Ciphertext-Policy Hierarchical Attribute-based Encryption for Fine-Grained Access Control of Encryption Data

Ximeng Liu[1], Jianfeng Ma[2], Jinbo Xiong[2], and Guangjun Liu[1,3]

(Corresponding author: Ximeng Liu)

School of Telecommunication Engineering, Xidian University[1]
No. 2 South Taibai Road, Xi'an, 710071, China
School of Computer Science and Technology, Xidian University[2]
No. 2 South Taibai Road, Xi'an, 710071, China
School of Mathematical and Computer Engineering, Xi'an University of Arts and Science[3]
No. 168 South Taibai Road, Xi'an, 710065, China
(Email: snbnix@gmail.com)

(Received Nov. 3, 2012; revised and accepted June 19, 2013)

Abstract

In the ciphertext-policy attribute based encryption (CP-ABE) scheme, a private key holder is related with a set of attributes while the data is encrypted under an access structure defined by the data provider. In most proposed schemes, the characteristics of the attributes are treated as same level. While in the real world circumstance, the attributes are always in the different levels. In this paper, In this paper, a scheme is proposed under a different hierarchy of attributes with the name of ciphertext-policy hierarchical attribute based encryption. The CP-HABE scheme is proved to be secure under the decisional q-parallel bilinear Diffie-Hellman exponent assumption, which can be considered as the generalization of the traditional CP-ABE.

Keywords: Access structure, attribute-based, bilinear pairings, encryption, hierarchy

1 Introduction

Encryption is the cryptographic primitive which provides confidentiality to the digital communication. The public key encryption provides a powerful mechanism for protecting the confidentiality of stored and transmitted information. When a data provider wants to share some information with a user, the provider must know exactly the one he/she wants to share with. In many applications, the data provider wants to share some information according to the policy based on the receiving of the users' credentials.

Attribute-based encryption (ABE) has prominent advantages over the traditional public key encryption which can be exemplified by the fact that the flexible one-to-many encryption will take the place of one-to-one encryption. The ABE scheme provides a powerful method to achieve both data security and fine-grained access control. In CP-ABE scheme, private keys are labeled with sets of descriptive attributes. Only when the set of descriptive attributes satisfies the access structure in the ciphertext can the user get the plaintext. When a data owner wants to provide a document to all the users who have a certain set of attributes, he/she could use ABE to encrypt the document, and the users could decrypt the document when they have satisfied a certain set of attributes. For example, the headmaster wants to encrypt a document to all the professors of 45 years old in the computer science department, the document would be encrypted with access structure {"professor" AND "CS department" AND "age 45"}, and only the users who hold the private key containing these three attributes can decrypt the document while others cannot get any information from the ciphertext. However, the professors can be classified into different types in reality, such as, full professor and distinguished professor. It is tricky for data provider to encrypt message by using the access structure to achieve both fine-grained access control while reflect importance of attributes. To solve this problem, we introduce hierarchical attributes to CP-ABE.

In this paper, the universal attributes in the scheme we proposed are classified into different levels according to their importance defined in the access control system. Every user in the system possesses a set of attributes in hierarchy. The data owner encrypts a data to users in the system who have a certain set of attributes. The ciphertext contains a kind of hierarchical access structure. In order to decrypt the message, users' attributes in hierarchy must satisfy the hierarchical access structure. The notion of CP-HABE can be considered as the generalization of traditional CP-ABE scheme where all attributes are in the same level.

1.1 Related Work

ABE is one of the important applications of fuzzy identity-based encryption [15] whose origin can be traced back to identity-based encryption [2, 3, 4, 18]. In the seminal paper, Sahai and Waters used biometric measurements as attributes in the following way: a user is equipped with the secret key for a set of attributes while the ciphertext is associated with another set of attributes. Only when the overlap between the two attribute sets exceeds the threshold could the user decrypt the ciphertext. There are two methods to access control based on ABE: key-policy attribute based encryption(KP-ABE) [8] and ciphertext-policy attribute based encryption(CP-ABE) [1, 6]. In KP-ABE, the ciphertext contains a set of attributes and the private key is related to the access structure. The construction of a KP-ABE scheme was first provided in [8]. In their scheme, when a user made a secret request, the trusted authority determined which combination of attributes must appear in the ciphertext for the user to decrypt. Instead of using the Shamir secret key technique [17] in the private key, this scheme used a more generalized form of secret sharing to enforce a monotonic access tree. Ostrovsky et al. [14] presented the first KP-ABE system which supported the non-monotone formulas in key policies. In CP-ABE, the idea is reversed: the ciphertext is associated with the access structure while the private key contains a set of attributes. The first CP-ABE scheme was proposed by Bethencourt et al. [1] which used threshold secret sharing scheme to enforce the policy during the encryption phase. However, the drawback of this construction was that security proof was only constructed under the generic group model. Due to this weakness, another construction was presented by Cheung and Newport [6]. The security of this scheme was proved under the standard model. Later in [7], Goyal et al. gave construction for some advanced access structures based on number theoretic. A new methodology for realizing CP-ABE schemes from a general set of access structures in the standard model was presented by Waters [21] under a concrete and non-interactive assumption. Linear secret sharing scheme(LSSS) matrix was used as access control over the attributes in this scheme. Predicate encryption scheme was proposed by Boneh and Waters [5] based on the primitive called hidden vector encryption and their scheme can realize the anonymous CP-ABE by using the opposite semantics of subset predicate. Wang et al. [20] combined the hierarchical identity-based encryption (HIBE) system and the CP-ABE system to provide fine-grained access control and full delegation. Later, Li et al. [12] proposed a scheme which enhanced ABE with hierarchical attributes. In this scheme, the universal attributes were classified into trees according to their relationship. This paper also gave a provably secure proof to this scheme. However, this scheme which uses threshold method can not provide fine-grained access control for encryption data. Recently, there are also several attempts to construct attribute-based signature [9, 10, 11, 13, 16]. Based on previous works, we construct ciphertext-policy hierarchical attribute-based encryption which can achieve both fine-grained access control for encryption data and hierarchical attributes.

1.2 Our Contributions

The contributions of this paper are listed as following: (1) We formalize the model of CP-HABE and give security model for CP-HABE. We also give specific construction about CP-HABE. (2) We prove our scheme is secure under the standard model by using decisional parallel bilinear Diffie-Hellman exponent assumption. (3) We make analysis of CP-HABE scheme. The analysis shows that our scheme can reach both fine-grained access control and hierarchical attributes.

1.3 Organization

In Section 2, we formalize model for CP-HABE and present the security model for CP-HABE. In Section 3, we review some concepts of the hierarchical access structure, birkhoff interpolation, hierarchical threshold secret sharing schemes, bilinear maps and decisional parallel bilinear Diffie-Hellman exponent assumption. In Section 4, we provide the specific construction about the CP-HABE scheme. In Section 5, we offer security proof under the security model for CP-HABE. In Section 6 we make analysis of CP-HABE scheme and Section 7 is the conclusion of this paper.

2 Ciphertext-policy Hierarchical Attribute based Encryption

In this section, we present the definition of CP-HABE scheme and its security model.

2.1 CP-HABE Scheme

A CP-HABE scheme consist of four fundamental algorithms: **Setup**, **Encrypt**, **KeyGen** and **Decrypt**.

Setup$(1^\lambda, \mathcal{U})$: The setup algorithm inputs a security parameter 1^λ and hierarchical attribute universe description $\mathcal{U}$. It outputs the public parameters *params* and master key MSK.

Encrypt$(params, m, \mathbb{A})$: The encryption algorithm inputs the public parameters *params*, hierarchical access structure $\mathbb{A}$ and the message m which the sender wants to encrypt. It outputs the ciphertext CT. We assume the ciphertext contains $\mathbb{A}$.

KeyGen(MSK, S): The key generation algorithm inputs the master key MSK and a set S of attributes in hierarchy. It outputs a private key SK.

Decrypt(CT, SK): The decryption algorithm inputs the ciphertext CT and the private key SK. When a set of attribute satisfies the hierarchical access structure, it can decrypt the ciphertext and return message m.

In the CP-ABE scheme, the ciphertext is related with the access structure while the private key is associated with the attribute set. In our security model, the adversary will choose challenge access structure $\mathbb{A}^*$ and ask for any private key SK containing the hierarchical attribute set S where S does not satisfy $\mathbb{A}^*$. We now give the formal security game for CP-HABE as below.

2.2 Security Model for CP-HABE

Init. The adversary declares the access structure $\mathbb{A}^*$ that he wishes to be challenged upon.

Setup. The challenger runs the *Setup* algorithm and outputs the public parameters *param*. Challenger gives *param* to the adversary.

Phase 1. The adversary makes repeated polynomially private key queries corresponding to the sets of hierarchical attributes $S_1, \cdots, S_{q_1}$ which none of these attribute sets satisfy the challenge hierarchical access structure $\mathbb{A}^*$.

Challenge. The adversary submits two equal length message m_0, m_1 and challenge access structure $\mathbb{A}^*$. The challenger flips a random coin β, and encrypts m_β under $\mathbb{A}^*$. The ciphertext CT* is given to the adversary.

Phase 2. Same as Phase 1.

Guess. The adversary output a guess β' of β.

Adversary $\mathcal{A}$ wins this game if $\beta' = \beta$. The advantage of $\mathcal{A}$ in this game is defined as $\mathrm{Adv}_{\mathcal{A}} = \Pr[\beta' = \beta] - \frac{1}{2}$.

If we allowing for decryption queries in Phase 1 and Phase 2, the model can easily be extended to prevent chosen-ciphertext attacks.

Definition 1. *An ciphertext-policy hierarchical attribute based encryption scheme is indistinguishable secure against selective chosen plaintext attack if no polynomial time adversaries win the above game with non-negligible advantage.*

3 Basic Constructions

In this section, we introduce the notions related to hierarchical access structure, hierarchical threshold secret sharing schemes, bilinear maps and decisional parallel bilinear Diffie-Hellman exponent assumption.

3.1 Hierarchical Access Structure

Definition 2 (Hierarchical access structure [19]). *Let $\mathcal{U}$ be a set of n participants and assume that $\mathcal{U}$ is consisted of levels $\mathcal{U} = \bigcup_{i=0}^{m} \mathcal{U}_i$, where $\mathcal{U}_i \cap \mathcal{U}_j = \emptyset$ for $0 \leq i \leq j \leq m$. Let $\mathbf{k} = \{k_i\}_{i=0}^{m}$ be a monotonically increasing sequence of integers $0 < k_0 < k_1 < \cdots < k_m$. Then the $(\mathbf{k}, n)$-hierarchical threshold access structure is*

$$\Gamma = \left\{ \mathcal{V} \subseteq \mathcal{U} : \left| \mathcal{V} \cap \left(\bigcup_{j=0}^{i} \mathcal{U}_j \right) \right| \geq k_i, \forall i \in \{0, 1, \cdots, m\} \right\}$$

3.2 Hierarchical Threshold Secret Sharing Schemes

In this subsection, we introduce the essential use of the hierarchical threshold secret sharing schemes. We adopt the idea proposed in [19].

Let $\mathcal{V} = \{v_1, \cdots, v_{|\mathcal{V}|}\} \subset \mathcal{U}$ where $\mathcal{V}$ is the hierarchical subset while $\mathcal{U}$ is hierarchical universe set. we assume that

$$\begin{gathered} v_1, \cdots, v_{l_0} \in \mathcal{U}_0, \\ v_{l_0+1}, \cdots, v_{l_1} \in \mathcal{U}_1, \\ \vdots \\ v_{l_{m-1}+1}, \cdots, v_{l_m} \in \mathcal{U}_m, \\ where \quad 0 \leq l_0 \leq l_1 \leq \cdots \leq l_m = |\mathcal{V}| \end{gathered}$$

$\mathcal{V}$ is authorized subset if and only if $l_i \geq k_i$ for all $0 \leq i \leq m$, where m denote as the number of total levels in this scheme and l_i is the number of element in subset $\mathcal{V}$ under level i. Let $\mathbf{r} : \mathbb{F} \to \mathbb{F}^k$ be defined as $\mathbf{r}(x) = (1, x, x^2, \cdots, x^{k-1})$ and $\mathbf{r}^{(i)}(x)$ denote the i-th derivative of $\mathbf{r}(x)$ for $i \geq 0$. The share which distributed to participants $u \in \mathcal{U}_i$ is $\sigma(u) = \mathbf{r}^{(k_{i-1})}(x) \cdot \mathbf{a}$, where $\mathbf{a} = (a_0 = s, a_1, \cdots, a_{k-1})$ is the vector of coefficient of $p(x)$. When all participants of $\mathcal{V}$ put their shares together, the system can calculate the unknown vector $\mathbf{a}$ is $M\mathbf{a} = \sigma$, where the coefficient matrix is:

$$\begin{gathered} M = (\mathbf{r}(v_1), \cdots, \mathbf{r}(v_{l_0}); \mathbf{r}^{(k_0)}(v_{l_0+1}), \cdots, \mathbf{r}^{(k_0)}(v_{l_1}); \cdots; \\ \mathbf{r}^{(k_{m-1})}(v_{l_{m-1}+1}), \cdots, \mathbf{r}^{(k_{m-1})}(v_{l_m})) \end{gathered}$$

while $\sigma = (\sigma(v_1), \sigma(v_2), \cdots, \sigma(v_{l_m}))^T$.

For all $j = 1, \cdots, l_0, \cdots, l_m$, the j'-*th* row of M we let the function ρ defined the party labeling row j as $\rho(j)$. Suppose $j = l_{i-1} + c$, then the share $\mathbf{r}^{(k_{i-1})}(v_{l_{i-1}+c})$ belong to party $\rho(j)$.

Suppose that $\prod$ is hierarchical threshold secret sharing scheme for the hierarchical threshold access structure $\mathbb{A}$. The set $S \in \mathbb{A}$ is defined as any authorized set, and let $I \subseteq \{1, \cdots, l_0, \cdots, l_m\}$ be defined as $I = \{j : \rho(j) \in S\}$. If $\{\lambda_j\}_{j \in I}$ are valid shares of secret s according to $\prod$ and authorized set S satisfy Pólya's Condition (the Pólya's Condition can be found in [19]), then exist constants $\{\omega_j \in \mathbb{Z}_p\}$ such that $\sum_{j \in I} \omega_j \lambda_j = s$. We said that the vector $(1, 0, \cdots, 0)$ is the target vector for secret sharing scheme. For any authorized set of rows I in M ,we will have that target vector is in the span of I. Otherwise, the target vector is not in the span of the rows of the set I. Moreover, there will exist a vector ω such that $\omega \cdot (1, 0, \cdots, 0) = -1$ and $\omega \cdot M_i = 0$ for all $i \in I$.

3.3 Bilinear Maps

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups of prime order p with the multiplication. Let g be a generator of $\mathbb{G}$ and e be a bilinear map. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a bilinear map has the following properties:

1) Bilinearity: for all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$.

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

3) Computability: There is efficient algorithm to compute bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$.

Notice that the map e is symmetric since $e(u^a, v^b) = e(u, v)^{ab} = e(u^b, v^a)$.

3.4 Decisional Parallel Bilinear Diffie-Hellman Exponent Assumption

We use the assumption proposed in [8] called decisional q-parallel bilinear Diffie-Hellman exponent assumption. The q-parallel bilinear Diffie-Hellman problem define as follows. Choose a group $\mathbb{G}$ of prime order p according to the security parameter. Let g be a generator of $\mathbb{G}$ and $a, s, b_1, \cdots, b_q \in \mathbb{Z}_p$ be chosen randomly. If an adversary is given $\mathbf{y} =$

$$g, g^s, g^a, \cdots, g^{(a^q)}, g^{(a^{q+2})}, \cdots, g^{(a^{2q})},$$

$$\forall_{1 \le j \le q} \quad g^{s \cdot b_j}, g^{a/b_j}, \cdots, g^{(a^q/b_j)}, g^{(a^{q+2}/b_j)}, \cdots, g^{(a^{2q}/b_j)}$$

$$\vdots$$

$$\forall_{1 \le j,k \le q; k \neq j} \quad g^{a \cdot s \cdot b_k / b_j}, \cdots, g^{a^q \cdot s \cdot b_k / b_j}$$

It remain hard to distinguish $e(g, g)^{a^{q+1}s} \in \mathbb{G}_T$ from a random element in $\mathbb{G}_T$.

We define the advantage of an adversary $\mathcal{A}$ in solving the decisional q-parallel bilinear Diffie-Hellman exponent problem as

$$\begin{aligned} \mathrm{Adv}_{\mathcal{A}} = \Pr\left[\mathcal{B}\left(\mathbf{y}, T = e(g, g)^{a^{q+1}s} = 0\right)\right] \\ - \Pr\left[\mathcal{B}\left(\mathbf{y}, T = R\right) = 0\right] \end{aligned}$$

Definition 3. *We say that the decision q-parallel DBHE assumption holds if no polytime algorithm has a non-negligible advantage in solving the decisional q-parallel DBHE problem.*

4 Our Construction

In this construction, the attributes are assumed to be divided into $m + 1$ levels. Different attributes belong to different levels according to their importance in the system and these attributes do not have any relationship for access control. We show how the attributes are categorized and constructed in Figure 1. As shown in the figure, each circle represents an attribute belong to one level. $h_{\rho(1)}, \cdots, h_{\rho(l_0)}$ belong to level 0 while $h_{\rho(l_{i-1}+1)} \cdots h_{\rho(l_i)}$ belong to level i. Every user holds a private key which is associated with a set of attributes in hierarchy. When these attributes match the hierarchical access structure in the ciphertext, the user can get message from sender. It is easy to verify that this construction is indeed a generalization of CP-ABE.

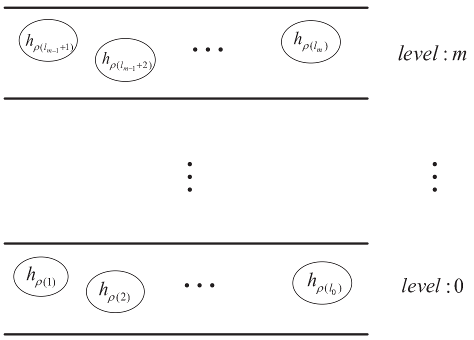

Figure 1: Hierarchical attribute structure

The concrete construction is as follows:
Setup($\mathcal{U}$): The setup algorithm inputs the set of universe attributes $\mathcal{U}$ in the system. The attributes are in the different hierarchy. The algorithm then chooses a group $\mathbb{G}$ of prime order p, a generator g and group element $h_1, \cdots, h_{|\mathcal{U}|} \in \mathbb{G}$ that associated with $|\mathcal{U}|$ the attributes in the system. In addition, it chooses random exponents $\alpha, a \in \mathbb{Z}_p$. The public parameters is published as:

$$params = \{g, e(g, g)^\alpha, g^a, h_1, \cdots, h_{|\mathcal{U}|}\}$$

The authority set MSK $=g^\alpha$ as the master secret key.

Encrypt($params, (M_{\mathcal{V}}, \rho), m'$): The encryption algorithm inputs the public parameters $params$ and a message m' to encrypt. In addition, it inputs a HTSSS access structure $(M_{\mathcal{V}}, \rho)$. The function ρ associates rows of $M_{\mathcal{V}}$ to attributes.

The algorithm first chooses a random vector $\mathbf{a} = (a_0 = s, a_1, \cdots, a_{k-1}) \in \mathbb{Z}_p^k$. These values will be used to share the encryption exponent s. For all $j = 1, \cdots, l_0, \cdots, l_m$, it calculates $\lambda_j = M_j \cdot \mathbf{a}$, where M_j is corresponding to the $j'th$ row of $M_{\mathcal{V}}$. In addition, the algorithm chooses random $r_{l_0}, \cdots, r_{l_m} \in \mathbb{Z}_p$. The ciphertext is published as:

$$\begin{aligned} \mathrm{CT} = \{C = me(g, g)^{\alpha s}, (M_{\mathcal{V}}, \rho), C' = g^s, C_1{=}g^{a\lambda_1} h_{\rho(1)}^{-r_{l_0}}, \cdots, \\ (C_j{=}g^{a\lambda_j} h_{\rho(j)}^{-\sum_{i=l_0,\cdots,l_k} r_i}, \cdots, C_{l_m}{=}g^{a\lambda_{l_m}} h_{\rho(l_m)}^{-\sum_{i=l_0,\cdots,l_m} r_i}, \\ D_{l_0}{=}g^{r_{l_0}}, \cdots, D_{l_m}{=}g^{r_{l_m}}\} \end{aligned}$$

where $k_{i-1} \le j \le k_i$

Keygen(MSK,S): The key generation algorithm inputs the master secret key MSK and a set S which has different hierarchical attributes. The algorithm first chooses a random $t \in \mathbb{Z}_p$. It creates the private key as

$$SK = \{K = g^{\alpha} g^{at}, L = g^t, \forall x \in S : K_x = h_x^t\}.$$

Decrypt(CT, SK): The decryption algorithm inputs a ciphertext CT for access structure $M_{\mathcal{V}}$ and private key for set S. Suppose that S satisfy the hierarchical access structure which the number of attributes in level $\mathcal{U}_i$ must exceed its threshold k_i. Let $I \subseteq \{1, \cdots, l_0, \cdots, l_m\}$ be defined as $I = \{j : \rho(j) \in S\}$. If $\{\lambda_j\}_{j\in I}$ are valid share according to M and set S satisfy Pólya's Condition, then $\sum_{j\in I} \omega_j \lambda_j = s$ where $\{\omega_j \in \mathbb{Z}_p\}$ be a set of constants. The decryption algorithm first computes

$$\begin{aligned} CW &= e(C', K)/\prod_{j\in I} (e(C_j, L) \cdot e(D_{l_0} D_{l_1} \cdots D_{l_{k_i}}, K_{\rho(j)}))^{\omega_j}) \\ &= e(g,g)^{\alpha s} e(g,g)^{ast}/(\prod_{j\in I} e(g,g)^{ta\lambda_j\omega_j}), \quad (k_{i-1} \leq j \leq k_i) \\ &= e(g,g)^{\alpha s}. \end{aligned}$$

Then algorithm divides out CW from C and obtain the message m.

5 Proof

Theorem 1. *Suppose the q-parallel DBHE assumption holds. Then no polytime adversary can selectively break our system with a challenge matrix of size $l^* \times n^*$, where $n^* \leq q$.*

Proof. Suppose we have an adversary $\mathcal{A}$ with non-negligible advantage $\epsilon = \mathrm{Adv}_{\mathcal{A}}$ and it choose a challenge matrix M^* of dimension at most q columns in the selective security game against our construction. We show how to build a simulator $\mathcal{B}$ to play the q-parallel DBHE problem.

Init: The simulator takes in the q-parallel DBHE challenge $\mathbf{y}$, T. The adversary gives the challenge access structure (M^*, ρ) to the algorithm, where M^* has $n^* \leq q$ columns.

Setup: The simulator chooses random $\alpha' \in \mathbb{Z}_p$ and sets $\alpha = \alpha' + a^{q+1}$. Then we have $e(g,g)^{\alpha} = e(g^a, g^{a^q}) \cdot e(g,g)^{\alpha'}$.

Here we make analysis of how the simulator programs the parameter $h_1, \cdots, h_{|\mathcal{U}|}$. For each $x = 1$ to $|\mathcal{U}|$, choose a random value $z_x \in \mathbb{Z}_p$. If there exist an j such that $\rho^*(j) = x$, then let $h_x = g^{z_x} g^{aM^*_{j,1}/b_j} g^{a^2 M^*_{j,2}/b_j} \cdots g^{a^{n*} M^*_{j,n*}/b_j}$. Otherwise, let $h_x = g^{z_x}$.

Phase 1: In this phase, the adversary $\mathcal{A}$ makes a private key query for a set S, where S does not satisfy M^*. Then the simulator answers private key queries.

The simulator first chooses a random $r \in \mathbb{Z}_p$. Because S does not satisfy M^*, simulator can finds a vector $\omega = (\omega_1, \omega_2, \cdots, \omega_{n^*}) \in \mathbb{Z}_p^{n^*}$ such that $\omega_1 = -1$. For all i satisfied $\rho^*(i) \in S$, we have that $\omega \cdot M^*_j = 0$.

The simulator defining t as:

$$t = r + \omega_1 a^q + \omega_2 a^{q-1} + \cdots + \omega_{n*} a^{q-n*+1}.$$

Then we have:

$$L = g^t = g^r \prod\nolimits_{i=1\cdots n*} \left(g^{a^{q+1-i}}\right)^{\omega_i}.$$

Here we calculate K_x where $\forall x \in S$. We first consider $x \in S$ where no j such that $\rho^*(j) = x$. In this circumstance, we simply let $K_x = L^{z_x}$.

Next we deal with the task to create keys for attribute x where x is used in the access structure. Because simulator can not simulate the terms of the form $g^{a^{q+1}}$, we must make sure private key do not have this terms. Notice that in calculating h_x^t all terms of this form in the exponent come from $M^*_{j,k} a^k \cdot \omega_k a^{q+1-j}/b_j$ for some k, where $\rho^*(j) = x$. However, we have that $M^*_j \cdot \omega = 0$ Therefore, all exponent of a^{q+1} can cancel when combined.

The simulator creates K_x as follows

$$\begin{aligned} K_x = h_x^t &= (g^{z_x} g^{aM^*_{j,1}/b_j} g^{a^2 M^*_{j,2}/b_j} \cdots g^{a^{n*} M^*_{j,n*}/b_j})^t \\ &= L^{z_x} \cdot \prod_{k=1,\cdots,n^*} (g^{a^k \cdot M^*_{j,k} \cdot t/b_j}) \\ &= L^{z_x} \cdot \prod_{k=1,\cdots,n^*} (g^{a^k \cdot r} \prod_{\substack{w=1,\cdots,n^* \\ k\neq j}} (g^{a^{q+1+k-w/b_j}})^{\omega_w})^{M^*_{j,k}} \end{aligned}$$

Challenge In this stage we build the challenge ciphertext. The adversary gives two message m_0 and m_1 to the simulator. The simulator flips a coin β, creates $C = m_\beta e(g,g)^{\alpha s} = m_\beta T \cdot e(g,g)^{\alpha' s}$ and $C' = g^s$.

The more difficult task is to simulate the C_i values since it contain g^{sa^i} that we can not simulate. However, the simulator can use the secret splitting such that these items cancel out. The simulator first choose random $y'_2, \cdots, y'_{n^*} \in \mathbb{Z}_p$, then share the secret using the vector $\mathbf{v} = (s, sa + y'_2, \cdots, sa^{n^*} + y'_{n^*}) \in \mathbb{Z}_p^{n^*}$. In addition, it chooses random values $r'_1, \cdots, r'_{l_m}$.

For $i = 1, \cdots, n^*$, the challenge ciphertext components are then generated as

$$D_1 = g^{{r'}_{l_0}} g^{sb_1}, \cdots, D_i = g^{{r'}_{l_{k_i}}} g^{sb_j}$$

where $\quad k_{i-1} \leq j \leq k_i$.

$$\begin{aligned} C_j &= g^{a\lambda_j} h_{\rho^*(j)}^{-\sum_i r_i} \\ &= g^{asM^*_{j,1}} g^{(sa^2 + {y'}_2 a)M^*_{j,2}} \cdots g^{(sa^{n*} + {y'}_{n*} a)M^*_{j,n*}} \\ &\cdot h_{\rho^*(j)}^{-\sum_{i=l_0,\cdots,l_k} r_i^*} (g^{b_j s})^{-z_{\rho^*(j)}} \\ &\cdot \prod_{\substack{{r'}_{l_{k_0}},\cdots,{r'}_{l_{k_i}} \\ i\neq j}} \prod_{w=1,\cdots,n*} (g^{-a^w s\cdot(b_i/b_j)})^{M^*_{j,w}} \\ &\cdot \prod_{w=1,\cdots,n*} (g^{-a^w s})^{M^*_{j,w}}. \end{aligned}$$

Table 1: Scheme comparison

System	**CT. Size**	**SK. Size**	**Assumption**	**Fine-grained AC**	**H. Attribute**
LSSS [21]	$\mathcal{O}(n)$	$\mathcal{O}(A)$	q-Parallel BDHE	YES	NO
Li's [12]	$\mathcal{O}(n)$	$\mathcal{O}(A^{k_{max}})$	l-wBDHI*	NO	YES
Ours	$\mathcal{O}(n^{m_{max}})$	$\mathcal{O}(A)$	q-Parallel BDHE	YES	YES

Phase 2: Same as Phase 1.

Guess: The adversary will eventually output a guess β' of β. The simulator outputs 0 to guess that $T = e(g,g)^{a^{q+1}s}$ if $\beta' = \beta$. Otherwise, it and outputs 1 to indicate that it believes T is a random group element in $\mathbb{G}_T$.

When T is a tuple the simulator $\mathcal{B}$ gives a perfect simulation so we have that

$$\Pr\left[\mathcal{B}(\vec{y}, T = e(g,g)^{a^{q+1}s}) = 0\right] = \frac{1}{2} + \mathrm{Adv}_{\mathcal{A}}$$

When T is a random group element, the message m_β is hidden from the adversary and we have $\Pr[\mathcal{B}(\vec{y}, T = R) = 0] = \frac{1}{2}$. Therefore, can play the decisional q-parallel DBHE game with non-negligible advantage. □

6 Analysis of the Proposed Scheme

Li et al. [12]. proposed a scheme enhancing ABE with attribute hierarchy. The universal attributes in this scheme were classified into trees according to their relationship. It is assumed that the private key is associated with the attribute set Ω and the ciphertext is associated with another attribute set Ω'. In order to encrypt the ciphertext, the number of attribute in Ω must cover the attribute in Ω' exceed threshold d. In our proposed scheme, the access control policy achieves fine-grained of encrypted data. We assume the ciphertext is related with the hierarchical access structure while the private key is associated with attribute. Each level of hierarchical access structure has threshold k_i. Only if all levels satisfy $l_i \geq k_i$ can we get the message in ciphertext. For example, the school encrypts a document with hierarchical access structure {level 3:{"professor", "department chairman"}, level 1:{"20 years working experience", "age 45"}, level 0:{"female", "height 180cm", "black hair"}}, the threshold of each level is { $d_3 = 1$, $d_2 = 1$, $d_1 = 2$ }. We assume John has the attribute set {"professor", "age 45", "height 180cm", "black hair"}and Ann has the attribute set {"age 45","female", "height 180cm", "black hair"}. In our scheme, John can decrypt the message while Ann cannot. If the threshold is 4 in Li's scheme, both John and Ann can decrypt the document.

Here we compare our scheme with schemes [12, 21]. We let n be the size of an access formula, m_{max} denotes the maximum number of attribute in each level. A is the number of attributes in a user's key and k_{max} denotes the maximum depth of hierarchcal attribute. The comparison is listed in the Table 1.

7 Conclusion

In this paper, we propose a scheme called ciphertext-policy hierarchical attribute based encryption in which the attributes in the system are not always in the same level. We present specific construction of CP-HABE which uses the hierarchical access structure that can be considered as a generalization of traditional ABE. Only when a set of attributes possessed by the user satisfies the hierarchical access structure can he/she decrypt the ciphertext. We also give a security model for CP-HABE. Finally, we prove our scheme under the security model by reducing it to decisional q-parallel bilinear Diffie-Hellman exponent assumption. More importantly, this construction can exhibit significant improvement over the traditional ABE schemes accordant with the practical situation.

This work motivates a few interesting problems in this topic: 1) How can we construct more efficient schemes with attributes in hierarchy. 2) In this paper, the size of the ciphertexts is not constant, how to improve CP-HABE scheme with a ciphertext of a constant size. 3) How can we revocation attributes in different levels more efficiently. Therefore, Our future work will be design a CP-HABE scheme to solve these problems.

Acknowledgments

This research is supported by Changjiang Scholars and Innovative Research Team in University under grant No. IRT1078; The Key Program of NSFC- Guangdong Union Foundation under grant No. U1135002; Major national S&T program under grant No. 2011ZX03005-002; the Fundamental Research Funds for the Central Universities under grant No. JY10000903001. We thank the sponsors for their support and the reviewers for helpful comments.

References

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption,"

in *IEEE Symposium on Security and Privacy*, pp. 321–334. IEEE, 2007.

[2] D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in *Advances in Cryptology-Eurocrypt '04*, pp. 223–238. Springer-Verlag, 2004.

[3] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in *Advances in Cryptology–Crypto '04*, pp. 197–206. Springer-Verlag, 2004.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology–Crypto '01*, pp. 213–229. Springer-Verlag, 2001.

[5] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," *Theory of Cryptography*, pp. 535–554, 2007.

[6] 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. ACM, 2007.

[7] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," *Automata, Languages and Programming*, pp. 579–591, 2008.

[8] 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. ACM, 2006.

[9] D. Khader, "Attribute based group signatures," *IACR Cryptology ePrint Archive*, vol. 2007, p. 159, 2007.

[10] J. Li, M.H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pp. 60–69. ACM, 2010.

[11] J. Li and K. Kim, "Attribute-based ring signatures," *IACR Cryptology ePrint Archive*, vol. 2008, p. 394, 2008.

[12] J. Li, Q. Wang, C. Wang, and K. Ren, "Enhancing attribute-based encryption with attribute hierarchy," *Mobile Networks and Applications*, vol. 16, no. 5, pp. 553–561, 2011.

[13] H. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," *Topics in Cryptology–CT-RSA '11*, pp. 376–392, 2011.

[14] 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. ACM, 2007.

[15] A. Sahai and B. Waters, "Fuzzy identity-based encryption," *Advances in Cryptology–Eurocrypt '05*, pp. 557–557, 2005.

[16] S. Shahandashti and R. Safavi-Naini, "Threshold attribute-based signatures and their application to anonymous credential systems," *Progress in Cryptology–Africacrypt '09*, pp. 198–216, 2009.

[17] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[18] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, pp. 47–53. Springer-Verlag, 1985.

[19] T. Tassa, "Hierarchical threshold secret sharing," *Theory of cryptography*, pp. 473–490, 2004.

[20] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, pp. 735–737. ACM, 2010.

[21] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," *Public Key Cryptography–PKC '11*, pp. 53–70, 2011.

Ximeng Liu is a Ph.D. student in School of Telecommunication Engineering at Xidian University. His research interests include public key cryptography and information security.

Jianfeng Ma received the Ph.D degrees in computer software and communications engineering from Xidian University, China, in 1995. Now he is a Professor, Ph.D supervisor, IEEE member and a senior member of Chinese Institute of Electronics (CIE). His current research interests are in distributed systems, wireless and mobile computing systems, computer networks, and network security. He has published over 150 refereed articles in these areas and coauthored ten books.

Jinbo Xiong received the M.S degree from Chongqing University of Posts and Telecommunications, China, in 2006. Currently, he is a lecturer in Fujian Normal University, a Ph.D candidate in Xidian University. His current research interests mainly focus on access control and structured document security.

Guangjun Liu is a lecturer at the School of Mathematical and Computer Engineering, Xi'an University of Arts and Science. He received his M.S degree in Applied Mathematics and Ph.D. degree in Cryptography from Xidian University in 2009 and 2013 respectively. His research interests include Cryptography and Information Security, Information Theory and Coding.