Identity Based Broadcast Encryption with Group of Prime Order

Yang Ming[1] and Yumin Wang[2]
[1]School of Information Engineering, Chang'an University, China
[2]State Key Lab of Integrated Service Network, Xidian University, China

Abstract: *Identity Based Broadcast Encryption (IBBE) is a cryptographic primitive, which allows a center 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. In this paper, based on bilinear groups, we propose a secure IBBE scheme with a constant-size system parameters, private keys and cipher texts. This construction uses dual pairing vector space technique in prime order groups, which can simulate the cancelling and parameter hiding properties of composite order groups. Furthermore, we show that the proposed scheme utilizes a nested dual system encryption argument to prove full secure (adaptive secure) under the Decisional Linear assumption (DLIN) (static, non q-based) in the standard model. To the best of our knowledge, our scheme is the first provably secure IBBE scheme in the literature to achieve this security level.*

Keywords: *Cryptography, encryption, IBBE, dual pairing vector space, full security, provable security.*

Received January 8, 2014; accepted September 9, 2014

1. Introduction

The concept of Broadcast Encryption (BE) was introduced by Fiat and Naor [13], which can be protecting secure group communication in networks. In a BE scheme, the broadcaster encrypts a message for some subset of users and sends the cipher text over the Internet. Any user in the designated subset can use his private key to decrypt the cipher text. However, nobody outside the subset can recover the message. BE plays a very important role in pay-TV, distribution of copyrighted materials (CD/DVD etc.,), secure audio streaming and internet multicasting, and satellite-based commerce. Since, it was firstly proposed in [13], BE has become a key topic in cryptography and many schemes have been proposed in the literature [5, 10, 11, 16, 21, 30, 38].

Shamir [37] introduced the notion of identity-based cryptography. The main idea of the Identity-Based Encryption (IBE) schemes [1, 2, 3, 4, 17, 37, 39] is that a user can encrypt a message using the recipient's identity (IP address, email address, etc.,) as public key. The direct derivation of public key eliminates the need for certificates and some of the problems associated with them. So, IBE can simplify many applications of public key encryption and is currently an active research area.

Identity Based Broadcast Encryption (IBBE) [9, 12, 16, 32, 36, 38] is a generalization of IBE. In IBBE, a broadcaster typically encrypts a message by combining public identities of receivers in designated subset and system parameters. The well known construction of IBBE was proposed by Delerablée [9]. This scheme achieved constant size cipher text and private keys, but was provably selective-identity secure in the random oracles. Ren and Gu [36] proposed the first IBBE scheme that is full security (adaptive security) in the standard model. The public key and cipher text are constant size and the private key size is linear in terms of the total number of receivers. Gentry and Waters [16] presented the first full secure system with sub linear cipher texts using a sub-algorithm at the encrypt phase, which was secure in the standard model. Although, the schemes in [9, 16, 36] achieved some security properties, but their security relied on the complex assumptions (q-based) which were dependent on the depth of user set and the number of queries made by an attacker.

For IBBE scheme (any cryptographic scheme), the following three aspects should be considered:

- Efficiency: An IBBE scheme is used in practice, its efficiency is a crucial aspect. Since, one of the most prominent applications of IBBE is real-time broadcasting, cipher text size is at the heart of efficiency measures for such scheme, and constructions with constant-size cipher text are desirable. Other important measures of efficiency for IBBE include the system parameter, private key and public key sizes and the computation cost of the encryption and decryption.
- Security: An important security paradigm for IBBE schemes is that of full security (adaptive secure). This paradigm captures the fact that an adversary can choose adaptively the identity he wants to attack in the system, based on its acquired knowledge of the system parameters and previously compromised private keys and cipher texts. Such a definition is

widely accepted as the security notion of IBBE schemes.

- Security Assumption: The q-based assumption was widely used to achieve security in the standard model. But, these assumptions were more complex, which dependent of the number of private keys queries the adversary makes. For IBBE scheme, the weak security assumption (non q-based) was needed in life.

Fully security, constant-size cipher text, system parameter, private key and the weak security assumption, have all been respective achieved for IBBE. Recently, the methodology of dual system encryption [25, 38] has emerged as a useful tool for achieving above all requirements. There works provide efficient systems with short parameters which are proven full secure in the standard model under static assumption (non q-based). In a dual system encryption scheme, keys and cipher text can each take on two forms: Normal and semi-functional. Semi-functional cipher texts and keys are not used in the real system; they are only used in the security proof. Normal keys can decrypt both form of cipher texts and a normal cipher text can be decrypted by normal or semi-functional keys. However, when a semi-functional key is used to decrypt a semi-functional cipher text, decryption will fail. More specifically, the semi-functional components of the key and cipher text will interact to mask the blinding factor by an additional random term. Security is proven by a hybrid argument (a sequence of games), which are shown to be indistinguishable for any adversary. The first game is the real security game (with normal cipher text and private keys). In the next game, the cipher texts are semi-functional, while all the keys are normal. For an adversary that makes q private key queries, games 1 through q follow. In game k, the first k keys are semi-functional while the remaining keys are normal. In game q, all the keys and the challenge cipher text given to the adversary are semi-functional. In the last game, the simulator needs only produce semi- functional objects, which cannot correctly decrypt. This greatly reduces the burden on the simulator and allows us to now proven security directly.

Waters [38] first proposed a BE scheme based on the dual system encryption technique in the composite order bilinear groups. However, the proposed scheme is not based on identity and is also inefficient since its cost of decryption is dependent on depth of user set. Zhang *et al.* [40] present a fully secure IBBE scheme using dual system encryption techniques in the subgroups, which achieved a constant size cipher text and private keys. In addition [8, 26, 40], several other cryptosystems [22, 23, 26, 27, 28, 29] have been constructed in the composite order bilinear groups and proven secure from instances (and close variants) of the general subgroup decision assumption. This works have achieved full security under the static assumption via the convenient features of the composite order bilinear groups, i.e., the presence of orthogonal subgroups of coprime orders. Though composite order bilinear groups have appealing features, it is desirable to obtain the same functionalities and strong guarantees achieved in composite order groups from other assumptions, particularly from the Decisional Linear assumption (DLIN) in prime order bilinear groups. The ability to work with prime order bilinear groups instead of composite order ones offers several advantages. First, we can obtain security under the more standard DLIN. Second, we can achieve much more efficient systems for the same security level. This is because in Composite order groups, security typically relies on the hardness of factoring the group order. This requires the use of large group orders, which result in considerably slower pairing operations. The use of composite order groups can be viewed as an intermediary step in the development of prime order systems whose security relies on the DLIN assumption.

Currently, these have been many previous proposed schemes [6, 15, 18, 19, 28, 33] that were first built in Composite order groups while later analogs were obtained in prime order groups. But these schemes in prime order groups were translated from Composite order groups using a specific-method separatively. Freeman [14] firstly identified that Composite order group has two features: Projecting and canceling (orthogonality). Then, Freeman [14] given a general technique to convert Composite order schemes into prime order schemes relying on either projecting or canceling. Lewko [31] pointed that the techniques of Freeman were insufficient and explores a general methodology for translating composite order pairing-based cryptosystems into the prime order setting using the dual pairing vector space approach [34, 35]. This new techniques were typically applicable for Composite order schemes relying on the canceling property and proven secure from variants of the subgroup decision assumption, and will result in prime order schemes that are proven secure from the DLIN. Lewko and Waters [24, 31] also provided a translation of the IBE, Hierarchical Identity Based Encryption (HIBE) and Attribute-Based Encryption (ABE). Chen and Wee [7] also present efficient identity based encryption using dual system encryption and dual pairing vector spaces techniques. Jia *et al.* [20] proposed an improved IBE scheme and get a full secure anonymous IBE scheme in the prime order setting that has a better message cipher text rate. Chen and Wee [7] present the first full secure IBE scheme from the standard assumptions where the security loss depends only on the system parameter and is independent of the number of the private key queries.

In this paper, we present a new IBBE scheme based on dual pairing vectors space technique in prime order groups, which can simulate the canceling and parameter hiding properties of Composite order settings.

Our scheme achieves constant-size system parameters, private keys and cipher texts. The new scheme is provable security in standard model and also obtains full security. In the security proof, we use dual system encryption technique. Firstly, we change the challenge cipher text to be semi-functional. Secondly, we answer to private key queries are changed to be semi-functional one by one. Finally, we change the challenge cipher text to a semi-functional encryption of a random message. We argue that any polynomial time adversary cannot tell the difference between two adjacent games.

In addition, we show that our scheme is can be implementation in the prime order groups under the decision linear assumption (non q-based).

2. Preliminaries

2.1. Prime Order Bilinear Groups

Let G_1 and G_2 be two cyclic groups of prime order q and g be a generator of G_1. A bilinear map is a map e: $G_1 \times G_1 \rightarrow G_2$ with the properties:

- Bilinearity: For all $u, v \in G_1$ and $a, b \in Z_q$, $e(u^a, v^b) = e(u, v)^{ab}$.
- Non-Degeneracy: $e(g, g) \neq 1$.
- Computability: There exists an efficient algorithm to compute $e(u, v)$ for all $u, v \in G_1$.

2.2. Dual Pairing Vector Space

For our construction, we will use dual pairing vector spaces, a tool introduced by Okamoto and Takashima [34, 35]. For a vector $v = (v_1, v_2, ..., v_n) \in Z_q^n$ and $g \in G_1$, we write g^v to denote a n-tuple of element of G_1. This notation should be interpreted as:

$$g^v = (g^{v_1}, g^{v_2}, \cdots, g^{v_n}) \tag{1}$$

We can also, perform scalar multiplication and vector addition in the exponent. For any $c \in Z_q^*$ and $v, w \in Z_q^n$, we have:

$$(g^v)^c = g^{cv} = (g^{cv_1}, g^{cv_2}, \cdots, g^{cv_n}) \tag{2}$$

$$g^{v+w} = (g^{v_1+w_1}, g^{v_2+w_2}, ..., g^{v_n+w_n}) \tag{3}$$

We define a bilinear map e_n on n-tuples of G_1 by pairing component wise and multiplying the result in G_2:

$$e_n(g^v, g^w) = \prod_{i=1}^{n} e(g^{v_i}, g^{w_i}) = e(g,g)^{v \times w} \tag{4}$$

Where dot product is computed module q.

For a fixed (constant) dimension n, we say two bases $B = (b_1, b_2, ..., b_n)$ and $B^* = (b^*_1, b^*_2, ..., b^*_n)$ of Z_q^n are "dual orthonormal" when: $b_i . b^*_j = 0 (mod\ q)$, whenever $i \neq j$ and $b_i . b^*_i = \psi$ for all i, where ψ is a uniformly random element of Z_q. (This is a slight abuse of the terminology "orthonormal", since ψ is not constrained to be 1.)

For a generator $g \in G_1$, we note that $e_n(g^{b_i}, g^{b^*_j}) = 1$, whenever $i \neq j$, where 1 here denoted the identity element in G_2.

We let $Dual(Z_q^n, \psi)$ denote the set of pairs of dual orthonormal bases of dimension n with dot products $b_i . b^*_i = \psi$. We let $(B, B^*) \xleftarrow{R} Dual(Z_q^n, \psi)$ denote choosing a random pair of bases from this set.

Dual pairing vector spaces provide a workable analog to prime order subgroups present in Composite order groups, since they come equipped with orthonormal subspaces under the pairing e_n. The notion of a subgroup can now be replaced by a subspace in the exponent, particularly a span of a subset of the basis vectors in a pair of dual orthonormal bases.

We use a lemma noted in [31] which roughly states that if one starts by sampling a random pair of dual orthonormal based and then applies a linear change of basis to a subset of the basis vectors (maintaining the orthonormal property), the resulting bases are also, distributed as a random pair, independent of the change of basis that was applied.

More formally, we let (B, B^*) denote a pair of dual orthonormal bases over Z_q^n and let $A \in Z_q^{m \times m}$ bean invertible matrix for $m \leq n$. We let $S_m \subseteq [n]$ be a subset of size m. We then define new dual orthonormal bases (B_A, B^*_A) as follows: Let B_m denote $n \times m$ matrix over Z_q whose columns are the vectors $b_i \in B$ such that, $i \in S_m$. Then, $B_m A$ is also an $n \times m$ matrix. We form B_A by retaining all of the vectors $b_i \in B$ for $i \notin S_m$ and exchanging the b_i for $i \in S_m$ with the columns of $B_m A$. To define B^*_A, we similarly let B^*_m denote the $n \times m$ matrix over Z_q whose columns are the vectors $b^*_i \in B^*$ such that $i \in S_m$. Then, $B^*_m (A^{-1})^T$ is also an $n \times m$ matrix, where $(A^{-1})^T$ denotes the transpose of A^{-1}. We form B^*_A by retaining all of the vectors $b^*_i \in B^*$ for $i \notin S_m$ and exchanging the b_i for $i \in S_m$ with the columns of $B^*_m (A^{-1})^T$.

2.3. Security Assumptions

- Subspace Assumption: Given G_1, G_2, e, q, $B = (b_1, b_2, ..., b_n)$, $B^* = (b^*_1, b^*_2, ..., b^*_n)$, pick randomly $g \in G_1$, η, β, τ_1, τ_2, τ_3, μ_1, μ_2, $\mu_3 \in Z^*_q$ and $U_1 = g^{\mu_1 b_1 + \mu_2 b_{k+1} + \mu_3 b_{2k+1}}$, $U_2 = g^{\mu_1 b_2 + \mu_2 b_{k+2} + \mu_3 b_{2k+2}}$, ..., $U_k = g^{\mu_1 b_k + \mu_2 b_{2k} + \mu_3 b_{3k}}$, $V_1 = g^{\tau_1 \eta b^*_1 + \tau_2 \beta b^*_{k+1}}$, $V_2 = g^{\tau_1 \eta b^*_2 + \tau_2 \beta b^*_{k+2}}$, ..., $V_k = g^{\tau_1 \eta b^*_k + \tau_2 \beta b^*_{2k}}$, $W_1 = g^{\tau_1 \eta b^*_1 + \tau_2 \beta b^*_{k+1} + \tau_3 b^*_{2k+1}}$, $W_2 = g^{\tau_1 \eta b^*_2 + \tau_2 \beta b^*_{k+2} + \tau_3 b^*_{2k+2}}$, ..., $W_k = g^{\tau_1 \eta b^*_k + \tau_2 \beta b^*_{2k} + \tau_3 b^*_{3k}}$.

  Let $D = (g^{b_1}, g^{b_2}, \cdots, g^{b_{2k}}, g^{b_{3k+1}}, \cdots, g^{b_n}, g^{\eta b^*_1}, \cdots, g^{\eta b^*_k}, g^{\beta b^*_{k+1}}, \cdots, g^{\eta b^*_{2k}}, g^{b^*_{2k+1}}, \cdots, g^{b^*_n}, U_1, U_2, \cdots, U_k, \mu_3)$.

  It is hard to distinguish V_1, V_2, ..., V_k and W_1, W_2, ..., W_k. The advantage of an algorithm is defined as:

$$Adv_A = | P[A(D, V_1, V_2, \cdots, V_k) = 1] | - | P[A(D, W_1, W_2, \cdots, W_k) = 1] | \tag{5}$$

- DLIN: Given G_1, G_2, e, q, picks randomly $g, f, h \in G_1$, c_1, c_2, wvG_1, c_1, $c_2 \in Z_q$ and compute $T_1 = g^{c_1+c_2}$, $T_2 = g^{c_1+c_2+w}$ and $D=(g, f, h, f^{c_1}, v^{c_2})$.

  It is hard to distinguish T_1 and T_2. The advantage of an algorithm A is defined as:

$$Adv_A = |P[A(D, T_1)=1]| - |P[A(D, T_2)=1]| \quad (6)$$

  According to [24], if the DLIN assumption holds, then the subspace assumption also holds.

2.4. Identity Based Broadcast Encryption

An IBBE scheme with security parameter λ and maximal size m of the target set is a tuple of algorithm IBBE=(*Setup*, *Extract*, *Encrypt*, *Decrypt*) described as follows:

- *Setup*: Given a security parameter and the maximal size m of the set of receivers for one encryption, the Private Key Generator (PKG) generates the system parameters π and the master key *msk*. The π is made public while *msk* is kept secret.
- *Extract*: Given π, *msk* and a user identity *ID*, this algorithm outputs a user private key k_{ID} and sends it to the corresponding user through a secure channel.
- *Encrypt*: Given π, a message M and a set of identities $c= (ID_1, ID_2, ..., ID_n)$ with $n \leq m$, this algorithm outputs a cipher text C.
- *Decrypt*: Given π, a subset $\Phi=(ID_1, ID_2, ..., ID_n)$ with $n \leq m$, an identity ID_i and the corresponding private key k_{ID_i}, if $ID_i \in \Phi$, this algorithm returns the plaintext M.

2.5. Security Model of IBBE

In order to deal with the security of cryptographic scheme, we need to define the adversarial model that determines the goal and the possible actions of the adversary. To discuss the security of our scheme, the adversary's capability should be as generic as possible, and the capability should capture the real behaviour of an adversary.

Following [36, 40], we give the full security model for IBBE. Both the adversary A and the challenger C are given as input m, the maximal size of a set of the receivers Ω.

- *Setup*: The challenger C runs algorithm Setup to obtain the system parameter π. Then, C gives π to A and keeps master key *msk* secret.

  1. *Phase* 1. A issues a number of private key queries and decryption queries. These queries can be issued adaptively. That is, each query may depend on the answers of previous ones.

     - Private Key Query: on a private key query upon ID_i, C runs algorithm Extract to generate the private key k_{ID_i} associated to ID_i, then sends it to A.
     - Decryption Query: On a decryption query upon (ID_i, Φ, C) with $\Phi \subseteq \Omega$ Φ and $ID_i \in \Phi$, firstly runs algorithm Extract to generate the private key k_{ID_i}. It then runs algorithm Decrypt to decrypt the cipher text C using the k_{ID_i} and sends the resulting the message M to A.
     - Challenge: Once A decides that phase 1 is over, it produces two messages M_0, M_1 and a set $\Phi^* = (ID_1^*, ID_2^*, \cdots, ID_n^*)$ on which it wishes to be challenged. The challenger C picks a random bit $b \in \{0, 1\}$ and sets the challenge cipher text $C^* = Encrypt(\pi, M_b, \Phi^*)$. At last, the challenger C sends C^* to A as its challenge cipher text.

  2. *Phase* 2: A continues issues private key queries and decryption queries as in Phase 1, C answers these queries in the same way as Phase 1 except that A is not allowed to make a private key query upon any $ID_i \in \Phi^*$ and a decryption query upon (C^*, Φ^*).

- *Guess*: Finally, A outputs a guess $b' \in \{0, 1\}$ and wins the game if $b'= b$.

We refer to such an adversary A in the above game an IND-ID-CCA adversary. The advantage of A in winning the game is defined as follows:

$$Adv_A^{IBBE} = |Pr[b = b'] - \frac{1}{2}| \quad (7)$$

Where the probability is taken over the random bits used by the challenger and A.

- ***Definition* 1**: An IBBE scheme is said to be (t, q_d, q_c, ε)-IND-ID-CCA secure, if for any adversary running in time t, making at most q_d private key queries and q_c decryption queries, we have $Adv_A^{IBBE} \leq \varepsilon$.
- ***Definition* 2**: An IBBE scheme is said to be (t, q_d, ε)-secure against chosen plaintext attacks (IND-ID-CPA secure) if it is (t, q_d, 0, ε) IND-ID-CCA secure.

3. Our Construction

Let n=6 and m denote the maximum number of the set of possible users. Our scheme works as follows:

- *Setup*: Given the security parameter λ and a bilinear map e: $G_1 \times G_1 \rightarrow G_2$, the PKG samples random dual orthonormal bases (D, D^*). We let d_1, ..., d_6 denote the elements of D and $d_1^*, \cdots, d_6^*$ denote the elements of D^*. It also randomly chooses a, θ, $\sigma \in Z_q^*$. The master key is $msk = \{g^{\alpha\theta d_1^*}, g^{\theta d_1^*}, g^{\theta d_2^*}, g^{\sigma d_3^*}, g^{\sigma d_4^*}\}$. The public parameters are:

$$\pi = \{G_1, G_2, g, e, q, e(g,g)^{\alpha\theta d_1 \cdot d_1^*}, g^{d_1}, g^{d_2}, g^{d_3}, g^{d_4}\}$$

- *Extract*: Given the identity $ID_i \text{™} \Phi$, where $\Phi = \{ID_1, \cdots, ID_n\}$ for $n \le m$, PKG randomly chooses $r_1^1, r_1^2, \cdots, r_1^n, r_2^1, r_2^2, \cdots, r_2^n \in Z_q^*$ and computes $k_{ID_i} = (k_1, k_2)$ as follows:

$$k_1 = g^{\alpha\theta d_1^* + r_1^i ID_i \theta d_1^* - r_1^i \theta d_2^* + r_2^i ID_i \sigma d_3^* - r_2^i \sigma d_4^*} \tag{8}$$

$$\begin{aligned} k_2 = {} & g^{(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)(ID_1 + ID_2 + \cdots + ID_n)\theta d_1^*} \\ & g^{r_1^i (ID_1 + ID_2 + \cdots + ID_{i-1} + ID_{i+1} + \cdots + ID_n)\theta d_1^*} \\ & g^{-(r_1^1 + r_1^2 + \cdots + r_1^{i-1} + r_1^{i+1} + \cdots + r_1^n)\theta d_2^*} \\ & g^{(r_2^1 + r_2^2 + \cdots + r_2^{i-1} + r_2^{i+1} + \cdots + r_2^n)(ID_1 + ID_2 + \cdots + ID_n)\sigma d_3^*} \\ & g^{r_2^i (ID_1 + ID_2 + \cdots + ID_{i-1} + ID_{i+1} + \cdots + ID_n)\sigma d_3^*} \\ & g^{-(r_2^1 + r_2^2 + \cdots + r_2^{i-1} + r_2^{i+1} + \cdots + r_2^n)\sigma d_4^*} \end{aligned} \tag{9}$$

- *Encrypt*: A broadcaster randomly chooses $s_1, s_2 \in Z_q^*$ and outputs C=(C_1, C_2) :

$$C_1 = M \cdot e(g,g)^{\alpha\theta s_1 d_1 \cdot d_1^*} \tag{10}$$

$$C_2 = g^{s_1 d_1 + s_1 (ID_1 + ID_2 + \cdots + ID_n) d_2 + s_2 d_3 + s_2 (ID_1 + ID_2 + \cdots + ID_n) d_4} \tag{11}$$

- *Decrypt*: Given the cipher text C=(C_1, C_2), any users $ID_i \text{™} \Phi$ uses the private key to compute $M = C_1 / e_n(k_1 k_2, C_2)$.
- *Correctness*: In fact if the cipher text C=(C_1, C_2) is valid, then one can obtain that the following equation holds.

$$\begin{aligned} & e_n(k_1 k_2, C_2) \\ = {} & e\left(\begin{array}{l} g^{\alpha\theta d_1^* + (r_1^1 + r_1^2 + \cdots + r_1^n)(ID_1 + ID_2 + \cdots + ID_n)\theta d_1^*} \cdot g^{-(r_1^1 + r_1^2 + \cdots + r_1^n)\theta d_2^*}, \\ g^{(r_2^1 + r_2^2 + \cdots + r_2^n)(ID_1 + ID_2 + \cdots + ID_n)\sigma d_3^*} \cdot g^{-(r_2^1 + r_2^2 + \cdots + r_2^n)\sigma d_4^*}, \\ g^{s_1 d_1 + s_1 (ID_1 + ID_2 + \cdots + ID_n) d_2 + s_2 d_3 + s_2 (ID_1 + ID_2 + \cdots + ID_n) d_4} \end{array} \right) \\ = {} & e(g,g)^{\alpha\theta s_1 d_1 \cdot d_1^* + (r_1^1 + r_1^2 + \cdots + r_1^n)(ID_1 + ID_2 + \cdots + ID_n) s_1 \theta d_1^* - (r_1^1 + r_1^2 + \cdots + r_1^n)\theta s_1 (ID_1 + ID_2 + \cdots + ID_n) d_2 \cdot d_2^*} \\ & {}^{+(r_2^1 + r_2^2 + \cdots + r_2^n)(ID_1 + ID_2 + \cdots + ID_n) s_2 \sigma d_3 \cdot d_3^* - (r_2^1 + r_2^2 + \cdots + r_2^n)\sigma s_2 (ID_1 + ID_2 + \cdots + ID_n) d_4 \cdot d_4^*} \\ = {} & e(g,g)^{\alpha\theta s_1 d_1 \cdot d_1^* + [(r_1^1 + r_1^2 + \cdots + r_1^n)(ID_1 + ID_2 + \cdots + ID_n) s_1 \theta - (r_1^1 + r_1^2 + \cdots + r_1^n)\theta s_1 (ID_1 + ID_2 + \cdots + ID_n)} \\ & {}^{+(r_2^1 + r_2^2 + \cdots + r_2^n)(ID_1 + ID_2 + \cdots + ID_n) s_2 \sigma - (r_2^1 + r_2^2 + \cdots + r_2^n)\sigma s_2 (ID_1 + ID_2 + \cdots + ID_n)]\psi} \\ = {} & e(g,g)^{\alpha\theta s_1 d_1 \cdot d_1^*} \end{aligned} \tag{12}$$

For proving the security of the proposed scheme, we first define semi-functional keys and semi-functional cipher texts. We note that semi-functional keys and cipher texts are only provided for definitional purpose, and are not part of the IBBE.

- *Semi-Functional Keys*: At first, a normal key (k_1', k_2') is obtained using the algorithm Extract. Then random value t_5, t_6, i_5, i_6 are chosen in Z_q^*. The semi-functional keys are set as follows: $k_1 = k_1' \cdot g^{t_5 d_5^* + t_6 d_6^*}$ and $k_2 = k_2' g^{i_5 d_5^* + i_6 d_6^*}$.
- *Semi-Functional Cipher texts*: At first, a normal cipher text (C_1', C_2') is obtained using the algorithm Encrypt. Then, random value z_5, z_6 are chosen in Z_q^*. The semi-functional cipher texts are set as follows:

$$C_1 = C_1' = M \cdot e(g,g)^{\alpha\theta s_1 d_1 \cdot d_1^*}$$

And

$$C_2 = C_2' \cdot g^{z_5 d_5 + z_6 d_6}$$

4. Security Proof

We prove this using a hybrid argument over a sequence of games. The first game will be the real security game, denoted by $Game_{real}$. The last one will be one in which the adversary has no advantage unconditionally, denoted by $Game_{final}$. We also denote q the number of private keys requested by the adversary. We will show that each game is indistinguishable from the next. We define the games as follows:

$Game_{real}$: This is a real IBBE security game

$Game_i$ for i=0, 1, ..., q: This game is a real IBBE security game with the two exceptions: The challenge cipher text will be a semi-functional cipher text on the challenge set Φ^*, the first i private keys will be semi-functional private keys, the rest of the private keys will be normal. We note that, in $Game_0$, all of the private keys are normal and in $Game_q$, all of the private keys are semi-functional.

$Game_{final}$: This game is the same with $Game_q$, except that the challenge cipher text is a semi-functional encryption of a random element in G_2.

We transition from $Game_{real}$ to $Game_0$, then to $Game_1$, and so on, until we arrive at $Game_q$. We prove that with each transition, the adversary's advantage cannot change by a non-negligible amount. As a last step, we transform to $Game_{final}$, where it is clear that the adversary's advantage is zero.

We will show that these games are indistinguishable in the following lemmas, all using the subspace assumption. Let Adv_A^{real} denote the advantage in the real game, Adv_A^i denote its advantage in $Game_i$ and Adv_A^{final} denote its advantage in $Game_{final}$.

- ***Lemma* 1**: Suppose that there exists a PPT algorithm A such that $Adv_A^{real} - Adv_A^0 = \varepsilon$, then we can build a PPT algorithm B with advantage ε in breaking the subspace assumption with (k, n)=(2, 6).
- ***Proof***: The algorithm B is given $D = (g^{b_1}, g^{b_2}, g^{b_3}, g^{b_4}, g^{\eta b_1^*}, g^{\eta b_2^*}, g^{\beta b_3^*}, g^{\beta b_4^*}, g^{b_5^*}, g^{b_6^*}, U_1, U_2, \mu_3$ and T_1, T_2.

The goal of B is to decide whether T_1 and T_2 are distributed as $g^{\tau_1 \eta b_1^* + \tau_2 \beta b_3^*}, g^{\tau_1 \eta b_2^* + \tau_2 \beta b_4^*}$ or $g^{\tau_1 \eta b_1^* + \tau_2 \beta b_3^* + \tau_3 b_5^*}, g^{\tau_1 \eta b_2^* + \tau_2 \beta b_4^* + \tau_3 b_6^*}$.

- *Setup*: B first chooses a random invertible matrix $A \in Z_q^{2\times 2}$ and defines a dual orthonormal bases $F=(f_1, f_2, f_3, f_4, f_5, f_6)$, $F^*=(f_1^*, f_2^*, f_3^*, f_4^*, f_5^*, f_6^*)$ as follows:

$$f_1=\eta b_1^*, f_2=\eta b_2^*, f_3=\beta b_3^*, f_4=\beta b_4^*, f_5=b_5^*, f_6=b_6^*,$$
$$f_1^*=\eta^{-1}b_1, f_2^*=\eta^{-1}b_2, f_3^*=\beta^{-1}b_3, f_4^*=\beta^{-1}b_4, f_5^*=b_5, f_6^*=b_6$$

  B implicitly sets $D=F_A, D^*=F_A^*$, where A is applied as a change of basis matrix to f_5, f_6 and $(A^{-1})^T$ is applied as a change of basis matrix to f_5^*, f_6^*.

  Since, F, F^* are distributed as a random pair of dual orthonormal bases, then D, D^* are properly distributed and reveal no information on A. For i= 1, ..., 4, $d_i=f_i$, $d^*_i=f^*_i$.

  B randomly chooses a, θ', $\sigma' \in Z_q^*$ and sets $\theta=\theta'\eta$, $\sigma=\sigma'\beta$. B sends the system parameters $\pi=\{G_1, G_2, g, e, q, e(g^{b_1}, g^{\eta b_1^*})^{\alpha\theta'}, g^{\eta b_1^*}, g^{\eta b_2^*}, g^{\beta b_3^*}, g^{\beta b_4^*}\}$ to A.

- *Query* 1: The adversary A issues a private key query on the identity $ID_i \in \Phi$, where $\Phi=\{ID_1, ID_2, ..., ID_n\}$, B first computes $msk=\{g^{\alpha b_1\theta}, g^{b_1\theta}, g^{b_2\theta}, g^{b_3\sigma'}, g^{b_4\sigma'}\}$ and runs the algorithm Extract to respond to all of A's queries.
- *Challenge*: The adversary A outputs two challenge message M_0 and M_1, and a challenge set $\Phi^*=\{ID^*_1, ID^*_2, ..., ID^*_n\}$. Then, B chooses a random bit $b \in \{0, 1\}$ and sets the cipher text $C=(C_1, C_2)$ as follows:

$$C_1=M_b \cdot e(T_1, g^{b_1})^{\alpha\theta'} \text{ and } C_2=T_1 \cdot (T_2)^{ID_1^*+ID_2^*+\cdots+ID_n^*}.$$

- *Query* 2: The adversary A continues to issue a private key query on ID_i with the constraint that $ID_i \notin \Phi^*$.
- *Guess*: Finally, the adversary A outputs a guess $b \in \{0, 1\}$ and wins the game if $b=b'$.

  Let $\tau_1=s_1$, $\tau_2=s_2$. If $T_1=g^{\tau_1\eta b_1^*+\tau_2\beta b_3^*}$ and $T_2=g^{\tau_1\eta b_2^*+\tau_2\beta b_4^*}$, then $C=(C_1, C_2)$ is a properly distributed normal cipher text. In this case, B has properly simulated $Game_{real}$.

  If $T_1=g^{\tau_1\eta b_1^*+\tau_2\beta b_3^*+\tau_3 b_5^*}$ and $T_2=g^{\tau_1\eta b_2^*+\tau_2\beta b_4^*+\tau_3 b_6^*}$, then, $C=(C_1, C_2)$ is a properly distributed semi-functional cipher text.

  The coefficients in the basis f_5, f_6 form the vector $(\tau_3, (ID_1^*+ID_2^*+\cdots+ID_n^*)\tau_3)$. The coefficients in the basis d_5, d_6 can be computed by multiplying the matrix A^{-1} with the transpose of this vector, i.e., $\tau_3 A^{-1}(1, ID_1^*+ID_2^*+\cdots+ID_n^*)^T$. Since, the matrix A is random, these coefficients are uniformly random. Therefore, in this case, B has properly simulated $Game_0$.

  Hence, B can use A's guess to break subspace assumption with advantage ε.

- ***Lemma* 2**: Suppose that, there exists an algorithm A that makes at most q private key queries and such that $Adv_A^{k-1}-Adv_A^k=\varepsilon$ for $1\le k\le q$. Then, we can build an algorithm B with advantage ε in breaking subspace assumption with (k, n)= (2, 6).
- ***Proof***: The algorithm B is given $D=(g^{b_1}, g^{b_2}, g^{b_3}, g^{b_4}, g^{\eta b_1^*}, g^{\eta b_2^*}, g^{\beta b_3^*}, g^{\beta b_4^*}, g^{b_5^*}, g^{b_6^*}, U_1, U_2, \mu_3)$ and T_1, T_2.

  The goal of B is to decide whether T_1, T_2 are distributed as $g^{\tau_1\eta b_1^*+\tau_2\beta b_3^*}, g^{\tau_1\eta b_2^*+\tau_2\beta b_4^*}$ or as $g^{\tau_1\eta b_1^*+\tau_2\beta b_3^*+\tau_3 b_5^*}, g^{\tau_1\eta b_2^*+\tau_2\beta b_4^*+\tau_3 b_6^*}$.

- *Setup*: B first chooses a random invertible matrix $A \text{ ™} Z_q^{2\times 2}$ and implicitly defines $D=B_A$ and $D^*=B^*_A$, where the change of basis matrix A is applied to b_5, b_6 and the change of basis matrix $(A^{-1})^T$ is applied to b^*_5, b^*_6. The first four basis vectors are unchanged:

$$d_1=b_1, d_2=b_2, d_3=b_3, d_4=b_4, d_1^*=b_1^*, d_2^*=b_2^*, d_3^*=b_3^*, d_4^*=b_4^*$$

  B randomly chooses $a \in Z_q^*$ and sets $\theta=\eta$, $\sigma=\beta$. B sends the system parameters $\pi=\{G_1, G_2, g, e, q, e(g^{b_1}, g^{\eta b_1^*})^{\alpha}, g^{b_1}, g^{b_2}, g^{b_3}, g^{b_4}\}$ to A.

- *Query* 1: The adversary A issues a private key query on the identity $ID_i \in \Phi$, where $\Phi=\{ID_1, ID_2, ..., ID_n\}$. B answers as follows:

  1. $i<k$, B firstly computes the master key $msk=\{g^{\alpha\eta b_1^*}, g^{\eta b_1^*}, g^{\eta b_2^*}, g^{\beta b_3^*}, g^{\beta b_4^*}\}$ and runs algorithm Extract to produce the normal private keys. Since, B knows $g^{b_5^*}, g^{b_6^*}$ and can create random linear combinations of $g^{d_5^*}$ and $g^{d_6^*}$ in the exponent by taking random combinations of b^*_5 and b^*_6, it can easily produce the semi-functional private keys.
  2. $i>k$, B knows the master key and runs algorithm Extract to produce the normal private keys.
  3. $i=k$, B randomly chooses $r_1^1, r_1^2, \cdots, r_1^{i-1}, r_1^{i+1}, \cdots, r_1^n, r_2^1, r_2^2, \cdots, r_2^{i-1}, r_2^{i+1}, \cdots, r_2^n \in Z_q^*$ and implicitly sets $r_1^i=\tau_1, r_2^i=\tau_2$ and computes $k_{ID_i}=(k_1, k_2)$ as follows:

$$k_1=(g^{\eta b_1^*})^{\alpha} T_1^{ID_i} (T_2)^{-1} \quad (13)$$

$$k_2=(g^{\eta b_1^*})^{(r_1^1+r_1^2+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)(ID_1+ID_2+\cdots+ID_n)} \cdot (g^{\eta b_2^*})^{-(r_1^1+r_1^2+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)} \cdot (g^{\beta b_3^*})^{(r_2^1+r_2^2+\cdots+r_2^{i-1}+r_2^{i+1}+\cdots+r_2^n)(ID_1+ID_2+\cdots+ID_n)} \cdot (g^{\beta b_4^*})^{-(r_2^1+r_2^2+\cdots+r_2^{i-1}+r_2^{i+1}+\cdots+r_2^n)} \cdot T_1^{(ID_1+ID_2+\cdots+ID_{i-1}+ID_{i+1}+\cdots+ID_n)} \quad (14)$$

  If $T_1=g^{\tau_1\eta b_1^*+\tau_2\beta b_3^*}$ and $T_2=g^{\tau_1\eta b_2^*+\tau_2\beta b_4^*}$, then this is a properly distributed normal key.

If $T_1 = g^{\tau_1\eta b_1^* + \tau_2\beta b_3^* + \tau_3 b_5^*}$ and $T_2 = g^{\tau_1\eta b_2^* + \tau_2\beta b_4^* + \tau_3 b_6^*}$, then this a semi-functional key.

- *Challenge*: The adversary A outputs two challenge message M_0 and M_1, and a challenge set $\Phi^*=\{ID^*_1, ID^*_2, ..., ID^*_n\}$. Then, B chooses a random bit b™{0, 1} and computes the semi-functional cipher text of M_b as follows:

$$C_1=M_b \cdot e(g^{\eta b_1^*}, U_1)^{\alpha} \text{ and } C_2=U_1 \cdot (U_2)^{ID_1^*+ID_2^*+\cdots+ID_n^*}$$

This implicitly set $s_1=\mu_1$, $s_2=\mu_2$. Using the change of basis matrix A, we can obtain the coefficients in the basis d_5, d_6 as $\mu_3 A^{-1}(1, ID_1, ID_2, ..., ID_n)$.

- *Query* 2: The adversary A continues to issue a private key query on ID_i with the constraint that $ID_i \notin \Phi^*$.
- *Guess*: Finally, the adversary A outputs a guess $b' \in \{0, 1\}$ and wins the game if $b=b'$.

Therefore, B has properly simulated either $Game_{k-1}$ or $Game_k$ for A, depending on the distribution of T_1, T_2. It can leverage A's difference in advantage between these games to obtain a non-negligible advantage against the subspace assumption.

It is easy to understand the security proof, we defines an additional game $Game^*_q$. This is exactly like $Game_q$, except C_2 term of the challenge cipher text, the coefficient of k_2 is changed from being s_1 $(ID^*_1+ID^*_2+ ...+ID^*_n)$ to a fresh random value in Z_q^*. We denote the advantage of an algorithm A in this game by Adv_A^{q*}.

- ***Lemma* 3**: Suppose that there exists an algorithm A that makes at most q private key queries and such that $Adv_A^{q} - Adv_A^{q^*} = \varepsilon$. Then, we can build an algorithm B with advantage ε in breaking subspace assumption with $(k, n)= (1, 6)$.
- ***Proof***: The algorithm B is given

$$D=(g^{b_1}, g^{b_2}, g^{b_4}, g^{b_5}, g^{b_6}, g^{\eta b_1^*}, g^{\beta b_2^*}, g^{b_3^*}, g^{b_4^*}, g^{b_5^*}, g^{b_6^*},$$

$$U_1=g^{\mu_1 b_1+\mu_2 b_2+\mu_3 b_3}, \mu_3) \text{ and } T_1.$$

The goal of B is to decide whether T_1 are distributed as $g^{\tau_1\eta b_1^* + \tau_2\beta b_2^*}$ or $g^{\tau_1\eta b_1^* + \tau_2\beta b_2^* + \tau_3 b_3^*}$.

- *Setup*: B first chooses a random invertible matrix $A \in Z_q^{2\times 2}$ and implicitly defines $D=B_A$ and $D^*=B^*_A$ as follows:

$$d_1=b_6, d_2=b_3, d_3=b_5, d_4=b_4, d_5=b_2, d_6=b_1,$$

$$d_1^*=b_6, d_2^*=b_3, d_3^*=b_5, d_4^*=b_4, d_5^*=b_2, d_6^*=b_1.$$

B randomly chooses θ, σ, $a \in Z_q^*$ and sends the system parameters $\pi=\{G_1, G_2, g, e, q, e(g^{b_6}, g^{b_6^*})^{\alpha\theta}, g^{b_6}, g^{b_3^*}, g^{b_5^*}, g^{b_4^*}\}$ to A.

- *Query* 1: The adversary A issues a private key query on the identity $ID_i \notin \Phi$, where $\Phi=\{ID_1, ID_2, ..., ID_n\}$. B randomly chooses random values $r_1^{i'}, t'_5, t'_6, t'_5, t'_6, r_1^1, r_1^2, \cdots, r_1^{i-1}, r_1^{i+1}, \cdots, r_1^n, r_2^1, r_2^2, \cdots, r_2^n \in Z_q^*$ and computes as follows:

$$k_1=(U_1)^{-\theta r_1^{i'}} (g^{b_6})^{(\alpha+\mu_3 r_1^i ID_i)\theta} (g^{b_5})^{r_2^i ID_i \sigma} (g^{b_4})^{-r_2^i \sigma} (g^{b_2})^{t'_5} (g^{b_1})^{t'_6} \quad (15)$$

$$\begin{aligned} k_2 = & (g^{b_6})^{(r_1^1+r_1^2+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)(ID_1+ID_2+\cdots+ID_n)\theta} \cdot \\ & (g^{b_6})^{\mu_3 r_1^{i'}(ID_1+ID_2+\cdots+ID_{i-1}+ID_{i+1}+\cdots+ID_n)\theta} \cdot \\ & (U_1)^{-(r_1^1+r_1^2+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)\theta/\mu_3} \cdot \\ & (g^{b_5})^{(r_2^1+r_2^2+\cdots+r_2^{i-1}+r_2^{i+1}+\cdots+r_2^n)(ID_1+ID_2+\cdots+ID_n)\sigma} \cdot \\ & (g^{b_5})^{r_2^i (ID_1+ID_2+\cdots+ID_{i-1}+ID_{i+1}+\cdots+ID_n)\sigma} \cdot \\ & (g^{b_4})^{-(r_2^1+r_2^2+\cdots+r_2^{i-1}+r_2^{i+1}+\cdots+r_2^n)\sigma} (g^{b_2})^{t'_5} (g^{b_1})^{t'_6} \end{aligned} \quad (16)$$

- *Challenge*: The adversary A outputs two challenge message M_0 and M_1, and a challenge set $\Phi^*=\{ID_1^*, ID_2^*, \cdots, ID_n^*\}$. Then, B chooses a random bit $b \in \{0, 1\}$, s_1, $s_2 \in Z_q^*$ and sets the semi-functional cipher text of M_b as follows:

$$C_1= M_b \cdot e(g, g)^{\alpha\theta s_1} \quad (17)$$

$$C_2=(g^{b_6^*})^{s_1} (g^{b_3^*})^{s_1(ID_1^*+ID_2^*+\cdots+ID_n^*)} (g^{b_5^*})^{s_2} (g^{b_4^*})^{s_2(ID_1^*+ID_2^*+\cdots+ID_n^*)} T_1 \quad (18)$$

- *Query* 2: The adversary A continues to issue a private key query on ID_i with the constraint that $ID_i \in \Phi^*$.
- *Guess*: Finally, the adversary A outputs a guess $b' \in \{0, 1\}$ and wins the game if $b=b'$.

If $T_1= g^{\tau_1\eta b_1^* + \tau_2\beta b_2^*} = g^{\tau_1\eta d_6 + \tau_2\beta d_5}$, then, the exponent vector of T_1 is random linear combination of d_5 and d_6, making this a well-distributed semi-functional cipher text in $Game_q$.

If $T_1 = g^{\tau_1\eta b_1^* + \tau_2\beta b_2^* + \tau_3 b_3^*} = g^{\tau_1\eta d_6 + \tau_2\beta d_5 + \tau_3 d_2}$, then the τ_3 randomizes the coefficient of d_2, making this a well-distributed semi-functional cipher text in $Game^*_q$.

Hence, B can use A's guess to break the subspace assumption with advantage ε.

- ***Lemma* 4**: Suppose that there exists an algorithm A that makes at most q private key queries and such that $Adv_A^{q^*} - Adv_A^{final} = \varepsilon$. Then, we can build an algorithm B with advantage ε in breaking subspace assumption with $(k, n)=(1, 6)$.
- ***Proof***: The algorithm B is given

$$D=(g^{b_1}, g^{b_2}, g^{b_4}, g^{\eta b_1^*}, g^{\beta b_2^*}, g^{b_3^*}, g^{b_4^*}, g^{b_5^*}, g^{b_6^*}, U_1=g^{\mu_1 b_{11}+\mu_2 b_{22}+\mu_3 b_{33}}, \mu_3) \text{ and } T_1.$$

The goal of B is to decide whether T_1 are distributed as $g^{\tau_1\eta b_1^* + \tau_2\beta b_2^*}$ or $g^{\tau_1\eta b_1^* + \tau_2\beta b_2^* + \tau_3 b_3^*}$.

- *Setup*: B first chooses a random invertible matrix $A \in Z_q^{2\times 2}$ and implicitly defines $D=B_A$ and $D^*=B^*_A$ as follows:

$$d_1=b_3^*, d_2=b_4^*, d_3=b_5^*, d_4=b_6^*, d_5=b_1^*, d_6=b_2^*,$$
$$d_1^*=b_3, d_2^*=b_4, d_3^*=b_5, d_4^*=b_6, d_5^*=b_1, d_6^*=b_2$$

B randomly chooses a', θ', $\sigma \in Z_q^*$ and implicitly sets $a=a'\mu_3$ and sends the system parameters $\pi=\{G_1,G_2,g,e,q,e(g^{b_4},g^{b_4^*})^{\alpha'\mu_3\theta},g^{b_3^*},g^{b_4^*},g^{b_5^*},g^{b_6^*}\}$ to A.

- *Query* 1: The adversary A issues a private key query on the identity $ID_i \notin \Phi^*$, where $\Phi=\{ID_1, ID_2, ..., ID_n\}$. B randomly chooses random values $r_1^{i'},t_5',t_6',t_5',t_6',r_1^1,r_1^2,\cdots,r_1^{i-1},r_1^{i+1},\cdots,r_1^n,r_2^1,r_2^2,\cdots,r_2^n \in Z_q^*$ and computes as follows:

$$k_1=(U_1)^{(\alpha'+r_1^{i'}ID_i)\theta}(g^{b_4})^{-r_1^{i'}\mu_3\theta}(g^{b_5})^{r_2^{i}ID_i\sigma}(g^{b_6})^{-r_2^{i}\sigma}(g^{b_1})^{t_5'}(g^{b_2})^{t_6'} \quad (19)$$

$$\begin{aligned} k_2=&(U_1)^{(r_1^1+r_1^2+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)(ID_1+ID_2+\cdots+ID_n)\theta/\mu_3}\cdot\\ &(U_1)^{\mu_3 r_1^{i'}(ID_1+ID_2+\cdots+ID_{i-1}+ID_{i+1}+\cdots+ID_n)\theta}\cdot\\ &(g^{b_4})^{-(r_1^1+r_1^2+\cdots+r_1^{i-1}+r_1^{i+1}+\cdots+r_1^n)\theta}\cdot\\ &(g^{b_5})^{(r_2^1+r_2^2+\cdots+r_2^{i-1}+r_2^{i+1}+\cdots+r_2^n)(ID_1+ID_2+\cdots+ID_n)\sigma}\cdot\\ &(g^{b_5})^{r_2^i(ID_1+ID_2+\cdots+ID_{i-1}+ID_{i+1}+\cdots+ID_n)\sigma}\cdot\\ &(g^{b_6})^{-(r_2^1+r_2^2+\cdots+r_2^{i-1}+r_2^{i+1}+\cdots+r_2^n)\sigma}\cdot(g^{b_1})^{t_5'}\cdot(g^{b_2})^{t_6'} \end{aligned} \quad (20)$$

- *Challenge*: The adversary A outputs two challenge message M_0 and M_1, and a challenge set $\Phi^*=\{ID_1^*,ID_2^*,\cdots,ID_n^*\}$. Then, B chooses a random bit $b \in \{0, 1\}$, $s_1,s_2,\omega \in Z_q^*$ and sets the semi-functional cipher text of M_b as follows:

$$C_1=M_b\cdot e(g^{b_4},g^{b_4^*})^{\alpha'\mu_3\theta s_1} \quad (21)$$

$$C_2=(g^{b_3^*})^{s_1}\cdot(g^{b_4^*})^{\omega}\cdot(g^{b_5^*})^{s_2}\cdot(g^{b_6^*})^{s_2(ID_1^*+ID_2^*+\cdots+ID_n^*)}\cdot T_1 \quad (22)$$

- *Query* 2: The adversary A continues to issue a private key query on ID_i with the constraint that $ID_i \notin \Phi^*$.
- *Guess*: Finally, the adversary A outputs a guess $b' \in \{0, 1\}$ and wins the game if $b=b'$.

If $T_1=g^{\tau_1\eta b_1^*+\tau_2\beta b_2^*}=g^{\tau_1\eta d_5+\tau_2\beta d_6}$, then the exponent vector of T_1 is random linear combination of d_5 and d_6, making this a well-distributed semi-functional cipher text in $Game_q^*$.

If $T_1=g^{\tau_1\eta b_1^*+\tau_2\beta b_2^*+\tau_3 b_3^*}=g^{\tau_1\eta d_5+\tau_2\beta d_6+\tau_3 d_1}$, then the τ_3 randomizes the coefficient of k_1, yielding a cipher text distributed as in $Game_q^{final}$ (Since, the distribution of C_2 is independent of s_1, which makes C_1 a random group element in G_2).

Hence, B can use A's guess to break the subspace assumption with advantage ε.

- ***Theorem* 1**. If the subspace assumption holds, then our proposed IBBE scheme is IND-ID-CPA secure.

- ***Proof***: If the subspace assumption holds, by the sequence of games and Lemmas 1, 2, 3, 4, the adversary's advantage in the real game must be negligible. Hence, our scheme is IND-ID-CPA secure.

5. Efficiency

We compare the efficiency and security of our scheme with the other six schemes in the literature [9, 16, 36, 40]. We denote by m and $|\Phi|$ the maximal size of the set of receivers and that for one encryption respectively.

We summarize the comparisons of the seven schemes in Table 1. The parameter size column, private key size column and cipher text size column indicates the length of system parameter, private key and cipher text, respectively. The hard problem column specifies the security assumption that the schemes rely on. The security model column shows the selective security or full 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 prime order group.

Table 1. Comparisons of seven IBBE schemes.

Schemes	System Parameters Size	Private Key Size	Ciphertext Size	Hard Problem	Security Model	Standard Model	Prime Order Group
[9]	O(m)	O(1)	O(1)	D-GDHE	Selective Security	No	Yes
[36]	O(1)	O(|Φ|)	O(1)	D-TBDHE	Full security	Yes	Yes
[16]1	O(m)	O(|Φ|)	O(1)	D-BDHE	Selective Security	Yes	Yes
[16]2	O(m)	O(1)	O(1)	D-BDHE	Selective Security	Yes	Yes
[16]3	O(m)	O(1)	Sublinear of |Φ|	D-BDHE	Full Security	Yes	Yes
[40]	O(m)	O(1)	O(1)	SD	Full Security	Yes	No
Our	O(1)	O(1)	O(1)	DLIN	Full Security	Yes	Yes

From Table 1, we know that our proposed scheme achieves constant-size system parameters, private keys and cipher text. Furthermore, the security of our scheme is reduced to decision linear assumption. This assumption is more natural than those in the other existing schemes.

6. Conclusions

In this paper, we have given a new IBBE scheme, which can be reduce to the decision linear assumption. The new construction utilizes the dual pairing vectors space technique and implements in prime order groups. The proposed scheme has short system parameters, private keys and cipher texts. Our scheme achieves full security in the standard model.

Acknowledgments

This work was supposed by the National Natural Science Foundation of China (Grant No. 61202438),

the China Postdoctoral Science Foundation (Grant No. 2011M501427) and the Project of Technology Transfer Promoting Engineering of Xi'an City (Grant No. CXY1437(10)).

References

[1] Boneh D. and Boyen X., "Efficient Selective-ID Secure Identity Based Encryption without Random Oracles," available at: http://crypto.stanford.edu/~dabo/papers/bbibe.pdf , last visited 2004.

[2] Boneh D. and Boyen X., "Secure Identity Based Encryption without Random Oracles," *in Proceedings of the 24th Annual International Cryptology Conference*, California, USA, pp. 443-459, 2004.

[3] Boneh D. and Franklin M., "Identity Based Encryption from the Weil Pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586-615, 2003.

[4] Boneh D., Boyen X., and Goh E., "Hierarchical Identity Based Encryption with Constant Size Cipher Text," *in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, Denmark, pp. 440- 456, 2005.

[5] Boneh D., Gentry C., and Waters B., "Collusion Resistant Broadcast Encryption with Short Cipher Texts and Private Keys," available at: https://eprint.iacr.org/2005/018.pdf, last visited 2005.

[6] Boneh D., Sahai A., and Waters B., "Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys," *in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Russia, pp. 573-592, 2006.

[7] Chen J. and Wee H., "Fully, (Almost) Tightly Secure IBE and Dual System Groups," *in Proceedings of the 33rd Annual Cryptology Conference*, Santa Barbara, USA, pp. 435-460, 2013.

[8] Chen J., Lim H., Ling S., Wang H., and Wee H., "Shorter IBE and Signatures via Asymmetric Pairings," *in Proceedings of the 5th International Conference on Pairing-Based Cryptography-Pairing 2012*, Cologne, Germany, pp. 122-140, 2012.

[9] Delerable C., "Identity-Based Broadcast Encryption with Constant Size Cipher texts and Private Keys," *in Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security*, Kuching, Malaysia, pp. 200-215, 2007.

[10] Delerable C., Paillier P., and Pointcheval D., "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," *in Proceedings of the 1st International Conference on Pairing-Based Cryptography-Pairing*, Tokyo, Japan, pp. 39-59, 2007.

[11] Dois Y. and Fazio N., "Public Key Broadcast Encryption Secure against Adaptive Chosen Ciphertext Attacks," *in Proceedings of the 6th International Workshop on Practice and Theory in Public Key Cryptography-PKC*, Miami, USA, pp. 100-115, 2003.

[12] Du X., Wang Y., Ge J., and Wang Y., "An ID-Based Broadcast Encryption Scheme for Key Distribution," *IEEE Transactions on Broadcasting*, vol. 51, no. 2, pp. 264-266, 2005.

[13] Fiat A. and Naor M., "Broadcast Encryption," available at: http://courses.cs.vt.edu/ cs6204/ Privacy-Security/Papers/Crypto/ Broadcast-Encryption.pdf, last visited 1993.

[14] Freeman D., "Converting Pairing-Based Cryptosystems from Composite-Order Groups to Prime-Order Groups," *in Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques*, French Riviera, pp. 44-61, 2010.

[15] Garg S., Kumarasubramanian A., Sahai A., and Waters B., "Building Efficient Fully Collusion Resilient Traitor Tracing and Revocation Schemes," *in Proceedings of the 17th ACM Conference on Computer and Communications Security*, Chicago, USA, pp. 121-130, 2010.

[16] Gentry C. and Waters B., "Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts)," *in Proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cologne, Germany,, pp. 171-188, 2009.

[17] Gentry C., "Practical Identity-Based Encryption without Random Oracles," *in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, St. Petersburg, Russia, pp. 445-464, 2006.

[18] Groth J., Ostrovsky R., and Sahai A., "Non-Interactive Zaps and New Techniques for NIZK," *in Proceedings of the 26th Annual International Cryptology Conference*, Crete, Greece, pp. 97-111, 2006.

[19] Groth J., Ostrovsky R., and Sahai A., "Perfect Non-Interactive Zero Knowledge for NP," *in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, St. Petersburg, Russia, pp. 339-358, 2006.

[20] Jia D., Li B., Liu Y., and Mei Q., "Improving the Message-Ciphertext Rate of Lewko's Fully Secure IBE Scheme," available at: https://eprint.iacr.org/2013/159.pdf, last visited 2013.

[21] Jin S., Yupu H., and Leyou Z., "A Key-Policy Attribute-Based Broadcast Encryption," *The International Arab Journal of Information Technology*, vol. 10, no. 5, pp. 444-452, 2013.

[22] Lai J., Deng R. H., and Li Y., "Fully Secure Cipertext-Policy Hiding CPABE," *in Proceedings of the 7th International Conference on Information Security Practice and Experience*, Verbania-Intra, Italy, pp. 24-39, 2011.

[23] Lewko A. and Waters B., "Decentralizing Attribute-Based Encryption," *in Proceedings of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, Tallinn, Estonia, pp. 568-588, 2011.

[24] Lewko A. and Waters B., "New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques," available at: https://eprint.iacr.org/2012/326.pdf, last visited 2012.

[25] Lewko A. and Waters B., "New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts," available at: https://eprint.iacr.org/2009/482.pdf, last visited 2009..

[26] Lewko A. and Waters B., "New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts," *in Proceedings of the 7th Theory of Cryptography Conference-TCC 2010*, Zurich, Switzerland, pp. 455-479, 2010.

[27] Lewko A. and Waters B., "Unbounded HIBE and Attribute-Based Encryption," *in Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Tallinn, Estonia, pp. 547-567, 2011.

[28] Lewko A., Okamoto T., Sahai A., Takashima K., and Waters B., "Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption," available at: https://eprint.iacr.org/2010/110.pdf, last visited 2010.

[29] Lewko A., Rouselakis Y., and Waters B., "Achieving Leakage Resilience through Dual System Encryption," *in Proceedings of the 8th Theory of Cryptography Conference-TCC 2011*, Providence, USA, pp. 70-88, 2011.

[30] Lewko A., Sahai A., and Waters B., "Revocation Systems with very Small Private Keys," *in Proceedings of the 31st IEEE Symposium on Security and Privacy-ISSP*, California, USA, pp. 273-285, 2010.

[31] Lewko A., "Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting," *in Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cambridge, UK, pp. 318-335, 2012.

[32] Mu Y., Susilo W., Lin Y., and Ruan C., "Identity Based Authenticated Broadcast Encryption and Distributed Authenticated Encryption," *in Proceedings of the 9th Asian Computing Science Conference-ASIAN 2004*, Chiang Mai, Thailand, pp. 169-181, 2004.

[33] Okamoto T. and Takashima K., "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption," *in Proceedings of the 30th Annual Cryptology Conference*, Santa Barbara, USA, pp. 191-208, 2010.

[34] Okamoto T. and Takashima K., "Hierarchical Predicate Encryption for Inner Products," *in Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security*, Tokyo, pp. 214-231, 2009.

[35] Okamoto T. and Takashima K., "Homomorphic Encryption and Signatures from Vector Decomposition," *in Proceedings of the 2nd International Conference on Pairing-based Cryptography- Pairing 2008*, Egham, UK, pp. 57-74, 2008.

[36] Ren Y. and Gu D., "Fully CCA2 Secure Identity Based Broadcast Encryption without Random Oracles," *Information Processing Letter*s, vol. 109, no. 11, pp. 527-533, 2009.

[37] Shamir A., "Identity-Based Cryptosystems and Signature Schemes," *Advances in Cryptology-CRYPTO 1984*, Santa Barbara, California, USA, pp. 47-53, 1985.

[38] Waters B., "Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions," *Advances in Cryptology-CRYPTO 2009*, Santa Barbara, USA, pp. 619-636, 2009.

[39] Waters B., "Efficient Identity Based Encryption without Random Oracles," *in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, pp. 114-127, 2005.

[40] Zhang L., Hu Y., and Wu Q., "Adaptively Secure Identity Based Broadcast Encryption with Constant Size Private Keys and Cipher texts from the Subgroups," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 12-18, 2012.

Yang Ming received the BS and MS degrees in mathematics 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 associate professor of Chang'an University. He is a member of Chinese Institute of Cryptography. His research interests include cryptography, network security and cloud computing security.

Yuming Wang received the BS degree from Department of Telecommunication Engineering, Xidian University in 1959. In 1979-1981, he was a visiting scholar in Department of Electronic Engineering, Hawaii University. Currently, he is a doctoral supervisor and professor of Xidian University. He is a fellow member of the Board of Governors of the Chinese Institute of Cryptography (preparatory committee) and also serves on the Committee of Information Theory Society for the Chinese Institute of Electronics, and a Senior Member (SM) of IEEE. His research interests include information theory, coding, and cryptography.