Constant Ciphertext Size Multi-Authority Attribute-based Scheme without Key Escrow

Shengzhou Hu[1,4], Jiguo Li[1,2,3], Yang Lu[5], Yichen Zhang[2,3]

[1] College of Computer and Information, Hohai University, China
[2] College of Mathematics and Informatics, Fujian Normal University, China
[3] State Key Laboratory of Cryptology, P.O. Box 5159, China
[4] Mathematics and Computer Science Department, Gannan Normal University, China
[5] School of Computer Science and Technology, Nanjing Normal University, China
jxgzhsz@126.com, ljg1688@163.com, luyangnsd@163.com, zyc_718@163.com

Abstract

With the development of cloud computing application, attribute based encryption (ABE) with flexibly fine-grained data access control is adopted widely. However, the honest but curious authorities often peep at the user data. How to eliminate the key escrow is also an important and challenging problem in ABE schemes. In this paper, a constant ciphertext size multi-authority ciphertext-policy ABE scheme (RKE-MA-ABE) which resists key escrow is presented. In the proposed scheme, a user credential issuer (UCI) is introduced to generate a credential for each user credibly. UCI decentralizes the managing privilege of attribute authorities (AAs) and helps to embed the user's secret value into the decryption key issued by the corresponding AAs. Additionally, AAs in this scheme work independently without interacting with each other to generate the master public key of the system during the system initialization phase. Our scheme avoids the collusion attacks by vicious users or authorities and has constant ciphertext length. It is proven CPA-secure under the decisional q-Bilinear Diffie-Hellman Exponent (q-BDHE) assumption in random oracle model.

Keywords: Attribute-based encryption, Key escrow, Multi-authority, Constant ciphertext size

1 Introduction

One important application in cloud computing service is storing data. The data owners transmit their data up to the cloud for some specified users who consume the data after obtaining the data access privilege. In the above data service, the owners and the consumers do not conduct a direct interaction. In order to realize data confidentiality, a lot of data encryption and access control methods are adopted to protect data resources from unauthorized accessing. The first attribute-based encryption (ABE) scheme [1] was presented and used for fine-grained data access control in distributed environments. In ABE, a user's identity is determined by his/her attributes. Data encrypted with certain attribute policy is capable of being correctly decrypted by any user whose attributes match the related access policy. ABE schemes [2-9] were presented in various application domains, such as ABE with outsourced data decryption [3, 9], ABE with efficient attribute revocation [4-5], ABE with privacy preserving [8], ABE with keyword search function [2], traceable ABE [7], collusion avoidance ABE [4], auditable ABE [6] etc.

In a complex cloud computing environment, the cloud server is often operated by a commercial agency that may provide the data access privilege to unauthorized users for some benefits. So it does not always guarantee the effectiveness of the security mechanisms. In ABE, the data owners do not trust the cloud server completely, such as attribute authority (AA). AA can directly generate the corresponding decryption key without knowing the user's attributes information. We say one ABE scheme exists in the key escrow problem when AA knows the user's attribute information to generate the corresponding private key, or can directly decrypt the user's ciphertext only by using its own master key happens. AA that is controlled for vicious purpose brings huge risks in protecting data access. For the purpose of eliminating the key escrow and reduce the costs of computation and communication, we provide one multi-authority ABE scheme (RKE-MA-ABE), which resists key escrow and has constant size ciphertext.

1.1 Related Work

ABE consists of two categories, namely key-policy ABE (KP-ABE) [10] and ciphertext-policy ABE (CP-ABE) [11]. In CP-ABE model, data owners select an access structure on attributes and encrypt data. Access

[*] Corresponding Author: Jiguo Li; E-mail: ljg1688@163.com

DOI: 10.3966/160792642020112106007

structure is embedded in the ciphertext, while the secret key is produced according to the attribute set of the data user. If there is a match between the attributes listed in the ciphertext and the attributes held by a user, then the user decrypts such ciphertext [11]. There are some CP-ABE schemes [12-16], in which the size of the ciphertext grows linearly with the number of attributes embedded in access policy. Some CP-ABE schemes were realized with constant ciphertext size, such as Emura's scheme in [17]. In KP-ABE model, the encryptor selects the depictive attributes to encrypt data. The authorities collect the corresponding combinations of attributes and determine which data users decrypt such data.

Chase [18] proposed the idea of generating the user secret keys from multiple attribute authorities (AAs) for reducing the dependence on the central authority (CA). Chase's scheme has a CA. The related AAs are responsible for handing out secret keys for different sets of attributes. Every user is assigned a unique global identifier (GID) and the keys from different authorities are bound together by GID to resist the collusion attack. The scheme requires CA knowing the master secret of the system and the secrets of all AAs . Later, many researches of multi-authority attribute-based encryption scheme (MA-ABE) [19-23] have arisen. In MA-ABE, the key escrow problem is eliminated to a certain extent. MA-ABE schemes [16-20] submit the user's GID to each AA for obtaining the homologous secret keys. However, multiple authorities have chance to gather the user's attribute information via GID and make collusion attack. Chase and Chow first presented a privacy-preserving MA-ABE (PPMA-ABE) scheme [21], where the trusted central authority is removed and an anonymous key distributing protocol is adopted. As a result, a user's attributes are collected by tracing his/her GID. The authorities don't know any information about the user's GID, but they know the user's attributes. Therefore, malicious authorities exploit the consistent GID as well as some sensitive attributes for illegal activities. More specifically, multiple malicious authorities cooperate to gather a specific user's attributes by tracing his/her GID and then identify the target user or even personate him for their benefits. In order to prevent above collusion, a distributed pseudorandom functions (PRF) introduced in [22] is used to randomize one user's GID for generating many different GID names. Besides, the protection of user's privacy is also a necessary demand in actual application sometimes. Some PPMA-ABE schemes were proposed, such as [12, 22-23], in which only the privacy of GID was considered. In fact, some sensitive attributes can release user's privacy. Recently, a privacy-preserving decentralized CP-ABE (PPDCP-ABE) scheme was presented by Han et al. [13]. These schemes need anonymous certificates for users who obtain secret keys from AAs without disclosing any information of their GIDs and attributes.

In some basic CP-ABE [10-11, 24] schemes, ciphertext sizes and the number of pairing operations increase linearly with the attribute number in access structure. It limits the application of ABE, especially in the scenarios of restricted resource. Focusing on reducing computation and communication costs of ABE, a CP-ABE scheme [17] with constant ciphertext size which is (t,t)-threshold is firstly given. The first KP-ABE scheme with constant ciphertext size was constructed in [25], which allows for expressive non-monotonic access structures. Chen et al. [26] presented a CP-ABE scheme with non-monotone and-gates access structure, which was proven CPA-secure. The schemes in [27-28] is proved to be CCA-secure in the standard model by using CHK technique, which was significantly efficient. Doshi N and Jinwala [29] introduce a constant length scheme which was based on decisional bilinear Diffie-Hellman (DBDH) problem. Ge et al. [30] put forward a CPA-secure CP-ABE scheme with constant ciphertext size. A multi-authority CP-ABE with constant ciphertext length was proposed in [31]. Chen et al. [32] presented a scheme based on and-gates access structure on multi-valued attributes. Data owner (DO) firstly sends his secret value to all related AAs before encrypting message according to an access policy. AAs generate and publish a set of public attribute keys belonging to DO specially. Recently, some new type ABE schemes and novel leakage-resilient ABE schemes [33-40] were presented, which can be applied in social network and cloud storage [41-49].

1.2 Our Motivation and Contribution

In this paper, we present an RKE-MA-ABE scheme on the basis of the access structure of and-gates on multi-valued attributes. Specifically, the main contributions are listed as below.

(1) Our scheme resists key escrow problem in the case that the target ciphertexts are directly decrypted by the related AAs who know their own master keys respectively.

In this scheme, we introduce a user's credential issuer UCI who issues the user's credential. We think that any system needs a role or mechanism, just like UCI , to check the user's legality. If any person can optionally pretend other legal identities to visit a system, then there is no any security in this system.

Specifically, let $\widetilde{AA_\delta}$ denote the δ -th attribute authority, α_δ denote the master key of $\widetilde{AA_\delta}$, g denote one element of one group, e be a bilinear map. For an attribute $v_{i,j}$ of a legal user U with the global identifier GID_U , UCI issues a credential $Cred^U_{v_{i,j},\delta}$ which is embedded with U's secret value ϖ_U and UCI's secret value π. U can decrypt ciphertext only by using ϖ_U and its private key received from the related AAs simultaneously. For instance, in order to resist key escrow problem, for the public parameter $e(g,g)^{\alpha_\delta}$ issued by $\widetilde{AA_\delta}$, UCI computes $e(g,g)^{\alpha_\delta \cdot \pi}$ which can prevent vicious $\widetilde{AA_\delta}$ from decrypting the target ciphertext blinded with $e(g,g)^{\alpha_\delta}$ directly since $\widetilde{AA_\delta}$ knows α_δ but do not know π. $Cred^U_{v_{i,j},\delta}$ has bound these messages $g^{\pi/\varpi_U}, (GID_U)^{1/\varpi_U}, v_{i,j}, \widetilde{AA_\delta}$ together, which are signed by UCI. $\widetilde{AA_\delta}$ authenticates U's identity and generates the related private key of $v_{i,j}$ after verifying $Cred^U_{v_{i,j},\delta}$ successfully.

(2) Our scheme achieves collusion-resistant among vicious AAs.

To create U's whole private key, we use global identifier GID_U to combine attribute-related private keys from different AAs together. Our scheme achieves collusion-resistant among vicious AAs since AAs do not provide the effective complete decryption key which includes the secret value ϖ_U only known by U. Unlike CA in the scheme [18] that uses the key randomization techniques to solve the collusion problem, UCI does not become a vulnerable point on security attacks because it does not grasp all master keys of AAs.

Our scheme is proven CPA-secure in random oracle model under the decision q-Bilinear Diffie-Hellman exponent (q-BDHE) [24] assumption and also can be extended to CCA security by using the CHK technology.

(3) Our scheme has good efficiency. It has low computation and communication costs because of constant ciphertext length and constant number of pairing operations. Those corresponding additional credentials for users are precomputed in initialization phase. Compared with scheme [32], our scheme is more reasonable in system structure. Authorities do not interact with each other for generating public information during the initialization phase. The master keys of AAs are generated by AAs themselves independently, rather than by data owner (DO) and AAs jointly.

1.3 Paper Organization

The related work is introduced in Section 1. The preliminaries are introduced in Section 2. In Section 3, our scheme is proposed and its security is proved in Section 4. Subsequently, we give the performance comparison between some CP-ABE schemes and our scheme in Section 5. Finally, we conclude our paper in Section 6.

2 Preliminaries

2.1 Access Structure

Our scheme adopts and-gates on multi-valued attributes access structure. Let $\aleph = \{att_1, \cdots, att_n\}$ denote the set of n attributes in this scheme. $\widehat{S_{att_i}} = \{v_{i,1}, \cdots, v_{i,n_i}\}$ denotes the set of possible n_i values for att_i. For the user U, $\widehat{U} = \{\gamma_1, \cdots, \gamma_{n_U}\}$ $(1 \le n_U \le n)$ is the set of U's attributes, in which each γ_i denotes one attribute value of attribute att_i and $\gamma_i \in \widehat{S_{att_i}}$. Let W_i denote an attribute value of att_i and $W_i \in \widehat{S_{att_i}}$. $\overline{\overline{W}} = \{W_1, \cdots, W_m\} (1 \le m \le n)$ can be denoted by one access structure.

2.2 Bilinear Map

Let G and G_T be two multiplicative cyclic groups with prime order p. Let g be a generator of G. Let $e: G \times G \to G_T$ be a bilinear map and e satisfies the following properties:

(1) Bilinearity: for all $\eta, \sigma \in Z_p, e(g^\eta, g^\sigma) = e(g,g)^{\eta\sigma}$.

(2) Non-degeneracy: $e(g,g) \ne 1$.

(3) Computability: There exits an efficient algorithm to compute $e(\lambda, \Im)$ for $\forall \lambda, \Im \in G$.

2.3 Decisional q-Bilinear Diffie-Hellman Exponent (q-BDHE) Assumption [24]

Assume that $s, a, q \in Z_p$ are randomly selected, $e: G \times G \to G_T$ is a bilinear map and g is a generator of G. Given a tuple $\vec{Y} =< g, g^s, g^a, \cdots, g^{a^q}, g^{a^{q+2}}, \cdots, g^{(a^{2q})} >$, a probabilistic polynomial time adversary $\widehat{\mathcal{A}}$ does not make a distinction between $e(g,g)^{a^{q+1} \cdot s}$ and a random element $\Re \in G_T$ with the advantage $adv_{\mathcal{A}} =| \Pr[\widehat{\mathcal{A}}(\vec{Y}, e(g,g)^{a^{q+1} \cdot s}) = 1] - \Pr[\widehat{\mathcal{A}}(\vec{Y}, \Re) = 1] | \ge \varepsilon$, where ε is a non-negligible function, then we state that the decisional q-BDHE assumption holds.

2.4 Outline of Our Scheme

2.4.1 System Model

As shown in Figure 1, we propose a scheme which includes four types of roles in the system: User's credential issuer (UCI), Attribute authorities (AAs), Data owner (DO), Data user (DU).

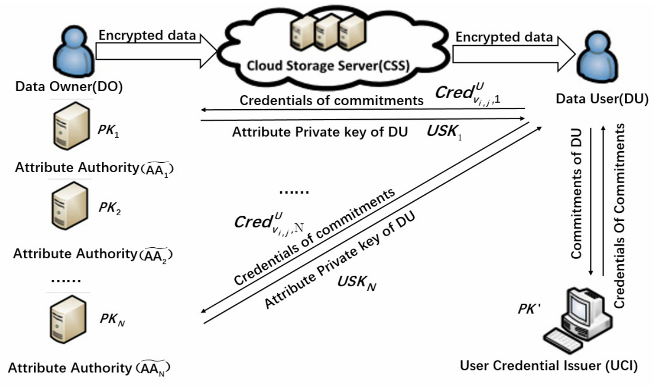

Encrypted data
Cloud Storage Server(CSS)
Encrypted data
Data Owner(DO)
Data User(DU)
Credentials of commitments $Cred^{U}_{v_{i,j},1}$
Attribute Private key of DU USK_1
PK_1
Attribute Authority($\widetilde{AA_1}$)
......
PK_2
Attribute Authority($\widetilde{AA_2}$)
......
$Cred^{U}_{v_{i,j},N}$
Credentials of commitments
Attribute Private key of DU
USK_N
Commitments of DU
Credentials Of Commitments
PK_N
PK'
Attribute Authority ($\widetilde{AA_N}$)
User Credential Issuer (UCI)

Figure 1. Our system model

Assume there are N AAs, $\widetilde{AA}_1, \widetilde{AA}_2, \cdots, \widetilde{AA}_N$. A data user DU submits his/her legal identity identifier and commitment value which hides his/her secret value to UCI. After checking DU's identity successfully, UCI generates and returns the corresponding credentials of DU's commitment to DU. When DU applies for the decryption key from related AAs, DU must submit the credentials to AAs at the same time. Then, AAs verify the signatures in credentials. Once AAs succeed in verifying the identity of DU, AAs compute the private key for DU respectively.

2.4.2 Algorithm Definition

$GlobalSetup(1^{\lambda}) \rightarrow Params$. Inputing the security parameter 1^{λ}, the algorithm establishes the system, and exports the public parameters $Params$.

$AASetup(Params) \rightarrow \{PK_{\delta}, SK_{\delta}\}$. Inputing $Params$, the algorithm exports a public-secret key pair $(PK_{\delta}, SK_{\delta})$ for each attribute authority $\widetilde{AA}_{\delta}$.

$UCISetup(Params, PK) \rightarrow \{PK', \pi, \chi, g^{\chi}\}$. Inputing $Params$ and $PK = \{PK_{\delta}\}_{\delta \in \{1,2,\cdots,N\}}$ generated by AAs, the algorithm exports one public key g^{χ} and two private keys π, χ, a public parameter set PK' which includes the UCI's signatures on master public keys of related AAs in PK.

$$UserCredential(Params, < Id_U, GID_U, \widehat{U}, g^{1/\varpi_U} >, \pi, \chi) \rightarrow \{Cred^{U}_{v_{i,j},\delta}\}_{v_{i,j} \in \widehat{U} \cap \widehat{AA_{\delta}} \neq \varnothing, \delta \in \{1,2,\cdots,N\}}.$$

This is an interactive procedure between UCI and the user U in secure communication channel. After receiving messages including the real identity Id_U, the global name GID_U, attribute set $\widehat{U}$ and the commitment g^{1/ϖ_U} from U and checking U's identity successfully, UCI generates the credential $Cred^{U}_{v_{i,j},\delta}$ for $v_{i,j} \in \widehat{U} \cap \widehat{AA_{\delta}}, \delta \in \{1,2,\cdots,N\}$ by using its secret values π, χ.

$Encrypt(Params, PK', PK, M, \overset{\frown}{W}) \rightarrow CT$. The algorithm inputs $Params$, PK', PK, a message M, and an access structure $\overset{\frown}{W}$. It exports a ciphertext CT.

$KeyGen(Params, \{Cred^{U}_{v_{i,j},\delta}, SK_{\delta}\}_{\delta \in \{1,2,\cdots,N\}, v_{i,j} \in \widehat{U} \cap \widehat{AA_{\delta}} \neq \varnothing}, \varpi_U) \rightarrow USK_U$. The algorithm inputs $Params$, U's identity credentials $\{Cred^{U}_{v_{i,j},\delta}\}_{\delta \in \{1,2,\cdots,N\}, v_{i,j} \in \widehat{U} \cap \widehat{AA_{\delta}} \neq \varnothing}$, the private key set $\{SK_{\delta}\}_{\delta \in \{1,2,\cdots,N\}, v_{i,j} \in \widehat{U} \cap \widehat{AA_{\delta}} \neq \varnothing}$ generated by related AAs and secret value ϖ_U generated by U. It outputs U's private key $USK_U = (\prod_{\delta \in \{1,2,\cdots,N\}, v_{i,j} \in \widehat{U} \cap \widehat{AA_{\delta}} \neq \varnothing} USK_{\delta})^{\varpi_U}$.

$Decrypt(Params, CT, USK_U) \rightarrow M$. Inputing $Params$, U's private key USK_U and ciphertext CT, the algorithm exports M.

2.5 Security Model

Suppose that $\widehat{\mathcal{B}}$ acts as the challenger and $\widehat{\mathcal{A}}$ acts as the adversary in the game. We present the security game as follows:

Init. An access structure $\overset{\frown}{W^*}$ selected by $\widehat{\mathcal{A}}$ is given to $\widehat{\mathcal{B}}$ for a challenge.

Setup. $\widehat{\mathcal{B}}$ runs $GlobalSetup$, $AASetup$ to generate the private key set SK_{δ} and the public key set PK_{δ} for $\widetilde{AA}_{\delta}$. $\widehat{\mathcal{B}}$ sends $\{PK_{\delta}\}_{\delta \in \{1,2,\cdots,N\}}$ to $\widehat{\mathcal{A}}$.

Phase 1. $\widehat{\mathcal{A}}$ makes some legal users to apply for corresponding identity credentials from UCI. In particular, a user U's attribute set $\widehat{U}$ does not satisfy the challenge access structure $\overset{\frown}{W^*}$, which is denoted by $\widehat{U} \mid\neq \overset{\frown}{W^*}$. U applies for his/her identity credential by sending his/her identity information and commitment value including his/her secret value to UCI. After verifying his/her identity successfully, UCI gives the corresponding credentials to U. We assume that adversary $\widehat{\mathcal{A}}$ knows U's credential information since they are intimate partners. Next, $\widehat{\mathcal{A}}$ adaptively queries $\widehat{\mathcal{B}}$ for its private keys by using above credential. The challenger $\widehat{\mathcal{B}}$ responses the private key USK_U for U. These queries are repeated adaptively.

Challenge. $\widehat{\mathcal{A}}$ hands over two messages M_1 and M_2. $\widehat{\mathcal{B}}$ randomly selects $\tau \in \{0,1\}$ and encrypts M_{τ} based on $\overset{\frown}{W^*}$. This corresponding ciphertext CT^* is outputed to $\widehat{\mathcal{A}}$.

Phase 2. Same as Phase 1.

Guess. The adversary $\widehat{\mathcal{A}}$ exports a guess τ' of τ and defines $\Pr[\tau = \tau'] - \frac{1}{2}$ as the advantage of $\widehat{\mathcal{A}}$ in the above game.

Definition1. The RKE-MA-ABE scheme is selective-access structure secure if no probably polynomial-time adversary $\widehat{\mathcal{A}}$ wins this game with the advantage $|\Pr(\tau' = \tau) - \frac{1}{2}| > \varepsilon$. Here, ε is a non-negligible probability.

3 The Proposed Scheme

GlobalSetup. There is a bilinear map $e: G \times G \to G_T$, where G and G_T are two multiplicative cyclic groups with prime order p. g is a generator of G. This algorithm chooses two cryptographic hash functions $H_1: \{0,1\}^* \to G$ and $H_2: G \times G \times \{0,1\}^* \times \{0,1\}^* \to G$. Suppose N authorities $\{\widetilde{AA_1}, \widetilde{AA_2}, \cdots, \widetilde{AA_N}\}$ are created. Each authority $\widetilde{AA_\delta}$ $(\delta \in \{1,2,\cdots,N\})$ manages an attribute set $\widehat{AA_\delta}$.. A user's credential issuer UCI is established. $H_1(\cdot)$ is sent to UCI and $H_2(\cdot)$ is published.

AASetup. Each authority $\widetilde{AA_\delta}$ randomly selects $\alpha_\delta \in \mathbb{Z}_p$ as its master key and calculates $e(g,g)^{\alpha_\delta}$.. For $\forall$ $\widehat{AA_{\delta_1}}, \widehat{AA_{\delta_2}}$, $\delta_1, \delta_2 \in \{1,2,\cdots,N\}$, $\delta_1 \neq \delta_2$, they always satisfy $\widehat{AA_{\delta_1}} \cap \widehat{AA_{\delta_2}} = \varnothing$. Let $n_{\widehat{AA_\delta}}$ denote the attribute number of $\widehat{AA_\delta}$. n_{att_i} represents the number of the values of the attribute att_i. Aiming at one attribute value $v_{i,j} \in \widehat{AA_\delta}$, $\widetilde{AA_\delta}$ randomly chooses $r_{i,j} \in \mathbb{Z}_p (1 \le i \le n_{\widehat{AA_\delta}}, 1 \le j \le n_{att_i})$ as the private attribute key. Then $\widetilde{AA_\delta}$ calculates the corresponding public attribute key $u_{i,j} = g^{-r_{i,j}}$. $\widetilde{AA_\delta}$ finally publishes the set of public key.

$$PK_\delta = \{e(g,g)^{\alpha_\delta}, \{u_{i,j}\}_{v_{i,j} \in \widehat{AA_\delta}}\} \quad \textbf{(1)}$$

and generates the private key set.

$$SK_\delta = \{\alpha_\delta, \{r_{i,j}\}_{v_{i,j} \in \widehat{AA_\delta}}\} \quad \textbf{(2)}$$

UCISetup. UCI randomly chooses $\pi, \chi \in \mathbb{Z}_p$. For $PK = \{PK_\delta\}_{\delta \in \{1,2,\cdots,N\}}$ generated by AAs, UCI computes $\{e(g,g)^{\alpha_\delta \cdot \pi}\}_{\delta \in \{1,2,\cdots,N\}}$ and g^χ. The algorithm keeps π, χ secret and publishes extended public key.

$$PK^{'} = \{g^\chi, \{e(g,g)^{\alpha_\delta \cdot \pi}\}_{\delta \in \{1,2,\cdots,N\}}\} \quad \textbf{(3)}$$

UserCredential. This is an interactive procedure between UCI and the user U in secure channel. Suppose there is ξ authorities such that $\widehat{AA_\delta} \cap \widehat{U} \neq \varnothing$, $\delta \in \{1,2,\cdots,\xi\}$. Let $N_{\widetilde{AA_\delta}}$ denote the name of $\widetilde{AA_\delta}$. The interactive procedure is described as below:

U sends to $UCI: Id_U, GID_U$.

UCI responses to $U: Id_U, H_1(GID_U)$.

U sends to $UCI: Id_U, H_1(GID_U)^{1/\varpi_U}, \widehat{U}, g^{1/\varpi_U}$

If Id_U is valid and $e(H_1(GID_U)^{1/\varpi_U}, g) = e(H_1(GID_U), g^{1/\varpi_U})$ then

UCI responses to U : $\{Cred^U_{v_{i,j},\delta}\}_{v_{i,j} \in \widehat{U} \cap \widehat{AA_\delta}, \delta \in \{1,2,\cdots,\xi\}}$, i.e.,

$\{g^{\pi/\varpi_U}, H_1(GID_U)^{1/\varpi_U}, v_{i,j}, N_{\widetilde{AA_\delta}}, (H_2(g^{\pi/\varpi_U}, H_1(GID_U)^{1/\varpi_U}, v_{i,j}, N_{\widetilde{AA_\delta}}))^\chi\}_{v_{i,j} \in \widehat{U} \cap \widehat{AA_\delta}, \delta \in \{1,2,\cdots,\xi\}}$.

The credential $Cred^U_{v_{i,j},\delta}$ illustrates the binding relationship of these messages $g^{\pi/\varpi_U}, (GID_U)^{1/\varpi_U}, v_{i,j}, N_{\widetilde{AA_\delta}}$.

Encrypt. This algorithm encrypts a message $M \in G_T$ according to an access structure $\widehat{W} = \{W_1, W_2, \cdots, W_m\}$. Suppose there are ζ authorities such that $\widehat{AA_\delta} \cap \widehat{W} \neq \varnothing, \delta \in \{1,2,\cdots,\zeta]$. This algorithm selects a random number $s \in \mathbb{Z}_p$ and calculates the ciphertext CT.

$$CT =< C_1 = g^s, C_2 = (\prod_{v_{i,j} \in \widehat{W}} g^{-r_{i,j}})^s, C_3 = M \cdot (\prod_{\delta \in \{1,2,\cdots,\zeta]} e(g,g)^{\alpha_\delta \cdot \pi})^s, \widehat{W} > \quad \textbf{(4)}$$

KeyGen. Each $\widetilde{AA_\delta}$ generates the private key as follows: U submits the $Cred^U_{v_{i,j},\delta}$ to $\widetilde{AA_\delta}$. $\widetilde{AA_\delta}$ decides that $Cred^U_{v_{i,j},\delta}$ is valid if $e(H_2(g^{\pi/\varpi_U}, H_1(GID_U)^{1/\varpi_U}, v_{i,j}, N_{\widetilde{AA_\delta}}), g^\chi) = e(H_2(g^{\pi/\varpi_U}, H_1(GID_U)^{1/\varpi_U}, v_{i,j}, N_{\widetilde{AA_\delta}})^\chi, g)$ for $v_{i,j} \in \widehat{U} \cap \widehat{AA_\delta}$. After successfully verifying the legitimacy of the signatures, $\widetilde{AA_\delta}$ computes $g^{\frac{\pi}{\varpi_U} \cdot \frac{1}{n_\delta} \cdot \alpha_\delta} \cdot H_1(GID_U)^{\frac{1}{\varpi_U} \cdot r_{i,j}}$ $(n_\delta = |\widehat{U} \cap \widehat{AA_\delta}|)$ for $v_{i,j} \in \widehat{U} \cap \widehat{AA_\delta}$. The private key is $\prod_{\delta \in \{1,2,\cdots,\xi\}, n_\delta = |\widehat{U} \cap \widehat{AA_\delta}|} \prod_{v_{i,j} \in \widehat{U} \cap \widehat{AA_\delta}} (g^{(\pi/\varpi_U) \cdot (1/n_\delta) \cdot \alpha_\delta} \cdot H_1(GID_U)^{(1/\varpi_U) \cdot r_{i,j}})$, which is sent to U. Then U calculates the final private key.

$$USK_U = \Big(\prod_{\delta\in\{1,2,\cdots,\xi\}, n_\delta=|\widehat{U}\cap\widehat{AA_\delta}|} \prod_{v_{i,j}\in\widehat{U}\cap\widehat{AA_\delta}} (g^{(\pi/\varpi_U)\cdot(1/n_\delta)\cdot\alpha_\delta} \cdot H_1(GID_U)^{(1/\varpi_U)\cdot r_{i,j}}) \Big)^{\varpi_U} \quad \textbf{(5)}$$
$$= \prod_{\delta\in\{1,2,\cdots,\xi\}, n_\delta=|\widehat{U}\cap\widehat{AA_\delta}|} \prod_{v_{i,j}\in\widehat{U}\cap\widehat{AA_\delta}} (g^{\pi\cdot(1/n_\delta)\cdot\alpha_\delta} \cdot H_1(GID_U)^{r_{i,j}})$$

ϖ_U is the secret key only known by U.

Decrypt. Assume there is a user U with $\widehat{W}\subseteq\widehat{U}$. The algorithm collects the private keys related to the attribute values in $\widehat{W}$ and generates the corresponding private key $USK_{\widehat{W}}$. Then it performs the decryption as follows:

$$\frac{C_3}{e(H_1(GID_U), C_2)\cdot e(USK_{\widehat{W}}, C_1)}$$
$$= \frac{M\cdot(\prod_{\delta\in[1,2,\cdots,\zeta]} e(g,g)^{\alpha_\delta})^{s\cdot\pi}}{e(H_1(GID_U), (\prod_{v_{i,j}\in\widehat{W}} g^{-r_{i,j}})^s)} \quad \textbf{(6)}$$
$$\cdot \frac{1}{e(\prod_{\delta\in[1,2,\cdots,\zeta], n_\delta=|\widehat{W}\cap\widehat{AA_\delta}|} \prod_{v_{i,j}\in\widehat{W}\cap\widehat{AA_\delta}} g^{\pi\cdot(1/n_\delta)\cdot\alpha_\delta} H_1(GID_U)^{r_{i,j}}, g^s)}$$
$$= M$$

4 Security Analysis

Theorem 1: The RKE-MA-ABE scheme is secure in the selective-access structure model if the decisional q-BDHE assumption holds.

Proof. We show a simulator $\widehat{\mathcal{B}}$ is built to break the decisional q-BDHE assumption by using the adversary $\widehat{\mathcal{A}}$, who breaks the RKE-MA-ABE with non-negligible probability ε in the selective-access structure security game.

Init. $\widehat{\mathcal{B}}$ takes in q-BDHE challenge with a tuple $(g, a, q, h = g^s, \vec{Y})$. Suppose that ∂ is randomly selected from $\{0,1\}$. Assume $T = e(g^s, g^{-a^{q+1}})$ if $\partial = 1$ and T is a random value in G_T if $\partial = 0$. $\widehat{\mathcal{A}}$ provides the challenge access structure $\widehat{W^*} = \{W_1^*, W_2^*, \cdots, W_m^*\}$, where $m = |\widehat{W^*}|$ and $i_{I_*} = \{i_1, i_2, \cdots, i_m\}$ denotes the index set of attribute value in $\widehat{W^*}$.

Setup. Let n be the number of all attributes. k is an arbitrary attribute index and n_{att_k} is the number of attribute value for attribute att_k. For att_k, $\widehat{\mathcal{B}}$ randomly chooses $r_{i,j}\in\mathbb{Z}_p$ as private attribute key for $1\le i\le n, 1\le j\le n_{att_k}$. I^* denotes the set of index for attribute values in $\widehat{W^*}$. For $w\in I^*$, $\widehat{\mathcal{B}}$ randomly selects $r_{i_w}\in\mathbb{Z}_p$ as the private attribute key of the corresponding attribute value in $\widehat{W^*}$. Moreover, $\widehat{\mathcal{B}}$ randomly selects a challenge index $w^*\in\{1,2,\cdots,m\}$ and the corresponding private attribute key $r_{i_{w^*}}\in\mathbb{Z}_p$.

For $v_{i,j}$ with $i = w\in I^* - \{w^*\}$, $\widehat{\mathcal{B}}$ produces the public attribute key as follows:

if $v_{i,j} = W_i^*, u_{i_w} = g^{r_{i_w}} g^{-a^{q+1-i_w}}$;

if $v_{i,j} \ne W_i^*, u_{i,j} = g^{-r_{i,j}}$.

For $v_{i,j}$ with $i = w^*$, $\widehat{\mathcal{B}}$ produces the public attribute key as follows:

if $v_{i,j} = W_i^*, u_{i_{w^*}} = g^{r_{i_{w^*}}} \prod_{k\in I^*-\{w^*\}} g^{a^{q+1-i_k}}$;

if $v_{i,j} \ne W_i^*, u_{i,j} = g^{-r_{i,j}}$.

For $v_{i,j}$ with $i\notin I^*$, $\widehat{\mathcal{B}}$ produces the public attribute key $u_{i,j} = g^{-r_{i,j}}$.

Phase 1. Assume $\widehat{\mathcal{A}}$ obtains corresponding identity credentials of some legal users who are intimate partners of $\widehat{\mathcal{A}}$ from UCI. Assume there are ξ authorities. A user $U(\widehat{\mathcal{A}})$ with $\widehat{U}|\ne\widehat{W^*}$ and $\widehat{AA_\delta}\cap\widehat{U}\ne\varnothing$, $\delta\in\{1,2,\cdots,\xi\}$ wants to apply for his/her credential. $\widehat{AA_\delta}$ denotes the attribute set of attribute authority $\widetilde{AA_\delta}$. The concrete processes are listed as follows:

$U(\widehat{\mathcal{A}})$ sends to $UCI : Id_U, GID_U$.

UCI responses to $U(\widehat{\mathcal{A}}) : Id_U, H_1(GID_U)$.

$U(\widehat{\mathcal{A}})$ sends to $UCI : Id_U, H_1(GID_U)^{1/\varpi_U}, \widehat{U}, g^{1/\varpi_U}$.

If Id_U is valid and $e(H_1(GID_U)^{1/\varpi_U}, g) = e(H_1(GID_U), g^{1/\varpi_U})$ then UCI responses to $U(\widehat{\mathcal{A}})$: $\{Cred_{v_{i,j},\delta}^U\}_{v_{i,j}\in\widehat{U}\cap\widehat{AA_\delta}, \delta\in\{1,2,\cdots,\xi\}}$.

$$\{Cred_{v_{i,j},\delta}^U\}_{v_{i,j}\in\widehat{U}\cap\widehat{AA_\delta}, \delta\in\{1,2,\cdots,\xi\}} =$$
$$\{g^{\pi/\varpi_U}, H_1(GID_U)^{1/\varpi_U}, v_{i,j}, N_{\widetilde{AA_\delta}}, H_2(g^{\pi/\varpi_U}, \quad \textbf{(7)}$$
$$H_1(GID_U)^{1/\varpi_U}, v_{i,j}, N_{\widetilde{AA_\delta}})^{\chi}\}_{v_{i,j}\in\widehat{U}\cap\widehat{AA_\delta}, \delta\in\{1,2,\cdots,\xi\}}$$

Above communication between UCI and $U(\widehat{\mathcal{A}})$ is performed over secure channel. $\widehat{\mathcal{A}}$ knows U's credential information for the relationship of intimate partner.

Next, $\widehat{\mathcal{A}}$ queries the private key of U with GID_U and the attribute set $\widehat{U}(\widehat{U}|\ne\widehat{W^*})$. Without loss of generality, we suppose that an necessary attribute value of $att_{w'}$ in $\widehat{U}$ is $v_{w',j}$ such that $v_{w',j}\notin\widehat{W^*}$ and $w'\in I^*$.

$\widehat{\mathcal{B}}$ runs the random oracle $H_1(x)$ which is defined in a table Γ. $\widehat{\mathcal{A}}$ submits GID_U to $\widehat{\mathcal{B}}$. If $H_1(GID_U)$ exists in Γ then $\widehat{\mathcal{B}}$ returns the same answer as before. If not, $\widehat{\mathcal{B}}$ selects a random value $\iota \in \mathbb{Z}_p$, and computes $H_1(GID_U) = g^{a^{i_{w'}}} g^{\iota}$. By calling *KeyGen* algorithm, $\widehat{\mathcal{B}}$ answers the query of a private key issued by $\widehat{\mathcal{A}}$ as follows:

(1) For $v_{i,j} \in \widehat{AA_\delta} \cap \widehat{U}$, $i = w'$, $\widehat{\mathcal{B}}$ randomly selects $\alpha_\delta \in \mathbb{Z}_p$ as the private key of $\widetilde{AA_\delta}$ who monitors $v_{w',j}$. $\widehat{AA_\delta}$ denotes the attribute set of $\widetilde{AA_\delta}$. For $v_{w',j}$, $\widehat{\mathcal{B}}$ randomly selects $r_{w',j} \in \mathbb{Z}_p$ and computes the private key element $\varsigma_{w',j}$.

$$\varsigma_{w',j} = g^{\alpha_\delta \cdot (\pi/\varpi_U)\cdot(1/n_\delta)} (g^{a^{i_{w'}}} g^{\iota})^{r_{w',j}\cdot(1/\varpi_U)}, n_\delta = |\widehat{AA_\delta} \cap \widehat{U}| \tag{8}$$

(2) For $v_{i,j} \in \widehat{AA_\delta} \cap \widehat{U}$, $i \neq w'$, $\widehat{\mathcal{B}}$ generates the private key as follows.

For $v_{i,j} \in \widehat{W^*}$, $i \in I^*$, $i = w^*$, $\widehat{\mathcal{B}}$ randomly chooses $\alpha' \in \mathbb{Z}_p$ and computes $n_{\delta*} = |\widehat{AA_{\delta*}} \cap \widehat{U}|$. Let $\alpha = (1/n_{\delta*}) \cdot \alpha' - a^{q+1} \cdot (1/\pi)$ denote the master key of $\widetilde{AA_{\delta*}}$. We have $e(g^\alpha, g) = e(g^{(1/n_{\delta*})\cdot\alpha'}, g) \cdot e(g,g)^{-a^{q+1}\cdot(1/\pi)}$. $\widehat{\mathcal{B}}$ randomly selects $r_{i_{w*}} \in \mathbb{Z}_p$ and generates $\varsigma_{i_{w*}}$ for $v_{i_{w*}}$.

$$\varsigma_{i_{w*}} = g^{\alpha\cdot(\pi/\varpi_U)} ((g^{a^{i_{w'}}})^{-r_{i_{w*}}} (\prod_{k\in I^*-\{w^*\}}^{i_k \neq i_{w'}} g^{-a^{q+1-i_k+i_{w'}}})(u_{i_{w^*}})^{-\iota})^{1/\varpi_U} \tag{9}$$

$\varsigma_{i,j}$ is well formed as being shown in the following equation.

$$\begin{aligned}
&\varsigma_{i,j} = \varsigma_{i_{w*}} \\
&= g^{\alpha\cdot(\pi/\varpi_U)} ((g^{a^{i_{w'}}})^{-r_{i_{w*}}} (\prod_{k\in I^*-\{w^*\}}^{i_k \neq i_{w'}} g^{-a^{q+1-i_k+i_{w'}}})(u_{i_{w^*}})^{-\iota})^{1/\varpi_U} \\
&= g^{\alpha\cdot(\pi/\varpi_U)} ((g^{a^{i_{w'}}})^{-r_{i_{w*}}} \\
&\cdot(\prod_{k\in I^*-\{w^*\}}^{i_k \neq i_{w'}} g^{-a^{q+1-i_k+i_{w'}}})(g^{r_{i_{w*}}} \prod_{k\in I^*-\{w^*\}} g^{a^{q+1-i_k}})^{-\iota})^{1/\varpi_U} \\
&= (g^{(1/n_{\delta*})\cdot\alpha'} g^{-a^{q+1}\cdot(1/\pi)})^{\cdot\pi/\varpi_U} ((g^{r_{i_{w*}}})^{-(a^{i_{w'}}+\iota)} \\
&\cdot(\prod_{k\in I^*-\{w^*\}}^{i_k \neq i_{w'}} g^{a^{q+1-i_k}})^{-a^{i_{w'}}} (\prod_{k\in I^*-\{w^*\}} g^{a^{q+1-i_k}})^{-\iota})^{1/\varpi_U} \\
&= g^{(\pi/\varpi_U)\cdot(1/n_{\delta*})\cdot\alpha'} ((g^{a^{i_{w'}}} g^{\iota})^{-(r_{i_{w*}} + \sum_{k\in I^*-\{w^*\}} (a^{q+1-i_k}))})^{1/\varpi_U}.
\end{aligned} \tag{10}$$

For $v_{i,j} \in \widehat{W^*}$, $k = i \in I^*$, $i_k \in i_{I^*} - \{i_{w*}\}$, $\widehat{\mathcal{B}}$ randomly chooses $\alpha_\delta \in \mathbb{Z}_p$ or adopts the existed α_δ ($\widetilde{AA_\delta}$'s master key has been created before) as the master key of $\widetilde{AA_\delta}$. Then $\widehat{\mathcal{B}}$ randomly selects $r_{i_k} \in \mathbb{Z}_p$, computes $n_\delta = |\widehat{AA_\delta} \cap \widehat{U}|$ and generates $\varsigma_{i,j}$.

$$\varsigma_{i,j} = \varsigma_{i_k} = g^{\alpha_\delta\cdot(\pi/\varpi_U)\cdot(1/n_\delta)} ((g^{a^{i_{w'}}})^{-r_{i_k}} g^{a^{q+1-i_k+i_{w'}}} (u_{i_k})^{-\iota})^{1/\varpi_U} \tag{11}$$

where $k \neq w^*$. $\varsigma_{i,j}$ is well formed as being shown in the following equation.

$$\begin{aligned}
&\varsigma_{i,j} = \varsigma_{i_k} \\
&= g^{\alpha_\delta\cdot(\pi/\varpi_U)\cdot(1/n_\delta)} ((g^{a^{i_{w'}}})^{-r_{i_k}} g^{a^{q+1-i_k+i_{w'}}} (u_{i_k})^{-\iota})^{1/\varpi_U} \\
&= g^{\alpha_\delta\cdot(\pi/\varpi_U)\cdot(1/n_\delta)} ((g^{a^{i_{w'}}})^{-r_{i_k}} (g^{a^{q+1-i_k}})^{a^{i_{w'}}} (g^{r_{i_k}} g^{-a^{q+1-i_k}})^{-\iota})^{1/\varpi_U} \\
&= g^{\alpha_\delta\cdot(\pi/\varpi_U)\cdot(1/n_\delta)} ((g^{a^{i_{w'}}} g^{\iota})^{(-r_{i_k} + a^{q+1-i_k})})^{1/\varpi_U}
\end{aligned} \tag{12}$$

For $v_{i,j} \notin \widehat{W^*}$, $\widehat{\mathcal{B}}$ randomly selects $\alpha_\delta \in \mathbb{Z}_p$ or adopts the existed α_δ ($\widetilde{AA_\delta}$'s master key has been created before) as the master key of $\widetilde{AA_\delta}$. Then $\widehat{\mathcal{B}}$ computes $n_\delta = |\widehat{AA_\delta} \cap \widehat{U}|$ and generates $\varsigma_{i,j}$.

$$\varsigma_{i,j} = g^{\alpha_\delta\cdot(\pi/\varpi_U)\cdot(1/n_\delta)} (g^{a^{i_{w'}}} g^{\iota})^{r_{i,j}\cdot(1/\varpi_U)} \tag{13}$$

At last, $\widehat{\mathcal{B}}$ gives the private key $< \forall v_{i,j} \in \widehat{U}, \varsigma_{i,j} >$ to $\widehat{\mathcal{A}}$. Then $\widehat{\mathcal{A}}$ obtains the private key.

$$USK_{\widehat{U}} =< \forall v_{i,j} \in \widehat{U}, (\varsigma_{i,j})^{\varpi_U} > \tag{14}$$

Challenge. $\widehat{\mathcal{A}}$ hands over two messages M_0 and M_1 to $\widehat{\mathcal{B}}$. $\widehat{\mathcal{B}}$ randomly selects a bit $\mho \in \{0,1\}$. Then $\widehat{\mathcal{B}}$ chooses a random number $s \in \mathbb{Z}_p$ and computes CT^*.

$$\begin{aligned}
&CT^* = (\widehat{W^*}, C_1^* = g^s, C_2^* = (\prod_{v_{i,j}\in\widehat{W^*}} g^{-r_{i,j}})^s \\
&, C_3^* = M_\mho \cdot (\prod_{\widehat{AA_\delta}\cap\widehat{W^*}\neq\varnothing} e(g,g)^{\alpha_\delta})^{s\cdot\pi})
\end{aligned} \tag{15}$$

$$\begin{aligned}
C_3^* &= M_\mho \cdot e(g,g)^{\alpha\cdot s\cdot\pi} \cdot \prod_{\delta\neq\delta*} e(g,g)^{\alpha_\delta\cdot s\cdot\pi} \\
&= M_\mho \cdot e(g^{\alpha'}, g)^{s\cdot\pi} \cdot T \cdot \prod_{\delta\neq\delta*} e(g,g)^{\alpha_\delta\cdot s\cdot\pi}
\end{aligned} \tag{16}$$

If $T = e(g^s, g)^{-a^{q+1}}$ then CT^* is a valid encryption of $M_\mho$.

Phase 2. Same as Phase 1.

Guess. $\widehat{\mathcal{A}}$ puts out a guess $\mho'$ of $\mho$. $\widehat{\mathcal{B}}$ outputs 1 to guess that $T = e(g^s, g)^{-a^{q+1}}$ if $\mho' = \mho$; otherwise, it outputs 0 to show that T is a random value in G_T. We have that $\Pr[\widehat{\mathcal{B}}(g, h, \overline{Y}, e(g^{a^{q+1}}, h)) = 1] = \frac{1}{2} + \varepsilon$, since $\widehat{\mathcal{B}}$ succeeds to simulate the game. Therefore, $\widehat{\mathcal{B}}$ finally plays the decisional q-BDHE game with ε.

5 Performance Analysis

5.1 Theoretical Analysis

We perform comparison between some CP-ABE schemes [13, 19, 32] and our scheme by using the follows symbols. n_A is denoted by a set of the indexes for *AAs*, which monitor the related attributes used to encrypt the message. TE_{G_T}, TE_G are exponential operation time on an element in group G_T and G, respectively. TP is the operation time of pairing. $l_{\widehat{W}}$ is the number of the attributes in the access policy. l_{Usk} is the number of the attributes in the private key. $|G|$, $|G_T|$ are the bit-length of the element of G and G_T, respectively. USK denotes the size of the private key and CT denotes the size of ciphertext.

In Table 1, all the listed schemes are linear with the number of attributes in the private key. The ciphertext size in our scheme and the schemes [31-32] are constant which is independent of the number of involved attributes. The ciphertext size in our scheme is shorter than that of the scheme [31]. In Table 2, the exponential operation and pairing operation in our scheme are also constant in *Encrypt* and *Decrypt* algorithm. Compared with that of the scheme [32], our scheme has similar costs in *Decrypt*, *Encrypt* algorithm. However, our scheme also has obvious cost advantage in *KeyGen* algorithm since l_{Usk} is bigger than n_A under normal condition.

Table 1. The size of private key and ciphertext

Scheme	USK	CT
Scheme [13]	$(l_{Usk} + 6n_A)\cdot\|G\|$	$\|G_T\| + (3n_A + 2l_{\widehat{W}})\|G\|$
Scheme [19]	$(l_{Usk} + 1)\cdot\|G\|$	$\|G_T\| + (l_{\widehat{W}} + 1)\|G\|$
Scheme [31]	$(l_{Usk} + 1)\cdot\|G\|$	$\|G_T\| + 3\|G\|$
Scheme [32]	$l_{Usk}\cdot\|G\|$	$\|G_T\| + 2\|G\|$
Our scheme	$l_{Usk}\cdot\|G\|$	$\|G_T\| + 2\|G\|$

Table 2. The computation cost

Scheme	*Decrypt*	*Encrypt*	*KeyGen*
Scheme [13]	$(l_{\widehat{W}} + n_A)TE_{G_T} + (4n_A + 2l_{\widehat{W}})TP$	$(n_A TE_{G_T} + 3n_A TE_G + (3l_{\widehat{W}})TE_G$	$(9n_A + l_{Usk})TE_G$
Scheme [19]	$(l_{\widehat{W}} + n_A)TP$	$(2l_{\widehat{W}} + 1)TE_G + TE_{G_T}$	$(2 + l_{Usk})TE_G$
Scheme [31]	$4TP$	$TE_{G_T} + 3TE_G$	$(2 + l_{Usk})TE_G$
Scheme [32]	$2TP$	$TE_{G_T} + 2TE_G$	$2l_{Usk}TE_G$
Our scheme	$2TP$	$TE_{G_T} + 2TE_G$	$(l_{Usk} + n_A + 1)TE_G$

In addition, our scheme shows stronger resistance to key escrow for embedding one secret of DU and one secret of UCI into the identity credential of DU respectively to resist the collusion of vicious authorities. Our scheme has no relation with the number of data owner DO in generating attribute keys compared to that of the scheme [32] where the related attribute keys need to be entirely reconstructed once a new DO encrypts messages. The property comparison of some schemes is listed in Table 3.

Table 3. The property comparison of some schemes

Scheme	Resistance to key escrow	The number of attribute keys	Access structure	Assumption	Constant ciphertext
Scheme [13]	General	No relation with DO	LSSS	q-BDHE	No
Scheme [19]	General	No relation with DO	LSSS	q-BDHE	No
Scheme [31]	General	No relation with DO	And-gates	q-BDHE	Yes
Scheme [32]	General	Linear with the number of DO	And-gates	q-BDHE	Yes
Our scheme	Stronger	No relation with DO	And-gates	q-BDHE	Yes

In our scheme, the user's additional credential issuance is conducted in offline preparation phase. The computation and communication cost can be ignored relatively compared with the low efficiency of user's registration on the spot.

5.2 Experimental Simulation

A simulation experiment on Windows 7 system with Intel(R) Core(TM) i7 CPU at 2.3GHZ and 4GB RAM is done. The scheme is implemented by using the pairing-based cryptography library (PBC) library [50]. We use a symmetric elliptic curve a-curve, where the base field size is 512-bit. The a-curve has a 160-bit group order, i.e., p is a 160-bit length prime.

To compare above schemes in practical operation, *Decrypt*, *Encrypt*, *KeyGen* algorithms are implemented ten times respectively and the average values are computed. We code all the algorithms by using C language under the default condition that each scheme contains 50 attribute authorities and 100 attributes in access policy. The running results are shown in Figure 2 from which we discover that the scheme in [32] is close to our scheme in efficiency. Since our scheme has the merits that attribute keys are unconcerned with *DO* and having strong resistance to key escrow, our scheme is more practical. The theoretical analysis and simulation result are consistent, and our scheme achieves high performance in *Encrypt* and *Decrypt* algorithms.

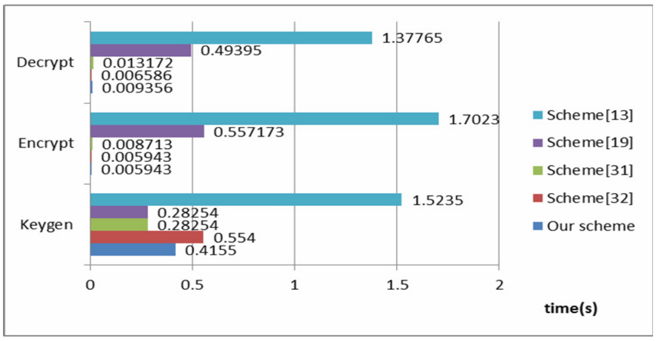


Figure 2. Running time of 3 algorithms

6 Conclusion

Our scheme eliminates the key escrow from three aspects. Firstly, adopting multi-authority model realizes separation of managing power. Secondly, a user's credential issuer *UCI* takes its own secret into the public parameter of *AAs* used to encrypt message and knows nothing about *AAs*' master keys, in which *AAs* cannot directly decrypt ciphertext with their master keys. Thirdly, the final decryption key also includes the user's secret value which prevents *AAs* from generating the decryption key directly for knowing the attribute information of the user. So, our scheme avoids key escrow problem. In addition, our scheme has good performance for constant ciphertext and private key length. The analysis and simulation results show that our scheme is scalable and efficient. The further work is to design constant ciphertext size MA-ABE scheme which is provably secure in the standard model.

Acknowledgements

This research was supported by the National Natural Science Foundation of China (62072104, 61972095, U1736112, 61772009, 61672207), the Natural Science Foundation of the Fujian Province, China (2020J01159), the Key Research and Development Project of Science Department in Jiangxi Province (20171BBE50065).

References

[1] A. Sahai, B. Waters, Fuzzy Identity-Based Encryption, *The 24th Annual International Conference on Theory and Applications of Cryptographic Techniques*, Aarhus, Denmark, 2005, pp. 457-473.

[2] J. Li, X. Lin, Y. Zhang, J. Han, KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage, *IEEE Transactions on Services Computing*, Vol. 10, No. 5, pp. 715-725, September-October, 2017.

[3] J. Li, Y. Wang, Y. Zhang, J. Han, Full Verifiability for Outsourced Decryption in Attribute Based Encryption, *IEEE Transactions on Services Computing*, Vol. 13, No. 3, pp. 478-487, May/June, 2020.

[4] J. Li, W. Yao, J. Han, Y. Zhang, J. Shen, User Collusion Avoidance CP-ABE with Efficient Attribute Revocation for Cloud Storage, *IEEE Systems Journal*, Vol. 12, No. 2, pp. 1767-1777, June, 2018.

[5] J. Li, W. Yao, Y. Zhang, H. Qian, J. Han, Flexible and Fine-grained Attribute-Based Data Storage in Cloud Computing, *IEEE Transactions on Services Computing*, Vol. 10, No. 5, pp. 785-796, September- October, 2017.

[6] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, L. Wei, Auditable σ-time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing, *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 1, pp. 94-105, January, 2018.

[7] J. Ning, X. Dong, Z. Cao, L. Wei, X. Lin, White-Box Traceable Ciphertext-policy Attribute-Based Encryption Supporting Flexible Attributes, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No, 6, pp. 1274-1288, June, 2015.

[8] H. Qian, J. Li, Y. Zhang, J. Han, Privacy-Preserving Personal Health Record Using Multi-Authority Attribute-Based Encryption with Revocation, *International Journal of Information Security*, Vol. 14, No. 6, pp. 487-497, November, 2015.

[9] C. Zuo, J. Shao, G. Wei, M. Xie, M. Ji, CCA-secure ABE with Outsourced Decryption for Fog Computing, *Future Generation Computer Systems*, Vol. 78, pp. 730-738, January, 2018.

[10] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data, *The 13th ACM Conference on Computer and Communications Security*, Alexandria, VA, USA, 2006, pp. 89-98.

[11] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-Policy Attribute-Based Encryption, *IEEE Symposium on Security and Privacy*, Berkeley/Oakland, CA, USA, 2007, pp. 321-334.

[12] J. Li, Y. Zhang, J. Ning, X. Huang, G. Poh, D. Wang,

Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT, *IEEE Transactions on Cloud Computing*, February, 2020, DOI: 10.1109/TCC.2020.2975184.

[13] J. Han, W. Susilo, Y. Mu, J. Zhou, M. H. Au, PPDCP-ABE: Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption, *European Symposium on Research in Computer Security-ESORICS 2014*, Wroclaw, Poland, 2014, pp. 73-90.

[14] M. Wang, Z. Zhang, C. Chen, Security Analysis of a Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption Scheme, *Concurrency & Computation Practice & Experience*, Vol. 28, No. 4, pp. 1237-1245, March, 2016.

[15] J. Hur, D. 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, July, 2011.

[16] J. Lai, R. Deng, Y. Li, Fully Secure Cipertext-Policy Hiding CP-ABE, *The 7th International Conference on Information Security Practice and Experience*, Guangzhou, China, 2011, pp. 24-39.

[17] K. Emura, A. Miyaji, A. Nomura, K. Omote, M. Soshi, A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length, *Information Security Practice and Experience- Fifth International Conference*, Xi'an, China, 2009, pp. 13-23.

[18] M. Chase, Multi-Authority Attribute Based Encryption, *The 4th Theory of Cryptography Conference*, Amsterdam, The Netherlands, 2007, pp. 515-534.

[19] K.Yang, X. Jia, Attributed-Based Access Control for Multi-Authority Systems in Cloud Storage, *International Conference on Distributed Computing Systems*, Macau, China, 2012, pp. 536-545.

[20] K. Yang, X. Jia, Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage, *IEEE Transactions on Parallel & Distributed Systems*, Vol. 25, No. 7, pp. 1735-1744, July, 2014.

[21] M. Chase, S. Chow, Improving Privacy and Security in Multi-Authority Attribute-Based Encryption, *ACM Conference on Computer and Communications Security*, Chicago, Illinois, US, 2009, pp. 121-130.

[22] M. Naor, B. Pinkas, O. Reingold, Distributed Pseudo-Random Functions and KDCs, *International Conference on the Theory and Applications of Cryptographic Techniques*, Prague, Czech Republic, 1999, pp. 327-346.

[23] J. Han, W. Susilo, Y. Mu, J. Yan, Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, No. 11, pp. 2150-2162, November, 2012.

[24] B. Waters, Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization, *The 14th International Conference on Practice and Theory in Public Key Cryptography*, Taormina, Italy, 2011, pp. 53-70.

[25] N. Attrapadung, B. Libert, E. Panafieu, Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts, *The 14th International Conference on Practice and Theory in Public Key Cryptography*, Taormina, Italy, 2011, pp. 90-108.

[26] C. Chen, Z. Zhang, D. Feng, Efficient Ciphertext Policy Attribute-Based Encryption with Constant-Size Ciphertext and Constant Computation-Cost, *International Conference on Provable Security*, Xi'an, China, 2011, pp. 84-101.

[27] J. Herranz, F. Laguillaumie, C. Ràfols, Constant Size Ciphertexts in Threshold Attribute-Based Encryption, *The 13th International Conference on Practice and Theory in Public Key Cryptography*, Paris, France, 2010, pp.19-34.

[28] L. Cheung, C. Newport, Provably Secure Ciphertext Policy ABE, *The Fourteenth ACM Conference on Computer and Communications Security (CCS'07)*, Alexandria, Virginia, USA, 2007, pp. 456-465.

[29] N. Doshi, D. Jinwala, Constant Ciphertext Length in CP-ABE, *Computer Science*, https://arxiv.org/abs/1208.5991, 2012.

[30] A. Ge, R. Zhang, C. Chen, C. Ma, Z. Zhang, Threshold Ciphertext Policy Attribute-Based Encryption with Constant Size Ciphertexts, *Information Security and Privacy-Seventeenth Australasian Conference*, Wollongong, NSW, Australia, 2012, pp. 336-349.

[31] N. Doshi, D. Jinwala, Constant Ciphertext Length in Multi-Authority Ciphertext Policy Attribute Based Encryption, *The 2nd International Conference on Computer and Communication Technology (ICCCT)*, Allahabad, India, 2011, pp. 451-456.

[32] Y. Chen, L. Song, G. Yang, Attribute-Based Access Control for Multi-Authority Systems with Constant Size Ciphertext in Cloud Computing, *China Communications*, Vol. 13, No. 2, pp. 146-162, February, 2016.

[33] L. Zhang, Y. Cui, Y. Mu, Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing, *IEEE Systems Journal*, Vol. 14, No. 1, pp. 387-397, March, 2020.

[34] L. Zhang, J. Zhang, Y. Mu, Novel Leakage-Resilient Attribute-Based Encryption from Hash Proof System, *The Computer Journal*, Vol. 60, No 4, pp. 541-554, March, 2017.

[35] J. Li, Q. Yu, Y. Zhang, J. Shen, Key-Policy Attribute-Based Encryption Against Continual Auxiliary Input Leakage, *Information Sciences*, Vol. 470, pp. 175-188, January, 2019.

[36] J. Li, N. Chen, Y. Zhang, Extended File Hierarchy Access Control Scheme with Attribute Based Encryption in Cloud Computing, *IEEE Transactions on Emerging Topics in Computing*, March, 2019, DOI: 10.1109/TETC.2019.2904637.

[37] J. Li, Q. Yu, Y. Zhang, Hierarchical Attribute Based Encryption with Continuous Leakage-Resilience, *Information Sciences*, Vol. 484, pp. 113-134, May, 2019.

[38] S. Hu, J. Li, Y. Zhang, Improving Security and Privacy-Preserving in Multi-Authorities Ciphertext-Policy Attribute-Based Encryption, *KSII Transactions on Internet and Information Systems*, Vol. 12, No. 10, pp. 5100-5119, October, 2018.

[39] J. Li, S. Hu, Y. Zhang, Two-Party Attribute-Based Key Agreement Protocol with Constant-Size Ciphertext and Key, *Security and Communication Networks*, Vol. 2018, Article ID 8738960, October, 2018, DOI: 10.1155/ 2018/8738960.

[40] J. Ning, Z. Cao, X. Dong, L. Wei, White-Box Traceable CP-ABE for Cloud Storage Service: How to Catch People Leaking Their Access Credentials Effectively, *IEEE*

Transactions on Dependable and Secure Computing, Vol. 15, No. 5, pp. 883-897, September-October, 2018.

[41] J. Li, H. Yan, Y. Zhang, Certificateless Public Integrity Checking of Group Shared Data on Cloud Storage, *IEEE Transactions on Services Computing*, January, 2018, DOI: 10.1109/TSC.2018.2789893.

[42] H. Yan, J. Li, J. Han, Y. Zhang, A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage, *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 1, pp. 78-88, January, 2017.

[43] J. Li, H. Yan, Y. Zhang, Identity-based Privacy Preserving Remote Data Integrity Checking for Cloud Storage, *IEEE Systems Journal*, March, 2020, DOI: 10.1109/JSYST.2020.2978146.

[44] C. Wang, C. Wang, Z. Wang, X. Ye, J. X. Yu, B. Wang, DeepDirect: Learning Directions of Social Ties with Edge-based Network Embedding, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 31, No. 12, pp. 2277-2291, December, 2019.

[45] J. Li, H. Yan, Y. Zhang, Efficient Identity-based Provable Multi-Copy Data Possession in Multi-Cloud Storage, *IEEE Transactions on Cloud Computing*, July, 2019, DOI: 10.1109/TCC.2019.2929045.

[46] L. Zhang, H. Xiong, Q. Huang, J. Li, K. K. R. Choo, J. Li, Cryptographic Solutions for Cloud Storage: Challenges and Research Opportunities, *IEEE Transactions on Services Computing*, August, 2019, DOI: 10.1109/TSC.2019.2937764.

[47] H. Yan, J. Li, Y. Zhang, Remote Data Checking with a Designated Verifier in Cloud Storage, *IEEE Systems Journal*, Vol. 14, No. 2, pp. 1788-1797, June, 2020.

[48] Y. Lu, J. Li, Y. Zhang, Privacy-Preserving and Pairing-Free MultiRecipient Certificateless Encryption with Keyword Search for Cloud-Assisted IIoT, *IEEE Internet of Things Journal*, Vol. 7, No. 4, pp. 2553-2562, April, 2020.

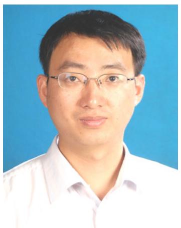
[49] T. Miao, J. Shen, X. Jin, J. Lai, Fine-grained and Efficient Access Control in E-health Environment, *Journal of Internet Technology*, Vol. 20, No. 7, pp. 2169-2176, December, 2019.

[50] B. Lynn, *Pairing-Based Cryptography (PBC) Library*, http://crypto.stanford.edu/pbc, 2013.

Biographies

Shengzhou Hu received the Ph.D. degree in computer science from the College of Computer and Information, Hohai University, Nanjing, China in 2019. He is currently an Associate Professor with Mathematics and Computer Science Department, Gannan Normal University, China. His research interests include cloud computing security and public key cryptography.

Jiguo Li received the Ph.D. degree in computer science from Harbin Institute of Technology, Harbin, China in 2003. He is currently a Professor with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China. His research interests include cryptography and information security, cloud computing security, wireless security and trusted computing, etc.



Yang Lu received the Ph.D. degree in computer science from PLA University of Science and Technology, Nanjing, China, in 2009. He is currently a Professor with the School of Computer Science and Technology, Nanjing Normal University, Nanjing, China. His research interests include cryptography and information security, cloud computing, etc.

Yichen Zhang received the Ph.D. degree in computer science from the College of Computer and Information, Hohai University, Nanjing, China in 2015. She is currently an Associate Professor with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China. Her research interests include cryptography and information security, cloud computing security, etc.