Accountable Multi-authority Ciphertext-Policy Attribute-Based Encryption Without Key Escrow and Key Abuse

Gang Yu[1,2(✉)], Xiaoxiao Ma[3(✉)], Zhenfu Cao[2(✉)], Weihua Zhu[1], and Junjie Zeng[1]

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Science and Technology Institute, Zhengzhou 450001, China
gyu1010@126.com, weihua1_2001@163.com, zengjj_lab@163.com

[2] Shanghai Key Lab for Trustworthy Computing, East China Normal University, Shanghai 200062, China
zfcao@sei.ecnu.edu.cn

[3] Zheng Zhou Vocational University of Information and Technology, Zhengzhou 450046, China
mxx1010@126.com

Abstract. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising public key encryption primitive enabling fine-grained access control on shared data in public cloud. However, two quite challenging issues, the prevention of key escrow and key abuse, still exist in CP-ABE system. In this paper, we propose a multi-authority CP-ABE scheme without key escrow and key abuse. To prevent key escrow, multiple authorities are employed to perform the same procedure of key generation for an attribute. Thus, no individual authority or colluded authorities that manage no common attribute can decrypt any ciphertext, and it can also resist collusion attack from curious authority with the help of dishonest users. To prevent key abuse of dishonest users, user's global identifier along with a signature is embedded into the secret key. Thus, any third party can learn the identity from a shared secret key and publicly verify its validity. An advantage of simultaneously preventing key escrow and key abuse is that the proposed scheme can achieve accountability, i.e. an auditor can publicly audit a user or authorities abuse the secret key. At last, the proposed scheme is fully secure in the random oracle model, and due to a key aggregate algorithm its efficiency is comparable to the decentralizing CP-ABE scheme [18] on which it is based.

Keywords: Attribute-based encryption · Multi-authority · Key escrow · Key abuse · Traceability · Accountability

© Springer International Publishing AG 2017
S. Wen et al. (Eds.): CSS 2017, LNCS 10581, pp. 337–351, 2017.
https://doi.org/10.1007/978-3-319-69471-9_25

1 Introduction

With the rapid development of cloud computing and Internet, more and more enterprises and individuals are willing to outsource data or applications to cloud storage servers to enjoy scalable services on-demand. Although cloud storage provides an ease of accessibility, it also raises concerns about data security and access control.

Attribute-based encryption (ABE) is a promising one-to-many encryption primitive with fine-grained access control. It usually has two classifications: key policy attribute-based encryption (KP-ABE) and ciphertext policy attribute-based encryption (CP-ABE). In CP-ABE, attributes of a user are specified in the secret key and access policy defined over some attributes is assigned in the ciphertext. In KP-ABE, the situation is reversed.

In CP-ABE access control system, a user can decrypt a ciphertext if and only if his/her attributes satisfy the access policy specified by the ciphertext, and the secret key is defined over a set of attributes that may be owned by multiple users. No user-specific information is specified in secret keys and ciphertexts. Thus, the secret keys are non-traceable, i.e. given a secret key it is hard to find out its owner due to the fact that the secret key may belong to multiple users. Consequently, a dishonest user dares to share its secret key among users without any risk of being caught.

In a single authority ABE system, all the secret keys are issued by the authority. The authority is able to generate and (re-)distribute secret keys associated with arbitrary set of attributes to unauthorized users without being detected. Even worse, the authority can illegally decrypt arbitrary ciphertext directly using its master key.

Thus, there are two challenging issues: (1) illegal key sharing among users and illegal key distribution by the authority (also called the key abuse problem) (2) illegal ciphertext decryption by the authority (also called the key escrow problem). To securely deploy an ABE access control system, both the misbehavior of dishonest users and curious authority should be prevented.

1.1 Related Works

Sahai and Waters [1] introduced the notion of ABE, and since then many ABE schemes [2–13] have been proposed aiming at better expressiveness, efficiency or security. These schemes [2–13] are single authority ABE that assume there is a central authority who issues secret keys for all users. However, in some applications, data owner may want to share data according to a policy written over attributes issued across different trust domains. A single-authority ABE system will not be appropriate in this scenario.

Multi-authority ABE helps alleviate the extent of trust on authority. In a single authority ABE system [1–13], the authority can directly decrypt all the ciphertexts. In multi-authority ABE schemes [14,15], a central authority can decrypt all ciphertexts. Schemes [16–18,20–24] do not require such a central

authority, and no individual authority can decrypt all ciphertexts, but individual authority can decrypt ciphertexts that the associated access policy can be satisfied by attributes that under its domain. To prevent individual authority from decrypting any ciphertext, scheme [19] introduced multiple central authorities (CAs) besides multiple attribute authorities (AAs). However, in the scheme [19] AA should register itself to the CAs which will need troublesome authenticated interaction and it cannot resist collusion attack from dishonest user and AA, i.e. with the help of a corrupted user AA can decrypt all cipher-texts that the associated access policy can be satisfied by attributes under its domain. In 2015, Zhang et al. [25] proposed a two-authority ABE scheme without key escrow where neither of the two authorities can decrypt the ciphertext even with the help of corrupted users. However, one of the two authorities in [25] manages all attributes, and so the scheme [25] is not suitable for applications across different trust domains.

To prevent illegal key sharing among users, Li et al. [26] gave an accountable ABE supporting AND gate with wildcards access policy. For a better expressiveness, Ning et al. [27] gave a white-box traceable CP-ABE supporting flexible attributes. But scheme [27] can't achieve accountability because nobody can prove whether a leaked key is shared by a malicious user or illegally generated by the authority. In 2015, Ning et al. [28] proposed an accountable ABE with white-box traceability and public auditing. However, schemes [26,28] can't resist key escrow.

1.2 Our Technique

To solve the key escrow problem in CP-ABE system, multiple authorities are employed to reduce the degree of trust. Concretely, different authorities that have different master keys perform the same procedure of key generation for an attribute. As illustrated in Fig. 1, there are n authority sets in the system, denoted by $\mathbb{A}_1, \mathbb{A}_2, ..., \mathbb{A}_n$. Each authority $A_{i,j} \in \mathbb{A}_i$ manages a different domain of attributes, and all the authorities $A_{i,j}$ in set $\mathbb{A}_i$ manage the attribute universe $\mathbb{U}$. Let $\mathcal{T}_i : \mathbb{U} \to \mathbb{A}_i, i = 1, ..., n$ be maps from an attribute $at \in \mathbb{U}$ to an

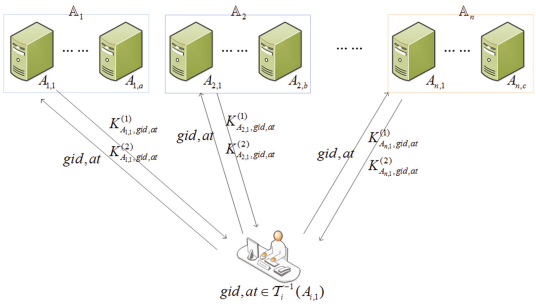

Fig. 1. Process of key generation in MCP-AABE

authority $A_{i,j} \in \mathbb{A}_i$. Let $\mathcal{T}_i^{-1}(A_{i,j}) = \{at \in \mathbb{U} : \mathcal{T}_i(at) = A_{i,j}\}$, then there is $\bigcup_{A_{i,j} \in \mathbb{A}_i} \mathcal{T}_i^{-1}(A_{i,j}) = \mathbb{U}$. When a user with identity gid and attribute set $S \in \mathbb{U}$ joins the system, for each attribute $at \in S$ the user submits the identity gid and attribute at to authorities $A_{i,j} \in \mathbb{A}_i, i = 1, ..., n$, where $\mathcal{T}_i(at) = A_{i,j}$ (takes $A_{i,1}, i = 1, ..., n$ for example in Fig. 1). For $i = 1, ..., n$, $A_{i,1}$ verifies the correctness of gid, at, and generates the corresponding secret key $K_{A_{i,1},gid,at}, i = 1, ..., n$ for user.

To improve efficiency, each authority independently issue secret key for users and no coordination between authorities is required. Secondly, to decrease the size of secret key, a simple key aggregate algorithm is proposed and each user can aggregate the received n secret keys from n different authorities into one aggregate secret key.

1.3 Our Contributions

This paper deals with both the key escrow and key abuse issues in CP-ABE system, and we propose an accountable multi-authority CP-ABE without key escrow and key abuse, denoted by MCP-AABE. The main features of the proposed MCP-AABE scheme can be summarized as follows.

- **High efficiency:** Although there are n attribute authority sets, each authority can independently issue secret keys for users, and no global coordination other than the generation of an initial set of common reference parameters is required. Due to a key aggregate algorithm, both the key/ciphertext size and encryption/decryption cost of the proposed MCP-AABE scheme are comparable to the decentralizing CP-ABE scheme [18].
- **Without key escrow:** The proposed MCP-AABE scheme can be proved to prevent the misbehavior of authorities. No individual authority can decrypt any ciphertext independently; no individual authority even with the help of corrupted users can decrypt ciphertexts not intended for the corrupted users; colluded authorities can't decrypt any ciphertext if they have no common attribute under their domains of attributes.
- **Without key abuse:** The identity gid, which is indispensable for decryption, is regarded as an essential part of a secret key, and thus anybody can trace the identity of an exposed secret key. In addition, the validity of identity can be publicly verified by any third party because a short signature of identity signed by n authorities is associated with secret key.
- **Accountability:** Due to the traceability and public verifiability of an exposed secret key, the owner of a secret key can't deny due to the effective resistance of misbehavior of authority. Thus the proposed scheme can achieve accountability.

1.4 Organization

In Sect. 2, we review the related preliminaries. In Sect. 3, we give the definition and security models. In Sect. 4, we give a concrete construction. And then, we

give the security analysis and property comparison with other works in Sect. 5. Finally, the paper is concluded in Sect. 6.

2 Preliminaries

Let $\mathbb{G}, \mathbb{G}_T$ denote two cyclic groups of order $N = p_1p_2p_3$, where p_1, p_2, p_3 are three distinct primes; for $i = 1, 2, 3$, let $\mathbb{G}_{p_i}$ denote the subgroup of order p_i in $\mathbb{G}$ and g_i denote a random generator of $\mathbb{G}_{p_i}$.

Definition 1. *A bilinear pairings e is a map such that: (1) Bilinearity: $\forall g, h \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$, we have $e(g^a, h^b) = e(g, h)^{ab}$; (2) Non-degeneracy: $\exists g \in \mathbb{G}$ such that $e(g, g)$ has order N in $\mathbb{G}_T$. (3) Computability: e can be efficiently computed.*

The subgroups are orthogonal to each other under the bilinear pairings e, i.e. for $\forall h_i \in \mathbb{G}_{p_i}, h_j \in \mathbb{G}_{p_j}, i \neq j$, there is $e(h_i, h_j) = 1$, where 1 is the identity element of $\mathbb{G}_T$.

Definition 2. *Given $g \in \mathbb{G}, g^a$, where $g \in \mathbb{G}, a \in_R \mathbb{Z}_N^*$, the discrete logarithm (DL) problem is to compute a.*

Assumption 1. *The advantage of an algorithm $\mathcal{A}$ in solving the DL problem is defined to be $Adv_{DL}(\mathcal{A}) = \Pr[\mathcal{A}(g, g^a) = a : g, g^a \leftarrow_R \mathbb{G}]$. We say that $\mathbb{G}$ satisfies the DL assumption if $Adv_{DL}(\mathcal{A})$ is a negligible function of security parameter λ for any polynomial algorithm $\mathcal{A}$.*

Definition 3. *Given g, g^a, g^b, where $g \in \mathbb{G}, a, b \in \mathbb{Z}_N$, the computational Diffie-Hellman (CDH) problem is to compute g^{ab}.*

Assumption 2. *The advantage of an algorithm in solving the CDH problem is defined to be $Adv_{CDH}(\mathcal{A}) = \Pr[\mathcal{A}(g, g^a, g^b) = g^{ab} : g, g^a, g^b \leftarrow_R \mathbb{G}]$. We say that $\mathbb{G}$ satisfies the CDH assumption if $Adv_{CDH}(\mathcal{A})$ is a negligible function of security parameter λ for any polynomial algorithm $\mathcal{A}$.*

3 Definition and Security Model

3.1 Definition

An MCP-AABE scheme consists of seven polynomial time algorithms.

Global Setup$(\lambda) \rightarrow GPP$**.** The global setup algorithm takes the security parameter λ as input, and outputs the global public parameters GPP.

Authority Setup$_{A_{i,j}(GPP)} \rightarrow SK_{A_{i,j}}, PK_{A_{i,j}}$**.** For $i = 1, ..., n$, each authority $A_{i,j} \in \mathbb{A}_i$ takes GPP as input, and outputs its master secret key $SK_{A_{i,j}}$ and public key $PK_{A_{i,j}}$.

Key Gen$(GPP, at, gid, SK_{A_{i,j}}) \rightarrow K_{A_{i,j},gid,at}$**.** For $i = 1, ..., n$, each authority $A_{i,j} \in \mathbb{A}_i$ takes GPP, a global identifier gid, an attribute at managed by $A_{i,j}$, master secret key $SK_{A_{i,j}}$ as input, and outputs a secret key $K_{A_{i,j},gid,at}$.

Key Agg$(GPP, \{K_{A_{i,j}}, gid, at\}_{i\in[n]}) \rightarrow D_{gid,at}$**.** The key aggregate algorithm takes GPP, secret keys $\{K_{A_{i,j},gid,at}\}_{i\in[n]}$ as input, and outputs an aggregate decryption key $D_{gid,at}$ of attribute at and identity gid.
Encrypt$(GPP, M, (\mathbb{W}, \rho)) \rightarrow CT$**.** The encryption algorithm takes GPP, a message M, an access structure $(\mathbb{W}, \rho)$ as input, and outputs a ciphertext CT.
Decrypt$(GPP, CT, \{D_{gid,at}{:}at \in S_{gid}\}) \rightarrow M$**.** The decryption algorithm takes in GPP, a ciphertext CT, a set of aggregate decryption keys $\{D_{gid,at}{:}at \in S_{gid}\}$, and outputs a plaintext M if S_{gid} satisfies the access policy; else, outputs a reject symbol $\perp$.
Audit$(GPP, \{D_{gid,at}{:}at \in S_{gid}\}) \rightarrow gid$ or $\perp$**.** The auditing algorithm takes GPP and a set of aggregate decryption keys $\{D_{gid,at}{:}at \in S_{gid}\}$ (or corresponding secret keys $\{K_{A_{i,j},gid,at}\}_{i\in[n]}$ for each $at \in S_{gid}$) as inputs, it outputs identity gid or a reject symbol $\perp$.

3.2 Full Security Model

The adversary in full security model, called **Type-I** adversary, is allowed to corrupt authorities, but it is naturally restricted that the corrupted authority can't directly decrypt the challenge ciphertext. The full security of MCP-AABE is defined by the following game run between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. Similarly with the security model in [18], we assume that $\mathcal{A}$ can corrupt authorities only statically, i.e. $\mathcal{A}$ should tell $\mathcal{C}$ the public keys of corrupted authorities after receiving the global parameters.
Setup. $\mathcal{C}$ runs the Global Setup(λ) algorithm and sends the global public parameters to $\mathcal{A}$. For $i = 1, ..., n$, $\mathcal{A}$ specifies sets $S_i \subset \mathbb{A}_i$ of corrupted authorities. For non-corrupted authorities in $\mathbb{A}_i - S_i$, $\mathcal{C}$ runs the Authority Setup$_{A_{i,j}}$ (GPP) algorithm to obtain master keys and gives public keys to $\mathcal{A}$.
Query Phase 1. The adversary $\mathcal{A}$ is given access to the following oracles which are simulated by the challenger $\mathcal{C}$.

- KQ(gid, at) Query: $\mathcal{A}$ submits an identity gid, an attribute at belonging to $A_{i,j} \in \mathbb{A}_i - S_i$ to $\mathcal{C}$, $\mathcal{C}$ returns $\{K_{A_{i,j},gid,at}\}_{i\in[n]}$ to $\mathcal{A}$.
- KA$(\{K_{A_{i,j},gid,at}\}_{i\in[n]})$ Query: $\mathcal{A}$ submits secret keys $\{K_{A_{i,j},gid,at}\}_{i\in[n]}$ of attribute at to $\mathcal{C}$, $\mathcal{C}$ returns aggregate decryption key $D_{gid,at}$ of at.

Challenge. $\mathcal{A}$ submits two messages M_0, M_1 of equal length, an access structure $(\mathbb{W}, \rho)$ to $\mathcal{C}$. $\mathcal{C}$ flips a random coin $b{\in_R}\{0, 1\}$ and generates the challenge ciphertext CT. At last, $\mathcal{C}$ returns CT to $\mathcal{A}$.
Query Phase 2. $\mathcal{A}$ further queries as in Query Phase 1.
Guess. $\mathcal{A}$ outputs a guess bit $b'{\in_R}\{0, 1\}$.

For an identity gid, a set W_{gid} is defined as $W_{gid} = \{at|\text{KQ}(gid, at)$ *is made by* $\mathcal{A}\}$. $\mathcal{A}$ wins the game if $b = b'$ under the restriction that for $i = 1, ..., n$ no W_{gid} such that $W_{gid} \cup \bigcup_{A_{i,j}\in S_i} \mathcal{T}_i^{-1}(A_{i,j})$ can satisfy the challenge access policy $(\mathbb{W}, \rho)$. The advantage of $\mathcal{A}$ is defined to be $Adv(\mathcal{A}) = |\Pr[b' = b] - 1/2|$.

Definition 4. *An MCP-AABE is full secure if all polynomial time adversaries have at most a negligible advantage in above game.*

3.3 Key Escrow Security Model

Key escrow security concerns about the attack from the authorities, which can be divided into two types, **Type-II** adversary and **Type-III** adversary.

Type-II adversary is defined as a dishonest authority, denoted by DA, colluding with corrupted authorities. Let $S_i \subset \mathbb{A}_i, i = 1, ..., n$ be corrupted authorities sets. Such an adversary is allowed to ask for master keys of corrupted authorities. But it is restricted that these authorities have no common attribute, i.e. $\bigcap_{DA, A_{i,j} \in S_i, i=1,\cdots,n} \mathcal{T}_i^{-1}(A_{i,j}) = \emptyset$.

Type-III adversary is defined as a dishonest authority colluding with dishonest users. Such an adversary owns an authority's master key, and is allowed to ask for secret keys of dishonest users. But it is restricted that corrupted authorities and dishonest users have no common attribute, i.e. $\bigcap_{A_{i,j} \in S_i, i=1,\cdots,n} \mathcal{T}_i^{-1}(A_{i,j}) \cap W_{gid} = \emptyset$, where $W_{gid} = \{at | \mathrm{KQ}(gid, at) \ \textit{is made by}\ \mathcal{A}\}$.

The goal of an adversary in key escrow attack is to generate an illegal secret key which is prevented by signatures signed by authorities. Thus, the key escrow security of MCP-AABE can be defined by the following unforgeability game run between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Setup. $\mathcal{C}$ runs the Global Setup(λ) algorithm and sends the global public parameters to $\mathcal{A}$. For $i = 1, ..., n$, $\mathcal{A}$ specifies sets $S_i \subset \mathbb{A}_i$ of corrupted authorities. For non-corrupted authorities, $\mathcal{C}$ runs the Authority Setup$_{A_{i,j} \in \mathbb{A}_i - S_i}$ (GPP) algorithm to obtain the master keys and gives public keys to $\mathcal{A}$.

Query Phase 1. The adversary $\mathcal{A}$ is given access to the following oracles which are simulated by the challenger $\mathcal{C}$.

- KQ(gid, at) Query: $\mathcal{A}$ submits an identity gid, an attribute at belonging to $A_{i,j} \in \mathbb{A}_i - S_i$ to $\mathcal{C}$, $\mathcal{C}$ returns $\{K_{A_{i,j},gid,at}\}_{i \in [n]}$ to $\mathcal{A}$.
- KA$(\{K_{A_{i,j},gid,at}\}_{i \in [n]})$ Query: $\mathcal{A}$ submits secret keys $\{K_{A_{i,j},gid,at}\}_{i \in [n]}$ of attribute at to $\mathcal{C}$, $\mathcal{C}$ returns an aggregate decryption key $D_{gid,at}$ of at.

Forge. $\mathcal{A}$ outputs a decryption key D_{gid^*,at^*} for some gid^*, at^*. $\mathcal{A}$ wins if D_{gid^*,at^*} can pass the Audit algorithm and $\bigcap_{A_{i,j} \in S_i, i=1,\cdots,n} \mathcal{T}_i^{-1}(A_{i,j}) \cap W_{gid^*} \neq at^*$, where $W_{gid^*} = \{at | \mathrm{KQ}(gid^*, at) \ \textit{is made by}\ \mathcal{A}\}$. The advantage of $\mathcal{A}$ is defined to be $Adv(\mathcal{A}) = \Pr[\mathcal{A}\, wins]$.

Definition 5. *An MCP-AABE is without key escrow if all polynomial time adversaries have at most a negligible advantage in the above game.*

3.4 Key Abuse Security Model

The key abuse of authority can be prevented if the CP-ABE scheme is without key escrow. Thus, we only consider the key abuse of user. It is defined as a dishonest user, denoted by DU, colluding with corrupted authorities. Let $S_i \subset \mathbb{A}_i, i = 1, ..., n$ be corrupted authorities sets. Such an adversary is allowed to ask for master keys of corrupted authorities. But it is naturally restricted that

they have no common attribute, i.e. $\bigcap_{A_{i,j} \in S_i, i=1,\cdots,n} \mathcal{T}_i^{-1}(A_{i,j}) \cap W_{DU} = \emptyset$, where W_{DU} is the attributes belongs to DU.

The key abuse security for MCP-AABE can be defined through following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Setup. $\mathcal{C}$ runs the Global Setup(λ) algorithm and sends the global public parameters to $\mathcal{A}$. For $i = 1, ..., n$, $\mathcal{A}$ specifies sets $S_i \subset \mathbb{A}_i$ of corrupted authorities. For non-corrupted authorities in $\mathbb{A}_i - S_i$, $\mathcal{C}$ runs Authority Setup$_{A_{i,j} \in \mathbb{A}_i - S_i}$ (GPP) algorithm to obtain the master keys and gives the public keys to $\mathcal{A}$.

Query Phase 1. The adversary $\mathcal{A}$ is given access to the following oracles which are simulated by the challenger $\mathcal{C}$.

- KQ(gid, at) Query: $\mathcal{A}$ submits an identity gid, an attribute at belonging to $A_{i,j} \in \mathbb{A}_i - S_i$ to $\mathcal{C}$, $\mathcal{C}$ returns $\{K_{A_{i,j},gid,at}\}_{i \in [n]}$ to $\mathcal{A}$.
- KA$(\{K_{A_{i,j},gid,at}\}_{i \in [n]})$ Query: $\mathcal{A}$ submits secret keys $\{K_{A_{i,j},gid,at}\}_{i \in [n]}$ of attribute at, $\mathcal{C}$ returns an aggregate decryption key $D_{gid,at}$ of attribute at.

Forge. $\mathcal{A}$ outputs a decryption key D_{gid^*,at^*} for some gid^*, at^*. $\mathcal{A}$ wins if D_{gid^*,at^*} can pass Audit algorithm and $\bigcap_{A_{i,j} \in S_i, i=1,\cdots,n} \mathcal{T}_i^{-1}(A_{i,j}) \cap W_{DU} \neq at^*$, where W_{DU} is the attributes belongs to dishonest user DU. The advantage of $\mathcal{A}$ is defined as $Adv(\mathcal{A}) = \Pr[\mathcal{A}\, wins]$.

Definition 6. *An MCP-AABE can resist key abuse of dishonest users if all polynomial time adversaries have at most a negligible advantage in above game.*

An MCP-AABE is accountable if it can both resist key abuse of dishonest users and authorities.

4 Our Construction

Global Setup$(\lambda) \rightarrow GPP$ **:** The algorithm runs the group generator with security parameter λ and obtains $(\mathbb{G}, \mathbb{G}_T, e, N = p_1 p_2 p_3)$, where p_1, p_2, p_3 are three distinct primes, $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups of order N, $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a bilinear map. Let $\mathbb{G}_{p_1}$ be the subgroup of order p_1 in $\mathbb{G}$, and $g \in \mathbb{G}_{p_1}$ be a random generator of $\mathbb{G}_{p_1}$. Let $\mathbb{U}$ be the attribute universe, $\mathbb{A}_1, ..., \mathbb{A}_n$ be n sets of authorities, and all the authorities in each set $\mathbb{A}_i$ manage the attribute universe $\mathbb{U}$. For $i = 1, ..., n$, let $\mathcal{T}_i : \mathbb{U} \rightarrow \mathbb{A}_i$ be a map from each attribute $at \in \mathbb{U}$ to an authority $A_{i,j} \in \mathbb{A}_i$, and let $\mathcal{T}_i^{-1}(A_{i,j}) = \{at \in \mathbb{U} : \mathcal{T}_i(at) = A_{i,j}\}$, where $A_{i,j} \in \mathbb{A}_i$. Let $\mathcal{F} : \mathbb{U} \rightarrow \mathbb{G}$ be a map from each attribute $at \in \mathbb{U}$ to an element of $\mathbb{G}$. Let $H : \{0,1\}^* \rightarrow \mathbb{G}$ be a secure Hash function modeled as random oracles. The global public parameters $GPP = \{N, \mathbb{G}, \mathbb{G}_T, e, g, \mathbb{U}, \mathbb{A}_1, ..., \mathbb{A}_n, \mathcal{T}_1, ..., \mathcal{T}_n, \mathcal{F}, H\}$.

Authority Setup$_{A_{i,j}}(GPP) \rightarrow SK_{A_{i,j}}, PK_{A_{i,j}}$ **:** For $i = 1, ..., n$, each authority $A_{i,j} \in \mathbb{A}_i$ randomly chooses $\alpha_{i,j}, x_{i,j} \in_R \mathbb{Z}_N^*$, keeps $SK_{A_{i,j}} = \{\alpha_{i,j}, x_{i,j}\}$ as its master key, and publishes its public key $PK_{A_{i,j}} = (e(g,g)^{\alpha_{i,j}}, g^{x_{i,j}})$.

Key Gen$(GPP, at, gid, SK_{A_{i,j}}) \rightarrow K_{A_{i,j},gid,at}$ **:** The secret key $K_{A_{i,j},gid,at}$ of attribute at and identity gid, where $\mathcal{T}_i(at) = A_{i,j}$, can be generated as follows.

- The user submits identity gid and attribute at to authority $A_{i,j}$, and the authority $A_{i,j}$ verifies the correctness of gid, at;
- If attribute at belongs to gid, $A_{i,j}$ chooses $r_i \in_R \mathbb{Z}_N^*$ randomly, and computes $K^{(1)}_{A_{i,j},gid,at} = g^{\alpha_{i,j}} H(gid)^{x_{i,j}} \mathcal{F}(at)^{r_i}, K^{(2)}_{A_{i,j},gid,at} = g^{r_i}$, and returns $(K^{(1)}_{A_{i,j},gid,at}, K^{(2)}_{A_{i,j},gid,at})$ to user secretly.

Key Agg$(GPP, \{K_{A_{i,j},gid,at}\}_{i\in[n]}) \rightarrow D_{gid,at}$ **:** Receiving $\{K_{A_{i,j},gid,at}\}_{i\in[n]}$ from $A_{i,j}$, for $i = 1, ..., n$, the user computes $D^{(1)}_{gid,at} = \prod_{i=1}^{n} K^{(1)}_{A_{i,j},gid,at}, D^{(2)}_{gid,at} = \prod_{i=1}^{n} K^{(2)}_{A_{i,j},gid,at}$. Here, gid is indispensable to decryption process, and regarded as part of secret key. At last, the aggregate decryption key $D_{gid,at}$ for identity gid with attribute at formats as $D_{gid,at} = (gid, D^{(1)}_{gid,at}, D^{(2)}_{gid,at})$.

Encrypt$(GPP, M, (\mathbb{W}, \rho)) \rightarrow CT$ **:** Given message M, access structure $(\mathbb{W}, \rho)$, where $\mathbb{W}$ is a $l \times l'$ matrix and ρ is a map from a row $\mathbb{W}_i$ of $\mathbb{W}$ to an attribute $at_{\rho(i)}$. For $i = 1, ..., l$ and $j = 1, ..., n$, let $\mathcal{T}_j(at_{\rho(i)}) = A_{j,\rho(i)}$. Then the ciphertext $CT = (C_0, \{C_{1,i}, C_{2,i}, C_{3,i}, C_{4,i}\}_{i\in[l]})$ can be generated as follows.

- Chooses $s, v_2, ..., v_{l'}, w_2, ..., w_{l'} \in_R \mathbb{Z}_N^*$ randomly, and constructs two vectors: $\vec{v} = (s, v_2, ..., v_{l'}), \vec{w} = (0, w_2, ..., w_{l'})$.
- For $i = 1, ..., l$, chooses $t_i \in_R \mathbb{Z}_N$ randomly, computes $\lambda_i = \mathbb{W}_i \cdot \vec{v}$ and $\mu_i = \mathbb{W}_i \cdot \vec{w}$, and computes: $C_0 = M \cdot e(g,g)^s$; $C_{1,i} = e(g,g)^{\lambda_i} \prod_{j=1}^{n} e(g,g)^{\alpha_{j,\rho(i)} t_i}$; $C_{2,i} = g^{t_i}$; $C_{3,i} = \prod_{j=1}^{n} g^{x_{j,\rho(i)} t_i} g^{\mu_i}$; $C_{4,i} = \mathcal{F}(at_{\rho(i)})^{t_i}$.

Decrypt$(GPP, CT, \{D_{gid,at} : at \in S_{gid}\}) \rightarrow M$ **:** If S_{gid} satisfies the access policy specified by $(\mathbb{W}, \rho)$, user gid with attribute set S_{gid} can recover message as follows.

- Computes $\{\omega_i : i \in I\}$ such that $\sum_{i\in I} \omega_i \mathbb{W}_i = (1, 0, ..., 0)$, where $I = \{i : at_{\rho(i)} \in S_{gid}\}$.
- Computes $\frac{C_{1,i} e(C_{3,i}, H(gid)) e(C_{4,i}, D^{(2)}_{gid,at_{\rho(i)}})}{e(C_{2,i}, D^{(1)}_{gid,at_{\rho(i)}})} = e(g,g)^{\lambda_i} e(g, H(gid))^{\mu_i}$.
- Computes $\prod_{i\in I} \left(e(g,g)^{\lambda_i} e(g, H(gid))^{\mu_i}\right)^{\omega_i} = e(g,g)^s$.
- Recovers $M = \frac{C_0}{e(g,g)^s}$.

Audit$(GPP, gid, \{D_{gid,at}{:}at \in S_{gid}\}) \rightarrow gid$ or $\perp$ **:** Given an aggregate decryption key $(gid, \{D_{gid,at}{:}at \in S_{gid}\})$, any third party can publicly verify whether it belongs to identity gid or not. If and only if $\exists at \in S_{gid}$ such that $e(D^{(1)}_{gid,at}, g) = \prod_{i=1}^{n} PK^1_{A_{i,j}} \prod_{i=1}^{n} e(PK^2_{A_{i,j}}, H(gid)) e(\mathcal{F}(at), D^{(2)}_{gid,at})$, where $\mathcal{T}_i(at) = A_{i,j}$ for $i = 1, ..., n$, the algorithm output an identity gid, else output $\perp$.

5 Security Analysis and Performance

The proposed MCP-AABE scheme can be proved fully secure based on the full security of the multi-authority CP-ABE scheme [18] by Theorem 1, and can be proved without key escrow based on the unforgeability of the short signature scheme [30] in Theorem 2, and can be proved without key abuse based on the unforgeability of signature schemes [29,30] by Theorem 3.

5.1 Confidentiality

Theorem 1. *If there is an adversary $\mathcal{A}$ that can break full security of the proposed MCP-AABE scheme with advantage ε, there will be an adversary $\mathcal{A}_1$ with advantage ε that can break the multi-authority CP-ABE scheme* [18].

Proof. We will prove that an adversary $\mathcal{A}$ against the proposed MCP-AABE scheme can be used to construct an adversary $\mathcal{A}_1$ against the multi-authority CP-ABE scheme [18] as follows.

Setup. Challenger $\mathcal{C}$ runs the Global Setup(λ) algorithm and sends the global public parameters $\{N, \mathbb{G}, \mathbb{G}_T, e, g, \mathbb{U}, \mathbb{A}_1, ..., \mathbb{A}_n, \mathcal{T}_1, ..., \mathcal{T}_n, \mathcal{F}, H\}$ to $\mathcal{A}$, and sends $\{N, \mathbb{G}, \mathbb{G}_T, e, g, \mathbb{U}, \}$ to $\mathcal{A}_1$. $\mathcal{A}$ and $\mathcal{A}_1$ specifies corrupted authorities. $\mathcal{C}$ runs the Authority Setup$_{A_{i,j}}(GPP)$ algorithm, and gives public keys of uncorrupted authorities to $\mathcal{A}$, computes $(e(g,g)^{\sum_{i=1}^{n} \alpha_{i,j}}, g^{\sum_{i=1}^{n} x_{i,j}})$ which implies the master key of uncorrupted authority is set to be $\alpha_j = \sum_{i=1}^{n} \alpha_{i,j}, x_j = \sum_{i=1}^{n} x_{i,j}$ and sends $(e(g,g)^{\sum_{i=1}^{n} \alpha_{i,j}}, g^{\sum_{i=1}^{n} x_{i,j}})$ to $\mathcal{A}_1$.

Query Phase 1. Given a KQ(gid, at) query from $\mathcal{A}_1$, $\mathcal{C}$ generates an aggregate decryption key $(D^{(1)}_{gid,at}, D^{(2)}_{gid,at})$ of attribute at with $r_i = 0, i = 1, ..., n$, and sends $D^{(1)}_{gid,at} = g^{\sum_{i=1}^{n} \alpha_{i,j}} H(gid)^{\sum_{i=1}^{n} x_{i,j}} \mathcal{F}(at)^{\sum_{i=1}^{n} r_i} = g^{\alpha_j} H(gid)^{x_j}$ to $\mathcal{A}_1$.

Challenge. Given two messages M_0, M_1 and an access structure $(\mathbb{W}, \rho)$. $\mathcal{C}$ generates a challenge ciphertext $CT = (C_0, \{C_{1,i}, C_{2,i}, C_{3,i}, C_{4,i}\}_{i\in[l]})$ for $\mathcal{A}$. $C_{1,i}, C_{3,i}$can be written as $C_{1,i} = e(g,g)^{\lambda_i} e(g,g)^{\alpha_{\rho(i)} t_i}, C_{3,i} = \prod_{j=1}^{n} g^{x_{j,\rho(i)} t_i} g^{\mu_i} = g^{x_{\rho(i)} t_i} g^{\mu_i}$. Thus, $\mathcal{C}$ sends $(C_0, \{C_{1,i}, C_{2,i}, C_{3,i}\}_{i\in[l]})$ to $\mathcal{A}_1$.

From above simulation, $\mathcal{C}$ can indistinguishably simulate all the queries asked from $\mathcal{A}_1$. Thus, if there is an adversary $\mathcal{A}$ that has advantage ε to have a correct guess $b = b'$, similarly $\mathcal{C}$ has advantage ε to break the multi-authority CP-ABE scheme [18].

5.2 Security Analysis for Problem of Key Escrow

Theorem 2. *Let $Adv_{DL}(\mathcal{A})$ denote the advantage of adversary $\mathcal{A}$ in solving the DL problem, and ε_1 denote the advantage of adversary $\mathcal{A}$ against the short*

signature scheme [30]*, then a Type II or Type III adversary* $\mathcal{A}$ *in the proposed MCP-AABE scheme can generate a valid decryption key with advantage at most* $Adv_{DL}(\mathcal{A}) + \varepsilon_1$.

Proof. The short signature in scheme [30] formats as $H(m)^x$, where x is the secret key. $D^{(1)}_{gid,at} = g^{\sum_{i=1}^{n} \alpha_{i,j}} H(gid)^{\sum_{i=1}^{n} x_{i,j}} \mathcal{F}(at)^{\sum_{i=1}^{n} r_i} = H(gid)^{\sum_{i=1}^{n} x_{i,j}} g'$, can be directly seen as a short signature [30] of identity signed by secret key $\sum_{i=1}^{n} x_{i,j}$.

The short signature scheme [30] is proved to be unforgeable under the CDH assumption. Then, we only need to reduce the key escrow security of our scheme to the unforgeability of scheme [30]. There are two kinds of adversaries in key escrow security model: Type II and Type III adversary.

Type-II adversary is defined as a dishonest authority colluding with corrupted authorities. Let DA denote the dishonest authority and $S_i \subset \mathbb{A}_i, i = 1, ..., n$ be corrupted authorities sets. However, it is restricted that corrupted authorities have no common attribute, i.e. $\bigcap_{DA, A_{i,j} \in S_i, i=1,\cdots,n} \mathcal{T}_i^{-1}(A_{i,j}) = \emptyset$. Without loss of generality, we assume authority $A_{1,1}$ denote the dishonest authority, and authorities $A_{i,j}, i \in [2, n], j \in J$, where J is an index set, are corrupted, and assume $at \notin \mathcal{T}_1^{-1}(A_{1,1})$ according to the restriction. Then, a Type-II adversary knows $\sum_{i=2}^{n} x_{i,j}$ and public key $g^{x_{1,1}}$. Owing to the unforgeability of signature scheme [30] and the DL assumption, a Type-II adversary can't generate $D^{(1)}_{gid,at} = H(gid)^{x_{1,1}} H(gid)^{\sum_{i=2}^{n} x_{i,j}} g'$.

Type-III adversary is defined as dishonest authorities colluding with dishonest users. It is naturally restricted that corrupted authorities and dishonest users have no common attribute, i.e. $\bigcap_{A_{i,j} \in S_i, i=1,\cdots,n} \mathcal{T}_i^{-1}(A_{i,j}) \cap W_{gid} = \emptyset$, where $W_{gid} = \{at | \mathrm{KQ}(gid, at) \ \ is\ made\ by\ \mathcal{A}\}$. We assume $at \notin \mathcal{T}_1^{-1}(A_{1,1})$, then a Type-III adversary can get $H(gid)^{\sum_{i=2}^{n} x_{i,j}} g^{\sum_{i=2}^{n} \alpha_{i,j}} \mathcal{F}(at)^{\sum_{i=2}^{n} r_i}$ from corrupted authorities and dishonest users, and public key $g^{x_{1,1}}$. Owing to the unforgeability of scheme [30], a Type-III adversary cannot generate a valid secret key $D^{(1)}_{gid,at} = H(gid)^{x_{1,1}} H(gid)^{\sum_{i=2}^{n} x_{i,j}} g'$.

5.3 Security Analysis for Problem of Key Abuse

Theorem 3. *Let* $Adv_{DL}(\mathcal{A})$ *denote the advantage of adversary* $\mathcal{A}$ *in solving the DL problem, and* ε_2 *denote the advantage of adversary* $\mathcal{A}$ *against the signature scheme* [29]*, then a malicious user* $\mathcal{A}$ *in the proposed MCP-AABE scheme can generate a forged decryption key with advantage at most* $Adv_{DL}(\mathcal{A}) + \varepsilon_2$.

Proof. The signature scheme in scheme [29] formats as $g_2^{\alpha} \mathcal{F}(at)^r, g^r$, where $g_2 \in_R \mathbb{G}$, $r \in_R \mathbb{Z}_N^*$ and α is the secret key. The decryption key $D^{(1)}_{gid,at} = g' g_2^{\sum_{i=1}^{n} x_{i,j}}$

$\mathcal{F}(at)^{\sum_{i=1}^{n} r_i}$, $D_{gid,at}^{(2)} = g^{\sum_{i=1}^{n} r_i}$, where $g_2 = H(gid), g' = g^{\sum_{i=1}^{n} \alpha_{i,j}}$, can be directly seen as a signature [29] of attribute at signed by secret key $\sum_{i=1}^{n} x_{i,j}$.

The signature scheme [29] is proved to be unforgeable under the CDH assumption. Then, we will reduce the key abuse security of the proposed scheme to the unforgeability of scheme [29]. The key abuse of authority can be prevented because the CP-ABE scheme is without key escrow. Thus, we only consider the key abuse of user.

The key abuse of user is defined as a dishonest user, denoted by DU, colluding with corrupted authorities. It is restricted that they have no common attribute, i.e. $\bigcap_{A_{i,j} \in S_i, i=1,\cdots,n} \mathcal{T}_i^{-1}(A_{i,j}) \cap W_{DU} = \emptyset$, where W_{DU} is the attributes belongs to dishonest user DU. We assume $at \notin \mathcal{T}_1^{-1}(A_{1,1})$, then a Type-III adversary can get $H(gid)^{\sum_{i=2}^{n} x_{i,j}} \mathcal{F}(at)^{\sum_{i=2}^{n} r_i} g^{\sum_{i=2}^{n} \alpha_{i,j}}, g^{\sum_{i=2}^{n} r_i}$ from corrupted authorities and dishonest users, and the public key $g^{x_{1,1}}$. Thus, owing to the unforgeability of signature scheme [29], a malicious user cannot generate a valid secret key $D_{gid,at}^{(1)} = g_2^{x_{1,1}} g_2^{\sum_{i=2}^{n} x_{i,j}} \mathcal{F}(at)^{\sum_{i=1}^{n} r_i} g', D_{gid,at}^{(2)} = g^{\sum_{i=1}^{n} r_i}$.

Furthermore, from Theorem 2 and Theorem 3, the key abuse of both dishonest user and authority can be prevented, so it can achieve accountability.

5.4 Feature and Efficiency Comparisons

Table 1 shows comparisons of security properties between multi-authority ABE schemes [18,19,25], traceable ABE schemes [26–28] and the MCP-AABE scheme, where TR denotes traceability and PV denotes public verifiability. The proposed MCP-AABE scheme is adaptively secure in the random oracle model, and is the first multi-authority CP-ABE that is without key escrow and key abuse.

Table 1. Security property comparison with related works

Scheme	Type I	Key Escrow			Key Abuse	
		Type II	Type III	Type IV	TR	PV
[18]	Full	×	×	×	✓	×
[19]	Full	✓	×	✓	×	×
[25]	Selective	✓	✓	×	×	×
[26]	Selective	✓	×	×	✓	✓
[27]	Full	×	×	×	✓	×
[28]	Full	×	×	×	✓	✓
MCP-AABE	Full	✓	✓	✓	✓	✓

We also give a comparison of efficiency with the multi-authority CP-ABE schemes [18,19]. Let $|A|$ denote the number of attributes associated with a secret

key, $|W|$ denote the number of attributes related to an access structure, $|D|$ denote the number of attributes needed for decryption, $|N|$ denote the number of CAs in [19].

Table 2. Efficiency comparison with scheme [18]

Scheme	Key	Ciphertext	Encryption		Decryption	
			Pairing	Exponential	Pairing	Exponential
[18]	$\|A\|$	$3\|W\|+1$	1	$5\|W\|+1$	$2\|D\|$	$\|D\|+1$
[19]	$2\|A\|+1$	$2\|W\|+1$	1	$3\|W\|+\|N\|+1$	$3\|D\|$	$\|D\|+1$
MCP-AABE	$2\|A\|$	$4\|W\|+1$	1	$6\|W\|+1$	$3\|D\|$	$\|D\|+1$

As shown in Table 2, the efficiency of MCP-AABE is comparable to the CP-ABE scheme [18,19]. Actually, if without considering the multiplication operation in group $\mathbb{G}$, the efficiency (including the key and ciphertext size) of the proposed MCP-AABE scheme can be decreased to the same as scheme [18] if we let an attribute relate to a master key instead of a master key managing many attributes, i.e. for $i = 1, ..., n, \forall A_{i,j} \in \mathbb{A}_i$, $|\mathcal{T}_i^{-1}(A_{i,j})| = 1$. Let $r_i = 0, i = 1, ..., n$, then $(D^{(1)}_{gid,at}, D^{(2)}_{gid,at}) = (g^{\alpha_j} H(gid)^{x_j}, g)$ is same as secret key in scheme [18] with master key $\alpha_j = \sum_{i=1}^{n} \alpha_{i,j}, x_j = \sum_{i=1}^{n} x_{i,j}$. Furthermore, in scheme [19], AAs should register itself to the CAs which will need troublesome authenticated interaction, and in MCP-AABE, each authority can independently issue secret keys for users.

6 Conclusion

Key escrow and key abuse are two quite challenging issues in an ABE access control system. We formalize the concept of MCP-AABE and propose a concrete MCP-AABE scheme. In the proposed scheme, authorities who are from different authority sets will independently distribute a secret key for an attribute, and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. In the proposed scheme, no individual authority can decrypt any ciphertext. Even with the help of any corrupted user, no individual authority can decrypt the ciphertext not intended for the corrupted user. Furthermore, corrupted authorities can't decrypt any ciphertext if they have no common attribute in their domains of attributes. In addition, any third party can publicly verify the identity of an exposed secret key. Thus, it can achieve accountability. At last, the computation cost and communication cost of our scheme is comparable to the decentralizing CP-ABE scheme [18].

Acknowledgment. This work was supported in part by China Postdoctoral Science Foundation of China (No. 2016M591629), in part by the National Natural Science

Foundation of China (No. 61602512, 61632012, 61373154, 61371083, 61411146001), in part by the Prioritized Development Projects through Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20130073130004).

References

1. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). doi:10.1007/11426639_27
2. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98. ACM (2006)
3. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy 2007, pp. 321–334. IEEE (2007)
4. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010). doi:10.1007/978-3-642-14623-7_11
5. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_4
6. Herranz, J., Laguillaumie, F., Ràfols, C.: Constant size ciphertexts in threshold attribute-based encryption. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 19–34. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13013-7_2
7. Lewko, A., Waters, B.: Unbounded HIBE and attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 547–567. Springer, Heidelberg (2011). doi:10.1007/978-3-642-20465-4_30
8. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011). doi:10.1007/978-3-642-19379-8_4
9. Yamada, S., Attrapadung, N., Hanaoka, G., Kunihiro, N.: Generic constructions for chosen-ciphertext secure attribute based encryption. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 71–89. Springer, Heidelberg (2011). doi:10.1007/978-3-642-19379-8_5
10. Okamoto, T., Takashima, K.: Fully secure unbounded inner-product and attribute-based encryption. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 349–366. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34961-4_22
11. Lewko, A., Waters, B.: New proof methods for attribute-based encryption: achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32009-5_12
12. Hohenberger, S., Waters, B.: Attribute-based encryption with fast decryption. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 162–179. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36362-7_11
13. Rouselakis, Y., Waters, B.: Practical constructions and new proof methods for large universe attribute-based encryption. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security, pp. 463–474. ACM (2013)

14. Chase, M.: Multi-authority attribute based encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007). doi:10.1007/978-3-540-70936-7_28
15. Mller, S., Katzenbeisser, S., Eckert, C.: On multi-authority ciphertext-policy attribute-based encryption. Bull. Korean Math. Soc. **46**(4), 803–819 (2009)
16. Lin, H., Cao, Z., Liang, X., et al.: Secure threshold multi authority attribute based encryption without a central authority. Inf. Sci. **180**(13), 2618–2632 (2010)
17. Chase, M., Chow, S.: Improving privacy and security in multi-authority attribute-based encryption. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 121–130. ACM (2009)
18. Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011). doi:10.1007/978-3-642-20465-4_31
19. Liu, Z., Cao, Z., Huang, Q., Wong, D.S., Yuen, T.H.: Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles. In: Atluri, V., Diaz, C. (eds.) ESORICS 2011. LNCS, vol. 6879, pp. 278–297. Springer, Heidelberg (2011). doi:10.1007/978-3-642-23822-2_16
20. Rouselakis, Y., Waters, B.: Efficient statically-secure large-universe multi-authority attribute-based encryption. In: Böhme, R., Okamoto, T. (eds.) FC 2015. LNCS, vol. 8975, pp. 315–332. Springer, Heidelberg (2015). doi:10.1007/978-3-662-47854-7_19
21. Qian, H., Li, J., Zhang, Y., Han, J.: Privacy preserving personal health record using multi-authority attribute-based encryption with revocation. Int. J. Inf. Secur. **14**(6), 487–497 (2015)
22. Chow, S.S.M.: A framework of multi-authority attribute-based encryption with out-sourcing and revocation. In: Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies 2016, pp. 215–226. ACM (2016)
23. Jiang, R., Wu, X., Bhargava, B.: Secure data sharing scheme in multi-authority cloud storage systems. Comput. Secur. **62**, 193–212 (2016). Elsevier
24. Zhong, H., Zhu, W., Xu, Y., et al.: Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. Soft Comput. (2016). doi:10.1007/s00500-016-2330-8
25. Zhang, X., Jin, C., Wen, Z., Shen, Q., Fang, Y., Wu, Z.: Attribute-based encryption without key escrow. In: Huang, Z., Sun, X., Luo, J., Wang, J. (eds.) ICCCS 2015. LNCS, vol. 9483, pp. 74–87. Springer, Cham (2015). doi:10.1007/978-3-319-27051-7_7
26. Li, J., Ren, K., Kim, K.: A2BE: accountable attribute-based encryption for abuse free access control. IACR Cryptology ePrint Arch 2009, 118 (2009)
27. Ning, J., Cao, Z., Dong, X., Wei, L., Lin, X.: Large universe ciphertext-policy attribute-based encryption with white-box traceability. In: Kutyłowski, M., Vaidya, J. (eds.) ESORICS 2014. LNCS, vol. 8713, pp. 55–72. Springer, Cham (2014). doi:10.1007/978-3-319-11212-1_4
28. Ning, J., Dong, X., Cao, Z., Wei, L.: Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In: Pernul, G., Ryan, P.Y.A., Weippl, E. (eds.) ESORICS 2015. LNCS, vol. 9327, pp. 270–289. Springer, Cham (2015). doi:10.1007/978-3-319-24177-7_14
29. Paterson, K.G., Schuldt, J.C.N.: Efficient identity-based signatures secure in the standard model. In: Batten, L.M., Safavi-Naini, R. (eds.) ACISP 2006. LNCS, vol. 4058, pp. 207–222. Springer, Heidelberg (2006). doi:10.1007/11780656_18
30. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1_30