Noname manuscript No.
(will be inserted by the editor)

IR-CP-ABE: Identity Revocable Ciphertext-Policy Attribute-Based Encryption for Flexible Secure Group-Based Communication

Weijia Wang · Bing Li · Zhijie Wang · Qiuxiang Dong · Dijiang Huang

Received: date / Accepted: date

Abstract Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is an access control mechanism over encrypted data and well suited for secure group-based communication. However, it also suffers from the following problem, *i.e.*, it is impossible to build all desired groups. For example, if two group members have exactly the same attributes, how to construct a group including only one of the two members? Obviously, attributes alone cannot distinguish these two members, therefore existing CP-ABE solutions do not work. To address this issue, in this paper, we present a new CP-ABE scheme (called IR-CP-ABE) that incorporates an Identity-based Revocation capability. With IR-CP-ABE, an access policy will be constructed by not only group members' attributes but also their identities. To build a group, first, build a candidate group based on all desired group members' attributes; second, remove undesired members by revoking their identities. By evaluating the security and efficiency of a proposed construction, we show that the IR-CP-ABE scheme is secure and efficient for practical applications.

Keywords Group-based Secure Communication · Ciphertext-Policy Attribute-Based Encryption · ID Revocation · Security · Efficiency

Weijia Wang
the School of Science, Beijing Jiaotong University, Beijing, China
E-mail: fauthor@example.com

Bing Li, Zhijie Wang, Qiuxiang Dong, Dijiang Huang
Arizona State University, Tempe, AZ, US
E-mail: {bingli5, zwang134, qiuxiang.dong, dijiang}@asu.edu

1 Introduction

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) provides a scalable mechanism of encrypting data where the data owner defines the access policy, and then the data user needs to hold the attribute set to decrypt the ciphertext. Thus far, CP-ABE mainly focuses on secure file-sharing in cloud computing. The main benefit derived from CP-ABE is the ability of untrusted or semi-trusted cloud servers to store sensitive or confidential files while data owners still preserve the access control over these files. Another context in which CP-ABE would be beneficial is in distributed computing and peer-to-peer networks. Different from cloud computing, there exists no centralized server after system setup. In these large-scale networks, access control and security can become untenably complex. Individual users are sending data to groups of recipients. Recipients, based on different levels of trust, need-to-know, and other identity attributes, are entitled to access different data streams. CP-ABE is the perfect candidate for these scenarios. Senders can encrypt data using an access policy, send it out widely, and all the intended recipients will be able to decrypt the data while unintended recipients will not. CP-ABE drastically reduces the complexity of providing fine-grained access control for large-scale, high-security-demanding peer-to-peer networks.

As promising as it is, one major issue of using CP-ABE in practice is that it is impossible to construct all desired groups. CP-ABE cannot pinpoint individual recipients when they all have the same attributes. For example, there is an attribute set $\{student, male, female\}$ assigned to a group of students $\{Alice, Bob, Carol\}$. Since all the students share the same attributes, it is obvious that by only using the given attributes, there is no way to construct a group which only includes $\{Alice, Bob\}$ or $\{Bob, Carol\}$.

To address this issue, in this paper, we present a new Identity (ID) Revocable CP-ABE scheme (IR-CP-ABE) that incorporates an ID-based Revocation capability. IR-CP-ABE addresses this issue by incorporating the identity revocation capability into the CP-ABE scheme, where attributes are allocated normally according to users' privilege, and a unique ID is assigned to each user. During the key generation procedure, the user's ID is incorporated into the private key of each attribute. It works by first specifying attribute literals in conjunctive/disjunctive normal forms as an attribute policy tree to cover the recipients of the target group with the minimum redundancy, and then removing the unintended recipients by incorporating ID revocation. As such, it makes it possible to build all possible groups that may not be constructed solely by attributes.

We herein illustrate how IR-CP-ABE makes it possible where the group construction cannot solely rely on attribute literals. In **Fig. 1**, $A_i (i \in [1, 3])$ denotes the i-th attribute and $I_j (j \in [1, 3])$ denotes the j-th user's identity. This example shows that it is impossible to construct the user groups $\{I_1, I_3\}$, $\{I_2, I_3\}$ by using only attributes. Nonetheless, with the help of identity revocation, they can be expressed in the form of *Sum-Of-Product Expression* as follows:

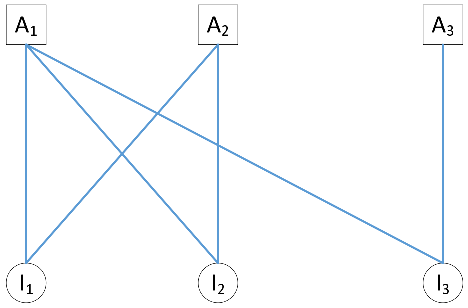

Fig. 1 An example of subgroups cannot be established based on users' assigned attributes.

$$\{I_1, I_3\} = A_1 \overline{I}_2,$$

$$\{I_2, I_3\} = A_1 \overline{I}_1.$$

Lewko *et al.* propose a similar approach to constructing groups more flexibly. Their focus is on public key encryption schemes and Key-Policy ABE schemes. In this paper, we focus on flexible group construction in CP-ABE schemes. CP-ABE scheme supporting negated clauses [1,**?**,**?**] allows to revoke individuals by conjunctively adding the AND of negations of undesired members' identities. In all of these schemes, each identity is mapped to an individual attribute. However, all these schemes lack efficacy in bandwidth terms. Among these schemes, the scheme in [2] is the most efficient one. Through efficiency comparison (Section 4), we can conclude that our scheme is more efficient. Our research contributions are summarized as follows:

- By incorporating identities into the secure group construction, IR-CP-ABE is capable to construct some groups which are impossible to construct by previous CP-ABE schemes.
- IR-CP-ABE simplifies the secure group construction by reducing the number of attributes and/or attribute policy trees;
- The presented solution is proved to be secure under selective security model;
- Performance analysis and evaluation shows that IR-CP-ABE does not increase the storage, computation, and communication complexity of the existing CP-ABE schemes, thus practical for real-world applications.

The remainder of this paper is organized as follows. Section 2 presents the system preliminaries and security assumptions. Section 3 elaborates the construction of IR-CP-ABE. Section 4 presents the performance analysis and evaluation. Section 5 discusses the related work. Section 6 concludes this paper. The security proof is presented in Appendix A.

2 Preliminaries

In this section, we present the foundations that are required to build the IR-CP-ABE scheme.

2.1 Access Structure

Access Structure We follow the same definition presented in [3]. Let $\{P_1, P_2, \ldots, P_n\}$ be a set of parties. A set $\mathbb{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}}$ is monotone if $\forall B, C$ if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$. An access structure is a set $\mathbb{A}$ of non-empty subsets of $\{P_1, P_2, \ldots, P_n\}, i.e., \mathbb{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}} \backslash \{\emptyset\}$. The sets in $\mathbb{A}$ are defined as authorized sets, and sets that do not belong to $\mathbb{A}$ are defined as unauthorized sets.

Roles of parties are determined by their attributes. Hence, the access structure $\mathbb{A}$ includes the authorized attributes. Although we only focus on monotone access structure in this paper, our proposed techniques can also be applied to the case having the "NOT" logic of using an attribute in the security policy to confine a group of users, and the number of attributes in the system will be doubled accordingly. We hereafter use the access structure $\mathbb{A}$ to refer to a monotone access structure.

2.2 Linear Secret Sharing Schemes

Linear Secret Sharing Schemes (LSSS) [3] plays an important role in our schemes, and it is defined as follows:

Linear Secret Sharing Schemes(LSSS). A secret sharing scheme $\mathcal{I}$ over a set of parties is linear over $\mathbb{Z}_p$ if

- the shares for each party form a vector over $\mathbb{Z}_p$;
- a share-generating matrix for $\mathcal{I}$ has l rows and n columns. For all $i = 1, \ldots, l$ and each i-th row of M, we define $\rho(i)$ as the party labeling row i. For the column vector $v = (s, r_2, r_3, \ldots, r_n)$ where $s \in \mathbb{Z}_p$ is the shared secret, and Mv is the vector of l shares of the secret s for $\mathcal{I}$ where $r_2, r_3, \ldots, r_n \in \mathbb{Z}$ are randomly chosen and the share $(Mv)_i$ belongs to party ρ_i.

According to the definition described above, every linear secret sharing-scheme according to the above definition also enjoys the linear reconstruction property and it is defined as follows: assume $\mathcal{I}$ is an LSSS for the access structure $\mathbb{A}$ and $S \in \mathbb{A}$ is an authorized set, we define $I \subset \{1, 2, \ldots, l\}$ as $I = \{i : \rho_i \in S\}$. Accordingly, there exist constants $\{w_i \in |\}_{i \in I}$ such that $\sum_{i \in I} w_i \lambda_i = s$ where $\{\lambda_i\}$ are valid shares of any secret s and these constants $\{w_i\}$ can be derived in polynomial time.

2.3 Algorithms of IR-CP-ABE

The ID-revocable ABE is comprised of four algorithms, and the implications of the algorithm are elaborated as below:

- *Setup*$(\mathcal{U}, \mathcal{I})$: Given the attribute universe description $\mathcal{U}$ and the identity set $\mathcal{I}$, the TA publishes its public key PK but keeps its master key MSK;
- *KeyGen*(MSK, S, ID): Given MSK, the user's ID and attribute set S, the TA issues private keys SK;
- *Encrypt*$(PK, (M, \rho), \mathcal{M}, \{ID_j\})$: Given the public key PK, the LSSS matrix M and its corresponding mapping ρ to each attribute, the message $\mathcal{M}$ and the revoked ID set $\{ID_j\}$, the data owner generates the ciphertext and sends it to a public place for storage;
- *Decrypt*(CT, SK): Given the ciphertext CT, the data user derives the message $\mathcal{M}$ by decrypting with its private key SK.

2.4 Security Model for ID Revokable CP-ABE

We now present the full security definition for IR-CP-ABE systems which derive from the security definitions for identity-based revocation framework [4] and general CP-ABE systems [5]. In the IR-CP-ABE security definition, we need to consider stronger adversaries whose attributes satisfy the attribute access policy of the challenge ciphertext but whose identity is in the revocation set.

Init: The adversary $\mathcal{A}$ commits to the challenge access structure $\mathbb{A}^*$ and the revoked identity set $\boldsymbol{ID}^*$ and send this to the challenger.

Setup: The challenger runs the setup algorithm. The master secret key MSK is kept secret and the public parameters PK are given to $\mathcal{A}$.

Phase1: The adversary $\mathcal{A}$ makes repeated private key queries $(\mathbf{S_i}, ID_i)_{i \in [1, q_1]}$ where if $\mathbf{S}_i$ satisfies $\mathbb{A}^*$ then the identity $ID_i = ID^*$.

Challenge: $\mathcal{A}$ submits two equal length messages $\mathcal{M}_0$ and $\mathcal{M}_1$. In addition, the adversary gives a challenge LSSS access structure $\mathbb{A}^* = \left(M^*, \rho^*\right)$ and a set $\boldsymbol{ID}^*$ of revoked identities such that $\boldsymbol{ID}^*$ must include all identities that were queried. The challenger picks up a random coin b, and encrypts $\mathcal{M}_b$ under the access structure $\mathbb{A}^*$ and the revoked identity set $\boldsymbol{ID}^*$. Then the challenge ciphertext CT^* is sent to $\mathcal{A}$.

Phase2: Repeat **Phase1** with the restriction that the queried sets of $(\mathbf{S_i}, ID_i)_{i \in [q_1+1, q]}$ where if $\mathbf{S}_i$ satisfies $\mathbb{A}^*$ then the identity $ID_i = ID^*$.

Guess: The adversary outputs a guess bit b' of b. Define $\mathrm{Adv}_{\mathcal{A}} = |\Pr[b' = b] - \frac{1}{2}|$ as the advantage of the adversary $\mathcal{A}$ winning the game.

The advantage of an adversary $\mathcal{A}$ in this game is defined as $\Pr[b' = b] - \frac{1}{2}$. Note that the above model can easily be extended to handle chosen-ciphertext attacks by allowing for decryption queries in **Phase 1** and **Phase 2**.

Definition 1 An identity revocable CP-ABE scheme is secure if all polynomial time adversaries have at most a negligible advantage in the above game.

We say that a system is selectively secure if we add an Init stage before setup where the adversary commits to the challenge access structure M and the revocation ID set S. All of our constructions will be proved secure in the selective security model.

2.5 Bilinear Maps

Bilinear pairings are the basic operations in our framework. Assume $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups with order q generated by a Bilinear Diffie-Hellman (BDH) parameter generator $\mathcal{G}$. Correspondingly we set up a bilinear map system $\mathbb{S} = (q, \mathbb{G}, \mathbb{G}_T, e)$ where e denotes a computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ with the following properties:

– Bilinearity: $\forall G, W \in \mathbb{G}, \forall a, b \in \mathbb{Z}, e(G^a, W^b) = e(G, W)^{ab}$;
– Non-degeneracy: G and W are the generators of $\mathbb{G}$, $e(G^a, W^b) \neq 1$;
– Computability: $e(G, W)$ is efficiently computable.

In our system,we set $G = W$ and make $G, \mathbb{G}, \mathbb{G}_T$ public.

2.6 Assumptions

We now present the q-type complexity assumptions that we will depend on to prove the security of our systems. This assumption is formulated on prime order bilinear groups, denoted by modified decisional q-parallel BDHE, which is similar to the Decisional Parallel Bilinear Diffie-Hellman Exponent (q-parallel BDHE) Assumption [5].

The modified decisional q-parallel Bilinear Diffie-Hellman problem is defined as follows. We select a group $\mathbb{G}$ of prime order p and a random generator g of $\mathbb{G}$ and random exponents $a, s, b_1, b_2, \cdots, b_q \in \mathbb{Z}_p$. Given

$$\begin{aligned}\mathbf{y} =& \{g, g^s, g^a, \cdots, g^{(a^q)}, , g^{(a^{q+2})}, \cdots, g^{(a^{2q})}\} \\ & \forall_{1 \le j \le q} g^{a/b_j}, \cdots, g^{a^q/b_j}, , g^{a^{q+2}/b_j}, ..., g^{a^{2q}/b_j} \\ & \forall_{1 \le j \le q} g^{a \cdot s/b_j}, \cdots, g^{(a^q \cdot s/b_j)},\end{aligned}$$

it is hard to distinguish $e(g, g)^{a^{q+1}s} \in \mathbb{G}_T$ from any random element R in $\mathbb{G}_T$.

An algorithm $\mathcal{B}$ that outputs $z \in \{0, 1\}$ has advantage ϵ in solving the modified decisional q-parallel BDHE in $\mathbb{G}$ if

$$|\Pr[\mathcal{B}(\mathbf{y}, T = e(g, g)^{a^{q+1}s}) = 0] - \Pr[\mathcal{B}(\mathbf{y}, T = R) = 0]| \ge \epsilon.$$

The modified decisional q-parallel BDHE assumption holds if only negligible advantage exists for any algorithm to solve the modified decisional q-parallel BDHE problem in polynomial time.

Proof: We briefly show that the M-q-parallel-BDHE assumption is generically secure. The generic proof template of BBG [5] and [6] is used. Using the terminology from BBG we need to show that $f = a^{q+1}s$ is independent of the polynomials P and Q. We set $Q = \{1\}$ since all given terms are in the bilinear group. P is set to be

$$P = \{1, s, \forall_{i \in [1,2q], j \in [1,q], i \neq q+1} a^i, a^i/b_j, a^i \cdot s/b_j\}.$$

We could choose a generator u and set $g = u^{\prod_{j \in [1,q]} b_j}$. All the above terms are substituted by a set of polynomials with the maximum degree $3q + 1$.

Now, we check whether f is symbolically independent of any two polynomials in P and Q. To realize f from P and Q, a term of the form $a^{m+1}s$ is needed. It can be seen that no such terms can be realized from the product of any two polynomials $p, p' \in P$. To form such a term, a polynomial with a single factor of s is needed. If s is used as p then p' has to be a^{q+1} which doesn't exist in P. If we set $p = a^i \cdot s/b_j$, there always exists b_j, which cannot be canceled. Based on the BBG framework, we can conclude that the M-q-parallel-BDHE assumption is generically secure.

3 Our Construction

In this section, we present the IR-CP-ABE scheme. We first present the construction of one ID revocation, which is represented as OIDR-CP-ABE. A multiple-ID revocation scheme, denote as MIDR-CP-ABE, is also presented. The main challenge to achieve multiple-ID revocation is due to the collusion problem. Our scheme can prevent collusion issue, and the security proofs are presented in Appendix A.

3.1 Notation Illustration

Before going into details of each scheme, we first present common notations that are used in the following sections, as shown in **TABLE 1**.

Table 1 Notations.

α	a random element chosen by a Trusted Authority (TA) from $\mathbb{G}$.
A_x	the x-th row of A.
b	a random element chosen by TA from $\mathbb{G}$.
g	the generator of the multiplicative cyclic group $\mathbb{G}$.
$\mathcal{I}$	the identity set defined in the system, $\lvert\mathcal{I}\rvert = n$.
l	the number of attributes involved in the encryption process.
$\mathcal{M}$	a message to be encrypted by the system.
M	an $l \times n$ matrix as part of an LSSS access structure.
m	the number of attributes defined in the system.
n	the number of identities in the system.
p	the prime order of the multiplicative cyclic group $\mathbb{G}$
ρ	a function that associates rows of M to attributes.
r	the number of identities involved in the encryption process .
S	the set of attributes created for a specific user.
$\mathcal{U}$	the attribute set defined in the system, $\lvert\mathcal{U}\rvert = m$.

3.2 One-ID Revocation for CP-ABE Scheme (OIDR-CP-ABE)

a. **Setup**$(\mathcal{U}, \mathcal{I})$

The *Setup* algorithm takes an attribute set $\mathcal{U}$ and an identity set $\mathcal{I}$ as inputs, where $|\mathcal{U}| = m$ and $|\mathcal{I}| = 1$. It chooses a group $\mathbb{G}$ of prime order p, a generator g, and m random group elements $h_1, h_2, \cdots, h_m \in \mathbb{G}$ that are associated with the m attributes in the system. It also chooses random exponents $\alpha, b \in \mathbb{Z}_p$.

Therefore, the public key is in the form:

$$PK = \{g, g^b, g^{b^2}, e(g,g)^\alpha, h_1^b, \cdots, h_m^b\}.$$

The Master secret key is in the form:

$$MSK = \{\alpha, b\}.$$

b. $\mathbf{KeyGen}(\mathbf{MSK}, \mathbf{S}, \mathbf{ID})$

S is the attribute set of user $ID \in \mathcal{I}$. *KeyGen* algorithm chooses a random $t \in \mathbb{Z}_p$ and generates secret keys for user ID as follows:

$$SK = (K = g^\alpha g^{b^2 t}, \{K_x = (g^{b \cdot ID} h_x)^t\}_{\forall x \in S}, L = g^{-t}).$$

c. $\mathbf{Encrypt}(\mathbf{PK}, (\mathbf{M}, \rho), \mathcal{M}, \mathbf{ID_1})$

Encrypt algorithm takes inputs as an LSSS access structure (M, ρ) and the function ρ associates each row of M to corresponding attributes. ID_1 is the identity to be revoked. Let M be an $l \times n'$ matrix. The *Encrypt* algorithm first chooses a random vector $v = (s, y_2, \cdots, y_{n'}) \in \mathbb{Z}_p^{n'}$. These values will be used to share an encryption exponent s. For $k \in [1, l]$, it calculates $\lambda_k = v \cdot M_k$, where M_k is the vector corresponding to the x-th row of M. Then, for message $\mathcal{M}$, the ciphertext is presented as follows:

$$C = \mathcal{M} e(g,g)^{\alpha s},$$

$$C_0 = g^s,$$

$$\hat{C} = \{C_k^* = g^{b \cdot \lambda_k}, C_k' = (g^{b^2 \cdot ID_1} h_{\rho(k)}^b)^{\lambda_k}\}_{k \in \{1, \cdots, l\}}.$$

d. $\mathbf{Decrypt}(\mathbf{CT}, \mathbf{SK})$

CT is the input ciphertext with access structure (M, ρ) and SK is a private key for a set S:

$$CT = (C, C_0, \hat{C}, (M, \rho)).$$

Suppose that S satisfies the access structure and let $I \subset \{1, 2, ..., l\}$ be defined as $I = \{i : \rho(i) \in S\}$. 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 $\Sigma_{i \in I} \omega_i \lambda_i = s$. If the identity ID combined in the SK is not equal to the revocation identity ID_1 in the ciphertext, we can perform

$$\begin{aligned}
&\frac{e(C_0, K)}{(\prod_{i \in I}[e(K_{\rho(i)}, C_i^*) \cdot e(L, C_i')]^{\omega_i})^{1/(ID - ID_1)}} \\
&= e(g^s, g^\alpha g^{b^2 t}) / (\textstyle\prod_{i \in I}[e((g^{b \cdot ID} h_{\rho(i)})^t, g^{b \cdot \lambda_i}) \\
&\quad \cdot e(g^{-t}, (g^{b^2 \cdot ID_1} h_{\rho(i)}^b)^{\lambda_i})]^{\omega_i})^{1/(ID - ID_1)} \\
&= e(g,g)^{\alpha s} \cdot e(g,g)^{b^2 st} / e(g,g)^{b^2 t \sum_{i \in I} \lambda_i \omega_i} \\
&= e(g,g)^{\alpha s}.
\end{aligned}$$

Theorem 1 *Suppose the modified decisional q-parallels BDHE challenge assumption holds. Then no poly-time adversary can selectively break OIDR-CP-ABE with a challenge matrix of size $l \times n$, where $n < q$.*

Proof Based on the attack model presented in Section 2.4, to prove the security of our scheme, we utilize the reduction technology **Fig. 2**, where a simulator is constructed to simulate a real attributed-based cryptography environment for attackers by answering their queries and programming the challenge access structure and revoked identity into the public parameters. Compared with the CP-ABE security model [5], where one only considers the situation that the queried attribute set does not satisfy the challenge policy, during the private key query procedure (Phase 1), our scheme considers that the queried attribute set can satisfy the challenge policy when the corresponding user is a revoked user. To address the presented security challenges, we construct a new matrix nearly equal to the challenge LSSS matrix and use it to simulate the environment. In the follows, we present the detailed proof.

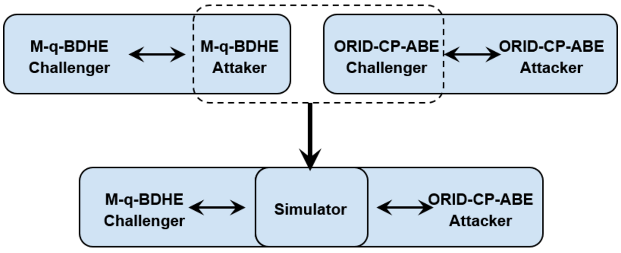

Fig. 2 The reduction of our scheme to the M-q-BDHE problem.

Suppose there is an adversary $\mathcal{A}$ with non-negligible advantage $\epsilon = \mathrm{Adv}_{\mathcal{A}}$ in the selective security game against our scheme. Moreover, suppose $\mathcal{A}$ attacks our construction with one revoked user and a challenge matrix M where both dimensions are less than q. We show how to build simulator, $\mathcal{B}$, that plays the modified decisional q-parallel $BDHE$ problem.

Init The simulator takes in a modified decisional q-parallel $BDHE$ challenge $\{\overrightarrow{Y}, T\}$. Then the adversary declares the revoked user ID_c and gives the simulator the challenge access structure (M, ρ), where M has n (less than q) columns. Let the challenge matrix $M = (\overrightarrow{M_1}, \overrightarrow{M_2}, ..., \overrightarrow{M_l})^T$, where each row vector $\overrightarrow{M_i} = (M_{i,1}, M_{i,2}, ...M_{i,n})$ for $1 \leq i \leq l$.

Setup The simulator chooses a random value α' and lets $e(g,g)^{\alpha} = e(g,g)^{\alpha'} e(g^a, g^{a^q})$ to implicitly set $\alpha = \alpha' + a^{q+1}$. Moreover, it implicitly sets $b = a$ by computing the public parameters as $g, g^b = g^a, g^{b^2} = (g^{a^2})$ To embed the revocation identification ID_c and the challenge access structure in the public parameters $h_1, ..., h_U$, we regard the challenge matrix M as a row vector set and divide it into three subsets M', M'' and M''' such that $M' \cup M'' \cup M''' = M$ and $M' \cap M'' \cap M''' = \emptyset$. Specifically, M', M'' and M''' are initially set to be empty set. Define the n-dimension vectors $\overrightarrow{e} = (1, 0, ..., 0)$ and $\overrightarrow{\mu} = (a^2, a^3, ..., a^{n+1})$. For $i = 1$ to l, if $\overrightarrow{M_i}$ is linearly independent on M' and $\overrightarrow{e}$ cannot be linearly expressed by $M' \cup \{\overrightarrow{M_i}\}$, then we merge $\overrightarrow{M_i}$ into M'; if $\overrightarrow{M_i}$ is linearly independent on M' and $\overrightarrow{e}$ can be linearly expressed by $M' \cup \{\overrightarrow{M_i}\}$, then we merge $\overrightarrow{M_i}$ into M'''; if $\overrightarrow{M_i}$ is linearly dependent on M', then we merge $\overrightarrow{M_i}$ into M''. As a result, M' is a linear independent vector group while each vector in M'' can be linearly expressed by M'. Although $\overrightarrow{e}$ cannot be spanned by M', it can be linearly expressed by M' merged with each vector in M'''. Therefore, each vector in M can be linearly expressed by $M' \cup \{\overrightarrow{e}\}$.

Next, we describe how the simulator "programs" the public parameters $h_1^b, h_2^b, ..., h_U^b$. Let X denote the set of indices i, such that $\rho(i) = x$. Assume that there are m vectors in M' and let $M' = (\overrightarrow{M_1'}, \overrightarrow{M_2'}, ..., \overrightarrow{M_m'})^T$. For each $i \in X$, its corresponding row vector $\overrightarrow{M_i}$ can be written as $\varepsilon_{i0}\overrightarrow{e} + \varepsilon_{i1}\overrightarrow{M_1'} + \varepsilon_{i2}\overrightarrow{M_2'} + ... + \varepsilon_{im}\overrightarrow{M_m'}$, where $(\varepsilon_{i0}, \varepsilon_{i1}, ..., \varepsilon_{im}) \in Z_p^m$. For each $\overrightarrow{M_i}$, we define a corresponding vector $\overrightarrow{M_i^*}$, where $\overrightarrow{M_i^*} = \varepsilon_{i1}\overrightarrow{M_1'} + \varepsilon_{i2}\overrightarrow{M_2'} + ... + \varepsilon_{im}\overrightarrow{M_m'}$. As a result, we get a new vector group $M^* = (\overrightarrow{M_1^*}, \overrightarrow{M_2^*}, ..., \overrightarrow{M_l^*})$ and each $\overrightarrow{M_i^*}$ in is in the span of M'. By choosing a random value z_x, the simulator programs h_x and h_x^b as:

$$\begin{aligned} h_x =& g^{z_x} g^{-aID_c} \prod_{i \in X} g^{(\varepsilon_{i1}\overrightarrow{M_1'} + \varepsilon_{i2}\overrightarrow{M_2'} +, ..., + \varepsilon_{im}\overrightarrow{M_m'}) \cdot \overrightarrow{\mu}/b_i} \\ =& g^{z_x} g^{-aID_c} (\prod_{i \in X} \prod_{j=1}^{n} g^{M_{i,j}^* a^{j+1}/b_i}). \\ h_x^b =& g^{z_x} g^{-a^2 ID_c} (\prod_{i \in X} \prod_{j=1}^{n} g^{M_{i,j}^* a^{j+1}/b_i}). \end{aligned}$$

If X is an empty set, we set $h_x^b = g^{z_x}$. Then the simulator publishes the above parameters $(g, g^b, g^{b^2}, h_1^b, h_2^b, \cdots, h_U^b, e(g,g)^{\alpha})$ as the public key. We observe that the public parameters are distributed randomly as the real system and both the revoked identification and the challenge matrix are reflected in the simulation's construction of the parameter h_x^b.

Phase I The algorithm simulates to answer private key queries. In the general CP-ABE security model [5], one only considers the weaker case, that is, the queried attribute set does not satisfy the challenge policy. In this case, to construct the private keys for the unsatisfied attribute set I, the simulator can find a vector $\overrightarrow{\omega} = (\omega_1, ..., \omega_n) \in \mathbb{Z}_p$ such that $\omega_1 = -1$ and $\overrightarrow{\omega} \cdot \overrightarrow{M_i} = 0$ for all i where $\rho(i) \in I$. Such a vector must exist, as the target vector $\overrightarrow{e}$ is not in the span of the rows in the challenge matrix M corresponding to the set I [5]. As a result, by utilizing $\overrightarrow{\omega}$, the simulator can cancel the item of the form $g^{a^{q+1}}$ in generating the queried private key.

In our selective security model, we consider a stronger adversary querying the private key of an attribute set which satisfies the challenge policy. Due to the authorized attribute set, the above mentioned vector $\overrightarrow{\omega}$ with $\omega_1 = -1$ and $\overrightarrow{\omega} \cdot M_i = 0$ corresponding to the queried attribute set does necessarily not exist. To overcome the problem, at the beginning we program the public parameter h_x based on the challenged policy row subset M'. Since each $\overrightarrow{M_i^*}$ is in the span of M' while $\overrightarrow{e}$ is not in the span of M', we can still find a vector $\overrightarrow{\omega}$ with $\omega_1 = -1$ and $\overrightarrow{\omega} \cdot \overrightarrow{M_i^*} = 0$, where $1 \leq i \leq m$.

Therefore, the simulator selects a random value r and calculates the private key L as

$$L = g^{r + \overrightarrow{\omega} \cdot \overrightarrow{\nu}} = g^r \prod_{i=1,...,n} (g^{a^{q-i}})^{\omega_i},$$

which implicitly sets the randomness t as

$$t = r + \overrightarrow{\omega} \cdot \overrightarrow{\nu} = r + \omega_1 a^{q-1} + \omega_2 a^{q-2} +, ..., + \omega_n a^{q-n},$$

where $\overrightarrow{\nu} = (a^{q-1}, a^{q-2}, ..., a^{q-n+2})$.

By doing this, we can first cancel out the g^{q+1} that the simulator does not know with g^{α} in building the K component as

$$K = g^{\alpha'} g^{a^2 r} \prod_{i=0,...,n-2} (g^{a^{q+i}})^{\omega_i}.$$

Next, as $\overrightarrow{\omega}$ is orthogonal to each vector in M^* and the queried identity is equal to ID_c, we can prevent the appearance of the term of the form $g^{a^{q+1}}$ in building the private components K_x as:

$$\begin{aligned}K_x =&(g^{z_x} g^{a(ID_d-ID_c)} \prod_{i\in X} g^{\overrightarrow{M_i^*}\cdot\overrightarrow{\mu}/b_i})^{(r+\overrightarrow{w}\cdot\overrightarrow{\nu})}\\ =&g^{z_x(r+\overrightarrow{w}\cdot\overrightarrow{\nu})} g^{a(ID_d-ID_c)(r+\overrightarrow{w}\cdot\overrightarrow{\nu})}\\ &\cdot\prod_{i\in X} g^{(M_{i1}^* a^2+,...,+M_{in}^* a^n)(r+\omega_1 a^{q-1}+,...,+\omega_n a^{q-n})}\\ =&g^{z_x(r+\overrightarrow{w}\cdot\overrightarrow{\nu})} g^{a(ID_d-ID_c)(r+\overrightarrow{w}\cdot\overrightarrow{\nu})}\\ &\cdot\prod_{i\in X} g^{(M_{i1}^* a^2+,...,+M_{in}^* a^n)r}\\ &\cdot\prod_{i\in X}\prod_{j=1}^{n}\prod_{k=1,k\neq j}^{n} g^{M_{ij}^*\omega_k a^{q+j-k+1}}.\end{aligned}$$

Challenge In this phase, the adversary provides to the simulator two challenge messages $\mathcal{M}_0$,$\mathcal{M}_1$ with the challenge matrix M of dimension at most n columns.

First, The simulator flips a coin β and creates the ciphertext component $C = \mathcal{M}_\beta T \cdot e(g^s, g^{\alpha'})$. Then the simulator chooses random value $y_2', y_3', ..., y_n'$ and share the secret s using the vector

$$\overrightarrow{v} = (s, y_2', y_3', ..., y_n').$$

Next, it calculates

$$\begin{aligned}\lambda_k =&\overrightarrow{v}\cdot(\varepsilon_{k0}\overrightarrow{e} + \varepsilon_{k1}\overrightarrow{M_1'} + \varepsilon_{k2}\overrightarrow{M_2'} + ... + \varepsilon_{km}\overrightarrow{M_m'})\\ =&\overrightarrow{v}\cdot(\varepsilon_{k0}\overrightarrow{e} + \overrightarrow{M_k^*}).\end{aligned}$$

And it generates the ciphertext component C_k^* as:

$$C_k^* = g^{as(M_{k1}^*+\varepsilon_{k0})}\cdot\prod_{i=2}^{n} g^{M_{ki}^* y_i'}$$

For $k = 1, ..., n$, we define X_k as the set of the index i in such that $\rho(i) = \rho(k)$. Finally, the simulator builds the ciphertext component C_k' as:

$$\begin{aligned}C_k' =&(g^{a^2 ID_c} g^{z_x} g^{-a^2 ID_c} \prod_{i\in X_k} g^{\overrightarrow{M_i^*}\cdot\overrightarrow{\mu}/b_i})^{\lambda_k}\\ =&g^{z_x\lambda_k}\prod_{i\in X_k} g^{(M_{i1}^* a^2+M_{i2}^* a^3+,...,+M_{in}^* a^{n+1})\lambda_k/b_i}.\end{aligned}$$

Phase II Same as phase I.

Guess The adversary will eventually output a guess β' of β. The simulator then outputs 0 to guess that $T = e(g,g)^{sa^{q+1}}$ if $\beta' = \beta$; otherwise, it outputs 1 to indicate that it believes T is a random group element in $\mathbb{G}_T$. When T is a tuple the simulator $\mathcal{B}$ gives a perfect simulation so we have that

$$Pr[\mathcal{B}(\overrightarrow{X}, T = e(g,g)^{sa^{q+1}}) = 0] = \frac{1}{2} + Adv_{\mathcal{A}}.$$

When T is a random group element, the message M_β is completely hidden from the adversary and we have $Pr[\mathcal{B}(\overrightarrow{X}, T = R) = 0] = \frac{1}{2}$. Therefore, $\mathcal{B}$ can play the modified decisional q-parallels $BDHE$ game with non-negligible advantage.

3.3 Multiple-ID Revocation for CP-ABE Scheme (MIDR-CP-ABE)

a. **Setup**$(\mathcal{U}, \mathcal{I})$

The algorithm takes an attribute set $\mathcal{U}$ and an identity set $\mathcal{I}$ as input where $|\mathcal{U}| = m$ and $|\mathcal{I}| = n$. It chooses a group $\mathbb{G}$ of prime order p, a generator p and m random group elements $h_1, h_2, \cdots, h_m \in \mathbb{G}$ that are associated with the m attributes in the system. It also chooses random exponents $\alpha, b \in \mathbb{Z}_p$.

Therefore, the public keys are output as:

$PK = \{g, g^b, g^{b^2}, e(g,g)^\alpha, h_1^b, \cdots, h_m^b\}$.

The Master secret key is: $MSK = \{\alpha, b\}$.

b. **KeyGen**$(\mathbf{MSK}, \mathbf{S}, \mathbf{ID})$

S is the attribute set of user $ID \in \mathcal{I}$. The algorithm chooses a random $t \in \mathbb{Z}_p$ and derive the secret keys as follows:

$SK = (K = g^\alpha g^{b^2 t}, \{K_x = (g^{b\cdot ID} h_x)^t\}_{\forall x\in S}, L = g^{-t})$.

c. **Encrypt**$(\mathbf{PK}, (\mathbf{M}, \rho), \mathcal{M}, \mathbf{S})$

It takes the input as an LSSS access structure (M, ρ) and the function ρ associates rows of M to attributes. ID_j is assumed to be the identity which will be revoked. Let M be an $l \times n'$ matrix. The algorithm first chooses a random vector $v = (s, y_2, \cdots, y_{n'}) \in \mathbb{Z}_p^{n'}$. These values will be used to share the encryption exponent s. For $x \in [1, l]$, it calculates $\lambda_x = v \cdot M_x$, where M_x is the vector corresponding to the x-th row of M. Let $r = |S|$ and ID_j denote the j-th identity in S. The algorithm chooses random $\mu_1, ..., \mu_r \in \mathbb{Z}_p$ such that $\mu = \mu_1 + ... + \mu_r$. It generates the first part of ciphertext:

$$C = \mathcal{M}e(g,g)^{\alpha s\mu}, C_0 = g^{s\mu},$$

$$\begin{aligned}&C_{1,1}^* = g^{b\cdot\lambda_1\mu_1}, C_{1,1}' = (g^{b^2\cdot ID_1} h_{\rho(1)}^b)^{\lambda_1\mu_1}\\ &\cdots \qquad C_{l,1}^* = g^{b\cdot\lambda_l\mu_1}, C_{l,1}' = (g^{b^2\cdot ID_1} h_{\rho(l)}^b)^{\lambda_l\mu_1}\\ &C_{1,2}^* = g^{b\cdot\lambda_1\mu_2}, C_{1,2}' = (g^{b^2\cdot ID_2} h_{\rho(1)}^b)^{\lambda_1\mu_2}\\ &\cdots \qquad C_{l,2}^* = g^{b\cdot\lambda_l\mu_2}, C_{l,2}' = (g^{b^2\cdot ID_2} h_{\rho(l)}^b)^{\lambda_l\mu_2}\\ &\qquad\qquad \cdots\\ &C_{1,r}^* = g^{b\cdot\lambda_1\mu_r}, C_{1,r}' = (g^{b^2\cdot ID_r} h_{\rho(1)}^b)^{\lambda_1\mu_r}\\ &\cdots \qquad C_{l,r}^* = g^{b\cdot\lambda_l\mu_r}, C_{l,r}' = (g^{b^2\cdot ID_r} h_{\rho(l)}^b)^{\lambda_l\mu_r}.\end{aligned}$$

d. **Decrypt**$(\mathbf{CT}, \mathbf{SK})$

CT is the input ciphertext with access structure (M, ρ) and SK is a private key for a set S. Suppose that S satisfies the access structure and let $I \subset \{1, 2, ..., l\}$ be defined as $I = \{i : \rho(i) \in S\}$. 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 $\Sigma_{i \in I} \omega_i \lambda_i = s$. If the identity ID combined in the SK is not equal to the revocation identity ID_j in the ciphertext, we can perform

$$
\begin{aligned}
&\frac{e(C_0,K)}{\prod_{i\in I}(\prod_{j=1}^{r}[e(K_{\rho(i)},C^*_{i,j})\cdot e(L,C'_{i,j})]^{1/(ID-ID_j)})^{\omega_i}}\\
&= e(g^{s\mu}, g^{\alpha} g^{b^2 t}) / \textstyle\prod_{i \in I}(\prod_{j=1}^{r}[e((g^{b \cdot ID} h_{\rho(i)})^t, g^{b \cdot \lambda_i \mu_j})\\
&\quad \cdot e(g^{-t}, (g^{b^2 \cdot ID_j} h^b_{\rho(i)})^{\lambda_i \mu_j})]^{1/(ID-ID_j)})^{\omega_i}\\
&= e(g^{s\mu}, g^{\alpha}) \cdot e(g^{s\mu}, g^{b^2 t}) / \textstyle\prod_{i \in I}(\prod_{j=1}^{r}[e(g^{b \cdot ID \cdot t}, g^{b \cdot \lambda_i \mu_j})\\
&\quad \cdot e(h^t_{\rho(i)}, g^{b \cdot \lambda_i \mu_j}) \cdot e(g^{-t}, g^{b^2 \cdot ID_j \cdot \lambda_i \mu_j})\\
&\quad \cdot e(g^{-t}, h^{b \cdot \lambda_i \mu_j}_{\rho(i)})]^{1/(ID-ID_j)})^{\omega_i}\\
&= e(g,g)^{\alpha s \mu} \cdot e(g,g)^{b^2 s \mu t} / \textstyle\prod_{i \in I}(\prod_{j=1}^{r}[e(g^{b \cdot ID \cdot t}, g^{b \cdot \lambda_i \mu_j})\\
&\quad \cdot e(g^{-t}, g^{b^2 \cdot ID_j \cdot \lambda_i \mu_j})]^{1/(ID-ID_j)})^{\omega_i}\\
&= e(g,g)^{\alpha s \mu} \cdot e(g,g)^{b^2 s \mu t}\\
&\quad \cdot 1 / \textstyle\prod_{i \in I}(\prod_{j=1}^{r}[e(g,g)^{b^2 t \lambda_i \mu_j (ID-ID_j)}]^{1/(ID-ID_j)})^{\omega_i}\\
&= e(g,g)^{\alpha s \mu} \cdot e(g,g)^{b^2 s \mu t} / \textstyle\prod_{i \in I}(\prod_{j=1}^{r} e(g,g)^{b^2 t \lambda_i \mu_j})^{\omega_i}\\
&= e(g,g)^{\alpha s \mu} \cdot e(g,g)^{b^2 s \mu t} / \textstyle\prod_{i \in I}(e(g,g)^{(\sum_{j=1}^{r} \mu_j) b^2 t \lambda_i})^{\omega_i}\\
&= e(g,g)^{\alpha s \mu} \cdot e(g,g)^{b^2 s \mu t} / e(g,g)^{b^2 t \mu \sum_{i \in I} \lambda_i \omega_i}\\
&= e(g,g)^{\alpha s \mu}.
\end{aligned}
$$

Theorem 2 *Suppose the modified decisional q-parallels BDHE challenge assumption holds. Then no poly-time adversary can selectively break MIDR-CP-ABE with a challenge matrix of size $l \times n$ and r revocation IDs, where $r, n < q$.*

It is obvious that the public parameters and private key structure of MIDR-CP-ABE is same as those of OIDR-CP-ABE. Furthermore, the ciphertext structure of MIDR-CP-ABE is essentially an extension for that of OIDR-CP-ABE. Therefore here we can directly implant the proof of OIDR-CP-ABE with some replacements of one revocation ID to a revocation ID set summation. We present the proof briefly as following.

Proof Suppose $\mathcal{A}$ attacks our construction with a revoked user set and a challenge matrix M where both dimensions are less than q. We show how to build simulator, $\mathcal{B}$, that plays the modified decisional q-parallel $BDHE$ problem.

Init The simulator takes in a modified decisional q-parallel $BDHE$ challenge $\{\overrightarrow{Y}, T\}$. Then the adversary declares the revoked user set $(ID_{c1}, ID_{c2}, ..., ID_{cr})$ and gives the simulator the challenge access structure (M, ρ), where M has n (less than q) columns. Let $M = (\overrightarrow{M_1}, \overrightarrow{M_2}, \cdots, \overrightarrow{M_l})^T$, where each row vector $\overrightarrow{M_i} = (M_{i,1}, M_{i,2}, \cdots, M_{i,n})$ for $1 \leq i \leq l$.

Setup The simulator chooses a random value α' and lets $e(g,g)^{\alpha} = e(g,g)^{\alpha'} e(g^a, g^{a^q})$ to implicitly set $\alpha = \alpha' + a^{q+1}$. Moreover, it implicitly sets $b = a$ by computing the public parameters as $g^b = g^a$ and $g^{b^2} = (g^{a^2})$.

The challenge matrix M is divided into three subsets M', M'' and M''' such that $M' \cup M'' \cup M''' = M$ and $M' \cap M'' \cap M''' = \emptyset$. Their generation method is same as that in the proof of OIDR-CP-ABE so that each vector in M can be linearly expressed by $M' \cup \{\overrightarrow{e}\}$. Define the n-dimension vectors $\overrightarrow{e} = (1, 0, ..., 0)$. Let X denote the set of indices i, such that $\rho(i) = x$. Assume that there is m vectors in M' and let $M' = (\overrightarrow{M'_1}, \overrightarrow{M'_2}, ..., \overrightarrow{M'_m})^T$. For each $i \in X$, its corresponding row vector $\overrightarrow{M_i}$ can be written as $\varepsilon_{i0} \overrightarrow{e} + \varepsilon_{i1} \overrightarrow{M'_1} + \varepsilon_{i2} \overrightarrow{M'_2} + ... + \varepsilon_{im} \overrightarrow{M'_m}$, where $(\varepsilon_{i0}, \varepsilon_{i1}, ..., \varepsilon_{im}) \in Z_p^m$. For each $\overrightarrow{M_i}$, we define a corresponding vector $\overrightarrow{M_i^*}$, where $\overrightarrow{M_i^*} = \varepsilon_{i1} \overrightarrow{M'_1} + \varepsilon_{i2} \overrightarrow{M'_2} + ... + \varepsilon_{im} \overrightarrow{M'_m}$. As a result, we get a new vector group $M^* = (\overrightarrow{M_1^*}, \overrightarrow{M_2^*}, ..., \overrightarrow{M_l^*})$ and each $\overrightarrow{M_i^*}$ in it is in the span of M'. By choosing a random value z_x, the simulator program h_x^b as:

$$
\begin{aligned}
h_x =& g^{z_x} g^{-a \sum_{\iota=1}^{r} ID_{c_\iota}} \Big(\prod_{i \in X} \prod_{j=1}^{n} g^{M^*_{i,j} a^{j+1} / b_i}\Big).\\
h_x^b =& g^{z_x} g^{-a^2 \sum_{\iota=1}^{r} ID_{c_\iota}} \Big(\prod_{i \in X} \prod_{j=1}^{n} g^{M^*_{i,j} a^{j+1} / b_i}\Big).
\end{aligned}
$$

If X is null, we set $h_x^b = g^{z_x}$. Then the simulator publishes the above parameters as public key.

Phase I Since each $\overrightarrow{M_i^*}$ is in the span of M' while $\overrightarrow{e}$ is not in the span of M', we can still find a vector $\overrightarrow{\omega}$ with $\omega_1 = -1$ and $\overrightarrow{\omega} \cdot \overrightarrow{M_i^*} = 0$, where $1 \leq i \leq m$. The simulator selects a random value r' and calculates the private key L as

$$L = g^{r'} \prod_{i=1,\ldots,n} (g^{a^{q-i}})^{\omega_i},$$

$$K = g^{\alpha'} g^{a^2 r'} \prod_{i=0,\ldots,n-2} (g^{a^{q+i}})^{\omega_i},$$

implicitly setting the randomness t as $t = r' + \omega_1 a^{q-1} + \omega_2 a^{q-2} +, ..., +\omega_n a^{q-n}$, where $\overrightarrow{\nu} = (a^{q-1}, a^{q-2}, ..., a^{q-n+2})$. Next, we prevent the appearance of the term of the form $g^{a^{q+1}}$ in building the private components K_x as:

$$
\begin{aligned}
K_x =& g^{z_x(r+\overrightarrow{w}\cdot\overrightarrow{\nu})} g^{a(ID_d-\sum_{\iota=1}^{r} ID_{c_\iota})(r+\overrightarrow{w}\cdot\overrightarrow{\nu})} \\
&\cdot \prod_{i\in X} g^{(M_{i1}^{*}a^2+,...,+M_{in}^{*}a^n)r} \\
&\cdot \prod_{i\in X}\prod_{j=1}^{n}\prod_{k=1,k\neq j}^{n} g^{M_{ij}^{*}\omega_k a^{q+j-k+1}}.
\end{aligned}
$$

Challenge The adversary provides to the simulator $\mathcal{M}_0$,$\mathcal{M}_1$ with the matrix M of dimension at most n columns.

First, The simulator flips a coin β, chooses random values $\mu_1, \mu_2, ..., \mu_r$ such that $\nu = \nu_1 + \nu_2 + ... + \nu_r$, and creates the ciphertext component $C = \mathcal{M}_\beta(T \cdot e(g^s, g^{\alpha'}))^\nu$. Then the simulator chooses random value $y_2', y_3', ..., y_n'$ and share the secret s using the vector

$$\overrightarrow{v} = (s, y_2', y_3', ..., y_n').$$

Next, it calculates

$$
\begin{aligned}
\lambda_k =& \overrightarrow{v} \cdot (\varepsilon_{k0}\overrightarrow{e} + \varepsilon_{k1}\overrightarrow{M_1'} + \varepsilon_{k2}\overrightarrow{M_2'} + ... + \varepsilon_{km}\overrightarrow{M_m'}) \\
=& \overrightarrow{v} \cdot (\varepsilon_{k0}\overrightarrow{e} + \overrightarrow{M_k^*}).
\end{aligned}
$$

And it generates the ciphertext component C_k^* as:

$$C_{k,\gamma}^* = g^{as\nu_\gamma(M_{k1}^*+\varepsilon_{k0})} \cdot \prod_{i=2}^{n} g^{M_{ki}^* y_i'}$$

For $k = 1, ..., n$, we define X_k as the set of the index i in such that $\rho(i) = \rho(k)$. Finally, the simulator builds the ciphertext component C_k' as:

$$
\begin{aligned}
C_k' =& (g^{a^2\sum_{\iota=1}^{r} ID_{c_\iota}} g^{z_x} g^{-a^2\sum_{\iota=1}^{r} ID_{c_\iota}} \prod_{i\in X_k} g^{\overrightarrow{M_i^*}\cdot\overrightarrow{\mu}/b_i})^{\lambda_k\nu_\gamma} \\
=& g^{z_x\lambda_k\nu_\gamma} \prod_{i\in X_k} g^{(M_{i1}^*a^2+M_{i2}^*a^3+,...,+M_{in}^*a^{n+1})\lambda_k\nu_\gamma/b_i}.
\end{aligned}
$$

Phase II Same as phase I.

Guess The adversary will eventually output a guess β' of β. The simulator then outputs 0 if $\beta' = \beta$; otherwise, 1. When T is a tuple, $\mathcal{B}$ gives a perfect simulation so we have that

$$Pr[\mathcal{B}(\overrightarrow{X}, T = e(g,g)^{sa^{q+1}}) = 0] = \frac{1}{2} + Adv_{\mathcal{A}}.$$

When T is a random group element, M_β is completely hidden from the adversary and we have $Pr[\mathcal{B}(\overrightarrow{X}, T = R) = 0] = \frac{1}{2}$. So $\mathcal{B}$ can play the modified decisional q-parallel $BDHE$ game with non-negligible advantage.

4 Performance Evaluation

In this section, the two schemes proposed in this paper are evaluated in terms of their computation, storage, and communication performance. The evaluation is performed in three parts: Firstly, we analyze the performance complexity of presented revocation schemes compared to the original CP-ABE scheme. Secondly, we implement the IR-CP-ABE schemes based on PBC library [7]. A computation performance evaluation is conducted including comparison with CP-ABE scheme. Finally, we present an experimental study to show the benefit of using IR-CP-ABE scheme for secure group construction.

4.1 Computation, Storage, and Communication Complexity Analysis

Following the notations provided in **TABLE 1**, a comparative analysis is carried out among the OIDR-CP-ABE scheme, the MIDR-CP-ABE scheme, the original CP-ABE scheme which are scheme is built on, the unbounded non-monotonic CP-ABE scheme (the last scheme in Yamada's paper, and we just call it Yamada's scheme in this paper) [2]. In Yamada's scheme, it provides a general approach by incorporating "Not" logic on one or multiple attributes. Revoking a user, it can simply consider user's ID as an attribute. However, this scheme can significantly increase the attributes management overhead when the group size is large. To measure these schemes' performance, we present four evaluated functions, *i.e.*, *Setup()*, *KeyGen()*, *Encrypt()*, and *Decrypt()*. The analysis is carried out corresponding to the same function in each scheme on computation cost, storage cost, and communication cost.

4.1.1 Computation Complexity Analysis

In these four schemes, there are mainly four types of operations that are time-consuming: Pairing, Exponentiation, Multiplication, and Inversion. According to [8], the most computation-intensive operations are *Pairing* and *Exponentiation.* Thus, in this section, we evaluate the number of *Pairing* and *Exponentiation* operations for each function as metrics for computation complexity. The complexity of all the schemes involved in a number of *Parings* and *Exponentiations* are presented in **TABLE 2** and **TABLE 3** respectively.

In *Setup()* function of all the four schemes, the number of pairing operation is 1. Pairing is only incurred in calculating the value of $e(g,g)^\alpha$. In CP-ABE and Yamada, the number of exponentiations in *Setup()* function is 3 and 2 respectively. In both OIDR-CP-ABE

Table 2 Computation Complexity Comparison in the Number of Pairing Operations

Function	CP-ABE	OIDR-CP-ABE	MIDR-CP-ABE	Yamada
Setup()	1	1	1	1
KeyGen()	0	0	0	0
Encrypt()	0	0	0	0
Decrypt()	$2\|I\| + 1$	$2\|I\| + 1$	$2\|I\|r + 1$	$(2\|I\| + 1)r + 3\|I\|$

Table 3 Computation Complexity Comparison in Exponentiation Operations

Function	CP-ABE	OIDR-CP-ABE	MIDR-CP-ABE	Yamada
Setup()	3	m+3	m+3	2
KeyGen()	$\|S\| + 2$	$\|S\| + 3$	$\|S\| + 3$	$6\|S\| + 7$
Encrypt()	$3l + 2$	$2l + 3$	$(2l + 1)r + 2$	$5l + 5r$
Decrypt()	$\|I\|$	$\|I\|$	$\|I\|r$	$\|I\|$

and MIDR-CP-ABE, the number of exponentiations is $m + 3$, where m is the number of attributes defined globally as illustrated in **TABLE 1**.

For all the schemes, there is no need for any pairing operation in key generation process. Exponentiation operation is the key contributor to the cost in *KeyGen()* function for all four schemes. In CP-ABE, the number of exponentiations needed is $|S|+2$. In both OIDR-CP-ABE and MIDR-CP-ABE, this number is increased to $|S|+3$. This increase comes from the fact that not only a random value t but also the ID of the user is used as the exponent in the key component for each attribute. In Yamada, the number is $6|S| + 7$.

For *Encrypt()* function, the computation cost in terms of pairing is the same for CP-ABE, OIDR-CP-ABE, MIDR-CP-ABE and Yamada. The number of exponentiation operations is significant in differentiating the computation cost among these schemes. In CP-ABE, it takes $3l+2$ exponentiations and in OIDR-CP-ABE, the number of exponentiations is $2l+3$. Here l is the number of attributes involved in the encryption process. Thus, the encryption cost of the OIDR-CP-ABE scheme is lower than CP-ABE. Comparatively, in MIDR-CP-ABE, the number is increased to $(2l + 1)r + 2$, here r is the number of IDs that are revoked in the ciphertext. In the Yamada scheme, the number of exponentiation operations is $5l + 5r$.

In CP-ABE, the number of pairing needed for *Decrypt()* is $2|I| + 1$, where I is the set of attributes involved in the decryption process. It requires the same amount of pairing in OIDR-CP-ABE. However, $2|I|r+1$ pairing operations are needed in MIDR-CP-ABE due to the fact that it conducts more computation for each of the IDs that are revoked. It shows that the computation overhead from exponentiation operations is less than pairing operations. The Yamada scheme incurs more pairing operations in decryption compared with our schemes.

The numbers of exponentiations in CP-ABE, OIDR-CP-ABE, MIDR-CP-ABE and Yamada are $|I|$, $|I|$, $|I|r$, $|I|r$ and $|I|$ respectively.

4.1.2 Storage and Communication Cost Analysis

The storage cost and communication cost are evaluated separately. From storage perspective, the main overhead is from *Setup()* and *KeyGen()* functions, in which both functions create secret materials that need to be stored locally. For communication cost, the function *Encrypt()* is evaluated as results from this function constitute the ciphertext of transmitted messages. There is no additional storage or communication cost for *Decrypt()* function as the result is directly used as plaintext. The storage for temporary variables that are normally used in computer memories are not considered. Only those needed for final results of each function are counted. Based on our implementation, which is further illustrated in the next section, each element is stored as an element_t data structure. Therefore, the number of elements is used as a metric for storage and communication cost analysis. **TABLE 4** and **TABLE 5** summarize the cost corresponding to each function in all the four schemes.

In *Setup()* function, the storage costs are almost the same as the first three schemes, which is related with the number of all attributes in the system. In the Yamada scheme, this cost is a constant.

In *KeyGen()*, the required storage space is $|S|+2$ in all the first three schemes and almost quadruples in the Yamada scheme. The storage cost for *Encrypt()* function equals to the size of the ciphertext, which is $2l+2$ in both CP-ABE and OIDR-CP-ABE. The size of ciphertext in MIDR-CP-ABE is $2lr + 2$. This difference is due to the fact that a separate pair of key components need to be generated for each revoked ID. The ciphertext size in the Yamada scheme is $3l + 3r + 2$.

Table 4 Storage Cost Comparison

Function	CP-ABE	OIDR-CP-ABE	MIDR-CP-ABE	Yamada
Setup()	$m+4$	$m+6$	$m+6$	9
KeyGen()	$\|S\|+2$	$\|S\|+2$	$\|S\|+2$	$4\|S\|+2$

Table 5 Communication Cost Comparison

Function	CP-ABE	OIDR-CP-ABE	MIDR-CP-ABE	Yamada
Encrypt()	$2l+2$	$2l+2$	$2lr+2$	$3l+3r+2$

Based on the analysis presented above, it can be seen that the proposed schemes are more computation intensive. Between the two schemes, OIDR-CP-ABE performs better than MIDR-CP-ABE in computation, storage, and communication. The costs for OIDR-CP-ABE have the same order of complexity as CP-ABE scheme, which means the presented solution does not incur significant overhead compared to CP-ABE. However, the new functional benefits for revoking users is useful in many applications. Compared with Yamada, both of our schemes suffer from higher public parameters storage, while the private key storage is only quarter of that in Yamada. Since private keys are often stored in tamper-resistant memory, which is more costly, our scheme is more suitable for small devices with constrained storage. As for the communication costs, compared with Yamada, our schemes are much more efficient when there is only one identity.

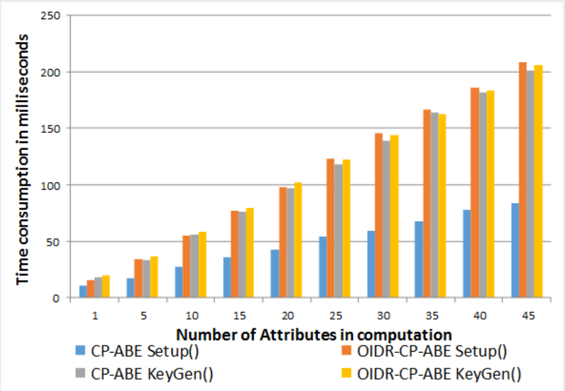

Fig. 3 Relations between the amount of attributes and time consumption for key assignment.

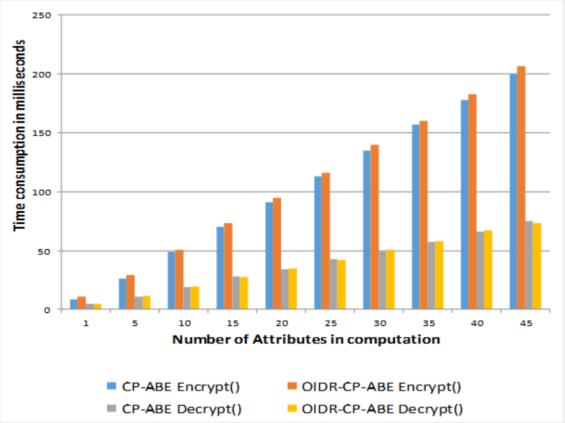

Fig. 4 Relations between the amount of attributes and time consumption for communication.

4.2 Implementation and Testing Results

The proposed schemes are implemented in C language using PBC library [7] on Ubuntu 14.04 64bit operating system. The hardware configuration for the machine that runs the experiment is: Intel i7 Quad-core CPU at 2.60GHz; 8GB memory. To test the relations between the amount of attributes involved and the time consumption, we fix the number of IDs revoked to 1 and increase the number of attributes that are involved in each of four functions *Setup()*, *KeyGen()*, *Encrypt()*, and *Decrypt()*. The time consumption of these functions are tested separately. Comparison is made for each function between CP-ABE scheme and OIDR-CP-ABE scheme. For each attribute setting, the experiments are run ten times and the average values are used as presented in **Fig. 3** and **Fig. 4**.

As can be seen in the figure, the time consumption for all the four functions are generally linear to the number of involved attributes. The difference in time consumption for *KeyGen()* function is relatively small between two schemes. The most significant time difference happens with *Setup()* function. The time cost in OIDR-CP-ABE is about twice of that in CP-ABE. In real-world application scenario, this function is run one time by the TA and can be precomputed. Therefore, such computation cost difference does not significantly influence the overall performance of the entire cryptosystem. When 45 attributes are involved for *Setup()*, *KeyGen()*, and *Encrypt()* function, the overall time cost is right over 200 milliseconds. The cost for *Decrypt()* is less than 100 milliseconds. The overall performance under this scenario is acceptable for real-world applications.

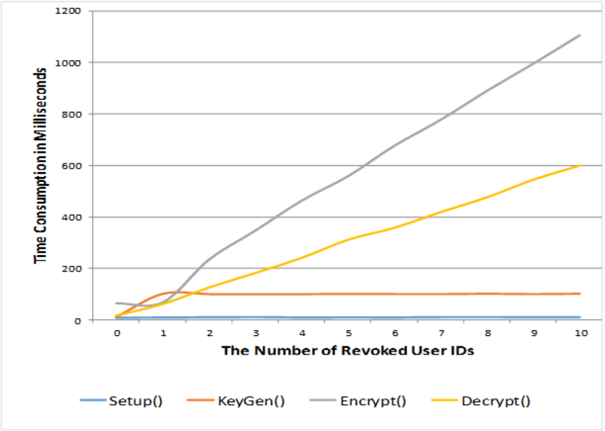

Fig. 5 Relations between the amount of revoked IDs and time consumption.

To further explore the influence on the time consumption from the number of IDs revoked, a second experiment is conducted with a fixed number of attributes and changing the number of revoked IDs. In this experiment, the number of attributes is set to 20 and the number of revoked IDs is gradually increased from 0 to 10. The evaluation result is shown in **Fig. 5** for MIDR-CP-ABE scheme. It can be seen that the time consumption of *Setup()* and *KeyGen()* are not sensitive to the number of IDs revoked. This is because both functions do not have the revoked ID list involved in their operations. The *Encrypt()* function is sensitive to the number of revoked IDs. Both *Encrypt()* and *Decrypt()* follow a linear trend in **Fig. 5**. When the number of revoked IDs is greater than 9, with 20 attributes involved, the overall time cost for *Encrypt()* increases over 1 second.

4.3 The Advantage of IR-CP-ABE in Secure Group Construction

In this subsection, we did simulation to demonstrate that IR-CP-ABE supports much more ID groups than CP-ABE does. Assume there exists 5 attributes in the system and the number of identities increases from 10 to 30. In addition, the probability p for each attribute to be assigned to an identity belongs to $[20\%, 40\%, 60\%, 80\%, 100\%]$. For each number value of identities and p value, the simulation ran 10 times to retrieve the average number of different ID groups generated by CP-ABE and that generated by IR-CP-ABE.

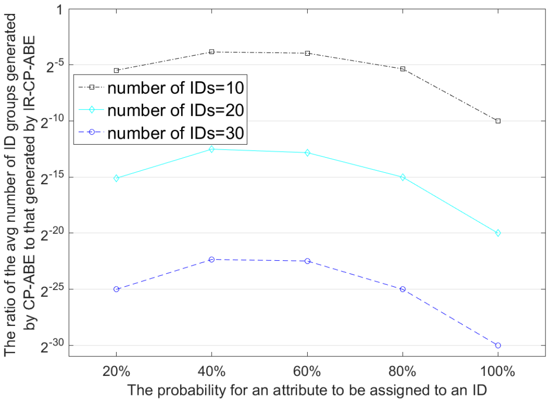

Fig. 6 The ratio of the average number of ID groups generated by CP-ABE to that generated by IR-CP-ABE

Fig. 6 illustrates that the ratio of the average number of different ID groups generated by CP-ABE to that generated by IR-CP-ABE is very small. The reason is that IR-CP-ABE could construct a very large number of different ID groups by combining all the IDs associated with the selected attributes first and then revoking any IDs, while CP-ABE can only generate ID groups based on attributes. Note that the ratio decreases when the number of identity increase, as the number of ID groups generated by IR-CP-ABE increases with the order of exponentiation. In addition, the ratio reaches its minimum when the number of identities is fixed and $p = 100\%$ because CP-ABE can only generate one ID group in this case. This implies IR-CP-ABE provides a more comprehensive solution in group construction than CP-ABE.

5 Related Work

The first fully functional Identity Based Encryption (IBE) scheme was proposed in [9]. In IBE, an identity or ID is a string one-to-one mapped to each user. A user can acquire a private key corresponding to his/her ID in an off-line manner from trusted authority and the ID is used as public key. The ciphertext encrypted by a particular ID can only be decrypted by the user with corresponding private key, i.e., the encryption is one-to-one.

Attribute Based Encryption (ABE) was first proposed as a fuzzy version of IBE in [10], where an identity is viewed as a set of descriptive attributes. The private key for an identity w can decrypt the message encrypted by the identity w' if and only if w and w' are closer to each other than a pre-defined threshold in terms of set overlap distance metric. In the paper [11], the authors further generalize the threshold-based set overlap distance metric to expressive access policies with AND and OR gates. There are two main variants of ABE proposed so far, namely Key Policy Attribute Based Encryption (KP-ABE [12]) and Ciphertext Policy Attribute Based Encryption (CP-ABE[13]). In KP-ABE, each ciphertext is associated with a set of attributes and each user's private key is embedded with an access policy. Decryption is enabled only if the attributes on the ciphertext satisfy the access policy of the user's private key. In CP-ABE [13–15, 1, 16], each user's private key is associated with a set of attributes and each ciphertext is encrypted by an access policy. To decrypt the message, the attributes in the user private key need to satisfy the access policy. The key difference between identity and attribute is identities are many-to-one mapped to users while attributes are many-to-many mapped to users. Thus, to simulate a constant size conjunctive header, one needs to encrypt the message using each receiver's identity and the size of ciphertext is linearly increasing.

ABE is a special case of functional encryption [17] which is superset of identity-based encryption, searchable encryption [18] [19], predicate encryption [15], etc. Another interesting related research topic is attribute-based authentication. Since nowadays, there are so many bots and malicious entities over the Internet [20] [21] [22] [23], whereas attribute-based encryption is identity less, our ABE scheme with identity revocable feature can be used to construct an authentication scheme which not only proves the attributes of the data senders but also their identities.

Boldyreva *et al.* [24] proposed an identity-based scheme with efficient user revocation capability. It applies key updates with significantly reduced computational cost based on a binary tree data structure and it is resistance against chosen-ciphertext attack. Nevertheless, Libert *et al.* [25] noticed the security problem left by Boldyreva that its security can only be proved in the selective-ID setting where adversaries need to reveal the victims' identities at the beginning of the game. Consequently, they proposed an identity-based encryption scheme with stronger adaptive-ID sense to address the remaining issue. Li *et al.* [26] first introduced outsourcing computation in identity-based encryption and presented a revocable in the server-aided settings. As a result, it achieves constant computation cost at public key generator and private key size at user, and the user does not have to contact public key generator for key update. Chen *et al.* [27] presented an identity-based encryption scheme based on lattices to realize efficient key revocation. Binary tree data structure is utilized to achieve logarithmic complexity in key updates. EASiER [28] architecture is described to support fine-grained access control policies and dynamic group membership based on attribute-based encryption. It relies on a proxy to participate in the decryption and enforce revocation, such that the user can be revoked without re-encrypting ciphertexts or issuing new keys to other users. Lewko *et al.* [4] two novel broadcast encryption schemes with effective user revocation capability. The first scheme is selectively secure in the standard model, and the second scheme achieves adaptive security by exploiting dual encryption technique. The ciphertext size only relates to the number of revoked users and the size of public/private keys are constant. Yu *et al.* [29] proposed an attribute-based data sharing scheme where each attribute gets three distinct values for its positive form, negative form as well as "don't care" form. It addressed the issue of attribute revocation by relying on a semi-trustable online proxy to perform re-encryption and take most laborious tasks. Li *et al.* [30] proposed an ABE scheme that supports efficient communication group set up and management. With such scheme, the group membership information is protected through a specially hidden attribute policy.

In the literature, there are several revocation mechanisms proposed for CP-ABE. In [31], Sahai *et al* proposed an indirect revocation mechanism. In this revocation mechanism, the trusted authority has to be online all the time to update and distribute the secret key information to non-revoked users. In [32], a direct revocation mechanism was proposed where there is revocation list to be specified directly in the encryption algorithm so that the ciphertext cannot be decrypted by the users in the revocation list. Liu and Wong [33] proposed a Traitor tracking approach (LW for short) that also supports user revocation with a very constrained situation, where it construct a user's ID to be a pair of integers from a predefined matrix. Therefore, a trusted authority is required to manage the mapping between a user and assigned unique pair of integers in order to allow a user to perform Traitor's ID checking. Whereas, in our scheme we allow a user's ID to have semantic meanings. Thus, we do not need a trusted authority to maintain the mapping table for ID checking. From the perspective of efficiency, in the LW scheme the encryption computation overhead and ciphertext size depends on the number of revoked users, thus not scalable to apply in networks with constrained resources.

6 Conclusions and Future Work

In this paper, we presented a new identity revocable CP-ABE scheme to improve the group management capability of existing CP-ABE solutions. With IR-CP-ABE, groups can be constructed in a much more flexible way compared with the previous CP-ABE schemes.

There are several research issues need to be further investigated. First, the ID revocation scheme still needs to explicitly specify which users need to be revoked in the revocation list. Ideally, revoked users should not be known by any group users. Second, a delegation scheme is desired to delegate all attributes and private key generation. Thus, revoking a delegator's ID will results in revoking a group of users in an efficient manner. A user can only get his/her attributes and private keys from one of the delegators. Moreover, a federated delegation approach is desired, in which a user can use his/her attributes and private keys generated from different delegators.

Acknowledgements This research is supported by Naval Research Lab (NRL) with grant number N00173-15-G017. The research work is conducted during Professor Weijia Wang's visit at Secure Networking And Computing (SNAC) research group, Arizona State University, US.

References

1. R. Ostrovsky, B. Waters, in *Proceedings of the 14th ACM conference on Computer and communications security* (ACM New York, NY, USA, 2007), pp. 195–203
2. S. Yamada, N. Attrapadung, G. Hanaoka, N. Kunihiro, in *International Workshop on Public Key Cryptography* (Springer, 2014), pp. 275–292
3. A. Beimel, *Secure schemes for secret sharing and key distribution* (Technion-Israel Institute of technology, Faculty of computer science, 1996)
4. A. Lewko, A. Sahai, B. Waters, in *Security and Privacy (SP), 2010 IEEE Symposium on* (IEEE, 2010), pp. 273–285
5. B. Waters, in *Public Key Cryptography - PKC 2011* (Springer-Verlag, 2011), pp. 53–70
6. D. Boneh, X. Boyen, E.J. Goh, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, 2005), pp. 440–456
7. B. Lynn. The pairing-based cryptography library (2006). URL https://crypto.stanford.edu/pbc/
8. B. Li, A.P. Verleker, D. Huang, Z. Wang, Y. Zhu, in *Communications and Network Security (CNS), 2014 IEEE Conference on* (2014), pp. 391–399
9. D. Boneh, M. Franklin, SIAM Journal of Computing **32**(2), 586 (2003)
10. A. Sahai, B. Waters, pp. 457–473 (2005)
11. M. Pirretti, P. Traynor, P. McDaniel, B. Waters, in *Proceedings of the 13th ACM conference on Computer and communications security* (ACM, 2006), p. 112
12. V. Goyal, O. Pandey, A. Sahai, B. Waters, Proceedings of the 13th ACM conference on Computer and communications security pp. 89–98 (2006)
13. J. Bethencourt, A. Sahai, B. Waters, in *IEEE SP'07* (Oakland, CA, 2007), pp. 321–334
14. L. Cheung, C. Newport, in *ACM conference on Computer and Communications Security* (Alexandria, Virginia, USA, 2007), pp. 456–465
15. J. Katz, A. Sahai, B. Waters, in *Proc. of EUROCRYPT 2008* (Springer-Verlag, 2008), pp. 146–162
16. V. Goyal, A. Jain, O. Pandey, A. Sahai, in *Automata, languages and programming* (Springer, 2008), pp. 579–591
17. L. Allison, O. Tatsuaki, S. Amit, T. Katsuyuki, W. Brent, in *Theory and Applications of Cryptographic Techniques* (Springer-Verlag, 2010), pp. 62–91
18. Q. Dong, Z. Guan, L. Wu, Z. Chen, in *International Conference on Web-Age Information Management* (Springer, 2013), pp. 729–740
19. D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, in *Eurocrypt*, vol. 3027 (Springer, 2004), vol. 3027, pp. 506–522
20. F. Morstatter, L. Wu, T.H. Nazer, K.M. Carley, H. Liu, in *Advances in Social Networks Analysis and Mining (ASONAM), 2016 IEEE/ACM International Conference on* (IEEE, 2016), pp. 533–540
21. L. Wu, F. Morstatter, X. Hu, H. Liu, Big Data in Complex and Social Networks pp. 123–152 (2016)
22. L. Wu, J. Li, X. Hu, H. Liu, in *Proceedings of the 2017 SIAM International Conference on Data Mining* (SIAM, 2017), pp. 99–107
23. L. Wu, X. Hu, F. Morstatter, H. Liu, in *ICWSM* (2017), pp. 696–699
24. A. Boldyreva, V. Goyal, V. Kumar, in *Proceedings of the 15th ACM conference on Computer and communications security* (ACM, 2008), pp. 417–426
25. B. Libert, D. Vergnaud, in *Topics in Cryptology–CT-RSA 2009* (Springer, 2009), pp. 1–15
26. J. Li, J. Li, X. Chen, C. Jia, W. Lou, Computers, IEEE Transactions on **64**(2), 425 (2015)
27. J. Chen, H.W. Lim, S. Ling, H. Wang, K. Nguyen, in *Information Security and Privacy* (Springer, 2012), pp. 390–403
28. S. Jahid, P. Mittal, N. Borisov, in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (ACM, 2011), pp. 411–415
29. S. Yu, K. Ren, W. Lou, Computer Networks **54**(3), 377 (2010)
30. B. Li, Z. Wang, D. Huang, in *2013 IEEE Global Communications Conference (GLOBECOM)* (2013), pp. 861–866
31. A. Sahai, H. Seyalioglu, B. Waters, in *Advances in Cryptology–CRYPTO 2012* (Springer, 2012), pp. 199–217
32. N. Attrapadung, H. Imai, in *International Conference on Pairing-Based Cryptography* (Springer, 2009), pp. 248–265
33. Z. Liu, D.S. Wong, in *International Conference on Applied Cryptography and Network Security* (Springer, 2015), pp. 127–146