GO-CP-ABE: group-oriented ciphertext-policy attribute-based encryption

Yang Li
Fujian Provincial Key Laboratory of Network Security and Cryptology,
School of Mathematics and Computer Science,
Fujian Normal University,
Fuzhou, China
Email: 1175168008@qq.com

Xiaoling Tao*
Key Laboratory of Cognitive Radio and Information Processing,
University of Electronic Technology,
Guilin 541004, China
and
Guangxi Colleges and Universities Key Laboratory of
Cloud Computing and Complex Systems,
Guilin University of Electronic Technology,
Guilin 541004, China
Email: txl@guet.edu.cn
*Corresponding author

Wei Wu
Fujian Provincial Key Laboratory of Network Security and Cryptology,
School of Mathematics and Computer Science,
Fujian Normal University,
Fuzhou, China
Email: weiwu81@gmail.com

Joseph K. Liu
Faculty of Information Technology,
Monash University, Australia
Email: ksliu9@gmail.com

Abstract: We introduce a variant of ciphertext-policy attribute-based encryption called group-oriented ciphertext-policy attribute-based encryption (GO-CP-ABE). In the new notion, message is encrypted under an access structure over attributes and users are described by their attributes. In addition, users are divided into different groups and each user belongs to only one group. Users within the same group can merge their attributes to decrypt successfully, if the union of their attributes satisfies the access structure embedded in the ciphertext. But users from different groups cannot realise this cooperative decryption. We define the security model of GO-CP-ABE and present an efficient design by revising an existing CP-ABE scheme.

Keywords: attribute-based encryption; group-oriented; access structure; cooperative decryption.


Biographical notes: Yang Li received his Bachelor’s degree from the School of Institute of Electrical and Information Engineering, Hubei University of Automotive Technology, China in 2013. He is currently a graduate student at the Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, China. His research interests include cryptography and information security.

Xiaoling Tao received her MS in Computer Application Technology from the Guilin University of Electronic Technology, Guilin, China in 2008 and became a faculty member of this university in 2000. She is currently an Associate Professor at the school of information and communication,
formulas over attributes are attached to ciphertexts. On the contrary, in KP-ABE schemes are designed to be collusion-resistant, which is believed as an critical property for building attribute-based cryptographic access control systems. The property of collusion-resistance disables users to decrypt ciphertexts by collusion. Namely, users can pool their attributes, but they cannot decrypt the ciphertexts if none of them is able to satisfy the encryption policy individually. However, this property is not always preferable in practical applications. As an example, ABE can be used to realise fine-grained secure sharing of personal health record (PHR) in cloud computing. In a nutshell, one’s health records are encrypted by CP-ABE and the encrypted records are uploaded to the cloud. Anyone, such as doctors, friends and insurance company staffs, is able to decrypt and retrieve the records if his/her attributes satisfy the access policy. As all health-related systems, ABE-based PHR systems are required to support ‘break-glass’ operations and ensure that encrypted health records can be decrypted in emergency situations. However, a special case exists in the ABE-based PHR systems. For example, a patient’s PHR is encrypted under an access structure (‘dermatologist’ and ‘gastroenterologist’), but there is no doctor who is a specialist in both dermatosis and cardiopathy. In this case, two doctors need to decrypt the record collaboratively. As a result, a normal ABE scheme cannot be used in this scenario. Motivated by this observation, the notion of group collaboration was proposed for the first time in group-oriented attribute-based encryption (GO-ABE), and this is also the motivation of our paper. Then, in Li et al. (2015), the concept of group collaboration was used in signature. Compared with normal ABE, in GO-ABE, an added feature is that users within the same group can decrypt ciphertexts by merging their attributes (and private keys). The decryption would be successful if the union of their attributes satisfies the access policy, but users from different groups cannot decrypt ciphertexts by collusion. The scheme proposed in Li et al. (2014) only supports threshold formula, rather than an expressive one. Based on this observation, we aim to propose a design of group-oriented ciphertext-policy attribute-based encryption (GO-CP-ABE) supporting more expressive formulas.
1.1 Our contributions

In this paper, we propose the concept of GO-CP-ABE with more expressive formulas. Compared with the GO-ABE with threshold structure, the scheme proposed in this paper supports monotone access tree structure. In our scheme, users within the same group can pool their decryption keys to decrypt a ciphertext encrypted under an access structure which none of them may be able to satisfy the access structure individually, but users from different groups cannot make it. We provide a concrete construction of our concept based on the CP-ABE scheme in Waters (2011). Our decryption algorithm requires less number of bilinear pairing operations than the original algorithm presented in Waters (2011). Besides, we prove the security of our scheme. Specifically, the security of our scheme can be reduced to the decisional $q$-parallel BDHE problem.

1.2 Organisation

The remainder of our paper is organised as follows. In Section 2, we present related work. Section 3 is devoted to the preliminaries required by this paper. In Section 4, we describe the definition of GO-CP-ABE. In Section 5, we give a detailed description of our scheme. We then prove the security of our scheme in Section 6. In section 7, we analyse the efficiency of our scheme in terms of time complexity. Section 8 concludes this paper.

2 Related work

Sahai and Waters (2005) first put forward the concept of ABE and also introduced a scheme called fuzzy identity-based encryption (FIBE). The scheme of FIBE builds upon several ideas from identity-based encryption (IBE) (Boneh and Franklin, 2001; Cocks, 2001; Shamir, 1984). ABE is a new encryption method, compared with the encryption in traditional public key cryptography, such as IBE (Luo, 2015; Wang et al., 2015). In ABE, user’s private keys and ciphertexts are associated with a set of attributes and a policy over attributes. Anyone is able to decrypt a ciphertext if there is a ‘match’ between his/her private key and the ciphertext. The original ABE system introduced by Sahai and Water (2005) is a threshold ABE system in which the ciphertext is labelled with a set of attributes $\alpha$ and the user’s private key is not only associated with a threshold parameter $\kappa$ but associated with another set of attributes $\beta$. A user can decrypt a ciphertext if and only if at least $\kappa$ attributes overlap between attribute sets $\alpha$ and $\beta$. One of the primary motivations for this was to design an error-tolerant or FIBE scheme that could use biometric identities. The primary drawback of the threshold ABE introduced by Sahai and Waters (2005) is that the threshold semantics is not very expressive and therefore is not suitable for designing more general systems.

Goyal et al. (2006) clarified the concept of ABE into KP-ABE and CP-ABE. In recent years, a great number of ABE schemes have been proposed.

- KP-ABE (such as Goyal et al., 2006; Ostrovsky et al., 2007; Attrapadung et al., 2011; Hohenberger and Waters, 2013). Goyal et al. (2006) introduced the idea of a more general KP-ABE. In KP-ABE, the private key is associated with a policy and the ciphertext is associated with a set of attributes. The construction of Goyal et al. (2006) can be viewed as an extension of the Sahai and Waters (2005) technique where instead of embedding a Shamir (1979) secret sharing scheme in the private key, the authority embeds a more general secret sharing scheme for the monotonic access tree. To enable more flexible access control policy, Ostrovsky et al. (2007) presented a KP-ABE scheme that supports non-monotone access structure. Recently, KP-ABE has been widely used in cloud storage (Yu et al., 2010a; Lee et al., 2013; Li et al., 2013) to protect the data security. In 2014, Hohenberger and Waters proposed a design of online/offline attribute-based encryption.

- CP-ABE (such as Bethencourt et al., 2007; Lewko et al., 2010; Yu et al., 2010b). In contrast, in CP-ABE, attributes are used to label the user’s private key and the policy over attributes is attached to ciphertext. The first CP-ABE scheme that allows any monotone access structures with the security proof in the generic bilinear group model was proposed by Bethencourt et al. in 2007. In 2011, Lai et al. proposed a scheme of hiding the access structure associated with ciphertexts. Now, CP-ABE has a wide range of applications, such as social networking sites and electronic medical systems (Qin et al., 2015; Yan et al., 2016).

In order to further enrich the application of ABE, a new variant of ABE has been proposed. It is called GO-ABE (Li et al., 2014). Compared with normal ABE, an added feature is that users within the same group can decrypt by merging their attributes (and private keys). The decryption would be successful if the union of their attributes satisfies the access policy. But users from different groups cannot make it. However, the scheme proposed in Li et al. (2014) only supports a threshold formula, rather than an expressive one.

3 Preliminaries

In this part, we first briefly review the bilinear pairings. Then, we present a definition of monotone access structure. Finally, we give some background information on linear secret sharing scheme and state the complexity assumption we use for our proof of security.

3.1 Bilinear pairings

We briefly present a few facts about groups with efficiently computable bilinear pairings. Let $G_1$ and $G_2$ be two multiplicative cycle groups of prime order $p$. $g$ is a generation of $G_1$, $e$ is a bilinear pairing, $e: G_1 \times G_1 \rightarrow G_2$, has the following properties:
Bilinearity: \( e(g^a, g^b) = e(g, g)^{ab} \) for any \( a, b \in \mathbb{Z}_p^* \)

Non-degeneracy: \( e(g, g) \neq 1 \)

Computability: There is an efficient algorithm to compute \( e(a, v) \) for all \( a, v \in G_1 \). The bilinear pairings, such as modified Weil or Tate pairings, can be obtained from certain elliptic curves (Boneh et al., 2001).

### 3.2 Access structure

**Definition 3.1:** [Access structure (Beimel, 1996)] Let \( \{P_1, P_2, \ldots, P_n\} \) be a set of parties. A collection \( \mathcal{A} \subseteq 2^{\{1, 2, \ldots, n\}} \) is monotone if \( \forall B, C: \text{if } B \subseteq C \text{ then } C \in \mathcal{A} \). An access structure is a collection \( \mathcal{A} \) of non-empty subsets of \( \{P_1, P_2, \ldots, P_n\} \); i.e., \( \mathcal{A} \subseteq 2^{\{1, 2, \ldots, n\}} \setminus \{\emptyset\} \). The sets in \( \mathcal{A} \) are called the authorised sets, and the sets not in \( \mathcal{A} \) are called the unauthorised sets.

In our scheme, we restrict our attention to monotone access structure.

### 3.3 Linear secret sharing schemes

**Definition 3.2:** (Linear secret sharing schemes (LSSS)) A secret-sharing scheme \( \Pi \) for the access structure \( \mathcal{A} \) over a set of attributes \( S \) is called linear if it satisfies the following properties:

1. The shares for each attribute form a vector over \( \mathbb{Z}_p^* \).
2. For each access structure \( \mathcal{A} \) over \( S \), there exists a matrix \( \mathcal{M} \) with \( l \) rows and \( n \) columns called the share-generating matrix for \( \Pi \). For all \( i = 1, \ldots, l \), a function \( \rho(i) \) is defined such that \( \mathcal{M} \) is the matrix with attributes from \( S \). When we consider the column vector \( \vec{v} = (s, r_2, \ldots, r_n) \), where \( s \in \mathbb{Z}_p^* \) is the secret to be shared, and \( r_2, \ldots, r_n \in \mathbb{Z}_p^* \) are randomly chosen, then \( \mathcal{M} \vec{v} \) is the vector of \( l \) shares of the secrets \( s \) according to \( \Pi \). The share \( (\mathcal{M} \vec{v})_i \) belongs to \( \rho(i) \).

It is shown in Beimel (1996) that every linear secret sharing scheme according to the above definition also enjoys the linear reconstruction property, defined as follows: Suppose that \( \Pi \) is a linear secret sharing scheme for the access structure \( \mathcal{A} \). Let \( \mathcal{A} \subseteq \mathcal{Y} \) be any authorised set, and let \( I \subset \{1, 2, \ldots, l\} \) be defined as \( I = \{i: \rho(i) \in \mathcal{A}\} \). Then, there exist constants \( \{o_i \in \mathbb{Z}_p^*\}_{i \in \mathcal{A}} \) such that, \( \{o_i \mathcal{M}_i \}_{i \in \mathcal{I}} \) are valid shares of secret \( s \) according to \( \Pi \), then \( \Sigma_{i \in \mathcal{I}} o_i \mathcal{M}_i = s \).

Furthermore, it has been proved in Beimel (1996) that these constants \( \{o_i\} \) can be found in polynomial-time in the size of share-generating matrix \( \mathcal{M} \).

### 3.4 Complexity assumption

**Definition 3.3:** (Decisional parallel bilinear Diffie-Hellman exponent (BDHE) assumption) Let \( a, s \in \mathbb{Z}_p^* \) be chosen at random and \( g \) be a generator of group \( G_1 \) of prime order \( p \). The decision \( q \)-BDHE introduced by Boneh et al. (2005) that no probabilistic polynomial-time adversary \( \mathcal{A} \) can distinguish the \( e(g, g)^{\alpha i} = e(g, g)^{\beta i} \) from a random element \( R \in G_2 \) with more than a non-negligible advantage when given \( \vec{y} = (g^\alpha, g^\beta, g^\alpha^2, \ldots, g^\alpha^p, g^\beta) \). The advantage of an algorithm \( \mathcal{B} \) in solving decisional \( q \)-BDHE is defined as follows:

\[
\Pr_{\vec{y}, R}[\mathcal{B}(\vec{y}, R) = 0] - \Pr_{\vec{v}}[\mathcal{B}(\vec{v}) = 0] \geq \epsilon
\]

### 4 Definitions of GO-CP-ABE

In GO-CP-ABE, we divide users into different groups. There is no user belonging to two or more groups. Like CP-ABE the ciphertext is encrypted under an access structure and user’s private key is associated with attributes. Only users from the same group can merge their private keys to decrypt ciphertexts, but users from different groups cannot make it. In other words, users from the same group are able to cooperate with each other to decrypt ciphertexts encrypted under an access structure satisfied by the union of their attributes. But users from different groups cannot collude to decrypt ciphertexts. A GO-CP-ABE scheme consists of four algorithms and is described as follows:

1. **Setup(U):** This is a randomised algorithm that takes a security parameter and an attribute universe as input. It outputs the public parameters \( PK \) and a master key \( MK \).

   \( (PK, MK) \leftarrow \text{Setup(U)} \).

2. **Enc(PK, M, Y):** The encryption algorithm takes as input the public parameters \( PK \), a message \( M \) and an access structure \( Y \) over the universe of the attributes. This algorithm will encrypt \( M \) and produce a ciphertext \( CT \) such that users from the same group will be able to decrypt \( CT \) if the union of their attributes satisfies the access structure \( Y \). We assume the ciphertext implicitly contains \( Y \).

   \( CT \leftarrow \text{Enc}(PK, M, Y) \).

3. **KeyGen(MK, S, g, PK):** The key generation algorithm takes as input the master key \( MK \), a group identifier \( g \), an attribute set \( S \) and the public parameters \( PK \). It outputs a private key \( SK_s \).

   \( SK_s \leftarrow \text{KeyGen}(MK, S, g, PK) \).

4. **Decrypt(PK, CT, U^k, SK_{iS}):** The decryption algorithm takes as input the public parameters \( PK \), a ciphertext \( CT \) that was encrypted under an access structure \( Y \), and a set of users (each with an attribute set \( S^i \), \( i = 1, 2, \ldots, N \)) from the same group \( g \). Let \( SK_{iS} \) be the private key of each user of attribute set \( S^i \). The algorithm can
decrypt the CT and output a message $M$, if $U^k$ satisfies the access structure $\Upsilon$, where $U^k = S_k^5 \cup S_k^3 \cup \ldots \cup S_k^5$. $M \leftarrow \text{Decrypt}\left(\mathcal{PK}, \mathcal{CT}, \mathcal{SK}_{U^k}, U\right)$. Here, $\mathcal{SK}_{U^k} = \{\mathcal{SK}_{S_k^5}, \mathcal{SK}_{S_k^3}, \ldots, \mathcal{SK}_{S_k^5}\}$ is the set of private keys of cooperating users.

### 4.1 Security model for GO-CP-ABE

**Setup**: The challenger runs the Setup algorithm of the GO-CP-ABE, and gives the public parameters $\mathcal{PK}$ to the adversary $\mathcal{A}$. 

**Phase 1**: The adversary $\mathcal{A}$ makes repeated private key queries. Let each query be $(S_i, g_i)$, where $S_i$ denotes the attribute set and $g_i$ denotes the group identifier. The attribute set $U^k = S_k^5 \cup S_k^3 \cup \ldots \cup S_k^5$ denotes the union of the attribute sets with the same group identifier $g_i$ that appeared in $\mathcal{A}$’s queries.

**Challenge**: The adversary $\mathcal{A}$ submits two equal length messages $M_0$ and $M_1$. In addition, the adversary $\mathcal{A}$ selects a challenge access structure $\Upsilon^\prime$ such that none of the union attribute sets $U^k$ from Phase 1 satisfies the access structure $\Upsilon^\prime$. The challenger flips a random coin $\beta$, and encrypts $M_{\beta}$ under $\Upsilon^\prime$. The ciphertext $\mathcal{CT}$ is given to the adversary $\mathcal{A}$.

**Phase 2**: Phase 1 is repeated with the restriction that none of the union attribute sets $U^k$ satisfies the access structure $\Upsilon^\prime$.

**Guess**: The adversary $\mathcal{A}$ outputs a guess $\beta'$ of $\beta$.

The advantage of the adversary $\mathcal{A}$ in this game is defined as $|\Pr[\beta' = \beta] - \frac{1}{2}|$.

**Definition 4.1**: A GO-CP-ABE scheme is secure in the above security model if all polynomial time adversaries have at most a negligible advantage in above game.

### 5 Our construction

Recall that we want to design an ABE scheme in which a ciphertext encrypted under an access structure $\Upsilon$ can be decrypted only by users from the same group $g$ if the union of their attribute set $U^k$ satisfies the access structure $\Upsilon$. Users from different groups cannot make it. So our scheme provides the security against collusion attack.

As described previously, in order to embody the concept of group collaboration, the basic method of our construction is to add a group identifier to reflect this feature. In order to achieve this goal, we modify the existing scheme (Waters, 2011) instead of building a new ABE scheme from scratch. When producing private keys, the authority associates a random value $\rho$ for each user from the same group $g$. Below we give a description of our construction. Let $G_1$ be a bilinear group of prime order $p$, and let $g$ be a generator of $G_1$. In addition, let $e: G_1 \times G_1 \to G_2$ denote the bilinear map. A security parameter, $k$, will determine the size of the group. In our construction, the encryption algorithm will take as input a LSSS access matrix $M$ and distribute a random exponent $s \in \mathbb{Z}_p$. Our construction as follows:

- **Setup($U$)**: This is a randomised algorithm that takes as input the number of attributes in the system. It then chooses a bilinear group $G_1$ of prime order $p$ with generator $g$ and $U$ random group elements $h_1, ..., h_U \in G_1$ that are associated with the $U$ attributes in the system. In addition, it will choose two random exponents $\alpha, \beta \in \mathbb{Z}_p$.

The published public parameters are:

$$\mathcal{PK} = g, e(g, g)^\alpha, g^\alpha, h_1, ..., h_U.$$ 

The master secret key is:

$$\mathcal{MSK} = g^\alpha.$$ 

- **Enc($\mathcal{PK}, M, (M, \rho)$)**: The encryption algorithm first takes as input the public parameters $\mathcal{PK}$, a message $M$ and $(M, \rho)$. $M$ is a $l \times n$ matrix converted from the access structure $\Upsilon$ and $\rho$ is a function that associates each row of the $M$ with an attribute. Next, the algorithm randomly selects an exponent $s$, then chooses a random vector $\bar{v} = (x, y_2, ..., y_n) \in \mathbb{Z}_p^n$. These values will be used to share the encryption exponent $s$. For $i = 1$ to $l$, it calculates $\lambda_i = \bar{v} \cdot M_i$, where $M_i$ is the vector corresponding to the $i^{th}$ row of $M$. Finally, the algorithm chooses randomly $\eta_1, ..., \eta_l \in \mathbb{Z}_p$.

The ciphertext $\mathcal{CT}$ is published as follows:

$$\mathcal{CT} = \left(\mathcal{C} = Me(g, g)^\rho, C_0 = g^\alpha, (C_1, D_1), ..., (C_l, D_l)\right).$$  

Here, for $i = 1, ..., l$, $C_i = g^{\alpha \lambda_i} h_i^\eta_i, D_i = g^\alpha$.

- **KeyGen($\mathcal{MK}, S^k, \rho, \mathcal{PK}$)**: To generate a private key for the attribute set $S^k$ from the group $g$, randomly chooses a $t_g \in \mathbb{Z}_p$ for a group $g$, then takes an input the master key $\mathcal{MK}$ and public parameters $\mathcal{PK}$. It creates the private key as follows:

$$\mathcal{K} = g^\alpha g^{\alpha \omega}, L = g^{\omega}, \forall s \in S^k, K_s = h_s^\omega.$$ 

- **Dec($\mathcal{PK}, \mathcal{CT}, U^k, \mathcal{SK}_{U^k}$)**: Given a ciphertext, $\mathcal{CT}$, encrypted under an access structure $(M, \rho)$ and the union of user attributes $U^k$, where $U^k = S_k^5 \cup S_k^3 \cup \ldots \cup S_k^5$. Let $\mathcal{SK}_{S^k}$ denotes the private key of attribute set $S^k$. So $\mathcal{SK}_{U^k}$ is the private key of attribute set $U^k$. Suppose that $U^k$ satisfies the access structure and let $I \subset [1, 2, ..., l]$ be $I = \{i : \rho(i) \in U^k\}$. Then, let $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ be a set of constants such
that if $\lambda_i$ are valid shares of any secret $s$ according to $M$, then $\sum_{i=1}^m a_i \lambda_i = s$.

The ciphertext can be decrypted by computing the following:

$$e(C_0, K) = e\left(\prod_{i=1}^m C_i^{a_i}, L\right) = e\left(\prod_{i=1}^m e(D_i, K_h), e(g^{a_0}, g^{a_m})\right)$$

$$= e\left(g^{a_0}, g^{a_m}\right) e\left(g^{-a_0}, \prod_{i=1}^m h_i\right) \prod_{i=1}^m e(g^{a_i}, h_i)$$

$$= e(g, g)^{a_a}$$

The decryption algorithm can then divide out this value from $C$ and obtain the message $M$.

6 Proof of security

In this section, we give a security proof of our scheme in the selective security model. The security of our scheme can be reduced to the hardness of decisional $q$-parallel BDHE problem.

Theorem 1: Suppose the decisional $q$-parallel BDHE assumption holds. Then no polynomial-time adversary can selectively break our scheme with a challenge matrix of size $l \times n$, where $l, n \leq q$.

Proof: Suppose there is an adversary $A$ with non-negligible advantage $\epsilon = Adv_A$ in the selective security model against our construction. Additionally, suppose it selects a challenge matrix $M$ where both dimensions are at most $q$. Below, we build an algorithm to solve the decisional $q$-parallel BDHE problem by running $A$ as the subroutine in the following:

Init. The simulator $B$ takes in a $q$-parallel BDHE challenge $y, T$. The adversary selects the challenge access structure $(M, \rho^{*})$, where $M$ has $n$ columns.

Setup. The simulator randomly chooses $\alpha' \in \mathbb{Z}_p$ and implicitly sets $\alpha = \alpha' + a_{q+1}$ by letting $e(g, g)^{\alpha} = e(g^{a_0}, g^{a_m})e(g, g)^{\alpha'}$.

The simulator sets the elements $h_i, ..., h_l$ as follows.

For each $x$, for $1 \leq x \leq U$, begin by choosing a random $x_i$. Let $X$ denote the set of indices $i, j$ such that $\rho^{*} (i)$ is $x$. The simulator sets $h_i$ as:

$$h_i = g^{a_0} \prod_{j \in X} g^{a_0} = g^{a_0} g^{a_0} \cdots g^{a_0}.$$ 

Note that if $X = \emptyset$ then we have $h_i = g^{a_0}$. All the parameters are distributed randomly due to the random value $x_i$.

Phase 1. $A$ issues queries for private keys for any attribute set. Suppose the adversary $A$ makes a request for secret key for an attribute set $S$, in the group $g$. The simulator chooses a random $r \in \mathbb{Z}_p$. Then, it finds a vector $\tilde{v} = (w_1, ..., w_r) \in \mathbb{Z}_p^r$ such that $w_1 = 1$ and for all $i$ where $\rho^{*} (i) \in S$, we have that $\tilde{v}_i M^{*}_{i} = 0$. Such a vector must exist according to the definition of LSSS.

The simulator implicitly defines the same $\tilde{t}_i$ for users in group $g$ as:

$$r + w_1 a_i + w_2 a_i a_i^{*} + \cdots + w_r a_i a_i^{* r}.$$ 

It is performed by setting $L$ as follows:

$$L = g^r \prod_{i=1}^{n} \left( g^{a_i} \right)^{w_i} = g^{a_i}.$$ 

According to the definition of $\tilde{t}_i$, we have that $g^{a_i}$ contains a term of $g^{a_i a_i^{*}}$, which will cancel out with the unknown term in $g^{a_i}$ when creating $K$. The simulator $B$ calculates $K$ as follows:

$$K = g^{a_i} g^{a_i} \prod_{i=1}^{n} \left( g^{a_i a_i^{*}} \right)^{w_i}.$$ 

Next, we compute $K_i$ for all $i$ such that $\rho^{*} (i) = x$. The simulator computes $K_i$ as follows:

$$K_i = L^{*} \prod_{i \in X} \left( g^{a_i} s^{a_i^{*}} \right)^{w_i} \prod_{i \in X} \left( g^{a_i a_i^{*}} \right)^{w_i}.$$ 

According to the above process, the simulator $B$ can calculate private key for the attribute set $S$.

Challenge. The adversary gives two messages $M_{0}, M_{1}$ to the simulator $B$. The simulator $B$ flips a coin $b$. It calculates $C = M_{b} \bar{e}(g^{a_i}, g^{a_i})$ and $C' = g^{a_i}$.

The difficult part is to simulate $C_i$ values since it contains term that we must cancel out. However, the simulator can choose the secret splitting, such that these cancel out. Intuitively, the simulator $B$ will choose random $y_2^{*}, ..., y_r^{*}$ and share the secret using the vector $\tilde{v} = (s, sa^{*}, sa^{*} + y_2^{*}, ..., sa^{*+1} + y_r^{*}) \in \mathbb{Z}_p^r$.

Moreover, the simulator chooses random values $n_1^{*}, ..., n_r^{*} \in \mathbb{Z}_p$.

For $i = 1, ..., n$, we define $R_i$ as the set of all $k \neq i$ such that $\rho^{*} (i) = \rho^{*} (k)$. That is, the set of all other row indices that have the same attribute as row $i$. Then the challenge ciphertext components are computed as follows:

$$D_i = g^{a_i} g^{a_i} \omega^{i}, C_i = L_i K_i.$$ 

Here,
\[ L_i = (g^{b_{ii}})^{-z_i} \prod_{j=1}^{r_i} \prod_{k=1}^{m} (g^{s_{ij}(h_i/b_k)})^{M_{ij}} \]
\[ K_i = h_i^{b_i} \prod_{j=2}^{r_i} (g^{s_{ij}})^{M_{ij}} \]

**Phase 2.** The simulator repeats Phase 1 under the same condition as Phase 1.

**Guess.** The adversary \( A \) will submit a guess \( \beta' \) of \( \beta \). If \( \beta = \beta' \) the simulator \( B \) will output \( \mu = 0 \) to indicate that \( T = e(g, g)^{\mu R} \). Otherwise, it will output \( \mu = 1 \) to denote that \( T \) is a random group element in \( \mathbb{G}_2 \).

If \( \mu = 0 \) then the adversary sees an encryption of \( M_\beta \). The advantage in this situation is \( \text{Adv}_A \) by definition. Therefore, we have \( \Pr[B(\bar{y}, T = e(g, g)^{\mu R}) = 0] \) as follows:

\[ \Pr[B(\bar{y}, T = e(g, g)^{\mu R}) = 0] = \frac{1}{2} + \text{Adv}_A. \]

If \( \mu = 1 \), the adversary \( A \) gains no information about \( \beta \). Consequently, we have \( \Pr[B(\bar{y}, T = R) = 0] = \frac{1}{2} \). Therefore, \( B \) can win the decisional \( q \)-parallel BDHE game with non-negligible advantages.

## 7 Complexity analysis

In this section, we aim to compare with (Li et al., 2014) from function and analyse the efficiency of the proposed GO-CP-ABE scheme in terms of time complexity.

- **Function comparison.** Compared with scheme (Li et al., 2014) with threshold structure, our scheme supports monotone access tree structure. Specifically, our scheme can provide a fine-grained access control for users. From the view of classification of ABE, our scheme belongs to CP-ABE, and the scheme (Li et al., 2014) belongs to KP-ABE. Both of the schemes support group cooperation. Namely, each user belongs to a certain group; users from the same group can pool their attributes to decrypt ciphertext.

- **Efficiency.** In the scheme of GO-CP-ABE, the number of public key is \( U + 3 \) and the size of the ciphertext is \( 2(1 + l) \). The number of bilinear pairing operations in decryption algorithm is \( k + 2 \), where \( k \) is the minimum number of attributes needed to satisfy the access structure. Below, we will give the concrete time cost of our scheme in encryption and decryption.

### 7.1 Simulation results

We simulate the performance of GO-CP-ABE by evaluating the time cost in encryption and decryption based on the pairing-based library (version 0.5.12). The details of the platform we use are shown in Table 1.

<table>
<thead>
<tr>
<th>OS</th>
<th>Ubuntu 10.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Pentium(R) Dual-Core</td>
</tr>
<tr>
<td>Memory</td>
<td>2.97 GB RAM</td>
</tr>
<tr>
<td>Hard disk</td>
<td>500 G/5,400 rpm</td>
</tr>
<tr>
<td>Programming language</td>
<td>C</td>
</tr>
</tbody>
</table>

In the experiment, we design three different monotone access tree structures. In the first scenario (the simple one), the access structure is \( Y_1: \ 'A \ AND(D \ OR(B \ AND \ C))' \). Alice and Bob are in the same group. Specifically, Alice with attributes \{A, B\}, and Bob with attributes \{B, C\}. The union of their attributes satisfy the access structure \( Y_1 \). Thus, they can pool their attributes to decrypt ciphertext encrypted under \( Y_1 \). The experiment shows that the time costs of our scheme in encryption and decryption are 0.129729 s and 0.108481 s.

In the second scenario (the complex one), the access structure is \( Y_2: \ '((A \ OR \ B)\ AND(C \ AND \ D)) \ AND(E \ OR \ F)\) \). Alice with attributes \{A, C\} and Bob with attributes \{D, E\}. The time costs of our scheme in encryption and decryption are 0.193378 s and 0.131719 s.

In the third scenario (the most complex one), the access structure is \( Y_3: \ '((A \ AND \ B)\ OR(C \ OR \ D)) \ AND(E \ OR \ F)\ AND(G \ AND \ H)\) \). Alice with attributes \{A, B, C\} and Bob with attributes \{D, E\}. The time costs of our scheme in encryption and decryption are 0.193378 s and 0.131719 s.
\{E, G, H\}. The experiment shows that the time costs of our scheme in encryption and decryption are 0.199432 s and 0.159991 s. The simulation results of our scheme are listed in Table 2. The construction of LSSS matrix for \(Y_1\) and \(Y_2\) are shown in Figure 1 and Figure 2, respectively. Figure 3 is the LSSS matrix we used in the experiment. From Table 2 and Figure 3, we can see that a more complex access structure results in a higher time cost.

**Figure 3** LSSS matrices of \(Y_1\), \(Y_2\) and \(Y_3\)

<table>
<thead>
<tr>
<th>Access structure</th>
<th>Encryption</th>
<th>Decryption</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Y_1): (A \land (D \lor (B \land C)))</td>
<td>0.129727 s</td>
<td>0.108481 s</td>
<td>0.238213 s</td>
</tr>
<tr>
<td>(Y_2): ((A \lor B) \land (C \land D) \land (E \lor F))</td>
<td>0.193378 s</td>
<td>0.121719 s</td>
<td>0.315098 s</td>
</tr>
<tr>
<td>(Y_3): ((A \lor D) \land (B \lor C \lor D) \land (E \lor F) \land (G \land H))</td>
<td>0.199432 s</td>
<td>0.159991 s</td>
<td>0.369213 s</td>
</tr>
</tbody>
</table>

### 8 Conclusions

In this paper, we proposed the concept of GO-CP-ABE with more expressive formulas. This can be viewed as an improvement over the threshold GO-ABE scheme in Li et al. (2014). Specifically, in our new notion, message is encrypted under an expressive access structure over attributes and users are described by their attributes. In addition, users are divided into different groups and each user belongs to only one group. Users within the same group can merge their attributes to decrypt successfully, if the union of their attributes satisfies the access structure embedded in the ciphertext. But users from different groups cannot decrypt successfully. We also gave a construction by extending an existing CP-ABE scheme in Waters (2011), together with a rigorous security proof.

### Acknowledgements

This work is supported by National Natural Science Foundation of China (61472083, 61402110, 61363006), Fok Ying Tung Education Foundation (141065), Program for New Century Excellent Talents in Fujian University (JA14067), Distinguished Young Scholars Fund of Fujian (2016J06013), and Fujian Normal University Innovative Research Team (No. IRTL1207).

### References


