Attribute-based Encryption with Non-Monotonic Access Structures Supporting Fine-grained Attribute Revocation in M-healthcare

Yang Zhao, Pengcheng Fan, Haoting Cai, Zhiguang Qin and Hu Xiong

(Corresponding author: Hu Xiong)

School of Information and Software Engineering, University of Electronic Science and Technology of China[1]

No. 4, North Jianshe Road, Chenghua District, chengdu, Sichuan 610054, China

(Email: xionghu.uestc@gmail.com)

(Received July 21, 2016; revised and accepted Jan. 15, 2017)

Abstract

By sharing the personal health information (PHI) in the healthcare provider (HP) which is equipped with cloud servers, mobile-healthcare (m-healthcare) significantly promotes a huge revolution of medical consultation. Nonetheless there is a series of challenges such as PHI confidentiality and the attribute revocation. To deal with these problems, we propose a scheme based on the attribute-based encryption. The scheme which supports non-monotonic access structures and fine-grained attribute revocation is established over the composite order bilinear groups. By utilizing this scheme, we can well protect PHI and achieve the goal of revocation. Furthermore, the security analysis and comparison show that our scheme is more expressive despite of the lower efficiency.

Keywords: Attribute-based Encryption; Attribute Revocation; M-healthcare System; Non-monotonic Access Structures

1 Introduction

M-healthcare cloud computing system has been spread widely all over the world. Due to its high efficiency and accessibility for medical consultation, it has been increasingly adopted by world-renowned organizations such as the European Commission activities. Both patients and HP greatly benefit from its great convenience [11, 24].

M-healthcare cloud computing system can be considered as a huge social network. PHI collected by body area networks (BANs) should be securely transmitted to HP and shared among the authorized physicians. The authorized physicians may access the PHI to accomplish medical treatment [27, 36, 40].

In such situation, many issues should be considered, especially preventing the patients' PHI from being eavesdropped and tampered, and having the authorities of authorized physicians revoked.

In terms of the security aspects, access control for patients' PHI is one of the most important issues. Namely, only the authorized physicians can recover the patients' PHI . Therefore, how to share the patients' PHI and who should be shared with should be considered carefully. To solve these challenges, there were a variety of achievements [16, 23, 29, 31, 32, 37, 40].

Recently, the scheme [40] is constructed for securing the PHI along with a multi-level model which contains four entities - patient, directly authorized physician, indirectly authorized physician and unauthorized physician. The directly authorized physician can access the patient's PHI. The indirectly physician can only access the data authorized by the directly authorized physician. So the directly authorized physician owns all the privileges of patient and controls the data which the indirectly authorized physician can access. However, if the directly authorized physician is bribed, he can be capable of colluding with the indirectly physicians who do not satisfy the access control. Moreover, the directly authorized physician who is bribed can share the fake information with the indirectly authorized physicians [39]. As a result, this scheme may suffer from collusion attack and forgery attack.

In order to solve the problems mentioned above, we proposed a scheme. In this scheme, PHI confidentiality and the revocation of authorities can be achieved with high flexibility by utilizing the fine-grained attribute revocation and non-monotonic access structures. With the non-monotonic access structures [26], private keys can represent any access structures involving AND, OR, NOT, and threshold operations. To accomplish it, a set of attributes was selected as the universe. Then a set of d attributes was selected from the universe which was used to encrypt the ciphertext and the negation of remaining attributes represented the negated attributes. As for the normal Attribute-based Encryption (ABE) supporting NOT operation over access structures, there is no

choice but to add more negated attributes to the set, like "Not Nurse". Therefore, by utilizing our scheme, we can encrypt the patients' PHI flexibly with a smaller attribute set.

Moreover, we implemented fine-grained attribute revocation [34] in our scheme. By providing a revocation list for every attribute, the scheme supports attribute/user revocation. So access control of PHI confidentiality can be achieved flexibly. By making use of the above methods, the authorities of physicians can be well controlled. Our contributions are outlined below:

1) We propose a new attribute-based encryption with non-monotonic access structures supporting fine-grained attribute revocation. our scheme achieves the goals of PHI confidentiality and the revocation of authorities.

2) For the first time, we bring attribute-based encryption with non-monotonic access structures and fine-grained attribute revocation into m-healthcare cloud computing system, which can flexibly achieve PHI confidentiality.

3) The security analysis is provided in this paper and we compared it with existing works to show the advantages and disadvantages of our scheme.

2 Related Work

2.1 Attribute-based Encryption

In the identity-based encryption (IBE) system, the public key to encrypt the message is the unique identity of user [6]. In order to send the ciphertext to the user, the data owner has to know the user's identity. Biometrics are always considered as the best carrier for user identity. In the Fuzzy IBE (FIBE) [30] which was Sahai and Waters firstly proposed, the identity was characterized as a set of attributes. The ciphertext which was encrypted by the set ω could be decrypted by the attributes set ω' only if $|\omega' \bigcap \omega| \geqslant d$, where d denotes the threshold. In 2006, Goyal, Sahai and Waters et al. [13] expanded the FIBE to ABE. In ABE, the identity information of user was generalized to attributes related to user identity. According to the relation between access structure and ciphertext or private key, ABE was categorized into key policy ABE (KP-ABE) and ciphertext policy ABE (CP-ABE) [3]. Moreover, they also provided a basic security property namely collusion resistance which could prevent adversary from decrypting the ciphertext illegally by cooperation. Then Chase et al. [7] made use of a certificate authority (CA) and multi authorities to prevent single authority from being corrupted. In this scheme they utilized globally unique identifier (GUID) to defend collusion attack.

In 2008, Bethencourt, Sahai and Waters [4] proposed the first CP-ABE scheme supporting tree access structure. The scheme defended collusion attack by using different random numbers for various private keys. In the same year, Cheung and Newport [9] introduced a provably secure CP-ABE based on standard model and the decisional bilinear Diffie-Hellman (DBDH) assumption. However, the scheme only supported AND operation. Considering the adaptive security, partitioning reduction could not be well applied into ABE. Dual system encryption [35] provided a new way to solve this problem. Lewko and Waters [17] constructed the first adaptive security ABE scheme by utilizing the dual system encryption. Due to involving the composite order bilinear maps, the scheme requires an extremely large group order which also results in low efficiency. Subsequently, the first adaptive security ABE based on prime order was proposed by Okamoto and Takashima [25]. The scheme effectively implemented the dual system encryption by using dual paring vector space. Although its efficiency had been greatly improved, there was always existing a gap comparing with selective security model. To improve the efficiency, various constant-size ciphertext ABE schemes [21, 33, 38] were constructed in different ways. Furthermore, in 2015, Gorbunov et al. [12] presented an ABE scheme for circuits of any arbitrary polynomial size, which could be a new framework for constructing ABE schemes.

2.2 Attribute Revocation

Attribute revocation can be classified as direct revocation and indirect revocation. Direct revocation performs revocation directly by the encryptor who establishes and updates the revocation list. Indirect revocation performs revocation indirectly by the private key authority which publishes private keys periodically. In practical scenarios, attribute revocation is conundrum waiting to be addressed [8, 22].

In 2006, Pirretti et al. [28] introduced a scheme to implement indirect revocation by revoking the latest version of users' attributes to achieve the goal. Prior to encryption, encryptor should negotiate with the authority to confirm the validity duration of attributes. Furthermore, users and authority must accomplish key update periodically online. Then Bethencourt et al. [4] put the expiry date of attributes into ciphertext to implement revocation and solved the problem of negotiation between encryptor and authority. Afterward, binary tree was used to revoke user [5] through updating the minimum set of unrevoked users. However, the drawback was that it only supported user revocation.

In 2007, Ostrovsky et al. [26], for the first time, presented a direct revocation scheme based on the ABE. But the size of ciphertext and key was slightly large. To reduce the expense of revocation, Attrapadung et al. [2] proposed a direct revocation scheme on KP-ABE and CP-ABE in conjunction with broadcast encryption. The advantage was that revocation would not influence other users. In 2011, Asim et al. [1] constructed a direct revocation scheme by taking advantage of polynomial to share secret. In this scheme, all revoked users' secret shares were put

into ciphertext, so that only authorized users can get message when decrypting. However the complexity of pairing calculation involved the count of revoked users, which resulted in its low efficiency. Then, [20] were proposed to achieve fine-grained revocation. However, the defect was that only an attribute of user could be revoked in an encryption. Until 2012, the direct revocation [34] was firstly introduced to supporting fully fine-grained attribute revocation by specifying a revocation list for every attribute. Recently, several applications of healthcare [10, 14] based on the fine-grained attribute revocation have been constructed.

3 Preliminaries

3.1 Definitions

Definition 1 (Access Structure). Let $\{P_1, ..., P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P1,...,Pn\}}$ is monotonic, for $\forall B$ and C, if $B \subseteq \mathbb{A}$ and $B \subseteq C$ then $C \subseteq \mathbb{A}$. An monotonic access structure is a monotonic collection $\mathbb{A}$ of non-empty subsets of $\{P_1, P_2, ..., P_n\}$, namely, $\mathbb{A} \subseteq 2^{\{P_1,P_2,...,P_n\}} \setminus \{\emptyset\}$. The sets in $\mathbb{A}$ are regarded as authorized sets and the sets not in $\mathbb{A}$ are unauthorized sets.

Definition 2 (Linear Secret-Sharing Schemes [26]). Call a secret-sharing scheme Π which depends on a set of parties $\mathcal{P}$ as linear (over $\mathbb{Z}_p$), if it satisfies the followings.

1) A vector over $\mathbb{Z}_p$ is composed by the shares for each party.

2) The share-generating matrix for Π is the name of A matrix M which consists of $n+1$ columns and l rows. For all $i = 1, ..., l$, mark the i'th row of M with a party $\breve{x}_i \subseteq \mathcal{P}$. The column vector $v = (s, r_1, r_2, ..., r_n)$, in which $s \subseteq \mathbb{Z}_p$ is the secret to be shared, $r_1, r_2, ..., r_n \subseteq \mathbb{Z}_p$ are chosen at random. Based on Π, l shares of which Mv is the vector make up the secret s. Correspond to $\breve{x}_i$ there exists a $(Mv)_i$.

On the basic of the above definitions there is a linear secret sharing-scheme (LSSS), which observes the definitions as follows: assume that for the access structure $\mathbb{A}$ there exists a LSSS Π. S is an authorized set that belongs to $\mathbb{A}$. Let $I = \{i : \breve{x}_i \in S\}$ and let $\{\lambda_i\}$ is a valid share of s, there is $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$, then $\sum_{i \in I} \omega_i \lambda_i = s$.

3.2 Non-Monotonic Access Structures

With the negated attributes, we can construct non-monotonic access structures based on the ABE monotonic access structures. To accomplish it, a set of attributes is selected as the universe. From the universe, a set of d attributes is selected to encrypt a ciphertext was setup by the authority. Attributes in the set were called positive attributes and the negation of remaining attributes were called negated attributes. To recover the ciphertext, the decryptor must have at least $d+1$ attributes to perform an interpolation. Moreover the decryptor has to check the rest namely the one point, if the point differs from the d attributes and it is in the negated attributes, then decryptor has the privilege to achieve the share of message. Otherwise, the decryptor can not obtain the message.

At first, there is a set of attributes $\mathcal{P}$ in which the attribute $\breve{x}$ can be positive like x or negated (the negation of attribute) like x'. $\mathcal{A}$ is a set of monotonic access structures over $\mathcal{P}$ for which we given a LSSS $\{\Pi_{\mathbb{A}}\}_{\mathbb{A} \in \mathcal{A}}$. $\tilde{\mathcal{A}}$ is a family of non-monotonic access structures over $\tilde{\mathcal{P}}$ including all positive attributes of $\mathcal{P}$. For $\forall \mathbb{A} \in \mathcal{A}$, there exists a non-monotonic access structure $\tilde{\mathbb{A}}$. Let $\tilde{S} \subset \tilde{\mathcal{P}}, N(\tilde{S}) \subset \mathcal{P}$, namely, the attributes in $\tilde{S}$ are positive, but the attributes in $N(\tilde{S})$ may be positive or negated. Then let $\tilde{S} \subset N(\tilde{S})$. For every attribute $x \in \tilde{\mathcal{P}}$ but $x \notin \tilde{S}$, we have $x' \in N(\tilde{S})$. Therefore, $N(\tilde{S})$ include all attributes in S and the other negated attributes not in S. So corresponding to the monotonic access structure $\mathbb{A}$ over $N(\tilde{S})$ there is a non-monotonic access structure $\tilde{\mathbb{A}}$ over $\tilde{S}$.

3.3 Mathematical Background

Composite Order Bilinear Maps. Let $N = p_1 p_2 p_3$ (p_1, p_2, p_3 are primes and different from each other), $\mathbb{G}, \mathbb{G}_T$ are cyclic groups of order N. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ denote a bilinear map. e is a valid bilinear map from G to G_T if e satisfies the properties as follows:

1) **Bilinear**: $\forall a, b \in \mathbb{Z}_N, e(g^a, g^b) = e(g, g)^{ab}$

2) **Non-degenerate**: There exists $g \in \mathbb{G}$ that make N is the order of $e(g, g)$.

3) **Computable**: For $\forall u, v \in G, e(u, v)$ is computable.

Lagrange Coefficients. For $\forall i \in \mathbb{Z}_p$ and a set $S \in \mathbb{Z}_p$, there is $\triangle_{i,S} = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$. By utilizing the collision-resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p^*$, we can link every attribute with one and only element in $\mathbb{Z}_p^*$.

3.4 Assumption

The Decisional Bilinear Diffie-Hellman (BDH) Assumption. The decisional BDH assumption is that: Choose randomly $a, b, c, z \in \mathbb{Z}_p$, any polynomial-time adversaries can not distinguish the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^{abc})$ from the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^z)$.

4 System Model

HP is honest but curious, which means HP will try to find as much PHI stored in cloud servers as possible, but it will observe the rules honestly. In a sense, the HP may be corrupted by some malicious users, moreover, some users may want to achieve authories beyond theirs. Since the HP is not considered to be fully trusted, the HP must

support patient to specify the access structure to control the data decryption. The main requirements of this scheme are presented as follows:

1) Confidentiality. Since the data storage is provided by the HP, the data should not be leaked even though HP is attacked by malicious users. At the same time, the unauthorized physicians who do not satisfy the access policy can not gain the plaintext of PHI.

2) *Revocability.* While patient has updated the revocation list, the physicians who possess the attributes revoked by patient can not decrypt ciphertext successfully.

In this paper, to guarantee the correctness of the scheme, we consider the transport channel is fully secure. Before giving the concrete construction, we illustrate our framework in Figure 1. There are five entities in our framework:

- Patient: Patient is equipped with sensors in body area. Sensors can collect PHI of patient and transmit the PHI to mobile. Patient who owns the PHI, has the privilege to specify the access structure and update the revocation list.
- Mobile: Mobile is a transmitter which is used to accept the PHI and transmit ciphertext of PHI to Base Station.
- Base Station: Base station is the repeater between Mobile and HP. Via base station, data is sent by Mobile can be transmitted to HP.
- Healthcare Provider (HP): The cloud infrastructures including processors, bandwidth, storage etc are preserved by HP. We suppose that the storage space, bandwidth, computing performance of HP can be expandable, so that HP owns powerful performance. In our system, HP provides several functions as follows: data storage, key distribution, data transmission, an update of revocation list.
- Physician: Serving as the end of the system, physician is the decryptor who can achieve PHI depending on his attributes.

The basic architecture of M-healthcare includes three components: body area networks (BANs), wireless transmission and healthcare which are illustrated in Figure 1. Via wireless transmission, the ciphertext of PHI is transmitted from BANs to healthcare. The system operates as follows:

At first, the sensors in body area collect the patient's PHI and transmit PHI securely to Mobile. Mobile will encrypt the PHI based on various sets of attributes which are chosen from the universe negotiated by patient and HP. Then mobile transmits the encrypted data to HP via base station. Finally, if the attributes that physician possesses satisfy the access structure and the physician's ID is not in the revocation list, HP will generate private key for physician. The authorized physicians may gain PHI.

5 Our Construction

In this section, we will give concrete construction of ABE with non-monotonic access structures supporting fine-grained attribute revocation, which involves quadruplicate algorithm: *Setup*, *Encryption*, *Key Generation* and *Decryption*. In our system, we consider the two users patient and physician as the encryptor and the decryptor respectively.

Let $N = p_1p_2p_3(p_1,\ p_2,\ p_3$ are primes and different), $\mathbb{G}$, $\mathbb{G}_T$ are cyclic groups of order N. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ denote a bilinear map where e is the generation of $\mathbb{G}_{p_1}$, and Y is the generation of $\mathbb{G}_{p_2}$.

Setup$(1^\lambda, d, n)$: The parameter d specifies the count of attributes for every ciphertext. Let positive attributes set $\tilde{S} = \{1, 2, ..., d\}$ and the user identity set $U = \{1, 2, ..., n\}$. Choose $t_i, \mu_i \in \mathbb{Z}_{p_1}$ randomly, for any attribute $i \in \tilde{S}$, compute $T_i = g^{t_i}, h_i = g^{\mu_i}$. Then, choose $c \in \mathbb{Z}_{p_1}$ randomly, for any $i \in \{1, 2, ..., n, n+2, ..., 2n\}$, compute $f_i = g^{c^i}$. Choose two secrets $\alpha, \beta \in \mathbb{Z}_{p_1}$ uniformly at random, and compute $g_1 = g^\alpha$ and $g_2 = g^\beta$. Choose two polynomials $h(x)$ and $q(x)$ of degree d randomly with the constraint is that $q(0) = \beta$. ($h(x)$ has no constraint.) Finally, choose a from $\mathbb{Z}_{p_1}$ randomly. The published public parameters are:

$$\begin{aligned} PK \quad = \quad & (N, g, g^a, g_1, g_2; g^{q(1)}, g^{q(2)}, ..., g^{q(d)}; g^{h(0)}, \\ & g^{h(1)}, ..., g^{h(d)}; \{T_i\}_{i\in\tilde{S}}, \{h_i\}_{i\in\tilde{S}}, \\ & \{f_i\}_{i\in\{1,2,...,n,n+2,...,2n\}}). \end{aligned}$$

The master key is:

$$MK = (\alpha, a, c, \{t_i, \mu_i\}_{i\in\tilde{S}}, Y).$$

The functions $T, V{:}\mathbb{Z}_{p_1}{\to}\mathbb{G}_{p_1}$ are defined by the public parameters, which are public and computable. Then, compute:

$$T(x) = g_2^{x^d} \cdot g^{h(x)}, V(x) = g^{q(x)}.$$

Encryption$(M, \tilde{S}, PK)$: Message $M \in \mathbb{G}_T$, then encrypt M(M can be PHI) under $\tilde{S}$. Then,choose $s, y \in \mathbb{Z}_{p_1}$ at random, and computes:

$$E^{(1)} = Me(g_1, g_2)^s \cdot e(f_1, f_n)^y,\ E^{(2)} = g^s,\ E^{(3)} = (g^a)^y$$

For any $x \in \tilde{S}$, then computes:

$$E_x^{(4)} = T(x)^s,\ E_x^{(5)} = V(x)^s$$

Choose a d degree polynomial $l(x)$ randomly with the constraint is $l(0) = y$. For any $x{\in}\tilde{S}$, S_x is the non-revocation list, R_x is the revocation list, let $S_x = U - R_x$ ($S_x \neq \varnothing$), then computes:

$$E_x^{(6)} = g^{l(x)},\ E_x^{(7)} = T_x^{l(x)}$$

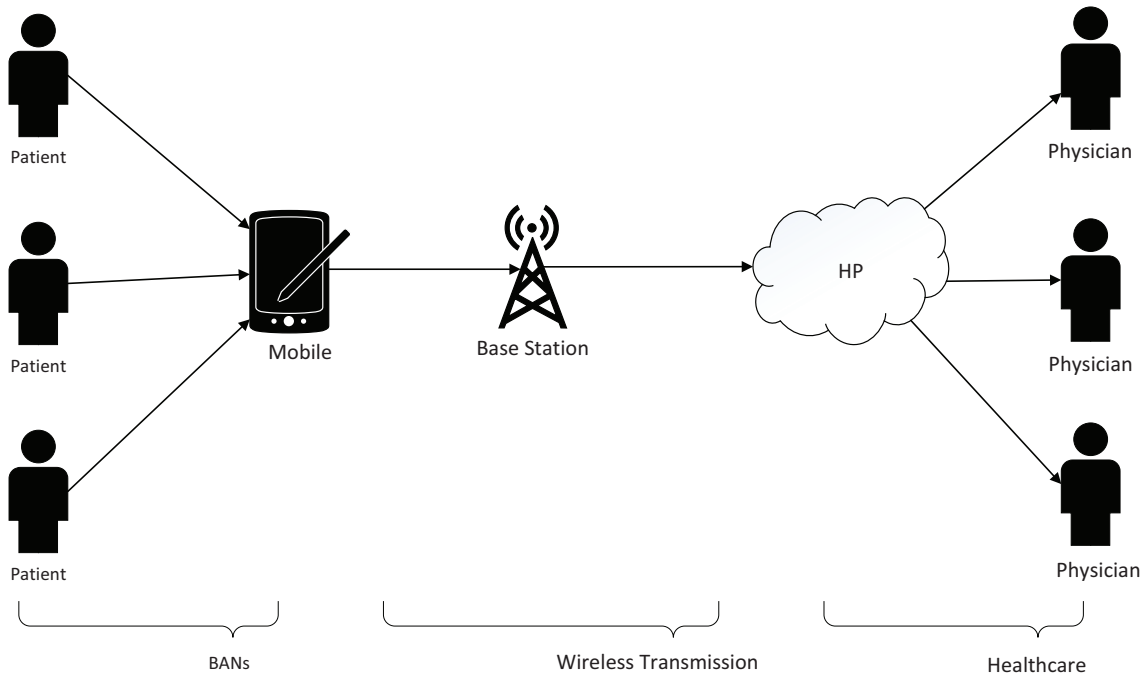

Figure 1: A basic architecture of M-healthcare

If $S_x \neq U$ namely $R_x \neq \varnothing$, choose η_x, s_x from $\mathbb{Z}_{p_1}$ at random and computes:

$$\begin{aligned} E_x^{(8)} &= g^{\eta_x}(h_x \prod_{j\in S_x} f_{n+1-j})^{l(x)}, \\ E_x^{(9)} &= g^{s_x}, \\ E_x^{(10)} &= g^{\eta_x}(\prod_{j\in R_x} f_{n+1-j})^{s_x} \end{aligned}$$

Remark: $\eta_x, s_x, E_x^{(9)}, E_x^{(10)}$ are used to randomize $E_x^{(8)}$ which is used for revocation to prevent $e(g_1, g_n)^{l(x)}$ from being computed by the potential adversary. If $S_x = U$ namely $R_x = \varnothing$, then computes:

$$E_x^{(8)} = (h_x \prod_{j\in S_x} f_{n+1-j})^{l(x)},\ E_x^{(9)} = E_x^{(10)} = 1$$

Namely:

$$\eta_x = s_x = 0$$

Then output the ciphertext as:

$$\begin{aligned} E = (\gamma, E^{(1)}, E^{(2)}, \{E_x^{(3)}, E_x^{(4)}, E_x^{(5)}, E_x^{(6)}, E_x^{(7)}, E_x^{(8)}, \\ E_x^{(9)}, E_x^{(10)}\}_{x\in\tilde{S}}). \end{aligned}$$

Key Generation$(\tilde{\mathbb{A}}, MK, PK)$: Except for the attributes which are in $\tilde{\mathbb{A}}$(suppose that can be checked efficiently), if the negation of remaining attributes are not the negated attributes of $N(\tilde{S})$, this algorithm will generate the private components for user with which the users can decrypt the ciphertext and obtain the data. By utilizing the LSSS to obtain the shares $\{\lambda_i\}$ of the secret α. We also select a $r_i \in \mathbb{Z}_{p_1}$ for each i.

For each $i, \tilde{x}_i$ is positive, we have:

$$D_i^{(1)} = g_2^{\lambda_i} \cdot T(x_i)^{r_i},\ D_i^{(2)} = g^{r_i}$$

The fine-grained attribute revocation performs under the set of positive attributes. At first, choose t, ξ_i from $\mathbb{Z}_{p_1}$ and Y_0 from $\mathbb{G}_{p_3}$ randomly. Then compute:

$$D_i^{(3)} = g^t Y_0,\ D_i^{(4)} = g^{at+c^{ID}\mu_i+t_i\xi_i} Y_{i,1},\ D_i^{(5)} = g^{\xi_i} Y_{i,2}$$

Then we can achieve the key component for positive attribute x:

$$D_i = (D_i^{(1)}, D_i^{(2)}, D_i^{(3)}, D_i^{(4)}, D_i^{(5)})$$

For each $i, \tilde{x}_i$ is negated, we have:

$$D_i^{(6)} = g_2^{\lambda_i+r_i},\ D_i^{(7)} = V(x_i)^{r_i},\ D_i^{(8)} = g^{r_i}$$

Then we can get the key component for negated attribute x':

$$D_i = (D_i^{(1)}, D_i^{(2)}, D_i^{(6)}, D_i^{(7)}, D_i^{(8)})$$

For all of the shares i, the private key D for decryptor to decrypt the ciphertext is made up of D_i.

Decryption(E, D): E and D are given as a ciphertext and private key. The decryption perform as follows: Let $I = \{i : \tilde{x} \in N(\tilde{S})\}$. An efficient process related to the LSSS can generate a set of coefficients $\Omega = \{\omega_i\}_{i\in I}$ which satisfy $\Sigma_{i\in I}\omega_i\lambda_i = \alpha$ (the λ_i, α is unknown to the decryption).

For each i, $\tilde{x} \in N(\tilde{S})$ and $x_i \in \tilde{S}$, namely the attribute is positive, we have:

$$\begin{aligned} Z_i &= e(D_i^{(1)}, E^{(2)})/e(D_i^{(2)}, E_i^{(2)}) \\ &= e(g_2^{\lambda_i} \cdot T(x_i)^{r_i}, g^s)/e(g^{r_i}, T(x)^s) \\ &= e(g_2, g)^{s\lambda_i} \end{aligned}$$

For each i, $\tilde{x} \in N(\tilde{S})$ and $x_i' \notin \tilde{S}$, namely the attribute is negated. Let $\tilde{S}_i = \tilde{S} \cup \{x_i'\}$, then $|\tilde{S}_i| = d+1$. Based on the function $V(x)$ and $\tilde{S}_i$, compute lagrangian coefficients $\{\sigma_x\}_{x\in\tilde{S}_i}$ which satisfy $\Sigma_{x\in\tilde{S}_i}\sigma_x qx = q(0) = \beta$, then compute:

$$\begin{aligned} Z_i &= \frac{e(D_i^{(6)}, E^{(2)})}{e(D_i^{(8)}, \prod_{x\in\tilde{S}}(E_x^{(5)})^{\sigma_x}) \cdot e(D_i^{(7)}, E^{(2)})^{\sigma_{x_i}}} \\ &= \frac{e(g_2^{\lambda_i + r_i}, g^s)}{e(g^{r_i}, \prod_{x\in\tilde{S}}(V(x)^s)^{\sigma_x}) \cdot e(V(x_i)^{r_i}, g^s)^{\sigma_{x_i}}} \\ &= \frac{e(g_2^{\lambda_i}, g^s) \cdot e(g_2^{r_i}, g^s)}{e(g^{r_i}, g^{s\sum_{x\in\tilde{S}}\sigma_x q(x)}) \cdot e(g^{r_i\sigma_{x_i}q(x_i)}, g^s)} \\ &= \frac{e(g_2, g)^{s\lambda_i} \cdot e(g, g)^{r_i s\beta}}{e(g, g)^{r_i s\sum_{x\in N(\tilde{S})}\sigma_x q(x)}} \\ &= e(g_2, g)^{s\lambda_i} \end{aligned}$$

Then compute the revocation component. At first, let $L = \{x_i | x_i \in \tilde{S}, ID \notin R_x\}$. For each $x \in L$, then compute:

$$\begin{aligned} X_i &= \frac{e(D_i^{(4)}, E_x^{(6)})e(E_x^{(6)}, \prod_{j\in S_x, j\neq ID} f_{n+1-j+ID})e(f_{ID}, E_x^{(10)})}{e(D_i^{(5)}, E_x^{(7)})e(f_{ID}, E_x^{(8)})e(E_x^{(9)}, \prod_{j\in R_x} f_{n+1-j+ID})} \\ &= \frac{e(g^{at}, g^{l(x)})}{e(f_1, f_n)^{l(x)}} \end{aligned}$$

Finally, let $A = \{i : x_i \in \tilde{S}\}$, the message is achieved by decryption as follows:

$$\begin{aligned} \frac{E^{(1)}}{\prod_{i\in I} Z_i} \cdot \frac{\prod_{i\in A} X_i}{e(D_i^{(3)}, E^{(3)})} &= \frac{Me(g_1, g_2)^s e(f_1, f_n)^y \cdot e(g^{at}, g^y)}{e(g_2, g)^{s\alpha} \cdot e(f_1, f_n)^y e(g^t, g^{ay})} \\ &= M \end{aligned}$$

Discussion. By utilizing our scheme, the patient can encrypt the PHI by specifying a set of attributes. The fine-grained attribute revocation supports that the patient revokes the attribute of physicians, such as revoking the physicians who possess the attribute "Nursing Care". So the physicians who hold the attribute can not access the PHI. According to the non-monotonic access structures, not only the encryption of the PHI was using less attributes but also NOT operation over the access structure can be achieved. The goal of PHI confidentiality can be attained flexibly.

6 Analysis

6.1 Security Analysis

In our scheme, a physician who can recover the data from ciphertext, must be an unrevoked user with valid authority. Therefore, we will analyse the security from two aspects that revocation and decryption.

At first, from the aspect of revocation, the adversary is an revoked user. If he wants to recover the data from $E^{(1)}$, what he must compute is $e(f_1, f_n)^y$ which is for revocation. But for y, there is a d degree polynomial $l(x)$ and the constraint is $l(0) = y$. Moreover, $y, l(x)$ are chosen randomly and the scope of $y, l(x)$ is the encryption algorithm. Therefore the y can not be computed. The only way to compute $e(f_1, f_n)^y$ is relying on the X_i. Note that if an attribute of the set of adversary is revoked, then he can only compute the result $e(g^{at}, g^{l(x)}) \cdot e(f_1, f_n)^{s_x}$. Due to the s_x is a random value, that is to say, the adversary can not compute $e(g^{at}, g^{l(x)})$. Namely the adversary can not compute $e(f_1, f_n)^y$.

Then, from the aspect of decryption, the adversary is an unrevoked user without valid authority, so he can gain the $e(f_1, f_n)^y$ legitimately. To prove he can attack the scheme, he should recover M from $Me(g_1, g_2)^s$. According to the decisional BDH assumption, think of $A = g_1 = g^\alpha, B = g_2 = g^\beta, C = g^s, Z = e(g_1, g_2)^s = e(g, g)^{\alpha\beta s}$, namely $a = \alpha, b = \beta, c = s$. Considering the M' is the message which is achieved by the adversary, if $M' \neq M$, then the adversary can not recover the message, otherwise $M' = M$, where $z = \alpha\beta s$, namely the adversary can distinguish the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^{abc})$ from the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^z)$. In other words, the adversary can solve the decisional BDH assumption. As a result, the semantic security of our scheme is that the construction can be easily broken by the adversary who can solve the decisional BDH assumption. However, the decisional BDH assumption is proven to be a hard problem to be solved.

6.2 Comparison

In this section, we compare our scheme with some existing works which are similar to our scheme in attribute-based encryption and healthcare.

There are three schemes [15, 18, 19] to be compared with our scheme. The first scheme [15] is a ciphertext-policy attribute-based encryption (CP-ABE) scheme, which applies direct revocation to revoke user or attribute. The difference of revocation between this paper and our scheme is that this paper makes use of a mediator who holds a revocation list to implement revocation. In the revocation list, there is a set of user identities which are respectively related to a set of attributes. The second scheme [18] is a multi-authority attribute-based encryption (MA-ABE) scheme and the third scheme [19] is a key-policy attribute-based encryption (KP-ABE) scheme, which all take advantage of the indirect revocation. Based on the indirect revocation, the second and third scheme have to rely on the authority to enforce revocation, which means the ciphertext and users' private key must be updated. Moreover the second scheme does not support revoking attributes. Further, the three schemes do not support non-monotonic access structures which means they can not support NOT operation over access structure. If a patient wants to encrypt the PHI with negated attributes

Table 1: Property comparison

Schemes	[15]	[18]	[19]	Ours
Encryption type	CP-ABE	MA-ABE	KP-ABE	KP-ABE
Revocation type	Direct	Indirect	Indirect	Direct
User revocation	√	√	√	√
Attribute revocation	√	×	√	√
Non-monotonic	×	×	×	√

Table 2: Computation comparison

Schemes	[15]	[18]	[19]	Ours
Key generation	$(2n+1)e$	$(n+1)e$	$(n+1)e$	$6ne$
Encryption	$(n+1)e+e_T$	$e_T+(n+1)e$	$e_T+(n+1)e$	$2e_T+(3n+2)e$
Decryption	$(3n+1)e_T+2np$	$(n+1)(p+e_T)$	$(n+1)(p+e_T)$	$(3n+5k)p+(n-k)e_T+(n-k)e$

by utilizing the above schemes, he has to input more attributes, for example, "Nurse" and "Not Nurse" and so on. Certainly, to accomplish the non-monotonic access structures in our scheme, we must sacrifice efficiency.

In addition, we present the theoretical comparison with the above schemes in Table 1 and Table 2 respectively for property and computation. The explanation of notations defined by us in tables are as follows: p, e_T and e represent the computation cost of a bilinear pairing, an exponentiation in $\mathbb{G}_T$ and an exponentiation in $\mathbb{G}$, respectively. Due to positive attributes and negated attributes in our scheme, k denotes the count of positive attributes.

7 Conclusions

In the paper, for the first time, we proposed an ABE scheme with non-monotonic access structures supporting fine-grained attribute revocation in m-healthcare. The advantage is that we provide a flexible solution for access control of m-healthcare. However, there exists some problems such as the slightly large size of ciphertext and the lower efficiency. The next step is to reduce the size of ciphertext and improve the efficiency while ensuring the properties of the scheme.

Acknowledgments

This work was supported in part by the National Science Foundation of China (No. 61370026), the National High Technology Research and Development Program of China (No. 2015AA016007), the Sichuan Key Technology Support Program (No. 2014GZ0106), Science Technology Project of Guangdong Province (No. 2016A010101002) and Fundamental Research Funds for the Central Universities under Grant ZYGX2016J091.

References

[1] M. Asim, L. Ibraimi, and M. Petković, "Ciphertext-policy attribute-based broadcast encryption scheme," in *Communications and Multimedia Security*, pp. 244–246, 2011.

[2] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in *Pairing-Based Cryptography (Pairing'09)*, pp. 248–265, 2009.

[3] M. Bayat, M. Aref, "An attribute based key agreement protocol resilient to KCI attack," *International Journal of Electronics and Information Engineering*, vol. 2, no. 1, pp. 10–20, 2015.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.

[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM Conference on Computer and Communications Security*, pp. 417–426, 2008.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (CRYPTO'01)*, pp. 213–229, 2001.

[7] M. Chase, "Multi-authority attribute based encryption," in *Theory of cryptography*, pp. 515–534, 2007.

[8] Y. Chen and J. Chou, "On the privacy of user efficient recoverable off-line e-cash scheme with fast anonymity revoking," *International Journal of Network Security*, vol. 17, no. 6, pp. 708–711, 2015.

[9] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM Conference on Computer and communications security*, pp. 456–465, 2007.

[10] M. K. Debnath, S. Samet, and K. Vidyasankar, "A secure revocable personal health record system with policy-based fine-grained access control," in *13th Annual Conference on Privacy, Security and Trust (PST'15)*, pp. 109–116, 2015.

[11] L. Gatzoulis and I. Iakovidis, "Wearable and portable ehealth systems," *Engineering in Medicine and Biology Magazine*, vol. 26, no. 5, pp. 51–56, 2007.

[12] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," *Journal of the ACM*, vol. 62, no. 6, pp. 45–78, 2015.

[13] V. Goyal, O. Pandey, A. Sahai, and 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*, pp. 89–98, 2006.

[14] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu, and K. R. Choo, "Fine-grained database field search using attribute-based encryption for e-healthcare clouds," *Journal of medical systems*, vol. 40, no. 11, p. 235, 2016.

[15] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Information security applications*, pp. 309–323, 2009.

[16] H. Jung and K. Chung, "Phr based life health index mobile service using decision support model," *Wireless Personal Communications*, vol. 86, no. 1, pp. 315–332, 2016.

[17] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology (EUROCRYPT'10)*, pp. 62–91, 2010.

[18] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in *International Conference on Security and Privacy in Communication Systems*, pp. 89–106, 2010.

[19] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[20] Q. Li, D. Feng, and L. Zhang, "An attribute based encryption scheme with fine-grained attribute revocation," in *Global Communications Conference (GLOBECOM'12)*, pp. 885–890, 2012.

[21] Q. Li, H. Xiong, F. Zhang, and S. Zeng, "An expressive decentralizing kp-abe scheme with constant-size ciphertext.," *International Journal of Network Security*, vol. 15, no. 3, pp. 161–170, 2013.

[22] C. Liu, W. Hsien, C. Yang, and M. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[23] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption," *Future Generation Computer Systems*, vol. 52, pp. 67–76, 2015.

[24] O. G. Morchon and H. Baldus, "Efficient distributed security for wireless medical sensor networks," in *International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp. 249–254, 2008.

[25] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in *Advances in Cryptology (CRYPTO'10)*, pp. 191–208, 2010.

[26] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 195–203, 2007.

[27] M. B. Parish and P. Yellowlees, "The rise of person-centered healthcare and the influence of health informatics and social network applications on mental health care," in *Mental Health Informatics*, pp. 17–39, 2014.

[28] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," *Journal of Computer Security*, vol. 18, no. 5, pp. 799–837, 2010.

[29] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," *International Journal of Information Security*, vol. 14, no. 6, pp. 487–497, 2015.

[30] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology (EUROCRYPT'05)*, pp. 457–473, 2005.

[31] S. Sarpong, C. Xu, and X. Zhang, "An authenticated privacy-preserving attribute matchmaking protocol for mobile social networks," *International Journal of Network Security*, vol. 17, no. 3, pp. 357–364, 2015.

[32] H. Shi and R. Guo, "Provably-secure certificateless key encapsulation mechanism for e-healthcare system," *International Journal of Network Security*, vol. 17, no. 5, pp. 548–557, 2015.

[33] K. Takashima, "Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption," in *International Conference on Security and Cryptography for Networks*, pp. 298–317, 2014.

[34] S. Tu, S. Niu, H. Li, Y. Xiao-ming, and M. Li, "Fine-grained access control and revocation for sharing data on clouds," in *26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW'12)*, pp. 2146–2155, 2012.

[35] B. Waters. "Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions,". in *Advances in Cryptology (CRYPTO'09)*, pp. 619–636. 2009.

[36] N. Xiao, R. Sharman, H. R. Rao, and S. Upadhyaya, "Factors influencing online health information search: An empirical analysis of a national cancer-related survey," *Decision Support Systems*, vol. 57, pp. 417–427, 2014.

[37] H. Xiong, J. Tao, and C. Yuan, "Enabling telecare medical information systems with strong authentication and anonymity," *IEEE Access*, 2017.

[38] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts," in *International Conference on Provable Security*, pp. 259–273, 2014.

[39] Y. Zhao, F. Yue, S. Wu, H. Xiong, and Z. Qin, "Analysis and improvement of patient self-controllable multi-level privacy-preserving cooperative authentication scheme," *International Journal of Network Security*, vol. 17, no. 6, pp. 779–786, 2015.

[40] J. Zhou, X. Lin, X. Dong, and Z. Cao, "Psmpa: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 6, pp. 1693–1703, 2015.

Biography

Yang Zhao is a Ph.D. Candidate at the School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests are in the area of network security and e-commerce protocol.

Pengcheng Fan received his B.S. degree from Hebei University of Science and Technology of China (HEBUST) in 2014. He is currently pursuing his M.S. degree in the School of Information and Software Engineering, UESTC. His research interests include cryptography and network security.

Haoting Cai received his B.S. degree from University of Electronic Science and Technology of China (UESTC) in 2014. He is currently pursuing his M.S. degree in the School of Information and Software Engineering, UESTC. His research interests include cryptography and network security.

Zhiguang Qin is the dean and professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC). He received his PH.D. degree from UESTC in 1996. His research interests include: information security and computer network.

Hu Xiong is an associate Professor at University of Electronic Science and Technology of China (UESTC). He received his Ph.D. degree from UESTC in 2009. His research interests include cryptographic protocols and network security.