Improving Security and Privacy-Preserving in Multi-Authorities Ciphertext-Policy Attribute-Based Encryption

Shengzhou Hu[1,3], Jiguo Li[1,2] and Yichen Zhang[1,2]
[1]College of Computer and Information, Hohai University, Nanjing, Jiangsu 211100, China
[2] College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China
[3] Mathematics and Computer Science Department, Gannan Normal University
Ganzhou, Jiangxi 341000, China
[e-mail: jxgzhsz@126.com, ljg1688@163.com, lijiguo@hhu.edu.cn, zyc_718@163.com]
*Corresponding author: Jiguo Li

Received December 6, 2017; revised February 20, 2018; accepted March 13, 2018; published October 31, 2018

Abstract

Most of existing privacy-preserving multi-authorities attribute-based encryption schemes (PP-MA-ABE) only considers the privacy of the user identity (ID). However, in many occasions information leakage is caused by the disclosing of his/her some sensitive attributes. In this paper, we propose a collusion-resisting ciphertext-policy PP-MA-ABE (CRPP-MACP-ABE) scheme with hiding both user's ID and attributes in the cloud storage system. We present a method to depict anonymous users and introduce a managerial role denoted by IDM for the management of user's anonymous identity certificate (AID_{Cred}). The scheme uses AID_{Cred} to realize privacy-preserving of the user, namely, by verifying which attribute authorities (AAs) obtain the blinded public attribute keys, pseudonyms involved in the AID_{Cred} and then distributes corresponding private keys for the user. We use different pseudonyms of the user to resist the collusion attack launched by vicious AAs . In addition, we utilize IDM to cooperate with multiple authorities in producing consistent private key for the user to avoid the collusion attack launched by vicious users. The proposed CRPP-MACP-ABE scheme is proved secure. Some computation and communication costs in our scheme are finished in preparation phase (i.e. user registration). Compared with the existing schemes, our scheme is more efficient.

Keywords: Attribute-based encryption, CP-ABE, multi-authorities, privacy-preserving

This work was supported by the National Natural Science Foundation of China (61672207, 61772009, U1736112), Jiangsu Provincial Natural Science Foundation of China (BK20161511), the Key Research and Development Project of Science Department in Jiangxi Province (20171BBE50065), Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, NJUPT.

http://doi.org/10.3837/tiis.2018.10.025 **ISSN : 1976-7277**

1. Introduction

Cloud computing regarded as a computing architecture with a bright future provides resources as services over the Internet. More and more enterprises need the computing and storage resources of cloud for the great benefits of economy, expandability and approachability. At the same time, data security and privacy are surely challenging issues for the cloud storage [1,2] and mobile social networks [3,4]. Sahai and Waters initially presented attribute-based encryption (ABE) [5], which was often used for fine-grained access control in the cloud environment [6-9]. Users' identity is determined by its attributes. ABE is often applied in a one-to-many encryption situation, where data encryption with certain attributes policy is correctly decrypted by any users whose attributes satisfy that access policy.

Attribute-based encryption scheme has attracted much concern and many schemes [6-40] have been presented successively. Only one authority in ABE schemes has the trouble of centralized power which reduces security. In order to avoid such trouble, multi-authority ABE (MA-ABE) scheme [10] is put forward, where the user obtains corresponding decryption key from multiple attribute authorities (AAs) respectively. However, AAs are often honest but curious in distributed environment, so they can collude with each other and impersonate a user with knowing the user's attributes information. Some privacy-preserving MA-ABE (PPMA-ABE) schemes [11-14] were proposed, where only the privacy of the identity (ID) was considered. However, those schemes do not address privacy leakage caused by the sensitive attributes, which can reveal the user's identity during the interaction with AAs . To illustrate it, a simple example is given as follows: Suppose there is only one principal in a school and his name is "Wan LI". Someone has the sets of attributes {Position="principal", Sex="male", Degree="Doctor", Department="headmaster's office"}, from which we know that the person must be principal "Wan LI" since there is only one principal even if his/her identity (ID) is unknown. So, Position= "principal" is a sensitive attribute. In order to protect privacy better, it is necessary to prevent the leakage of subtle attribute information. Han et al. [15] first proposed a scheme to address the privacy of attributes via anonymous protocol. Nevertheless, Wang et al. [16] pointed out such solution was vulnerable to collusion attack and showed that the privacy-preserving key extract protocol from [15] didn't provide the privacy protection of attributes. Wang et al. [16] didn't propose an improved scheme. It is meaningful to further explore the privacy protection of attributes of the user.

1.1 Our Motivation and Contribution

We present a privacy-preserving collusion-resisting ciphertext-policy MA-ABE (CRPP-MACP-ABE) scheme. There have been several main technologies listed as follows.

(1) In this scheme, we introduce a method to depict an anonymous user. If any person can optionally pretend other legal identities to visit a system, then there is no any security in this system. Those occasions where we needn't confirm one's legal identity are also the occasions where we needn't use cryptograph technique. So, we think any system needs a role or mechanism to check user's legality, which we even need some times to hide his/her real identity (ID) for the purpose of privacy protection. In this model, a legal user first offers the initial information(ID or nickname or code name, etc.) to some authoritative institutiont(AI), just like a police station, a government sector, etc., or some authentication mechanism(AM). The user obtains his/her legitimacy evidence (LE) if some concrete checking is passed. For example, the ability to drive is a kind of LE. Any person can prove the ability by passing the

driving examination and then gain the corresponding LE with initial information which is not his/her ID. According to the above analysis, there always exist some kind of AI/AM to confirm the user's legality and depict the user's anonymity. In this paper, we denote Id_U as user U 's real initial information checked by AI/AM successfully. U randomly selects $\hbar \in \mathbb{Z}_p$, which is a finite field with prime order p. Let g be a group element, $\wp \in \mathbb{Z}_p$ be a signature factor randomly generated by AI/AM and $H_*(\cdot), H_1(\cdot)$ be two hash functions. Let $a_{j,i}$ be the i th attribute of U 's attributes monitored by the j th attribute authority $\widetilde{A}_j$, $N_{\widetilde{A}_j}$ be the name of $\widetilde{A}_j$, $Z_{j,i}$ be $a_{j,i}$'s corresponding public attribute key computed by $\widetilde{A}_j$. U randomly selects a blinding factor $d_U \in \mathbb{Z}_p$ and computes $g^{\wp d_U}$ and each blinded public attribute key $Z_{j,i}^{d_U}$. AI/AM generates $RId_U = H_1(Id_U \parallel g^{\hbar})^{\wp}$ as U 's pseudonym and $H_*(\aleph_U)^{\wp}$, where $\aleph_U = RId_U, g^{\hbar}, g^{\wp}, g^{\wp d_U}, < N_{\widetilde{A}_j}, Z_{j,i}^{d_U} >_{a_{j,i} \in \widehat{U} \cap \widehat{A}_j, j \in I}$. $\aleph_U$ along with $H_*(\aleph_U)^{\wp}$ is denoted by LV_U as a description of legality evidence consisting of anonymous information. AI/AM can verify the truth of binding relationship for those message parts in $\aleph_U$ since it grasps the real initial information (Id_U). Based on above works, we provide a user identity management role named IDM for generating anonymous identity certificate (AID_{Cred}) of legal users satisfying some detection condition, such as $\{e(H_*(\aleph_U), g^{\wp}) = e(H_*(\aleph_U)^{\wp}, g)$ for U .

(2) We realize the privacy protection by using the user's pseudonyms and verifying the IDM 's signature on binding messages in AID_{Cred} , which include the user's corresponding blinded public attribute keys and pseudonyms, the names of corresponding AAs . In our ABE, each authority is responsible for different attributes. Decryption keys are issued by AAs according to checking the signed binding messages successfully. When U makes registration, for each $\widetilde{A}_j$, IDM generates U 's pseudonym $Pid_{U,j}$ and a signature on the binding $Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j}$, which is expressed as $Sig(Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j})$. Suppose that I is the index set of attribute authorities who manages U 's attributes and l_j is the number of U 's attributes monitored by $\widetilde{A}_j$, U obtains all signatures $\{Sig(Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j})\}_{j \in I, i \in [1, l_j]}$ and $\{Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j}\}_{j \in I, i \in [1, l_j]}$, which are viewed as anonymous identity certificate (AID_{Cred}). Generating AID_{Cred} for a user is finished in a preparation phase. We imagine that there are many users carrying such AID_{Cred} in that system. Only users themselves know their real identities, which are unknown to IDM and AAs . So long as $\widetilde{A}_j$ successfully verifies the signature $Sig(Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j})$ with IDM 's public key, it directly produces partial private keys for U based on the received $Z_{j,i}^{d_U}$ and $Pid_{U,j}$.

(3) We propose a PP-MACP-ABE scheme with the capability to resist collusion. To avoid collusion launched by malicious users, whose attributes respectively stride one attribute field managed by one of attribute authorities, we refer to the Chase's idea [10]. Here IDM is fully trusted in our scheme and also acts as the role of central authority (CA) in [10]. Suppose α_j is the original private key of an arbitrary authority $\widetilde{A}_j$, $PRF()$ is a pseudorandom function which inputs two parameters, one of which is the master key of one attribute authority and another is the user's one pseudonym, just like α_j and $Pid_{U,j}$. When $\widetilde{A}_j$ issues a partial private key for U, $\widetilde{A}_j$ generates a new master key $\alpha_j^{'} = PRF_{\alpha_j}(Pid_{U,j})$. At the same time, IDM gathers all α_j from $\widetilde{A}_j$ $(j \in I)$ and also computes $\alpha_j^{'} = PRF_{\alpha_j}(Pid_{U,j})$. Then IDM computes α_0 as IDM's master key. α_0 and all $\alpha_j^{'}(j \in I)$ are combined into the master secret key y_0 of the system. In our paper, AAs do not collude with each other to directly produce private keys according to the user's attribute information for knowing nothing about both user's attributes and identity. In addition, since U's pseudonym received by one attribute authority is different from that received by other AAs, AAs do not assemble all the partial private keys of U from different pseudonyms to realize collusion.

Moreover, when decrypting ciphertext, U uses not only the key from AAs but also its secret value d_U, which is only owned by U secretly and is updated timely. So antiquated keys collected by AAs are not used again in collusion attack.

1.2 Organization

The related work is introduced in Section 2. The preliminaries are introduced in Section 3. In Section 4, a CRPP-MACP-ABE scheme is proposed and it is proved to be secure in Section 5. Subsequently, we give the performance comparison between PPDC-MACP-ABE scheme [15] and our scheme in Section 6. We conclude our paper in Section 7.

2. Related Work

ABE mainly includes two categories called ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In CP-ABE, data owners choose an access structure on attributes and encrypt data with the corresponding attribute public keys. Access structure is embedded in the ciphertext, while the secret keys are produced according to the attribute set of data users. If the attributes embedded in the ciphertext fit those held by the user, then he/her decrypts such ciphertext [17]. There are some basic CP-ABE schemes [18-21,24,27,28,31], in which the size of the ciphertext grows linearly with the number of attributes embedded in access policy. In order to improve efficiency, Emura et al. [21] presented a CP-ABE scheme with constant ciphertext size. Furthermore, Li et al. [22] proposed a verifiably outsourced decryption of ABE with constant ciphertext length. In KP-ABE schemes [11,12,32,40], the encryptor selects the descriptive attributes to encrypt data. The authorities collect the corresponding combinations of attributes and determine which data users decrypt such data. To achieve scalable, flexible, and fine-grained access control, some hierarchical attribute-based encryption schemes [23-25] were presented. In order to protect the privacy, Lai et al. [27] and Li et al. [28] provided ABE schemes with hidden access policy. Li et al. [34,35] presented two searchable outsourced ABE schemes, which can implement ciphertext keyword search for cloud storage. In order to resist collusion attack, Li et al. [31] proposed efficiently CP-ABE schemes for avoiding user collusion with attribute revocation. Rahulamathavan et al. [32] proposed an improved scheme, which mitigated the user collusion security vulnerability with preserving the user's privacy. In ABE scheme, the malicious users may leak their access credentials for profits, which severely damages data security. To solve this issue, Ning et al. [38,39] presented two white-box traceable CP-ABE schemes.

In order to reduce the trust on the central authority, Chase [10] gave a multi-authority ABE (MA-ABE) scheme which supported several attribute authorities and one central authority (CA). Each attribute authority issued secret key for a different set of attributes. MA-ABE schemes [10,26,27,29,30] submit the user's global identifier (GID) to each authority to obtain the corresponding secret keys. However, multiple authorities have chance to collect the user's attributes by his/her GID and launch collusion attack. Because each authority seems not to be fully trusted, the protection of user's privacy is an essential demand. Chase and Chow first proposed a privacy-preserving MA-ABE (PPMA-ABE) scheme [12], where the trusted central authority was removed instead of using an anonymous key issuing protocol. As a result, the user's attributes were not collected by tracing his/her GID. The solution used distributed pseudorandom functions (PRF) introduced in [41], which made the authorities not know any information about the user's GID, but they knew the user's attributes. Chase and Chow [11] proposed a CA-free MA-ABE with user privacy that resolved the key escrow problem by using PRF. In this setting, each pair of authorities communicated with each other by a 2-party key exchange protocol to generate users' private keys. In some PPMA-ABE schemes, such as [11-13], only the privacy of GID was considered. Furthermore, some sensitive attributes are sufficiently used to identify a specific user or lead to user's privacy disclosure. Recently, a privacy-preserving decentralized CP-ABE (PPDCP-ABE) scheme was proposed by Han et al. [15]. This scheme makes users interact with AAs for keeping both users' identifiers and attributes secret by using a privacy-preserving key extract protocol. Namely, a user can obtain secret keys from multiple authorities without releasing any information about his/her GID and attributes. Anonymous certificates for users are required in that scheme [15]. However, the solution in [15] is vulnerable to collusion attack. Wang [16] presented a concrete collusion attack on their basic DCP-ABE scheme, i.e., two colluding users jointly obtained private keys from AAs for an attribute set which a third legal user held. In addition, they also pointed out that the privacy-preserving key extract protocol didn't provide the privacy protection of attributes. The scheme [33] proposed by Liu et al. has multiple central authorities (CAs) and AAs. The CAs generate identity related keys to users and AAs generate attribute related keys to users. Then AAs verify whether the information that users submit to AAs for private keys is really generated by the CAs to the related users.

3. Preliminaries

3.1 Access Structure

Supposed that $P = \{p_1, p_2, \cdots, p_n\}$ emprises n attributes in our system, an access structure is a non-empty subset $\mathbb{A} \subseteq 2^{\{p_1, p_2, \cdots, p_n\}} \setminus \{\varnothing\}$. In particular, a collection $\mathbb{A}$ is monotone if $\overset{\frown}{B} \in \mathbb{A}$ and $\overset{\frown}{B} \subseteq \overset{\frown}{C}$, then $\overset{\frown}{C} \in \mathbb{A}$ for $\forall B, C$. If a user with a set in $\mathbb{A}$ then he/her is authorized for accessing some resources.

3.2 Linear Secret Sharing Schemes [43]

A secret sharing scheme $\prod$ over an attribute set P is linear if

(1) The shares for each attribute form a vector over $\mathbb{Z}_p$;

(2) There exists a matrix $\overset{\frown}{M}$ (with l rows and n columns) called the share-generating matrix. For the i th row of $\overset{\frown}{M}$, $i = 1, 2, \cdots, l$, we let the function ρ define the attribute labeled row i as $\rho(i)$. When we consider the column vector $\vec{V} = (s, v_2, \cdots, v_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared, and $v_2, \cdots, v_n \in \mathbb{Z}_p$ are randomly selected, then $\overset{\frown}{M} \cdot \vec{V}$ is the vector of shares for the secret s according to $\prod$. The share $(\overset{\frown}{M} \cdot \vec{V})_i$ belongs to attribute $\rho(i)$. It is shown in [6] that every linear secret-sharing scheme as above also enjoys the linear reconstruction property: Suppose that $\prod$ is a linear secret-sharing scheme for the access structure $\mathbb{A}$. Let $P_U \in \mathbb{A}$ be any authorized set, and let $\Gamma = \{i : \rho(i) \in P_U\}$. Then, there exist a set of constants $\{\varpi_i\}_{i \in \Gamma}$ such that if $\{\lambda_i\}_{i \in \Gamma}$ are valid shares of any secret s according to $\prod$, then $\sum_{i \in \Gamma} \varpi_i \lambda_i = s$. Furthermore, these constants $\{\varpi_i\}_{i \in \Gamma}$ can be found in polynomial time with the size of the share-generating matrix $\overset{\frown}{M}$.

3.3 Bilinear Maps

Let $\mathbb{G}, \mathbb{G}_{\mathbb{T}}$ be two multiplicative cyclic groups of prime order p. Let g be a generator of $\mathbb{G}$ and e be a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$. The bilinear map e satisfies the following properties:

(1) Bilinearity: for all $\iota, \kappa \in \mathbb{Z}_p, e(g^{\iota}, g^{\kappa}) = e(g, g)^{\iota\kappa}$.

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

(3) Computability: There is an efficient algorithm to compute $e(\phi, \zeta)$ for $\forall \phi, \zeta \in \mathbb{G}$.

3.4 Decisional q-Parallel Bilinear Diffie-Hellman Exponent (q-PBDHE) Assumption [20]

Assume that $s, a, b_1, b_2, b_3, \cdots, b_q$ are random elements of $\mathbb{Z}_p$, $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$ is a bilinear map, g is a generator of $\mathbb{G}$. Given a tuple $\vec{Y} = g, g^s, g^a, \cdots, g^{a^q}, g^{a^{q+2}}, \cdots, g^{(a^{2q})}$, $g^{s \cdot b_j}, g^{\frac{a}{b_j}}, \cdots, g^{\frac{a^q}{b_j}}, g^{\frac{a^{q+2}}{b_j}}, \cdots, g^{\frac{a^{2q} \cdot b_k}{b_j}}, g^{\frac{a \cdot s \cdot b_k}{b_j}}, g^{\frac{a^2 \cdot s \cdot b_k}{b_j}}, \cdots, g^{\frac{a^q \cdot s \cdot b_k}{b_j}}$ $(\forall 1 \leq j, k \leq q, k \neq j)$. If no probabilistic polynomial time adversary $\mathcal{A}$ makes a distinction between $e(g, g)^{a^{q+1} \cdot s}$ and $R \in \mathbb{G}_{\mathbb{T}}$ selected randomly, then we state that the decisional q-PBDHE assumption holds with the advantage $adv_{\mathcal{A}} = | \Pr[\mathcal{A}(\vec{Y}, e(g, g)^{a^{q+1} \cdot s}) = 1] - \Pr[\mathcal{A}(\vec{Y}, R) = 1] | \geq \varepsilon$, where ε is a negligible function.

3.5 CRPP-MACP-ABE Scheme

We propose a CRPP-MACP-ABE scheme which consists of four types of roles in the system: identity management (IDM), attribute authorities (AAs), data owners (DO), data users (DU).

Fig. 1 depicts an overview of the system. All the data are saved in a cloud storage system. A user U submits his/her legality evidence LV_U to IDM. Then IDM generates and sends an anonymous credential AID_{cred} to the user U. When U sends the valid partial credential $AID_{cred,j}$ related to $\widetilde{A}_j (j \in I)$ to $\widetilde{A}_j$, $\widetilde{A}_j$ responds the corresponding partial private key $sk_{U,j}$ to U. In addition, IDM communicates with $\widetilde{A}_j (j \in I)$ and obtains their master keys to compute sk_0. U further groups sk_0 and all $sk_{U,j} (j \in I)$ together into the whole private key.

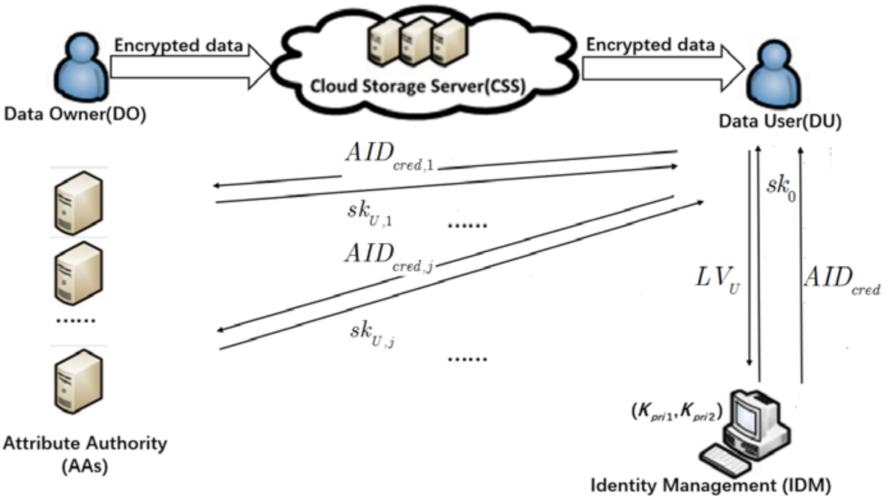


Fig. 1. System model of CRPP-MACP-ABE

$Setup(1^\lambda) \rightarrow PP$. Taking as input a security parameter 1^λ, the algorithm outputs PP consisting of the following public parameters. There are L authorities $\{\widetilde{A}_1, \widetilde{A}_2, \cdots, \widetilde{A}_L\}$. Each attribute authority $\widetilde{A}_j$ manages a set of attributes $\widehat{A}_j$. An identity management IDM is established for checking the legality of the users with two public-secret key pairs (K_{pub1}, K_{pri1}), (K_{pub2}, K_{pri2}). There are four hash functions H_*, H_0, H_1, H_2. Any user U has corresponding legality evidence LV_U issued by authoritative institution (AI) or authentication mechanism (AM).

$AuthoritiesSetup(1^\lambda) \rightarrow (PK, SK)$. Taking as input a security parameter 1^λ, the algorithm outputs (PK, SK), where PK_j, SK_j are the public key set and private key set respectively for each attribute authority $\widetilde{A}_j$, $PK = \bigcup_{j \in [1,2,\ldots,L]} PK_j$, $SK = \bigcup_{j \in [1,2,\ldots,L]} SK_j$.

$UserRegister(PP, K_{pri1}, LV_U) \rightarrow AID_{cred}$. Taking as input public parameters PP, U's legality evidence LV_U, IDM's private key K_{pri1}, the algorithm outputs AID_{cred} to U in secure channel. User registration is an interactive procedure on the spot between IDM and U.

U sends LV_U to IDM. After validating LV_U successfully, IDM issues corresponding anonymous identity credential AID_{cred} created by using its private key K_{pri1} to U.

$EnCryption(PP, \mathbb{A}, M) \to ct$. Taking as input the public parameters PP, message M, an access structure $\mathbb{A}$ about corresponding attributes, this algorithm outputs the ciphertext ct encrypted by K_{pub2} in PP.

$KeyGeneration(PP, K_{pub1}, AID_{cred}) \to sk_U$. This algorithm takes as input the public parameters PP, IDM's public key K_{pub1}, U's anonymous identity credential AID_{cred} and outputs U's private key sk_U. Suppose that $AID_{cred,j}$ is denoted by the part of AID_{cred} related to $\widetilde{A}_j$, there is an interactive procedure between U and $\widetilde{A}_j$. U sends $AID_{cred,j}$ to the corresponding authority $\widetilde{A}_j$. If $AID_{cred,j}$ is valid then $\widetilde{A}_j$ computes the secret key $sk_{U,j}$ based on the received blinded public attribute keys and the pseudonym of U in $AID_{cred,j}$. In addition, IDM computes sk_0 for U. Both $\{sk_{U,j}\}_{\widehat{U} \cap \widehat{A}_j \neq \varnothing, j \in [1, 2, \cdots, L]}$ and sk_0 constitute the whole secret key sk_U.

$Decryption(PP, ct, sk_U) \to M \quad or \quad \perp$. The decryption algorithm takes as input the public parameters PP, a secret key sk_U, and a ciphertext ct. If sk_U is valid then the algorithm outputs M. Otherwise, it outputs $\perp$.

3.6 Security model of confidentiality for CRPP-MACP-ABE scheme

We use the selective-access structure model of CRPP-MACP-ABE scheme as the security model of confidentiality, which is similar to that introduced in [20,10]. $\mathcal{B}$ acts as the challenger in the game.

Setup: The challenger $\mathcal{B}$ runs $Setup$, $AuthoritiesSetup$ algorithms and randomly selects x_0, v and sends the public parameters PP to the attacker $\mathcal{A}$. Then $\mathcal{A}$ declares a challenge access structure $\mathbb{A}^*$ to $\mathcal{B}$.

Phase 1. For a user U with pseudonyms $\{Pid_{U,j}\}_{\widehat{U} \cap \widehat{A}_j \neq \varnothing, j \in [1, 2, \cdots, L]}$, $\mathcal{A}$ adaptively queries secret keys corresponding to $\widehat{U}$, which does not satisfy $\mathbb{A}^*$. $\mathcal{B}$ runs $UserRegister$ to produce all signatures for U. $\mathcal{B}$ returns sk_U to the attacker according to $KeyGeneration$ after successfully verifying those signatures.

Challenge. Given M_0, M_1 from $\mathcal{A}$, $\mathcal{B}$ builds a challenge ciphertext under a challenging access structure $\mathbb{A}^*$. Note that the access structure does not be satisfied by any queried attribute set. $\mathcal{B}$ flips a random coin and obtains a bit $\tau \in \{0, 1\}$ and returns CT^* of M_τ as the challenge ciphertext to $\mathcal{A}$ by calling $EnCryption$.

Phase 2. Same as Phase 1.

Guess. $\mathcal{A}$ wins the game, if $\mathcal{A}$ outputs a guess τ', which is equal to τ.

Definition1: A CRPP-MACP-ABE scheme is selective-access structure secure if no probably polynomial-time adversary $\mathcal{A}$ wins the above game with the advantage $Adv_{\mathcal{A}}^{\text{CRPP-MACP-ABE}} =| \Pr(\tau' = \tau) - \frac{1}{2} |> \varepsilon$.

3.7 Selective-failure blindness (SFB)

SFB means that vicious authorities do not know anything about his/her identity and attributes, and make $KeyGeneration$ algorithm selectively fail depending on his/her identity and attributes. Two characters are formalized as follows.

Blindness of attributes. Let $\mathbb{G}$ be multiplicative cyclic groups of prime order p. Assume that a user U randomly selects $Z_{j,i} \in \mathbb{G}$, $d_U \in \mathbb{Z}_p$, where $Z_{j,i}$ denotes an arbitrary public attribute key and computes $(Z_{j,i})^{d_U}$, which satisfies uniform distribution in $\mathbb{G}$. No probabilistic polynomial-time malicious authority A_j calculates $Z_{j,i}$ from $(Z_{j,i})^{d_U}$ for d_U known only by the user U and the hardness of discrete logarithm of $(Z_{j,i})^{d_U}$.

Pseudonym. Given a hash function $H:\{0,1\}^* \to \mathbb{G}$, we assume Id_U is the initial information about his/her identity and compute $H(Id_U)$. No probabilistic polynomial time adversary extracts Id_U from $H(Id_U)$ for one-way property of hash function.

Definition 2: We say that a scheme is secure with privacy preserving and collusion-resisting (PPCR security) if and only if the following properties hold:

(1) CRPP-MACP-ABE scheme is secure in the selective-access structures model;

(2) The signature part of CRPP-MACP-ABE scheme is existentially unforgeable under an adaptive chosen-message attack;

(3) The privacy-preserving part of CRPP-MACP-ABE scheme is selective-failure blindness.

(4) CRPP-MACP-ABE scheme is collusion-resisting among users or AAs.

4. CRPP-MACP-ABE SCHEME

A concrete construction is proposed as follows:

$Setup(1^\lambda) \to PP$. Given a security parameter 1^λ, this algorithm generates a bilinear group $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_{\mathbb{T}}$. g is a generator of the group $\mathbb{G}$ with prime order p. Suppose that there are L attribute authorities $\{\widetilde{A}_1, \widetilde{A}_2, \cdots, \widetilde{A}_L\}$, where $\widetilde{A}_j (j \in [1, 2, \cdots, L])$ monitors a set of attributes $\overset{\frown}{A}_j = \{a_{j,1}, a_{j,2}, \cdots, a_{j,q_j}\}$. This algorithm chooses 4 cryptographic hash functions: $H_*:\{0,1\}^* \times \mathbb{G}\times\mathbb{G}\times\mathbb{G}\times\{<\{0,1\}^*\times\mathbb{G}>\cdots\}\to\mathbb{G}$, $H_0:\{0,1\}^*\times\mathbb{G}\times\cdots\times\mathbb{G}\to\{0,1\}^*$, $H_1:\{0,1\}^*\times\mathbb{G}\to\{0,1\}^*$, $H_2:\mathbb{G}\times\{0,1\}^*\times\{0,1\}^*\to\mathbb{G}$. There exits some authoritative institutiont or authentication mechanism (AI/AM) who confirms the user's legality and generates legality evidence LV_U, i.e., $\aleph_U, H_*(\aleph_U)^{\wp}$, where $\aleph_U = RId_U, g^{\hbar}, g^{\wp}, g^{\wp d_U}, < N_{\widetilde{A}_j}, Z_{j,i}^{d_U} >_{a_{j,i} \in \overset{\frown}{U} \cap \overset{\frown}{A}_j, j \in I}$. The meaning of all symbols is the same as stated before. For serving users' registration this algorithm establishes an identity management IDM who randomly chooses $x_0, v \in \mathbb{Z}_p$ and generates two public-secret key pairs (g^v, v) , (X_0, x_0) . Here, x_0 acts as the master secret value of the system and $X_0 = e(g,g)^{x_0}$ is the relevant public key. v is the secret key used to generate a signature verified by g^v when checking validity of the signature. The public parameters are $PP = (g, e, p, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, X_0, g^{\wp}, g^v, H_*, H_0, H_1, H_2)$.

$AuthoritiesSetup$. Each attribute authority $\widetilde{A}_j$ $(j = 1, 2, \cdots, L)$ randomly chooses $\alpha_j, x_j \in \mathbb{Z}_p$ as its master keys and computes $A_j = g^{x_j}$. $\widetilde{A}_j$ randomly selects $z_{j,i} \in \mathbb{Z}_p$ for each attribute $a_{j,i} \in \widehat{A}_j$ and computes $Z_{j,i} = g^{z_{j,i}}$. Let $PK_j = \{A_j, (Z_{j,i})_{a_{j,i} \in \widehat{A}_j}\}$, $SK_j = \{\alpha_j, x_j, (z_{j,i})_{a_{j,i} \in \widehat{A}_j}\}$. The algorithm outputs a public-secret attribute key pair (PK, SK), where $SK = \bigcup_{j \in [1, 2, \ldots, L]} SK_j$ and $PK = \bigcup_{j \in [1, 2, \ldots, L]} PK_j$.

$UserRegister$. When making registration, U with his/her attribute set $\widehat{U}$ provides IDM the legality evidence LV_U , where $LV_U = \aleph_U, H_*(\aleph_U)^{\wp}$ and $\aleph_U = RId_U, g^{\hbar}, g^{\wp}, g^{\wp d_U}, < N_{\widetilde{A}_j}, Z_{j,i}^{d_U} >_{a_{j,i} \in \widehat{U} \bigcap \widehat{A}_j, j \in I}$. After receiving LV_U provided by U , IDM checks its validity by judging whether $e(H_*(\aleph_U), g^{\wp}) = e(H_*(\aleph_U)^{\wp}, g)$. If equation holds then IDM utilizes the signature scheme [42] to make signature. First, IDM randomly selects $R_{U,j} \in \mathbb{G}$ for each $\widetilde{A}_j (j \in I)$ and generates corresponding pseudonym $Pid_{U,j} = H_1(RId_U \| R_{U,j})$. For each $a_{j,i} \in \widehat{U}$, IDM computes a signature $Sig_{a_{j,i}, IDM} = H_2(Z_{j,i}^{d_U}, H_1(RId_U \,||\, R_{U,j}), N_{\widetilde{A}_j})^v$, which illustrates the binding relationship among one blinded public attribute key $Z_{j,i}^{d_U}$, U 's one pseudonym $H_1(RId_U \,||\, R_{U,j})$ and the name $N_{\widetilde{A}_j}$ of $\widetilde{A}_j$. Finally, IDM computes all signatures $\{Sig_{a_{j,i}, IDM}\}_{a_{j,i} \in \widehat{U}, j \in I}$ and anonymous identity credential $AID_{cred} = \{Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j}, Sig_{a_{j,i}, IDM}\}_{a_{j,i} \in \widehat{U}, j \in I}$ for U .

$KeyGeneration$. Assume that the user U has anonymous identity credential AID_{cred} . Secret key Generation for U is as follows. Firstly, U sends $\{Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j}, Sig_{a_{j,i}, IDM}\}_{a_{j,i} \in \widehat{U} \bigcap \widehat{A}_j}$, parts of AID_{cred} to $\widetilde{A}_j$. Secondly, for each $a_{j,i} \in \widehat{U} \bigcap \widehat{A}_j$, $\widetilde{A}_j$ generates the corresponding U 's partial private key if $e(Sig_{a_{j,i}, IDM}, g) = e(H_2(Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j}), g^v)$. That is, $\widetilde{A}_j$ randomly chooses $w_{U,j} \in \mathbb{Z}_p$ and computes $\alpha_j^{'} = PRF_{\alpha_j}(Pid_{U,j})$ and $K_j = g^{\alpha_j^{'}} g^{x_j w_{U,j}}$, $P_j = g^{w_{U,j}}$, $(F_{j,i} = Z_{j,i}^{d_U w_{U,j}})_{a_{j,i} \in \widehat{U} \bigcap \widehat{A}_j}$. Besides, IDM stores all the seeds of $PRF(\cdot)$, just like α_j generated by $\widetilde{A}_j (j \in I)$. These seeds are transmitted in secure channel. Thirdly, IDM also computes $\alpha_j^{'} = PRF_{\alpha_j}(Pid_{U,j})$ and $\alpha_{IDM} = x_0 - \sum_{j \in I} \alpha_j^{'}$. IDM gives $K_0 = g^{\alpha_{IDM}}$ to U after confirming his/her legal identity. At last, the user U gets the whole secret key $\{K_0, (K_j, P_j = g^{w_{U,j}}, (F_{j,i} = Z_{j,i}^{d_U w_{U,j}})_{a_{j,i} \in \widehat{U} \cap \widehat{A}_j})_{j \in I}\}$.

$EnCryption$. The data owner encrypts a message $M \in \mathbb{G}_{\mathbb{T}}$ as follows: Let I' be a set which includes the indexes of the authorities whose attributes are selected to encrypt M. This algorithm first chooses an access structures $(\widehat{M}, \rho)$ and vector $\vec{V} = (s, v_2, \cdots, v_n)$, where $s, v_2, \cdots, v_n \in \mathbb{Z}_p$ are randomly selected and $\widehat{M}$ is a $\sum_{j \in I'} l_j \times n$ matrix. Then, it computes $\lambda_{j,i} = \widehat{M}_j^i v$, where $\widehat{M}_j^i$ is the ith row of $\widehat{M}_j$, which is only composed of rows related to attributes monitored by $\widetilde{A}_j$ from $\widehat{M}$. Let the function ρ define the attribute labeled row i as $\rho(i)$. Finally, it randomly selects $r_{j,1}, r_{j,2}, \cdots, r_{j,l_j} \in \mathbb{Z}_p$ and computes $C_0 = M \cdot e(g,g)^{x_0 \cdot s}, X = g^s, (C_{j,1} = g^{x_j \lambda_{j,1}} Z_{\rho_j(1)}^{-r_{j,1}}, D_{j,1} = g^{r_{j,1}}), \cdots, (C_{j,l_j} = g^{x_j \lambda_{j,l_j}} Z_{\rho_j(l_j)}^{-r_{j,l_j}}, D_{j,l_j} = g^{r_{j,l_j}}))_{j \in I'}$.

The ciphertext is $CT = \{C_0, X, (C_{j,r}, D_{j,r})_{r \in [1, l_j]})_{j \in I'}\}$.

$Decryption$. This algorithm decrypts a ciphertext CT with $I = I'$ as follows.

$$\frac{C_0 \cdot \prod_{j \in I} \prod_{i=1}^{l_j} (e(C_{j,i}, P_j) \cdot e(D_{j,i}, F_{\rho_j(i)}^{\frac{1}{d_U}}))^{\varpi_{j,i}}}{e(K_0, X) \cdot \prod_{j \in I} e(K_j, X)}$$

$$= M \cdot e(g,g)^{x_0 s} \cdot \frac{\prod_{j \in I} \prod_{i=1}^{l_j} (e(g^{x_j \lambda_{j,i}} Z_{\rho_j(i)}^{-r_{j,i}}, g^{w_{U,j}}) \cdot e(g^{r_{j,i}}, Z_{\rho_j(i)}^{d_U \cdot w_{U,j} \cdot \frac{1}{d_U}}))^{\varpi_{j,i}}}{e(g^{x_0 - \sum_{j \in I'} \alpha_j^{'}}, g^s) \cdot \prod_{j \in I} e(g^{\alpha_j^{'}} g^{x_j w_{U,j}}, g^s)}$$

$$= M$$

Where $\{(\varpi_{j,i} \in \mathbb{Z}_p)_{i=1}^{l_j}\}_{j \in I}$ are a set of constants such that $\sum_{j \in I} \sum_{i=1}^{l_j} \varpi_{j,i} \lambda_{j,i} = s$ if $\{\{\lambda_{j,i}\}_{i=1}^{l_j}\}_{j \in I}$ are the valid shares of secret values according to the access structure $(\widehat{M}, \rho)$.

5. Security Analysis

Theorem 1. Suppose (T', ε')-decisional q-PBDHE assumption holds. CRPP-MACP-ABE is (T, q, ε) secure in the selective-access structure model, where $T' = T + O(T), \varepsilon' = \frac{1}{2}\varepsilon$.

Proof: We show that there exists an algorithm $\mathcal{B}$ to break the decisional q-PBDHE assumption by using the adversary $\mathcal{A}$, who breaks our CRPP-MACP-ABE at (T, q, ε). The challenger generates the bilinear group $(e, p, \mathbb{G}, \mathbb{G}_{\mathbb{T}})$ and selects a generator $g \in \mathbb{G}$. Let $\overrightarrow{Y} = g, g^{s}, g^{a}, \cdots, g^{a^{q}}, g^{a^{q+2}}, \cdots, g^{(a^{2q})}, g^{s \cdot b_j}, g^{\frac{a}{b_j}}, \cdots, g^{\frac{a^q}{b_j}}, g^{\frac{a^{q+2}}{b_j}}, \cdots, g^{\frac{a^q \cdot s \cdot b_k}{b_j}} \ (\forall 1 \le j \le q).$ Suppose R is randomly selected in $\mathbb{G}_{\mathbb{T}}$. The challenger determines to output a bit $\vartheta \in \{0,1\}$ by flipping an unbiased coin. If $\vartheta = 1$ then $(\overrightarrow{Y}, \Omega = R)$ is sent to $\mathcal{B}$, else $(\overrightarrow{Y}, \Omega = e(g, g)^{a^{q+1}s})$ is sent to $\mathcal{B}$ who outputs a guess ϑ' on ϑ .

$Setup$. Let I^* be an index set of the related $\widetilde{A}_j$. $\mathcal{A}$ submits access structure $\mathbb{A}=\{\widehat{M_j^*}, \rho_j^*\}_{j \in I^*}$. Suppose that $(\widehat{M^*}, \rho^*)$ is specified by $\widetilde{A}^*$ and not satisfied by the attributes chosen by $\mathcal{A}$ to inquire private keys. $\mathcal{B}$ chooses 4 cryptographic hash functions: $H_* : \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \times \mathbb{G} \times < \{0,1\}^* \times \mathbb{G} \cdots > \rightarrow \mathbb{G}$, $H_0 : \{0,1\}^* \times \mathbb{G} \times \cdots \times \mathbb{G} \rightarrow \{0,1\}^*$, $H_1 : \{0,1\}^* \times \mathbb{G} \rightarrow \mathbb{G}$, $H_2 : \mathbb{G} \times \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{G}$. There exits some authoritative institutiont or authentication mechanism (AI/AM) who confirms the user’s legality and generates legality evidence LV_U , i.e., $\aleph_U$, $H_*(\aleph_U)^{\wp}$, where $\aleph_U = RId_U, g^{\hbar}, g^{\wp}, g^{\wp d_U}, < N_{\widetilde{A}_j}, Z_{j,i}^{d_U} >_{a_{j,i} \in \widehat{U} \cap \widehat{A}_j, j \in I}$. $\mathcal{B}$ randomly selects $x_0, v \in \mathbb{Z}_p$ and computes the public key $X_0 = e(g, g)^{x_0}$ and g^{v} . $PP = (g, e, p, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, X_0, \ g^{\wp}, g^{v}, H_0, H_1, H_2)$ is open to $\mathcal{A}$.

$AuthoritiesSetup$. For the authority $\widetilde{A}_j \neq \widetilde{A}^*$, $\mathcal{B}$ gives the following simulation. $\widetilde{A}_j$ randomly chooses $\alpha_j, x_j \in \mathbb{Z}_p$, publishes the public key $PK_j = \{B_j = g^{x_j}, Z_{j,i} = (g^{z_{j,i}})_{a_{j,i} \in \widehat{A}_j}\}$ where $\widehat{A}_j$ is the attributes set of $\widetilde{A}_j$ and keeps $SK_j = \{\alpha_j, x_j, (z_{j,i})_{a_{j,i} \in \widehat{A}_j}\}$ secret.

For the authority $\widetilde{A}^*$, $\mathcal{B}$ randomly chooses $\alpha_0, \beta \in \mathbb{Z}_p$ and computes $B = g^{\beta}$. For the attribute $a_x \in \widehat{A^*}$, let $\widehat{X}$ stand for the set of indices i ($\rho^*(i) = a_x$).

(1) If attribute $a_x \in \widehat{A^*}$ and $a_x = \rho^*(i)$, then $\mathcal{B}$ randomly selects $z_x \in \mathbb{Z}_p$. $\mathcal{B}$ computes $Z_x = g^{z_x} \prod_{i \in \widehat{X}} g^{\frac{a \widehat{M_{i,1}^*}}{b_i}} \cdot g^{\frac{a^2 \widehat{M_{i,2}^*}}{b_i}} \cdots g^{\frac{a^{n*} \widehat{M_{i,n*}^*}}{b_i}}$, which is randomly distributed for the randomness of g^{z_x} .

(2) If attribute $a_x \in \widehat{A^*}$ and $\rho^*(i) \neq a_x$, then $\mathcal{B}$ randomly selects $z_x \in \mathbb{Z}_p$ and calculates $Z_x = g^{z_x}$.

$\mathcal{B}$ sends the public parameter $PK^* = (B, Z_x)$ of the authority $\widetilde{A}^*$ to $\mathcal{A}$.

$UserRegister$. We assume $\mathcal{A}$ acts as some legal users, such as U , whose register is an interactive procedure on the spot between $\mathcal{B}$ and $\mathcal{A}$ in secure communication channel. $U(\mathcal{A})$ also provides a legal legality evidence LV_U and sends it to IDM . If

$e(H_*(\aleph_U), g^{\wp}) = e(H_*(\aleph_U)^{\wp}, g)$ Then IDM responds to $U(\mathcal{A})$ the corresponding anonymous identity credential $AID_{cred} = \{Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j}, Sig_{a_{j,i},IDM}\}_{a_{j,i}\in\widehat{U}, j\in I}$.

Phase 1 Querying secret key

Assume querying secret key for U with pseudonyms $\{R_{U,j}\}_{\widehat{U}\cap\widehat{A}_j\neq\varnothing}$. The corresponding $\widehat{U}$ does not satisfy $\widehat{M^*}$.

$\mathcal{B}$ decides whether $Z_{j,i}^{d_U}, H_1(RId_U \,||\, R_{U,j}), N_{\widetilde{A}_j}$ is valid if $e(H_2(Z_{j,i}^{d_U}, H_1(RId_U \,||\, R_{U,j}), N_{\widetilde{A}_j})^v, g) = e(H_2(Z_{j,i}^{d_U}, H_1(RId_U \,||\, R_{U,j}), N_{\widetilde{A}_j}), g^v)$ for $a_{j,i} \in \widehat{U} \cap \widehat{A}_j$. $\mathcal{B}$ collects and records all valid $Z_{j,i}^{d_U}$ for each $R_{U,j}$.

(1) For $\widetilde{A}_j = \widetilde{A}^*$, $\mathcal{B}$ randomly selects $\alpha_0 \in \mathbb{Z}_p$ and computes $\alpha_0^{'} = PRF_{\alpha_0}(R_{U,j})$. $\mathcal{B}$ sets $\alpha = \alpha_0^{'} + a^{q+1}$ and computes $Y^* = e(g,g)^{\alpha} = e(g^a, g^{a^q})e(g,g)^{\alpha_0^{'}}$.

(a) If $a_x \in \widehat{A^*} \cap \widehat{U}$ and $\rho^*(i) = a_x$, $\mathcal{B}$ randomly selects $r \in \mathbb{Z}_p$ and a vector $\vec{V} = (v_1, v_2, \cdots, v_{n^*}) \in \mathbb{Z}_p^{n^*}$ such that $v_1 = -1$ and $\widehat{M_i^*} \cdot \vec{V} = 0$ for all $\rho^*(i) \in \widehat{A^*} \cap \widehat{U}$. $\mathcal{B}$ computes $K = g^{\alpha_0^{'}} g^{ra} \prod_{i=2}^{n^*} g^{v_i a^{q-i+2}}$ and $P = g^r \prod_{i=1}^{n^*} (g^{a^{q-i+1}})^{v_i} = g^w$. $\mathcal{B}$ implicitly defines $w = r + v_1 a^q + v_2 a^{q-1} + \cdots + v_{n^*} a^{q^{q-n^*+1}}$. $\mathcal{B}$ computes $F_x = (P^{z_x} \prod_{i\in\widehat{X}} \prod_{j=1}^{n^*} (g^{\frac{ra^j}{b_i}} \prod_{k=1,k\neq j}^{n^*} g^{\frac{v_k a^{q+1+j-k}}{b_i}})^{\widehat{M_{i,j}^*}})^{d_U} = (Z_x^{d_U})^w$.

(b) If $a_x \in \widehat{A^*} \cap \widehat{U}$ and $\rho^*(i) \neq a_x$, $\mathcal{B}$ computes $Z_x = g^{z_x}$ and $F_x = (P^{z_x})^{d_U} = (g^{z_x d_U})^w = (Z_x^{d_U})^w$.

For $a_x \in \widehat{A^*}$, because $K = g^{\alpha_0^{'}} g^{ra} \prod_{i=2}^{n^*} g^{v_i a^{q-i+2}} = g^{\alpha} g^{aw}, P = g^r \prod_{i=1}^{n^*} (g^{a^{q-i+1}})^{v_i} = g^w$, we say that the above secret key is right. Finally, $\mathcal{B}$ sends the private key $\{K, P, (F_x)_{a_x \in \widehat{U}\cap\widehat{A^*}}\}$ to $\mathcal{A}$.

(2) For $\widetilde{A}_j \neq \widetilde{A}^*$, $\mathcal{B}$ randomly selects $\alpha_j, w_j \in \mathbb{Z}_p$ and computes $\alpha_j{'} = PRF_{\alpha_j}(R_{U,j}), K_j = g^{\alpha_j^{'}} g^{x_j w_j}, P_j = g^{w_j}$, $F_{j,i} = Z_{j,i}^{w_j}$. Finally, $\mathcal{B}$ sends the private key $\{K_j, P_j, (F_{j,i})_{a_{j,i}\in\widehat{U}\cap\widehat{A}_j}\}$ to $\mathcal{A}$.

(3) For IDM, $\mathcal{B}$ computes $\alpha_{IDM} = x_0 - \sum_{j\in I''} \alpha_j^{'}$, gives $K_0 = g^{\alpha_{IDM}} = g^{x_0 - \sum_{j\in I'} \alpha_j^{'}}$ to $\mathcal{A}$.

Challenge: Two messages M_0, M_1 are presented by $\mathcal{A}$. $\mathcal{B}$ selects $\hat{\theta}$ by flipping a coin with {0,1}.

(1) For $\widetilde{A}^*$, $\mathcal{B}$ generates $X = g^a$. Then, $\mathcal{B}$ randomly selects $r_1, r_2, \cdots r_{l*}, f_2, f_3, \cdots, f_{n*} \in \mathbb{Z}_p$, and sets $\vec{f} = (s, sa + f_2, sa^2 + f_3, \cdots, sa^{n*-1} + f_{n*})$ which is applied for sharing the secret s. Λ_i is a set including all $\partial \neq i$ with $\rho^*(\partial) = \rho^*(i)$. $\mathcal{B}$ calculates $C_k = Z^{r_k}_{\rho^*(k)}(\prod_{j=2}^{n*}(g^a)^{\overbrace{M^*_{i,j}}f_j})(g^{b_k s})^{-z_{\rho^*(k)}} \cdot (\prod_{l\in\Lambda_i}\prod_{j=1}^{n*}(g^{a^j s(b_k/b_l)})^{\overbrace{M^*_{k,j}}})$ and $D_k = g^{-r_k}g^{-sb_k}$ where $k = 1, 2, \cdots, l^*$.

(2) For $\widetilde{A}_j$ ($j \in I^*$, $\widetilde{A}_j \neq \widetilde{A}^*$), $\mathcal{B}$ computes $X_j = g^{x_j}$ and randomly chooses $r_{j,1}, r_{j,2}, \cdots, r_{j,l_j}, f_{j,2}, f_{j,3}, \cdots, f_{j,n_j} \in \mathbb{Z}_p$. $\mathcal{B}$ sets $\vec{f}_j = (s, f_{j,2}, \cdots, f_{j,n_j})$ which is applied for sharing the secret s. $\mathcal{B}$ computes $C_{j,k} = g^{x_j s\overbrace{M_j^{k,1}}}\prod_{i=2}^{n_j} g^{f_{j,i}\overbrace{M_j^{k,i}}} Z^{-r_{j,k}}_{\rho_j(k)}$, $D_{j,k} = g^{r_{j,k}}$ ($k = 1, 2, \cdots, l_j$) and $C_0^* = M_{\hat{\theta}} \cdot e(g^{\alpha_{IDM}}, g^s) \cdot \Omega \cdot e(g^{\alpha_0'}, g^s) \cdot \prod_{j\in I^*, \widetilde{A}_j \neq \widetilde{A}^*} e(g,g)^{\alpha_j' s}$. That is $C_0^* = M_{\hat{\theta}} \cdot e(g,g)^{x_0 \cdot s}$. $\mathcal{B}$ finally computes $CT^* = \{C_0^*, X, (C_k, D_k)_{k=1}^{l*}, (X_j, (C_{j,k}, D_{j,k})_{k=1}^{l_j})_{j\in I^*, \widetilde{A}_j \neq \widetilde{A}^*}\}$.

Phase 2: repeat phase 1 again.

Guess: The simulation is successful. $\mathcal{A}$ outputs his/her guess $\tilde{\theta}$ of $\hat{\theta}$ flipped by $\mathcal{B}$, then $\mathcal{B}$ outputs $\vartheta' = 0$, which shows $\vartheta = 0$, $\Omega = e(g,g)^{a^{q+1}s}$ and CT^* is well formed about M_0. If $\tilde{\theta}$ is not equal to $\hat{\theta}$, then $\mathcal{B}$ outputs $\vartheta' = 1$, which indicates that Ω is a random number in $\mathbb{G}_{\mathbb{T}}$, $\vartheta = 1$. If $\vartheta = 0$, $\Pr[\mathcal{B}(\vec{Y}, \Omega = e(g,g)^{a^{q+1}s})] > \frac{1}{2} + \varepsilon$. If $\vartheta = 1$, $\Pr[\tilde{\theta} \neq \hat{\theta} \mid \vartheta = 1] = \frac{1}{2}$, which shows $\mathcal{A}$ outputs $\tilde{\theta} \neq \hat{\theta}$ with no advantage.

Since ϑ'=1 when $\tilde{\theta} \neq \hat{\theta}$, $\Pr[\vartheta' = 1 \mid \vartheta = 1] = \frac{1}{2}$, namely $\Pr[\vartheta' = \vartheta \mid \vartheta = 1] = \frac{1}{2}$. The advantage with which $\mathcal{B}$ breaks the decisional q-PBDHE is $|\frac{1}{2}\Pr[\tilde{\theta} = \hat{\theta} \mid \vartheta = 0] - \frac{1}{2}\Pr[\vartheta' = \vartheta \mid \vartheta = 1] | > \frac{1}{2} \times \frac{1}{2} + \frac{1}{2}\varepsilon - \frac{1}{2} \times \frac{1}{2} = \frac{1}{2}\varepsilon$.

Theorem 2. Given (g^v, v) and $h \in \mathbb{G}$, where $v \in \mathbb{Z}_p$, $g, g^v \in \mathbb{G}$, the signature h^v is existentially unforgeable under an adaptive chosen-message attack (ACMA) in CRPP-MACP-ABE.

Proof. In our scheme, we adopt the signature scheme of [42]. Given $g, g^v \in \mathbb{G}$, and $h \in \mathbb{G}$, where $h = H_2(Z^{d_U}_{j,i}, H_1(RId_U \,||\, R_{U,j}), \widetilde{A}_j)$, the signer outputs corresponding signature h^v and others verify the signature by checking whether $e(h, g^v) = e(h^v, g)$ or not. According to the proof in [42], we prove that the signature h^v is existentially unforgeable under an ACMA. Here, we do not go into details.

Theorem 3. Privacy-preserving that AAs do not know the user's identity and attributes holds in CRPP-MACP-ABE if the hardness of discrete logarithm and one-way property of hash functions holds.

Proof. For each attribute $a_{j,i}$, $\widetilde{A}_j$ randomly selects $z_{j,i} \in \mathbb{Z}_p$ satisfying $Z_{j,i} = g^{z_{j,i}} \neq \hat{e}$ ($\mathbb{G}$'s unit element). $Z_{j,i}$ is uniformly distributed in $\mathbb{G}$. Any element except unit element is generator in the prime order cyclic group, so $g^{z_{j,i}}$ is another new generator of $\mathbb{G}$. When registering, the user U randomly selects $d_U \in \mathbb{Z}_p$ and computes $(g^{z_{j,i}})^{d_U}$ which also satisfies uniform distribution in $\mathbb{G}$. Any other roles do not extract d_U from $(g^{z_{j,i}})^{d_U}$ for the hardness of discrete logarithm. d_U is only known by the user itself and IDM. U does not open the commitment g^{d_U}, so AAs and other users do not judge whether $Z_x = g^{z_{j,i}}$ by verifying $e(g^{d_U}, Z_x) = e(g, (g^{z_{j,i}})^{d_U})$ for Z_x denoted by each public attribute key. Above all, no probabilistic polynomial time role knows or distinguishes $g^{z_{j,i}}$ from $(g^{z_{j,i}})^{d_U}$. IDM generates a pseudonym $H_1(RId_U \,||\, R_{U,j})$. According to one-way property of hash functions, no probabilistic polynomial time adversary extracts his/her origin information RId_U from $H_1(RId_U \,||\, R_{U,j})$. This scheme realizes that authorities correctly issue keys for the user and know nothing about the user's identity and attributes.

Theorem 4. CRPP-MACP-ABE scheme is collusion-resisting among users or AAs.

Analysis of Users Collusion. Suppose malicious users $U_{adv}, U_{adv1}, U_{adv2}$ try to simulate the attacked target user $U_{T\arg et}$ when collusion happens. Without loss of generality, there are the following two cases: $(\overset{\frown}{U}_{adv1} \bigcup \overset{\frown}{U}_{adv2}) \bigcap \overset{\frown}{A}_j = \overset{\frown}{U}_{T\arg et} \bigcap \overset{\frown}{A}_j$ and $\overset{\frown}{U}_{T\arg et} \bigcap \overset{\frown}{A}_j = \overset{\frown}{U}_{adv} \bigcap \overset{\frown}{A}_j$, where $\overset{\frown}{U}_{T\arg et}$ denotes the attribute set of $U_{T\arg et}$ and $\overset{\frown}{U}_{adv}$, $\overset{\frown}{U}_{adv1}$, $\overset{\frown}{U}_{adv2}$ denote those of $U_{adv}, U_{adv1}, U_{adv2}$ respectively.

For two users $U_{T\arg et}$, U_{adv} such that $\overset{\frown}{U}_{T\arg et} \bigcap \overset{\frown}{A}_j = \overset{\frown}{U}_{adv} \bigcap \overset{\frown}{A}_j$, IDM assembles all $e(g,g)^{\alpha_j^{'} \cdot s}$ from related AAs and computes private key $e(g,g)^{\alpha_{IDM} \cdot s}$ for the user. Each $e(g,g)^{\alpha_j^{'} \cdot s}$ is determined by $\widetilde{A}_j$'s private key $\alpha_j^{'}$. U_{adv} does not obtain the same private key as that of the user $U_{T\arg et}$ from $\widetilde{A}_j$, since $\widetilde{A}_j$ generates different master keys by $\alpha_{j,_{T\arg et}}^{'} = PRF_{\alpha_j}(U_{T\arg et})$ and $\alpha_{j,adv}^{'} = PRF_{\alpha_j}(U_{adv})$ respectively. From what has been discussed above, U_{adv} does not obtain $\alpha_{j,adv}^{'} = \alpha_{j,T\arg et}^{'}$ to compute the right private key for decrypting related ciphertext blinded by $e(g,g)^{\alpha_{j,T\arg et}^{'} \cdot s}$. Similar with the above analysis, the users U_{adv1} and U_{adv2}, such that $(\overset{\frown}{U}_{adv1} \bigcup \overset{\frown}{U}_{adv2}) \bigcap \overset{\frown}{A}_j = \overset{\frown}{U}_{T\arg et} \bigcap \overset{\frown}{A}_j$, do not make collusion.

Analysis of authorities' collusion. In our paper, the protection of pseudonyms $H_1(RId_U \,||\, R_{U,j})$ and privacy of attributes make AAs not know the user's identity. $R_{U,j}$ is a different random value when facing different $\widetilde{A_j}$. AAs do not gather all relevant decryption keys by using the same pseudonym to realize collusion. Moreover, the user U must use d_U to decrypt the private key from AAs in advance when decrypting the ciphertext, which decentralizes the privilege of IDM or AAs. In other words, someone who obtains U's key also does not decrypt corresponding ciphertext. Antiquated blinded attribute public keys collected by AAs do not be combined to decrypt the ciphertext too.

6. Efficiency

Performance comparison between PPDC-MACP-ABE scheme [15] and our scheme are presented in the following three tables.

$\hat{L}$ stands for the number of AAs in our scheme. Let I be the index set of AAs who manages the attributes of the user U. $\widetilde{TE_{\mathbb{G}_{\mathbb{T}}}}$, $\widetilde{TE_{\mathbb{G}}}$ are exponentiation operation time of an element in $\mathbb{G}_{\mathbb{T}}$ and $\mathbb{G}$, respectively. Let $\widetilde{TP}$ be the operation time of bilinear pairing operation and l_j be the number of the rows of the matrix of access structure. Besides, $\widehat{U}$ is the set of attributes held by U. q_j is the quantity of the attributes managed by $\widetilde{A_j}$. Our scheme spends less computation cost than that of $AuthoritiesSetup$, $KeyGeneration$, $EnCryption$ in PPDC-MACP-ABE. Users' registration is precomputed in the preparation phase, in which IDM generates identity credentials for all users.

Table 1. The comparison of computation cost on DC-MACP-ABE schemes and CR-MACP-ABE

Algorithm	**DC-MACP-ABE** [15]	**CR-MACP-ABE**
$UserRegister$	Anonymous Credential	Identity Credential (issued by IDM)
$AuthoritiesSetup$	$(\sum_{i=1}^{\hat{L}} 3q_i)\widetilde{TE_{\mathbb{G}}} + \hat{L}(4\widetilde{TE_{\mathbb{G}}} + \widetilde{TE_{\mathbb{G}_{\mathbb{T}}}})$	$(\sum_{j=1}^{\hat{L}} q_j)\widetilde{TE_{\mathbb{G}}} + \hat{L}\cdot\widetilde{TE_{\mathbb{G}}}$
$KeyGeneration$	$(9\hat{L}+\mid\widehat{U}\mid)\widetilde{TE_{\mathbb{G}}}$	$(1+3\hat{L}+\mid\widehat{U}\mid)\widetilde{TE_{\mathbb{G}}}$
$Decryption$	$(\mid I\mid\widetilde{TE_{\mathbb{G}}} + 3\mid I\mid\widetilde{TE_{\mathbb{G}}}$ $+(3\sum_{j\in I} l_j)\widetilde{TE_{\mathbb{G}}}$	$(\mid I\mid+1)\widetilde{TE_{\mathbb{G}}} +$ $(3\sum_{j\in I} l_j)(\widetilde{TE_{\mathbb{G}_{\mathbb{T}}}} + \widetilde{TE_{\mathbb{G}}})$
$EnCryption$	$(\mid I\mid\widetilde{TE_{\mathbb{G}_{\mathbb{T}}}} + 3\mid I\mid\widetilde{TE_{\mathbb{G}}} + (3\sum_{j\in I} l_j)\widetilde{TE_{\mathbb{G}}}$	$\widetilde{TE_{\mathbb{G}_{\mathbb{T}}}} + (3\sum_{j\in I} l_j + 1)\widetilde{TE_{\mathbb{G}}}$

Table 2. The computation cost of the interactive algorithm between user U and AAs

Scheme	$User \quad U$	$Authority \quad \widetilde{A_j}$
PPDC-MACP-ABE [15]	$3\mid\widehat{U}\cap\widehat{A_j}\mid\widetilde{TE_{\mathbb{G}_{\mathbb{T}}}} + (35+7\mid I\mid)\widetilde{TE_{\mathbb{G}}}$ $+(4+3\mid\widehat{U}\cap\widehat{A_j}\mid)\widetilde{TP}$	$4\mid\widehat{U}\cap\widehat{A_j}\mid\widetilde{TE_{\mathbb{G}_{\mathbb{T}}}} +$ $(18+5\mid\widehat{U}\cap\widehat{A_j}\mid)\widetilde{TE_{\mathbb{G}}}+$ $(3+5\mid\widehat{U}\cap\widehat{A_j})\widetilde{TP}$
CRPP-MACP-ABE	0	$2\mid\widehat{U}\cap\widehat{A_j}\mid\widetilde{TP}$

In PPDC-MACP-ABE, U pays a lot of computing cost which makes $\widetilde{A}_j$ not know the U's private key. In our scheme, U does not compute but only give $AID_{cred,j}$ to $\widetilde{A}_j$ who checks whether $e(Sig_{a_{j,i},IDM}, g)$ is equal to $e(H_2(Z_{j,i}^{d_U}, Pid_{U,j}, N_{\widetilde{A}_j}), g^v)$ for each blinded attribute public key after receiving $AID_{cred,j}$. Our scheme reduces dramatically the computation cost of the interactive procedure between U and AAs, relative to that of PPDC-MACP-ABE.

7. Conclusion

We propose a CRPP-MACP-ABE scheme, which improves security in privacy-preserving and collusion-resisting aspects. Protecting sensitive attributes is extremely important in privacy-preserving system. In order to keep ABE scheme's traditional design idea, i.e., decrypting ciphertext only depends on user's attributes and it is different from the fully pure identity-based cryptography, we adopt pseudonyms plus binding each blind attribute model, where the user convinces AAs to believe that these attributes belong to legal user and issue corresponding secret keys by checking signatures issued by essential IDM without knowing both the identities and attributes of users.

AAs generate their private keys related user's identity effectively to resist users' collusion. The privacy-preserving of our scheme prevents AAs from impersonating one user by directly using his/her attributes' information. The user selects a secret and random value, which prevents antiquated blinded public attribute keys collected by AAs.

Our subsequent work is trying to weaken the requirement of the fully trusted IDM and building a decentralized CRPP-MACP-ABE scheme, where each authority works independently without any collaboration.

References

[1] Hao. Yan, J. Li, J. Han. "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, August, 2017. Article (CrossRef Link)

[2] J. Li, H. Yan, and Y. Zhang. "Certificateless public integrity checking of group shared data on cloud storage," *IEEE Transactions on Services Computing*, 2018. Article (CrossRef Link)

[3] H. Li, H. Zhu, S. Du, X. Liang, X. (Sherman) Shen, "Privacy leakage of location sharing in mobile social networks: attacks and defense," *IEEE Transactions on Dependable and Secure Computing*, August, 2016. Article (CrossRef Link)

[4] H. Li, Q. Chen, H. Zhu, D. Ma, H. Wen, X. (Sherman) Shen, "Privacy leakage via de-anonymization and aggregation in heterogeneous social networks," *IEEE Transactions on Dependable and Secure Computing*, 2017, Article (CrossRef Link)

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. of 24th Annu. Int.Conf. Theory Appl. Cryptograph*. Techn, pp. 457-473, May 22-26, 2005. Article (CrossRef Link)

[6] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. of 13th ACM Conf. Comput. Commun. Security*, pp. 89-98, October 30 - November 03, 2006. Article (CrossRef Link)

[7] J. Li, W. Yao, Y. Zhang, H. Qian and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Trans. Service Comput*, vol. 10, no. 5, pp. 785-796, 2017. Article (CrossRef Link)

[8] S.Yu, C. Wang, K. Ren, et al., "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. of IEEE INFOCOM 2010*, pp. 1-9, March 14-19, 2010. Article (CrossRef Link)

[9] K. Yang, X. Jia, R. Kui, "Attributed-based fine-grained access control with efficient revocation in cloud storage systems," in *Proc. of the 8th ACM SIGSAC symposium on Information, Computer and Communications Security*. ACM, pp. 523-528, May 08 – 10, 2013. Article (CrossRef Link)

[10] M. Chase, "Multi-authority attribute based encryption," in *Proc. of Theory of Cryptography (Lecture Notes in Computer Science)*, vol. 4392, Heidelberg, Germany: Springer-Verlag, pp. 515-534, 2007. Article (CrossRef Link)

[11] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proc. of 16th ACM Conf. CCS*, pp. 121-130, November 09–13, 2009. Article (CrossRef Link)

[12] J. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 11, pp. 2150-2162, Nov. 2012. Article (CrossRef Link)

[13] H. Qian, J. Li and Y. Zhang, "Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure," in *Proc. of Information and Communications Security (Lecture Notes in Computer Science)*, vol. 8233, Heidelberg, Germany: Springer-Verlag, pp. 363-372, 2013.Article (CrossRef Link)

[14] H. Qian, J. Li, Y. Zhang and J. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," *Int. J. Inf. Secur*., vol. 14, no. 6, pp. 487-497, November, 2015. Article (CrossRef Link)

[15] J. Han, W. Susilo, Y. Mu, et al., "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," *IEEE Transactions on information forensics and security*, vol. 10, no. 3, pp. 665-678, Mar. 2015. Article (CrossRef Link)

[16] 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, August 18, 2016. Article (CrossRef Link)

[17] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. of IEEE Symp. SP*, pp. 321–334, May, 2007. Article (CrossRef Link)

[18] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. of 14th ACM Conf. CCS*, pp. 195–203, 2007. Article (CrossRef Link)

[19] A. Lewko, T. Okamoto, A. Sahai, K. Takashima and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. of International Conference on Theory and Applications of Cryptographic Techniques (Lecture Notes in Computer Science)*, vol. 6110. Heidelberg, Germany: Springer-Verlag, pp. 62-91, May 30 – June 3, 2010. Article (CrossRef Link)

[20] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *Proc. of Public Key Cryptography (Lecture Notes in Computer Science)*, vol. 6571. Heidelberg, Germany: Springer-Verlag, pp. 53-70, March 6-9, 2011. Article (CrossRef Link)

[21] K. Emura, A. Miyaji, A. Nomura, et al., "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Proc. of International Conference on Information Security Practice and Experience, Springer-Verlag*, pp. 13-23, April 13-15, 2009. Article (CrossRef Link)

[22] J. Li, F. Sha, Y. Zhang, X. Huang and J. Shen. "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length," *Security and Communication Networks*, 2017. Article (CrossRef Link)

[23] Z. Wan, J. Liu, RH. Deng, "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Transaction on Information Forensics and Security*, vol. 7, no. 2, pp. 743-754, April, 2012. Article (CrossRef Link)

[24] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu, W. Shi. "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," *Information Sciences*. vol. 275, pp. 370-384, August, 2014. Article (CrossRef Link)

[25] Y. Guo, J. Li, Y. Zhang, J. Shen. "Hierarchical attribute-based encryption with continuous auxiliary inputs leakage," *Security and Communication Networks*, vol. 18, no. 9, pp. 4852-4862, 2016. Article (CrossRef Link)

[26] J. Hur and D.K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214- 1221, July, 2011. Article (CrossRef Link)

[27] J. Lai, RH. Deng, Y. Li, "Fully secure ciphertext-policy hiding CP-ABE," in *Proc. of International Conference on Information Security Practice and Experience*, Springer-Verlag, pp. 24-39, May 30 - June 1, 2011. Article (CrossRef Link)

[28] J. Li, H. Wang, Y. Zhang, J. Shen. "Ciphertext-policy attribute-based encryption with hidden access policy and testing," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 7, pp. 3339-3352, July, 2016. Article (CrossRef Link)

[29] K. Yang, X. Jia, "Expressive efficient and revocable data access control for multi-authority cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp.1735-1744, July, 2014. Article (CrossRef Link)

[30] Y. Chen, L. Song, G. Yang, "Attribute-based access control for multi-authority systems with constant size ciphertext in cloud computing," *China Communication*, vol. 13, no. 2, pp. 146-162, February, 2016. Article (CrossRef Link)

[31] J. Li, W. Yao, J. Han, Y. Zhang and J. Shen, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE Systems Journal*, 2017. Article (CrossRef Link)

[32] Y. Rahulamathavan, S. Veluru, J. Han, et al., "User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption," *IEEE Transactions on Computers*, vol. 65, no. 9, pp.2939-2946, Sept 9, 2016. Article (CrossRef Link)

[33] Z. Liu, Z. Cao, Q. Huang, et al., "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in *Proc. of European Conference on Research in Computer Security*, Springer-Verlag, pp.278-297, September 12-14, 2011. Article (CrossRef Link)

[34] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Trans. Service Comput.*, 10(5): 715-725, 2017. Article (CrossRef Link)

[35] J. Li, Y. Shi, Y. Zhang. "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," *International Journal of Communication Systems*, vol. 30, no. 1, January, 2017. Article (CrossRef Link).

[36] J. Ning, Z. Cao, X. Dong, H. Ma, L. Wei, K. Liang. "Auditable σ-times outsourced attribute-based encryption for access control in cloud computing". *IEEE Transactions on Information Forensics and Security*. Article (CrossRef Link)

[37] J. Li, Y. Wang, Y. Zhang, J. Han. "Full verifiability for outsourced decryption in attribute based encryption," *IEEE Transactions on Services Computing*, May, 2017. Article (CrossRef Link)

[38] J. Ning, X. Dong, Z. Cao, L. Wei and 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. Article (CrossRef Link).

[39] J. Ning, Z. Cao, X. Dong, and 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*. Article (CrossRef Link)

[40] J. Li, Q. Yu, Y. Zhang. "Key-policy attribute-based encryption against continual auxiliary input leakage," *Information Sciences*, 2018. Article (CrossRef Link)

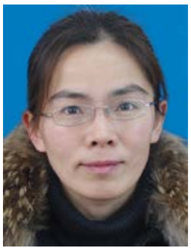
[41] Moni Naor, Benny Pinkas and Omer Reingold, "Distributed pseudo-random functions and KDCs," in *Proc. of EUROCRYPT' 1999*, vol. 1592, pp. 327-346, Springer, April 15, 1999. Article (CrossRef Link)

[42] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptology*, vol. 17, no.4, pp. 297-319, Sept, 2004. Article (CrossRef Link)

[43] A. Beime, "Secure schemes for secret sharing and key distribution," *Ph.D. dissertation, Dept. Comput. Sci.*, Technion—Israel Inst. Technol., Haifa, Israel, 1996. Article (CrossRef Link)

Shengzhou Hu received the B.S. and M.S. degrees in computer information engineering from Jiangxi Normal University, Jiangxi, China, in 1998 and 2006, respectively. He is currently a Ph.D student of Hohai University, China. His research interests include cloud computing security and public key cryptography.

Jiguo Li received his B.S. degree in mathematics from Heilongjiang University, Harbin, China in 1996, M.S. degree in mathematics and Ph.D. degree in computer science from Harbin Institute of Technology, Harbin, China in 2000 and 2003, respectively. During 2006.9-2007.3, he was a visiting scholar at Centre for Computer and Information Security Research, School of Computer Science & Software Engineering, University of Wollongong, Australia. During 2013.2-2014.1, he was a visiting scholar in Institute for Cyber Security in the University of Texas at San Antonio. He is currently a professor with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China and College of Computer and Information, Hohai University, Nanjing, China. His research interests include cryptography and information security, cloud computing, wireless security and trusted computing etc. He has published over 150 research papers in refereed international conferences and journals. His work has been cited more than 3000 times at Google Scholar. He has served as program committee member in over 20 international conferences and served as the reviewers in over 90 international journals and conferences.



Yichen Zhang received the Ph.D. degree in the College of Computer and Information, Hohai University, Nanjing, China in 2015. She is currently an associate professor. Her research interests include cryptography, network security. She has published over 30 research papers in refereed international conferences and journals.