3-2018

An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited

Hui CUI
Royal Melbourne Institute of Technology

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Junzuo LAI
Jinan University - China

Xun YI
Royal Melbourne Institute of Technology

Surya NEPAL
CSIRO

Published in Computer Networks, Volume 133, 14 March 2018, Pages 157-165.
https://doi.org/10.1016/j.comnet.2018.01.034

An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited☆

Hui Cui[a,b,*], Robert H. Deng[b], Junzuo Lai[c], Xun Yi[a], Surya Nepal[d]

[a] School of Science, Royal Melbourne Institute of Technology (RMIT) University, Melbourne, Australia
[b] School of Information Systems, Singapore Management University, Singapore
[c] Department of Computer Science, Jinan University, Guangzhou, China
[d] Data 61, CSIRO, Sydney, Australia

Keywords:
Cloud storage
Data security and privacy
Access control

A B S T R A C T

Ciphertext-policy attribute-based encryption (CP-ABE) has been regarded as one of the promising solutions to protect data security and privacy in cloud storage services. In a CP-ABE scheme, an access structure is included in the ciphertext, which, however, may leak sensitive information about the underlying plaintext and the privileged recipients in that anyone who sees the ciphertext is able to learn the attributes of the privileged recipients from the associated access structure. In order to address this issue, CP-ABE with partially hidden access structures was introduced where each attribute is divided into an attribute name and an attribute value and the attribute values of the attributes in an access structure are not given in the ciphertext. Though a number of CP-ABE schemes with partially hidden access structures have been proposed, most of them only enable restricted access structures, whereas several other schemes supporting expressive access structures are computationally inefficient due to the fact that they are built in the composite-order groups. To our knowledge, there has been little attention paid to the design of expressive CP-ABE schemes with partially hidden access structures in the prime-order groups. In this paper, we revisit this problem, and present an expressive CP-ABE scheme supporting partially hidden access structures in the prime-order groups with improved efficiency.

1. Introduction

In recent years, there has been an increasing demand for storing data to the cloud [2–4]. Users may not like to store his/her data containing sensitive information to a public cloud without security and privacy guarantee, but they may need to share their data with others possessing certain attributes (or credentials). Ciphertext-policy attribute-based encryption (CP-ABE) [5] is a mechanism meeting this requirement, where each user is given a private attribute-key in terms of his/her attributes issued by an attribute authority (AA), each message is encrypted under an access structure (or access policy) over a set of attributes, and a user can decrypt a ciphertext with his/her private attribute-key if his/her attributes satisfy the access policy ascribed to this ciphertext.

Though a ciphertext generated by a CP-ABE scheme (e.g., [5–8]) does not reveal the identities of the recipients, anyone accessible to a ciphertext may learn some information about the underlying message and the privileged recipients from the access structure clearly included in the ciphertext [9–11]. For example, in a cloud system storing electrical medical records (EMRs) [12,13] of patients as in Fig. 1, there is a ciphertext on an EMR under an access structure "(Patient: NR005289 AND Hospital: City Hospital) OR (Doctor: Cardiologist AND Hospital: General Hospital)". The access structure defines that a patient numbered as NR005289 at the City Hospital or any Cardiologist at the General Hospital can decrypt the ciphertext to obtain the EMR, from which it is not difficult to conclude that a patient NR005289 in the City Hospital is suffering a heart problem. Definitely, cloud users do not expect such an information leakage, so it is crucial to build CP-ABE schemes with attributes hidden in the access structures.

It has been stated in [9] that a CP-ABE scheme with hidden access structures can be built from an attribute-hiding inner-product predicate encryption (IPE) scheme [14], but it is inefficient to implement a CP-ABE scheme with fully hidden access structures (where the attributes are completely hidden from the ciphertext) built from an attribute-hiding IPE scheme [7]. In order to have a trade off between fully hidden access structures and efficient CP-ABE, many CP-ABE schemes with partially hidden access structures (e.g., [9,15–18]) have been proposed. However, some schemes

☆ This paper is an extension to the original publication in ProvSec 2016 [1].

* Corresponding author at: School of Science, Royal Melbourne Institute of Technology (RMIT) University, Melbourne, Australia.
E-mail address: hui.cui@rmit.edu.au (H. Cui).

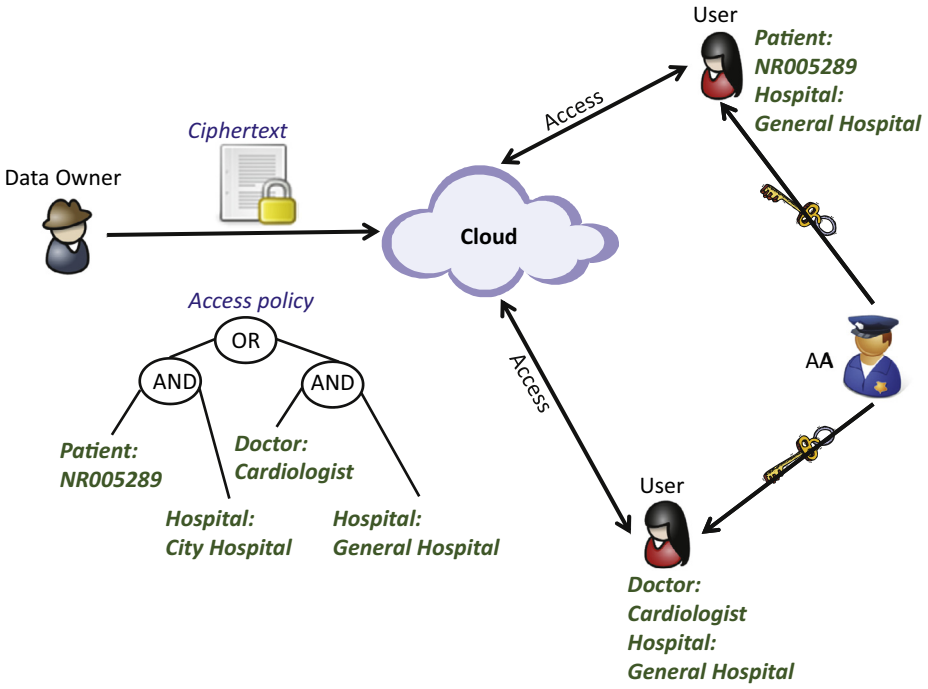

Fig. 1. An architecture of a cloud storage system based on a CP-ABE scheme.

(e.g., [15–18]) only allow restricted access structures (expressed in AND gates), while other schemes (e.g., [9]) supporting expressive access structures are built in the inefficient composite-order groups (note that "a Tate pairing on a 1024-bit composite-order elliptic curve is roughly 50 times slower than the same pairing on a comparable prime-order curve, and this performance gap will only get worse at higher security levels" [19]). There exist techniques (e.g., [19]) to convert schemes in the composite-order groups to that in the prime-order groups, but they cause a significant degradation in the performance [20]. Consequently, it is desirable to construct expressive CP-ABE schemes with partially hidden access structures in the prime-order groups.

1.1. Our contributions

Generally, generic attribute names contain less sensitive information than concrete attribute values. Take the scenario in Fig. 1 as an instance, it is obvious that the attribute values "Cardiologist" and "NR005289" are more sensitive than the attribute names "Doctor" and "Patient". Motivated by this observation, it has been suggested to use CP-ABE with partially hidden access structures [9,15] which divides each attribute into an attribute name and an attribute value, and the attribute values of an access structure are not included in the ciphertext. Specifically, the full access structure in Fig. 1 is replaced by a partially hidden access structure "(Patient: * AND Hospital: *) OR (Doctor: * AND Hospital: *)" to be included in the ciphertext.

One naive method to build a CP-ABE scheme with partially hidden access structures is to simply remove the attribute names from the access structure of the ciphertext. The resulting scheme, however, suffers off-line dictionary attacks [1], by running which an adversary can determine whether an attribute value is associated with an access structure if the space of the attribute values is not sufficiently large. To overcome this challenge and build an expressive CP-ABE scheme with partially hidden access structures in the prime-order groups, Cui et al. [1] applied the "randomness splitting" [21] technique to the Rouselakis–Waters CP-ABE scheme [20] to hide the sensitive attribute values from the ciphertext. In this way, an access structure with only attribute names (i.e., attribute values are not present) is sent along with the ciphertext. Besides, to convince a user that he/she is a privileged user to the resulting "anonymous" ciphertext, Cui et al. [1] combined a commitment scheme [22] on the message to the corresponding ciphertext such that a user can check the correctness of the decryption result. In this paper, we revisit the expressive CP-ABE scheme with partially hidden access structures in the prime-order groups given in [1], and improve its efficiency by removing the commitment scheme without weakening the security. In the proposed expressive CP-ABE scheme with partially hidden access structures in the prime-order groups, the encryption and decryption algorithms add no exponentiation or pairing calculations to that of the underlying Rouselakis–Waters scheme [20], while the expressive CP-ABE scheme with partially hidden access structures in the prime-order groups in [1] adds several exponentiation operations to that of the underlying Rouselakis–Waters scheme [20].

In summary, the proposed expressive CP-ABE scheme with partially hidden access structures in this paper is similar to the one in [1] except that the former improves the efficiency of the latter by removing the commitment scheme yet allowing a user to check whether he/she is a privileged recipient of a ciphertext without including the associated attribute values.

1.2. Related work

Attribute-based encryption (ABE) was introduced by Sahai and Waters [23], which was then formulated into key-policy ABE (KP-ABE) and CP-ABE [24]. In a KP-ABE scheme, the ciphertext is associated with an attribute set and the private attribute-key is ascribed to an access policy, while the situation is reversed in a CP-ABE scheme. Nevertheless, a CP-ABE scheme is more flexible than a KP-ABE scheme because the access policy in the latter is determined once the user's private attribute-key is issued. The first CP-ABE scheme was proposed by Bethencourt, Sahai and Waters [5], but it was secure under the generic group model. The first CP-ABE scheme secure in the standard model was presented by Cheung and Newport [6], but it only supported the access structures

in AND gates. The first CP-ABE scheme enabling advanced access structures was designed by Goyal et al. [25] based on the number theoretic assumption. The first large universe CP-ABE scheme in the prime-order groups was built by Rouselakis and Waters [20], where the size of the attribute space is polynomially unbounded. CP-ABE schemes with partially hidden access structures (e.g., [15,16,18]) were presented to better preserve privacy, but they were selectively secure or allowed restricted access structures (expressed in AND gates). Lai, Deng and Li [17] gave a fully secure CP-ABE scheme with partially hidden access structures, but it only supported the restricted access structures. Later, Lai, Deng and Li [9] proposed a fully secure and expressive CP-ABE scheme to partially hide access structures, but it had an efficiency issue due to the use of bilinear pairings in the composite-order groups. To overcome the inefficient implementation of the composite-order groups, Cui et al. [1] presented an expressive CP-ABE scheme with partially hidden access structures in the prime-order groups. In this paper, we revisit the expressive CP-ABE scheme with partially hidden access structures in the prime-order groups in [1], and further improve its efficiency.

1.3. Organization

The rest of this paper is organized as follows. In Section 2, we briefly review the definitions that are related to this paper. In Section 3, we describe the framework for CP-ABE with partially hidden access structures, and then define its security model. In Section 4, we give a concrete expressive CP-ABE scheme with partially hidden access structures, and analyze its security and performance. Finally, we conclude this paper in Section 5.

2. Preliminaries

We review some basic cryptographic notions and definitions that are to be used in this paper in this section.

2.1. Bilinear pairings and complexity assumptions

Let G be a group of a prime order p with a generator g. We say that $\hat{e}: G\times G \to G_1$ is a bilinear map [26] if it is Bilinear such that for all $g\in G$, and $a, b\in Z_p$, it holds that $\hat{e}(g^a, g^b) = \hat{e}(g,g)^{ab}$, and Non-degenerate such that $\hat{e}(g,g)\neq 1$.

Decisional $(q-1)$ assumption [20]. The decisional $(q-1)$ problem is that for any probabilistic polynomial-time (PPT) algorithm, given $\vec{y} =$

$$
\begin{array}{ll}
g, g^{\mu}, & \\
g^{a^i}, g^{b_j}, g^{\mu\cdot b_j}, g^{a^i b_j}, g^{a^i/b_j^2} & \forall\ (i,j)\in[q,q], \\
g^{a^i/b_j} & \forall\ (i,j)\in[2q,q] \text{ with } i\neq q+1, \\
g^{a^i b_j/b_{j'}^2} & \forall\ (i,j,j')\in[2q,q,q] \text{ with } j\neq j', \\
g^{\mu a^i b_j/b_{j'}}, g^{\mu a^i b_j/b_{j'}^2} & \forall\ (i,j,j')\in[q,q,q] \text{ with } j\neq j',
\end{array}
$$

it is difficult to distinguish $(\vec{y},\ \hat{e}(g,g)^{a^{q+1}\mu})$ from $(\vec{y},\ Z)$, where $g\in G$, $Z\in G_1$, $a, \mu, b_1, \ldots, b_q\in Z_p$ are randomly chosen.

Decisional linear assumption [27]. The decisional linear problem is that for any PPT algorithm, given $g, g^{x_1}, g^{x_2}, g^{x_1x_3}, g^{x_2x_4}$, it is difficult to distinguish $(g, g^{x_1}, g^{x_2}, g^{x_1x_3}, g^{x_2x_4}, g^{x_3+x_4})$ from $(g, g^{x_1}, g^{x_2}, g^{x_1x_3}, g^{x_2x_4}, Z)$, where $g, Z\in G$, $x_1, x_2, x_3, x_4\in Z_p$ are randomly chosen.

2.2. Pseudo-random functions

Let H: $\mathrm{K}_\lambda \times \mathrm{D}_\lambda \to \mathrm{R}_\lambda$ be a pseudo-random function (PRF) [28] under a security parameter λ with arbitrary finite sets K_λ, D_λ and R_λ. The advantage of an adversary $\mathcal{A}$ against the PRF H is

$$\mathbf{Adv}^{\mathrm{PRF}}_{H,\mathcal{A}}(\lambda) = \Pr[\mathrm{REAL}^{\mathcal{A}}_H \Rightarrow 1] - \Pr[\mathrm{RAND}^{\mathcal{A}}_H \Rightarrow 1],$$

where the security games are given in Fig. 2. If the advantage of any PPT adversary is negligible in the security parameter λ, then H is a secure PRF.

2.3. Symmetric encryption

A symmetric encryption (SE) scheme $\mathcal{SE}$ with a key space $\mathcal{K}$ and a message space $\mathcal{M}$ is composed of an encryption algorithm $\mathcal{SE}$.Enc(K, M) which outputs a ciphertext CT on input a key K (in the key space) and a message M (in the message space), and a decryption algorithm $\mathcal{SE}$.Dec(K, CT) which outputs M or a failure symbol $\perp$ on input a key K and a ciphertext CT.

The scheme $\mathcal{SE}$ is secure under chosen plaintext attacks (IND-CPA secure), if for any PPT adversary $\mathcal{A}$, the advantage function

$$\mathbf{Adv}^{\text{IND-CPA}}_{\mathcal{SE},\mathcal{A}}(\lambda) = \Pr\left[b'=b \middle| \begin{array}{l} K\leftarrow\mathcal{K}; b\leftarrow\{0,1\} \\ (M_0, M_1, state)\leftarrow\mathcal{A}(1^\lambda) \\ \mathrm{CT}^*\leftarrow\mathcal{SE}.\mathrm{Enc}(K, M_b) \\ b'\leftarrow\mathcal{A}(par, M_0, M_1, state, \mathrm{CT}^*) \end{array} \right] - 1/2$$

is negligible in the security parameter λ, where $|M_0| = |M_1|$.

2.4. Access structures and linear secret sharing schemes

Access structures [8,29]. Denote $\{P_1, \ldots, P_n\}$ as a set of parties. A collection $\mathbb{A}\subseteq 2^{\{P_1,\ldots,P_n\}}$ is monotone if $\forall B, C$: if $B\in\mathbb{A}$ and $B\subseteq C$, then $C\subseteq\mathbb{A}$. An (monotone) access structure is a (monotone) collection $\mathbb{A}$ of non-empty subsets of $\{P_1, \ldots, P_n\}$, i.e., $\mathbb{A}\subseteq 2^{\{P_1,\ldots,P_n\}}\setminus\{\emptyset\}$. The sets that are in $\mathbb{A}$ are known as the authorized sets, and the sets that are not in $\mathbb{A}$ are known as the unauthorized sets.

Linear secret sharing schemes (LSSSs) [8,29]. Let P be a set of parties, $\mathbb{M}$ be an $l\times n$ matrix (i.e., the matrix $\mathbb{M}$ has l rows and n columns), and ρ: $\{1, \ldots, l\}\to P$ be a function mapping a row to a party for labeling. A secret sharing scheme Π over a set of parties P is a linear secret-sharing scheme (LSSS) over Z_p if (1) the shares for each party form a vector over Z_p; and (2) there exists an $l\times n$ matrix $\mathbb{M}$ called the share-generating matrix for Π. For $x = 1, \ldots, l$, the x-th row of the matrix $\mathbb{M}$ is labeled by a party $\rho(i)$ with ρ: $\{1, \ldots, l\}\to P$ being a function to map a row to a party for labeling. Assuming that the column vector $\vec{v} = (\mu, r_2, \ldots, r_n)$, where $\mu\in Z_p$ is the secret to be shared and $r_2, \ldots, r_n\in Z_p$ are randomly chosen, and then $\mathbb{M}\vec{v}$ is the vector of l shares of the secret μ according to Π. The share $(\mathbb{M}\vec{v})_i$ belongs to the party $\rho(i)$.

Note that every LSSS enjoys the linear reconstruction property [29]. Let Π be an LSSS for an access structure $\mathbb{A}$, and $\mathbf{A}$ be an authorized set. Define $I\subseteq\{1, \ldots, l\}$ as $I = \{i|\rho(i)\in\mathbf{A}\}$. Then the vector $(1, 0, \ldots, 0)$ is in the span of rows of a matrix $\mathbb{M}$ indexed by I, and there exist constants $\{w_i\in Z_p\}_{i\in I}$ such that, for any valid shares $\{v_i\}$ of a secret μ according to Π, it holds that $\Sigma_{i\in I} w_i v_i = \mu$. These constants $\{w_i\}$ can be found in polynomial time with respect to the size of the share-generating matrix $\mathbb{M}$ [30]. On the other hand, for an unauthorized set $\mathbf{A}'$, such constants $\{w_i\}$ do not exist. Also, in this case, if $I' = \{i|\rho(i)\in\mathbf{A}'\}$, there exists a vector $\vec{w}$ such that its first component w_1 is any non-zero element in Z_p and $<\mathbb{M}_i, \vec{w}> = 0$ for all $i\in I'$, where $\mathbb{M}_i$ is the i-th row of the matrix $\mathbb{M}$ [20].

Boolean formulas. Access structures can be described in terms of monotonic boolean formulas as well. LSSS access structures can be derived from representations as boolean formulas, which are more general. There are generic methods to convert a monotonic boolean formula into an LSSS matrix[1] A boolean formula can be represented as an access tree, in which the AND or OR gates are denoted by the interior nodes, and the attributes are denoted by

[1] For the details about how to convert a boolean formula into an equivalent LSSS matrix, please refer to [29].

proc Initialize	proc $H(x)$	proc Initialize	proc $H(x)$
$K \leftarrow \mathrm{K}_\lambda$	Return $H_k(x)$	CoinTab $\leftarrow \emptyset$	If CoinTab$[x] = \perp$ then
Return 1^λ		Return 1^λ	CoinTab$[x] \leftarrow \mathrm{R}_\lambda$
proc Finalize(b)		proc Finalize(b)	Return CoinTab$[x]$
Return b		Return b	

Fig. 2. Games defining security for a PRF. Left: Game REAL. Right: Game RAND.

the leaf nodes. The number of rows in an LSSS matrix will be equal to the number of leaf nodes in its corresponding access tree.

3. System architecture and security model

In this section, the framework and the corresponding security model of ciphertext-policy attribute-based encryption with partially hidden access structures are described.

3.1. Framework

A CP-ABE scheme with partially hidden access structures consists of a setup algorithm Setup, a private attribute-key generation algorithm KeyGen, an encryption algorithm Encrypt and a decryption algorithm Decrypt.

- Setup(1^λ) $\rightarrow$ (*pars, msk*). Taking the security parameter λ as the input, this algorithm, running by the AA, outputs the public parameter *pars* and the master private key *msk*.
- KeyGen(*pars, msk*, $\mathbf{A}$) $\rightarrow$ $K_{\mathbf{A}}$. Taking the public parameter *pars*, the master private key *msk* and an attribute set $\mathbf{A}$ as the input, this algorithm, running by the AA, outputs a private attribute-key $K_{\mathbf{A}}$.
- Encrypt(*pars, M*, ($\mathbb{M}$, ρ, $\{A_{\rho(i)}\}$)) $\rightarrow$ CT. Taking the public parameter *pars*, a message *M* and an access structure ($\mathbb{M}$, ρ, $\{A_{\rho(i)}\}$) where the function ρ associates the rows of the matrix $\mathbb{M}$ to generic attribute names, and $\{A_{\rho(i)}\}$ are the corresponding attribute values as the input, this algorithm, running by the data owner, outputs a ciphertext CT.
- Decrypt(*pars*, CT, $K_{\mathbf{A}}$) $\rightarrow$ $M/\perp$. Taking the public parameter *pars*, a ciphertext CT under an access structure ($\mathbb{M}$, ρ, $\{A_{\rho(i)}\}$) and a private attribute-key $K_{\mathbf{A}}$ over an attribute set $\mathbf{A}$ as the input, this algorithm, running by the user, outputs a message *M* if the attributes $\mathbf{A}$ satisfy the access structure ($\mathbb{M}$, ρ, $\{A_{\rho(i)}\}$), or a failure symbol $\perp$ otherwise.

A CP-ABE scheme with partially hidden access structures is said to be correct, meaning that for all messages *M* (in the message space), all attribute sets $\mathbf{A}$ (in the attribute space) satisfying access structures ($\mathbb{M}$, ρ, $\{A_{\rho(i)}\}$), if (*pars, msk*) $\leftarrow$ Setup(1^λ), $K_{\mathbf{A}} \leftarrow$ KeyGen(*pars, msk*, $\mathbf{A}$), CT $\leftarrow$ Encrypt(*pars, M*, ($\mathbb{M}$, ρ, $\{A_{\rho(i)}\}$)), then Decrypt(*pars*, CT, $K_{\mathbf{A}}$) $= M$.

3.2. Security definitions

A CP-ABE scheme with partially hidden access structures should preserve confidentiality and anonymity. Below we review the security definitions for these two requirements, following the description in [1].

- **Confidentiality.** The security game for confidentiality is defined by the following game between a challenger algorithm $\mathcal{C}$ and an adversary algorithm $\mathcal{A}$.
  - Setup. Algorithm $\mathcal{C}$ runs the setup algorithm to obtain the public parameter *pars* and the master private key *msk*. It keeps the master private key *msk* and gives the public parameter *pars* to algorithm $\mathcal{A}$.
  - Phase 1. Algorithm $\mathcal{A}$ adaptively issues queries to the key generation oracle. For each query on an attribute set $\mathbf{A}_i$, algorithm $\mathcal{C}$ returns a private attribute-key $K_{\mathbf{A}_i}$ to algorithm $\mathcal{A}$.
  - Challenge. Algorithm $\mathcal{A}$ outputs two messages M_0^*, M_1^* of the same size and an access structure ($\mathbb{M}^*$, ρ^*, $\{A_{\rho^*(i)}\}$) with the constraint that there is no attribute set $\mathbf{A}_i$ in the key generation queries in Phase 1 satisfying the challenge access structure ($\mathbb{M}^*$, ρ^*, $\{A_{\rho^*(i)}\}$). Algorithm $\mathcal{C}$ randomly chooses a bit $\beta \in \{0, 1\}$, generates the challenge ciphertext CT* of the message M_β^* under the access structure ($\mathbb{M}^*$, ρ^*, $\{A_{\rho^*(i)}\}$), and sends the challenge ciphertext CT* to algorithm $\mathcal{A}$.
  - Phase 2. Algorithm $\mathcal{A}$ continues issuing queries on attribute sets to the key generation oracle with the restriction that the attribute sets cannot satisfy the challenge access structure in the challenge phase. Algorithm $\mathcal{C}$ responds as in Phase 1.
  - Guess. Algorithm $\mathcal{A}$ makes a guess $\beta' \in \{0, 1\}$ for β, and it wins the game if $\beta' = \beta$.
- **Anonymity.** The security game for anonymity is defined under chosen-plaintext attacks (ANON-CPA) between a challenger algorithm $\mathcal{C}$ and an adversary algorithm $\mathcal{A}$ as follows.
  - Setup. Algorithm $\mathcal{C}$ runs the setup algorithm to obtain the public parameter *pars* and the master private key *msk*. It forwards the public parameter *pars* to algorithm $\mathcal{A}$ and keeps the master private key *msk*.
  - Phase 1. Algorithm $\mathcal{A}$ issues key generation queries to algorithm $\mathcal{C}$. For each key generation query on an attribute set $\mathbf{A}_i$, algorithm $\mathcal{C}$ returns a private attribute-key $K_{\mathbf{A}_i}$ to algorithm $\mathcal{A}$.
  - Challenge. Algorithm $\mathcal{A}$ outputs a message M^*, two access structures ($\mathbb{M}^*$, ρ^*, $\{A_{\rho^*(i)}\}_0$) and ($\mathbb{M}^*$, ρ^*, $\{A_{\rho^*(i)}\}_1$) (i.e., the access matrix ($\mathbb{M}^*$, ρ^*) can be satisfied by the attribute sets $\{A_{\rho^*(i)}\}_0$ and $\{A_{\rho^*(i)}\}_1$) with the constraint that there are no key generation queries in Phase 1 that can satisfy ($\mathbb{M}^*$, ρ^*, $\{A_{\rho^*(i)}\}_0$) or ($\mathbb{M}^*$, ρ^*, $\{A_{\rho^*(i)}\}_1$). Algorithm $\mathcal{C}$ randomly chooses a bit $\beta \in \{0, 1\}$, and sends a challenge ciphertext CT* for the message M^* under the access structure ($\mathbb{M}^*$, ρ^*, $\{A_{\rho^*(i)}\}_\beta$) to algorithm $\mathcal{A}$.
  - Phase 2. Algorithm $\mathcal{A}$ continues issuing the key generation queries to algorithm $\mathcal{C}$ except that any attribute set $\mathbf{A}_i$ satisfying the access structure c($\mathbb{M}^*$, ρ^*, $\{A^*_{\rho(i)}\}_0$) or ($\mathbb{M}^*$, ρ^*, $\{A^*_{\rho(i)}\}_1$) are disallowed. Algorithm $\mathcal{C}$ responds as in Phase 1.
  - Guess. Algorithm $\mathcal{A}$ makes a guess $\beta' \in \{0, 1\}$ for β, and it wins the game if $\beta' = \beta$.

The advantage of algorithm $\mathcal{A}$ in the above confidentiality (or anonymity) game is defined to be $\Pr[\beta = \beta'] - 1/2$. A CP-ABE scheme with partially hidden access structures is said to be indistinguishable (or anonymous) under the chosen-plaintext attacks if any PPT adversary has at most a negligible advantage in the security parameter λ. Also, a CP-ABE scheme with partially hidden access structures is said to be selectively indistinguishable (or anonymous) if an Init stage is added before the Setup phase where algorithm $\mathcal{A}$ commits to the challenge access structure ($\mathbb{M}^*$, ρ^*,

$\{A_{\rho^*(i)}\}$) (or the challenge access structures $(\mathbb{M}^*, \rho^*, \{A_{\rho^*(i)}\}_0)$ and $(\mathbb{M}^*, \rho^*, \{A_{\rho^*(i)}\}_1)$.

4. Expressive ciphertext-policy attribute-based encryption with partially hidden access structures in prime-order groups

In this section, a concrete expressive CP-ABE scheme with partially hidden access structures in the prime-order groups, as well as its security and efficiency analysis are given.

4.1. Construction

We present an expressive CP-ABE scheme supporting partially hidden access structures in the prime-order groups $\mathcal{ABE}$ by improving the scheme $\mathcal{ABE}'$ in [1]. Assume that $\mathcal{SE} = (\mathcal{SE}.\mathrm{Enc}, \mathcal{SE}.\mathrm{Dec})$ is a symmetric encryption scheme with a key space $\mathcal{K}$ and a message space $\mathcal{M}$. Let G be a group of a prime order p with a generator g, and $\hat{e} : G \times G \to G_1$ be a bilinear map.

- Setup. Similar to that in $\mathcal{ABE}'$ [1], this algorithm takes the security parameter λ as the input. It computes $g_1 = g^{d_1}$, $g_2 = g^{d_2}$, $g_3 = g^{d_3}$, $g_4 = g^{d_4}$, where $u, h, v, w \in G$, $d_1, d_2, d_3, d_4, \alpha \in Z_p$ are randomly chosen. The master private key is $msk = (d_1, d_2, d_3, d_4, g^{\alpha})$, and the public parameter is $pars = (H, H', g, u, h, w, v, g_1, g_2, g_3, g_4, \hat{e}(g,g)^{\alpha})$ where H is a collision-resistant hash function to map elements in G_1 to elements in $\mathcal{K}$ and H' is a pseudo-random function to map elements in G_1 and $\mathcal{M}$ to elements in $\mathcal{M}$.
- KeyGen. This algorithm is the same as that in $\mathcal{ABE}'$ [1], which takes the public parameter $pars$, the master private key msk and an attribute set $\mathbf{A}$[2] as the input. Let k be the size of $\mathbf{A}$ such that $A_1, \ldots, A_k \in Z_p$ are the attribute values of $\mathbf{A}$. It computes

$$K_1 = g^{\alpha} w^{d_1 d_2 r + d_3 d_4 r'}, \quad K_2 = g^{r d_1 d_2 + r' d_3 d_4},$$
$$K_{i,1} = ((u^{A_i} h)^{r_i} v^{-r})^{d_2}, \quad K_{i,2} = ((u^{A_i} h)^{r_i} v^{-r})^{d_1}, \quad K_{i,3} = g^{d_1 d_2 r_i + d_3 d_4 r'_i},$$
$$K_{i,4} = ((u^{A_i} h)^{r'_i} v^{-r'})^{d_4}, \quad K_{i,5} = ((u^{A_i} h)^{r'_i} v^{-r'})^{d_3},$$

  where $r, r', r_1, \ldots, r_k, r'_1, \ldots, r'_k \in Z_p$ are randomly chosen. It outputs a private attribute-key $K_{\mathbf{A}} = (K_1, K_2, \{K_{i,1}, K_{i,2}, K_{i,3}, K_{i,4}, K_{i,5}\}_{i \in [1,k]})$.
- Encrypt. This algorithm mostly follows that in $\mathcal{ABE}'$ [1], which takes the public parameter $pars$, a message M and an access structure $(\mathbb{M}, \rho, \{A_{\rho(i)}\})$ as the input. It randomly chooses a vector $\vec{v} = (\mu, y_2, \ldots, y_n) \in Z_p^n$ of which the values are used to share μ, and computes $v_i = \vec{v} \cdot \mathbb{M}_i$ (for $i = 1, \ldots, l$), where $\mathbb{M}_i$ is the vector corresponding to the i-th row of the matrix $\mathbb{M}$. Then, it randomly chooses $R \in G_1$, $s_{i,1}, \ldots, s_{i,l}, s_{1,2}, \ldots, s_{l,2}, z_1, \ldots, z_l \in Z_p$, and computes $k = H(R)$, $\tau = H'(R, M)$,

$$C = R \cdot \hat{e}(g,g)^{\alpha\mu}, \quad D = g^{\mu}, \quad E = \mathcal{SE}.\mathrm{Enc}(k, M),$$
$$C_i = w^{v_i} v^{z_i}, \quad D_{i,1} = g_1^{z_i - s_{i,1}}, \quad E_{i,1} = g_3^{z_i - s_{i,2}},$$
$$D_{i,2} = g_2^{s_{i,1}}, \quad E_{i,2} = g_4^{s_{i,2}}, \quad F_i = (u^{A_{\rho(i)}} h)^{-z_i}.$$

  It outputs a ciphertext $\mathrm{CT} = \big((\mathbb{M}, \rho), C, D, \{(C_i, D_{i,1}, D_{i,2}, E_{i,1}, E_{i,2}, F_i)\}_{i \in [1,l]}, E, \tau\big)$.
- Decrypt. This algorithm mostly follows that in $\mathcal{ABE}'$ [1], which takes the public parameter $pars$, a ciphertext $\big((\mathbb{M}, \rho), C, D, \{(C_i, D_{i,1}, D_{i,2}, E_{i,1}, E_{i,2}, F_i)\}_{i \in [1,l]}, E, \tau\big)$ and a private attribute-key $K_{\mathbf{A}}$ for an attribute set $\mathbf{A}$ as the input. It computes a set of minimum subsets of attributes satisfying $(\mathbb{M}, \rho)$ as $I_{\mathbb{M},\rho}$. Denote $\{w_i \in Z_p\}_{i \in \mathcal{I}}$ as a set of constants such that if $\{v_i\}$ are valid shares of the secret μ in terms of the matrix $\mathbb{M}$, then $\sum_{i \in \mathcal{I}} w_i v_i = \mu$. For an $\mathcal{I} \in I_{\mathbb{M},\rho}$, it computes

$$\frac{\hat{e}(D, K_1)}{\prod_{i \in \mathcal{I}} (\hat{e}(C_i, K_2)\hat{e}(D_{i,1}, K_{i,1})\hat{e}(D_{i,2}, K_{i,2})\hat{e}(F_i, K_{i,3})\hat{e}(E_{i,1}, K_{i,4})\hat{e}(E_{i,2}, K_{i,5}))^{w_i}}$$
$$= \frac{\hat{e}(g,g)^{\alpha\mu}\hat{e}(g^{\mu}, w)^{r_1 d_1 d_2}\hat{e}(g^{\mu}, w)^{r_2 d_3 d_4}}{\prod_{i \in I} (\hat{e}(g, w^{v_i})^{d_1 d_2 r_1 + d_3 d_4 r_2})^{w_i}} = \hat{e}(g,g)^{\alpha\mu}.$$

  It cancels out this value from C to have R', and computes $M' = \mathcal{SE}.\mathrm{Dec}(H(R'), E)$. It outputs M' if $\tau = H'(R', M')$, or $\perp$ otherwise.

[2] Each attribute is denoted as $N_i = A_i$, where N_i is the generic attribute name and A_i is the corresponding attribute value.

4.2. Security proof

Theorem 1. *Assuming that H' is a secure pseudo-random function, the decisional $(q-1)$ assumption holds in G, the decisional linear assumption holds in G, the scheme $\mathcal{SE}$ is IND-CPA secure, and then the proposed scheme $\mathcal{ABE}$ is selectively indistinguishable and anonymous.*

Proof. The proof is reduced via a sequence of games by concluding that these games are computationally indistinguishable from each other. To simplify the description, the access structures are removed from the ciphertexts. Denote $(C^*, D^*, \{(C_i^*, D_{i,1}^*, D_{i,2}^*, E_{i,1}^*, E_{i,2}^*, F_i^*)\}_{i \in [1,l]}, E^*, \tau^*)$ as the challenge ciphertext given to the adversary during an attack in the real world. Let Z be a random element of G_1, and $\{Z_{i,1}\}$, $\{Z'_{i,1}\}$ be sets of random elements of G. Denote Z_E^*, Z_τ^* as the elements randomly chosen from the ciphertext space and the message space of $\mathcal{SE}$, respectively. A sequence of games Game_0, Game_1, …, Game_l, Game_{l+1}, …, Game_{2l+1}, Game_{2l+2}, Game_{2l+3} are defined which differ on which challenge ciphertext is given to the adversary, where Game_0 is the original game, Game_1 changes the term C^* to Z, and Game_2 to Game_{l+1} change the term $D_{i,1}^*$ to $Z_{i,1}$ one by one for $i \in [1, l]$, and Game_{l+2} to Game_{2l+1} change the term $E_{i,1}^*$ to $Z'_{i,1}$ one by one for $i \in [1, l]$, Game_{2l+2} changes the term E^* to Z_E^*, and Game_{2l+3} changes the term τ^* to Z_τ^*.

- Game_0: The challenge ciphertext is $\mathrm{CT}_0^* = (C^*, D^*, \{(C_i^*, D_{i,1}^*, D_{i,2}^*, E_{i,1}^*, E_{i,2}^*, F_i^*)\}_{i \in [1,l]}, E^*, \tau^*)$.
- Game_1: The challenge ciphertext is $\mathrm{CT}_1^* = (Z, D^*, \{(C_i^*, D_{i,1}^*, D_{i,2}^*, E_{i,1}, E_{i,2}, F_i^*)\}_{i \in [1,l]}, E^*, \tau^*)$.
- Game_2: The challenge ciphertext is $\mathrm{CT}_2^* = (Z, D^*, (C_1, Z_{1,1}, D_{1,2}^*, E_{1,1}^*, E_{1,2}^*, F_1^*), \{(C_i^*, D_{i,1}^*, D_{i,2}^*, E_{i,1}^*, E_{i,2}^*, F_i^*)\}_{i \in [2,l]}, E^*, \tau^*)$.
- ……
- Game_{l+1}: The challenge ciphertext is $\mathrm{CT}_{l+1}^* = (Z, D^*, \{(C_i, Z_{i,1}, D_{i,2}^*, E_{i,1}^*, E_{i,2}^*, F_i^*)\}_{i \in [1,l]}, E^*, \tau^*)$.
- Game_{l+2}: The challenge ciphertext is $\mathrm{CT}_{l+2}^* = (Z, D^*, (C_1^*, Z_{1,1}, D_{1,2}^*, Z'_{1,1}, E_{1,2}^*, F_1^*), \{(C_i^*, Z_{i,1}, D_{i,2}^*, E_{i,1}^*, E_{i,2}^*, F_i^*)\}_{i \in [2,l]}, E^*, \tau^*)$.
- ……
- Game_{2l+1}: The challenge ciphertext is $\mathrm{CT}_{2l+1}^* = (Z, D^*, \{(C_i^*, Z_{i,1}, D_{i,2}^*, Z'_{i,1}, E_{i,2}^*, F_i^*)\}_{i \in [1,l]}, E^*, \tau^*)$.
- Game_{2l+2}: The challenge ciphertext is $\mathrm{CT}_{2l+2}^* = (Z, D^*, \{(C_i^*, Z_{i,1}, D_{i,2}^*, Z'_{i,1}, E_{i,2}^*, F_i^*)\}_{i \in [1,l]}, Z_E^*, \tau^*)$.
- Game_{2l+3}: The challenge ciphertext is $\mathrm{CT}_{2l+3}^* = (Z, D^*, \{(C_i^*, Z_{i,1}, D_{i,2}^*, Z'_{i,1}, E_{i,2}^*, F_i^*)\}_{i \in [1,l]}, Z_E^*, Z_\tau^*)$.

The proof is completed by showing that the games Game_0, Game_1, …, Game_{2l+1}, Game_{2l+2} and Game_{2l+3} are computationally indistinguishable from each other. □

Lemma 1. *Assuming that the decisional $(q-1)$ assumption holds in G, and then there is no adversary that distinguishes between the games Game_0 and Game_1.*

Proof. Assume that there exists an adversary algorithm $\mathcal{A}$ that can distinguish Game_0 from Game_1. Then we can build a challenger algorithm $\mathcal{C}$ that solves the decisional $(q-1)$ problem. The proof

Table 1
Comparison of the storage overheads.

Schemes	Public parameter	Master private key	Private attribute-key	Ciphertext
$\mathcal{ABE}'$ [1]	11	5	$5k+3$	$6l+3+\lvert\mathbb{A}\rvert$
$\mathcal{ABE}$	12	5	$5k+3$	$6l+4+\lvert\mathbb{A}\rvert$

Table 2
Comparison of the computational costs.

Schemes	Encrypt		Decrypt	
	Expo	Pairing	Expo	Pairing
$\mathcal{ABE}'$ [1]	$8l+4$	0	$\leq \chi_2+2\chi_1$	$\leq 6\chi_2+\chi_1$
$\mathcal{ABE}$	$8l+2$	0	$\leq \chi_2$	$\leq 6\chi_2+\chi_1$

is similar to that in [1] except that the term E^* in the challenge ciphertext is calculated using the scheme $\mathcal{SE}$ with an additional element τ^*, and we omit the details here. □

Lemma 2. *Assuming that the decisional linear assumption holds in G, and then there is no adversary that distinguishes between the games $Game_{j+1}$ and $Game_j$ for $j \in [1, l]$.*

Proof. Assume that there exists an adversary algorithm $\mathcal{A}$ that can distinguish Game_j from Game_{j+1}. Then we can build a challenger algorithm $\mathcal{C}$ that solves the decisional linear problem. The proof is similar to that in [1] except that the term E^* in the challenge ciphertext is calculated using the scheme $\mathcal{SE}$ with an additional element τ^*, and we omit the details here. □

Lemma 3. *Assuming that the decisional linear assumption holds in G, and then the advantage of an adversary that can distinguish between the games $Game_{j+l+1}$ and $Game_{j+l}$ for $j \in [1, l]$ is negligible.*

Proof. This proof follows almost the same as that of Lemma 2, except that the simulation is done over the parameters g_3 and g_4 instead of g_1 and g_2. Thus, we omit the details here. □

Lemma 4. *Assuming that the symmetric encryption scheme $\mathcal{SE}$ is IND-CPA secure, and then the advantage of an adversary that can distinguish between the games $Game_{2l+1}$ and $Game_{2l+2}$ is negligible.*

Proof. This game Game_{2l+2} is the same as that in the game Game_{2l+1} except that in the challenge phase, algorithm $\mathcal{C}$ randomly chooses Z_E^* in the ciphertext space of $\mathcal{SE}$ in place of E^* rather than creating E^* as required. In the view of algorithm $\mathcal{A}$, this game Game_{2l+2} is identical to the game Game_{2l+1} except that algorithm $\mathcal{A}$ breaks the security of the scheme $\mathcal{SE}$. □

Lemma 5. *Assuming that H' is a secure pseudo-random function, and then the advantage of an adversary that can distinguish between the games $Game_{2l+2}$ and $Game_{2l+3}$ is negligible.*

Proof. This game Game_{2l+3} is the same as that in the game Game_{2l+2} except that in the challenge phase, algorithm $\mathcal{C}$ randomly chooses $Z_\tau^* \in \mathcal{M}$ in place of τ^* rather than generating τ^* as required. In the perspective of algorithm $\mathcal{A}$, this game Game_{2l+3} is identical to the game Game_{2l+1} except that algorithm $\mathcal{A}$ breaks the security of the pseudo-random function H'. □

This completes the proof of Theorem 1.

4.3. Performance evaluation and implementation

In this paper, we propose an expressive CP-ABE scheme supporting partially hidden access structures in the prime-order groups, which improves the efficiency of the one given in [1]. Denote l as the number of attributes in an access structure, k as the size of an attribute set possessed by each user, χ_1 as the number of elements in $I_{\mathbb{M},\rho} = \{\mathcal{I}_1, \ldots, \mathcal{I}_{\chi_1}\}$, χ_2 as $|\mathcal{I}_1| + \ldots + |\mathcal{I}_{\chi_1}|$. Let $|\mathbb{A}|$ be the size of an access structure. Table 1 shows the storage complexity of the proposed $\mathcal{ABE}$ and the scheme $\mathcal{ABE}'$ in [1] in terms of the sizes of the public parameter, the master private key, the private attribute-key and the ciphertext. It is straightforward to see that the proposed scheme $\mathcal{ABE}$ almost has the same storage overheads as the scheme $\mathcal{ABE}'$ in [1]. Table 2 compares the computational costs incurred by the encryption and decryption algorithms between the scheme $\mathcal{ABE}'$ in [1] and the scheme $\mathcal{ABE}$ proposed in this paper. It is not difficult to see that the proposed scheme $\mathcal{ABE}$ is more efficient than the scheme $\mathcal{ABE}'$ in [1].

Table 3
Computational costs of exponentiation and pairing operations.

Elliptic Curves (ms)	Expo of G	Expo of $\hat{G}$	Expo of G_1	Pairing
SS512	1.853	1.896	0.174	2.555
MNT159	0.649	5.351	1.212	9.237

The scheme $\mathcal{ABE}'$ in [1] and the scheme $\mathcal{ABE}$ in this paper are implemented in the Charm framework [31]. Both of them are transformed into that in the asymmetric setting (note that the assumptions and the security proofs in the symmetric groups can be converted to the asymmetric setting in a generic way [20]) before the implementation, since the Charm framework is designed under the asymmetric groups. Thus, three groups G, $\hat{G}$ and G_1 are used in the pairing function as $\hat{e} : G \times \hat{G} \to G_1$.

The experiments are conducted on a laptop running the 64-bit Ubuntu 16.04 with the Intel Core i5-4210U CPU @ 1.70GHz and 8.00 GB RAM. The Charm-0.43, the Python 3.4 and the PBC library (for the underlying cryptographic operations) are installed for the implementation.

The algorithms of both schemes $\mathcal{ABE}$ and $\mathcal{ABE}'$ are simulated over elliptic curves SS512 (a symmetric curve with a 512-bit base field) and MNT159 (an asymmetric curve with a 159-bit base field) to provide the security level of 80-bit. The average running time for exponentiation (i.e., Expo) and pairing operations over the groups of two curves is summarized in Table 3.

We focus on the computational overheads of the Encrypt and Decrypt algorithms in both schemes, as the computational overheads of the Setup and KeyGen algorithms in the schemes $\mathcal{ABE}$ and $\mathcal{ABE}'$ are close to each other. The performances of the encryption and decryption algorithms in the proposed scheme $\mathcal{ABE}$ and the scheme $\mathcal{ABE}'$ in [1] are shown in Fig. 3 in terms of the SS512 and MNT159 curves, respectively. With respect to the MNT159 curve, the average computation time of running the Encrypt algorithm to generate a ciphertext with an access policy of 1 attribute to 10 attributes ranges from 0.08s to 0.60s for the scheme $\mathcal{ABE}'$ in [1] and 0.05s to 0.40s for the proposed scheme $\mathcal{ABE}$, and the average computation time of running the Decrypt algorithm to decrypt a ciphertext with an access policy of 1 attribute to 10 attributes ranges from 8s to 61s for the scheme $\mathcal{ABE}'$ in [1] and 8s to 40s for the proposed scheme $\mathcal{ABE}$. Concerning the SS512 curve, the average computation time of running the Encrypt algorithm of generating a ciphertext with an access policy of 1 attribute to 10 attributes ranges from 0.03s to 0.30s for the scheme $\mathcal{ABE}'$ in [1] and 0.03s to 0.20s for the proposed scheme $\mathcal{ABE}$, and the average computation time of running the Decrypt algorithm to get the message from a ciphertext with an access policy of 1 attribute to 10 attributes ranges from 3s to 26s for the scheme $\mathcal{ABE}'$ in [1] and 2s to 21s for the proposed scheme $\mathcal{ABE}$.

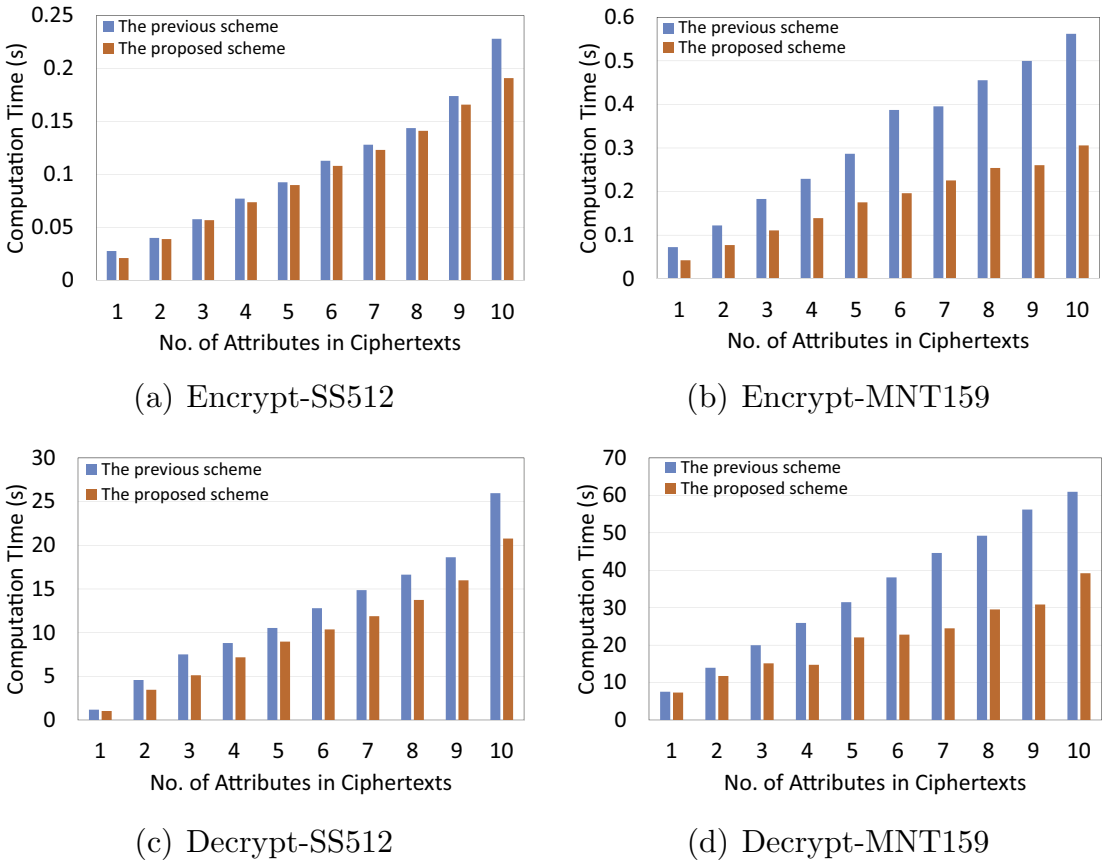

Fig. 3. Performance of the schemes $\mathcal{ABE}$ and $\mathcal{ABE}'$.

5. Conclusions

Ciphertext-policy attribute-based encryption (CP-ABE) has been considered as a useful technique to provide data security and privacy in cloud storage scenarios, as it enables data owners to upload their data in encrypted forms to the cloud while sharing them with users possessing certain credentials or attributes. However, a ciphertext produced by a CP-ABE scheme includes a clear access structure, which may leak some information about the privileged recipients or the underlying message of the ciphertext. To solve this problem, it has been suggested to use CP-ABE with partially hidden access structures (e.g., [9,15–18]) to generate the ciphertext such that the sensitive attribute values in the access structure of a ciphertext can be hidden from the public view. Unfortunately, many existing CP-ABE schemes with partially hidden access structures (e.g., [9,15–18]) either only support restricted access structures or are built in the inefficient composite-order groups. To our knowledge, there are few expressive CP-ABE schemes with partially hidden access structures that are built in the prime-order groups. In this paper, we revisited the expressive CP-ABE scheme with partially hidden access structures in [1], and improved its efficiency. After analyzing the security of the proposed scheme, we evaluated its performance by simulating its algorithms and those in [1].

Acknowledgments

This research work is supported by the Singapore National Research Foundation under the NCR Award No. NRF2014NCR-NCR001-012 and the AXA Research Fund.

References

[1] H. Cui, R.H. Deng, G. Wu, J. Lai, An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, in: Provable Security - 10th International Conference, ProvSec 2016, Nanjing, China, November 10–11, 2016, Proceedings, in: Lecture Notes in Computer Science, 10005, 2016, pp. 19–38.
[2] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, Y. Xiang, A secure cloud computing based framework for big data information management of smart grid, 2015.
[3] K. Liang, M.H. Au, J.K. Liu, W. Susilo, D.S. Wong, G. Yang, Y. Yu, A. Yang, A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing, Future Gener. Comp. Syst. 52 (2015) 95–108.
[4] K. Liang, W. Susilo, J.K. Liu, Privacy-preserving ciphertext multi-sharing control for big data storage, IEEE Trans. Inf. Forensics Secur. 10 (8) (2015) 1578–1589.
[5] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20–23 May 2007, Oakland, California, USA, IEEE Computer Society, 2007, pp. 321–334.
[6] L. Cheung, C.C. Newport, Provably secure ciphertext policy ABE, in: Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28–31, 2007, ACM, 2007, pp. 456–465.
[7] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption, in: Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30, - June 3, 2010. Proceedings, in: Lecture Notes in Computer Science, 6110, Springer, 2010, pp. 62–91.
[8] B. Waters, Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization, in: Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6–9, 2011. Proceedings, in: Lecture Notes in Computer Science, 6571, Springer, 2011, pp. 53–70.
[9] J. Lai, R.H. Deng, Y. Li, Expressive CP-ABE with partially hidden access structures, in: 7th ACM Symposium on Information, Computer and Communications Security, ASIACCS '12, Seoul, Korea, May 2–4, 2012, ACM, 2012, pp. 18–19.
[10] H. Qian, J. Li, Y. Zhang, J. Han, Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation, Int. J. Inf. Sec. 14 (6) (2015) 487–497.
[11] T.H. Yuen, J.K. Liu, M.H. Au, X. Huang, W. Susilo, J. Zhou, K-times attribute-based anonymous access control for cloud computing, IEEE Trans. Comput. 64 (9) (2015) 2595–2608.

[12] F. Xhafa, J. Wang, X. Chen, J.K. Liu, J. Li, P. Krause, An efficient PHR service system supporting fuzzy keyword search and fine-grained access control, Soft Comput. 18 (9) (2014) 1795–1802.
[13] K. He, J. Weng, J.K. Liu, W. Zhou, J. Liu, Efficient fine-grained access control for secure personal health records in cloud computing, in: Network and System Security - 10th International Conference, NSS 2016, Taipei, Taiwan, September 28–30, 2016, Proceedings, 2016, pp. 65–79.
[14] J. Katz, A. Sahai, B. Waters, Predicate encryption supporting disjunctions, polynomial equations, and inner products, J. Cryptol. 26 (2) (2013) 191–224.
[15] T. Nishide, K. Yoneyama, K. Ohta, Attribute-based encryption with partially hidden encryptor-specified access structures, in: Applied Cryptography and Network Security, 6th International Conference, ACNS 2008, New York, NY, USA, June 3–6, 2008. Proceedings, in: Lecture Notes in Computer Science, 5037, Springer, 2008, pp. 111–129.
[16] J. Li, K. Ren, B. Zhu, Z. Wan, Privacy-aware attribute-based encryption with user accountability, in: Information Security, 12th International Conference, ISC 2009, Pisa, Italy, September 7–9, 2009. Proceedings, in: Lecture Notes in Computer Science, 5735, Springer, 2009, pp. 347–362.
[17] J. Lai, R.H. Deng, Y. Li, Fully secure cipertext-policy hiding CP-ABE, in: Information Security Practice and Experience - 7th International Conference, ISPEC 2011, Guangzhou, China, May 30, - June 1, 2011. Proceedings, in: Lecture Notes in Computer Science, 6672, Springer, 2011, pp. 24–39.
[18] Y. Zhang, X. Chen, J. Li, D.S. Wong, H. Li, Anonymous attribute-based encryption supporting efficient decryption test, in: 8th ACM Symposium on Information, Computer and Communications Security, ASIA CCS'13, Hangzhou, China - May 08 - 10, 2013, ACM, 2013, pp. 511–516.
[19] D.M. Freeman, Converting pairing-based cryptosystems from composite-order groups to prime-order groups, in: Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30, - June 3, 2010. Proceedings, in: Lecture Notes in Computer Science, 6110, Springer, 2010, pp. 44–61.
[20] Y. Rouselakis, B. Waters, Practical constructions and new proof methods for large universe attribute-based encryption, in: 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4–8, 2013, ACM, 2013, pp. 463–474.
[21] X. Boyen, B. Waters, Anonymous hierarchical identity-based encryption (without random oracles), in: Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20–24, 2006, Proceedings, in: Lecture Notes in Computer Science, 4117, Springer, 2006, pp. 290–307.
[22] M. Fischlin, R. Fischlin, Efficient non-malleable commitment schemes, J. Cryptol. 24 (1) (2011) 203–244.
[23] A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, 2005, Proceedings, in: Lecture Notes in Computer Science, 3494, Springer, 2005, pp. 457–473.
[24] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine–grained access control of encrypted data, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, October 30 - November 3, 2006, in: Lecture Notes in Computer Science, 5126, Springer, 2006, pp. 89–98.
[25] V. Goyal, A. Jain, O. Pandey, A. Sahai, Bounded ciphertext policy attribute based encryption, in: Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7–11, 2008, Proceedings, Part II - Track B: Logic, Semantics, and Theory of Programming & Track C: Security and Cryptography Foundations, in: Lecture Notes in Computer Science, 5126, Springer, 2008, pp. 579–591.
[26] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, in: CRYPTO, in: Lecture Notes in Computer Science, 2139, Springer-Verlag, 2001, pp. 213–219.
[27] D. Boneh, X. Boyen, H. Shacham, Short group signatures, in: Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15–19, 2004, Proceedings, in: Lecture Notes in Computer Science, 3152, Springer, 2004, pp. 41–55.
[28] O. Goldreich, S. Goldwasser, S. Micali, How to construct random functions, J. ACM 33 (4) (1986) 792–807.
[29] A.B. Lewko, B. Waters, Decentralizing attribute-based encryption, in: Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15–19, 2011. Proceedings, in: Lecture Notes in Computer Science, 6632, Springer, 2011, pp. 568–588.
[30] A. Beimel, Secure Schemes for Secret Sharing and Key Distribution, Israel Institute of Technology, Israel Institute of Technology, 1996 Ph.D. thesis.
[31] J.A. Akinyele, C. Garman, I. Miers, M.W. Pagano, M. Rushanan, M. Green, A.D. Rubin, Charm: a framework for rapidly prototyping cryptosystems, J. Cryptograph. Eng. 3 (2) (2013) 111–128.

Hui Cui received her Ph.D. degree in the School of Computing and Information Technology, University of Wollongong, Australia. She then worked as a research fellow in the Secure Mobile Centre under the School of Information Systems, Singapore Management University, Singapore. Now, she is a research fellow in the School of Science, RMIT University, Melbourne, Australia.

Robert H. Deng has been a Professor at the School of Information Systems, Singapore Management University since 2004. Prior to this, he was Principal Scientist and Manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. His research interests include data security and privacy, multimedia security, network and system security. He has served/is serving on the editorial boards of many international journals in security, such as IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, the International Journal of Information Security, and IEEE Security and Privacy Magazine. He is the chair of the Steering Committee of the ACM Asia Conference on Computer and Communications Security (ASIACCS). He received the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006. He was named Community Service Star and Showcased Senior Information Security Professional by (ISC)2 under its Asia-Pacific Information Security Leadership Achievements program in 2010. He is Fellow of IEEE. conferences and journals, and served in the program committees for over 80 international conferences and workshops. Yingjiu Li is a senior member of the ACM and a member of the IEEE Computer Society. The URL for his web page is http://www.mysmu.edu/faculty/yjli/.