Recipient Anonymous Ciphertext-Policy Attribute-based Broadcast Encryption

Leyou Zhang, Hongjian Yin
(Corresponding author: Hongjian Yin)
School of Mathematics and Statistics, Xidian University
Xi'an, Shaanxi 710171, China
(Email: xidianyhj@163.com)
(Received Oct. 15, 2016; revised and accepted Feb. 20, 2017)

Abstract

The ciphertext-policy (CP) attribute-based broadcast encryption (CP-ABBE) is a more flexible broadcast encryption (BE), in which the broadcaster encrypts the data with an access policy and a receiver set. Only receivers in the valid set who satisfy the access policy will be able to decrypt the ciphertext. However, most existing CP-ABBE schemes only pay attention to plaintext privacy rather than access policy privacy and broadcast list privacy. It results in the fact that the adversary can determine the access policy or the broadcast set from ciphertexts and public parameters. However, in the real life, the access policy or the receiver set may be sensitive. To overcome this shortcoming, we propose a recipient anonymous CP-ABBE scheme, where it can protect the description of the access structures and broadcast sets associated with ciphertexts. The proposed scheme achieves full security based on the dual system encryption and constant size ciphertexts.

Keywords: Attribute-based Encryption; Broadcast Encryption; Fully Secure; Recipient Anonymity

1 Introduction

Broadcast encryption (BE) [7, 9, 11, 13] is a one-to-many encryption technique which is efficient to data sharing. It allows the broadcaster to send an encrypted message to a subset of privileged users only such listeners who are in this set can decrypt the ciphertext. In recent years, there have been many broadcast encryption schemes such as identity-based BE [15], attribute-based BE [18], and anonymous identity-based BE [23].

The notion of attribute-based encryption (ABE) was introduced by Sahai and Weters [21], which allows users to control their encrypted data at a fine-grained level. In ABE, the data owner can share their data with those users who have the specified attributes [4, 17]. There are two kinds of ABE involving ciphertext-policy ABE (CP-ABE) [3] and key-policy ABE (KP-ABE) [8, 19]. In a CP-ABE scheme, ciphertext is related to access structure and the private key of user is associated with an attribute set. Only the user whose private key satisfies the access structure associated with the ciphertext will be able to decrypt the ciphertext successfully. In contrast, in a KP-ABE scheme, ciphertext is related to an attribute set and the private key of user is associated with access structure [12, 24]. The user will be able to decrypt ciphertext only if the attributes associated with the ciphertext satisfy the access structure of the private key.

Attribute-based broadcast encryption (ABBE) was first proposed by David and Thomas [18], in which the broadcaster encrypted data with an access structure and a receiver list. Only receivers who satisfy the access policy and are in this list will be able to decrypt the ciphertext. As normal ABE, ABBE also allows fine-grained and flexible access control. However, compared with the traditional broadcast encryption, ABBE is a more flexible broadcast encryption and supply direct revocation by removing the revoked users from the receiver list. It is an important capability for real time applications such as Pay-TV.

After the first ABBE scheme [18], there have been proposed many efficient and provably secure ABBE schemes. Attrapadung and Imai proposed CP-ABBE and KP-ABBE [1] based on CP-ABE and KP-ABE, respectively. Both schemes are efficient revocable scheme. However, they only achieve selective security which is a weak security for ABBE. A strong secure ABBE scheme was proposed by Li and Zhang [16], where the scheme achieved full security by employing dual system encryption technique [22], but the ciphertext and decryption pairings grow linearly with the number of attributes and recipients. To improve the efficiency, Phuong et al. [20] proposed an ABBE scheme with short ciphertexts and private keys. Especially, their scheme achieves constant size ciphertexts and decryption pairings. However, its security is based on the decision n-Bilinear Diffie-Hellman exponent assumption which is a strong hardness assumption.

Nevertheless, all of the above mentioned ABBE schemes cannot achieve recipient anonymous, and it means that any intermediate user can only use public parameters to determine whether the ciphertexts are encrypted under the given access structure and receiver set or not. The recipient anonymity is an important property for encryption schemes. For instance, in Phuong's second ABBE scheme [20], an intermediate user can use some parts of the ciphertexts $C_1 = g^r$, $C_2 = (\prod_{j\in S^*} g_{n+1-j})^r$ to run the Decision Diffie-Hellman (DDH) test $e(C_1, \prod_{j\in S} g_{n+1-j}) \stackrel{?}{=} e(C_2, g)$, to determine whether the ciphertexts are encrypted under a given receiver set or not, where ν, g and g_l are the public parameters ($l = 1, 2, \cdots, 2n$). The maximum number of DDH-test is 2^{2n}, that is, the adversary run the DDH-test at most 2^{2n} times then he will be able to ascertain whether the S^* is broadcast list or not. Furthermore, the access structure of the CP-ABBE scheme [26] also can be determined by the DDH-test.

In this paper, we present a recipient anonymous CP-ABBE scheme. In the proposed scheme, both the access structure and the broadcast list are hidden. That is, any one cannot get any information about the access structure or the broadcast list by DDH-test from ciphertexts. Based on three static assumptions in composite order groups, our scheme is proven to be fully secure with the dual system encryption technique [22]. Furthermore, compared with some previously known ABBE schemes, the proposed scheme is an efficient CP-ABBE scheme in which the size of the ciphertexts and the number of pairings are at a constant size level.

The paper is organized as follows. In Section 2, some preliminaries are given. Section 3 gives the definition of recipient anonymous CP-ABBE scheme and its security model. The recipient anonymous CP-ABBE scheme is presented in Section 4. Security proof is introduced in Section 5. In Section 6, some comparisons between our scheme and previous works in security and efficiency are given. Finally, we conclude this paper in Section 7.

2 Preliminaries

Let $x \in_R X$ denote that x is randomly chosen from a set X.

2.1 Composite Order Bilinear Groups

The first composite order bilinear group was introduced by Boneh, Goh, and Nissim in 2005 [5]. Then it was used for many cryptographic constructions. This paper will use the bilinear group whose order is product of three distinct primes.

Let $\mathcal{G}(\cdot)$ be an algorithm that takes a security parameter λ as input and outputs a tuple $(N = p_1p_2p_3, \mathbb{G}, \mathbb{G}_T, e)$, where p_1, p_2, p_3 are distinct primes, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of composite order $N = p_1p_2p_3$ and e: $\mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$ is a map such that

1) for all $g, h \in \mathbb{G}$ and $a, b \in \mathbb{Z}_N$, $e(g^a, h^b) = e(g, h)^{ab}$;

2) exists $g \in \mathbb{G}$ such that $e(g, h)$ has order N in $\mathbb{G}_T$.

Let $\mathbb{G}_{p_1}, \mathbb{G}_{p_2}$ and $\mathbb{G}_{p_3}$ denote the subgroups of order p_1, p_2 and p_3 in $\mathbb{G}$ respectively. And g_1, g_2 and g_3 are the generators of subgroups $\mathbb{G}_{p_1}$, $\mathbb{G}_{p_2}$ and $\mathbb{G}_{p_3}$ respectively. As Lewko and Waters [14] illuminated, when $h_i \in \mathbb{G}_i$, and $h_j \in \mathbb{G}_j$ for $i \neq j$, then $e(h_i, h_j) = 1$. This property is called orthogonal property of $\mathbb{G}_{p_1}, \mathbb{G}_{p_2}, \mathbb{G}_{p_3}$.

2.2 Complexity Assumptions

The security of our recipient anonymous CP-ABBE scheme will be reduced to three static assumptions [14]. And these assumptions are described below:

Assumption 1. *Given a group parameters generator $\mathcal{G}$, we define the following distribution: $\Theta = (N = p_1p_2p_3, \mathbb{G}, \mathbb{G}_T, e) \in_R \mathcal{G}$, $g_1 \in_R \mathbb{G}_{p_1}$, $X_3 \in_R \mathbb{G}_{p_3}$, $D = (\Theta, g_1, X_3)$, $T_1 \in_R \mathbb{G}$, $T_2 \in_R \mathbb{G}_{p_1p_3}$. Now the advantage of an algorithm $\mathcal{A}$ in breaking Assumption 1 is defined to be*

$$Adv^1_{\mathcal{A}} = |Pr[\mathcal{A}(D, T_1) = 1] - Pr[\mathcal{A}(D, T_2) = 1]|.$$

Assumption 2. *Given a group parameters generator $\mathcal{G}$, we define the following distribution: $\Theta = (N = p_1p_2p_3, \mathbb{G}, \mathbb{G}_T, e) \in_R \mathcal{G}$, $g_1 \in_R \mathbb{G}_{p_1}$, $X_i \in_R \mathbb{G}_{p_i} (i = 1, 2, 3)$, $Y_2 \in_R \mathbb{G}_{p_2}$, $D = (\Theta, g_1, X_1X_2X_3, Y_2)$, $T_1 \in_R \mathbb{G}_{p_1}$, $T_2 \in_R \mathbb{G}_{p_1p_2}$. Now the advantage of an algorithm $\mathcal{A}$ in breaking Assumption 2 is defined to be*

$$Adv^2_{\mathcal{A}} = |Pr[\mathcal{A}(D, T_1) = 1] - Pr[\mathcal{A}(D, T_2) = 1]|.$$

Assumption 3. *Given a group parameters generator $\mathcal{G}$, we define the following distribution: $\Theta = (N = p_1p_2p_3, \mathbb{G}, \mathbb{G}_T, e) \in_R \mathcal{G}$, $g_1 \in_R \mathbb{G}_{p_1}$, $X_3 \in_R \mathbb{G}_{p_3}$, $D = (\Theta, g_1, X_3)$, $T_1 \in_R \mathbb{G}_T$, $T_2 = e(g_1, g_1)^{\alpha s}$. Now the advantage of an algorithm $\mathcal{A}$ in breaking Assumption 3 is defined to be*

$$Adv^3_{\mathcal{A}} = |Pr[\mathcal{A}(D, T_1) = 1] - Pr[\mathcal{A}(D, T_2) = 1]|.$$

2.3 Access Structure

Our construction will employ AND-gate on multi-valued attributes access structure, which is similar to what used in [2, 6]. The access structure of AND-gate on multi-valued attributes is described as follows.

Let $\mathbb{U} = \{att_1, att_2, \cdots, att_n\}$ be a set of attributes. For $att_i \in \mathbb{U}$, $S_i = \{v_{i,1}, v_{i,2}, \cdots v_{i,m_i}\}$ is a set of possible values, where m_i is the number of possible values for each att_i. Let $L = [L_1, L_2, \cdots L_n]$ be an attribute list for a user where $L_i \in S_i$. Let $\mathbb{A} = [w_1, w_2, \cdots w_n]$ be an access structure where $w_i \in S_i$. The notation $L \models \mathbb{A}$ expresses that an attribute list L satisfies an access structure $\mathbb{A}$ and $\not\models$ refers to not satisfy symbol.

3 Definitions and Security Model

3.1 Definitions of CP-ABBE Scheme

A recipient anonymous ciphertext-policy attribute-based broadcast encryption (CP-ABBE) scheme consists of the following four algorithms:

Setup$(1^\lambda, \mathcal{U}, \mathcal{N})$**.** Take as input a security parameter λ, the broadcast index set $\mathcal{U}$ and the universal attribute set $\mathcal{N}$. Then this algorithm outputs a public parameters PK and a master secret key MSK.

KeyGen(MSK, k, L)**.** Take as input the master secret key MSK, the user's index $k \in \mathcal{U}$ and attribute set $L \subseteq \mathcal{N}$. Then this algorithm outputs the user's private key $SK_{(k,L)}$.

Encrypt$(PK, S, \mathbb{A})$**.** Take as input the public parameters PK, a broadcast index list $S \subseteq \mathcal{U}$ and an access structure $\mathbb{A} \in AS$, where AS is an access structure family over $\mathcal{N}$. Then this algorithm outputs a broadcast header Hdr and a massage encryption key K.

Decrypt$(SK_{(k,L)}, Hdr)$**.** Take as input the a private key $SK_{(k,L)}$ as well as a broadcast header, if $k \in S$ and $L \models \mathbb{A}$, then this algorithm outputs K.

3.2 Security Model

Following [10], we describe the indistinguishability against chosen plaintext attack (IND-CPA) definition of recipient anonymous CP-ABBE in the fully secure model. The formal secure game between adversary $\mathcal{A}$ and challenger $\mathcal{B}$ is as follows.

Setup. Assume universal attribute set $\mathcal{N}$, broadcast index set $\mathcal{U}$ and access structure family AS are predefined. The challenger $\mathcal{B}$ runs the **Setup** algorithm to obtain a public parameters PK and a master secret key MSK. Then it gives adversary $\mathcal{A}$ the public parameters PK and keeps MSK to itself.

Key Query Phase 1. The adversary queries the challenger $\mathcal{B}$ for private keys corresponding to index $k \in \mathcal{U}$ and attribute set $L \subseteq \mathcal{N}$. The challenger runs the **KeyGen** algorithm and gives the corresponding private keys $SK_{(k,L)}$ to $\mathcal{A}$.

Challenge. When the adversary decides that **Phase 1** is over, $\mathcal{A}$ outputs two same-length messages M_0 and M_1. The adversary also outputs a challenge broadcast index set S^* and access structure $\mathbb{A}^*$ such that for all index k and attribute set L queried in **Phase 1**, we have $k \notin S^*$ and $L \not\models \mathbb{A}^*$. Then $\mathcal{B}$ runs **Encrypt** algorithm to get $\langle Hdr^*, K_0 \rangle$ and randomly chooses $K_1 \in_R \mathcal{K}$, where $\mathcal{K}$ is the symmetric key space. It flips a coin $\mu \in \{0,1\}$ and gives $\langle Hdr^*, K_\mu \rangle$ to $\mathcal{A}$.

Key Query Phase 2. In this phase, $\mathcal{B}$ acts almost the same as in **Phase 1** except it is unable to ask key for attribute set L and index k such that $L \models \mathbb{A}^*$ and $k \in S^*$.

Guess. Finally, the adversary $\mathcal{A}$ outputs the guess bit $\mu' \in \{0,1\}$ for μ and wins the game if $\mu' = \mu$.

The advantage of the adversary in this game is defined as follows:

$$Game_{\mathcal{A}}(\lambda) = |Pr[\mu = \mu'] - \frac{1}{2}|,$$

where the probability is taken over the random bits used by the challenger and the adversary.

Definition 1. *A recipient anonymous CP-ABBE scheme is IND-CPA secure if for all polynomial time adversary $\mathcal{A}$, the $Game_{\mathcal{A}}(\lambda)$ is negligible.*

4 Recipient Anonymous CP-ABBE Scheme

In this section, we will present our recipient anonymous CP-ABBE scheme construction and show the recipient anonymity of our scheme by employing composite order bilinear groups. There are four algorithms in our scheme, which are defined in Section 3.1. First, we briefly summarized our idea. In order to realize recipient anonymity, some random numbers are added to each part of the ciphertexts. And these random numbers can prevent adversary from determining user information by running DDH-test. Thanks to employ composite order group, these random numbers will not affect the decryption process in our scheme. The detailed algorithms are described in the following. The abbreviations and notations used throughout the paper are shown in Table 1.

4.1 Construction

– **Setup**$(1^\lambda, \mathcal{N}, \mathcal{U})$**:** To generate the system parameters, the setup algorithm takes a security parameter λ, an universal attribute set $\mathcal{N}$ and a broadcast index set $\mathcal{U}$ where $|\mathcal{U}| = h$ as inputs. Then it runs the group generator $\mathcal{G}$ to get a description of bilinear composite order group $\Theta = (N = p_1p_2p_3, \mathbb{G}, \mathbb{G}_T, e)$. The algorithm picks random elements a, α in $\mathbb{Z}_N$, g_1, $u_{j'}$ in $\mathbb{G}_{p_1}$ and R_0 in $\mathbb{G}_{p_3}$, where $j' \in \mathcal{U}$. For each attribute $v_{i,j} \in \mathcal{N}$, the setup algorithm chooses random elements $a_{i,j}$ in $\mathbb{Z}_N$ and $R_{i,j}$ in $\mathbb{G}_{p_3}$. Then the setup algorithm computes $A_{i,j} = g_1^{a_{i,j}} \cdot R_{i,j}$, $A_0 = g_1 \cdot R_0$. The public parameters PK is defined as

$$PK = \langle e(g_1, g_1)^\alpha, A_0, A_{i,j}, \{u_{j'}\}_{j' \in \mathcal{U}} \rangle,$$

and the master secret key MSK is defined as $MSK = \langle g_1, \alpha, a, a_{i,j}, a_j \rangle$, where $1 \le i \le n, 1 \le j \le m_i$.

Table 1: Parameters declaration

Symbol	Description
p_i	The primes, where $i = 1, 2, 3$.
g_i	Generators with order p_i, over $\mathbb{G}_{p_i}$, where $i = 1, 2, 3$.
$\mathbb{Z}_N$	The set of positive integers.
MSK	The master secret key.
$SK_{(k,L)}$	The private key associated with attributes set L and user index k.
M	Message.
K	Symmetric key.
Hdr	The broadcast header.
$e(\cdot)$	Bilinear pairing.
$\|B\|$	The number of elements in set B.

– **KeyGen**(MSK, k, L)**:** Given a user index $k \in \mathcal{U}$, an attributes set $L = [v_{1,j_1}, v_{2,j_2}, \cdots v_{n,j_n}] \in \mathcal{N}$ and the master secret key, the key generation algorithm chooses a random element $r \in_R \mathbb{Z}_N$ and computes:

$$D_1 = g_1^{\alpha+ar} u_k^r, \qquad D_2 = g_1^r,$$
$$\{D_{3,j'} = u_{j'}^r\}_{j' \in \mathcal{U}\setminus\{k\}}, \quad D_4 = \left(g_1^{a+\sum_{v_{i,j_i} \in L} a_{i,j_i}}\right)^r.$$

Finally, this algorithm outputs the private key associated with attributes set L and user index k

$$SK_{(k,L)} = \langle D_1, D_2, D_{3,j'}, D_4 \rangle_{j' \in \mathcal{U}\setminus\{k\}}.$$

– **Encrypt**$(PK, S, \mathbb{A})$**:** Let $M \in \mathbb{G}_T$ be the message to be encrypted and let $\mathbb{A} = \wedge_{i=1}^n w_{i,j_i}$ where $w_{i,j_i} \in Att_i$, be an access policy and a broadcast set $S \subseteq \mathcal{U}$. A broadcaster randomly selects $s \in_R \mathbb{Z}_N$ and $R_1, R_2, R_3 \in_R \mathbb{G}_{p_3}$. Then this algorithm computes the symmetric key K and broadcast header Hdr as follows.

$$K = e(g_1, g_1)^{\alpha s}, \qquad C_1 = (\textstyle\prod_{v_{i,j_i} \in \mathbb{A}} A_{i,j_i})^s \cdot R_1,$$
$$C_2 = A_0^s \cdot R_2, \qquad C_3 = (\textstyle\prod_{j' \in S} u_{j'})^s \cdot R_3,$$
$$Hdr = (C_1, C_2, C_3).$$

In this system, K is used to encrypt the massage M in a symmetric encryption scheme. Note that a random element $R \in \mathbb{G}_{p_3}$ can be selected by choosing a random $\eta \in \mathbb{Z}_N$ and setting $R = g_3^\eta$ where g_3 is publicly given.

– **Decrypt**$(SK_{(k,L)}, Hdr)$**:** The decryption algorithm takes a broadcast header Hdr and a private key $SK_{(k,L)}$ as input. If the private key of the recipient $SK_{(k,L)}$ satisfies the policy of the ciphertext, then this algorithm will compute the symmetric key K as follows,

$$\frac{e(D_1 \cdot \prod_{j' \in S\setminus\{k\}} D_{3,j'}, C_2) \cdot e(D_2, C_1)}{e(D_2, C_3) \cdot e(D_4, C_2)}$$
$$= e(g_1, g_1)^{\alpha s}$$
$$= K.$$

4.2 Correctness

The correctness will subsequently be checked by applying the orthogonality property of $\mathbb{G}_{p_i}$ $(i = 1, 2, 3)$.

If the user index $k \in S$ and attributes set $L \models \mathbb{A}$, then one can obtain the below equations hold.

$$\begin{aligned} & e(D_1 \textstyle\prod_{j' \in S\setminus\{k\}} D_{3,j'}, C_2) \\ =& e(g_1^{\alpha+ar} u_k^r \textstyle\prod_{j' \in S\setminus\{k\}} u_{j'}^r, g_1^s R_0^s \cdot R_2) \\ =& e(g_1, g_1)^{\alpha s} \cdot e(g_1, g_1)^{ars} \cdot e(u_k^r \textstyle\prod_{j' \in S\setminus\{k\}} u_{j'}^r, g_1^s) \\ =& e(g_1, g_1)^{\alpha s} \cdot e(g_1, g_1)^{ars} \cdot e(\textstyle\prod_{j' \in S} u_{j'}, g_1)^{rs} \\ =& B_1. \end{aligned} \tag{1}$$

$$\begin{aligned} e(D_2, C_3) =& e(g_1^r, (\textstyle\prod_{j' \in S} u_{j'})^s \cdot R_3) \\ =& e(\textstyle\prod_{j' \in S} u_{j'}, g_1)^{rs} \\ =& B_2. \end{aligned} \tag{2}$$

$$\begin{aligned} & \frac{e(D_2, C_1)}{e(D_4, C_2)} \\ =& \frac{e(g_1^r, (\prod_{v_{i,j_i} \in \mathbb{A}} g_1^{a_{i,j_i}} \cdot R_{i,j})^s \cdot R_1)}{e\left(\left(g_1^{a+\sum_{v_{i,j_i} \in L} a_{i,j_i}}\right)^r, g_1^s R_0^s \cdot R_2\right)} \\ =& \frac{e(g_1, \prod_{v_{i,j_i} \in \mathbb{A}} g_1^{a_{i,j_i}})^{rs}}{e(g_1, g_1)^{ars} \cdot e\left(g_1^{\sum_{v_{i,j_i} \in L} a_{i,j_i}}, g_1\right)^{\alpha s}} \\ =& B_3. \end{aligned} \tag{3}$$

Then from the above three Equations (1), (2) and (3), it will be easy to obtain that

$$\frac{B_1 B_3}{B_2} = e(g_1, g_1)^{\alpha s} = K.$$

Note that in the *KeyGen* algorithm, this paper assumes $\forall L, L'(L \neq L')$, $\sum_{v_{i,j_i} \in L} a_{i,j_i} \neq \sum_{v_{i,j_i} \in L'} a_{i,j_i}$ because the parameter r has no effect on decryption. If the above condition is not met, various users associated with attribute set L, L' will have the same decryption ability [6].

4.3 Recipient Anonymous

This section will show that the proposed scheme achieve recipient anonymity in the composite order bilinear groups.

Compared with [16, 20], our scheme adds a random number to each part of the ciphertexts, these random numbers will not affect the decryption process. However, they are necessary for recipient anonymity of scheme, because if there is no such a random number, then for some access structure $\mathbb{A}^*$ and broadcast list S^* the adversary may perform the DDH-test to determine whether the ciphertext is encrypted under the $\mathbb{A}^*, S^*$ or not. In our scheme, by utilizing the DDH-test $e(C_2, \prod_{v_{i,j_i}\in\mathbb{A}^*} A_{i,j_i}) \stackrel{?}{=} e(A_0, C_1)$ to determine whether the ciphertext is encrypted under the $\mathbb{A}^*$ or not will be fail. The DDH-test $e(C_2, \prod_{v_{i,j_i}\in\mathbb{A}^*} A_{i,j_i}) \stackrel{?}{=} e(A_0, C_1)$ is same as $e(C_2, \prod_{v_{i,j_i}\in\mathbb{A}^*} A_{i,j_i})/e(A_0, C_1) \stackrel{?}{=} 1_T$, where 1_T is the identity element in $\mathbb{G}_T$, on the public parameters of attributes occur in $\mathbb{A}^*$ and the ciphertext components. The following is the detailed analysis.

$$
\begin{aligned}
& e(C_2, \textstyle\prod_{v_{i,j_i}\in\mathbb{A}^*} A_{i,j_i}) \qquad (4)\\
=& e(g_1^s R_0^s R_2, \textstyle\prod_{v_{i,j_i}\in\mathbb{A}^*} g_1^{a_{i,j_i}} R_{i,j_i})\\
=& e(g_1^s, \textstyle\prod_{v_{i,j_i}\in\mathbb{A}^*} g_1^{a_{i,j_i}}) \cdot e(R_0^s, R_{\mathbb{A}^*}) \cdot e(R_2, R_{\mathbb{A}^*}),
\end{aligned}
$$

$$
\begin{aligned}
& e(A_0, C_1) \qquad (5)\\
=& e(g_1 R_0, \textstyle\prod_{v_{i,j_i}\in\mathbb{A}} g_1^{s a_{i,j_i}} \cdot R_{\mathbb{A}}^s \cdot R_1)\\
=& e(g_1, \textstyle\prod_{v_{i,j_i}\in\mathbb{A}} g_1^{s a_{i,j_i}}) \cdot e(R_0, R_{\mathbb{A}}^s) \cdot e(R_0, R_1),
\end{aligned}
$$

where $R_{\mathbb{A}^*} = \prod_{v_{i,j_i}\in\mathbb{A}^*} R_{i,j_i}$, $R_{\mathbb{A}} = \prod_{v_{i,j_i}\in\mathbb{A}} R_{i,j_i}$.

If $\mathbb{A} = \mathbb{A}^*$, then $j_i' = j_i$ for all i, $1 \le i \le n$, and hence $\sum_{i=1}^n a_{i,j_i'} = \sum_{i=1}^n a_{i,j_i}$ and $R_{\mathbb{A}} = R_{\mathbb{A}^*}$. Therefore,

$$
\frac{e(C_2, \prod_{v_{i,j_i}\in\mathbb{A}^*} A_{i,j_i})}{e(A_0, C_1)} = \frac{e(R_2, R_{\mathbb{A}^*})}{e(R_0, R_1)}.
$$

If $\mathbb{A} \neq \mathbb{A}^*$, there exists at last one k, $1 \le k \le n$ such that $j_k' \neq j_k$. Without loss of generality, let $j_i' = j_i$, for all i, $1 \le i \le n$ except $i = k$. Then $a_{i,j_i'} = a_{i,j_i}$, $R_{i,j_i'} = R_{i,j_i}$, for all i, $1 \le i \le n$, except $i = k$. Therefore,

$$
\begin{aligned}
& \frac{e(C_2, \prod_{v_{i,j_i}\in\mathbb{A}^*} A_{i,j_i})}{e(A_0, C_1)}\\
=& \frac{e(g_1^s, g_1^{a_{k,j_k'}}) \cdot e(R_0^s, R_{k,j_k'}) \cdot e(R_2, R_{\mathbb{A}^*})}{e(g_1, g_1^{s a_{k,j_k'}}) \cdot e(R_0, R_{\mathbb{A}}^s) \cdot e(R_0, R_1)}.
\end{aligned}
$$

In both the cases, $\mathbb{A} = \mathbb{A}^*$ and $\mathbb{A} \neq \mathbb{A}^*$, the DDH-test gives a random element of $\mathbb{G}_T$ so that the adversary will be not able to determine whether the ciphertext is encrypted under the $\mathbb{A}^*$ or not. By the same way, the user index DDH-test $e(C_2, \prod_{j'\in S^*} u_{j'}) \stackrel{?}{=} e(A_0, C_3)$ will be fail, too. So both the access structure and the broadcast set are hidden, which means the proposed scheme is recipient anonymous.

5 Proof of Security

This section will show that the proposed scheme achieves the full security by employing the dual system encryption technique. In dual system encryption schemes [14, 22], ciphertexts and keys can take on two forms: normal or semi-functional. Semi-functional ciphertexts and semi-functional keys are only used in security proof, but not used in the real system. Let g_2 be a generator of the subgroup $\mathbb{G}_{p_2}$. The semi-functional ciphertexts and the semi-functional keys are created as follows.

Semi-functional ciphertexts: For an access structure $\mathbb{A} = \wedge_{i=1}^n w_{i,j_i}$, where $w_{i,j_i} \in Att_i$, and a broadcast set $S = \{1, 2, \cdots, q\} \in \mathcal{U}$, we first run the encryption algorithm *Encrypt* to obtain normal ciphertexts K', C_1', C_2', C_3'. Then choose some random elements δ, $b_{j'}$ and z_{i,j_i} in $\mathbb{Z}_N$ where $j' = \{1, 2, \cdots, q\}$, $i = \{1, 2, \cdots, n\}$. Semi-functional ciphertexts are computed as follows:

$$
\begin{aligned}
K &= K', & C_1 &= C_1' g_2^{\delta \sum_{i=1}^n z_{i,j_i}},\\
C_2 &= C_2' g_2^{\delta}, & C_3 &= C_3' g_2^{\delta \sum_{j'=1}^q b_{j'}}.
\end{aligned}
$$

Semi-functional keys: There are two types of semi-functional keys in our proof. Firstly, run the key generation algorithm *KeyGen* to get normal private key for index t and attribute set L as: $D_1, D_2, \{D_{3,j'}\}_{j'\in\mathcal{U}\setminus\{t\}}$ and D_4. Then choose random values γ, σ, σ' and $\delta_{j'}$ in $\mathbb{Z}_N$ where $j' = 1, 2, \cdots, h$ and compute two types of semi-functional private keys components as follows.

Type 1.

$$
\begin{aligned}
D_1 &= D_1' g_2^{\gamma}, & D_2 &= D_2' g_2^{\sigma},\\
\{D_{3,j'} &= D_{3,j'}' g_2^{\sigma\delta_{j'}}\}_{j'\in\mathcal{U}\setminus\{t\}}, & D_4 &= D_4' g_2^{\sigma' + \sigma \sum_{v_{i,j_i}\in L} z_{i,j_i}}.
\end{aligned}
$$

Type 2.

$$
\begin{aligned}
D_1 &= D_1' g_2^{\gamma}, & D_2 &= D_2',\\
\{D_{3,j'} &= D_{3,j'}'\}_{j'\in\mathcal{U}\setminus\{t\}}, & D_4 &= D_4'.
\end{aligned}
$$

When the semi-functional ciphertexts are used to decrypt semi-functional keys, the regular decryption will be prevented by a blind factor.

The security of the proposed scheme will be proved by using a hybrid argument over a sequence of games. Let q denote the number of secret key queries made by the adversary. The games are defined as follows.

$Game_{Real}$: It is a real CP-ABBE security game in which both private keys and challenge ciphertexts are in normal form.

$Game_0$: In this game, the challenge ciphertexts are semi-functional, but all private keys are normal.

$Game_{k,1}$: The challenge ciphertexts are semi-functional, the fist $k-1$ keys are type 2 semi-functional private keys and the k^{th} key is semi-functional of type 1. The rest of keys are replied in normal form.

$Game_{k,2}$: This game is like $Game_{k,1}$ expect for the k^{th} key is a semi-functional of type 2.

$Game_{q,2}$: In this game, the challenge ciphertexts are semi-functional, and all the private keys are in semi-functional of type 2.

$Game_{Final}$: This final game $Game_{Final}$ is the same as $Game_{q,2}$, except that the challenge ciphertext is semi-functional encryption of random message, other than neither of the two chosen massages by adversary, so the advantage of adversary in this game is 0.

We will prove that these games are indistinguishable in a set of Lemmas. Let $Game_* Adv_{\mathcal{A}}$ denote the advantage of adversary $\mathcal{A}$ in $Game_*$. Note that we have $Game_{Real} Adv_{\mathcal{A}} = Adv_{\mathcal{A}}(\lambda)$ for some fixed security parameter λ.

Lemma 1. *Suppose there exists a polynomial time algorithm $\mathcal{A}$ such that $Game_{Real} Adv_{\mathcal{A}} - Game_0 Adv_{\mathcal{A}} = \epsilon$. Then we can build a polynomial time algorithm $\mathcal{B}$ with advantage ϵ in breaking Assumption 1.*

Proof. We establish an algorithm $\mathcal{B}$ which has received $\langle \Theta, g_1, T \rangle$, where T is either an element of $\mathbb{G}$ or an element of $\mathbb{G}_{p_1 p_3}$ from the challenger. Note that a random element $d \in \mathbb{G}_{p_i}$ can be selected by choosing a random $\tau \in \mathbb{Z}_N$ and setting $d = g_i^{\tau}$, where g_i is the generator of $\mathbb{G}_{p_i}$ for $i \in \{1, 2, 3\}$.

Setup. The algorithm $\mathcal{B}$ randomly selects $R_0, R_{i,j} \in_R \mathbb{G}_{p_3}$, $\alpha, a, a_{i,j}$ and $a_{j'} \in_R \mathbb{Z}_N$. Then $\mathcal{B}$ computes $Y = e(g_1, g_1)^{\alpha}$, $A_0 = g_1 \cdot R_0$, $A_{i,j} = g_1^{a_{i,j}} \cdot R_{i,j}$, for all $1 \le i \le n$ and $1 \le j \le m_i$. The algorithm $\mathcal{B}$ produces the public parameters $PK = \langle Y, A_0, \{u_{j'} = g_1^{a_{j'}}\}_{j' \in \mathcal{U}}, \{A_{i,j} | 1 \le i \le n, 1 \le j \le m_i\} \rangle$.

Key Query Phase 1 and Phase 2. Consider the adversary $\mathcal{A}$ requires the private key for any attribute set L and index $t \in \mathcal{U}$. $\mathcal{B}$ can answer it in normal form readily because it knows the master key MSK.

Challenge. The algorithm $\mathcal{A}$ outputs an access structure $\mathbb{A}^*$ and a broadcast index set S^* to challenger $\mathcal{B}$. In order to compute the challenge ciphertexts, $\mathcal{B}$ randomly chooses $t_1, t_2, t_3 \in_R \mathbb{Z}_N$ then flips a coin $\mu \in \{0, 1\}$ and computes

$$K_0 = e(g_1, T)^{\alpha}, \qquad C_1 = T^{\sum_{v_{i,j_i} \in \mathbb{A}^*} a_{i,j_i}} g_3^{t_1},$$
$$C_2 = T g_3^{t_2}, \qquad C_3 = T^{\sum_{j \in S^*} a_{j'}} g_3^{t_3}.$$

Then $\mathcal{B}$ chooses a random symmetric key K_1 in the key space $\mathcal{K}$ and sends $\langle Hdr^*, K_{\mu} \rangle$ to $\mathcal{A}$, where $Hdr^* = (C_1, C_2, C_3)$. Here we note that if there exists $L \not\models \mathbb{A}^*$ and $t \notin S^*$ such that $\sum_{v_{i,j_i} \in \mathbb{A}} = \sum_{v_{i,j_i} \in \mathbb{A}^*}$ and $\sum_{j' \in S} a_{j'} = a_t \sum_{j' \in S^* \setminus \{t\}} a_{j'}$ hold, then the algorithm $\mathcal{B}$ aborts.

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

Note that for $i \neq j$, the values ρ modulo p_i are uncorrelated from the values ρ modulo p_j by the Chinese Remainder Theorem. If $T \in \mathbb{G}$, then it can be written as $T = g_1^s g_2^{\delta} X_3$, where g_1^s and g_2^{δ} is the $\mathbb{G}_{p_1}$ and $\mathbb{G}_{p_2}$ part of T respectively and X_3 is a random element in $\mathbb{G}_{p_3}$. This implicitly sets $z_{i,j_i} = a_{i,j_i}$ and $b_{j'} = a_{j'}$. Hence Hdr^* is a properly distributed semi-functional ciphertext, in this case, $\mathcal{B}$ simulates the game $Game_0$. If $T \in \mathbb{G}_{p_1 p_3}$, Hdr^* is a properly distributed normal ciphertext and hence $\mathcal{B}$ will simulate the game $Game_{Real}$. Therefore, if $\mathcal{A}$ can distinguish these two games then $\mathcal{B}$ will distinguish the two distributions so as to break the Assumption 1. □

Lemma 2. *Suppose there exists a polynomial time algorithm $\mathcal{A}$ such that $Game_{k-1,2} Adv_{\mathcal{A}} - Game_{k,1} Adv_{\mathcal{A}} = \epsilon$. Then we can build a polynomial time algorithm $\mathcal{B}$ with advantage ϵ in breaking Assumption 2.*

Proof. We establish an algorithm $\mathcal{B}$ which has received $\langle \Theta, g_1, X_1 X_2 X_3, Y_2, T \rangle$, where X_i and Y_i are random elements in $\mathbb{G}_{P_i}$ and T is either an element of $\mathbb{G}_{p_1 p_2}$ or an element of $\mathbb{G}_{p_1}$ from the challenger.

Setup. The algorithm $\mathcal{B}$ chooses random elements $R_0, R_{i,j}$ in $\mathbb{G}_{p_3}$, and $\alpha, a, a_{i,j}$ and a_j in $\mathbb{Z}_N$, then it computes $Y = e(g_1, g_1)^{\alpha}$, $A_0 = g_1 \cdot R_0$, $A_{i,j} = g_1^{a_{i,j}} \cdot R_{i,j}$, for all $1 \le i \le n$ and $1 \le j \le m_i$. The algorithm $\mathcal{B}$ products the public parameters $PK = \langle Y, A_0, \{u_{j'} = g_1^{a_{j'}}\}_{j' \in \mathcal{U}}, \{A_{i,j} | 1 \le i \le n, 1 \le j \le m_i\} \rangle$, and keeps the master key MSK.

Key Query Phase 1 and Phase 2. To compute the first $k-1$ private semi-functional keys, the algorithm $\mathcal{B}$ chooses random elements ϑ, r in $\mathbb{Z}_N$ and implicitly sets $Y_2 = g_2^l$ and responds to each private key request on a set of attributes L and broadcast index $t (t < k)$ from $\mathcal{A}$ by setting

$$D_1 = g_1^{\alpha + ar} u_t^r \cdot Y_2^{\vartheta}, \quad D_2 = g_1^r,$$
$$D_{3,j'} = u_{j'}^r, \qquad D_4 = \left(g_1^{a + \sum_{v_{i,j_i} \in L} a_{i,j_i}} \right)^r.$$

This implicitly sets $z_{i,j_i} = a_{i,j_i}$, $b_{j'} = a_{j'}$ and $Y_2^{\vartheta} = g_1^{\delta}$, so D_1, D_2, D_3 and D_4 are properly distributed semi-functional private key components.

To compute the k^{th} private key, the algorithm $\mathcal{B}$ will implicitly set g_1^r as the $\mathbb{G}_{p_1}$ part of T and sets

$$D_1 = g_1^{\alpha} \cdot T^{a + a_t}, \qquad D_2 = T,$$
$$D_{3,j'} = T^{a_{j'}}, \qquad D_4 = T^{a + \sum_{v_{i,j_i} \in L} a_{i,j_i}}.$$

Suppose $T \in \mathbb{G}_{p_1 p_2}$. Let $T = g_1^r g_2^{\sigma}$ for some $r, \sigma \in \mathbb{Z}_N$. Here we implicitly set $\sigma = (a + a_t), b_{j'} = a_{j'}, \sigma' = a\sigma$, and $z_{i,j_i} = a_{i,j_i}$. So the key is a semi-functional key of type 1. Similarly if $T \in \mathbb{G}_{p_1}$, the private key is normal.

Challenge. The adversary $\mathcal{A}$ submits an access structure $\mathbb{A}^*$ and a broadcast index set S^*. The algorithm $\mathcal{B}$

flips a coin $\mu \in \{0,1\}$ and sets $X_1X_2 = g_1^s g_2^\sigma$ implicitly. Then it prepares challenge ciphertexts as:

$$K_0 = e(X_1X_2X_3, g_1)^\alpha, \quad C_1 = (X_1X_2X_3)^{\sum_{v_{i,j_i} \in \mathbb{A}^*} a_{i,j_i}} g_3^{t_1},$$
$$C_2 = (X_1X_2X_3) \cdot g_3^{t_2}, \quad C_3 = (X_1X_2X_3)^{\sum_{j \in S^*} a_{j'}} g_3^{t_3}.$$

Then algorithm $\mathcal{B}$ chooses a random symmetric key K_1 in the key space $\mathcal{K}$ and sends $\langle Hdr^*, K_\mu \rangle$ to $\mathcal{A}$, where $Hdr^* = (C_1, C_2, C_3)$.

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

If $T \in \mathbb{G}_{p_1}$, then $\mathcal{B}$ has properly simulated $Game_{k-1}$. If $T \in \mathbb{G}_{p_1p_2}$, then $\mathcal{B}$ has properly simulated $Game_k$. Hence, the algorithm $\mathcal{B}$ can use the output of $\mathcal{A}$ to distinguish $Game_{k-1}$ and $Game_k$. □

Lemma 3. *Suppose there exists a polynomial time algorithm $\mathcal{A}$ such that $Game_{k,1}Adv\mathcal{A} - Game_{k,2}Adv\mathcal{A} = \epsilon$. Then we can build a polynomial time algorithm $\mathcal{B}$ with advantage ϵ in breaking Assumption 2.*

Proof. This proof is very similar to the proof of the previous lemma. After receiving the challenge parameters, the algorithm $\mathcal{B}$ forms the public parameters $PK = \langle Y, A_0, \{u_{j'} = g_1^{a_{j'}}\}_{j' \in \mathcal{U}}, \{A_{i,j} | 1 \le i \le n, 1 \le j \le m_i\}\rangle$. The adversary $\mathcal{A}$ forms first $k-1$ private keys and challenge ciphertext as the previous lemma and forms last $q-k$ keys by employing master secret key respectively. For k^{th} key, the algorithm $\mathcal{B}$ chooses a random value ϕ in $\mathbb{Z}_N$ and computes:

$$D_1 = g_1^\alpha \cdot T^{a+a_t} Y_2^\phi, \quad D_2 = T,$$
$$D_{3,j'} = T^{a_{j'}}, \quad D_4 = T^{a+\sum_{v_{i,j_i} \in L} a_{i,j_i}}.$$

Let g_1^r be the $\mathbb{G}_{p_1}$ part of T. It is easy to see that if $T \in \mathbb{G}_{p_1}$, this is a well-formed type 2 semi-functional key and $\mathcal{B}$ has properly simulated $Game_{k,2}$. Otherwise, $T \in \mathbb{G}_{p_1p_2}$, this is type 1 semi-functional key and $\mathcal{B}$ has properly simulated $Game_{k,1}$. In the both cases the decryption test will be fail because the random element Y_2^ϑ cannot be cancelled out. Hence the algorithm $\mathcal{B}$ can use $\mathcal{A}$'s output to break Assumption 2 with advantage ϵ. □

Lemma 4. *Suppose there exists a polynomial time algorithm $\mathcal{A}$ such that $Game_{q,2}Adv\mathcal{A} - Game_{Final}Adv\mathcal{A} = \epsilon$. Then we can build a polynomial time algorithm $\mathcal{B}$ with advantage ϵ in breaking Assumption 3.*

Proof. We establish an algorithm $\mathcal{B}$ which has received $\langle \Theta, g_1, g_1^\alpha X_2, Y_2Y_3, Z_2, T\rangle$ and the algorithm needs to decide $T = e(g_1, g_1)^{\alpha s}$ or T is a random element of $\mathbb{G}_T$.

Setup. The algorithm $\mathcal{B}$ randomly selects $R_0, R_{i,j} \in_R \mathbb{G}_{p_3}$, $\alpha, a, a_{i,j}$ and $a_{j'} \in_R \mathbb{Z}_N$, then it computes $Y = e(g_1^\alpha X_2, g_1)$, $A_0 = g_1 \cdot R_0$, $A_{i,j} = g_1^{a_{i,j}} \cdot R_{i,j}$, for all $1 \le i \le n$ and $1 \le j \le m_i$. The algorithm $\mathcal{B}$ forms the public parameters $PK = \langle Y, A_0, \{u_{j'} = g_1^{a_{j'}}\}_{j' \in \mathcal{U}}, \{A_{i,j} | 1 \le i \le n, 1 \le j \le m_i\}\rangle$. Here $e(g_1^\alpha X_2, g_1) = e(g_1, g_1)^\alpha$.

Key Query Phase 1 and Phase 2. For attribute set L and user index t, The algorithm $\mathcal{B}$ randomly picks $r, t \in \mathbb{Z}_N$ and sets type 2 semi-functional key as

$$D_1 = g_1^{\alpha+ar} u_t^r \cdot Z_2^t, \quad D_2 = g_1^r,$$
$$D_{3,j'} = u_{j'}^r, \quad D_4 = \left(g_1^{a+\sum_{v_{i,j_i} \in L} a_{i,j_i}}\right)^r.$$

Challenge. The adversary $\mathcal{A}$ sends $\mathcal{B}$ an access structure $\mathbb{A}^*$ and a broadcast index set S^*. Then $\mathcal{B}$ flips a coin $\mu \in \{0,1\}$ and sets challenge ciphertexts as

$$K_0 = T, \quad C_1 = (g_1Y_2Y_3)^{\sum_{v_{i,j_i} \in \mathbb{A}^*} a_{i,j_i}} g_3^{t_1},$$
$$C_2 = g_1^s Y_2Y_3 g_3^{t_2}, \quad C_3 = (g_1^s Y_2Y_3)^{\sum_{j' \in S^*} a_{j'}} g_3^{t_3}.$$

This implicitly sets $Y_2 = g_2^\delta, z_{i,j_i} = z_{i,j_i}, b_{j'} = a_{j'}$. Then $\mathcal{B}$ chooses a random symmetric key K_1 in the key space $\mathcal{K}$ and sends $\langle Hdr^*, K_\mu \rangle$ to $\mathcal{A}$, where $Hdr^* = (C_1, C_2, C_3)$.

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

If $T = e(g_1, g_1)^{\alpha s}$, then challenge ciphertext is a valid semi-functional ciphertext. If T is a random element in $\mathbb{G}_T$ challenge ciphertext is a valid semi-functional ciphertext for a random message. Hence the algorithm $\mathcal{B}$ can use $\mathcal{A}$'s output to break Assumption 3 with advantage ϵ. □

Theorem 1. *If assumptions 1,2,3 hold, then our scheme is fully CPA secure.*

Proof. If Assumption 1, 2 and 3 hold, by the sequence of games and Lemma from 1 to 4, the adversary's advantage in the real game must be negligible. Hence the adversary cannot attain a non-negligible advantage in breaking our scheme. □

6 Performance Analysis

In this section, we will present the comparisons between previous CP-ABBE schemes and our scheme with regard to security and efficiency.

Some previous CP-ABBE schemes are compared with ours in terms of public key size, private key size, ciphertext size, and decryption pairings cost in Table 2, access structure, full security, recipient anonymity, and hardness assumption in Table 3. Pairing denotes the decryption pairings cost. Hardness is hardness assumption. "m" and "h" are respectively used to denote the total number of attributes and users in the system. "n" and "k" represent the number of attributes in an access structure and an attribute list, respectively. "N" is maximum number of wildcard in an access structure; "m'" is maximum size of objective attribute set allowed to be associated with ciphertext.

Table 2: Efficiency comparison among different CP-ABBE schemes

Scheme	Public parameter size	Private key size	Ciphertext size	Pairing
[1]	$\mathcal{O}(m'+h)$	$\mathcal{O}(k)$	$\mathcal{O}(n)$	$\mathcal{O}(n)$
[20](Scheme 2)	$\mathcal{O}(m+h)$	$\mathcal{O}(N)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$
[16]	$\mathcal{O}(m+h)$	$\mathcal{O}(h+k)$	$\mathcal{O}(n)$	$\mathcal{O}(n)$
[25]	$\mathcal{O}(log(h)+m)$	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(n)$
Ours	$\mathcal{O}(m+h)$	$\mathcal{O}(h)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$

Table 3: Security comparison among different CP-ABBE schemes

Scheme	Access Structure	Full Security	Recipient Anonymity	Hardness
[1]	LSSS	No	No	n-BDHE, MEBDH
[20](Scheme 2)	AND+wildcard	No	No	n-BDHE
[16]	LSSS	Yes	No	Static
[25]	AND	No	No	n-BDHE
Ours	AND	Yes	Yes	Static

In Table 2, it is quite obvious to see that our scheme is efficient in that the ciphertext size and the costs of decryption pairing do not depend on the number of attributes. Furthermore, our scheme only needs four decryption pairing computations, $e(D_1 D_{3,j'}, C_2)$, $e(D_2, C_3)$, $e(D_2, C_1)$, and $e(D_4, C_2)$, respectively.

In Table 3, it is apparent to see that only the proposed scheme provide recipient anonymity. Recipient anonymity is an important property for encryption schemes. Recalling the example in Section 1, an intermediate user can determine receiver set by running the DDH-test. To make up for the loophole, the proposed scheme adds a random number to each part of the ciphertexts such that each side of the equation contains different random numbers, which can prevent both access structure DDH-test and user index DDH-test. In addition, our scheme adopts AND-gate access structure and achieves full security. The security of the scheme is reduced to the static assumptions.

7 Conclusions

In this paper, a recipient anonymous ciphertext-policy attribute-based broadcast encryption (CP-ABBE) scheme is introduced. In the proposed scheme, the adversary cannot learn any information about the access structure and the broadcast list just from public parameters and ciphertexts. In addition, the proposed scheme enjoys high efficiency and achieves full security in the standard model.

A drawback of the new scheme is that our access structure is restricted, where it only supports AND-gate on multi-valued attributes. So the future works are to construct a recipient anonymous CP-ABBE scheme with more flexible access structure that is holding up high efficiency under a stronger security model.

Acknowledgments

This study was supported by the Nature Science Foundation of China (61472307, 61402112, 61100165, 61100231), Natural Science Basic Research Plan in Shaanxi Province of China (2016JM6004).

References

[1] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in *Third International Conference on Pairing-based Cryptography (Pairing'09)*, pp. 248–265, 2009.

[2] A. Balu and K. Kuppusamy, *Privacy Preserving Ciphertext Policy Attribute Based Encryption*, Springer Berlin Heidelberg, 2010.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE Symposium on Security and Privacy (SP'07)*, pp. 321–334, 2007.

[4] P. S. Chung, C. W. Liu, and M. S. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments," *International Journal of Network Security*, vol. 16, no. 1, pp. 1–13, 2014.

[5] B. Dan, E. J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," *Lecture Notes in Computer Science*, vol. 3378, pp. 325–341, Springer, 2005.

[6] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," *International Journal of Applied Cryptography*, vol. 5451, no. 1, pp. 13–23, 2009.

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

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.

[9] 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.

[10] J. Lai, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding CP-ABE," in *International Conference on Information Security Practice and Experience*, pp. 24–39, 2011.

[11] 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.

[12] C. C. Lee, P. S. Chung, M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231–240, July 2013.

[13] K. Lee and H. L. Dong, "Adaptively secure broadcast encryption under standard assumptions with better efficiency," *IET Information Security*, vol. 9, no. 3, pp. 149–157, 2014.

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

[15] M. Li, X. Xu, R. Zhuang, and C. Guo, "Identity-based broadcast encryption schemes for open networks," in *Ninth International Conference on Frontier of Computer Science and Technology*, pp. 104–109, 2015.

[16] Q. Li and F. Zhang, "A fully secure attribute based broadcast encryption scheme," *International Journal of Network Security*, vol. 17, no. 3, pp. 263–271, 2015.

[17] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage", *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.

[18] D. Lubicz and T. Sirvent, "Attribute-based broadcast encryption scheme made efficient," in *Cryptology in Africa International Conference on Progress in Cryptology*, pp. 325–342, 2008.

[19] H. Ma, T. Peng, Z. Liu, "Directly revocable and verifiable key-policy attribute-based encryption for large universe," *International Journal of Network Security*, vol. 19, no. 2, pp. 272–284, 2017.

[20] T. V. X. Phuong, G. Yang, W. Susilo, and X. Chen, *Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key*, 2015.

[21] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *International Conference on Theory and Applications of Cryptographic Techniques*, pp. 457–473, 2005.

[22] B. Waters, *Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions*, Springer Berlin Heidelberg, 2009.

[23] L. Zhang, Q. Wu, and Y. Mu, *Anonymous Identity-Based Broadcast Encryption with Adaptive Security*, Springer International Publishing, 2013.

[24] Y. Zhao, P. Fan, H. Cai, Z. Qin and H. Xiong, "Attribute-based encryption with non-monotonic access structures supporting fine-grained attribute revocation in M-healthcare," *International Journal of Network Security*, vol. 19, no. 6, pp. 1044–1052, 2017.

[25] Z. Zhou and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption: extended abstract," in *ACM Conference on Computer and Communications Security (CCS'10)*, pp. 753–755, 2010.

[26] Z. Zhou, D. Huang, and Z. Wang, "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 126–138, 2015.

Biography

Leyou Zhang is a professor in the school of mathematics and statistics at Xidian University, Xi'an China. He received his PhD from Xidian University in 2009. From Dec. 2013 to Dec. 2014, he is a research fellow in the school of computer science and software engineering at the University of Wollongong. His current research interests include network security, computer security, and cryptography.

Hongjian Yin is a master degree student in the school of mathematics and statistics, Xidian University. His research interests focus on computer and network security.