k_1, k_2\}$ is a semi-functional key, whose exponent vector includes $\tau_2[(ID_1 + \cdots + ID_n)b_3^* - b_4^*]$ as its component in the span of b_3^*, b_4^*. To compute the coefficients in the basis d_3, d_4, we multiply the matrix A^{T} by the transpose of this vector and obtain $\tau_2 \mathrm{A}^{\mathrm{T}}[(ID_1 + \cdots + ID_n) - 1]^{\mathrm{T}}$.

Challenge: $\mathcal{A}$ outputs two challenge messages M_0^*, M_1^* and two challenge sets $S_0^* = \{ID_{01}^*, \cdots, ID_{0n}^*\}$, $S_1^* = \{ID_{11}^*, \cdots, ID_{1n}^*\}$. B_k randomly picks a bit $\theta \in \{0, 1\}$ and defines the semi-functional ciphertext as follows:

$$C_1 = M_\theta^* \cdot e(U_1, g_2^{b_1^*})^\alpha,\ C_2 = U_1 \cdot U_2^{(ID_{\theta 1}^* + \cdots + ID_{\theta n}^*)}.$$

B_k sets $z = u_1$. To calculate the coefficients of the basis d_3, d_4, we multiply the matrix A^{-1} by the vector $u_2[1 + (ID_{\theta 1}^* + \cdots + ID_{\theta n}^*)]$ and obtain $u_2 \mathrm{A}^{-1}[1 + (ID_{\theta 1}^* + \cdots + ID_{\theta n}^*)]$. Since A is random, these coefficients of d_3, d_4 are uniformly random according to statistical indistinguishability lemma [19].

Query 2: $\mathcal{A}$ continues to make the private key queries on ID_i where $ID_i \notin S_0^*, S_1^*$.

Guess: Eventually, $\mathcal{A}$ outputs a guess $\theta' \in \{0, 1\}$. $\mathcal{A}$ wins the game if $\theta' = \theta$.

Therefore, according to the distribution of T_1 and T_2, B_k has properly simulated either $Game_{k-1}$ or $Game_k$. B_k can leverage $\mathcal{A}$'s advantage between these games to achieve an advantage $Adv_{B_k}^{DS2} = \varepsilon - 1/q$ in solving the DS2 problem. □

Lemma 3. For any adversary $\mathcal{A}$, we have $Adv_{\mathcal{A}}^{Game_{q_n}} = Adv_{\mathcal{A}}^{Game_{Final}}$.

Proof. We prove that the joint distributions of $\{params, \{SK_{ID_{li}}^{(SF)}\}_{l \in [1, q_n]}, CT_{ID_{\theta i}^*}^{(SF)}\}$ in $Game_{q_n}$ and that of $\{params, \{SK_{ID_{li}}^{(SF)}\}_{l \in [1, q_n]}, CT_{ID_{Ri}^*}^{(R)}\}$ in $Game_{Final}$ are equivalent for $\mathcal{A}$'s view, where $CT_{ID_{Ri}^*}^{(R)}$ is a semi-functional encryption of a random message.

We randomly pick a matrix $\mathrm{A} = (\xi_{i,j}) \in \mathbb{Z}_q^{2 \times 2}$ and define new dual orthonormal bases $\mathrm{F} = (f_1, \cdots, f_4)$ and $\mathrm{F}^* = (f_1^*, \cdots, f_4^*)$ as follows:

$$\begin{pmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \xi_{1,1} & \xi_{1,2} & 1 & 0 \\ \xi_{2,1} & \xi_{2,2} & 0 & 1 \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix},$$

$$\begin{pmatrix} f_1^* \\ f_2^* \\ f_3^* \\ f_4^* \end{pmatrix} = \begin{pmatrix} 1 & 0 & -\xi_{1,1} & -\xi_{2,1} \\ 0 & 1 & -\xi_{1,2} & -\xi_{2,2} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} d_1^* \\ d_2^* \\ d_3^* \\ d_4^* \end{pmatrix}$$

It is easy to verify that F and F* are also dual orthonormal, and are distributed the same as D and D*.

The system parameters, private keys and the challenge ciphertext $\{params, \{SK_{ID_{li}}^{(SF)}\}_{l \in [1, q_n]}, CT_{ID_{\theta i}^*}^{(SF)}\}$ in $Game_{q_n}$ are expressed over the bases D and D* as follows:

$$params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, q, e(g_1, g_2)^{\alpha d_1 d_1^*}, g_1^{d_1}, g_1^{d_2}\}$$

$$\{SK_{ID_{li}}^{(SF)}\}_{l \in [1, q_n]} = \left\{ \begin{aligned} k_1 &= g_2^{(\alpha + r_l^i ID_{li})d_1^* - r_l^i d_2^* + v_{1,l} d_3^* + v_{2,l} d_4^*} \\ k_2 &= g_2^{(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)(ID_{l1}+\cdots+ID_{ln})d_1^*} \\ &\quad \cdot g_2^{r_l^i(ID_{l1}+\cdots+ID_{li-1}+ID_{li+1}+\cdots+ID_{ln})d_1^*} \\ &\quad \cdot g_2^{-(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)d_2^*} \\ &\quad \cdot g_2^{\dot{v}_{1,l} d_3^* + \dot{v}_{2,l} d_4^*} \end{aligned} \right\}_{l \in [1, q_n]}$$

$$\begin{aligned} CT_{ID_{\theta i}^*}^{(SF)} = \{ &C_1 = M_\theta^* \cdot e(g_1, g_2)^{\alpha z d_1 d_1^*}, \\ &C_2 = g_1^{z d_1 + z(ID_{\theta 1}^* + \cdots + ID_{\theta n}^*)]d_2 + \chi_1 d_3 + \chi_2 d_4}\}. \end{aligned}$$

They are expressed over the bases F and F* as follows:

$$params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, q, e(g_1, g_2)^{\alpha f_1 f_1^*}, g_1^{f_1}, g_1^{f_2}\}$$

$$\{SK_{ID_{li}}^{(SF)}\}_{l \in [1, q_n]} = \left\{ \begin{aligned} k_1 &= g_2^{(\alpha + r_l^i ID_{li})f_1^* - r_l^i f_2^* + v'_{1,l} f_3^* + v'_{2,l} f_4^*} \\ k_2 &= g_2^{(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)(ID_{l1}+\cdots+ID_{ln})f_1^*} \\ &\quad \cdot g_2^{r_l^i(ID_{l1}+\cdots+ID_{li-1}+ID_{li+1}+\cdots+ID_{ln})f_1^*} \\ &\quad \cdot g_2^{-(r_l^1+\cdots+r_l^{i-1}+r_l^{i+1}+\cdots+r_l^n)f_2^*} \\ &\quad \cdot g_2^{\dot{v}'_{1,l} f_3^* + \dot{v}'_{2,l} f_4^*} \end{aligned} \right\}_{l \in [1, q_n]}$$

$$\begin{aligned} CT_{ID_{\theta i}^*}^{(SF)} = \{ &C_1 = M_\theta^* \cdot e(g_1, g_2)^{\alpha z f_1 f_1^*}, \\ &C_2 = g_1^{z'_1 f_1 + z'_2 f_2 + \chi_1 f_3 + \chi_2 f_4}\}. \end{aligned}$$

where

$$z'_1 = z - \chi_1 \xi_{1,1} - \chi_2 \xi_{2,1},$$

$$z'_2 = z(ID_{\theta 1}^* + \cdots + ID_{\theta n}^*) - \chi_1 \xi_{1,2} - \chi_2 \xi_{2,2},$$

Table 1: Comparison I of IBBE schemes

Schemes	System Parameter Size	Private Key Size	Ciphertext Size	Decryption
[3]	$\lvert\mathbb{G}_1\rvert + (m+1)\lvert\mathbb{G}_2\rvert + \lvert\mathbb{G}_T\rvert$	$\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert + \lvert\mathbb{G}_T\rvert$	$2P$
[8]2	$(m+1)\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$\lvert\mathbb{G}_0\rvert$	$2\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$2P$
[8]3	$4m\lvert\mathbb{G}_0\rvert$	$2\lvert\mathbb{G}_0\rvert$	$4\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$2P$
[25]	$7\lvert\mathbb{G}_0\rvert + 3\lvert\mathbb{Z}_q^*\rvert$	$(\lvert\mathrm{S}\rvert + 2)\lvert\mathbb{G}_0\rvert$	$5\lvert\mathbb{G}_0\rvert + \lvert\mathbb{Z}_q^*\rvert$	$3P$
[33]	$(m+2)\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$3\lvert\mathbb{G}_0\rvert$	$3\lvert\mathbb{G}_0\rvert$	$2P$
[13]	$(2m+3)\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$(\lvert\mathrm{S}\rvert + 4)\lvert\mathbb{G}_0\rvert$	$4\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$4P$
[35]	$(m+4)\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$(\lvert\mathrm{S}\rvert + 1)\lvert\mathbb{G}_0\rvert$	$3\lvert\mathbb{G}_0\rvert$	$2P$
[31]	$m(\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert) + \lvert\mathbb{G}_T\rvert$	$3\lvert\mathrm{S}\rvert\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+\lvert\mathbb{G}_T\rvert$	$2P$
[26]	$\lvert\mathbb{G}_1\rvert + m\lvert\mathbb{G}_2\rvert + \lvert\mathbb{G}_T\rvert$	$\lvert\mathrm{S}\rvert\lvert\mathbb{G}_2\rvert$	$\lvert\mathrm{S}\rvert\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_T\rvert$	$2P$
[9]	$\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{Z}_q^*\rvert$	$\lvert\mathbb{G}_0\rvert$	$\lvert\mathrm{S}\rvert\lvert\mathbb{G}_\mathrm{T}\rvert$	P
[10]	$5\lvert\mathbb{G}_0\rvert$	$\lvert\mathbb{G}_0\rvert$	$3\lvert\mathbb{G}_0\rvert + (\lvert\mathrm{S}\rvert + 1)\lvert\mathbb{Z}_q^*\rvert$	$2P$
[32]	$\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$\lvert\mathbb{G}_0\rvert$	$2\lvert\mathbb{G}_0\rvert + 2\lvert\mathrm{S}\rvert\lvert\mathbb{G}_\mathrm{T}\rvert$	$2P$
[11]	$3\lvert\mathbb{G}_0\rvert$	$2\lvert\mathbb{G}_0\rvert$	$2\lvert\mathbb{G}_0\rvert + 2\lvert\mathrm{S}\rvert\lvert\mathbb{Z}_q^*\rvert$	$2P$
[23]	$24\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$6\lvert\mathbb{G}_0\rvert$	$6\lvert\mathbb{G}_0\rvert + \lvert\mathbb{G}_T\rvert$	$6P$
Our	$8\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$	$4\lvert\mathbb{G}_2\rvert$	$4\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$	$4P$

$$\left\{\begin{array}{l} v'_{1,l} = v_{1,l} + (\alpha + r_l^i ID_{li})\xi_{1,1} - r_l^i \xi_{1,2} \\ v'_{2,l} = v_{2,l} + (\alpha + r_l^i ID_{li})\xi_{2,1} - r_l^i \xi_{2,2} \\ \dot{v}'_{1,l} = \dot{v}_{1,l} + (r_l^1 + \cdots + r_l^{i-1} + r_l^{i+1} + \cdots + r_l^n) \\ \qquad (ID_{l1} + \cdots + ID_{ln})\xi_{1,1} \\ \qquad + r_l^i(ID_{l1} + \cdots + ID_{li-1} + ID_{li+1} + \cdots + ID_{ln})\xi_{1,1} \\ \qquad -(r_l^1 + \cdots + r_l^{i-1} + r_l^{i+1} + \cdots + r_l^n)\xi_{1,2} \\ \dot{v}'_{2,l} = \dot{v}_{2,l} + (r_l^1 + \cdots + r_l^{i-1} + r_l^{i+1} + \cdots + r_l^n) \\ \qquad (ID_{l1} + \cdots + ID_{ln})\xi_{2,1} \\ \qquad + r_l^i(ID_{l1} + \cdots + ID_{li-1} + ID_{li+1} + \cdots + ID_{ln})\xi_{2,1} \\ \qquad -(r_l^1 + \cdots + r_l^{i-1} + r_l^{i+1} + \cdots + r_l^n)\xi_{2,2} \end{array}\right\}_{l\in[1,q_n]}$$

which are all uniformly distributed because $\xi_{1,1}, \xi_{1,2}, \xi_{2,1}, \xi_{2,2}, v_{1,1}, v_{2,1}, \cdots, v_{1,q_n}, v_{2,q_n}, \dot{v}_{1,1}, \dot{v}_{2,1}, \cdots, \dot{v}_{1,q_n}, \dot{v}_{2,q_n}$ are all uniformly chosen from $\mathbb{Z}_q$.

That is to say, the coefficients $z[1, (ID^*_{\beta 1} + \cdots + ID^*_{\beta n})]$ of d_1, d_2 in the C_2 term of the challenge ciphertext is changed to random coefficients $(z'_1, z'_2) \in \mathbb{Z}_q^n$ of f_1, f_2, thus the challenge ciphertext can be seen as a semi-functional encryption of a random message. Furthermore, all coefficients $\{(\dot{v}'_{1,l}, \dot{v}'_{2,l})\}_{l\in[1,q_n]}$ of f_3^*, f_4^* in the $SK^{(SF)}_{ID_{li}}$ are all uniformly distributed because $\{(\dot{v}_{1,l}, \dot{v}_{2,l})\}_{l\in[1,q_n]}$ of d_3^*, d_4^* are all independent random values. Therefore,

$$\{params, \{SK^{(SF)}_{ID_{li}}\}_{l\in[1,q_n]}, CT^{(SF)}_{ID^*_{\theta i}}\}$$

expressed over bases F and F* is properly distributed as

$$\{params, \{SK^{(SF)}_{ID_{li}}\}_{l\in[1,q_n]}, CT^{(R)}_{ID^*_{Ri}}\}$$

in $Game_{Final}$.

In terms of $\mathcal{A}$'s view, both (D,D*) and (F,F*) are identical under the same public system parameters. Hence, the private keys and challenge ciphertext can be depicted in two manners, in $Game_{q_n}$ over bases (D,D*) and in $Game_{Final}$ over bases (F,F*). Therefore, $Game_{q_n}$ and $Game_{Final}$ are statistically indistinguishable. □

Lemma 4. For any adversary $\mathcal{A}$, we have $Adv_{\mathcal{A}}^{Game_{Final}} = 0$.

Proof. In $Game_{Final}$, the value θ selected is independent from the adversary $\mathcal{A}$'s view. Therefore, $Adv_{\mathcal{A}}^{Game_{Final}}(\lambda) = 0$. The challenge ciphertext is a semi-functional encryption of a random message, independent of the two challenge messages and the challenge identity sets chosen by $\mathcal{A}$. Therefore, the proposed scheme is anonymous (weakly attribute-hiding). □

Theorem 1. *The proposed scheme is fully secure and anonymous under the symmetric external Diffie-Hellman assumption. Specifically, if any adversary $\mathcal{A}$ breaks the proposed scheme, there exist the algorithms $B_0, B_1, \cdots, B_{q_n}$ with advantage*

$$Adv_{\mathcal{A}} \leq Adv_{B_0}^{DS1} + \sum_{k=1}^{q_n} Adv_{B_k}^{DS2} + \frac{q_n}{q},$$

whose running time is essentially equal to that of $\mathcal{A}$.

Proof. From Lemma 1-4, we obtain Theorem 1. □

5.3 Efficiency

We compare the proposed scheme with the existing related works [3, 8–11, 13, 23, 25, 26, 31–33, 35] in terms of performance and security. We denote by m and |S| the maximal size of receivers set and that for one encryption, respectively. We also denote by $\lvert\mathbb{G}_X\rvert$ and $\lvert\mathbb{G}_0\rvert$ the length of the group $\mathbb{G}_X$ and the group of symmetric bilinear pairs, where $X \in \{0, 1, 2, T\}$. Let P the pairing computation.

We summarize the comparisons of the fifteen schemes in Tables 1-2. The *System Parameter Size* column, *Private Key Size* column and *Ciphertext Size* column indicates the length of system parameter, private key and ciphertext, respectively. The *Decryption* stands for the

Table 2: Comparison II of IBBE schemes

Schemes	Hard Problem	Security Model	Standard Model	Prime Order Group	Anonymity
[3]	D-GDHE	Selective Security	×	√	×
[8]2	D-BDHE	Fully Secure	√	√	×
[8]3	D-BDHE	Fully Secure	√	√	×
[25]	D-TBDE	Fully Secure	√	√	×
[33]	DLIN	Fully Secure	√	×	×
[13]	GSD	Fully Secure	√	×	×
[35]	DLIN	Fully Secure	√	×	√
[31]	D-BDHE	Fully Secure	√	√	√
[26]	DBDH	Fully Secure	×	√	√
[9]	DBDH	Fully Secure	×	√	√
[10]	DBDH	Fully Secure	×	√	√
[32]	DBDH	Selective Secure	×	√	√
[11]	DBDH	Fully Secure	×	√	√
[23]	DLIN	Fully Secure	√	√	×
Our	SXDH	Fully Secure	√	√	√

number of pairing computation in the algorithm decryption. The *Hard Problem* column specifies the security assumption that the schemes rely on. The *Security Model* column shows the selective security or fully secure (adaptive security) that the schemes achieve. The *Standard Model* column demonstrates whether the scheme is secure in standard model. The *Prime Order Group* column means whether the scheme is secure in the group of prime order. The *Anonymity* column describes whether the scheme achieves anonymity property. The entry √ indicates "satisfy" and × refers to "not satisfy".

From Tables 1-2, we can see that the proposed scheme is the provably secure (fully secure) anonymous IBBE scheme. We note that the computation of the pairing is the most consuming. Although there have been many papers discussing the complexity of pairings and how to speed up the pairing computation, the pairing computation is the operation which by far takes the most running time. In decryption phase, our scheme needs 4 pairing computations and is more efficient than the scheme in [23] that needs 6 pairing computations. Moreover, the proposed scheme satisfies the anonymity. Thus, our scheme outperforms the scheme in [23] in terms of security and computational efficiency in decryption phase. At the same time, although the scheme in [9] needs one pairing computation, the schemes in [3,8,10,11,26,31–33,35] need two pairing computations and the scheme in [25] needs three pairing computations, the schemes in [3, 8, 26, 31, 33, 35] haven't constant-size system parameters, the schemes in [25, 26, 31, 35] haven't constant-size private keys, and the schemes in [10, 11, 32] haven't constant-size ciphertexts. But, the proposed scheme can simultaneously satisfy constant-size system parameters, private keys and ciphertexts.

We assume that $|\mathbb{Z}_q^*| = 256$ bits. Under the level of 256-bit AES security, the bit length of group $|\mathbb{G}_0|$ is 2560 bits, the bit length of group $|\mathbb{G}_1|$ is 640 bits, the bit length of group $|\mathbb{G}_2|$ is 2560 bits, the bit length of group $|\mathbb{G}_T|$ is 15360 bits.

We give the relationship between the system parameter size and the maximal size of the set of receivers in Figure 2, the relationship between the private key size and number of recipients in a single encryption process in Figure 3 and the relationship between the ciphertext size and number of recipients in a single encryption process in Figure 4.

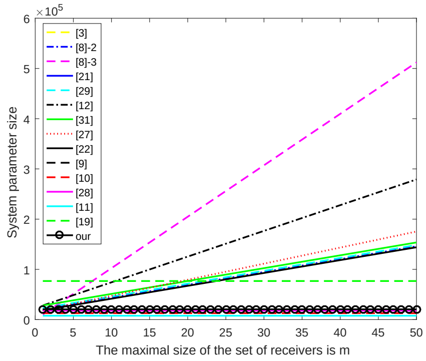

Figure 2: System parameter size versus maximal size of the set of receivers

From Figures 2-4, we find that the system parameter size, the private key size and the ciphertext size in the proposed scheme are constant and smaller than that in scheme [23]; the private key size in schemes [3,8–11,32,33] are constant and smaller than that of the proposed scheme, but the system parameter size increase quickly when the maximal size of receivers set become bigger in schemes [3, 8, 33] and the ciphertext size increase quickly when the number of recipients in a single encryption process become bigger in schemes [9–11, 32]; the ciphertext size in schemes [25, 35] are constant and smaller than the proposed scheme, however the private key size increase quickly when the number of recipients in a single encryption process become bigger in schemes [25,35]; the system parameter size and the private key size are not constant in schemes [26,31]. Therefore, our proposed scheme is fully secure anonymous IBBE scheme with group of prime order in the standard model, which satisfies simultaneously the constant-size of system parameters, private keys and ciphertexts.

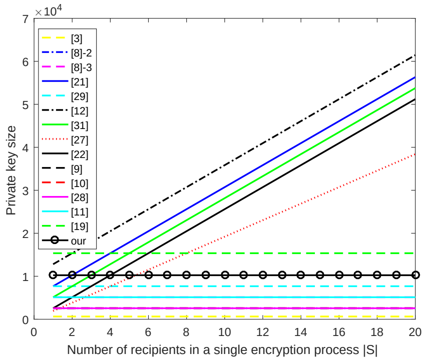

Figure 3: Private key size versus number of recipients in a single encryption process

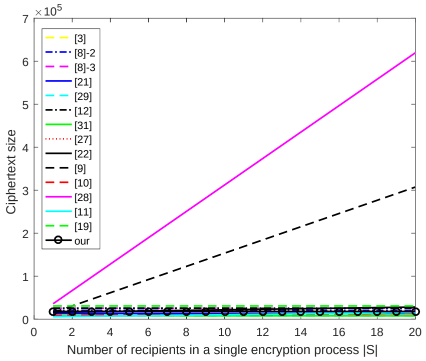

Figure 4: Ciphertext size versus number of recipients in a single encryption process

6 Conclusion

In this paper, we propose a new anonymous IBBE scheme with group of prime order using the asymmetric bilinear pairing. Under the dual system encryption methodology, we showed that the proposed scheme satisfies the fully secure in the standard model. In addition, the proposed scheme has constant size system parameters, private keys and ciphertexts, and achieves the receiver identity anonymity.

Acknowledgments

This work was supported by the Natural Science Foundation of Shaanxi Province (No.2018JM6081) and the Project of Science and Technology of Xi'an City (2017088CG/RC051(CADX002)).

References

[1] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Advances in Cryptology (CRYPTO'05)*, pp. 258–275, 2008.

[2] J. Chen, H.W. Lim, S. Ling, H. Wang, and H. Wee, "Shorter IBE and signatures via asymmetric pairings," in *Proceedings of International Conference on Pairing-Based Cryptography (Pairing'12)*, pp. 122–140, 2012.

[3] C. Delerable, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Advances in Cryptology (ASIACRYPT'07)*, pp. 200–215, 2007.

[4] C. Delerable, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys," in *Proceedings of International Conference on Pairing-Based Cryptography (Pairing'07)*, pp. 39–59, 2007.

[5] Y. Dodis and N. Fazio, "Public key broadcast encryption secure against adaptive chosen ciphertext attacks," in *Proceedings of International Workshop on Theory and Practice in Public Key Cryptography (PKC'03)*, pp. 100–115, 2003.

[6] A. Fiat and M. Naor, "Broadcast encryption," in *Advances in Cryptology (CRYPTO'93)*, pp. 480–491, 1993.

[7] D. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in *Advances in Cryptology (EUROCRYPT'10)*, pp. 44–61, 2010.

[8] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," in *Advances in Cryptology (EUROCRYPT'09)*, pp. 171–188, 2009.

[9] K. He, J. Weng, M. Au, Y. Mao, and R. H. Deng, "Generic anonymous identity-based broadcast encryption with chosen-ciphertext security," in *Proceedings of Australasian Conference on Information Security and Privacy (ACISP'16)*, pp. 207–222, 2016.

[10] K. He, J. Weng, J. N. Liu, J. K. Liu, W. Liu, and R. H. Deng, "Anonymous identity-based broadcast encryption with chosen-ciphertext security," in *Proceedings of ACM on Asia Conference on Computer and Communications Security (ASIACCS'16)*, pp. 247–225, 2016.

[11] K. He, J. Weng, Y. Mao, and H. Yuan, "Anonymous identity-based broadcast encryption technology for smart city information system," *Personal and Ubiquitous Computing*, vol. 4, pp. 1–13, 2017.

[12] M. S. Hwang, C. C. Lee, T. Y. Chang, "Broadcasting cryptosystem in computer networks using geometric properties of lines", *Journal of Information Science and Engineering*, vol. 18, no. 3, pp. 373–379, May 2002.

[13] 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*, vol. 10, no. 3, pp. 679–693, 2015.

[14] A. V. N. Krishna, A. H. Narayana, K. M. Vani, "Window method based cubic spline curve public key cryptography," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 94–102, 2016.

[15] J. Lai, Y. Mu, F. Guo, and R. Chen, "Fully privacy-preserving ID-based broadcast encryption with authorization," *The Computer Journal*, vol. 60, no. 12, pp. 1809–1821, 2017.

[16] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Anonymous identity-based broadcast encryption with revocation for file sharing," in *Proceedings of Australasian Conference on Information Security and Privacy (ACISP'16)*, pp. 223–239, 2016.

[17] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city," *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp. 855–868, 2017.

[18] C. C. Lee, T. Y. Chang, M. S. Hwang, "A simple broadcasting cryptosystem in computer networks using exclusive-OR", *International Journal of Computer Applications in Technology*, vol. 24, no. 3, pp. 180–183, 2005.

[19] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology (EUROCRYPT'10)*, pp. 62–91, 2010.

[20] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in *Procddeings of Theory of Cryptography Conference (TCC'10)*, pp. 455–479, 2010.

[21] B. Libert, K. G. Paterson, and E. A. Quaglia, "Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model," in *Proceedings of International Workshop on Theory and Practice in Public Key Cryptography (PKC'12)*, pp. 206–224, 2012.

[22] L. Liu and Z. Cao, "A note on efficient algorithms for secure outsourcing of bilinear pairings," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 30–36, 2016.

[23] Y. Ming and Y. Wang, "Identity based broadcast encryption with group of prime order," *The International Arab Journal of Information Technology*, vol. 13, no. 5, pp. 531–541, 2016.

[24] T. Okamoto and K Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in *Advances in Cryptology (CRYPTO'10)*, pp. 191–208, 2010.

[25] Y. Ren and D. Gu, "Fully CCA2 secure identity based broadcast encryption without random oracles," *Information Processing Letters*, vol. 109, no. 11, pp. 527–533, 2009.

[26] Y. Ren, Z. Niu, and X. Zhang, "Fully anonymous identity-based broadcast encryption without random oracles," *Internatinal Journal Network Security*, vol. 16, no. 4, pp. 256–264, 2014.

[27] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology (CRYPTO'84)*, pp. 47–53, 1984.

[28] J. Sun, Y. Hu, and L. Zhang, "A key-policy attribute-based broadcast encryption," *The International Arab Journal of Information Technology*, vol. 10, no. 5, pp. 444–452, 2013.

[29] W. Susilo, R. Chen, F. Guo, G. Yang, Y. Mu, and Y. W. Chow, "Recipient revocable identity-based broadcast encryption," in *Proceedings of ACM on Asia Conference on Computer and Communications Security (ASIACCS'16)*, pp. 201–210, 2016.

[30] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology (CRYPTO'09)*, pp. 619–636, 2009.

[31] L. Xie and Y. Ren, "Efficient anonymous identity-based broadcast encryption without random oracles," *International Journal of Digital Crime and Forensics*, vol. 6, no. 2, pp. 40–51, 2014.

[32] P. Xu, J. Li, W. Wang, and H. Jin, "Anonymous identity-based broadcast encryption with constant decryption complexity and strong security," in *Proceeding of ACM on Asia Conference on Computer and Communications Security (ASIACCS'16)*, pp. 223–233, 2016.

[33] L. Zhang, Y. Hu, and Q. Wu, "Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups," *Mathematical and Computer Modelling*, vol. 55, no. 1, pp. 12–18, 2012.

[34] L. Zhang, Z. Wang, and Q. Wu, "Leakage-resilient anonymous identity-based broadcast encryption in the standard model," in *Proceeding of International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP'15)*, pp. 201–210, 2015.

[35] L. Zhang, Q. Wu, and Y. Mu, "Anonymous identity-based broadcast encryption with adaptive security," in *Proceedings of the Symposium on Cyberspace Safety and Security (CSS'13)*, pp. 258–271, 2013.

Yang Ming received the B.S. and M.S. degrees from Xi'an University of Technology in 2002 and 2005 respectively, and the Ph.D. degree in cryptography from Xidian University in 2008. Currently he is a supervisor of postgraduate and professor of Chang'an University. His research interests include cryptography and information security.

Hongping Yuan received the B.S. degrees from Nanyang Institute of Technology in 2014. Currently she is a postgraduate of Chang'an University. His research interests include cryptography and public key encryption.