SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2018, Vol. 61 032102:1–032102:13
doi: 10.1007/s11432-016-9019-8

Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability

Kai ZHANG[1], Hui LI[2], Jianfeng MA[3*] & Ximeng LIU[4]

[1]*School of Telecommunications Engineering, Xidian University, Xi'an* 710071*, China;*
[2]*School of Cyber Engineering, Xidian University, Xi'an* 710071*, China;*
[3]*School of Computer Science and Technology, Xidian University, Xi'an* 710071*, China;*
[4]*School of Information Systems, Singapore Management University, Singapore* 178902*, Singapore*

Received 10 April 2016/Accepted 10 January 2017/Published online 29 June 2017

Abstract Traceable multi-authority ciphertext-policy attribute-based encryption (CP-ABE) is a practical encryption method that can achieve user traceability and fine-grained access control simultaneously. However, existing traceable multi-authority CP-ABE schemes have two main limitations that prevent them from practical applications. First, these schemes only support small universe: the attributes must be fixed at system setup and the attribute space is restricted to polynomial size. Second, the schemes are either less expressive (the access policy is limited to "AND gates with wildcard") or inefficient (the system is constructed in composite order bilinear groups). To address these limitations, we present a traceable large universe multi-authority CP-ABE scheme, and further prove that it is statically secure in the random oracle model. Compared with existing traceable multi-authority CP-ABE schemes, the proposed scheme has four advantages. First, the attributes are not fixed at setup and the attribute universe is not bounded to polynomial size. Second, the ciphertext polices can be expressed as any monotone access structures. Third, the proposed scheme is constructed in prime order groups, which makes this scheme more efficient than those in composite order bilinear groups. Finally, the proposed scheme requires neither a central authority nor an identity table for tracing.

Keywords attribute-based encryption, multi-authority, ciphertext-policy, traceability, large universe

Citation Zhang K, Li H, Ma J F, et al. Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability. Sci China Inf Sci, 2018, 61(3): 032102, doi: 10.1007/s11432-016-9019-8

1 Introduction

Attribute-based encryption (ABE) [1], where a user's decryption privilege is based on his attributes, is a useful method for a user to share data with a targeted group of recipients. Depending on whether the access policy is associated with the ciphertext or the private key, ABE can be further categorized into ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In CP-ABE, the data owner encrypts the data by a specific policy in the form of a Boolean formula. An authority issues each user a secret key that is associated with the user's attributes. A user can decrypt the ciphertext if and only if his attributes satisfy the Boolean formula. For example, a data owner wants to share sensitive medical data with all female doctors in a hospital. She must encrypt the medical data with the access policy ("Doctor"

* Corresponding author (email: jfma@mail.xidian.edu.cn)

AND "Female") such that only those users whose attributes satisfy the policy can decrypt it. Since the introduction of ABE, many ABE schemes [2–8] have been proposed. One key limitation of these schemes is that a central authority is required to control all attributes and issue all private keys. This inevitably limits the application of ABE, because different attribute sets must be managed by different authorities in many scenarios. For instance, consider an e-healthcare cloud system, a patient wants to send his medical information to users who are both doctors and professors. As the attribute of "Professor" is managed by a university while the attribute of "Doctor" is managed by a hospital, the ABE scheme with a single authority is obviously unsuitable in this scenario. Chase [9] presented a multi-authority ABE scheme to address this problem. In particular, according to multi-authority CP-ABE, different authorities issue secret keys for different attribute sets and the user's secret key is associated with his attributes. In the above example, the university issues each professor a secret key associated with the attribute "Professor" and the hospital issues each doctor a secret key associated with the attribute "Doctor".

Note that multi-authority CP-ABE is a one-to-many encryption; different users may have the same attributes and decryption privileges. This may cause the problem that a user with the required attributes could illegally sell his secret key for financial benefit without being caught. For instance, a hospital utilizes a multi-authority CP-ABE scheme to build an e-healthcare cloud system to provide secure and fine-grained data access control. The patients encrypt their medical data by the specified access polices and store the ciphertexts in the cloud server. The users whose attributes satisfy the access policies can recover the corresponding medical data. Suppose Alice and Bob are both doctors and professors in this system, hence, their decryption keys are associated with the attribute set {"Professor", "Doctor"}. When a patient encrypts his medical data with the policy ("Doctor" AND "Professor"), both Alice and Bob can use their decryption keys to access the medical data. However, if one of them sells his decryption key to someone else, how can we determine who leaked the decryption key?

To address this problem, Li et al. [10] presented the first traceable multi-authority CP-ABE, which is limited to expressing a strict "AND gates with wildcard" policy. However, Liu et al. [11] pointed out that the malicious user cannot be traced simply by the approach in [10]. Recently, Zhou et al. [12] proposed a traceable multi-authority CP-ABE scheme where the policies can be expressed in any monotone access structures. While Ref. [12] supports both high expressiveness and traceability, there are three major aspects that restrict its practical applications.

(1) The scheme can only support a small universe of attributes. In their construction, the attributes must be fixed at setup, the attribute universe is restricted to polynomial size, and the size of the public parameters increases linearly with the size of the attribute universe. This will cause unnecessary burden in the actual application of multi-authority CP-ABE. If the attribute universe is chosen to be too small, the system will need to be completely rebuilt when a large number of new attributes are added into the system. If the attribute universe is chosen to be too large, the storage cost will be tremendous owing to the increased size of the public parameters.

(2) Multiple central authorities are required in their scheme and each of them must maintain an identity table. The size of the identity table is related to the number of users and this will cause a significant storage cost for tracing.

(3) The scheme is constructed in composite order bilinear groups. Since the pairing and exponentiation operations in composite order groups are considerably slower than those in prime order groups, their scheme has a significant computation overhead in comparison to schemes that are constructed in prime order groups.

Reconsider the e-healthcare cloud system example, where there are multiple data owners and data users. The data owner can be a patient; the data user can be a doctor, researcher, or pharmacist. Each user is associated with an attributes set and the attributes are managed by multiple attribute authorities. To achieve data confidential and fine-grained access control with traceability, the traceable multi-authority CP-ABE can be adopted by the e-healthcare cloud system. In this system, the authorities issue the secret keys for each user; the owner encrypts the data by an access policy and stores the ciphertexts in the cloud. Then, the users whose attributes satisfy the access policy can access the data. However, there are two major challenges that affect the practical application of the state-of-the-art traceable multi-authority

Table 1 Features summary of traceable multi-authority CP-ABE results

	Large universe[a)]	Supportting any monotone access structures[b)]	Efficient[c)]	No identity table[d)]
Ref. [10]	×	×	×	✓
Ref. [12]	×	✓	×	×
This paper	✓	✓	✓	✓

a) The schemes in [10, 12] only support small universe.
b) In [10], the ciphertext policy is limited to "AND gates with wildcard".
c) In [10], the ciphertext size grows linearly with the size of the attribute universe. The scheme in [12] is constructed in composite order bilinear groups, which is significantly slower than that in prime order groups.
d) In [12], there exist multiple central authorities and each central authority must manage an identity table for tracing.

CP-ABE [12] in the e-healthcare cloud system. First, as the attributes must be fixed at the system setup phase, the e-healthcare cloud system must be completely rebuilt when the system expands and the new attributes exceed the attribute universe. Note that the attribute universe can be chosen sufficiently large to avoid the reconstruction of the system. However, this will cause an unnecessary efficiency burden because the size of the public parameters increases linearly with the size of the attribute universe. Second, the high storage and computation overheads cause system inefficiency in real-world usage. On one hand, the storage cost for tracing leads to a huge burden for the system with a large number of users. On the other hand, the decryption operation in composite order bilinear groups could potentially lead to unacceptable wait times for the users who want to access a large amount of medical data.

1.1 Our contribution

In this paper, to address the aforementioned limitations in traceable multi-authority CP-ABE, we construct a large universe multi-authority CP-ABE scheme with white-box traceability in prime order bilinear groups. To the best of our knowledge, this is the first multi-authority CP-ABE scheme that supports both large universe and traceability. Also, we prove that the scheme achieves static security in the random oracle model. The features of the proposed scheme are highlighted as follows:

(1) **Multi-authority.** The proposed scheme is a multi authority CP-ABE scheme, where neither a central authority nor coordination between different authorities is required. This feature allows the proposed scheme to be more practical for practical application.

(2) **Traceability.** In the proposed scheme, the malicious user who discloses his decrypt key for commercial profit can be identified by the tracing algorithm.

(3) **Large universe.** The proposed scheme supports large universe. In this scheme, any string can be used as an attribute, so the attribute universe is not restricted to polynomial size and the attributes do not need to be fixed at setup. Besides, the size of the public parameters does not increase with the size of the attribute universe.

(4) **High expressiveness.** The proposed scheme allows the policies to be expressed as any monotone access structures.

(5) **Efficient.** The proposed scheme is constructed in prime order bilinear groups, which is significantly faster than that in composite order bilinear groups. In addition, the ciphertext size grows linearly with respect to the number of the access matrix rows used in decryption, rather than the size of the attribute universe.

(6) **No identity table.** The proposed scheme does not require an identity table; hence, the storage cost for tracing can be significantly reduced.

In Table 1, we summarize the key features of the proposed scheme as well as several state-of-the-art traceable multi-authority CP-ABE works.

1.2 Related work

ABE was first introduced by Sahai and Waters [1]. Later, Goyal et al. [2] divided ABE into KP-ABE and CP-ABE. The CP-ABE scheme for monotonic access structures was presented in [3] and the CP-ABE scheme for non-monotonic access structures was presented in [5]. The fully secure CP-ABE scheme was first given in [6]. Chase [9] presented the first multi-authority ABE, but with a central authority that

could decrypt every ciphertext. Chase and Chow [13] removed the central authority in the multi-authority ABE scheme. However, a ciphertext policy can only be a strict "AND" policy over a pre-determined set of authorities in their scheme. The first highly expressive (i.e., the policies can be expressed as any monotonic access structures) and adaptively secure multi-authority ABE was presented in [14]. Ying et al. [15] presented a multi-authority ABE scheme with policy updating. The large universe ABE in composite order bilinear groups was given in [16], while the large universe CP-ABE in prime order bilinear groups was given in [17]. Recently, Rouselakis and Waters [18] presented a large-universe multi-authority ABE scheme in the random oracle model.

The trace problem in ABE was first considered in [19]. Traceable ABE can be divided into white-box traceable ABE and black-box traceable ABE. In white-box traceable ABE [11, 20, 21], the malicious user who leaks his decryption keys to others can be caught. While for black-box traceable ABE [22], the malicious user leaks a decryption equipment (i.e., a black box is constructed by his decryption key and unknown algorithm) that can decrypt some ABE ciphertexts. Since the introduction of traceable ABE [19], several traceable ABE schemes [10–12, 20–25] have been proposed for different requirements. Liu et al. presented the first highly expressive white-box traceable CP-ABE in [11] and black-box traceable CP-ABE in [22]. The first multi-authority CP-ABE with traceability was presented in [10]. However, its ciphertext policy is limited to "AND gates with wildcard" and its ciphertext size grows linearly with the size of the attribute universe. Recently, a highly expressive traceable multi-authority CP-ABE was presented for an e-healthcare cloud computing system [12]. However, it suffers from a limited universe of attributes and excessive time cost. In comparison, in this paper we present a more efficient multi-authority CP-ABE with white-box traceability, which supports both high expressiveness and large universe.

1.3 Organization

The rest of this paper is outlined as follows. In Section 2, we give background information on access structures, linear secret-sharing schemes, bilinear groups, and complexity assumptions. The formal definition and security model for traceable multi-authority CP-ABE are in Section 3. We present an efficient large universe traceable multi-authority CP-ABE scheme and the proof of its security and traceability in Section 4. We provide an efficiency study of our scheme in Section 5 and conclude the paper in Section 6.

2 Background

2.1 Access structures

Definition 1 (Access structure [26]). Let $\{P_1, P_2, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}}$ is monotone if and only if: for $\forall B, C$, if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$. An access structure (respectively monotone access structure) is a collection (respectively monotone collection) $\mathbb{A}$ of non-empty subsets of $\{P_1, P_2, \ldots, P_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}} \setminus \{\emptyset\}$. The sets in $\mathbb{A}$ are called authorized sets, while the sets not in $\mathbb{A}$ are called unauthorized sets.

In our construction, the attributes play the role of the parties and we only focus on the monotone access structures. Nevertheless, in our scheme, it is also possible to (inefficiently) realize general access structures by enclosing the negation of an attribute as a new separate attribute.

2.2 Linear secret sharing schemes

Definition 2 (Linear secret-sharing schemes (LSSS) [26]). A secret-sharing scheme Π over a set of parties P is called linear over Z_p if

(1) The shares of a secret $s \in Z_p$ for each party form a vector over Z_p.

(2) There exists a matrix $A \in Z_p^{l \times n}$ called the share-generating matrix for Π. For $i = 1, \ldots, l$, the i-th row of A is labeled by a party $\rho(i)$. When we consider the column vector $v = (s, r_2, \ldots, r_n)^{\mathrm{T}}$, where $r_2, \ldots, r_n \in Z_p$ are randomly chosen, then the vector of l shares of the secret s according to Π is equal to Av. The share $(Av)_i$ belongs to party $\rho(i)$.

According to [26], the linear secret-sharing scheme enjoys the linear reconstruction property. To be specific, let Π be an LSSS for the access structure $\mathbb{A}$ and let $S \in \mathbb{A}$ be an authorized set. We define $I \subset \{1, 2, \ldots, l\}$ as $I = \{i : \rho(i) \in S\}$. Then, for any valid shares $\{\lambda_i\}$ of a secret s according to Π, there exist constants $\{\omega_i \in Z_p\}_{i \in I}$ such that $\sum_{i \in I} \omega_i \lambda_i = s$. Note that no such constants exist for any unauthorized sets. In our construction, the pair (A, ρ) denotes the policy of the access structure $\mathbb{A}$.

2.3 Bilinear groups and complexity assumptions

We will construct our scheme in prime order bilinear groups and prove its security based on two q-type assumptions in prime order bilinear groups.

Let G and G_T be cyclic groups of prime order p, and let g be a generator of G. The bilinear map $e : G \times G \longrightarrow G_T$ is a map such that

(1) Bilinear: $\forall u, v \in G, a, b \in Z_p, e(u^a, v^b) = e(u, v)^{ab}$;

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

We say that G is a prime order bilinear group if the bilinear map $e : G \times G \longrightarrow G_T$ as well as the group operations in G are both efficiently computable.

Definition 3 (Strong Diffie-Hellman assumption [27])**.** Let G be a cyclic group of order p and g be a generator of G. The q-strong Diffie-Hellman (q-SDH) problem in group G is stated as follows: Choose a random $x \in Z_p^*$, given a $q+1$-tuple $(g, g^x, g^{x^2}, \ldots, g^{x^q})$, compute a pair $(c, g^{\frac{1}{x+c}})$ where $c \in Z_p^*$.

An algorithm $\mathscr{A}$ solves the the q-SDH problem in group G with advantage ϵ if

$$\Pr\left[\mathscr{A}\left(g, g^x, g^{x^2}, \ldots, g^{x^q}\right) = \left(c, g^{\frac{1}{x+c}}\right)\right] \geqslant \epsilon.$$

We say that the q-SDH assumption holds in G if no polynomial time algorithm has a non-negligible advantage in solving the q-SDH problem in G.

Definition 4 (Decisional parallel bilinear Diffie-Hellman exponent 2 assumption [18])**.** Let G be a bilinear group of order p and g be a generator of G. The q-decisional parallel bilinear Diffie-Hellman exponent 2 (q-DPBDHE2) problem in group G is stated as follows: Choose random values $s, a, b_1, b_2, \ldots, b_q \in Z_p^*$, given

$$D = \left(p, g, G, e, g^s, \{g^{a^i}\}_{i \in [2q], i \neq q+1}, \{g^{b_j a^i}\}_{(i,j) \in [2q,q], i \neq q+1}, \{g^{\frac{s}{b_i}}\}_{i \in [q]}, \left\{g^{\frac{s a^i b_j}{b_{j'}}}\right\}_{(i,j,j') \in [q+1,q,q], j \neq j'}\right),$$

distinguish $e(g, g)^{s a^{q+1}} \in G_T$ from a random element $R \in G_T$.

An algorithm $\mathscr{A}$ solves the q-DPBDHE2 problem in group G with advantage ϵ if

$$\left|\Pr\left[\mathscr{A}\left(D, e(g, g)^{s a^{q+1}}\right) = 0\right] - \Pr[\mathscr{A}(D, R) = 0]\right| \geqslant \epsilon.$$

We say that the q-DPBDHE2 assumption holds in G if no polynomial time algorithm has a non-negligible advantage in solving the q-DPBDHE2 problem in G.

3 Definition of traceable multi-authority CP-ABE

Here we define the traceable multi-authority CP-ABE and give its security model. Further, we give the notion of traceability in multi-authority CP-ABE.

3.1 Definition

A traceable multi-authority CP-ABE scheme is composed of six algorithms: global setup, authority setup, encryption, key generation, decryption, and tracing.

Global setup(λ). The global setup algorithm takes in a security parameter λ and outputs the global parameters GP.

Authority setup(GP). Each authority θ calls the authority setup algorithm with GP as input, and produces its public key PK_θ and secret key SK_θ.

Encrypt$(\mathrm{GP}, \{\mathrm{PK}_\theta\}, M, (A, \rho))$. The encryption algorithm takes as input the global parameters GP, the set of public keys $\{\mathrm{PK}_\theta\}$ for the relevant authorities, a message M, and an access policy (A, ρ). It will output a ciphertext CT that can only be decrypted by users whose attributes satisfy the access policy (A, ρ).

KeyGen$(\mathrm{GID}, S, \{\mathrm{SK}_\theta\}, \mathrm{GP})$. The key generation algorithm takes as input a user's identity GID, the user's attribute set S, the set of secret keys $\{\mathrm{SK}_\theta\}$ for relevant authorities, and the global parameters GP. It outputs a private key $\mathrm{SK}_{S,\mathrm{GID}}$ for the user.

Decrypt$(\mathrm{GP}, \mathrm{SK}_{S,\mathrm{GID}}, \mathrm{CT})$. The decryption algorithm takes as input the global parameters GP, a private key $\mathrm{SK}_{S,\mathrm{GID}}$ for an attributes set S, and a ciphertext CT for an access policy (A, ρ). If the attribute set S satisfies the access policy (A, ρ), it outputs the message M. Otherwise, it outputs the error symbol $\perp$.

Trace$(\mathrm{GP}, \{\mathrm{PK}_\theta\}, \mathrm{SK}_{S,\mathrm{GID}})$. The tracing algorithm takes in the global parameters GP, a private key $\mathrm{SK}_{S,\mathrm{GID}}$ for a set of attributes S, and the set of public keys $\{\mathrm{PK}_\theta\}$ for relevant authorities. If $\mathrm{SK}_{S,\mathrm{GID}}$ passes the key sanity check which is defined as a deterministic algorithm, it outputs an identity GID. Otherwise, it outputs the symbol $\top$ meaning that $\mathrm{SK}_{S,\mathrm{GID}}$ does not need to be traced.

3.2 Static security

We now give a static security model for traceable multi-authority CP-ABE schemes by a security game between an adversary and a challenger. Like the ABE scheme [18], the adversary need to send all queries to the challenger immediately after seeing the global parameters. We also allow the adversary to select and corrupt several authorities for malicious attack. In our security model, an authority can manage multiple attributes, while each attribute can only be controlled by one authority. Let U_θ be the authority universe and U be the attribute universe. $T : U \to U_\Theta$ is a function that maps each attribute to the authority that controls the attribute. The formal security game is described as follows.

Setup. The challenger runs the global setup algorithm of traceable multi-authority CP-ABE and gives the global parameters GP to the adversary.

Adversary's queries. The adversary proceeds as follows:

(1) It chooses a corrupt authority set $C_\theta \subseteq U_\theta$ and sends the public keys of these corrupt authorities to the challenger.

(2) It chooses a good authority set $N_\theta \subseteq U_\theta$ and queries the public keys of these good authorities.

(3) It makes secret key queries for a sequence $\{(S_j, \mathrm{GID}_j)\}_{j=1}^m$, where GID_j is an identity and $S_j \subseteq U$ is an attributes set. In this sequence, we require that the identities $\{\mathrm{GID}_j\}$ are different and none of these keys come from a corrupt authority, i.e., $T(S_j) \cap C_\theta = \emptyset$.

(4) It specifies two equal length messages M_0, M_1 and an access structure (A, ρ) to the challenger for a challenge ciphertext. We require that for each identity GID_j, this access structure (A, ρ) cannot be satisfied by $S_{C_\theta} \cup S_j$, where S_{C_θ} is the set of all the attributes that are controlled by the corrupt authorities.

Challenger's replies. The challenger flips a random coin $\beta \in \{0, 1\}$ and gives the adversary with

(1) The public keys $\{\mathrm{PK}_\theta\}_{\theta \in N_\theta}$ corresponding to the good authorities N_θ;

(2) The secret keys $\{\mathrm{SK}_{S_j,\mathrm{GID}_j}\}_{j=1}^m$ corresponding to $\{(S_j, \mathrm{GID}_j)\}_{j=1}^m$;

(3) The challenge ciphertext $\mathrm{CT}^* \leftarrow$ **Encrypt**$(\mathrm{GP}, \{\mathrm{PK}_\theta\}, M_\beta, (A, \rho))$.

Guess. The adversary outputs a guess β' for β.

The advantage of the adversary in this game is defined as $\Pr[\beta = \beta'] - \frac{1}{2}$.

Definition 5. A traceable multi-authority CP-ABE scheme is statically secure (against static corruption of authorities) if all polynomial time adversaries have at most a negligible advantage in this security game.

3.3 Traceability

Traceability of the multi-authority CP-ABE is also described by a game between a challenger and an adversary. The formal security game is described as follows.

Setup. The challenger runs the global setup algorithm and the authority setup algorithm. It then gives the global parameters GP and the public keys $\{\mathrm{PK}_\theta\}$ to the adversary.

Key query. The adversary queries the private keys corresponding to pairs $\{(S_j, \mathrm{GID}_j)\}_{j=1}^m$, where GID_j is an identity and S_j is an attribute set. The challenger sends the corresponding private keys $\{\mathrm{SK}_{S_j,\mathrm{GID}_j}\}_{j=1}^m$ to the adversary.

Key forgery. The adversary outputs a decryption key SK^*.

The advantage of the adversary in this game is defined as

$$\Pr[\mathbf{Trace}(\mathrm{GP}, \{\mathrm{PK}_\theta\}, \mathrm{SK}^*) \notin \{\top, \mathrm{GID}_1, \ldots, \mathrm{GID}_m\}].$$

Definition 6. A traceable multi-authority CP-ABE scheme is fully traceable if all polynomial time adversaries have at most a negligible advantage in this game.

4 Our traceable multi-authority CP-ABE scheme

In this section, we construct a traceable large universe multi-authority CP-ABE scheme in a prime order bilinear group G. Inspired by [18], to realize multiple authorities and large universe, we adopt two hash functions H and F which will be viewed as the random oracles in the security proof. On one hand, the function H that maps user identities to the elements in group G allows the authorities to personalize the secret key for each user, then the scheme can achieve multiple authorities and collusion-resistance simultaneously. On the other hand, we use the function F that maps attributes to the elements in group G to achieve a large universe scheme. More specifically, as the hash function F can map any string to an element in group G, our construction can add a new attribute i into the system by embedding the group element $F(i)$ into the private key and ciphertext, unlike the small universe constructions [10,12,14], which introduce a public parameter $\mathrm{pk}_i \in G$ for attribute i. Hence, in our scheme, any string can be used as an attribute and the public parameters size does not increase with the size of the attribute universe. Afterwards, we employ the Boneh-Boyen full signature scheme [27] to realize traceability without an identity table. Finally, we prove that our scheme is statically secure and fully traceable in the random oracle model by two black-box reductions. In our scheme, the user can specify any access policy that can be expressed in terms of a linear secret-sharing scheme. Further, there is no requirement for coordination between different authorities or any central authority in our scheme.

4.1 Construction

In our construction, U is the attribute universe and U_Θ is the authority universe. For an attribute $i \in U$ which is controlled by a specific authority $\theta \in U_\Theta$, a publicly computable function $T : U \to U_\Theta$ maps the attribute i to the authority θ. For an $l \times n$ access matrix A with ρ mapping its rows to attributes, the function $\delta(\cdot) = T(\rho(\cdot))$ maps its rows to authorities. Suppose G is a bilinear group of prime order p and $e : G \times G \longrightarrow G_T$ is a bilinear map.

Global setup(λ). The algorithm first chooses a bilinear group G of prime order p. g is a generator of G and $e : G \times G \longrightarrow G_T$ is a bilinear map in G. It then chooses a hash function $H : Z_p^* \to G$ that maps user identities to elements of group G, and a hash function $F : U \to G$ that maps user attributes to elements of group G. We will view H and F as the random oracles in the security proof. The global public parameters are published as $\mathrm{GP} = \{p, G, g, H, F, U, U_\Theta, T\}$.

Authority setup(GP). Each authority $\theta \in U_\Theta$ chooses four random exponents $\alpha_\theta, y_\theta, a_\theta, b_\theta \in Z_p^*$ and computes the public key $\mathrm{PK}_\theta = \{e(g,g)^{\alpha_\theta}, g^{y_\theta}, g^{a_\theta}, g^{b_\theta}\}$. The authority θ publishes the public key PK_θ and sets $\mathrm{SK}_\theta = \{\alpha_\theta, y_\theta, a_\theta, b_\theta\}$ as its secret key.

Encrypt$(\mathrm{GP}, \{\mathrm{PK}_\theta\}, M, (A, \rho))$. Given a message M, an access policy (A, ρ), and the public keys of the relevant authorities, the algorithm first chooses two random vectors $v = (s, v_2, \ldots, v_n)^{\mathrm{T}}, \omega = (0, \omega_2, \ldots, \omega_n)^{\mathrm{T}} \in Z_p^n$. For each $x \in \{1, 2, \ldots, l\}$, it calculates $\lambda_x = A_x \cdot v$ and $\omega_x = A_x \cdot \omega$, where A_x is the x-th row of A. For each $x \in \{1, 2, \ldots, l\}$, it chooses a random $r_x \in Z_p$ and computes the ciphertext CT as

$$C_0 = Me(g,g)^s, \quad C_{1,x} = e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\delta(x)} r_x}, \quad C_{2,x} = g^{-r_x}, \quad C_{3,x} = g^{y_{\delta(x)} r_x} g^{\omega_x},$$

$$C_{4,x} = F(\rho(x))^{r_x}, \quad C_{5,x} = g^{-a_{\delta(x)} r_x}, \quad C_{6,x} = g^{-b_{\delta(x)} r_x}.$$

KeyGen$(\mathrm{GP}, \mathrm{GID}, S, \{\mathrm{SK}_\theta\})$. Given the global parameters GP, an identity $\mathrm{GID} \in Z_p^*$, an attribute set S, and the secret keys of the relevant authorities, for each $i \in S$, if $T(i) = \theta$, the authority θ chooses two random values $t \in Z_p, r \in Z_p \backslash \{-\frac{a_\theta + \mathrm{GID}}{b_\theta}\}$ and computes a key for GID for attribute i as follows:

$$\mathrm{SK}_{i,\mathrm{GID}} = \Big\{ K_{1,i,\mathrm{GID}} = g^{\frac{\alpha_\theta}{a_\theta + \mathrm{GID} + b_\theta r}} H(\mathrm{GID})^{\frac{y_\theta}{a_\theta + \mathrm{GID} + b_\theta r}} F(i)^t, K_{2,\mathrm{GID}} = \mathrm{GID},$$

$$K_{3,i,\mathrm{GID}} = r, K_{4,i,\mathrm{GID}} = g^t, K_{5,i,\mathrm{GID}} = g^{(a_\theta + b_\theta r)t} \Big\}.$$

Here, the inverses $\frac{1}{y}$ and $\frac{1}{a_\theta + \mathrm{GID} + b_\theta r}$ are computed modulo p. The private key for GID for attribute set S is set as $\mathrm{SK}_{S,\mathrm{GID}} = (K_{2,\mathrm{GID}}, \{K_{1,i,\mathrm{GID}}, K_{3,i,\mathrm{GID}}, K_{4,i,\mathrm{GID}}, K_{5,i,\mathrm{GID}}\}_{i \in S})$.

Decrypt$(\mathrm{GP}, \mathrm{CT}, \mathrm{SK}_{S,\mathrm{GID}})$. The input consist of the global parameters GP, a secret key $\mathrm{SK}_{S,\mathrm{GID}}$ for a set S, and a ciphertext $(C_0, \{C_{1,x}, C_{2,x}, C_{3,x}, C_{4,x}, C_{5,x}, C_{6,x}\}_{x \in \{1,2,\ldots,l\}})$ for an access policy (A, ρ). Let $I \subset \{1, 2, \ldots, l\}$ be defined as $I = \{x : \rho(x) \in S\}$. If S does not satisfy the access policy (A, ρ), it outputs $\perp$. Otherwise, for each $x \in I$, it first computes

$$D_x = C_{1,x} e\left(K_{1,\rho(x),\mathrm{GID}}, C_{2,x}^{K_{2,\mathrm{GID}}} C_{5,x} C_{6,x}^{K_{3,\rho(x),\mathrm{GID}}}\right) e(H(K_{2,\mathrm{GID}}), C_{3,x}) e\left(K_{4,\rho(x),\mathrm{GID}}^{K_{2,\mathrm{GID}}} K_{5,\rho(x),\mathrm{GID}}, C_{4,x}\right).$$

Then, it computes constants $\{c_x \in Z_p\}_{x \in I}$ such that $\sum_{x \in I} c_x A_x = (1, 0, \ldots, 0)$ and calculates

$$\prod_{x \in I} D_x^{c_x} = e(g,g)^s.$$

Finally, the message can be recovered as $M = C_0 / e(g,g)^s$.

Trace$(\mathrm{SK}_{S,\mathrm{GID}}, \mathrm{GP}, \{\mathrm{PK}_\theta\})$. Given a secret key $\mathrm{SK}_{S,\mathrm{GID}}$, the global parameters GP, and the public keys of the relevant authorities. If $\mathrm{SK}_{S,\mathrm{GID}}$ is not in the form of

$$\mathrm{SK}_{S,\mathrm{GID}} = (K_{2,\mathrm{GID}}, \{K_{1,i,\mathrm{GID}}, K_{3,i,\mathrm{GID}}, K_{4,i,\mathrm{GID}}, K_{5,i,\mathrm{GID}}\}_{i \in S}),$$

it outputs $\top$. Otherwise, it runs a key sanity check on $\mathrm{SK}_{S,\mathrm{GID}}$ as follows.

Key sanity check: $\exists i \in S$, s.t.

$$K_{1,i,\mathrm{GID}},\ K_{4,i,\mathrm{GID}},\ K_{5,i,\mathrm{GID}} \in G, \quad K_{2,\mathrm{GID}},\ K_{3,i,\mathrm{GID}} \in Z_p^*, \tag{1}$$

$$e(g, K_{5,i,\mathrm{GID}}) = e(K_{4,i,\mathrm{GID}}, g^{a_\theta} \cdot (g^{b_\theta})^{K_{3,i,\mathrm{GID}}}), \tag{2}$$

$$e(K_{1,i,\mathrm{GID}}, g^{a_\theta} g^{K_{2,\mathrm{GID}}} (g^{b_\theta})^{K_{3,i,\mathrm{GID}}}) = e(g,g)^{\alpha_\theta} e(H(K_{2,\mathrm{GID}}), g^{y_\theta}) e(F(i), K_{4,i,\mathrm{GID}}{}^{K_{2,\mathrm{GID}}} K_{5,i,\mathrm{GID}}), \tag{3}$$

where $\theta = T(i)$. If $\mathrm{SK}_{S,\mathrm{GID}}$ passes the key sanity check, the algorithm outputs the identity $K_{2,\mathrm{GID}}$. Otherwise, it outputs $\top$.

Correctness.

$$\begin{aligned} D_x &= C_{1,x} e\left(K_{1,\rho(x),\mathrm{GID}}, C_{2,x}^{K_{2,\mathrm{GID}}} C_{5,x} C_{6,x}^{K_{3,\rho(x),\mathrm{GID}}}\right) e(H(K_{2,\mathrm{GID}}), C_{3,x}) e\left(K_{4,\rho(x),\mathrm{GID}}^{K_{2,\mathrm{GID}}} K_{5,\rho(x),\mathrm{GID}}, C_{4,x}\right) \\ &= e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\delta(x)} r_x} e\left(g^{\frac{\alpha_{\delta(x)}}{a_{\delta(x)} + \mathrm{GID} + b_{\delta(x)} r}} H(\mathrm{GID})^{\frac{y_{\delta(x)}}{a_{\delta(x)} + \mathrm{GID} + b_{\delta(x)} r}} F(\rho(x))^t, g^{-r_x (a_{\delta(x)} + GID + b_{\delta(x)} r)}\right) \end{aligned}$$

$$\begin{aligned}
&\cdot e(H(\mathrm{GID}), g^{y_{\delta(x)} r_x} g^{\omega_x}) e(g^{t(a_{\delta(x)}+GID+b_{\delta(x)}r)}, F(\rho(x))^{r_x}) \\
&= e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\delta(x)} r_x} e(g,g)^{-\alpha_{\delta(x)} r_x} e(H(\mathrm{GID}), g)^{-y_{\delta(x)} r_x} e(g, F(\rho(x)))^{-r_x t(a_{\delta(x)}+\mathrm{GID}+b_{\delta(x)}r)} \\
&\quad \cdot e(H(\mathrm{GID}), g)^{y_{\delta(x)} r_x} e(H(\mathrm{GID}), g)^{\omega_x} e(g, F(\rho(x)))^{r_x t(a_{\delta(x)}+\mathrm{GID}+b_{\delta(x)}r)} \\
&= e(g,g)^{\lambda_x} e(H(\mathrm{GID}), g)^{\omega_x}.
\end{aligned}$$

If the attribute set S satisfies the access policy (A, ρ), we can compute constants $\{c_x \in Z_p\}_{x\in I}$ such that $\sum_{x\in I} c_x A_x = (1, 0, \ldots, 0)$. Then, we have $\sum_{x\in I} \lambda_x c_x = \sum_{x\in I} A_x \cdot v \cdot c_x = v \cdot (1, 0, \ldots, 0) = s$, $\sum_{x\in I} \omega_x c_x = \sum_{x\in I} A_x \cdot \omega \cdot c_x = \omega \cdot (1, 0, \ldots, 0) = 0$. Therefore,

$$\begin{aligned}
\prod_{x\in I} D_x^{c_x} &= \prod_{x\in I} (e(g,g)^{\lambda_x} e(H(\mathrm{GID}), g)^{\omega_x})^{c_x} \\
&= e(g,g)^{\sum_{x\in I} \lambda_x c_x} e(H(\mathrm{GID}), g)^{\sum_{x\in I} \omega_x c_x} \\
&= e(g,g)^{s}.
\end{aligned}$$

Hence, we have $C_0/(\prod_{x\in I} D_x^{c_x}) = M$.

4.2 Proof of static security

In this subsection, we will prove the static security of our scheme from the q-DPBDHE2 assumption. Before that, we firstly prove the following lemma.

Lemma 1. Our traceable multi-authority CP-ABE scheme is statically secure assuming that the Rouselakis-Waters scheme [18] is a statically secure CP-ABE scheme.

Proof. Suppose there is a polynomial-time adversary $\mathscr{A}$ that has advantage ϵ against our traceable multi-authority CP-ABE scheme in the static security game. We show how to build a simulator $\mathscr{B}$ that has advantage ϵ against the Rouselakis-Waters (RW) scheme. Let $\mathscr{C}$ be the challenger of the RW scheme.

Setup. The challenger $\mathscr{C}$ sends the global parameters $\mathrm{GP} = \{p, G, g, H, F, U, U_\Theta, T\}$ to the simulator $\mathscr{B}$. $\mathscr{B}$ passes the global parameters GP to the adversary $\mathscr{A}$.

Adversary's queries. The adversary $\mathscr{A}$ chooses a set $C_\theta \subseteq U_\theta$ of corrupt authorities and creates their corresponding public keys in the RW scheme as $\{\mathrm{PK}'_\theta\}_{\theta\in C_\theta}$. For each $\theta \in C_\theta$, $\mathscr{A}$ chooses two random exponents $a_\theta, b_\theta \in Z_p^*$ and sets the public key of corrupt authority θ in our multi-authority traceable CP-ABE scheme as $\mathrm{PK}_\theta = \{\mathrm{PK}'_\theta, g^{a_\theta}, g^{b_\theta}\}$. The adversary $\mathscr{A}$ responds to $\mathscr{B}$ with

(1) A corrupt authority set $C_\theta \subseteq U_\theta$, $\{a_\theta, b_\theta\}_{\theta\in C_\theta}$, and $\{\mathrm{PK}_\theta\}_{\theta\in C_\theta}$.

(2) A good authority set $N_\theta \subseteq U_\theta$.

(3) A sequence $\{(S_j, \mathrm{GID}_j)\}_{j=1}^m$ with the following restrictions: First, if $i \neq j$, then $\mathrm{GID}_i \neq \mathrm{GID}_j$. Second, $S_j \subseteq U$ and $T(S_j) \cap C_\theta = \emptyset$. A pair (S_j, GID_j) denotes that the adversary requests the secret key for the global identity GID_j for the attribute set S_j.

(4) The challenge access structure (A, ρ) and two messages, M_0, M_1. Let S_{C_θ} be the set of all the attributes controlled by the corrupt authorities. For each $j \in [m]$, we require that the set $S_{C_\theta} \cup S_j$ does not satisfy the access policy (A, ρ).

Challenger's replies. When the simulator $\mathscr{B}$ receives the above responds, it sends C_θ, $\{\mathrm{PK}'_\theta\}_{\theta\in C_\theta}$, N_θ, $\{(S_j, \mathrm{GID}_j)\}_{j=1}^m$, M_0, M_1 and (A, ρ) to $\mathscr{C}$ to request the corresponding public keys, secret keys, and challenge ciphertext in the RW scheme. Then, $\mathscr{C}$ replies with the public keys $\{\mathrm{PK}'_\theta = (e(g,g)^{\alpha_\theta}, g^{y_\theta})\}$ for all $\theta \in N_\theta$, the secret keys $\{\mathrm{SK}'_{S_j,\mathrm{GID}_j} = (g^{\alpha_\theta} H(\mathrm{GID}_j)^{y_\theta} F(i)^t, g^t)_{i\in S_j}\}$ for all $j \in [m]$, and the challenge ciphertext $\mathrm{CT}' = (C_0 = M_b e(g,g)^s, \{C_{1,x} = e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\delta(x)} r_x}, C_{2,x} = g^{-r_x}, C_{3,x} = g^{y_{\delta(x)} r_x} g^{\omega_x}, C_{4,x} = F(\rho(x))^{r_x}\}_{x\in\{1,2,\ldots,l\}})$. Then $\mathscr{B}$ creates the public keys, the secret keys and challenge ciphertext in our traceable multi-authority CP-ABE scheme as follows:

(1) For each $\theta \in N_\theta$, $\mathscr{B}$ chooses two random exponents $a_\theta, b_\theta \in Z_p^*$ and sets the public key as $\mathrm{PK}_\theta = \{e(g,g)^{\alpha_\theta}, g^{y_\theta}, g^{a_\theta}, g^{b_\theta}\}$.

(2) For each $j \in [m]$ and $i \in S_j$, $\mathscr{B}$ chooses a random value r. Implicitly setting $t' = \frac{t}{a_\theta + \mathrm{GID}_j + b_\theta r}$, $\mathscr{B}$ computes

$$K_{1,i,\mathrm{GID}_j} = (g^{\alpha_\theta} H(\mathrm{GID}_j)^{y_\theta} F(i)^t)^{\frac{1}{a_\theta + \mathrm{GID}_j + b_\theta r}} = g^{\frac{\alpha_\theta}{a_\theta + \mathrm{GID}_j + b_\theta r}} H(\mathrm{GID}_j)^{\frac{y_\theta}{a_\theta + \mathrm{GID}_j + b_\theta r}} F(i)^{t'},$$

$$K_{2,\mathrm{GID}_j} = \mathrm{GID}_j, \quad K_{3,i,\mathrm{GID}_j} = r, \quad K_{4,i,\mathrm{GID}_j} = (g^t)^{\frac{1}{a_\theta + \mathrm{GID}_j + b_\theta r}} = g^{t'},$$

$$K_{5,i,\mathrm{GID}_j} = K_{4,i,\mathrm{GID}_j}^{(a_\theta + b_\theta r)} = g^{(a_\theta + b_\theta r)\frac{t}{a_\theta + \mathrm{GID}_j + b_\theta r}} = g^{(a_\theta + b_\theta r)t'}.$$

In the unlikely event that $a_\theta + \mathrm{GID}_j + b_\theta r = 0$, $\mathscr{B}$ chooses another random value r and try again. Finally, $\mathscr{B}$ sets the secret key as $\mathrm{SK}_{S_j,\mathrm{GID}_j} = (K_{2,\mathrm{GID}_j}, \{K_{1,i,\mathrm{GID}_j}, K_{3,i,\mathrm{GID}_j}, K_{4,i,\mathrm{GID}_j}, K_{5,i,\mathrm{GID}_j}\}_{i \in S_j})$.

(3) For each $x \in \{1, 2, \ldots, l\}$, $\mathscr{B}$ computes $C_{5,x} = C_{2,x}^{a_{\delta(x)}} = g^{-a_{\delta(x)} r_x}$, $C_{6,x} = C_{2,x}^{b_{\delta(x)}} = g^{-b_{\delta(x)} r_x}$. $\mathscr{B}$ sets the challenge ciphertext as $\mathrm{CT} = (C_0, \{C_{1,x}, C_{2,x}, C_{3,x}, C_{4,x}, C_{5,x}, C_{6,x}\}_{x \in \{1,2,\ldots,l\}})$.

Finally, $\mathscr{B}$ sends the public keys $\{\mathrm{PK}_\theta\}_{\theta \in N_\theta}$, the secret keys $\{\mathrm{SK}_{S_j,\mathrm{GID}_j}\}_{j=1}^m$ and the challenge ciphertext CT to $\mathscr{A}$.

Guess. Eventually, $\mathscr{A}$ outputs a guess $\beta' \in \{0, 1\}$, then $\mathscr{B}$ outputs β'.

This ends the description of the simulation. Thus, if $\mathscr{A}$ can break our scheme with advantage ϵ, then $\mathscr{B}$ can break the RW scheme with the same probability.

Moreover, in [18], the following lemma has been proved.

Lemma 2 ([18])**.** If the q-DPBDHE2 assumption holds, then the Rouselakis-Waters scheme is statically secure in the random oracle model.

Theorem 1. If the q-DPBDHE2 assumption holds, then our traceable multi-authority CP-ABE scheme is statically secure in the random oracle model.

Proof. It follows directly from Lemmas 1 and 2.

4.3 Proof of traceability

In this subsection, we prove the traceability of our scheme from the q-SDH assumption. Before that, we firstly present the following lemmas.

Lemma 3. Our traceable multi-authority CP-ABE scheme is fully traceable assuming that the Boneh-Boyen full signature scheme [27] is secure against strong existential forgery under an adaptive chosen message attack.

Proof. Suppose there is a polynomial-time adversary $\mathscr{A}$ that has advantage ϵ against our traceable multi-authority CP-ABE scheme in the traceability game. We show how to build a simulator $\mathscr{B}$ that has advantage ϵ against the Boneh-Boyen full signature scheme (BB scheme) under an adaptive chosen message attack. Let $\mathscr{C}$ be the challenger of the BB scheme and U_Θ be the authority universe. For each $\theta \in U_\Theta$, Sig_θ is a BB scheme in the prime order group G; the public key of Sig_θ is $\{p, G, g, g^{a_\theta}, g^{b_\theta}\}$.

Setup. The challenger $\mathscr{C}$ sends the public keys $\{p, G, g, g^{a_\theta}, g^{b_\theta}\}_{\theta \in U_\Theta}$ to the simulator $\mathscr{B}$. For each $\theta \in U_\theta$, $\mathscr{B}$ chooses two random exponents $\alpha_\theta, y_\theta \in Z_p^*$ and sets the public key as $\mathrm{PK}_\theta = \{e(g,g)^{\alpha_\theta}, g^{y_\theta}, g^{a_\theta}, g^{b_\theta}\}$. $\mathscr{B}$ sends global parameters $\mathrm{GP} = \{p, G, g, U, U_\Theta, T\}$ and the public keys $\{\mathrm{PK}_\theta\}_{\theta \in U_\theta}$ to the adversary $\mathscr{A}$. Two random oracles H and F are controlled by $\mathscr{B}$.

Key query. The adversary $\mathscr{A}$ makes private key queries by submitting pairs $\{(S_j, \mathrm{GID}_j)\}_{j=1}^m$ to $\mathscr{B}$, where S_j is an attribute set and GID_j is an identity. $\mathscr{B}$ initializes two empty tables T_1, T_2 and answers the adversary's queries as follows:

(1) Random oracle hash $H(\mathrm{GID})$: If there is an entry $(\mathrm{GID}, t_{\mathrm{GID}}, g^{t_{\mathrm{GID}}})$ in T_1, then $\mathscr{B}$ outputs $g^{t_{\mathrm{GID}}}$. Otherwise, $\mathscr{B}$ chooses a random value $t_{\mathrm{GID}} \in Z_p^*$, records $(\mathrm{GID}, t_{\mathrm{GID}}, g^{t_{\mathrm{GID}}})$ in T_1 and outputs $g^{t_{\mathrm{GID}}}$.

(2) Random oracle hash $F(i)$: If there is an entry (i, t_i, g^{t_i}) in T_2, then $\mathscr{B}$ outputs g^{t_i}. Otherwise, $\mathscr{B}$ chooses a random value $t_i \in Z_p^*$, records (i, t_i, g^{t_i}) in T_2 and outputs g^{t_i}.

(3) Create secret key $\mathrm{SK}_{S_j,\mathrm{GID}_j}$: For each $i \in S_j$, if $i \in T^{-1}(\theta)$, $\mathscr{B}$ submits (GID_j, θ) to $\mathscr{C}$ and obtains the corresponding signature $(r, \sigma = g^{\frac{1}{a_\theta + \mathrm{GID}_j + b_\theta r}})$ where r is a random value. $\mathscr{B}$ first chooses a random value $t \in Z_p^*$ and computes

$$K_{1,i,\mathrm{GID}_j} = \sigma^{(\alpha_\theta + y_\theta t_{\mathrm{GID}_j})} (g^{t_i})^t$$

$$= g^{\frac{\alpha_\theta}{a_\theta+\mathrm{GID}_j+b_\theta r}}(g^{t_{\mathrm{GID}_j}})^{\frac{y_\theta}{a_\theta+\mathrm{GID}_j+b_\theta r}}F(i)^t$$
$$= g^{\frac{\alpha_\theta}{a_\theta+\mathrm{GID}_j+b_\theta r}}H(\mathrm{GID}_j)^{\frac{y_\theta}{a_\theta+\mathrm{GID}_j+b_\theta r}}F(i)^t.$$

Then, $\mathscr{B}$ sets $K_{2,\mathrm{GID}_j}=\mathrm{GID}_j, K_{3,i,\mathrm{GID}_j}=r, K_{4,i,\mathrm{GID}_j}=g^t, K_{5,i,\mathrm{GID}_j}=(g^{a_\theta})^r(g^{b_\theta})^{rt}=g^{(a_\theta+b_\theta r)t}$. The private key for GID_j for attribute set S_j is set as

$$\mathrm{SK}_{S_j,\mathrm{GID}_j}=(K_{2,\mathrm{GID}_j},\{K_{1,i,\mathrm{GID}_j},K_{3,i,\mathrm{GID}_j},K_{4,i,\mathrm{GID}_j},K_{5,i,\mathrm{GID}_j}\}_{i\in S}).$$

Finally, $\mathscr{B}$ sends $\{\mathrm{SK}_{S_j,\mathrm{GID}_j}\}_{j=1}^m$ to $\mathscr{A}$.

Key forgery. The adversary $\mathscr{A}$ outputs a decryption key SK^* to $\mathscr{B}$.

The adversary's advantage in this game is $\Pr[\mathbf{Trace}(\mathrm{GP},\{\mathrm{PK}_\theta\},\mathrm{SK}^*)\notin\{\top,\mathrm{GID}_1,\ldots,\mathrm{GID}_m\}]=\epsilon$. If $\mathbf{Trace}(\mathrm{GP},\{\mathrm{PK}_\theta\},\mathrm{SK}^*)\notin\{\top,\mathrm{GID}_1,\ldots,\mathrm{GID}_m\}$, it implies that the decryption key SK^* is in the form of $\mathrm{SK}^*=(K_{2,\mathrm{GID}},\{K_{1,i,\mathrm{GID}},K_{3,i,\mathrm{GID}},K_{4,i,\mathrm{GID}},K_{5,i,\mathrm{GID}}\}_{i\in S})$ and passes the key sanity check, and $K_{2,\mathrm{GID}}\notin\{\mathrm{GID}_1,\ldots,\mathrm{GID}_m\}$. Hence, $\exists i\in S$, s.t.

$$K_{1,i,\mathrm{GID}},\ K_{4,i,\mathrm{GID}},\ K_{5,i,\mathrm{GID}}\in G,\quad K_{2,\mathrm{GID}},\ K_{3,i,\mathrm{GID}}\in Z_p^*, \tag{4}$$

$$e(g,K_{5,i,\mathrm{GID}})=e(K_{4,i,\mathrm{GID}},g^{a_\theta}\cdot(g^{b_\theta})^{K_{3,i,\mathrm{GID}}}), \tag{5}$$

$$e(K_{1,i,\mathrm{GID}},g^{a_\theta}g^{K_{2,\mathrm{GID}}}(g^{b_\theta})^{K_{3,i,\mathrm{GID}}})=e(g,g)^{\alpha_\theta}e(H(K_{2,\mathrm{GID}}),g^{y_\theta})e(F(i),K_{4,i,\mathrm{GID}}{}^{K_{2,\mathrm{GID}}}K_{5,i,\mathrm{GID}}). \tag{6}$$

Without loss of generality, assuming $\mathscr{A}$ makes the random oracle hash $H(K_{2,\mathrm{GID}})$ and $F(i)$, before outputting the above forgery key SK^* that passes the key sanity check. Assuming $K_{4,i,\mathrm{GID}}=g^{t_4}$ where $t_4\in Z_p$ is unknown. $\mathscr{B}$ obtains the record $(K_{2,\mathrm{GID}},t_{K_{2,\mathrm{GID}}},g^{tK_{2,\mathrm{GID}}})$ from T_1, and the record (i,t_i,g^{t_i}) from T_2. From (5), we have $K_{5,i,\mathrm{GID}}=g^{(a_\theta+b_\theta K_{3,i,\mathrm{GID}})t_4}$. From (6), we have

$$K_{1,i,\mathrm{GID}_j}=g^{\frac{\alpha_\theta+y_\theta tK_{2,\mathrm{GID}}+t_it_4(a_\theta+K_{2,\mathrm{GID}}+b_\theta K_{3,i,\mathrm{GID}})}{a_\theta+K_{2,\mathrm{GID}}+b_\theta K_{3,i,\mathrm{GID}}}}$$
$$=g^{\frac{\alpha_\theta+y_\theta tK_{2,\mathrm{GID}}}{a_\theta+K_{2,\mathrm{GID}}+b_\theta K_{3,i,\mathrm{GID}}}}g^{t_it_4}$$
$$=g^{\frac{\alpha_\theta+y_\theta tK_{2,\mathrm{GID}}}{a_\theta+K_{2,\mathrm{GID}}+b_\theta K_{3,i,\mathrm{GID}}}}K_{4,i,\mathrm{GID}}{}^{t_i}.$$

Then, $\mathscr{B}$ computes

$$\sigma_\theta=\left(\frac{K_{1,i,\mathrm{GID}_j}}{K_{4,i,\mathrm{GID}}{}^{t_i}}\right)^{\frac{1}{\alpha_\theta+y_\theta tK_{2,\mathrm{GID}}}}=g^{\frac{1}{a_\theta+K_{2,\mathrm{GID}}+b_\theta K_{3,i,\mathrm{GID}}}}.$$

Note that $K_{2,\mathrm{GID}},K_{3,i,\mathrm{GID}}\in Z_p^*$, hence $(\sigma_\theta,K_{3,i,\mathrm{GID}})$ is a valid signature on message $K_{2,\mathrm{GID}}$ in the BB scheme Sig_θ. From $K_{2,\mathrm{GID}}\notin\{\mathrm{GID}_1,\ldots,\mathrm{GID}_m\}$, we know $\mathscr{B}$ has never queried a signature on message $K_{2,\mathrm{GID}}$, then $\mathscr{B}$ breaks the BB scheme with advantage ϵ.

From [27], we have another lemma as follows.

Lemma 4 ([27])**.** If the q-SDH assumption holds in G, then the Boneh-Boyen full signature scheme is secure against strong existential forgery under an adaptive chosen message attack.

Theorem 2. If the q-SDH assumption holds in G, then our traceable multi-authority CP-ABE scheme is fully traceable.

Proof. It follows directly from Lemmas 3 and 4.

5 Efficiency analysis

Table 2 summarizes the efficiency of our multi-authority CP-ABE scheme with other two traceable multi-authority CP-ABE schemes [10,12]. We denote by $|U|$ the size of the attribute universe, by $|U_\Theta|$ ($|U_\Theta|\ll|U|$) the number of attribute authorities, by l an LSSS access structure with an $l\times n$ matrix, by $|S|$ the number of attributes in the user's key, and by $|I|$ ($|I|\leqslant l$) the number of rows used in decryption.

Table 2 Efficiency summary of traceable multi-authority CP-ABE results

	Ref. [10]	Ref. [12]	This paper
Public key size	$3\|U\| + \|U_\Theta\| + 3\rho + 4$	$\|U\| + D(\|U_\Theta\| + 3)$	$4\|U_\Theta\|$
Private key size	$3\|S\| + 3\rho$	$\|S\| + D(\|U_\Theta\| + 5)$	$4\|S\| + 1$
Ciphertext size	$2\|U\| + 4\rho + 2$	$2l + D + 2$	$6l + 1$
Pairing operations for decryption	$3\|S\| + 3\rho$	$4\|I\| + D + 2$	$3\|I\|$
Identity tables for tracing	0	D	0
In prime order groups	✓	×	✓

In [10], the scheme defines a parameter ρ, which is the bit length of the user identity. D is the number of central authorities in [12]. The public key, private key, and ciphertext sizes are given in terms of the number of group elements, pairing operations for decryption in terms of the number of pairing operations in decryption, and identity tables for tracing in terms of the number of identity tables in the scheme.

We observe from Table 2 that the public key size in our scheme only grows linearly with the number of attribute authorities, whereas the public key size in [10, 12] grows linearly with the size of the attribute universe. In the multi-authority CP-ABE scheme, each authority is in charge of a disjoint attribute set, so the public key size in our scheme is significantly shorter than that in [10, 12]. Note that in [10], the scheme requires coordination between the authorities, the ciphertext policy is limited to "AND gates with wildcard", and the ciphertext size grows linearly with the size of the attribute universe. This makes the scheme in [10] less practical than the schemes in [12] and this paper.

From Table 2, we also observe our scheme is constructed in prime order groups, whereas the scheme in [12] is constructed in composite order groups. Note that the pairing operation in prime order groups is 1–2 orders of magnitude faster than that in composite order groups, hence, our scheme is significantly faster than the scheme in [12]. The timings in prime and composite order groups exhibits a significant gap, which has been discussed in detail in [18]. Furthermore, the storage overhead in [12] is greater than that in our scheme because each central authority in [12] must manage an identity table for tracing.

6 Conclusion

In this paper, we presented an efficient large universe multi-authority CP-ABE with white-box traceability in the prime order groups. In our construction, the ciphertext polices can be expressed as any monotone access structures and the malicious user who discloses his secret key to others can be identified by the tracing algorithm. The efficiency analysis results confirm that the proposed scheme is more efficient than other traceable multi-authority CP-ABE schemes. In addition, our construction supports large universe and does not require a central authority, which makes the proposed scheme more flexible and practical.

Acknowledgements This work was supported by National High Technology Research and Development Program of China (863 Program) (Grant No. 2015AA016007), Fundamental Research Funds for the Central Universities (Grant No. BDZ011402), China 111 Project (Grant No. B16037), and National Natural Science Foundation of China (Grant Nos. U1405255, 61472310).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Sahai A, Waters B. Fuzzy identity-based encryption. In: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 457–473
2 Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, 2006. 89–98
3 Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute based encryption. In: Proceedings of the 28th IEEE Symposium on Security and Privacy, Berkeley, 2007. 321–334
4 Cheung L, Newport C. Provably secure ciphertext policy ABE. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, 2007. 456–465

5 Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, 2007. 195–203

6 Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco and Nice, 2010. 62–91

7 Okamoto T, Takashima K. Fully secure functional encryption with general relations from the decisional linear assumption. In: Proceedings of the 30th International Cryptology Conference, Santa Barbara, 2010. 191–208

8 Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, 2011. 53–70

9 Chase M. Multi-authority attribute based encryption. In: Proceedings of the 4th Theory of Cryptography Conference, Amsterdam, 2007. 515–534

10 Li J, Huang Q, Chen X, et al. Multi-authority ciphertext-policy attribute-based encryption with accountability. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, 2011. 386–390

11 Liu Z, Cao Z, Wong D. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Trans Inf Foren Secur, 2013, 8: 76–88

12 Zhou J, Cao Z, Dong X, et al. TR-MABE: white-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems. In: Proceedings of the IEEE Conference on Computer Communications, Hong Kong, 2015. 2398–2406

13 Chase M, Chow S S M. Improving privacy and security in multi-authority attribute-based encryption. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, 2009. 121–130

14 Lewko A, Waters B. Decentralizing attribute-based encryption. In: Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, 2011. 568–588

15 Ying Z B, Li H, Ma J F, et al. Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating. Sci China Inf Sci, 2016, 59: 042701

16 Lewko A, Waters B. Unbounded HIBE and attribute-based encryption. In: Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, 2011. 547–567

17 Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption. In: Proceedings of the 20th ACM Conference on Computer and Communications Security, Berlin, 2013. 463–474

18 Rouselakis Y, Waters B. Efficient statically-secure large-universe multi-authority attribute-based encryption. In: Financial Cryptography and Data Security. Berlin: Springer, 2015. 315–332

19 Hinek M J, Jiang S, Safavi-Naini R, et al. Attribute-based encryption without key cloning. Int J Appl Cryptogr, 2012, 2: 250–270

20 Ning J, Dong X, Cao Z, et al. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. IEEE Trans Inf Foren Secur, 2015, 10: 1274–1288

21 Ning J, Dong X, Cao Z, et al. Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In: Proceedings of the European Symposium on Research in Computer Security, Vienna, 2015. 270–289

22 Liu Z, Cao Z, Wong D S. Traceable CP-ABE: how to trace decryption devices found in the wild. IEEE Trans Inf Foren Secur, 2015, 10: 55–68

23 Li J, Ren K, Kim K. A2BE: accountable attribute-based encryption for abuse free access control. Cryptology ePrint Archive, Report 2009/118, 2009. https://eprint.iacr.org/2009/118

24 Wang Y T, Chen K F, Long Y, et al. Accountable authority key policy attribute-based encryption. Sci China Inf Sci, 2012, 55: 1631–1638

25 Ning J T, Cao Z F, Dong X L, et al. Traceable and revocable CP-ABE with shorter ciphertexts. Sci China Inf Sci, 2016, 59: 119102

26 Beimel A. Secure schemes for secret sharing and key distribution. Dissertation for Ph.D. Degree. Haifa: Technion-Israel Institute of Technology, 1996

27 Boneh D, Boyen X. Short signatures without random oracles and the SDH assumption in bilinear groups. J Crypt, 2008, 21: 149–177