SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2015; **8**:4098–4109
Published online 25 August 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1326

RESEARCH ARTICLE

Provably secure unbounded multi-authority ciphertext-policy attribute-based encryption

Qi Li[1,2]*, Jianfeng Ma[1,2], Rui Li[3], Jinbo Xiong[4] and Ximeng Liu[2,5]

[1] School of Computer Science and Technology, Xidian University, Xi'an, China
[2] Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an, China
[3] School of Software and Institute of Software Engineering, Xidian University, Xi'an, China
[4] Faculty of Software, Fujian Normal University, Fuzhou, China
[5] School of Telecommunications Engineering, Xidian University, Xi'an, China

ABSTRACT

Multi-authority attribute-based encryption (ABE) is a generation of ABE where the descriptive attributes are managed by different authorities. In current multi-authority ABE schemes, the scale of attribute universe employed in encryption is restricted by various predefined thresholds. In this paper, we propose an unbounded multi-authority ciphertext-policy ABE system without such restriction. Our scheme consists of multiple attribute authorities (AAs), one central authority (CA), and users labeled by the set of attributes. Each AA governs a different universe of attributes and operates separately. Moreover, there is no cooperation between the CA and AAs. To provide the private keys for a user, the AAs first issue partial attribute-related keys according to the attributes; the CA then issues identity-related keys and links these attribute-keys with the user's global identifier. Both the identity-related and the linked attribute-related keys will be used in decryption. The proposed multi-authority ciphertext-policy ABE scheme can support arbitrary linear secret sharing scheme as the access policy. Performance analysis and security proof indicate that our scheme is efficient and secure. Copyright © 2015 John Wiley & Sons, Ltd.

KEYWORDS
access control; unbounded; ciphertext-policy; multi-authority; attribute-based encryption

***Correspondence**
Qi Li, Nanjing University of Posts and Telecommunications, No.9 Wenyuan Road, Nanjing, 210046, China.
E-mail: qilijs@gmail.com

1. INTRODUCTION

In identity-based encryption (IBE) schemes, data can be encrypted by the identity of target recipient, which is indicated by any string (such as email address). However, IBE is powerless in such scenarios, when the target receivers are expressed by a set of attributes rather than concrete identities. For instance, Alice wants to encrypt a massage for all professors or PhD Candidates in the Department of Computer Science. She needs to encrypt the message under such access policy ("department of Computer Science" AND "professor" OR "PhD Candidate"). Only the receivers who possess a set of attributes that matches the policy can recover the message. Moreover, the encryption system should provide collusion-resistance security. That is, the colluding receivers cannot find success in decryption unless one of them is authorized. Thereby, an encryption system that supports various attributes and provides the security against the collusion attack should be addressed.

To address this concern, Sahai and Waters (SW) [1] proposed an encryption scheme that was called attribute-based encryption (ABE). In order to support s more expressive access structure (policy), Goyal *et al.* [2] extended SW results [1] into key-policy ABE (KP-ABE) and introduced another type of ABE that can be called ciphertext-policy ABE (CP-ABE). In general, in KP-ABE, the ciphertext is annotated with some attributes, and for each user, the private key is annotated with a specific access structure to specify which ciphertext the user can decrypt. In contrast, the ciphertext is annotated with a specified access policy and the user's private keys are associated with some attributes in CP-ABE. In both KP-ABE and CP-ABE, the decryption succeeds if the attributes match the access structure. Bethencourt *et al.* [3] gave the first explicit CP-ABE construction. All of the schemes mentioned above only supported a single authority. It means that the attributes in the system are administered by a single

Copyright © 2015 John Wiley & Sons, Ltd.

authority. Since then, various varieties of single-authority ABE schemes [4–15] are proposed.

Because the ABE scheme with a single authority is not ideal in such applications that the attributes may be issued by different authorities. For example, a user may have such set of attributes ("patient" and "undergraduate student") where "patient" is issued by a "hospital" and "undergraduate student" is issued by a "university". To overcome this drawback, Chase [16] introduced the notion of multi-authority ABE (MA-ABE) and presented the first MA-ABE system. In the construction, one central authority (CA) and multiple attribute authorities (AAs) exist. Each user is labeled with a unique global identifier (GID). The CA generates an identity-related (GID-related) key for each user. The AAs are responsible for managing the attributes and issuing the attribute-related keys. The components of a user's attribute-related keys issued by the AAs are tied to his GID to prevent collusion attacks. Since then, many MA-ABE systems [17–23] are proposed.

The limitation of the previous multi-authority ABE schemes is that, once the public parameters have been chosen in the setup stage, a user is not allowed to construct completely arbitrary and flexible access structures and attribute sets in encryption. Lewko *et al.* [24] first introduced this restriction and classified the ABE system into two types: small attribute universe and large attribute universe. In the former system, the scale of attribute universe is polynomially bounded in the security parameters, which are chosen in initializing the system. Furthermore, the scale of public parameters depends on the amount of system attributes. In the latter system, the attribute domain can be set exponentially large. Unfortunately, in such large attribute universe systems [1,2,23], the number of the attributes employed in encryption cannot overrun a predefined threshold. Thus, such systems [1,2,23] can be called semi-large construction. This restriction will cause a bottleneck in dynamically practical applications. More precisely, if the system parameters are set too large, the needlessly large public parameters will cause superfluous inefficient computing and prevent the scheme from being deployed in resource-limited situations. On the other hand, if the system initialization parameters are set too small, such system has to be rebuilt while its restrictive condition is outstripped. Lewko *et al.* [24] constructed the first unbounded KP-ABE system on composite order groups, which can support fully large attribute universe without such restriction. Subsequently, Rouselakis *et al.* [25] extended their technique into the prime order groups. These schemes [24,25] were constructed in single-authority settings. Recently, Li *et al.* [26] proposed a multi-authority KP-ABE scheme with unbounded attribute universe. However, their approach does not work in CP-ABE settings. It remains open how to construct a CP-ABE scheme that can simultaneously support unbounded attribute universe and multiple authorities.

1.1. Our Contributions

- We present a new unbounded multi-authority CP-ABE scheme. Unlike all previous MA-CP-ABE schemes, we do not impose any restrictions in the initial phase. The scale of system public parameters in our scheme is independent of the amount of attributes.
- In our system, any participant can be an AA by announcing its public parameters along with the unique attribute universe it manages. The private keys of a user are generated as follows: The AAs first produce partial attribute-related keys according to the user's attributes. They execute independently from each other. Then the CA issues keys according to the user's GID and links the GID with the partial attribute-related keys to resist collusion attacks.
- The proposed scheme supports arbitrary monotonic linear secret sharing scheme (LSSS) access policy and is secure against at most F AAs corruptions,* where F denotes the total number of AAs. Our scheme is constructed over prime order groups and proved to be selectively secure in the standard model.

We briefly introduce the organization of the paper. Section 2 reviews some relevant literatures, and Section 3 introduces the preliminaries we will use in this paper. Section 4 formalizes the definitions of our multi-authority CP-ABE. In Section 5, we first introduce the challenges and our techniques used in designing the unbounded multi-authority CP-ABE system. Then, we give the detail construction of our MA-CP-ABE scheme. Section 6 describes the security model and analyzes the selective security of our scheme. We compare the characteristics and performance with some related systems in Section 7. Finally, the paper concludes in Section 8.

2. RELATED WORK

Identity-based encryption is first introduced by Shamir [27] and subsequently constructed by Boneh *et al.* [28] and Cocks [29]. Later, IBE systems were widely studied [29–32]. By refining IBE techniques, Sahai and Waters first proposed the notion of ABE [1]. Subsequently, Goyal *et al.* [2] presented the first construction of KP-ABE scheme. Bethencourt *et al.* [3] gave the first CP-ABE construction.

The problem of constructing ABE schemes with attributes coming from different authorities was answered by Chase. She gave the first MA-KP-ABE scheme [16], where there are a CA and multiple authorities. To prevent a collusion attack, A GID of the user was employed to bind the private keys from different authorities. Lin *et al.* [22] proposed an MA-ABE system without the CA by

* From the security proof in Section 6, we can see that even if F AAs are all corrupted, the adversary still cannot decrypt the challenge ciphertext as long as the queried attributes for each GID do not satisfy the challenge access structure.

applying threshold techniques. The scheme cannot resist the attack from k or more users collusion, where k is a predefined parameter chosen at the setup stage. Chase and Chow [17] also proposed a MA-KP-ABE system without a CA by employing distributed pseudorandom functions. In addition, the privacy (GID) of a user was preserved by using an anonymous key issuing protocol. Müller *et al.* [20,21] presented the first MA-CP-ABE scheme with the CA remains. In contrast to all previous MA-ABE schemes, Lewko *et al.* presented an adaptively secure MA-CP-ABE scheme [18] in the random oracle model where no CA is required and each AA operates separately. Liu *et al.* [23] proposed another adaptively secure MA-CP-ABE system in the standard model basing on the single-authority CP-ABE scheme [7]. Both the systems [18,23] were constructed on composite order bilinear groups. In order to trace the user who leaked the private key to someone else, Li *et al.* [19] presented an accountable MA-ABE system.

The large universe problem in ABE schemes was first addressed in [1]. Goyal *et al.* [2] presented a semi-large universe KP-ABE scheme. In this scheme, the scale of attribute set S used while encrypting is limited to a value n, which was fixed in the system initialization stage. The overhead of public parameters increases linearly with n. Lewko *et al.* [24] introduced the first unbounded KP-ABE scheme without such restriction. The presented scheme was proved selectively secure by employing the dual system technique [7,8]. However, because the scheme [24] was constructed over composite order groups, the overhead of paring computations is inefficient to a comparable prime order ABE schemes. In [25], Rouselakis *et al.* showed how to construct an unbounded single-authority CP-ABE scheme over prime order groups.

3. PRELIMINARIES

In this section, the definitions of bilinear pairings and LSSS are presented. We also introduce the complexity assumption, which is used in the security proof.

3.1. Bilinear pairings

Definition 1. *Choose two multiplicative cyclic groups $\mathbb{G}$ and $\mathbb{G}_1$ of prime order p. g denotes a generator of group $\mathbb{G}$. We say the map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ is bilinear if*

(1) (Bilinear) for all $h, \zeta \in \mathbb{G}$, we have $e(h^x, \zeta^y) = e(h, \zeta)^{xy}$ where $x, y \in \mathbb{Z}_p$.
(2) (Non-degenerate): $e(g, g) \neq 1$.

The map e is symmetric because $e(g^x, g^y) = e(g, g)^{xy} = e(g^y, g^x)$.

3.2. Linear secret sharing scheme

Definition 2. *A secret sharing scheme $\Im$ over a collection of attributes $\mathbb{P}$ is linear if*

(1) The shares for each attribute form a share vector over $\mathbb{Z}_p$.
(2) A matrix A with ℓ rows and n columns is said to be the share-generating matrix if for all $i = 1, \ldots, \ell$, the ith row of A is labeled with an attribute $\rho(i)$ (the function ρ maps $\{i = 1, \ldots, \ell\}$ to $\mathbb{P}$). While considering the vector $\upsilon = (s, \hbar_2, \ldots, \hbar_n)^\top$, where $s \in \mathbb{Z}_p$ is the secret and $\hbar_2, \ldots, \hbar_n \in \mathbb{Z}_p$ are randomly picked, $A\upsilon$ denotes the vector of ℓ shares, and $(A\upsilon)_i$ belongs to the attribute $\rho(i)$.

As mentioned in [33], every LSSS has the linear reconstruction property, defined in the following: let $\Im$ be an LSSS for an access policy $\mathbb{A}$. We let $S \in \mathbb{A}$ denote an authorized attribute set and define $I \subset \{1, 2, \ldots, \ell\}$ as $I = \{i : \rho(i) \in S\}$. Then we can find constants $\omega_i \in \mathbb{Z}_p$, if the shares $\{\lambda_i = (A\upsilon)_i\}$ are valid, then we can recover s by $\sum_{i \in I} \omega_i \lambda_i$. Nevertheless, if S is unauthorized, there are no such constants.

3.3. Assumption

The security of our scheme relies on a z-type assumption [25], which is similar compared with the decisional z-type assumption [9]. We now give the definition as follows:

Select a group $\mathbb{G}$ of prime order p. We denote g as a generator of $\mathbb{G}$ and randomly choose exponents $d, s, t_1, t_2, \ldots, t_z \in \mathbb{Z}_p$. $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ is a bilinear map. If an adversary receives the group specification $(p, \mathbb{G}, \mathbb{G}_1, e)$ and the following terms,

$$
\begin{aligned}
&T = \\
&g, g^s, \\
&g^{d^i}, g^{t_j}, g^{st_j}, g^{d^i t_j}, g^{d^i/t_j^2}, \forall (i,j) \in [z, z]; \\
&g^{d^i/t_j}, \forall (i,j) \in [2z, z] \text{ with } i \neq z+1; \\
&g^{d^i t_j/t_{j'}^2}, \forall (i,j,j') \in [2z, z, z] \text{ with } j \neq j'; \\
&g^{sd^i t_j/t_{j'}}, g^{d^i t_j/b_{j'}^2} \forall (i,j,j') \in [z, z, z] \text{ with } j \neq j.'
\end{aligned}
$$

the adversary has to distinguish $e(g, g)^{d^{z+1}s} \in \mathbb{G}_1$ from a randomly chosen element $R \in \mathbb{G}_1$.

The advantage of the adversary $\mathcal{A}$ in solving the z-type problem is defined as $| Pr[\mathcal{A}(T, W = e(g, g)^{d^{z+1}s}) = 0] - Pr[\mathcal{A}(T, W = R) = 0] |$.

Definition 3. *The z-type assumption holds if no probabilistic polynomial time (PPT) adversary can win the previous security game with a non-negligible advantage.*

4. DEFINITION OF MULTI-AUTHORITY CP-ABE

We now introduce the background of the unbounded multi-authority CP-ABE as shown in Figure 1. In our MA-CP-ABE scheme, there exist three sets of entities, denoted

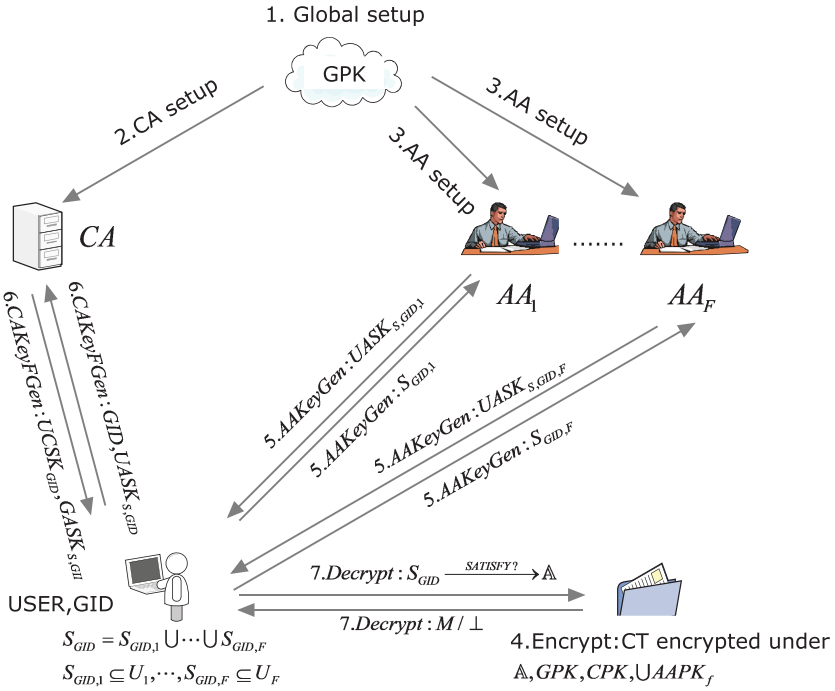

Figure 1. Overview of the unbounded multi-authority ciphertext-policy attribute-based encryption. CA, central authority; AA, attribute authority; GID, global identifier; CT, ciphertext.

by (1) a central authority (CA), (2) attribute authorities (AAs), and (3) users. Each user in the system is labeled by a unique GID and issued some descriptive attributes. Each AA is in charge of governing a distinct universe of attributes and issuing partial attribute-keys to a user according to his descriptive attributes. The CA assigns keys to a user according to his/her GID and associates the attribute-keys with his GID.

Let $\mathbb{F} = \{1, \ldots, F\}$ denote the index set of AAs ($f \in \mathbb{F}$ denotes the index of the attribute authority AA_f). Let U_f be the attribute domain administrated by AA_f. For all $i \neq j \in \mathbb{F}$, we have $U_i \bigcap U_j = \varnothing$. The total system attribute domain is denoted by $U = \bigcup_{f=1}^{F} U_f$.

A MA-CP-ABE scheme consists of the following seven PPT algorithms:

GlobalSetup $(\lambda) \rightarrow (GPK)$: By taking as input a security parameter λ, the **GlobalSetup** algorithm then outputs the system global public parameters GPK.

CASetup $(GPK) \rightarrow (CPK, CMK)$: The **CASetup** algorithm takes GPK as input and produces the CA's public parameter CPK and the CA's master secret key CMK.

AASetup $(GPK, f, U_f) \rightarrow (AVK_f, ASIG_f, APK_f, AMK_f)$: The **AASetup** algorithm takes GPK, the AA's index f, and its attribute universe U_f as input and generates the AA's public parameter APK_f and the AA's master secret key AMK_f. Additionally, each AA_f generates a key pair $(AVK_f, ASIG_f)$. AVK_f will be used by the CA only.

Encrypt $(M, \mathbb{A}, GPK, CPK, \bigcup APK_f) \rightarrow (CT)$: This algorithm takes a plaintext message M, an access policy $\mathbb{A}$, GPK, CPK, and the relevant AAs' public parameters as input. It makes a ciphertext CT.

AAKeyGen $(S_{GID,f}, GPK, ASIG_f, AMK_f) \rightarrow (UASK_{S,GID,f})$: We let $S_{GID,f}$ be the set of attributes that belongs to user GID and is managed by AA_f. When a user requests the partial attribute-key of $S_{GID,f}$, AA_f runs the **AAKeyGen** algorithm with GPK, $ASIG$, and AMK_f as input and outputs the partial attribute-key $UASK_{S,GID,f} = \{UASK_{ATT,GID} | ATT \in S_{GID,f}\}$, where $UASK_{S,GID,f}$ will be used by the CA in producing the final attribute-key. We denote $UASK_{S,GID} = \bigcup UASK_{S,GID,f}$ as the partial attribute-key of S_{GID}, where $S_{GID} = \bigcup S_{GID,f}$.

CAKeyGen $(GID, GPK, CMK, UASK_{S,GID}, \{AVK_f | f \in \mathbb{F}\}) \rightarrow (GCSK_{GID}, GASK_{S,GID})$: After receiving $UASK_{S,GID}$ and GID, the CA first verifies the validity of $UASK_{S,GID}$. If not, it outputs $\perp$. Otherwise, the CA runs this algorithm with a user's GID, GPK, and CMK as input to produce the GID-key $GCSK_{GID}$ and the final attribute-key $GASK_{S,GID}$.

Decrypt $(CT, GPK, GCSK_{GID}, GASK_{S,GID}) \rightarrow (M)$: The **Decrypt** algorithm takes CT, GPK, $GCSK_{GID}$, and $GASK_{S,GID}$ as input. If S_{GID} satisfies $\mathbb{A}$, the algorithm outputs M; otherwise, it outputs $\perp$.

For simplicity, we assume each attribute is used only once in the access structure (such a scheme is called one-use scheme). Our scheme can be transformed to support multiple used attributes by employing the technique in [7]. Identical to previous

Table I. Description of symbols employed in the scheme.

Symbol	Description
GPK	The global public parameters
CPK, CMK	The public parameters and master secret key of the CA, respectively
f	The index of AA_f
U	The system attribute universe
U_f	The attribute domain governed by AA_f
$AVK_f, ASIG_f$	A pair of verification and sign keys of AA_f
APK_f, AMK_f	The public parameters and master secret key of the AA_f, respectively
$\mathbb{A}$	Access structure
GID	The unique global identifier of a user
S_{GID}	The attribute set possessed by the user with GID
$S_{GID,f}$	The set of a user's attributes issued by AA_f
$UASK_{S,GID,f}$	The partial attribute-key generated by AA_f
$GCSK_{GID}$	The GID-key issued by the CA
$GASK_{S,GID}$	The final attribute-key generated by the CA

constructions, our system can only support static attributes.* To facilitate the understanding, Table I introduces the description of symbols employed in the scheme.

5. UNBOUNDED MULTI-AUTHORITY CP-ABE

We first introduce the challenges and our techniques in designing the unbounded MA-CP-ABE scheme. Then we propose the detailed unbounded MA-CP-ABE scheme.

5.1. Overview of our approach

Our goal is to construct a secure CP-ABE scheme which can support multiple authorities and fully large universe simultaneously. Inspired by the schemes in [16,23,25], we achieve this goal by proposing a provably secure large universe multi-authority CP-ABE scheme. However, there is no obvious way to combine the schemes in [16,23] with the scheme in [25]. More precisely, Chase's scheme can be considered to be an MA-KP-ABE scheme. Additionally, the scheme by Liu *et al.* was created on the composite order groups and proved secure under the hardness of subgroup decision problem. If we extend the scheme by Rouselakis *et al.* [25] to the multi-authority setting in a simple way, it is not sure if the security of the designed scheme can be proved, or it may result in an insecure system that is subjected to the collusion attacks incurred by combining the keys from different authorities.

To prevent such attacks, a valid approach is to associate the user's GID with his keys from different authorities during the key generation stage. In the detailed construction (introduced in Section 5.2), the CA uses an exponent 'c' as the bond to link the GID with the user's keys issued by different AAs. Because of the randomization of the chosen c, the malicious users cannot recover the unauthorized ciphertext by combining their keys. We observe that the users have to gain the partial attribute-keys from the AAs before the link operation. Such process is insecure when some malicious users put their partial attribute-keys together to obtain the final keys, for instance, two malicious users, called Jack and Tom. We assume that $S_{Jack} = \{ATT_1\}$ and $S_{Tom} = \{ATT_2\}$. Normally, Jack should not obtain the keys relevant to the attribute set $\{ATT_1, ATT_2\}$. But, Jack can submit $(UASK_{S_{Jack},GID_{Jack}}, UASK_{S_{Tom},GID_{Tom}})$ to request the final keys, and the CA cannot defend such attack. Our solution is to employ the signature technique, which enables the CA to check whether $UASK_{S,GID,f}$ is really generated by the AA_f for the user with S_{GID}.

Note that, if $K_{4,m}$ is trivially set to be $K'_{4,m}\nu^{-c}$, one can still decrypt the ciphertext by using $K_{4,m}$ and other necessary keys. However, the AA_f may deduce ν^{-c} by computing $K_{4,m}/K'_{4,m}$. It may surmount the CA and generate illegal keys for profit purposes. To resist such attacks, we first choose an extra exponent ψ_m for each attribute. Then we associate ψ_m with the corresponding user's partial attribute-key and obtain $K'^{\psi_m}_{4,m}$. Finally, we link it with ν^{-c}. As a result, we create a provably secure MA-CP-ABE scheme that can efficiently support a fully large attribute universe.

5.2. Our unbounded multi-authority CP-ABE scheme

The detailed construction of our scheme is given as follows:

GlobalSetup $(\lambda)\rightarrow (GPK)$: By taking a security parameter λ as input, this algorithm outputs the group description $(p, \mathbb{G}, \mathbb{G}_1, e)$, where $\mathbb{G}$ and $\mathbb{G}_1$ are two groups of prime order p. $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$

* 'Static' means that the keys of the attributes issued for each GID can be requested only once [16].

DOI: 10.1002/sec

is a bilinear map. g is a generator of group $\mathbb{G}$. It also randomly chooses ω, u, h, and v from $\mathbb{G}$. Furthermore, a strongly existentially unforgeable signature framework $\sum_{sign} = (SigKeyGen, Sign, Verify)$ is employed. The global public parameters is $GPK = (p, \mathbb{G}, \mathbb{G}_1, e; g, \omega, u, h, v, \sum_{sign})$.

CASetup $(GPK) \rightarrow (CPK, CMK)$: The CA chooses a random exponent $\alpha \in \mathbb{Z}_p$ and computes $CPK = e(g,g)^{\alpha}$. $CMK = \alpha$ is kept as the corresponding master secret key.

AASetup $(GPK, f, U_f) \rightarrow (AVK_f, ASIG_f, APK_f, AMK_f)$: Each AA_f runs the SigKeyGen algorithm and outputs a signing–verification key pair $(AVK_f, ASIG_f)$. It then randomly chooses $k_f \in \mathbb{Z}_p$ and sets its public parameter $APK_f = (u^{k_f}, h^{k_f})$. Its master secret key is $AMK_f = k_f$.

Encrypt $(M, \mathbb{A} = (A, \rho), GPK, CPK, \bigcup APK_f) \rightarrow (CT)$: M is the plaintext massage. $\mathbb{A}$ is an access structure expressed by an $\ell \times n$ LSSS matrix A, and ρ maps each row A_x to an descriptive attribute. The encryption algorithm randomly chooses a vector $\overrightarrow{\upsilon} = (s, \upsilon_2, \ldots, \upsilon_n)^{\top} \in \mathbb{Z}_p$. It computes $\overrightarrow{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)^{\top} = A \cdot \overrightarrow{\upsilon}$. Finally, it computes $C = M \cdot e(g,g)^{\alpha \cdot s}$, $C_0 = g^s$, and for each $x \in \{1, 2, \ldots, \ell\}$, the algorithm chooses random exponent $\varsigma_x \in \mathbb{Z}_p$. Then it calculates $C_{x,1} = \omega^{\lambda_x} v^{\varsigma_x}$, $C_{x,2} = (u^{\rho(x)k_f} h^{k_f})^{-\varsigma_x}$, and $C_{x,3} = g^{\varsigma_x}$. The ciphertext is $CT = ((A, \rho), C, C_0, \{C_{x,1}, C_{x,2}, C_{x,3}\}_{x \in [\ell]})$.

AAKeyGen $(S_{GID,f}, GPK, ASIG_f, AMK_f) \rightarrow (UASK_{S,GID,f})$: When a user with GID submits the set $S_{GID,f}$ to AA_f to request the corresponding attribute-keys, AA_f responds as follows:

Firstly, because $S_{GID,f} \subseteq U_f$, for each attribute $ATT_m \in S_{GID,f}$ where $m \in \{1, 2, \ldots, |S_{GID}|\}$, AA_f chooses a random exponent $c_m \in \mathbb{Z}_p$ and computes

$$K'_{3,m} = UASK_{GID,ATT_m,1} = g^{\frac{1}{c_m k_f}}$$

and

$$K'_{4,m} = UASK_{GID,ATT_m,2} = \left(u^{ATT_m} h\right)^{1/c_m}$$

The partial attribute-keys are denoted as

$$UASK_{S,GID,f} = \{K'_{3,m}, K'_{4,m} | ATT_m \in \{1, 2, \ldots, |S_{GID,f}|\}\}$$

Finally, it uses the key $ASIG_f$ to sign on $(ASIG_f, S_{GID,f} \| UASK_{S,GID,f})$ and gets the signature $\sigma_{GID,f}$. Then it gives $(S_{GID,f}, UASK_{S,GID,f}, \sigma_{GID,f})$ to the user.

CAKeyGen $(GID, GPK, CMK, UASK_{S,GID}, \{AVK_f | f \in \mathbb{F}\}) \rightarrow (GCSK_{GID}, GASK_{S,GID})$: After receiving $UASK_{S,GID}$ from a user with his GID, the CA first verifies the validity of $\sigma_{GID,f}$. If not, it aborts. Otherwise, it responds as follows:

It picks a random exponent $c \in \mathbb{Z}_p$. Then, it computes the GID-keys $K_1 = GCSK_{GID,1} = g^{\alpha} \omega^c$ and $K_2 = GCSK_{GID,2} = g^c$.

For each ATT_m, it randomly chooses $\psi_m \in \mathbb{Z}_p$ and computes $K_{3,m} = K'^{\psi_m}_{3,m} = g^{\frac{\psi_m}{c_m k_f}}$ and $K_{4,m} = K'^{\psi_m}_{4,m} \cdot v^{-c} = (u^{ATT_m} h)^{\psi_m / c_m} \cdot v^{-c}$.

Finally, it returns the GID-keys $GCSK_{GID} = (K_1, K_2)$ and the final attribute-keys $GASK_{S,GID} = \{K_{3,m}, K_{4,m}\}_{ATT_m \in S_{GID}}$.

Decrypt $(CT, GPK, GCSK_{GID}, UASK_{S,GID}) \rightarrow (M)$: If S_{GID} is an authorized set, the decryption algorithm denotes the set of rows in the matrix A as $I = \{i : \rho(i) \in S_{GID}\}$. It then calculates such constants $\{\varphi_i \in \mathbb{Z}_p\}_{i \in I}$ satisfying $\sum_{i \in I} \varphi_i \lambda_i = s$. If S_{GID} is an unauthorized set, no such φ_i exists. The algorithm computes

$$B = \frac{e(K_1, C_0)}{\prod_{i \in I} \left(e(K_2, C_{i,1}) e(K_{3,i}, C_{i,2}) e(K_{4,i}, C_{i,3})\right)^{\varphi_i}} = e(g,g)^{\alpha \cdot s}$$

Finally, the algorithm computes $M = C/B$.

6. SECURITY MODEL AND PROOF

In this section, we first describe the security model for our MA-CP-ABE scheme. Then we give the detailed proof of selective security.

6.1. Security model

We now give the security definition of our MA-CP-ABE scheme. Our security model requires the adversary to submit the challenge access matrix $\mathbb{A}^*$ before the initialization phase. Such security model is called selective security model [1]. Moreover, same as the static corruption model in [16–18], the adversary must specify a list of corrupted AAs before seeing the public parameters. In addition, to simplify the previous security model, we assume the keys for each GID can be queried only once in **Phases 1** and **2**.

We assume that the corrupted AAs also run the proposed algorithm in general. Let $\mathbb{F}_c \subseteq \mathbb{F}$ and $\mathbb{F}_{uc} = \mathbb{F} \backslash \mathbb{F}_c$ denote the index set of corrupted and uncorrupted AAs, respectively.

Initialization. The adversary $\mathcal{A}$ specifies the access matrix $\mathbb{A}^*$, which will be challenged in the game. Meanwhile, $\mathcal{A}$ submits a list of corrupted AAs.

Setup. By running the **GlobalSetup**, **CASetup**, and **AASetup** algorithms, the simulator $\mathcal{B}$ generates $GPK, \{ASIG_f, AVK_f | f \in \mathbb{F}\}$, CPK, and $\{APK_f | f \in \mathbb{F}\}$ and sends these public parameters to the adversary $\mathcal{A}$. Additionally, for each corrupted AA_f, $ASIG_f$ and the master secret key AMK_f are given to the adversary.

Phase 1. We note that the secret key queries on S_{GID} must be executed under the restriction that S_{GID} cannot satisfy the challenge access matrix $\mathbb{A}^*$. The adversary can query $UCSK_{GID}$ and $GASK_{S,GID}$ for (GID, S_{GID}) by the following:

$AKQ(S_{GID})$: For $f \in \mathbb{F}_c$, the adversary can make $UASK_{S,GID,f}$ itself. Otherwise, the simulator returns $UASK_{S,GID,f}$ to the adversary.

$CKQ(GID)$: After receiving $UASK_{S,GID}$, the simulator first verifies the validity of $UASK_{S,GID}$. If so, it returns $GCSK_{GID}$ and $GASK_{S,GID}$. Otherwise, it aborts.

Challenge phase. The adversary $\mathcal{A}$ declares two equal-length messages M_0 and M_1. $\mathcal{B}$ first flips a random coin $b \in \{0, 1\}$. It then encrypts M_b under $\mathbb{A}^*$ and transmits the ciphertext CT^* to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ requests the keys as in **Phase 1**.

Guess. $\mathcal{A}$ outputs its guess b' on b.

The advantage of $\mathcal{A}$ is $| Pr[b' = b] - 1/2 |$.

Definition 4. *An MA-CP-ABE scheme is selectively secure if the advantage of all PPT adversaries is negligible in the previous game.*

6.2. The proof of selective security

We prove the security of the proposed MA-CP-ABE scheme by the following theorem.

Theorem 1. *Suppose that the z-type assumption holds and the signature scheme $\sum_{sign}$ is existentially unforgeable. Then no PPT adversary $\mathcal{A}$ with a $\ell \times n(\ell, n < z)$ challenge access matrix can selectively break our MA-CP-ABE system with a non-negligible advantage.*

Proof. In order to prove this theorem, we assume that there exists an adversary $\mathcal{A}$, which can selectively break our MA-CP-ABE scheme with a non-negligible advantage ϵ. By employing $\mathcal{A}$, we can create a PPT simulator $\mathcal{B}$ that can break the assumption with advantage $\frac{1}{2}\epsilon$.

The challenger* sets the groups $(p, \mathbb{G}, \mathbb{G}_1, e)$ and sends the tuple T to the simulator $\mathcal{B}$. In the challenge stage, the challenger flips an unbiased coin $o \in \{0, 1\}$. If $o = 0$, it passes $W = e(g, g)^{d^{z+1}s}$ to $\mathcal{B}$. Otherwise, it transmits $W = R$ to $\mathcal{B}$. Finally, $\mathcal{B}$ needs to output its guess o' on o. Now, we show how the simulator plays the security game with the adversary $\mathcal{A}$.

Initialization: The simulator $\mathcal{B}$ is given the terms of the z-type assumption and receives a challenge access policy $\mathbb{A}^*(A^*, \rho)$ from $\mathcal{A}$. Meanwhile, $\mathcal{A}$ has to specify a list of corrupt AAs. Without loss of generality, $\mathcal{A}$ is assumed to corrupt all AAs.

Setup. To set the public parameters, the simulator acts as follows:

GlobalSetup. The simulator borrows the terms from the assumption and sets $g = g$ and $\omega = g^d$.

$$v = g^{v'} \cdot \prod_{(j,k)\in[\ell,n]} \left(g^{d^k/t_j}\right)^{A^*_{j,k}}$$

$$u = g^{u'} \cdot \prod_{(j,k)\in[\ell,n]} \left(g^{d^k/t_j^2}\right)^{A^*_{j,k}}$$

$$h = g^{h'} \cdot \prod_{(j,k)\in[\ell,n]} \left(g^{d^k/t_j^2}\right)^{-\rho(j)A^*_{j,k}}$$

Simultaneously, a signature scheme $\sum_{sign}$ is also employed.

CASetup. $\mathcal{B}$ randomly picks an exponent $\alpha' \in \mathbb{Z}_p$. It sets $CAMSK = \alpha = d^{z+1} + \alpha'$. CPK is calculated by $e(g, g)^{\alpha} = e(g, g)^{\alpha'} \cdot e(g^d, g^{d^z})$.

AASetup. For each AA_f, $\mathcal{B}$ randomly selects $AMK_f = k_f \in \mathbb{Z}_p$ and sets AVK_f, $ASIG_f$, and APK_f as in Section 4.

Finally, besides the system public parameters, $\mathcal{B}$ gives $\{AMK_f | f \in \mathbb{F}\}$ to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ now makes the private key queries on pairs (GID, S_{GID}) in the following way:

$AKQ(S_{GID})$: For $f \in \mathbb{F}$, the adversary can make $UASK_{S,GID,f}$ and $\sigma_{GID,f}$ itself.

$CKQ(GID)$: After receiving GID, S_{GID}, $UASK_{S,GID}$, and $\sigma_{GID,f}$ from the adversary. The simulator first verifies the validity of $\sigma_{GID,f}$. If not, it aborts. Otherwise, it responds as follows:

Because the set S_{GID} does not satisfy $\mathbb{A}^*(A^*, \rho)$, there must be a vector $\overrightarrow{\varphi} = (\varphi_1, \varphi_2, \ldots, \varphi_n)^\top \in \mathbb{Z}_p^n$ such that $\varphi_1 = -1$ and $\langle A_i^*, \overrightarrow{\varphi} \rangle = 0$ for all $i \in I = \{i | \rho(i) \in S_{GID} \bigwedge i \in [\ell]\}$. $\mathcal{B}$ can compute $\overrightarrow{\varphi}$ by employing linear algebra. It then randomly selects $c' \in \mathbb{Z}_p$ and sets

$$\begin{aligned} c &= c' + \varphi_1 d^z + \varphi_2 d^{z-1} + \ldots + \varphi_n d^{z+1-n} \\ &= c' + \sum_{i\in[n]} \varphi_i d^{z+1-i} \end{aligned}$$

Then the GID central-keys are computed as

$$\begin{aligned} K_1 &= g^{\alpha}\omega^c \\ &= g^{d^{z+1}+\alpha'} \cdot g^{dc'} \prod_{i\in[n]} g^{\varphi_i d^{z+2-i}} \\ &= g^{\alpha'} g^{dc'} \prod_{i=2}^{n} \left(g^{d^{z+2-i}}\right)^{\varphi_i} \end{aligned}$$

$$K_2 = g^c = g^{c'} \prod_{i\in[n]} \left(g^{d^{z+1-i}}\right)^{\varphi_i}$$

* We note that the challenger that tries to break the assumption can also be the simulator that interacts with the adversary in the security game.

The simulator then computes

$$\begin{aligned}
\nu^c &= \nu^{c'} \cdot \left(g^{\nu'} \prod_{(j,k)\in[\ell,n]} g^{A^*_{j,k} d^k / t_j} \right)^{\sum_{i\in[n]} \varphi_i d^{z+1-i}} \\
&= \nu^{c'} \cdot \prod_{i\in[n]} \left(g^{d^{z+1-i}} \right)^{\nu' \varphi_i} \\
&\quad \cdot \prod_{(i,j,k)\in[n,\ell,n]} \left(g^{d^{z+1+k-i}/t_j} \right)^{\varphi_i A^*_{j,k}} \\
&= \Delta \cdot \prod_{(i,j)\in[n,\ell]} g^{\varphi_i A^*_{j,k} d^{z+1}/t_j} \\
&= \Delta \cdot \prod_{j\in[\ell]} g^{\left\langle \overrightarrow{\varphi}, A^*_j \right\rangle d^{z+1}/t_j} \\
&= \Delta \cdot \prod_{\substack{j\in[\ell], \\ \rho(j)\notin S_{GID}}} g^{\left\langle \overrightarrow{\varphi}, A^*_j \right\rangle d^{z+1}/t_j}
\end{aligned}$$

where

$$\begin{aligned}
\Delta = \nu^{c'} &\cdot \prod_{i\in[n]} \left(g^{d^{z+1-i}} \right)^{\nu' \varphi_i} \\
&\cdot \prod_{\substack{(i,j,k)\in[n,\ell,n], \\ i\neq k}} \left(g^{d^{z+1+k-i}/t_j} \right)^{\varphi_i A^*_{j,k}}
\end{aligned}$$

Remark that $\prod_{\substack{j\in[\ell], \\ \rho(j)\notin S_{GID}}} g^{\langle \overrightarrow{\varphi}, A^*_j \rangle d^{z+1}/t_j}$ cannot be computed while Δ can be correctly calculated by suitable elements from the assumption. That is, the simulator has to provide a "cancel" between ν^{-c} and $(u^{ATT_m} h)^{1/c_m}$ for each $ATT_m \in S_{GID}$.

For each $ATT_m \in S_{GID}$, $\mathcal{B}$ randomly chooses $\psi_{m,1} \in \mathbb{Z}_p$ and sets $\psi_m = c_m \psi'_m$ where

$$\begin{aligned}
\psi'_m &= \psi_{m,1} + c \cdot \sum_{\substack{i'\in[\ell], \\ \rho(i')\notin S_{GID}}} \frac{t_{i'}}{ATT_m - \rho(i')} \\
&= \psi_{m,1} + c' \cdot \sum_{\substack{i'\in[\ell], \\ \rho(i')\notin S_{GID}}} \frac{t_{i'}}{ATT_m - \rho(i')} \\
&\quad + \sum_{\substack{(i,i')\in[n,\ell], \\ \rho(i')\notin S_{GID}}} \frac{\varphi_i t_{i'} d^{z+1-i}}{ATT_m - \rho(i')}
\end{aligned}$$

Then, the simulator can compute

$$\begin{aligned}
K_{3,m} &= g^{\frac{\psi_m}{c_m k_f}} \\
&= g^{\psi_{m,1}/k_f} \\
&\quad \cdot \prod_{\substack{i'\in[\ell], \\ \rho(i')\notin S_{GID}}} \left(g^{t_{i'}} \right)^{c'/k_f (ATT_m - \rho(i'))} \\
&\quad \cdot \prod_{\substack{(i',i)\in[\ell,n], \\ \rho(i')\notin S_{GID}}} \left(g^{t_{i'} d^{z+1-i}} \right)^{\varphi_i / k_f (ATT_m - \rho(i'))}
\end{aligned}$$

$$\begin{aligned}
K_{4,m} &= \left(u^{ATT_m} h \right)^{\psi_m / c_m} \nu^{-c} \\
&= \nu^{-c} \cdot \left(u^{ATT_m} h \right)^{c'_m} \\
&\quad \cdot \left(K^{k_f,2}_{4,m} / g^{\psi_{m,1}} \right)^{u' ATT_m + h'} \\
&\quad \cdot \prod_{\substack{(i',j,k)\in[\ell,\ell,n], \\ \rho(i')\notin S_{GID}}} \left(g^{t_{i'} d^k / t_j^2} \right)^{y_3} \\
&\quad \cdot \prod_{\substack{(i',j,i,k)\in[\ell,\ell,n,n], \\ \rho(i')\notin S_{GID}}} \left(g^{t_{i'} d^{z+1+k-i}/t_j^2} \right)^{y_4} \\
&= \nu^{-c} \cdot \Upsilon \cdot \prod_{\substack{(j,i)\in[\ell,n], \\ \rho(j)\notin S_{GID}}} \left(g^{t_j d^{z+1+i-i}/t_j^2} \right)^{\alpha_i A^*_{j,k}} \\
&= \Upsilon \cdot \Delta \cdot \prod_{\substack{(j)\in[\ell], \\ \rho(j)\notin S_{GID}}} g^{\left\langle \overrightarrow{\varphi}, A^*_j \right\rangle d^{z+1}/t_j} \\
&\quad \cdot \prod_{\substack{(j)\in[\ell], \\ \rho(j)\notin S_{GID}}} g^{-\left\langle \overrightarrow{\varphi}, A^*_j \right\rangle d^{z+1}/t_j} \\
&= \Upsilon \cdot \Delta
\end{aligned}$$

where

$$y_1 = c' \cdot \sum_{\substack{i'\in[\ell], \\ \rho(i')\notin S_{GID}}} \frac{t_{i'}}{ATT_m - \rho(i')}$$

$$y_2 = \sum_{\substack{(i,i')\in[n,\ell], \\ \rho(i')\notin S_{GID}}} \frac{\varphi_i t_{i'} d^{z+1-i}}{ATT_m - \rho(i')}$$

$$y_3 = c' A^*_{j,k} \frac{ATT_m - \rho(j)}{ATT_m - \rho(i')}$$

$$y_4 = \varphi_i A^*_{j,k} \frac{ATT_m - \rho(j)}{ATT_m - \rho(i')}$$

and

$$\Upsilon = (u^{ATT_m}h)^{\psi_{m,1}} \cdot \left(K_{4,m}/g^{\psi_{m,1}}\right)^{u'ATT_m+h'} \cdot \prod_{\substack{(i',j,k)\in[\ell,\ell,n],\\ \rho(i')\notin S_{GID}}} \left(g^{t_{i'}d^k/t_j^2}\right)^{y_3} \cdot \prod_{\substack{(i',j,i,k)\in[\ell,\ell,n,n],\\ \rho(i')\notin S_{GID},\\ (i'\neq j\vee i\neq k)}} \left(g^{t_{i'}d^{z+1+k-i}/t_j^2}\right)^{y_4}$$

Finally, $\mathcal{B}$ transmits $UCSK_{GID}$ and $GASK_{S,GID}$ to the adversary.

Challenge. $\mathcal{A}$ submits two same-length messages M_0 and M_1 to the simulator. $\mathcal{B}$ chooses a random value $b \in \{0,1\}$ and calculates

$$C = M_b \cdot W \cdot e(g^s, g)^{\alpha'}, C_0 = g^s$$

The simulator then selects random exponents $\upsilon_2, \ldots, \upsilon_n \in \mathbb{Z}_p$ and sets $\overrightarrow{\upsilon} = (s, sd + \upsilon_2, sd^2 + \upsilon_3, \ldots, sd^{n-1} + \upsilon_n)^\top$. For each $x \in [\ell]$, we have

$$\lambda_x = \sum_{i\in[n]} A^*_{x,i} sd^{i-1} + \sum_{i=2}^{n} A^*_{x,i}\upsilon_i = \sum_{i\in[n]} A^*_{x,i} sd^{i-1} + \lambda'_x$$

For each $x \in [\ell]$, $\mathcal{B}$ sets $\varsigma_x = -st_x$. If $\rho(x) \in U_f$, it computes

$$\begin{aligned} C_{x,1} &= \omega^{\lambda_x}\nu^{\varsigma_x} \\ &= \omega^{\lambda'_x} \cdot \prod_{i\in[n]} g^{A_{x,i}sd^i} \cdot \left(g^{st_x}\right)^{-\nu'} \cdot \prod_{(j,k)\in[\ell,n]} g^{-A'_{j,k}d^k st_x/t_j} \\ &= \omega^{\lambda'_x} \cdot \left(g^{st_x}\right)^{-\nu'} \cdot \prod_{i\in[n]} g^{A_{x,i}sd^i} \cdot \prod_{k\in[n]} g^{-A_{x,i}sd^k t_x/t_x} \cdot \prod_{\substack{(j,k)\in[\ell,n],\\ j\neq x}} g^{-A'_{j,k}d^k st_x/t_j} \\ &= \omega^{\lambda'_x} \cdot \left(g^{st_x}\right)^{-\nu'} \cdot \prod_{\substack{(j,k)\in[\ell,n],\\ j\neq x}} g^{-A'_{j,k}d^k st_x/t_j} \end{aligned}$$

$$\begin{aligned} C_{x,2} &= \left(u^{\rho(x)}h\right)^{-k_f\varsigma_x} \\ &= \left(g^{st_x}\right)^{k_f(u'\rho(x)+h')} \cdot \left(\prod_{(j,k)\in[\ell,n]} g^{A'_{j,k}(\rho(x)-\rho(j))d^k/t_j^2}\right)^{k_f st_x} \\ &= \left(g^{sb_x}\right)^{k_f(u'\rho(x)+h')} \cdot \prod_{\substack{(j,k)\in[\ell,n],\\ j\neq x}} \left(g^{sd^k t_x/t_j^2}\right)^{k_f A'_{j,k}(\rho(x)-\rho(j))} \end{aligned}$$

$$C_{x,3} = g^{\varsigma_x} = \left(g^{st_x}\right)^{-1}$$

Finally, $\mathcal{B}$ gives the challenge ciphertext $CT = ((A^*, \rho), C, C_0, \{C_{x,1}, C_{x,2}, C_{x,3}\}_{x\in[\ell]})$ to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ acts same as in **Phase 1**.

Guess. In this phase, $\mathcal{A}$ has to output its guess b' on b. If $b' = b$, the simulator guesses $o' = 0$. Otherwise, it guesses $o' = 1$.

We now calculate the advantage of the challenger in breaking the z-type assumption.

If $o = 0$, we can see that the challenge ciphertext of M_b is correctly computed. The advantage of the adversary is ϵ. Thus, we have $Pr[b' = b|o = 0] = \frac{1}{2} + \epsilon$. Because $\mathcal{B}$ outputs $o' = 0$ when $b' = b$, we have $Pr[o' = o|o = 0] = \frac{1}{2} + \epsilon$.

If $o = 1$, $\mathcal{A}$ obtains no useful information. Thereby, we have $Pr[b' \neq b|o = 1] = \frac{1}{2}$. Because the guess of $\mathcal{B}$ is $o' = 1$ when $b' \neq b$, we have $Pr[o' = o|o = 1] = \frac{1}{2}$.

As a result, the overall advantage of the challenger in breaking the z-type assumption is $\frac{1}{2}Pr[o' = o|o = 0] + \frac{1}{2}Pr[o' = o|o = 1] - \frac{1}{2} = \frac{1}{2}\epsilon$. □

7. CHARACTERISTIC AND PERFORMANCE ANALYSIS

In this section, we give the characteristics comparison and performance analysis between some relevant systems and ours.

7.1. Characteristics comparison

In Table II, we compare the characteristics between the current works and ours in terms of the ABE form, multi-authority support, security level, group order, and the type of attribute universe. From Table II, we can easily find that our MA-CP-ABE scheme is the only CP-ABE scheme who can support multiple authorities and unbounded attribute universe simultaneously, while the other schemes are limited to either single authority or restricted attribute universe.

DOI: 10.1002/sec

Table II. A comparison between relevant attribute-based encryption schemes and ours.

Schemes	KP/CP	Multiple authorities	Security	Group order	Attribute universe
[16,17]	KP	Yes	Selective	Prime	Semi-large
[18]	CP	Yes	Adaptive	Composite	Small
[23]	CP	Yes	Adaptive	Composite	Semi-large
[24]	KP	No	Selective	Composite	Fully large
[25]	CP	No	Selective	Prime	Fully large
Ours	CP	Yes	Selective	Prime	Fully large

KP, key-policy; CP, ciphertext-policy.

Table III. The comparison of parameter size of ciphertext-policy attribute-based encryption schemes.

Schemes	Rouselakis's [25]	Lewko's [18]	Liu's [23]	Ours
Size of PK	$5\|\mathbb{G}\| + 1\|\mathbb{G}_1\|$	$\|U\|\|\mathbb{G}\| + \|U\|\|\mathbb{G}_1\|$	$(\|U\| + 3)\|\mathbb{G}\| + Y\|\mathbb{G}_1\|$	$1\|\mathbb{G}_1\| + (2F + 5)\|\mathbb{G}\|$
Ciphertext size	$(3\ell + 1)\|\mathbb{G}\| + 1\|\mathbb{G}_1\|$	$2\ell\|\mathbb{G}\| + (\ell + 1)\|\mathbb{G}_1\|$	$(2\ell + 1)\|\mathbb{G}\| + 1\|\mathbb{G}_1\|$	$(3\ell + 1)\|\mathbb{G}\| + 1\|\mathbb{G}_1\|$
Private key size	$(2\|S\| + 2)\|\mathbb{G}\|$	$\|S\|\|\mathbb{G}\|$	$(\|S\| + 2Y)\|\mathbb{G}\|$	$(2\|S\| + 2)\|\mathbb{G}\|$

Table IV. Computation cost comparison.

Schemes	Rouselakis's [25]	Lewko's [18]	Liu's [23]	Ours
System setup	$1E_1 + 1P$	$\|U\|(E + E_1) + 1P$	$(\|U\| + YF)E$ $YE_1 + 1P$	$2FE + 1E_1 + 1P$
KeyGen	$(3\|S\| + 4)E$	$2\|S\|E$	$(3Y + YF + Y\|S\|)E$ $+2\|I_K\|YP$	$(5\|S\| + 4)E$
Encryption	$(5\ell + 1)E + 1E_1$	$3\ell E + (2\ell + 1)E_1$	$(3\ell + 1)E + YE_1$	$(5\ell + 1)E + 1E_1$
Decryption	$\|I\|E_1 + (3\|I\| + 1)P$	$\|I\|E_1 + 2\|I\|P$	$\|I\|E_1 + (2\|I\| + 1)P$	$\|I\|E_1 + (3\|I\| + 1)P$

7.2. Performance analysis

Here we analyze the performance between the systems [18,23,25] and ours, in terms of the size of parameter and the computation cost in each stage. Let $|\mathbb{G}|$ and $|\mathbb{G}_1|$ be the bit length of the element in $\mathbb{G}$ and $\mathbb{G}_1$, respectively. We let ℓ denote the amount of rows in the matrix A and S denote the set of attributes possessed by a user. Let Y and F be the total number of CAs and AAs, respectively. I denotes the set of attributes used in decryption; U denotes the total attribute domain. We denote I_K as the index set of AAs related to S. Let P be one pairing operation. We denote E and E_1 as one exponential operation in $\mathbb{G}$ and $\mathbb{G}_1$, respectively.

Table III compares the size of parameters in the systems in [18,23,25] and ours, in terms of the bit length of elements in public parameters (PK), ciphertexts, and private keys. More precisely, the size of PK and keys are calculated in terms of the amount of elements that will be employed in encryption and decryption, respectively. For our scheme, $UASK_{S,GID}$ that is used to generate the final attribute-key is not calculated in the size of private keys. The total size of $UASK_{S,GID}$ is $2|S||\mathbb{G}|$. The parameter size in the scheme in [23] is gathered from the basic construction. For the semi-large attribute universe construction, the size of PK is $(\sum_{f=1}^{F}(n_f + 1) + 3)|\mathbb{G}| + Y|\mathbb{G}_1|$, where n_f denotes the restriction value of attributes applied in encryption. From Table III, we can find that the size of PK in the schemes in [18,23] goes linearly with the size of the attribute universe $|U|$. On the contrary, the size of PK in Rouselakis's scheme and ours is unrelated to $|U|$. Compared with Rouselakis's scheme, although the PK in our scheme requires $2F$ more elements, the size of ciphertexts and private keys remains the same. Because the number of AAs is much less than $|U|$, such increment is acceptable.

Table IV compares the computation cost between the systems in [18,23,25] and ours, in terms of the times of pairing and exponent operations executed during each stage of the scheme. From Table IV, we can see that our MA-CP-ABE scheme requires a bit more exponent operations in the system setup and key generation phase than Rouselakis's scheme. In the encryption and decryption stage, the computation overhead in Rouselakis's scheme and our scheme is the same. We note that the systems in [18,23] were constructed on composite order groups, where the computation overhead may take more resources than that on prime order groups.

From the previous performance analysis, it is easy to see that our system has almost the same efficiency as the basic single-authority CP-ABE scheme [25]. Furthermore, unlike the other multi-authority ABE schemes, we achieve the first fully large universe MA-CP-ABE construction, while the other systems are limited to various restrictions.

8. CONCLUSION

In this paper, we proposed an unbounded MA-CP-ABE scheme, with no needless restriction on the public parameters. In this system, one CA and multiple AAs exist. The AAs are not required to interact with each other and are in charge of generating partial attribute-keys for users. The CA generates identity-keys for users and links each user's partial attribute-keys with his/her GID. Our proposed scheme is proved selectively secure under the standard model and can support any monotone LSSS access policy. While the proposed scheme is created over prime order groups, it is efficient in comparison with those ABE schemes constructed on composite order groups.

ACKNOWLEDGEMENTS

This work is supported by PCSIRT IRT1078; NSFC nos. 61370078, 61402109, and 61202389; the key program of NSFC-Guangdong Union Foundation under grant no. U1135002; major national S&T program under grant no. 2011ZX03005-002; NUPTSF (Grant No.NY215008); and the Fundamental Research Funds for the Central Universities under no. JB142001-12. We thank the referees for helpful comments.

REFERENCES

1. Sahai A, Waters B. Fuzzy identity-based encryption, *Advances in Cryptology–EUROCRYPT 2005*, Aarhus, Denmark, 2005; 457–473.
2. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data, *Proceedings of the 13th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, 2006; 89–98.
3. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption, *Security and Privacy, 2007. SP'07. IEEE Symposium on*, Oakland, California, USA, 2007; 321–334.
4. Attrapadung N, Libert B, De Panafieu E. Expressive key-policy attribute-based encryption with constant-size ciphertexts, *Public Key Cryptography–PKC 2011*, Taormina, Italy, 2011; 90–108.
5. Cheung L, Newport C. Provably secure ciphertext policy ABE, *Proceedings of the 14th ACM Conference on Computer and Communications Security*, Alexandria, VA, USA, 2007; 456–465.
6. Goyal V, Jain A, Pandey O, Sahai A. Bounded ciphertext policy attribute based encryption, *Automata, Languages and Programming-ICALP 2008*, Reykjavik, Iceland, 2008; 579–591.
7. Lewko A, Okamoto T, Sahai A, Takashima K, Waters B. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption, *Advances in Cryptology–EUROCRYPT 2010*, French Riviera, 2010; 62–91.
8. Waters B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions, *Advances in Cryptology-CRYPTO 2009*, Santa Barbara, California, USA, 2009; 619–636.
9. Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization, *Public Key Cryptography–PKC 2011*, Taormina, Italy, 2011; 53–70.
10. Lewko A. Tools for simulating features of composite order bilinear groups in the prime order setting, *Advances in Cryptology-EUROCRYPT 2012*, Cambridge, UK, 2012; 318–335.
11. Yu S, Wang C, Ren K, Lou W. Attribute based data sharing with attribute revocation, *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, Beijing, China, 2010; 261–270.
12. Hur J, Noh DK. Attribute-based access control with efficient revocation in data outsourcing systems. *Parallel and Distributed Systems, IEEE Transactions on* 2011; **22**(7): 1214–1221.
13. Wan Z, Liu J, Deng RH. Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *Information Forensics and Security, IEEE Transactions on* 2012; **7** (2): 743–754.
14. Hur J, Noh DK. Attribute-based access control with efficient revocation in data outsourcing systems. *Parallel and Distributed Systems, IEEE Transactions on* 2011; **22**(7): 1214–1221.
15. Hur J, Park C, Hwang SO. Fine-grained user access control in ciphertext-policy attribute-based encryption. *Security and Communication Networks* 2012; **5**(3): 253–261.
16. Chase M. Multi-authority attribute based encryption, *Proceedings of the 4th Conference on Theory of Cryptography*, Amsterdam, The Netherlands, 2007; 515–534.
17. Chase M, Chow S. Improving privacy and security in multi-authority attribute-based encryption, *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, Illinois, USA, 2009; 121–130.
18. Lewko A, Waters B. Decentralizing attribute-based encryption, *Advances in Cryptology–EUROCRYPT 2011*, Tallinn, Estonia, 2011; 568–588.
19. Li J, Huang Q, Chen X, Chow SSM, Wong DS, Xie D. Multi-authority ciphertext-policy attribute-based encryption with accountability, *Proceedings of the 6th ACM Symposium on Information, Computer and*

Communications Security, Hong Kong, China, 2011; 386–390.
20. Müller S, Katzenbeisser S, Eckert C. Distributed attribute-based encryption, *Information Security and Cryptology–ICISC 2008*, Springer, Berlin Heidelberg, 2009; 20–36.
21. Müller S, Katzenbeisser S, Eckert C. On multi-authority ciphertext-policy attribute-based encryption. *Bulletin of the Korean Mathematical Society* 2009; **46**(4): 803–819.
22. Lin H, Cao Z, Liang X, Shao J. Secure threshold multi authority attribute based encryption without a central authority, *Progress in Cryptology-INDOCRYPT 2008*, Kharagpur, India, 2008; 426–436.
23. Liu Z, Cao Z, Huang Q, Wong D, Yuen T. Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles, *Computer Security–ESORICS 2011*, Leuven, Belgium, 2011; 278–297.
24. Lewko A, Waters B. Unbounded HIBE and attribute-based encryption, *Advances in Cryptology-EUROCRYPT 2011*, Tallinn, Estonia, 2011; 547–567.
25. Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13*, Berlin, Germany, 2013; 463-474.
26. Li Q, Ma J, Li R, Xiong J, Liu X. Large universe decentralized key-policy attribute-based encryption. *Security and Communication Networks* 2014; **8** (3): 501–509.
27. Shamir A. Identity-based cryptosystems and signature schemes, *Advances in cryptology-CRYPTO 1984*, Santa Barbara, California, USA, 1985; 47–53.
28. Boneh D, Franklin M. Identity-based encryption from the weil pairing, *Advances in Cryptology–CRYPTO 2001*, Santa Barbara, California, USA, 2001; 213–229.
29. Cocks C. An identity based encryption scheme based on quadratic residues, *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, Cirencester, UK, 2001; 360–363.
30. Canetti R, Halevi S, Katz J. A forward-secure public-key encryption scheme, *Advances in Cryptology–Eurocrypt 2003*, Warsaw, Poland, 2003; 255–271.
31. Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption, *Advances in Cryptology–Eurocrypt 2004*, Interlaken, Switzerland, 2004; 207–222.
32. Boneh D, Boyen X. Efficient selective-id secure identity-based encryption without random oracles, *Advances in Cryptology-EUROCRYPT 2004*, Interlaken, Switzerland, 2004; 223–238.
33. Beimel A. Secure schemes for secret sharing and key distribution. *PhD thesis, Israel Institute of Technology*, Technion, Haifa, Israel, 1996.