HIR-CP-ABE: Hierarchical Identity Revocable Ciphertext-Policy Attribute-Based Encryption for Secure and Flexible Data Sharing

Qiuxiang Dong$^\sharp$, Dijiang Huang$^\sharp$, Jim Luo*, and Myong Kang*
$^\sharp$Arizona State University, Tempe, AZ 85281, US
* Naval Research Lab, Washington DC, 20375, US
{qiuxiang.dong, dijiang}@asu.edu
{jim.luo, myong.kang}@nrl.navy.mil

Abstract—**Ciphertext Policy Attribute-Based Encryption (CP-ABE) has been proposed to implement the attribute-based access control model. In CP-ABE, data owners encrypt the data with a certain access policy such that only data users whose attributes satisfy the access policy could obtain the corresponding private decryption key from a trusted authority. Therefore, CP-ABE is considered as a promising fine-grained access control mechanism for data sharing where no centralized trusted third party exists, for example, cloud computing, mobile ad hoc networks (MANET), Peer-to-Peer (P2P) networks, information centric networks (ICN), *etc.*. As promising as it is, user revocation is a cumbersome problem in CP-ABE, thus impeding its application in practice. To solve this problem, we propose a new scheme named HIR-CP-ABE, which implements *hierarchical identity-based* user revocation from the perceptive of *encryption*. In particular, the revocation is implemented by data owners directly *without any help from any third party*. Compared with previous *attribute-based revocation* solutions, our scheme provides the following nice properties. First, the trusted authority could be offline after system setup and key distribution, thus making it applicable in mobile ad hoc networks, P2P networks, *etc.*, where the nodes in the network are unable to connect to the trusted authority after system deployment. Second, a user does not need to update the private key when user revocation occurs. Therefore, key management overhead is much lower in HIR-CP-ABE for both the users and the trusted authority. Third, the revocation mechanism enables to revoke a group of users affiliated with the same organization in a batch without influencing any other users. To the best of our knowledge, HIR-CP-ABE is the first CP-ABE scheme to provide affiliation-based revocation functionality for data owners. Through security analysis and performance evaluation, we show that the proposed scheme is secure and efficient in terms of computation, communication and storage.**

Index Terms—**Attribute-Based Access Control, Encryption, CP-ABE, Revocation, Hierarchical Identity**

I. INTRODUCTION

The literature has proposed a diversity of access control systems supporting policies including basic access control lists [1], group-based [2], role-based [3] and attribute-based controls [4]. Most of these approaches rely on a fully-trusted access monitoring server to implement policy checking, which is not applicable in practical applications where no fully-trusted server exists. Secure data sharing in these application scenarios pushes the development and usage of cryptographic schemes in supporting access control. Among these cryptographic schemes, Ciphertext Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most expressive technologies and is a natural fit for attribute-based access control in secure data sharing.

In CP-ABE, each user is entitled a set of attributes based on his/her role or identity, which are embedded into the private key by the trusted authority that is responsible for system setup and key generation/distribution. A data owner enforces an access policy over the shared data directly by encrypting the data with the access structure extracted from the access policy. Instead of by the server, the access checking is done "inside the cryptography", where only data users with eligible attributes (*i.e.*, satisfying the access structure) could decrypt the ciphertext. Different from identity-based and role-based cryptographic schemes, the public key and ciphertext size of CP-ABE are not related with the number of data users and no interactions among data owners and data users are needed. Moreover, CP-ABE is resistant against collusion attacks from unauthorized users. All these nice properties make CP-ABE very suitable for implementing fine-grained access control for secure data sharing in cloud computing where the cloud servers can't be fully trusted or mobile ad hoc networks (MANET), Peer-to-Peer(P2P) networks, and the recently proposed information centric networks (ICN) where no centralized server exists after system deployment.

As promising as it is, multiple users might share common attributes with each other, thus making user management, especially user revocation extremely difficult to handle when applying state-of-the-art CP-ABE schemes to practical applications. Previous researches define the revocation problem as *attribute-based revocation*. The basic idea of attribute-based revocation is to cease certain access privileges of users from the perspective of *key generation*. In particular, it is a key re-distribution process. Whenever an attribute revocation occurs, the trusted authority generates some secret information for non-revoked users to update their private key. Since the revoked user doesn't have the secret updating information, the components of his/her private key corresponding to the revoked attributes will not work any more when used to decrypt newly generated ciphertexts, thus achieving the goal of ceasing certain users' access privilege(s).

Although attribute-based revocation is a feasible solution to the user revocation problem in CP-ABE, it suffers the following deficiencies when applied in practice. First, trusted authority has to be online all the time to deal with each revocation and keeps a mapping between each attribute and the corresponding list of the non-revoked users in order to distribute secret information. Once the authority is down, the user revocation functionality cannot be implemented any more. Moreover, in some application scenarios, such as MANET, P2P networks, once the system is set up, there would be no communication between the trusted authority and the nodes in the network except for system re-setup. Second, non-revoked users owning common attributes with the revoked user(s) have to update their private keys, which will bring in great computation and communication overheads when the revoked users have a great number of attributes, the number of the non-revoked users sharing common attributes with the revoked users is big, or user revocation frequency is high.

The reason leading to the aforementioned deficiencies is that revocation is performed from the perspective of key generation. To this end, we propose a new scheme HIR-CP-ABE, which implements user revocation from the perceptive of *encryption*. Different from previous attribute-based approaches, HIR-CP-ABE supports *identity-based revocation*. In the key generation phase, on the one hand attributes are allocated to users as in state-of-the-art CP-ABE schemes, on the other hand a unique identity (ID) is assigned to each user. That is, both attributes and the ID are embedded into a user's private key. The encryption algorithm works by two steps: first, specify attribute literals in conjunctive/disjunctive normal forms as an attribute structure to cover the recipients of the target group; second, revoke unauthorized users by incorporating their identities into the ciphertext. In this way, only users whose attributes satisfy the access structure and meanwhile are not revoked by the data owners could decrypt the ciphertext. In order to revoke users who are affiliated with the same organization in a batch, we introduce *hierarchical identity-based revocation*. If an organization is revoked, then all the affiliated users will be revoked as well. The contributions of this paper could be summarized as follows:

- We propose firstly an identity-based CP-ABE user revocation mechanism. During data sharing, the owners are able to revoke any user directly without the help of trusted authority and do not need to re-distribute private keys.
- We propose a new primitive named hierarchical identity revocable CP-ABE (HIR-CP-ABE) and define its security model. This scheme not only supports revocation of particular users but also is capable to revoke all the users affiliated with the same organization in a batch.
- We present a construction of the HIR-CP-ABE scheme and prove that the construction is secure in terms of the proposed security model.
- We perform performance evaluation and show that the proposed HIR-CP-ABE construction is practical for real-world applications.

The remainder of this paper is organized as follows. In section II, we introduce some preliminaries and notations. In section III, we show the formal definition of the HIR-CP-ABE scheme together with its security definition. In section IV, we present a construction of the HIR-CP-ABE scheme. In section V, we evaluate the efficiency of the proposed construction. Section VI discusses the related work. Section VII concludes the paper. Security proofs are presented in the appendices.

II. Preliminaries and Notations

In this section, we first present the definition of *access structure*, *linear secret sharing schemes*, *bilinear map*, as well as the *M-q-parallel-BDHE* assumption. Then some notations used in the following sections are summarized and an explanation of the hierarchical identity structure is presented.

A. Preliminaries

Access Structure [5]. Let $\{P_1, P_2, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1,P_2,\ldots,P_n\}}$ 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 collection $\mathbb{A}$ 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.

Linear Secret Sharing Schemes(LSSS) [5]. A secret sharing scheme Π over a set of parties is called linear over $\mathbb{Z}_p$ if the following two conditions are satisfied

- the shares for each party form a vector over $\mathbb{Z}_p$;
- a share-generating matrix for Π has ℓ rows and n columns. For all $i = 1, \ldots, \ell$, the 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 $r_2, r_3, \ldots, r_n \in \mathbb{Z}$ are randomly chosen numbers, Mv is the vector of ℓ shares of the secret s according to Π. The share $(Mv)_i$ belongs to party $\rho(i)$.

As shown in [5], every linear secret sharing-scheme according to the above definition also enjoys the following **linear reconstruction** property:

Assume that Π is an LSSS for the access structure $\mathbb{A}$. Define $\mathbf{S} \in \mathbb{A}$ as an authorized set and $\mathbf{I} \subset [1, l]$ as $\mathbf{I} = \{i : \rho(i) \in \mathbf{S}\}$. Then, constants $\{w_i \in \mathbb{Z}_p\}_{i \in \mathbf{I}}$ can be derived in polynomial time such that for valid shares $\{\lambda_i\}$ of any secret s we have $\sum_{i \in \mathbf{I}} w_i \lambda_i = s$.

Bilinear Map. Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be multiplicative cyclic groups of prime order p. Let g_1 and g_2 be the generator of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. A bilinear map is a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ with the following properties:

- Computable: there exists an efficiently computable algorithm for computing e;
- Bilinear: for all $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_p$, $e(u^a, v^b) = e(u, v)^{ab}$; For any $u \in \mathbb{G}_1, v_1, v_2 \in \mathbb{G}_2, e(u, v_1 v_2) = e(u, v_1) \cdot e(u, v_2)$;
- Non-degenerate: $e(g_1, g_2) \neq 1$.

The bilinear map is called symmetric, if $\mathbb{G}_1$ and $\mathbb{G}_2$ are a same group denoted by $\mathbb{G}$.

M-q-parallel-BDHE. The definition of the modified (decisional) q parallel Bilinear Diffie-Hellman Exponent problem is as follows. Choose a group $\mathbb{G}$ of prime order p according to the security parameter and a random generator g of $\mathbb{G}$. Choose $a, s, b_1, b_2, \cdots, b_q \in \mathbb{Z}_p$ at random. Given

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

it is hard for a probabilistic polynomial time (PPT) adversary to distinguish $e(g,g)^{a^{q+1}s} \in \mathbb{G}_T$ from a random element R chosen from $\mathbb{G}_T$. An algorithm $\mathcal{B}$ that outputs $z \in \{0,1\}$ has advantage ϵ in solving the M-q-parallel-BDHE problem defined as above if the follwing equation holds

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

*The **M-q-parallel-BDHE assumption** holds if the advantage ϵ of any PPT adversary $\mathcal{B}$ to solve the M-q-parallel-BDHE problem is a negligible function of the security parameter.*

Theorem 1. *The Modified (decisional) q parallel Bilinear Diffie-Hellman Exponent assumption generically holds.*

B. Notations

Notations used in following sections are listed as follows.

TABLE I Notations.

i-LID	local identity of an organization or a user on the i^{th} layer
i-ID	global identity of an organization or a user on the i^{th} layer
$\mathbf{U}$	the attribute universe defined in the system
m	the number of attributes defined in the system, *i.e.*, $\lvert\mathbf{U}\rvert = m$
$\mathbb{Z}_p$	a set of integers between 0 and $p-1$
M_i	the i^{th} row of a matrix M
H	the number of layers in the identity structure tree
H'	the number of layers in a particular identity ID
r	the number of revoked identities
$\mathbf{S}$	the set of attributes created for a specific user

C. Hierarchical Identity Structure

In HIR-CP-ABE, identities are represented in a hierarchical tree structure as illustrated in **Fig. 1**.

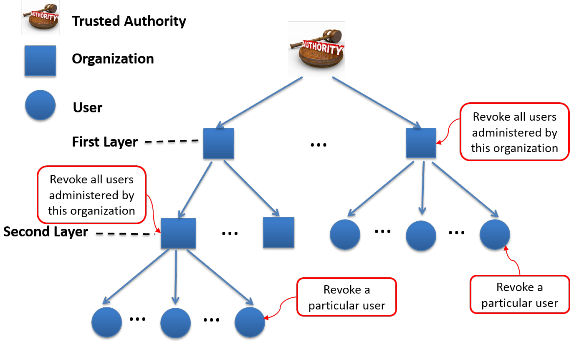

Fig. 1 Hierarchical Identity Structure Tree.

The non-leaf nodes represent organizations, among which the root node represents the trusted authority. The leaf nodes represent users. Each organization (and user) has a unique identity under the parent organization, which is called local identity (LID), and meantime a unique global identity (denoted by ID) within the whole system. Assume that the hierarchical identity structure tree has $H+1$ layers (the root node is on the 0^{th} layer), then the organizations and users' identities can be constructed according to the following syntax:

$$\begin{gathered}0\text{-}ID := ID \text{ of the root trusted authority,} \\ i\text{-}ID := \text{parent } (i-1)\text{-}ID \parallel i\text{-}LID,\ (1 \leq i \leq H)\end{gathered}$$

Take the hierarchical identities of a university U_A as an example. U_A is the trusted authority. There exist several schools under her administration, such as S_1, S_2. Under the administration of S_1, there are several departments, such as D_1 and D_2. Student Alice majors in D_1. Student Bob majors in D_2. Then for S_1, the identity will be "$\mathrm{U}_A \| \mathrm{S}_1$". For D_1, the identity will be denoted by $ID =$ "$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_1$". For users, Alice's ID is "$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_1 \|$Alice"; Bob's ID is "$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_2 \|$Bob".

For a user on the i^{th} layer, we also define:

$$ID_{|h} := \text{ancestor } h\text{-}ID,$$

where $h \in [1, i-1]$ and "ancestor h-ID" denotes the identity of the ancestor node on the h^{th} layer from root node to the user node. For Alice, $ID_{|1} =$ "$\mathrm{U}_A \| \mathrm{S}_1$", $ID_{|2} =$ "$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_1$". For Bob, $ID_{|1} =$ "$\mathrm{U}_A \| \mathrm{S}_1$", $ID_{|2} =$ "$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_2$". Both the user identity and the ancestors' identity will be embedded into the user's private key. In the hierarchical identity structure tree, users can be on any layer of the tree (except for the 0^{th} layer). With the proposed identity-based revocation mechanism and the hierarchical identity structure, on each layer, both individual users and organizations can be revoked. Furthermore, if an organization is revoked, then all the affiliated users will be revoked, thus achieving the goal of revocation in a batch.

III. Algorithm Definition and Security Model

In this section, we will present the definition of the proposed HIR-CP-ABE scheme as well as its security model.

A. Algorithm Definition

The HIR-CP-ABE scheme consists of four algorithms:

- **Setup**$(\lambda, \mathbf{U}) \rightarrow (PK, MSK)$: Input the security parameter λ and the attribute universe $\mathbf{U}$. Output public parameters *PK* and the master secret key *MSK*.
- **KeyGen**$(MSK, ID, \mathbf{S}) \rightarrow SK$: Input the master secret key *MSK*, a user's hierarchically structured identity *ID*, and a set of attributes $\mathbf{S}$ that describe the user's access privilege. Output the private key *SK*.
- **Encrypt**$(PK, (M, \rho), \mathcal{M}, \mathbf{ID}') \rightarrow CT$: Input the public parameters *PK*, the LSSS matrix M and its corresponding mapping ρ to each attribute (M and ρ are derived from an access structure $\mathbb{A}$ as described in Section II), the message $\mathcal{M}$ and the set $\mathbf{ID}'$ of revoked identities. Output the ciphertext *CT*.

- $\mathbf{Decrypt}(CT, SK) \rightarrow \mathcal{M}$ or $\perp$: Input the ciphertext *CT* and the private key *SK*. Output the message $\mathcal{M}$ if and only if the attributes of the secret key holder satisfy the access policy enforced on the ciphertext *CT*.

Note: In the $\mathbf{Encrypt}$ algorithm, the revoked identity set might contain individual users' identities or organizations' identities or both kinds of identities.

Consistency Constraint: Given that SK is the private key generated by $\mathbf{KeyGen}$ when it takes inputs of an identity ID and an attribute set $\mathbf{S}$; CT is the ciphtertext generated by $\mathbf{Encrypt}$ when it takes inputs of a revoked identity set $\mathbf{ID}'$ and (M, ρ) corresponding to an LSSS access structure $\mathbb{A}$. The HIR-CP-ABE scheme should satisfy the following consistency constraint:

$$\forall \mathcal{M} : \mathbf{Decrypt}(CT, SK) = \mathcal{M}, \text{ if } ID \notin \mathbf{ID}' \text{ and } \mathbf{S} \in \mathbb{A}$$
$$\textbf{AND}$$
$$\mathbf{Decrypt}(CT, SK) = \perp \text{ if } ID \in \mathbf{ID}' \text{ or } \mathbf{S} \notin \mathbb{A}.$$

In particular, only if a user is not revoked and his/her attribute set $\mathbf{S}$ satisfies the access structure $\mathbb{A}$, can the decryption algorithm work correctly. Here $ID \notin \mathbf{ID}'$ means the user's ID is not in the revoked identity set and meanwhile the user is not under the administration of the organization(s) whose ID is included in the revoked identity set. For example, if the identity "$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_1$" $\in \mathbf{ID}'$, *i.e.,* the department D_1 is revoked, then all the students, professors and staffs affiliated with this department will be revoked. Therefore, the HIR-CP-ABE scheme not only supports individual user revocation but also supports affiliation-based revocation.

B. Security Model

Compared with the CP-ABE scheme, we need to consider stronger adversaries whose attributes satisfy the access structure of the challenge ciphertext. The HIR-CP-ABE security model is formalized by the game between a challenger and an adversary $\mathcal{A}$ as follows.

- **Init**: The adversary $\mathcal{A}$ commits to a challenge access structure $\mathbb{A}^*$ and a revoked identity set $\boldsymbol{ID}^*$ and sends them to the challenger.
- **Setup**: The challenger runs the setup algorithm. The generated master secret key *MSK* is kept secret and the public parameters *PK* are given to the adversary.
- **Phase1**: The adversary $\mathcal{A}$ makes repeated private key queries $(\mathbf{S_i}, ID_i)_{i \in [1,q_1]}$ with two constrains: (1) if $\mathbf{S}_i \in \mathbb{A}^*$, then $ID_i \in \boldsymbol{ID}^*$; (2) if $ID_i \notin \boldsymbol{ID}^*$, then $\mathbf{S}_i \notin \mathbb{A}^*$.
- **Challenge**: The adversary sends to the challenger two randomly selected equal length messages $\mathcal{M}_0$ and $\mathcal{M}_1$. The challenger picks up a random bit $b \in \{0, 1\}$, and encrypts $\mathcal{M}_b$ under the access structure $\mathbb{A}^*$ and the revoked identity set $\boldsymbol{ID}^*$. The generated challenge ciphertext CT^* is sent back to the adversary $\mathcal{A}$.
- **Phase2**: Repeat **Phase1** with the same constrains.
- **Guess**: The adversary outputs a guess bit b' of b.

Definition 1. *Define* $Adv_{\mathcal{A}} = |Pr[b' = b] - \frac{1}{2}|$ *as the advantage of the adversary* $\mathcal{A}$ *winning the game above. The HIR-CP-ABE scheme is secure if* $Adv_{\mathcal{A}}$ *of any PPT adversary* $\mathcal{A}$ *is a negligible function of the security parameter.*

IV. HIR-CP-ABE Constructions

In this section, we will present a construction of the HIR-CP-ABE scheme. For clarity, we firstly show a construction performing revocation of a single identity. The revoked identity could be a user's identity or an organization's identity. For example, if the revoked identity is "$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_1 \|$Alice", then only the user "Alice" affiliated with "'$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_1$" will be revoked; if the revoked identity is "$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_1$", then all the users affiliated with "$\mathrm{U}_A \| \mathrm{S}_1 \| \mathrm{D}_1$" will be revoked.

A. One Identity Revocation in HIR-CP-ABE

Let $\mathbb{G}$ be a bilinear group of prime order p, and let g be the generator of $\mathbb{G}$. When we mention an identity in a math formula, it is an element in $\mathbb{Z}_p$ obtained by enforcing a hash function. The HIR-CP-ABE scheme supporting one identity revocation (O-HIR-CP-ABE for short) is presented as follows.

$\mathbf{Setup}(\lambda, \mathbf{U})$: Choose random exponents $\alpha, b \in \mathbb{Z}_p$ and random group elements $\{h_{xh}\}_{x \in \mathbf{U}, h \in [1,H]}$. The public parameters and master secret key are as follows

$$PK = \big(g, g^b, g^{b^2}, e(g,g)^{\alpha}, \{h_{xh}^b\}_{x \in \mathbf{U}, h \in [1,H]}\big),$$
$$MSK = \big(\alpha, b\big)$$

$\mathbf{KeyGen}$(*MSK*, $\mathbf{S}$, *ID*): *ID* is the identity of a user on the H'^{th} layer, where $1 \leq H' \leq H$. Choose a random $t \in \mathbb{Z}_p$. The private key for user ID is as follows

$$SK = (K = g^{\alpha} g^{b^2 t}, K_x, L = g^{-t}), \text{ where}$$
$$K_x = \{K_{xh} = (g^{b \cdot ID_{|h}} h_{xh})^t\}_{\forall x \in \mathbf{S}, h \in [1,H], ID_{|h} = ID(h \in [H',H]})$$

$\mathbf{Encrypt}(PK, (M, \rho), \mathcal{M}, ID')$: M is an $l \times n$ matrix. Choose a random vector $v = (s, y_2, \cdots, y_n) \in \mathbb{Z}_p^n$ and for $k \in [1, l]$ calculate $\lambda_k = v \cdot M_k$. Assume that the revoked user is on the H'^{th} layer in the hierarchical identity structure. The ciphertext of the message $\mathcal{M}$ is as follows

$$CT = (C, C', \hat{C}, (M, \rho), ID'), \text{ where}$$
$$C = \mathcal{M} e(g,g)^{\alpha s},$$
$$C' = g^s,$$
$$\hat{C} = \{\hat{C}_k = g^{b \cdot \lambda_k}, \hat{C}'_k = (g^{b^2 \cdot ID'} h^b_{\rho(k)H'})^{\lambda_k}\}_{k \in [1,l]}$$

$\mathbf{Decrypt}(CT, SK)$: *CT* is the input ciphertext with an access structure (M, ρ) and revoked identity ID'. *SK* is a private key for a set $\mathbf{S}$ and identity ID. Suppose that $\mathbf{S}$ satisfies the access structure and let $\mathbf{I} \subset [1, l]$ be defined as $\mathbf{I} = \{i : \rho(i) \in \mathbf{S}\}$. Let $\{\omega_i \in \mathbb{Z}_p\}_{i \in \mathbf{I}}$ be a set of constants such that if $\{\lambda_i\}_{i \in \mathbf{I}}$ are valid shares of any secret s according to M, then $\Sigma_{i\in\mathbf{I}}\omega_i\lambda_i = s$. If the condition $ID \neq ID'$ holds, calculate A as follows

$$\begin{array}{rcl} A & = & \prod_{i\in\mathbf{I}}[e(K_{\rho(i)H'}, \hat{C}_i)\cdot e(L, \hat{C}'_i)]^{\frac{\omega_i}{ID-ID'}} \\ & = & (\prod_{i\in\mathbf{I}}[e((g^{b\cdot ID}h_{\rho(i)H'})^t, g^{b\cdot\lambda_i}) \\ & & \cdot e(g^{-t}, (g^{b^2\cdot ID'}h^b_{\rho(i)H'})^{\lambda_i})]^{\frac{\omega_i}{ID-ID'}} \\ & = & (\prod_{i\in\mathbf{I}}[e(g^{b\cdot ID\cdot t}, g^{b\cdot\lambda_i})\cdot e(h^t_{\rho(i)H'}, g^{b\cdot\lambda_i}) \\ & & \cdot e(g^{-t}, g^{b^2\cdot ID'\cdot\lambda_i})\cdot e(g^{-t}, h^{b\cdot\lambda_i}_{\rho(i)H'})]^{\frac{\omega_i}{ID-ID'}} \\ & = & (\prod_{i\in I}[e(g^{b\cdot ID\cdot t}, g^{b\cdot\lambda_i})\cdot e(g^{-t}, g^{b^2\cdot ID'\cdot\lambda_i})]^{\omega_i})^{1/(ID-ID')} \\ & = & (\prod_{i\in\mathbf{I}}[e(g,g)^{b^2 t\lambda_i(ID-ID')}]^{\frac{\omega_i}{ID-ID'}} \\ & = & \prod_{i\in\mathbf{I}} e(g,g)^{b^2 t\lambda_i\omega_i} \\ & = & e(g,g)^{b^2 t\sum_{i\in\mathbf{I}}\lambda_i\omega_i} \\ & = & e(g,g)^{b^2 ts} \end{array}$$

We can get the value $e(g,g)^{\alpha s}$ by evaluating $\frac{e(C',K)}{A}$. The decryption algorithm then divides out this value from C and obtains the message $\mathcal{M}$.

Theorem 2. *Suppose that the M-q-parallel-BDHE assumption holds. Then no PPT adversary can selectively break the O-HIR-CP-ABE scheme with a challenge access structure* (M^*, ρ^*)*, where the size of* M^* *is* $\ell^* \times n^*$ *and* $\ell^*, n^* \leq q$.

B. Multiple Identities Revocation in HIR-CP-ABE

In this section, we show how to construct an HIR-CP-ABE scheme supporting revokation of multiple identities (M-HIR-CP-ABE for short). The **Setup** and **KeyGen** algorithm are the same as those of the O-HIR-CP-ABE scheme, thus we only show the **Encrypt** and **Decrypt** algorithm below.

Encrypt$(PK, (M,\rho), \mathcal{M}, \mathbf{ID}')$: $\mathbf{ID}' = \{ID'_1, \cdots, ID'_r\}$ is the revoked identity set, where identity ID'_j is on the H'^{th}_j layer in the identity structure tree, where $j \in [1,r]$. M is an $l \times n$ matrix. Choose a random vector $v = (s, y_2, \cdots, y_n) \in \mathbb{Z}_p^n$. For $k \in [1,l]$, calculate $\lambda_k = v \cdot M_k$. Choose random $\mu_1, ..., \mu_r \in \mathbb{Z}_p$ such that $\mu = \mu_1 + ... + \mu_r$. The ciphertext is as follows:

$$\begin{array}{c} CT = (C, C', \hat{C}, (M,\rho), \mathbf{ID}'), \text{ where} \\ C = \mathcal{M}e(g,g)^{\alpha s\mu}, \\ C' = g^{s\mu}, \\ \hat{C} = \{\hat{C}_{k,j} = g^{b\cdot\lambda_k\mu_j}, \hat{C}'_{k,j} = (g^{b^2\cdot ID'_j}h^b_{\rho(k)H'_j})^{\lambda_k\mu_j}\}^{j\in[1,r]}_{k\in[1,l]} \end{array}$$

Decrypt(CT, SK): CT is the input ciphertext with the access structure (M,ρ) and the revoked identity set $\mathbf{ID}'$. SK is the private key for a set $\mathbf{S}$ and identity ID. Suppose that $\mathbf{S}$ satisfies the access structure and define $\mathbf{I} \subset [1,l]$ as $\mathbf{I} = \{i : \rho(i) \in \mathbf{S}\}$. Let $\{\omega_i \in \mathbb{Z}_p\}_{i\in\mathbf{I}}$ be a set of constants such that if $\{\lambda_i\}_{i\in\mathbf{I}}$ are valid shares of any secret s according to M, then $\Sigma_{i\in\mathbf{I}}\omega_i\lambda_i = s$. If $ID \notin \mathbf{ID}'$, we first calculate A as follows

TABLE II Computation Complexity Comparison in terms of the Number of Pairing Operations

Schemes	CP-ABE	O-HIR-CP-ABE	M-HIR-CP-ABE
Setup	1	1	1
KeyGen	0	0	0
Encrypt	0	0	0
Decrypt	$2\vert\mathbf{I}\vert + 1$	$2\vert\mathbf{I}\vert + 1$	$2\vert\mathbf{I}\vert r + 1$

$$\begin{array}{rcl} A & = & \prod_{j=1}^r \prod_{i\in\mathbf{I}}[e(K_{\rho(i)H'_j}, \hat{C}_{k,j})\cdot e(L, \hat{C}'_{k,j})]^{\frac{\omega_i}{ID_j - ID'_j}} \\ & = & \prod_{j=1}^r(\prod_{i\in\mathbf{I}}[e((g^{b\cdot ID_j}h_{\rho(i)H'_j})^t, g^{b\cdot\lambda_i\mu_j}) \\ & & \cdot e(g^{-t}, (g^{b^2\cdot ID'_j}h^b_{\rho(i)H'_j})^{\lambda_i\mu_j})]^{\frac{\omega_i}{ID_j-ID'_j}} \\ & = & \prod_{j=1}^r(\prod_{i\in\mathbf{I}}[e(g,g)^{b^2 t\lambda_i\mu_j(ID_j-ID'_j)}]^{\frac{\omega_i}{ID_j-ID'_j}} \\ & = & \prod_{j=1}^r(\prod_{i\in\mathbf{I}} e(g,g)^{b^2 t\lambda_i\omega_i\mu_j}) \\ & = & \prod_{j=1}^r e(g,g)^{b^2 t\mu_j\sum_{i\in\mathbf{I}}\lambda_i\omega_i} \\ & = & \prod_{j=1}^r e(g,g)^{b^2 t\mu_j s} \\ & = & e(g,g)^{b^2 st\sum_{j=1}^r \mu_j} \\ & = & e(g,g)^{b^2 st\mu}. \end{array}$$

We can get the value $e(g,g)^{\alpha s\mu}$ by evaluating $\frac{e(C',K)}{A}$. The decryption algorithm then divides out this value from C and obtains the message $\mathcal{M}$.

Theorem 3. *Suppose that the M-q-parallel-BDHE assumption holds. Then no PPT adversary can selectively break the M-HIR-CP-ABE scheme with a challenge access structure* (M^*, ρ^*)*, where the size of* M^* *is* $\ell^* \times n^*$ *and* $\ell^*, n^* \leq q$.

V. Performance Evaluation

The advantages of the HIR-CP-ABE scheme over the previous attribute-based revocation schemes lie in the following three aspects: First, it revokes users from data owners' perspective, any data owner could revoke any data user without any help from the trusted authority. Second, user revocation does not require key re-distribution, which will bring in great computation and communication overheads to the system when the revoked users have a great number of attributes, the number of the non-revoked users sharing common attributes with the revoked users is big, or user revocation frequency is high. Finally, our scheme enables data owners to revoke a group of users based on their affiliation.

With so many nice properties that are not provided by the previous attribute-based revocation schemes, will HIR-CP-ABE be efficient in practical applications? To answer this question, in this section, we evaluate the two scheme constructions proposed in this paper in terms of their computation, storage, and communication performance. Since the revocation scheme is constructed based on the ciphertext-policy attribute-based encryption scheme (denoted by CP-ABE) [6], which itself or constructions based on it are broadly used [7]–[9], we use this scheme as the baseline.

TABLE III Computation Complexity Comparison in terms of the Number of Exponentiation Operations

Schemes	CP-ABE	O-HIR-CP-ABE	M-HIR-CP-ABE
Setup	$m+3$	$mH+3$	$mH+3$
KeyGen	$\|\mathbf{S}\|+3$	$H\|\mathbf{S}\|+H'+3$	$H\|\mathbf{S}\|+H'+3$
Encrypt	$3l+2$	$2l+3$	$(2l+1)r+2$
Decrypt	$\|\mathbf{I}\|$	$\|\mathbf{I}\|$	$\|\mathbf{I}\|r$

A. Complexity Analysis

There are four types of time-consuming operations in all the schemes, *i.e.*, pairing, exponentiation, multiplication and inversion. According to [11], the pairing and exponentiation operations take the dominant computation costs. Therefore, we use the number of pairing and exponentiation operations as metrics for computation complexity.

1) Computation Complexity Analysis: **TABLE II** and **TABLE III** present computation costs comparisions of the three schemes. I and l are notations used in the section **IV**. In the setup algorithm of all these three schemes, there is only one pairing operation that is brought by evaluating $e(g,g)^{\alpha}$. In CP-ABE, the number of exponentiations in the setup algorithm is $m+3$. In both O-HIR-CP-ABE and M-HIR-CP-ABE, $mH+3$ exponentiation operations are needed because of the hierarchical identity structure. In the key generation algorithm of all the three schemes, no pairing operation is performed. In CP-ABE, the number of exponentiations needed is $|S|+3$. In both O-HIR-CP-ABE and M-HIR-CP-ABE, this number increases to be $H|S|+H'+3$. This increase comes from the fact that all layers in a user's hierarchical identity structure are embedded in the key component for each attribute.

For the encryption algorithm, the same as the key generation algorithm, exponentiation operations are the dominant costs. In the encryption algorithm of CP-ABE, the number of exponentiation operations is $3l+2$. In the O-HIR-CP-ABE scheme, the number is $2l+3$. In M-HIR-CP-ABE, the number is $(2l+1)r+2$ because of multiple revoked identities. In CP-ABE, the number of pairing needed for decryption is $2|\mathbf{I}|+1$, which is the same as that of the O-HIR-CP-ABE scheme. The number increases to be $2|\mathbf{I}|r+1$ in M-HIR-CP-ABE since there are multiple identities revoked. The numbers of exponentiations in CP-ABE, O-HIR-CP-ABE and M-HIR-CP-ABE are $|\mathbf{I}|$, $|\mathbf{I}|$, $|\mathbf{I}|r$ respectively.

TABLE IV Storage Overhead Comparison

Setup	$m+4$	$Hm+6$	$Hm+6$
KeyGen	$\|\mathbf{S}\|+2$	$H\|\mathbf{S}\|+3$	$H\|\mathbf{S}\|+3$

TABLE V Communication Overhead Comparison

Schemes	CP-ABE	OM-HIR-CP-ABE	MM-HIR-CP-ABE
Encrypt	$2l+2$	$2l+2$	$2lr+2$

2) Storage and Communication Overhead Analysis: The main storage overheads come from the setup algorithm and key generation algorithm. The communication overheads come from the ciphertext generated by the encryption algorithm. **TABLE IV** and **TABLE V** summarize the storage and communication overhead of the three schemes.

The storage overhead in the setup algorithm of the CP-ABE scheme is $m+4$. In O-HIR-CP-ABE and M-HIR-CP-ABE, it is $mH+6$ because of the public parameters generated for hierarchical identity structure. In CP-ABE, the overhead of storing the private key is $|\mathbf{S}|+2$. In both the O-HIR-CP-ABE and the M-HIR-CP-ABE scheme, the private key storage overhead is $H|\mathbf{S}|+3$. The ciphertext size of the CP-ABE scheme and the O-HIR-CP-ABE scheme is $2l+2$. The ciphertext size of M-HIR-CP-ABE is $2lr+2$.

B. Implementation and Testing Results

The proposed schemes are implemented in C using PBC library [10] on Ubuntu 14.04 operating system. All of the results are obtained by running the programs ten times. First, we set the number of revoked identities to 1 and evaluate the relations between the number of attributes and the computation overhead. Comparisons are made for each algorithm between the CP-ABE scheme and the O-HIR-CP-ABE scheme. Furthermore, we also test how the number of revoked identities influences the computation costs of the encryption and decryption algorithm in **Fig. 6** (setup and key generation are the same in O-HIR-CP-ABE and M-HIR-CP-ABE). We set the number of attributes to be 20. The blue line represents the encryption time and the red line represents the decryption time. The overhead could be reduced in the following ways. First, the data owner could delete a group of user affiliated with the same organization with one ID. Second, M-HIR-CP-ABE could be easily parallelized. The extra overheads added by the new hierarchical identity-based revocation mechanism to the basic CP-ABE scheme is moderate. The proposed constructions of the HIR-CP-ABE schemes are efficient in practice.

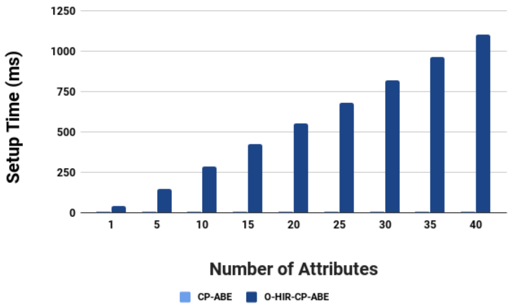

Fig. 2 Relations between the number of attributes and time consumption for setup.

VI. Related Work

Traditionally, access control is enforced based on the identity of a user, either directly or through predefined attributes. However, practitioners have noted that this access control approach usually needs cumbersome management. Meanwhile, identities, groups and roles are not sufficient in expressing the

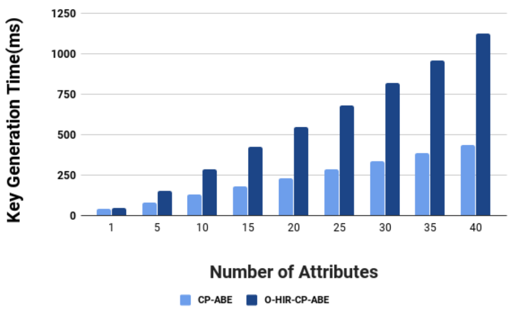

Fig. 3 Relations between the number of attributes and time consumption for key generation.

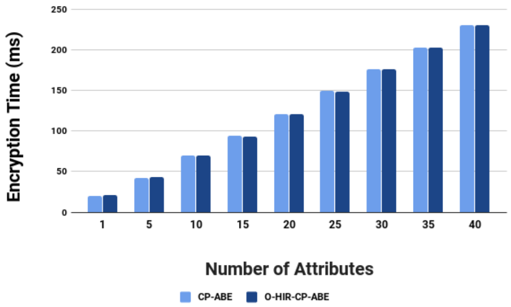

Fig. 4 Relations between the number of attributes and time consumption for encryption.

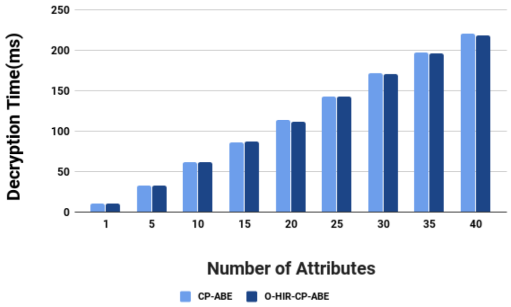

Fig. 5 Relations between the number of attributes and time consumption for decryption.

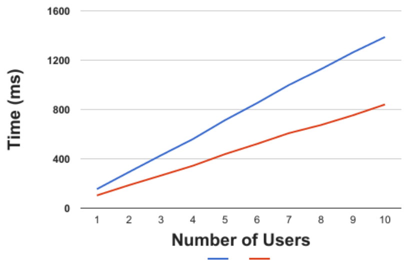

Fig. 6 Relations between the number of revoked identities and time consumption in M-HIR-CP-ABE.

access control policies in the real world. Therefore, a new approach which is referred to as attribute-based access control (ABAC) is proposed [12]. Compared with role-based access control, ABAC provides the following nice properties. First, ABAC is more expressive; Second, ABAC enables access control policy enforcement without prior knowledge of the specific subjects. Because of its flexibility, ABAC is nowadays the fastest-growing access control model [13].

There are several approaches to implementing ABAC, among which attribute-based encryption (ABE) is regarded as the most suitable one for data access control in applications scenarios where no trusted monitoring server exists. There exist two complementary forms of ABE, *i.e.*, Key-Policy ABE (KP-ABE) [14] where the decryption key is associated to the access control policy and CP-ABE [15]–[19] where the ciphertext is associated to the access control policy. CP-ABE allows data owners to define an access structure on attributes and upload the data encrypted under this access structure to the cloud servers. Therefore, CP-ABE enables users to define the attributes a data user needs to possess in order to access the data. As promising as it is, CP-ABE suffers from user revocation problem. This issue is first addressed in [20] as a rough idea. There are also several following researches [21]–[24], which as we discussed in the introduction are not applicable in some applications.

Boldyreva *et al.* [25] 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, which is also applicable to KP-ABE and fuzzy IBE user revocation. However, its applicability to CP-ABE is not clear. Libert *et al.* [26] proposed an identity-based encryption scheme with stronger adaptive-ID sense to address the selective security issue of [25]. Lewko *et al.* [27] proposed two novel broadcast encryption schemes with effective user revocation capability. 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. Chen *et al.* [29] presented an identity-based encryption scheme using lattices to realize revocation. Li *et al.* [30] first introduced outsourcing computation in identity-based encryption and presented a revocable scheme in the server-aided settings. 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.

VII. Conclusions and Future Work

In this paper, we investigate the problem of how to revoke users when applying the CP-ABE scheme for secure data sharing. Different from the previous researches on attribute-based revocation, our approach focuses on identity-based revocation mechanism. The revocation mechanism remedies the deficiencies of attribute-based revocation that cannot work without the help of the trusted authority and provides more flexible and efficient affiliation-based revocation. We propose the primitive of HIR-CP-ABE, give its security definition and present the constructions. Through analysis and experimental evaluation, we validate the security and efficiency of the proposed scheme. There are several research issues need to be further investigated. First, the revoked users' identities must be included in the ciphertext, which might lead to private information leakage. Second, in this work all the private components of a user's private key are obtained from the trusted authority, in the future we will investigate how to delegate key generation to the organizations in the hierarchical identity structure tree.

References

[1] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, 1975.

[2] R. Krishnan, J. Niu, R. Sandhu, and W. H. Winsborough, "Group-centric secure information-sharing models for isolated groups," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 3, p. 23, 2011.

[3] R. Sandhu, "Rationale for the rbac96 family of access control models," in *Proceedings of the first ACM Workshop on Role-based access control*. ACM, 1996, p. 9.

[4] X. Jin, R. Krishnan, and R. Sandhu, "A unified attribute-based access control model covering dac, mac and rbac," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2012, pp. 41–55.

[5] A. Beimel, *Secure schemes for secret sharing and key distribution*. Technion-Israel Institute of technology, Faculty of computer science, 1996.

[6] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *Public Key Cryptography - PKC 2011*. Springer-Verlag, 2011, pp. 53–70.

[7] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2011, pp. 75–86.

[8] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1343–1354, 2013.

[9] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems," *Journal of Cryptographic Engineering*, vol. 3, no. 2, pp. 111–128, 2013.

[10] B. Lynn, "The pairing-based cryptography library," 2006. [Online]. Available: https://crypto.stanford.edu/pbc/

[11] B. Li, A. P. Verleker, D. Huang, Z. Wang, and Y. Zhu, "Attribute-based access control for icn naming scheme," in *Communications and Network Security (CNS), 2014 IEEE Conference on*, 2014, pp. 391–399.

[12] V. C. Hu, D. Ferraiolo, and D. R. Kuhn, *Assessment of access control systems*. US Department of Commerce, National Institute of Standards and Technology, 2006.

[13] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone *et al.*, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST Special Publication*, vol. 800, no. 162, 2013.

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

[15] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE SP'07*, Oakland, CA, pp. 321–334.

[16] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in *ACM conference on Computer and Communications Security*, Alexandria, Virginia, USA, 2007, pp. 456–465.

[17] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Proc. of EUROCRYPT 2008*. Springer-Verlag, 2008, pp. 146–162.

[18] R. Ostrovsky and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM New York, NY, USA, 2007, pp. 195–203.

[19] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Automata, languages and programming*. Springer, 2008, pp. 579–591.

[20] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in *Secure Network Protocols, 2008. NPSec 2008. 4th Workshop on*. IEEE, 2008, pp. 39–44.

[21] ——, "Attribute-based on-demand multicast group setup with membership anonymity," *Computer Networks*, vol. 54, no. 3, pp. 377–386, 2010.

[22] B. Li, Z. Wang, and D. Huang, "An efficient and anonymous attribute-based group setup scheme," in *2013 IEEE Global Communications Conference (GLOBECOM)*, 2013, pp. 861–866.

[23] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, 2011.

[24] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*. ACM, 2013, pp. 523–528.

[25] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 417–426.

[26] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity-based encryption," in *Topics in Cryptology–CT-RSA 2009*. Springer, 2009, pp. 1–15.

[27] A. Lewko, A. Sahai, and B. Waters, "Revocation systems with very small private keys," in *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 273–285.

[28] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-based access control in social networks with efficient revocation," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ACM, 2011, pp. 411–415.

[29] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, "Revocable identity-based encryption from lattices," in *Information Security and Privacy*. Springer, 2012, pp. 390–403.

[30] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *Computers, IEEE Transactions on*, vol. 64, no. 2, pp. 425–437, 2015.

[31] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization."

[32] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2005, pp. 440–456.

Appendix A
Security Proof of Theorem 1

The generic proof template of BBG [31] and [32] is used in this proof. 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

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

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, 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. Whereas, 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.

Appendix B
Security Proof of Theorem 2

Because of limited spaces, we only provide proof of **Theorem 2**. **Theorem 3** could be proven in a similar way.

The basic idea of our proof is using the reduction technology as shown **Fig. 7**, where a simulator is constructed to simulate an O-HIR-CP-ABE game for the attacker by answering their queries and programming the challenge access structure together with the revoked identity into the public parameters. Compared with the CP-ABE security model [6], 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.

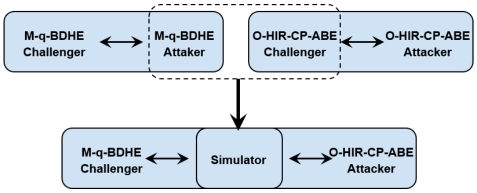

Fig. 7 Process of Reduction to the M-q-BDHE problem.

Proof. **Init** The simulator takes in an M-q-BDHE challenge $\{\mathbf{y}, T\}$. Then the adversary declares the revoked identity ID^* and gives the simulator the challenge access structure $\mathcal{A}^*$ that is described by (M^*, ρ^*), where M^* has n^* (less than q) columns. Let the challenge matrix $M^* = (\overrightarrow{M_1^*}, \cdots, \overrightarrow{M_l^*})^T$, where each row vector $\overrightarrow{M_i^*} = (M_{i,1}^*, \cdots, M_{i,n}^*)$ 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, let $g^b = g^a,\ g^{b^2} = (g^{a^2})$ to implicitly set $b = a$.

To embed the revocation identification ID^* and the challenge access structure in the public parameters $\{h_{xi}^b\}_{x \in \mathbf{U}, i \in [1,H]}$, we regard the challenge matrix M^* as a row vector set and divide it into three subsets $M^{*\prime}$, $M^{*\prime\prime}$ and $M^{*\prime\prime\prime}$ such that $M^{*\prime} \cup M^{*\prime\prime} \cup M^{*\prime\prime\prime} = M^*$ and $M^{*\prime} \cap M^{*\prime\prime} \cap M^{*\prime\prime\prime} = \emptyset$. Specifically, $M^{*\prime}$, $M^{*\prime\prime}$ and $M^{*\prime\prime\prime}$ 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 $M^{*\prime}$ and $\overrightarrow{e}$ cannot be linearly expressed by $M^{*\prime} \cup \{\overrightarrow{M_i^*}\}$, then we merge $\overrightarrow{M_i^*}$ into $M^{*\prime}$; if $\overrightarrow{M_i^*}$ is linearly independent on $M^{*\prime}$ and $\overrightarrow{e}$ can be linearly expressed by $M^{*\prime} \cup \{\overrightarrow{M_i^*}\}$, then we merge $\overrightarrow{M_i^*}$ into $M^{*\prime\prime\prime}$; if $\overrightarrow{M_i^*}$ is linearly dependent on $M^{*\prime}$, then we merge $\overrightarrow{M_i^*}$ into $M^{*\prime\prime}$. As a result, $M^{*\prime}$ is a linear independent vector group while each vector in $M^{*\prime\prime}$ can be linearly expressed by $M^{*\prime}$. Although $\overrightarrow{e}$ cannot be spanned by $M^{*\prime}$, it can be linearly expressed by $M^{*\prime}$ merged with each vector in $M^{*\prime\prime\prime}$. Therefore, each vector in M can be linearly expressed by $M^{*\prime} \cup \{\overrightarrow{e}\}$.

Next, we describe how the simulator "programs" the public parameters $\{h_{xi}^b\}_{x \in \mathbf{U}, i \in [1,H]}$. Let X denote the set of indices i, such that $\rho^*(i) = x$. Assume that there are m vectors in $M^{*\prime}$ and let $M^{*\prime} = (\overrightarrow{M_1^{*\prime}}, \cdots, \overrightarrow{M_m^{*\prime}})^T$. For each $i \in X$, its corresponding row vector $\overrightarrow{M_i^*}$ can be written as $\varepsilon_{i0}\overrightarrow{e} + \varepsilon_{i1}\overrightarrow{M_1^{*\prime}} + \cdots + \varepsilon_{im}\overrightarrow{M_m^{*\prime}}$, where $(\varepsilon_{i0}, \varepsilon_{i1}, \cdots, \varepsilon_{im}) \in Z_p^m$. For each $\overrightarrow{M_i^*}$, we define a corresponding vector $\overrightarrow{M_i^{**}}$, where $\overrightarrow{M_i^{**}} = \varepsilon_{i1}\overrightarrow{M_1^{*\prime}} + \cdots + \varepsilon_{im}\overrightarrow{M_m^{*\prime}}$. As a result, we get a new vector group $M^{**} = (\overrightarrow{M_1^{**}}, \cdots, \overrightarrow{M_l^{**}})$ and each $\overrightarrow{M_i^{**}}$ is in the span of $M^{*\prime}$. By choosing a random value z_{xi}, the simulator programs h_{xi} and h_{xi}^b as follows:

$$\begin{aligned} h_{xh} &= g^{z_{xh}} g^{-aID^*_{|h}} \textstyle\prod_{i \in X} g^{(\varepsilon_{i1}\overrightarrow{M_1^{*\prime}} +, \cdots, + \varepsilon_{im}\overrightarrow{M_m^{*\prime}}) \cdot \overrightarrow{\mu}/b_i} \\ h_{xh}^b &= g^{z_{xh}} g^{-a^2 ID^*_{|h}} (\textstyle\prod_{i \in X} \prod_{j=1}^{n} g^{M_{i,j}^{**} a^{j+1}/b_i}). \end{aligned}$$

If X is an empty set, we set $h_{xh}^b = g^{z_{xh}}$. Then the simulator publishes the above parameters $(g, g^b, g^{b^2}, \{h_{xh}^b\}_{x \in \mathbf{U}, h \in [1,H]}, e(g,g)^\alpha)$ as the public parameters.
Phase I For a query (S, ID), the simulator constructs the private key as follows. Since each $\overrightarrow{M_i^{**}}$ is in the span of $M^{*\prime}$ while $\overrightarrow{e}$ is not in the span of $M^{*\prime}$, 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

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

which implicitly sets the randomness t as

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

where $\overrightarrow{\nu} = (a^{q-1}, a^{q-2}, \cdots, a^{q-n^*+2})$. Since $g^{a^2 t}$ contains a term of $g^{-a^{q+1}}$ we can cancel out the unknown term in g^α when creating the K component in the private key. The simulator constructs K as follows.

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

For $\forall x \in \mathbf{S}$, if there is no i such that $\rho^*(i) = x$, the simulator simply sets $K_{xh} = L^{z_{xh}}$. For those used in the challenge access structure, we must make sure that there are no terms of the form g^{a^{q+1}/b_i} that the simulator cannot simulate. Since $\overrightarrow{w} \cdot M_i^{**\prime} = 0$, all of these terms can be canceled. Define X as the set of all i such that $\rho^*(i) = x$, the simulator creates K_{xh} as follows.

$$K_{xh} = (g^{z_{xh}} g^{a(ID_{|h} - ID^*_{|h})} \prod_{i \in X} g^{\overrightarrow{M_i^{**}} \cdot \overrightarrow{\mu}/b_i})^{(r + \overrightarrow{w} \cdot \overrightarrow{\nu})}$$

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 $C = \mathcal{M}_\beta T \cdot e(g^s, g^{\alpha'})$, $C' = g^s$. 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

$$\lambda_k = \overrightarrow{v} \cdot (\varepsilon_{k0}\overrightarrow{e} + \varepsilon_{k1}\overrightarrow{M_1^{*\prime}} + \varepsilon_{k2}\overrightarrow{M_2^{*\prime}} + ... + \varepsilon_{km}\overrightarrow{M_m^{*\prime}})$$

And it generates the ciphertext component C_k^* as:

$$\hat{C}_k = g^{as(M_{k1}^{**} + \varepsilon_{k0})} \cdot \prod_{i=2}^{n} g^{M_{ki}^{**} y'_i}$$

For $k = 1, \cdots, n^*$, 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:

$$\hat{C}'_k = (g^{a^2 ID^*} g^{z_{xH'}} g^{-a^2 ID^*} \prod_{i \in X_k} g^{\overrightarrow{M_i^{**}} \cdot \overrightarrow{\mu} / b_i})^{\lambda_k}$$

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.

□