J Ambient Intell Human Comput (2018) 9:1039–1048
DOI 10.1007/s12652-017-0509-1

ORIGINAL RESEARCH

Efficient and privacy-aware attribute-based data sharing in mobile cloud computing

Yinghui Zhang[1,2,3] · **Axin Wu**[1,3] · **Dong Zheng**[1,3]

Received: 13 March 2017 / Accepted: 18 May 2017 / Published online: 30 May 2017

Abstract In the era of cloud computing, it is convenient to share large-scale data among various kinds of users. As a kind of attribute-based encryption, ciphertext-policy attribute-based encryption (CP-ABE) is a potential technique for realizing fine-grained access control on shared data. However, traditional CP-ABE is not suitable for mobile cloud computing, where mobile users are resource-limited and privacy is fragile. In this paper, we propose an efficient and privacy-aware attribute-based data sharing system supporting offline key generation and offline encryption. In the proposed system, sensitive attribute values specified in an access structure are not explicitly sent along with a ciphertext. The online/offline encryption mechanism alleviates the computational burden of mobile users by performing most of encryption tasks without draining the battery. In addition, the online/offline key generation mechanism allows the attribute authority to finish most of operations in the key generation process in advance, which enables efficient mobile user registration. Finally, the proposed system is proven fully secure in the standard model and performance analysis shows its effectiveness in mobile cloud computing.

Keywords Cloud computing · Attribute-based encryption · Privacy · Offline computation · Data sharing

1 Introduction

The past decade has witnessed a rapid development of computing paradigm technologies. A large number of people have uploaded their various types of data, including the highly sensitive data, into third-party cloud platforms either for ease of sharing or for cost saving. Recently, the combination of cloud computing and wireless communication technologies together with mobile devices has significantly promoted the development of mobile cloud computing, which can provide users with attractive services any time and any where. Nevertheless, data security and privacy concerns have been the biggest obstacles that hamper the widespread adoption of mobile cloud computing.

To address this challenge, a promising public key primitive, attribute-based encryption (ABE), can be adopted. The concept of ABE was proposed by Sahai and Waters (2005), in which scalable and fine-grained access rights can be assigned to individual users. ABE are categorized into Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) by Goyal et al. (2006). In a CP-ABE scheme, each user can apply for a secret key by submitting his/her attributes to the attribute authority. During the encryption phase, the data owner first specifies an access structure and then encrypts the message with respect to the access structure. A successful decryption can be done only if the attributes associated the secret key satisfy the access structure.

A preliminary version of this paper appears in BWCCA 2016.

✉ Yinghui Zhang
yhzhaang@163.com

Axin Wu
waxinsec@163.com

Dong Zheng
zhengdong@xupt.edu.cn

[1] National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, People's Republic of China

[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, People's Republic of China

[3] Westone Cryptologic Research Center, Beijing 100070, People's Republic of China

CP-ABE is more suitable for realizing outsourced data security in cloud computing in that it puts access decisions in the hands of data owners. However, traditional CP-ABE schemes cannot be directly used in mobile cloud computing environment. In mobile cloud computing, there exists several special security and efficiency requirements. For one thing, privacy issues need more attentions because mobility promotes frequent interactions between different users. For another, mobile users are usually resource-constrained and they cannot take expensive cryptographic operations. Thirdly, concurrent registration requests of large volume of users bring forward higher requirements on the attribute authority. On the other hand, traditional attribute-based data sharing systems cannot preserver users' attribute privacy because the sensitive access structure is sent along with ciphertexts explicitly. Besides, the key generation phase, the encryption phase and the decryption phase involve a large number of computation tasks. To the best of the authors' knowledge, most of existing data sharing systems based on CP-ABE schemes either suffer privacy disclosure or bad efficiency.

Our contributions

The contributions of this paper can be summarized as follows.

- Aiming to realize fine-grained data sharing in mobile cloud computing, we propose an efficient and privacy-aware attribute-based data sharing system supporting offline key generation and offline encryption. In the proposed system, the computation tasks required in the key generation process and the encryption phase are split into an offline phase and an online phase. In the offline phase, the attribute authority can finish the majority of the work to issue attribute secret keys before knowing users' attributes. The mobile data owner does most of the computation tasks in encryption without needing the message and the access structure. Furthermore, the online phase can easily assemble the final secret key and ciphertexts once related specifications become known. In particular, the proposed scheme preserve users' attribute privacy by hiding the attribute values specified in the access structure in ciphertexts.
- The proposed attribute-based data sharing system is proven semantically secure in the standard model. Specifically, it is fully secure under four assumptions. Our scheme allows any monotonic access structures encoded in a linear secret sharing scheme. Performance analysis indicates that the proposed system is suitable for data sharing in mobile cloud computing.

2 Related work

Since the introduction of ABE by Sahai and Waters (2005), a plenty of researches have been done on various ABE schemes. Goyal et al. (2006) presented a KP-ABE scheme by generating the private key according to the monotonic access structures. The first CP-ABE scheme was proposed by Bethencourt et al. (2007), which is proven secure in the generic group model. Based on this scheme, Wang and Li (2013) proposed an attribute-based signature scheme. To improve the security proof, Cheung and Newport (2007) proposed another CP-ABE construction and proved its security in the standard model. The construction supports the access structures of AND gate on different attributes. In addition, applications of ABE have been studied (Zhu and Yang 2015).

Although ABE can be directly adopted to enable secure data sharing, there is an increasing need to preserve users' attribute privacy in mobile cloud computing environment. In order to tackle this issue, anonymous ABE was introduced by Kapadia et al. (2007). Kapadia et al. (2007) realized hidden AND gate policies with positive and negative attributes, but it is not collusion-resistant. Based on the technique of hidden vector encryption, Boneh and Waters (2007) proposed a predicate encryption scheme, which can realize anonymous CP-ABE by using the opposite semantics of subset predicates. An inner product predicate encryption scheme was presented by Katz et al. (2008). Based on this predicate scheme, we can achieve hidden CP-ABE schemes. A more efficient anonymous CP-ABE scheme was constructed by Nishide et al. (2008). The security was based on the decisional bilinear Diffie–Hellman assumption and the decision linear assumption. Li et al. (2009) proposed an accountable anonymous CP-ABE scheme. To achieve full security and expressiveness, an anonymous CP-ABE scheme under new assumptions was proposed by Lai et al. (2012). Park and Chung (2014) realized attribute privacy protection by combining security policy publication service and ABE. There are many other researches on anonymous ABE (Zhang et al. 2013; Lai et al. 2011; Rao and Dutta 2015; Jung et al. 2015; Zhang et al. 2016a, 2017; Phuong et al. 2016).

To improve the efficiency of ABE, online/offline ABE schemes have recently been presented by Hohenberger and Waters (2014). The idea of online/offline was initiated by Even et al. (1996) for digital signatures. An online/offline signature scheme consists of two phases and it can efficiently enables handover authentication in wireless networks (Zhang et al. 2014). Before the message to be signed is known, the first offline phase is performed. To solve the key exposure problem, a special double-trapdoor hash family was proposed by Chen et al. (2007), and they applied the hash-sign-switch paradigm to propose a much more

efficient generic online/offline signature scheme (Chen et al. 2008). The technique of online/offline encryption was introduced by Guo et al. (2008). The first fully secure online/offline predicate encryption and attribute-based encryption schemes have recently been presented by Datta et al. (2015), in which only the online/offline encryption is considered. There are many other ABE constructions, such as ABE with outsourced decryption (Green et al. 2011; Li et al. 2014; Lai et al. 2013), constant-size ABE (Zhang et al. 2016b) and full security (Lewko et al. 2010; Lewko and Waters 2012). As far as the authors' knowledge, no ABE schemes can simultaneously support attribute privacy protection and offline key generation and encryption mechanisms.

Organization

The remaining of this work is organized as follows. We first review some preliminaries in Sect. 3. In Sect. 4, we present the system architecture and security model. The proposed privacy-aware attribute-based data sharing system is given in Sect. 5. In Sect. 6, security results and performance analysis are presented. We draw our conclusions in Sect. 7.

3 Preliminaries

In this section, we give a brief review on some cryptographic background and access structures.

3.1 Cryptographic background

Definition 1 (*Composite order bilinear groups*) Composite order bilinear groups are widely used in IBE and ABE systems, which are first introduced by Boneh et al. (2005). We denote by $\mathcal{G}$ a group generator, which takes a security parameter λ as inputs and outputs a description of a bilinear group $\mathbb{G}$. We define the output of $\mathcal{G}$ as $(p_1, p_2, p_3, p_4, \mathbb{G}, \mathbb{G}_T, \hat{e})$, where p_1, p_2, p_3, p_4 are distinct primes, $\mathbb{G}$ and $\mathbb{G}_T$ are two cyclic groups of order $N = p_1p_2p_3p_4$, and $\hat{e}: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear map satisfying:

1. Bilinear: $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$ for all $a, b \in \mathbb{Z}_N$ and $g, h \in \mathbb{G}$.
2. Non-degenerate: There exists $g \in \mathbb{G}$ such that $\hat{e}(g, g)$ has order N in $\mathbb{G}_T$.

Assume that group operations in $\mathbb{G}$ and $\mathbb{G}_T$ as well as the bilinear map $\hat{e}$ are computable in polynomial time with respect to λ. Let $\mathbb{G}_{p_i}$ be the subgroup of order p_i in $\mathbb{G}$ for $1 \le i \le 4$. Note that for any $X_i \in \mathbb{G}_{p_i}$ and $X_j \in \mathbb{G}_{p_j}$, $\hat{e}(X_i, X_j) = 1$ holds for $i \ne j$.

Assumption 1 Given a group generator $\mathcal{G}$, define the following distribution:

$$
\begin{aligned}
&(N = p_1p_2p_3p_4, \mathbb{G}, \mathbb{G}_T, \hat{e}) \xleftarrow{R} \mathcal{G} \\
&g \xleftarrow{R} \mathbb{G}_{p_1}, X_3 \xleftarrow{R} \mathbb{G}_{p_3}, X_4 \xleftarrow{R} \mathbb{G}_{p_4}, \\
&D = (N, \mathbb{G}, \mathbb{G}_T, \hat{e}, g, X_3, X_4), \\
&T_1 \xleftarrow{R} \mathbb{G}_{p_1p_2}, T_2 \xleftarrow{R} \mathbb{G}_{p_1}.
\end{aligned}
$$

The advantage of an algorithm $\mathcal{A}$ in breaking this assumption is defined to be: $\mathsf{Adv1}_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|$.

Definition 2 We say that $\mathcal{G}$ satisfies Assumption 1 if $\mathsf{Adv1}_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any probabilistic polynomial time (PPT) algorithm $\mathcal{A}$.

Assumption 2 Given a group generator $\mathcal{G}$, define the following distribution:

$$
\begin{aligned}
&(N = p_1p_2p_3p_4, \mathbb{G}, \mathbb{G}_T, \hat{e}) \xleftarrow{R} \mathcal{G} \\
&g, X_1 \xleftarrow{R} \mathbb{G}_{p_1}, X_2, Y_2 \xleftarrow{R} \mathbb{G}_{p_2}, X_3, Y_3 \xleftarrow{R} \mathbb{G}_{p_3}, X_4 \xleftarrow{R} \mathbb{G}_{p_4}, \\
&D = (N, \mathbb{G}, \mathbb{G}_T, \hat{e}, g, X_1X_2, Y_2Y_3, X_3, X_4), \\
&T_1 \xleftarrow{R} \mathbb{G}_{p_1p_2p_3}, T_2 \xleftarrow{R} \mathbb{G}_{p_1p_3}.
\end{aligned}
$$

The advantage of an algorithm $\mathcal{A}$ in breaking this assumption is defined to be: $\mathsf{Adv2}_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|$.

Definition 3 We say that $\mathcal{G}$ satisfies Assumption 2 if $\mathsf{Adv2}_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$.

Assumption 3 Given a group generator $\mathcal{G}$, define the following distribution:

$$
\begin{aligned}
&(N = p_1p_2p_3p_4, \mathbb{G}, \mathbb{G}_T, \hat{e}) \xleftarrow{R} \mathcal{G}, \alpha, s \xleftarrow{R} \mathbb{Z}_N \\
&g \xleftarrow{R} \mathbb{G}_{p_1}, g_2, X_2, Y_2 \xleftarrow{R} \mathbb{G}_{p_2}, X_3 \xleftarrow{R} \mathbb{G}_{p_3}, X_4 \xleftarrow{R} \mathbb{G}_{p_4}, \\
&D = (N, \mathbb{G}, \mathbb{G}_T, \hat{e}, g, g_2, g^{\alpha}X_2, g^{s}Y_2, X_3, X_4), \\
&T_1 = \hat{e}(g, g)^{\alpha s}, T_2 \xleftarrow{R} \mathbb{G}_T.
\end{aligned}
$$

The advantage of an algorithm $\mathcal{A}$ in breaking this assumption is defined to be: $\mathsf{Adv3}_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|$.

Definition 4 We say that $\mathcal{G}$ satisfies Assumption 3 if $\mathsf{Adv3}_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$.

Assumption 4 Given a group generator $\mathcal{G}$, define the following distribution:

$$(N = p_1p_2p_3p_4, \mathbb{G}, \mathbb{G}_T, \hat{e}) \xleftarrow{R} \mathcal{G}, t', r' \xleftarrow{R} \mathbb{Z}_N$$
$$g, h \xleftarrow{R} \mathbb{G}_{p_1}, g_2, X_2, A_2, B_2, D_2 \xleftarrow{R} \mathbb{G}_{p_2}, X_3 \xleftarrow{R} \mathbb{G}_{p_3}, X_4, Z, A_4, D_4 \xleftarrow{R} \mathbb{G}_{p_4},$$
$$D = (N, \mathbb{G}, \mathbb{G}_T, \hat{e}, g, g_2, g^{t'}B_2, h^{t'}Y_2, X_3, X_4, hZ, g^{r'}D_2D_4),$$
$$T_1 = h^{r'}A_2A_4, T_2 \xleftarrow{R} \mathbb{G}_{p_1p_2p_4}.$$

The advantage of an algorithm $\mathcal{A}$ in breaking this assumption is defined to be: $\mathsf{Adv4}_{\mathcal{G},\mathcal{A}}(\lambda) = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|$.

Definition 5 We say that $\mathcal{G}$ satisfies Assumption 4 if $\mathsf{Adv4}_{\mathcal{G},\mathcal{A}}(\lambda)$ is a negligible function of λ for any PPT algorithm $\mathcal{A}$.

3.2 Access structures and linear secret sharing schemes

Definition 6 [*Access structures* (Beimel 1996)] Let $\mathcal{U}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\mathcal{U}}$ is monotone if $\forall B \in \mathbb{A}$ and $C \in 2^{\mathcal{U}}$: if $B \subseteq C$ then $C \in \mathbb{A}$. An access structure (resp. monotone access structure) on $\mathcal{U}$ is a collection (resp. monotone collection) $\mathbb{A}$ of non-empty subsets of $\mathcal{U}$, *i.e.*, $\mathbb{A} \subseteq 2^{\mathcal{U}} \backslash \{\emptyset\}$. The sets in $\mathbb{A}$ are called authorized sets, otherwise, the sets are called unauthorized sets.

Definition 7 Let $\mathcal{U}$ be the attribute universe, where each attribute includes two parts: attribute name and its values. Each attribute has multiple values. An LSSS can be used to represent an access structure $(\mathbf{A}, \rho)$ on $\mathcal{U}$, where $\mathbf{A}$ is an $\ell \times n$ matrix which is called the share-generating matrix and ρ maps a row of $\mathbf{A}$ into an attribute name index. An LSSS consists of two algorithms:

- **Share**$((\mathbf{A}, \rho), s)$: This algorithm is used to share a secret value s based on $\mathbf{A}$. Considering a vector $v = (s, y_2, ..., y_n)^{\mathrm{T}}$, where $s \in \mathbb{Z}_p$ is the secret to be shared and $y_2, ..., y_n \in_R \mathbb{Z}_p$, then $\lambda_x = A_x \cdot v$ is a share of the secret s which corresponding to the attribute name indexed by $\rho(x)$.
- **Reconstruction**$(\lambda_1, ..., \lambda_\ell, (M, \rho))$: This algorithm is used to reconstruct s from secret shares. Let S be any authorized set and $I = \{i | \rho(i) \in S\} \subseteq \{1, 2, ..., \ell\}$. Then there exists coefficients $\{\omega_i\}_{i \in I}$ such that $\sum_{i \in I} \omega_i A_i = (1, 0, ..., 0)$, thus we have $\sum_{i \in I} \omega_i \lambda_i = s$.

We say that $I \subseteq \{1, 2, \ldots, \ell\}$ satisfies $(\mathbf{A}, \rho)$ if there exists constants $\{\omega_i\}_{i \in I}$ such that $\sum_{i \in I} \omega_i A_i = (1, 0, ..., 0)$. A subset I of $\{1, 2, \ldots, \ell\}$ is said to be a minimum authorized set of $(\mathbf{A}, \rho)$ if I satisfies $(\mathbf{A}, \rho)$ and any $I' \subset I$ does not satisfy $(\mathbf{A}, \rho)$. We define $\mathbf{I}_{\mathbf{A},\rho}$ as the set of subsets of $\{1, 2, \ldots, \ell\}$ that are minimum authorized sets of $(\mathbf{A}, \rho)$.

Suppose a user has a secret key associated with a set of attribute name indexes I_S and the corresponding attribute value set is $S = (s_1, s_2, \ldots, s_n)$. We use $\mathbb{A} = (\mathbf{A}, \rho, T)$ to represent the adopted access structure, where $T = (t_{\rho(1)}, t_{\rho(2)}, \ldots, t_{\rho(n)})$ is the attribute value set specified by $(\mathbf{A}, \rho)$. We also say that S matches $\mathbb{A}$ if there exist an $I \subseteq \{1, 2, \ldots, \ell\}$ satisfying $(\mathbf{A}, \rho)$, $I \subseteq \{i | \rho(i) \in I_S\}$ and $s_{\rho(i)} = t_{\rho(i)}$ for each $i \in I$.

4 System architecture and security model

In this section, we first describe the system architecture of data sharing in mobile cloud computing. Then we give the specification of an anonymous CP-ABE scheme with online/offline key generation and online/offline encryption mechanisms. Finally, we give a formalized security model.

4.1 System architecture

As shown in Fig. 1, the system architecture of data sharing in mobile cloud computing consists of four entities: attribute authority, mobile cloud service provider, data owner, and data user. The attribute authority is a key entity who generates system public parameters and master keys. In particular, it manages users in the system and is fully trusted. The process of key generation is split into an offline phase and an online phase. Most of computation is accomplished in the offline phase. A data owner aims to safely store his/her data on the cloud for fine-grained sharing. Before the data is specified, the data owner can generate offline ciphertexts. When the data becomes known, the data owner can calculate final ciphertexts online without significantly draining the battery. The mobile cloud service provider is in charge of saving the ciphertext data of data owners and it consists of a lot of cloud storage servers. A data user is an entity who has an attribute secret key and intends to access data stored on the cloud.

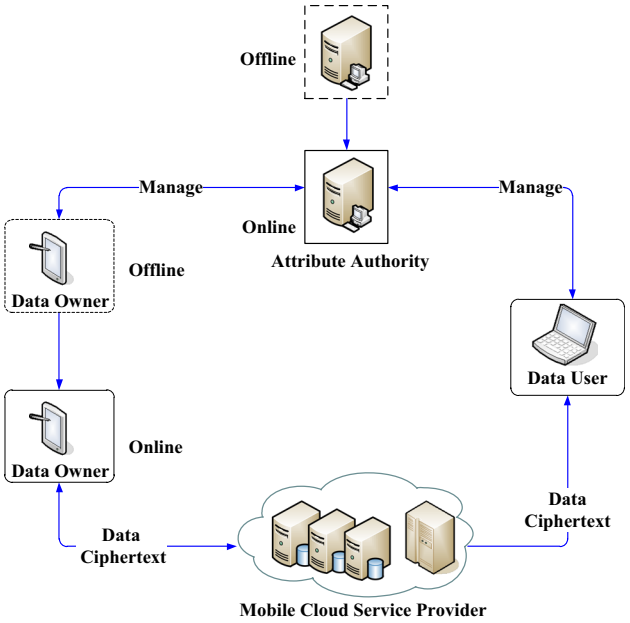

Fig. 1 System architecture of data sharing in mobile cloud computing

Before giving the formalized security model, we first lay out the definition of anonymous CP-ABE scheme with online/offline key generation and online/offline encryption mechanisms.

4.2 Definition of anonymous CP-ABE with offline key generation and offline encryption

An anonymous CP-ABE scheme with online/offline key generation and online/offline encryption mechanisms consists of six algorithms as below:

- **Setup** $(1^\lambda) \rightarrow (PK, MK)$: The setup algorithm takes as inputs the security parameter λ, and it outputs the system public key PK and the master key MK.
- **Offline.KeyGen**$(PK, MK) \rightarrow SK_{\text{off}}$: The offline key generation algorithm takes as inputs the system public key PK and the master key MK. It outputs SK_{off} as an offline key.
- **Online.KeyGen**$(PK, SK_{\text{off}}, S) \rightarrow SK_S$: Upon receiving an attribute set S, the online key generation algorithm takes as inputs the system public key PK and an offline key SK_{off}. It generates SK_S as the secret key associated with S.
- **Offline.Enc** $(PK) \rightarrow CT_{\text{off}}$: The offline encryption algorithm takes as input the system public key PK, and it generates an offline ciphertext CT_{off}.
- **Online.AnonEnc**$(PK, CT_{\text{off}}, M, \mathbb{A}) \rightarrow CT_{\mathbb{A}}$: To encrypt a message M with the access structure $\mathbb{A}$, the online anonymous encryption algorithm generates the final ciphertext $CT_{\mathbb{A}}$ based on the system public key PK and an offline ciphertext CT_{off}. It's noted that the values of attributes in $\mathbb{A}$ cannot be explicitly included in $CT_{\mathbb{A}}$ considering the requirement of anonymity.
- **AnonDec**$(PK, SK_S, CT_{\mathbb{A}}) \rightarrow M$ or $\perp$: The anonymous decryption algorithm takes as inputs the system public key PK, a secret key SK_S with respect to S and a ciphertext $CT_{\mathbb{A}}$ associated with $\mathbb{A}$ which is hidden in $CT_{\mathbb{A}}$. If S matches $\mathbb{A}$, it outputs the potential message M, and it outputs $\perp$ otherwise.

In the following, we define the indistinguishability against chosen access structure and chosen plaintext attacks in anonymous CP-ABE supporting offline key generation and offline encryption.

4.3 Security model

The formal security model is defined by a game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$.

Setup: The challenger $\mathcal{B}$ runs $(PK, MK) \leftarrow$ **Setup**(1^λ). It gives the system public key PK to $\mathcal{A}$ and keeps MK secret.

Phase 1: The adversary $\mathcal{A}$ issues a polynomially bounded number of queries to the following key generation oracle.

- $\mathcal{O}_{KeyGen}$: The adversary $\mathcal{A}$ submits an attribute set S. The challenger $\mathcal{B}$ runs $SK_{\text{off}} \leftarrow$ **Offline.KeyGen**(PK, MK) and $SK_S \leftarrow$ **Online.KeyGen**(PK, SK_{off}, S), then gives $\mathcal{A}$ the secret key SK_S for S.

Challenge: Once $\mathcal{A}$ decides that **Phase 1** is over, it submits to $\mathcal{B}$ two messages M_0, M_1 of equal length and two access structures $\mathbb{A}_1^* = (\mathbf{A}^*, \rho^*, T_0)$, $\mathbb{A}_2^* = (\mathbf{A}^*, \rho^*, T_1)$ with the restriction that $\mathbb{A}_1^*$ and $\mathbb{A}_2^*$ cannot be satisfied by any of the queried attribute sets in **Phase 1**. $\mathcal{B}$ flips a random coin $b \in \{0, 1\}$, and encrypts M_b under $\mathbb{A}$ by running $CT_{\text{off}} \leftarrow$ **Offline.Enc**(PK) and $CT_{\mathbb{A}_b^*} \leftarrow$ **Online.AnonEnc**$(PK, CT_{\text{off}}, M_b, \mathbb{A}_b^*)$. Then it sends $CT_{\mathbb{A}_b^*}$ to $\mathcal{A}$.

Phase 2: The same as **Phase 1** with the restriction that $\mathbb{A}_1^*$ and $\mathbb{A}_2^*$ cannot be satisfied by any of the queried attribute sets.

Guess: The adversary $\mathcal{A}$ outputs a guess bit $b' \in \{0,1\}$ and wins the game if $b' = b$. The advantage of an adversary $\mathcal{A}$ in the above game is defined as $\left|Pr[\,b' = b\,] - \frac{1}{2}\right|$, where the probability is taken over the random bits used by $\mathcal{A}$ and $\mathcal{B}$.

Definition 8 An anonymous CP-ABE scheme supporting offline key generation and offline encryption is semantically secure if all PPT adversaries have at most a negligible advantage in this security game.

5 Efficient and privacy-aware attribute-based data sharing in mobile cloud computing

5.1 The proposed data sharing system

5.1.1 System initialization

In the initialization phase, the attribute authority generates system public parameters and master keys by performing the following setup algorithm.

Setup(1^λ): The setup algorithm first generates $(p_1, p_2, p_3, p_4, \mathbb{G}, \mathbb{G}_T, \hat{e})$ with $\mathbb{G} = \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \mathbb{G}_{p_3} \times \mathbb{G}_{p_4}$, where p_1, p_2, p_3, p_4 are distinct primes, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $N = p_1p_2p_3p_4$, and $\hat{e}: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear map. The attribute universe is $\mathcal{U} = \{1, 2, \ldots, U\} \subseteq \mathbb{Z}_N$. Then it uniformly chooses $\alpha, a, a_1, a_2, \ldots, a_n \in_R \mathbb{Z}_N$, $g, h \in_R \mathbb{G}_{p_1}$, $X_3 \in_R \mathbb{G}_{p_3}$, $Z, X_4 \in_R \mathbb{G}_{p_4}$ and computes $Y = \hat{e}(g,g)^\alpha, H = hZ$. The system public parameters are published as

$$PK = (N, g, g^a, \{a_i\}_{1 \le i \le U}, Y, H, X_4),$$

and the master key is $MK = (\alpha, h, X_3)$.

5.1.2 Registration preparation phase

Before knowing an attribute set from users, the attribute authority generates an offline secret key based on the following algorithm, which is a preparation of the online key generation.

Offline.KeyGen(PK, MK): The offline key generation algorithm uniformly chooses $t, \hat{s}_1, \hat{s}_2, \ldots, \hat{s}_U \in_R \mathbb{Z}_N$ and $R, R', R_1, R_2, \ldots, R_U \in_R \mathbb{G}_{p_3}$. It computes $u_i = g^{a_i}$, for $1 \le i \le U$, and outputs the offline secret key $SK_{\text{off}} = (K, K', \{\hat{s}_i, K_i\}_{1 \le i \le U})$, where

$$K = g^\alpha g^{at} R,\ K' = g^t R',\ K_i = (u_i^t)^{\hat{s}_i} h^t R_i.$$

5.1.3 New user registration

Upon receiving an attribute set $S = (s_1, s_2, \ldots, s_n)$ from a user, the attribute authority performs the following online key generation algorithm for the user registration.

Online.KeyGen(PK, SK_{off}, S): Based on $SK_{\text{off}} = (S, K, K', \{\hat{s}_i, K_i\}_{1 \le i \le U})$, the online key generation algorithm outputs $SK_S = (S, K, K', \{L_i, K_i\}_{i \in I_S})$ as the final secret key associated with S, where $I_S \subseteq \{1, 2, \ldots, U\}$ is the attribute name index set corresponding to the attribute value set S, $|I_S| = n$ and $L_i = s_i - \hat{s}_i$. Without loss of generality, it is supposed that the i-th attribute name in S has attribute value s_i for simplicity of description.

5.1.4 Data sharing preparation

Before specifying an access structure, the data owner generates an offline ciphertext based on the following algorithm, which is a preparation of the online data sharing phase.

Offline.Enc (PK) The offline encryption algorithm chooses $s, s' \in_R \mathbb{Z}_N$ and $\hat{t}_k \in_R \mathbb{Z}_N$ for $1 \le k \le U$. It also uniformly chooses $\hat{\lambda}'_x, \hat{\lambda}_x, r'_x, r_x \in_R \mathbb{Z}_N$ and $Z_{0,x}, Z'_{0,x}, Z_{1,x}, Z'_{1,x} \in_R \mathbb{G}_{p_4}$, for $1 \le x \le U$. Then it calculates $u_k = g^{a_k}$ for $k \in \{1, 2, \ldots, U\}$ and sets the offline ciphertext as

$$CT_{\text{off}} = \big(\{\hat{t}_k\}_{1 \le k \le U}, s', \tilde{C}_0, \bar{C}_0, \{\hat{\lambda}'_x, C_{0,x,k}, D_{0,x}\}_{1 \le x \le U, 1 \le k \le U}, s, \hat{C}_1, \bar{C}_1, \{\hat{\lambda}_x, C_{1,x,k}, D_{1,x}\}_{1 \le x \le U, 1 \le k \le U}\big),$$

where

$$\tilde{C}_0 = Y^{s'}, \bar{C}_0 = g^{s'}, C_{0,x,k} = g^{a\hat{\lambda}'_x}(u_k^{\hat{t}_k} H)^{-r'_x} Z_{0,x}, D_{0,x} = g^{r'_x} Z'_{0,x},$$

$$\hat{C}_1 = Y^s, \bar{C}_1 = g^s, C_{1,x,k} = g^{a\hat{\lambda}_x}(u_k^{\hat{t}_k} H)^{-r_x} Z_{1,x}, D_{1,x} = g^{r_x} Z'_{1,x}.$$

5.1.5 Privacy-aware data sharing

When the access structure is specified, the data owner chooses an offline ciphertext CT_{off} and generates final online ciphertexts for online privacy-aware and fine-grained data sharing. Specifically, to encrypt a message $M \in \mathbb{G}_T$ under an access structure $\mathbb{A} = (\mathbf{A}, \rho, T)$, where $\mathbf{A}$ is an $\ell \times m$ matrix, ρ is a map from each row A_x of $\mathbf{A}$ to an attribute name index in $\{1, 2, \ldots, U\}$, and $T = (t_{\rho(1)}, t_{\rho(2)}, \ldots, t_{\rho(\ell)}) \in \mathbb{Z}_N^\ell$, the data owner performs the following algorithm. Similar to the scheme due to Lai et al. (2012), each attribute name can only be used once in an access structure. Therefore, $\ell \le U$.

Online.AnonEnc $(PK, CT_{\text{off}}, M, \mathbb{A})$: The online anonymous encryption algorithm chooses $v'_i, v_i \in_R \mathbb{Z}_N$, for $i \in \{2, 3, \ldots, m\}$, and sets $v' = (s', v'_2, \ldots, v'_m)$ and $v = (s, v_2, \ldots, v_m)$. Then, it computes $\lambda'_x = \mathbf{A}_x \cdot v', \lambda_x = \mathbf{A}_x \cdot v$, $F_{0,x} = \lambda'_x - \hat{\lambda}'_x$, $F_{1,x} = \lambda_x - \hat{\lambda}_x$, $E_{\rho(x)} = t_{\rho(x)} - \hat{t}_{\rho(x)}$, for $1 \le x \le \ell$. Finally, it sets the final ciphertext as

$$CT_{\mathbb{A}} = ((\mathbf{A}, \rho), \{E_{\rho(x)}\}_{1\le x\le \ell}, \tilde{C}_0, \bar{C}_0, \{F_{0,x}, C_{0,x}, D_{0,x}\}_{1\le x\le \ell}, \tilde{C}_1, \bar{C}_1, \{F_{1,x}, C_{1,x}, D_{1,x}\}_{1\le x\le \ell}),$$

where $\tilde{C}_1 = \hat{C}_1 \cdot M$, $C_{0,x} = C_{0,x,\rho(x)}$ and $C_{1,x} = C_{1,x,\rho(x)}$ for $1 \le x \le \ell$.

5.1.6 Privacy-aware data access

A data user downloads a ciphertext $CT_{\mathbb{A}}$ from the mobile cloud service provider, and performs the following privacy-aware decryption algorithm based on his/her secret key SK_S to recover the corresponding data.

AnonDec$(PK, SK_S, CT_{\mathbb{A}})$: Let $CT_{\mathbb{A}} = ((\mathbf{A}, \rho), \{E_{\rho(x)}\}_{1\le x\le \ell}, \tilde{C}_0, \bar{C}_0, \{F_{0,x}, C_{0,x}, D_{0,x}\}_{1\le x\le \ell}, \tilde{C}_1, \bar{C}_1, \{F_{1,x}, C_{1,x}, D_{1,x}\}_{1\le x\le \ell})$, $SK_S = (S, K, K', \{L_i, K_i\}_{i\in I_S})$ and $S = (s_1, s_2, \ldots, s_n)$. The anonymous decryption algorithm first calculates $\mathbf{I}_{\mathbf{A},\rho}$ from $(\mathbf{A}, \rho)$, where $\mathbf{I}_{\mathbf{A},\rho}$ denotes the set of minimum subsets of $\{1, 2, \ldots, \ell\}$ that satisfies $(\mathbf{A}, \rho)$. Then it checks if there exists an $I \in \mathbf{I}_{\mathbf{A},\rho}$ that satisfies

$$\tilde{C}_0 = \frac{\hat{e}(\bar{C}_0, K)}{\prod_{i\in I}\left(\hat{e}(C_{0,i}\cdot(g^a)^{F_{0,i}}\cdot D_{0,i}^{-a_{\rho(i)}E_{\rho(i)}}, K')\hat{e}(D_{0,i}, K_{\rho(i)}\cdot(K')^{a_{\rho(i)}L_{\rho(i)}})\right)^{\omega_i}}, \tag{1}$$

where $I \subseteq \{i|\rho(i) \in I_S\}$ and $\sum_{i\in I}\omega_i A_i = (1, 0, \ldots, 0)$ for some constants $\{\omega_i\}_{i\in I}$. If no such I exists, it outputs $\perp$ to indicate that S does not satisfy the hidden access structure $\mathbb{A}$. Otherwise, it returns $M = \frac{\tilde{C}_1}{E}$, where

$$E = \frac{\hat{e}(\bar{C}_1, K)}{\prod_{i\in I}\left(\hat{e}(C_{1,i}\cdot(g^a)^{F_{1,i}}\cdot D_{1,i}^{-a_{\rho(i)}E_{\rho(i)}}, K')\hat{e}(D_{1,i}, K_{\rho(i)}\cdot(K')^{a_{\rho(i)}L_{\rho(i)}})\right)^{\omega_i}}. \tag{2}$$

5.2 Consistency of the proposed data sharing system

The proposed data sharing system is correct. Obviously, we only need to show the correctness of Eq. (1) and $M = \frac{\tilde{C}_1}{E}$ based on Eq. (2). On one hand, if and only if $s_{\rho(i)} = t_{\rho(i)}$ for $i \in I$, we have

$$\begin{aligned}
&\frac{\hat{e}(\bar{C}_0, K)}{\prod_{i\in I}\left(\hat{e}(C_{0,i}\cdot(g^a)^{F_{0,i}}\cdot D_{0,i}^{-a_{\rho(i)}E_{\rho(i)}}, K')\hat{e}(D_{0,i}, K_{\rho(i)}\cdot(K')^{a_{\rho(i)}L_{\rho(i)}})\right)^{\omega_i}}\\
&= \frac{\hat{e}(\bar{C}_0, K)}{\prod_{i\in I}\left(\hat{e}((g^{a\hat{\lambda}'_i}(u_{\rho(i)}^{\hat{t}_{\rho(i)}}H)^{-r'_i}Z_{0,i})\cdot(g^a)^{\lambda'_i-\hat{\lambda}'_i}\cdot(g^{r'_i}Z'_{0,i})^{-a_{\rho(i)}(t_{\rho(i)}-\hat{t}_{\rho(i)})}, g^tR')\hat{e}(g^{r'_i}Z'_{0,i}, ((u_{\rho(i)}^t)^{\hat{s}_{\rho(i)}}h^tR_{\rho(i)})\cdot(g^tR')^{a_{\rho(i)}(s_{\rho(i)}-\hat{s}_{\rho(i)})})\right)^{\omega_i}}\\
&= \frac{\hat{e}(\bar{C}_0, K)}{\prod_{i\in I}\left(\hat{e}(g^{a\lambda'_i}(u_{\rho(i)}^{t_{\rho(i)}}H)^{-r'_i}Z_{0,i}(Z'_{0,i})^{-a_{\rho(i)}(t_{\rho(i)}-\hat{t}_{\rho(i)})}, g^tR')\hat{e}(g^{r'_i}Z'_{0,i}, (u_{\rho(i)}^t)^{s_{\rho(i)}}h^tR_{\rho(i)}(R')^{a_{\rho(i)}(s_{\rho(i)}-\hat{s}_{\rho(i)})})\right)^{\omega_i}}\\
&= \frac{\hat{e}(\bar{C}_0, K)}{\prod_{i\in I}\left(\hat{e}(g^{a\lambda'_i}(u_{\rho(i)}^{t_{\rho(i)}}h)^{-r'_i}, g^t)\hat{e}(g^{r'_i}, (u_{\rho(i)}^t)^{s_{\rho(i)}}h^t)\right)^{\omega_i}}\\
&= \frac{\hat{e}(g^{s'}, g^{\alpha}g^{at}R)}{\prod_{i\in I}\left(\hat{e}(g^{a\lambda'_i}, g^t)\right)^{\omega_i}}\\
&= \frac{\hat{e}(g^{s'}, g^{\alpha}g^{at})}{(\hat{e}(g^a, g^t))^{\sum_{i\in I}\omega_i\lambda'_i}}\\
&= \hat{e}(g, g)^{\alpha s'} = Y^{s'} = \tilde{C}_0.
\end{aligned}$$

Therefore, Eq. (1) holds. On the other hand,

$$
\begin{aligned}
&\frac{\hat{e}(\bar{C}_1, K)}{\prod_{i\in I}\left(\hat{e}(C_{1,i}\cdot(g^a)^{F_{1,i}}\cdot D_{1,i}^{-a_{\rho(i)}E_{\rho(i)}}, K')\hat{e}(D_{1,i}, K_{\rho(i)}\cdot(K')^{a_{\rho(i)}L_{\rho(i)}})\right)^{\omega_i}}\\
&= \frac{\hat{e}(\bar{C}_1, K)}{\prod_{i\in I}\left(\hat{e}((g^{a\hat{\lambda}_i}(u_{\rho(i)}^{\hat{t}_{\rho(i)}}H)^{-r_i}Z_{1,i})\cdot(g^a)^{\lambda_i-\hat{\lambda}_i}\cdot(g^{r_i}Z'_{1,i})^{-a_{\rho(i)}(t_{\rho(i)}-\hat{t}_{\rho(i)})}, g^tR')\hat{e}(g^{r_i}Z'_{1,i}, ((u_{\rho(i)}^t)^{\hat{s}_{\rho(i)}}h^tR_{\rho(i)})\cdot(g^tR')^{a_{\rho(i)}(s_{\rho(i)}-\hat{s}_{\rho(i)})})\right)^{\omega_i}}\\
&= \frac{\hat{e}(\bar{C}_1, K)}{\prod_{i\in I}\left(\hat{e}(g^{a\lambda_i}(u_{\rho(i)}^{t_{\rho(i)}}H)^{-r_i}Z_{1,i}(Z'_{1,i})^{-a_{\rho(i)}(t_{\rho(i)}-\hat{t}_{\rho(i)})}, g^tR')\hat{e}(g^{r_i}Z'_{1,i}, (u_{\rho(i)}^t)^{s_{\rho(i)}}h^tR_{\rho(i)}(R')^{a_{\rho(i)}(s_{\rho(i)}-\hat{s}_{\rho(i)})})\right)^{\omega_i}}\\
&= \frac{\hat{e}(\bar{C}_1, K)}{\prod_{i\in I}\left(\hat{e}(g^{a\lambda_i}(u_{\rho(i)}^{t_{\rho(i)}}h)^{-r_i}, g^t)\hat{e}(g^{r_i}Z'_{1,i}, (u_{\rho(i)}^t)^{s_{\rho(i)}}h^t\right)^{\omega_i}}\\
&= \frac{\hat{e}(g^s, g^\alpha g^{at}R)}{\prod_{i\in I}\left(\hat{e}(g^{a\lambda_i}, g^t)\right)^{\omega_i}}\\
&= \frac{\hat{e}(g^s, g^\alpha g^{at})}{(\hat{e}(g^a, g^t))^{\sum_{i\in I}\omega_i\lambda_i}}\\
&= \hat{e}(g,g)^{\alpha s} = Y^s,
\end{aligned}
$$

and hence $\frac{\tilde{C}_1}{E} = \frac{\hat{C}_1\cdot M}{E} = \frac{Y^s\cdot M}{Y^s} = M$ based on Eq. (2).

6 Analysis of the proposed system

6.1 Security analysis

Theorem 1 *If assumptions 1, 2, 3 and 4 hold, then the proposed privacy-aware attribute-based data sharing system supporting offline key generation and offline encryption is secure.*

Proof Because the proposed attribute-based data sharing system is based on an anonymous CP-ABE scheme supporting offline key generation and offline encryption, we just need to show the security of the proposed anonymous CP-ABE scheme. The proposed anonymous CP-ABE scheme $\Pi = (\mathsf{Setup}, \mathsf{Offline.KeyGen}, \mathsf{Online.KeyGen}, \mathsf{Offline.Enc}, \mathsf{Online.AnonEnc}, \mathsf{AnonDec})$ is an improved version of the scheme due to Lai et al. (2012), denoted by $\Pi_o = (\mathsf{Setup}_o, \mathsf{KeyGen}_o, \mathsf{Encrypt}_o, \mathsf{Decrypt}_o)$. Because the scheme Π_o is secure under Assumptions 1, 2, 3 and 4, if we can reduce the security of Π to that of Π_o, then the proposed scheme is secure in the proposed security model under Assumptions 1, 2, 3 and 4. Suppose there exists a PPT attacker $\mathcal{A}$ with a non-negligible advantage ϵ in the proposed security game against Π. We show how to design a PPT simulator $\mathcal{B}$, which can break the security of Π_o with an advantage ϵ.

Setup: It is noted that, in the security analysis of Π_o, the challenger of Π_o randomly chooses $a_i \in \mathbb{Z}_N$ to generate the pubic parameter $u_i = g^{a_i}$ for each $1 \le i \le U$. Therefore, it is feasible to replace the public parameter u_i in Π_o with a_i and g^{a_i} is used for computation, which is same as our proposed scheme. Hence, we suppose the challenger $\mathcal{B}$ receives public parameters $PK = (N, g, g^a, \{a_i\}_{1\le i\le U}, Y, H, X_4)$ from the challenger of Π_o. Then, $\mathcal{B}$ sends PK to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ makes key generation queries.

– $\mathcal{O}_{KeyGen}(S)$: $\mathcal{A}$ submits an attribute set S to $\mathcal{B}$. $\mathcal{B}$ just passes S to the challenger of Π_o and obtains the secret key $SK_o = (S, K, K', \{K_i^o\}_{i\in I_S})$. Then, $\mathcal{B}$ chooses $L_i \in_R \mathbb{Z}_N$, computes $K_i = K_i^o \cdot (K')^{-a_i L_i}$ and gives $\mathcal{A}$ the secret key $SK_S = (S, K, K', \{L_i, K_i\}_{i\in I_S})$.

Challenge: The adversary $\mathcal{A}$ submits to $\mathcal{B}$ two messages M_0, M_1 of equal length and two access structures $\mathbb{A}_0^* = (\mathbf{A}^*, \rho^*, T_0)$, $\mathbb{A}_1^* = (\mathbf{A}^*, \rho^*, T_1)$ with the restriction that $\mathbb{A}_0^*$ and $\mathbb{A}_1^*$ cannot be satisfied by any of the queried attribute sets. $\mathcal{B}$ sends them to the Π_o challenger and receives a challenge ciphertext $CT_o^* = ((\mathbf{A}^*, \rho^*), \tilde{C}_0, \bar{C}_0, \{C_{0,x}^o, D_{0,x}\}_{1\le x\le \ell^*}, \tilde{C}_1, \bar{C}_1, \{C_{1,x}^o, D_{1,x}\}_{1\le x\le \ell^*})$, which is the Π_o ciphertext of the message M_b with $b \in_R \{0,1\}$ chosen by the challenger of Π_o. It then chooses $\{E_{\rho(x)}, F_{0,x}, F_{1,x} \in_R \mathbb{Z}_N\}_{1\le x\le \ell^*}$, and sets

$$
\begin{aligned}
CT_{\mathbb{A}_b^*} = ((\mathbf{A}^*, \rho^*), \{E_{\rho(x)}\}_{1\le x\le \ell^*}, \tilde{C}_0, \bar{C}_0, \{F_{0,x}, C_{0,x}, D_{0,x}\}_{1\le x\le \ell^*},\\
\tilde{C}_1, \bar{C}_1, \{F_{1,x}, C_{1,x}, D_{1,x}\}_{1\le x\le \ell^*}),
\end{aligned}
$$

Table 1 Comparisons of typical CP-ABE schemes

Schemes	Privacy	Offline KeyGen	Offline Enc	Full security	Policy	Online KeyGen	Online Enc
Hohenberger and Waters (2014)[a]	×	✓	✓	×	LSSS	$n\mathbf{M} + n\mathbf{A}$	$(k + \ell)\mathbf{M}$
Nishide et al. (2008)	✓	×	×	×	AND[b]	$4n\mathbf{E} + 3n\mathbf{M}$	$(2N + 2)\mathbf{E}$
Lai et al. (2012)	✓	×	×	✓	LSSS	$(4 + n)\mathbf{E} + n\mathbf{M}$	$(4 + 8\ell)\mathbf{E} + 2k\mathbf{M}$
Ours	✓	✓	✓	✓	LSSS	$n\mathbf{A}$	$2k\mathbf{M}$

[a]In CP-ABE Hohenberger and Waters (2014), offline key generation and offline encryption are not given simultaneously

[b]AND-gates on multi-valued attributes with wildcards

where $C_{0,x} = C^o_{0,x} \cdot (g^a)^{-F_{0,x}} \cdot D^{a_{\rho(x)} E_{\rho(x)}}_{0,x}$ and $C_{1,x} = C^o_{1,x} \cdot (g^a)^{-F_{1,x}} \cdot D^{a_{\rho(x)} E_{\rho(x)}}_{1,x}$. Obviously, $CT_{\mathbb{A}^*_b}$ is a challenge ciphertext of Π, and $\mathcal{B}$ just sends it to $\mathcal{A}$.

Phase 2: The same as **Phase 1** with the restriction that $\mathbb{A}^*_1$ and $\mathbb{A}^*_2$ cannot be satisfied by any of the queried attribute sets.

Guess: Finally, the adversary $\mathcal{A}$ outputs a guess bit $b_{\mathcal{A}} \in \{0, 1\}$. The challenger $\mathcal{B}$ just sets its guess bit as $b_{\mathcal{B}} = b_{\mathcal{A}}$. Therefore, if $\mathcal{A}$ can break the proposed scheme with an advantage ϵ, then $\mathcal{B}$ breaks the scheme Π_o with the same probability. □

6.2 Performance analysis

In the proposed scheme, we realize offline computation in anonymous CP-ABE for the first time. It easily follows that only n subtraction operations **A** in arithmetic are needed for the attribute authority to generate a secret key in the online phase, where n means the number of attributes in the attribute set. In the online encryption phase, a data owner only needs to perform multiplication operations **M** in arithmetic determined by $k = \ell \cdot m$, where ℓ and m are respectively the number of rows and columns in the matrix of the access structure. In the offline encryption phase, the data owner does not know the message and access structure. The final ciphertext generated in the online phase does not explicitly include the attribute values specified in the access structure. Accordingly, the proposed scheme can preserve users' attribute privacy. Similar to the anonymous CP-ABE scheme due to Lai et al. (2012), our scheme is proven fully secure in the standard model and it supports any monotonic access structures. The comparisons of the proposed scheme with some typical CP-ABE schemes are shown in Table 1, where **E** represents an exponentiation operation in groups and N is the number of attribute values in the scheme due to Nishide et al. (2008).

7 Conclusion

We propose a privacy-aware attribute-based data sharing system supporting online/offline key generation and online/offline encryption. The proposed system is proven fully secure in the standard model. Because the attribute values of access structures are hidden in ciphertexts, our system can protect users' attribute privacy. The offline mechanism ensures that the attribute authority can provide better registration services and the system is suitable for resource-limited data owners in mobile cloud computing.

Acknowledgements This work is supported by National Natural Science Foundation of China (Nos. 61402366, 61472472, 61502248), Natural Science Basic Research Plan in Shaanxi Province (Nos. 2015JQ6236, 2016JM6033, 2015JQ6262, 2013JZ020), Scientific Research Program Funded by Shaanxi Provincial Education Department (No. 15JK1686). Yinghui Zhang is supported by New Star Team of Xi'an University of Posts and Telecommunications.

References

Beimel A (1996) Secure schemes for secret sharing and key distribution. Dissertation, Technion-Israel Institute of Technology

Bethencourt J, Sahai A, Waters B (2007) Ciphertext-policy attribute-based encryption. In: IEEE symposium on security and privacy, SP'07, IEEE, Oakland, pp 321–334. doi:10.1109/SP.2007.11

Boneh D, Waters B (2007) Conjunctive, subset, and range queries on encrypted data. In: Salil V (ed) Proceedings of the 4th theory of cryptography conference, TCC'07. Lecture notes in computer science, vol 4392. Springer, Berlin, pp 535–554. doi:10.1007/978-3-540-70936-7_29

Boneh D, Goh EJ, Nissim K (2005) Evaluating 2-DNF formulas on ciphertexts. In: Kilian J (ed) Proceedings of the 2th theory of cryptography conference, TCC'05. Lecture notes in computer science, vol 3378. Springer, Berlin, pp 325–341. doi:10.1007/978-3-540-30576-7_18

Chen X, Zhang F, Susilo W, Mu Y (2007) Efficient generic on-line/off-line signatures without key exposure. In: Katz J, Yung M (eds) Proceedings of the 5th international conference on applied cryptography and network security, ACNS'07. Lecture notes in computer science, vol 4521. Springer, Berlin, pp 18–30. doi:10.1007/978-3-540-72738-5_2

Chen X, Zhang F, Tian H, Wei B, Susilo W, Mu Y, Lee H, Kim K (2008) Efficient generic on-line/off-line (threshold)

signatures without key exposure. Inf Sci 178(21):4192–4203. doi:10.1007/978-3-540-72738-5_2

Cheung L, Newport C (2007) Provably secure ciphertext policy ABE. In: Proceedings of the 14th ACM conference on computer and communications security, CCS'07, ACM, New York, pp 456–465. doi:10.1145/1315245.1315302

Datta P, Dutta R, Mukhopadhyay S (2015) Fully secure online/offline predicate and attribute-based encryption. In: Lopez J, Wu Y (eds) Proceedings of the 11th international conference on information security practice and experience, ISPEC'15. Lecture notes in computer science, vol 9065. Springer, Berlin, pp 331–345. doi:10.1007/978-3-319-17533-1_23

Even S, Goldreich O, Micali S (1996) On-line/off-line digital signatures. J Cryptol 9(1):35–67. doi:10.1007/BF02254791

Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on computer and communications security, CCS'06, ACM, New York, pp 89–98. doi:10.1145/1180405.1180418

Green M, Hohenberger S, Waters B (2011) Outsourcing the decryption of ABE ciphertexts. In: Proceedings of the 20th USENIX conference on security, USENIX'11, USENIX Association, Berkeley. http://static.usenix.org/events/sec11/tech/full_papers/Green.pdf. Accessed 8 Aug 2011

Guo F, Mu Y, Chen Z (2008) Identity-based online/offline encryption. In: Tsudik G (ed) Proceedings of the 12th international conference on financial cryptography and data security, FC'08. Lecture notes in computer science, vol 12. Springer, Berlin, pp 247–261. doi:10.1007/978-3-540-85230-8_22

Hohenberger S, Waters B (2014) Online/offline attribute-based encryption. In: Krawczyk H (ed) Proceedings of the 17th international conference on practice and theory in public-key cryptography, PKC'14. Lecture notes in computer science, vol 8383. Springer, Berlin, pp 293–310. doi:10.1007/978-3-642-54631-0_17

Jung T, Li XY, Wan Z, Wan M (2015) Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption. IEEE Trans Inf Forensics Secur 10(1):190–199. doi:10.1109/TIFS.2014.2368352

Kapadia A, Tsang PP, Smith SW (2007) Attribute-based publishing with hidden credentials and hidden policies. In: Proceedings of the network and distributed system security symposium, NDSS'07, The Internet Society, pp 179–192. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.7574&rep=rep1&type=pdf. Accessed 28 Feb 2007

Katz J, Sahai A, Waters B (2008) Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart N (ed) Advances in cryptology-EUROCRYPT'08. Lecture notes in computer science, vol 4965. Springer, Berlin, pp 146–162. doi:10.1007/978-3-540-78967-3_9

Lai J, Deng RH, Li Y (2011) Fully secure cipertext-policy hiding CP-ABE. In: Bao F, Weng J (eds) Proceedings of the 7th international conference on information security practice and experience, ISPEC'11. Lecture notes in computer science, vol 6672. Springer, Berlin, pp 24–39. doi:10.1007/978-3-642-21031-0_3

Lai J, Deng RH, Li Y (2012) Expressive cp-abe with partially hidden access structures. In: Proceedings of the 7th ACM symposium on information, computer and communications security, ASIACCS'12, ACM, New York, pp 18–19. doi:10.1145/2414456.2414465

Lai J, Deng R, Guan C, Weng J (2013) Attribute-based encryption with verifiable outsourced decryption. IEEE Trans Inf Forensics Secur 8(8):1343–1354. doi:10.1109/TIFS.2013.2271848

Lewko A, Waters B (2012) New proof methods for attribute-based encryption: achieving full security through selective techniques. In: Safavi-Naini R, Canetti R (eds) Advances in cryptology–CRYPTO'12. Lecture notes in computer science, vol 7417. Springer, Berlin, pp 180–198. doi:10.1007/978-3-642-32009-5_12

Lewko A, Okamoto T, Sahai A, Takashima K, Waters B (2010) Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert H (ed) Advances in cryptology-EUROCRYPT'10. Lecture notes in computer science, vol 6110. Springer, Berlin, pp 62–91. doi:10.1007/978-3-642-13190-5_4

Li J, Ren K, Zhu B, Wan Z (2009) Privacy-aware attribute-based encryption with user accountability. In: Samarati P, Yung M, Martinelli F, Ardagna C (eds) Proceedings of the international information security conference, ISC'09. Lecture notes in computer science, vol 5735. Springer, Berlin, pp 347–362. doi:10.1007/978-3-642-04474-8_28

Li J, Huang X, Li J, Chen X, Xiang Y (2014) Securely outsourcing attribute-based encryption with checkability. IEEE Trans Parallel Distrib Syst 25(8):2201–2210. doi:10.1109/TPDS.2013.271

Nishide T, Yoneyama K, Ohta K (2008) Attribute-based encryption with partially hidden encryptor-specified access structure. In: Bellovin S, Gennaro R, Keromytis A, Yung M (eds) Proceedings of applied cryptography and network security, ACNS'08. Lecture notes in computer science, vol 5037. Springer, Berlin, pp 111–129. doi:10.1007/978-3-540-68914-0_7

Park SM, Chung SM (2014) Privacy-preserving attribute-based access control for grid computing. Int J Grid Util Comput 5(4):286–296. doi:10.1504/IJGUC.2014.065372

Phuong TVX, Yang G, Susilo W (2016) Hidden ciphertext policy attribute-based encryption under standard assumptions. IEEE Trans Inf Forensics Secur 11(1):35–45. doi:10.1109/TIFS.2015.2475723

Rao YS, Dutta R (2015) Fully secure bandwidth-efficient anonymous ciphertext-policy attribute-based encryption. Secur Commun Netw 8(18):4157–4176. doi:10.1002/sec.1331

Sahai A, Waters B (2005) Fuzzy identity-based encryption. In: Cramer R (ed) Advances in cryptology-EUROCRYPT'05. Lecture notes in computer science, vol 3494. Springer, Berlin, pp 557–557. doi:10.1007/11426639_27

Wang C, Li W (2013) An efficient attribute-based signature scheme with claim-predicate mechanism. Int J Grid Util Comput 4(2–3):151–159. doi:10.1504/IJGUC.2013.056251

Zhang Y, Chen X, Li J, Wong DS, Li H (2013) Anonymous attribute-based encryption supporting efficient decryption test. In: Proceedings of the 8th ACM SIGSAC symposium on information, computer and communications security, ASIACCS'13, ACM, New York, pp 511–516. doi:10.1145/2484313.2484381

Zhang Y, Chen X, Li J, Li H (2014) Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks. Comput Netw 75:192–211. doi:10.1016/j.comnet.2014.10.009

Zhang Y, Li J, Chen X, Li H (2016a) Anonymous attribute-based proxy re-encryption for access control in cloud computing. Secur Commun Netw 9(14):2397–2411. doi:10.1002/sec.1509

Zhang Y, Zheng D, Chen X, Li J, Li H (2016b) Efficient attribute-based data sharing in mobile clouds. Pervasive Mob Comput 28:135–149. doi:10.1016/j.pmcj.2015.06.009

Zhang Y, Chen X, Li J, Wong DS, Li H, You I (2017) Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Inf Sci 379:42–61. doi:10.1016/j.ins.2016.04.015

Zhu S, Yang X (2015) Protecting data in cloud environment with attribute-based encryption. Int J Grid Util Comput 6(2):91–97. doi:10.1504/IJGUC.2015.068824