Multimedia Social Network Authorization Scheme of Comparison-based Encryption

Cheng Li, Zhiyong Zhang, Guoqin Chang
(Corresponding author: Zhiyong Zhang)

School of Information Engineering, Henan University of Science and Technology,
Luoyang, Henan 471023, China
(Email: xidianzzy@126.com)

(Received Nov. 9, 2017; revised and accepted Mar. 5, 2018)

Abstract

In many Ciphertext-Policy Attributed Based Encryption (CP-ABE) schemes, the level of attributes is ignored; while the comparison based attribute encryption scheme is not flexible enough. In this paper, an encryption scheme based on comparative attributes is proposed. In this scheme, users can't only make more granular and flexible access control policies based on the level of attributes, but also support more diverse forms of access control policy. At the same time, in order to solve the computational pressure of the user terminal, a third-party proxy is added to the solution to assist the user to decrypt the ciphertext. Through the comparative and experimental data analysis, the scheme can be better applied to multimedia social networks.

Keywords: Comparison-Based Attribute; CP-ABE; Multimedia Social Networks; Third-Party Decrypt

1 Introduction

With the development of multimedia social networks, more and more people are willing to publish their personal life and privacy to the multimedia social network. But the security problems caused by privacy leaking and data authorization of social network users (hereinafter referred to as "users") are followed. The user uploads his or her private data to a social network service provider, such as the health condition of the user, travel information, and payment (consumption) information, via a social network provider or a third party storage agent to save the user data. However, the social network provider and third-party storage (or "Cloud") are often untrustworthy, and they are likely to spy on the user's private data or to leak privacy data due to problems such as failures and malicious user attacks, which leads to unnecessary problems to the user.

In order to protect the user's privacy, the user can encrypt the encrypted data and then upload the ciphertext to the cloud; then the user uses a flexible authorization method to share the encryption key, while users can also specify a fine-grained access control strategy to achieve efficient and secure data authorization. Sahai and Waters first proposed attribute based encryption (ABE) scheme in the [1], which can achieve fine-grained one to many authorization. ABE encrypted data can not only ensure the security and integrity of user data, but also have good flexibility. In 2006, Goyal proposed a Key-Policy Attributed Based Encryption (KP-ABE) and Ciphertext-Policy Attributed Based Encryption (CP-ABE) in the [2], and implemented the first KP-ABE algorithm. In 2007, Bethencourt [3] and Cheung [4] implemented the CP-ABE algorithm, respectively. After that, with the continuous development of ABE technology, has been widely used in multimedia social networks [5–7], cloud computing [8,9], cloud storage [10,11] and electronic health management [12,13] and many other areas. At the same time, users can use the "Boolean expression" [14], "and/or" access structure [6], (t, n) threshold [15,16] and linear secret sharing scheme (LSSS) [17], constructing a relatively flexible access control policy to meet the user's needs.

However, the current attribute-based encryption authorization scheme is often used to use specific attributes, such as the access strategy "President AND July 1", which states that "only the president has access rights in July 1st", in other words, Other people in this time or "President" in addition to this time cannot access the data, although this is a relatively extreme example, but it does show that most proposal is not flexible, because "President" can be divided into "president" and "vice-president", and even more detailed division, the date is the same reason, for these can be refined attribute authorization program research is relatively less.

Therefore, the attributes can be divided into sub-attributes according to a certain order, making data authorization more in line with the actual needs. The order relationship between these sub-attributes can be compared. Only when the user attribute level satisfies the access authorization policy can the data be decrypted.

1.1 Related Work

After Sahai and Waters proposed ABE algorithm, ABE is widely used in cloud storage, multimedia social networks, health management and so on. It can be divided into CP-ABE and KP-ABE program. The KP-ABE ciphertext is associated with the attribute set, and the user's key is associated with the access structure. The ciphertext in CP-ABE scheme is associated with the access control policy, and the user is associated with the attribute set. As the CP-ABE scheme is more close to the actual life, it has been widely used in the fields of multimedia, social networking and other related fields. However, most researchers do not pay enough attention to the weight of attributes, so that the scheme can't adapt well to the scene of practical application. In [18], an algorithm for transforming the threshold access strategy to LSSS is proposed. The scheme is improved on the basis of [19], which makes it more efficient and reduces storage space and computation cost effectively.

In [20], an encryption scheme based on attribute comparison is proposed, which introduces attribute comparison into attribute-based encryption, realizes the constraint on the scope of authorization attribute, and increases the flexibility of data authorization effectively. In [21], Liu proposed a hierarchical fine-grained attribute authorization scheme, which implements a scheme based on attribute weights. However, this scheme only reached the single contrast capability, which cannot be set to the interval attribute weights. (For example, it can only set "attribute weight" or "attribute weight ¡value" (later called "monotonically contrast"), unable to set "a value ¡= attribute weight ¡= a value" (after the text referred to as "interval contrast ") situation).

In [22], it uses attribute weights and uses binary way to compare, increasing the flexibility of the program. In [23], a flexible attribute weights comparison authorization scheme is proposed, which not only supports monotonically contrast, but also supports attribute interval (range) contrast, which makes attribute-based authorization scheme more suitable for practical application scenarios. In [24], the attributes are compared using 0-encoding and 1-encoding encoding. In [25], the first ABE system with adaptive safety is proposed using dual system encryption. In [26], a CP-ABE scheme with multiple central authority is proposed, which effectively improves the computational efficiency of a single CA, and solves the security problem caused by a single CA mastering the global master key. In [27], a hierarchical attribute encryption authorization system is also proposed, but the system idea is to divide the user with different levels of authorization, but the thought is different from the [21], its main idea is to reduce the complexity of the task from high to low so as to reduce the computing pressure of a single institution.

1.2 Contribution

After this article carries on the analysis combined with the development of multimedia social networks and user needs, it found that users in the use of multimedia social networks not only needs efficient sharing authorization mechanism, but also needs the protection of private data security. But the current scheme lacks some flexibility. Therefore, this paper proposes a multimedia social network authorization scheme based on comparative attributes, which has three contributions to the future research work:

1) The proposed scheme supports monotonic access structure and has some flexibility;

2) In considering the order of attributes can not only be a simple comparison, it can also set the attribute authorization order interval;

3) The ABE scheme is improved in this paper: the introduction of third party auxiliary user decryption reduces the user operation pressure. At the same time, with half hidden access Control strategy, it become more suitable for multimedia social networks.

The schematic diagram of the scheme is shown in Figure 1.

1.3 Organization

The first section of this paper mainly introduces the discovery, causes and research status of the problem. In the second section, the background knowledge related to the scheme proposed in this paper will be introduced, so that readers can better understand it. In section three, a formal description of the solution model and its security model is presented. Section 4 introduces the specific process of the algorithm in this scheme. The fifth section will prove the security of the proposed scheme and make a simple comparison with other schemes proposed in the literature. The work of this paper will be reviewed and summarized in the last section, and a simple prospect for future research or development direction will be carried out.

2 Background

2.1 Bilinear Maps

Assume that G and G_T are two multiplication cyclic groups, of which the order is prime number P, g, a generator of Group G, and then a bilinear map; $e : G \times G \rightarrow G_T$ exists with the following properties [28]:

- Bilinearity: For any $u, v \in G$; $a, b \in Z_p$, $e(u^a, v^b) = e(u, v)^{ab}$;
- Non-degeneracy: For calculation, $e(g, g) \neq 1$;
- Symmetry: $e()$ is a symmetry operation, *i.e.*, $e(g^a, g^b) = e(g^b, g^a)$.

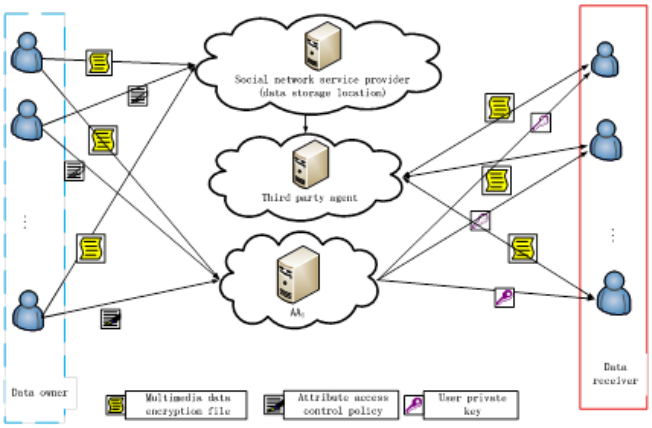

Figure 1: Scheme diagram of the program model

2.2 q-parallel Bilinear Diffie-Hellman Exponent

Definition 1 (q-parallel Bilinear Diffie-Hellman Exponent (q-parallel BDHE)). *Suppose G, G_T are the multiplication cycle of prime order p, the generator of G is g, there are bilinear mapping $e: G \times G \to G_T$, random selection $a, s, b_1, b_2, \cdots, b_q \in Z_p$. If an adversary is given $y = \{g, g^s, g^a, \cdots, g^{a^q}, g^{a^{q+2}}, \cdots, g^{2^{2q}}, (g^{sb_j}, g^{a/b_j}, \cdots, g^{a^q/b_j}, g^{a^{q+2}/b_j}, \cdots, g^{a^{2q/b_j}}, \forall_{1\le j\le q}), (g^{asb_k/b_j}, \cdots, g^{a^q sb_k/b_j}, \forall_{1\le j,k\le q;k\neq j})$. It is not possible for an adversary to distinguish $e(g,g)^{a^{q+1}s} \in G_T$ from other elements randomly selected from G_T in probabilistic polynomial time.*

2.3 Structure of Access Structure and Attribute Weights

2.3.1 Definition and Construction of Comparison-Based Attributes

Based on the previous question, we construct a user attribute level (range) derivation algorithm: In this algorithm, the user can specify the attribute $U_i \in U(i = 1, \cdots, m)$, allocate attribute range for U_i to $0 < u_{i,1}, \cdots, < u_{i,j} < Z$, where m is the number of global attributes and Z is the maximum value assigned by attribute U_i. The attribute $U_i = \{u_{i,j}, u_{i,t}\}_{U_i \in U}$ indicates that the specified range of the attribute in the access policy is $u_{i,j} \le U_{i,user} \le u_{i,t}$, where $U_{i,user}$ only represents the attribute value of the user (which may be a fixed value or range, for example, "18 o'clock" only means that the attribute sequence a fixed value). There are mapping of $U_i \to \Psi$: when $U_i = \{u_{i,j}, u_{i,t}\}_{U_i \in U}$ is established, $\Psi(\{u_{i,j}, u_{i,t}\}_{U_i \in U})$ is established. Assuming that the relationship is $u_{i,user} = (u_{i,user,j'}, u_{i,user,t'}) \subseteq$ and $u_{i,j} \le u_{i,user,j'}, u_{i,user,t'} \le u_{i,user,t}$, there are $\Psi(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) \le \Psi(\{u_{i,user,j'}, u_{i,j}\}_{U_i \in U})$ and $\Psi(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) \le \Psi(\{u_{i,j}, u_{i,user,t'}\}_{U_i \in U})$ order relationships.

Definition 2. *Compare Attribute Level Operation Methods:*

1) *Strategy generation algorithm (Ψ): Randomly select a parameter $\varphi \in Z_p$, at the same time for the property U_i select two random parameters $theta_i, \mu_i \in Z_p$; Ψ that attribute U all attributes mapped to an integer, $\Psi(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) = \varphi^{\theta_i^{u_{i,j}} \mu_i^{Z-u_{i,k}}}$.*

2) *Strategy recovery (verification) algorithm (γ): The algorithm is designed to verify the relationship between user weight and access strategy. There are only two structures:*

- *If $u_{i,j} \le u_{i,user,j'}$ and $u_{i,user,t'} \le (u_{i,user,t}$, $U_{i,user} = (u_{i,user,j'}, u_{i,user,t'} \subseteq U_i$, γ can calculate the result $\gamma_{(u_{i,j} \le u_{i,user,j'}, u_{i,user,t'} \le u_{i,user,t} | U_i \in U)}(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) \in Z_p$ in polynomial time;*
- *If $u_{i,j} > u_{i,user,j'}$ or $u_{i,user,t'} > u_{i,user,t}$, $U_{i,user} = (u_{i,user,j'}, u_{i,user,t'} \subseteq U_i$ then γ cannot be obtained in the polynomial time $\{u_{i,j}, u_{i,t}\}_{U_i \in U}$ corresponding to the results.*

The calculation process of is as follows:

$$\begin{aligned} & \gamma_{(u_{i,j} \le u_{i,user,j'}, u_{i,user,t'} \le u_{i,user,t} | U_i \in U)}(\{u_{i,j}, u_{i,t}\}_{U_i \in U}) \\ = \; & (\varphi^{\theta_i^{u_{i,j}} \mu_i^{Z-u_{i,k}}})(\varphi^{\theta_i^{u_{i,user,j'} - u_{i,j}} \mu_i^{u_{i,k} - u_{i,user,t'}}}) \\ = \; & \varphi^{\theta_i^{u_{i,user,j'}} \mu_i^{Z-u_{i,k}}} \end{aligned}$$

2.3.2 Linear Secret Sharing Scheme (LSSS)

Set $P = \{P_1, P_2, \cdots, P_n\}$ as a set of participants, if P meets the following conditions of Π of linear secret sharing scheme:

1) The share of the participant on the secret s constitutes a vector on Z_p;

2) There is a m rows n columns for the secret sharing generation matrix M. Existing Map f maps all participants $i = 1, 2, \cdots, m$ to U, $f(i)$ maps each row of matrix M to a participant. Choose a vector $v = (s, v_2, v_3, \cdots, v_n)$, $s \in Z_p$ for the required shared secret, $v_2, v_3, \cdots, v_n \in Z_p$ randomly selected. Then Mv is s about Π's n shares, and the ith share λ_i belongs to the participant $f(i)$.

By using the access structure transformation method in [18], a monotonic access structure is transformed with linear secret sharing, which is linearly reconstructed for each linear secret sharing scheme. The specific reconstruction method is as follows: Let (M, ρ) represent an access structure T, $S \in U$ is an authorization set, let the set $I = \{i : f)i) \in S\}$, the existence of constant set $\{w_i \in Z_p\}_{i \in I}$, If λ_i is a legitimate authorized set for Π for s, $\sum_{i \in I} w_i \lambda_i = s$ exists, otherwise there will be no such constant set.

3 Scheme Formalization and Security Model

3.1 Concepts of the Scheme Formalization

In an authorization model comparison-based attributes (range), there is a number of users. In the system, each user is assigned a unique identity identifier GID. The CA is responsible for distributing the key and managing the attribute domain to the user, for the global attribute set $U = \{1, 2, \cdots, m\}$.

In this paper, there are five algorithms, namely, Setup, Encrypt, KeyGen, Tp-Dencrypt and Dencrypt. The next five algorithms will be give a formal description:

1) $setup(1^\lambda \rightarrow \delta)$: In the system given a safe random parameter 1^λ as input, the system outputs the global public parameter δ and the system's master key parameter MK.

2) $Encrypt(\delta, MSG, T \rightarrow CT)$: The message MSG, the global public parameter δ and the user specified access structure T as input, export ciphertext CT. T as input should be a monotone access structure.

3) $KeyGen(MK, S \rightarrow SK)$: The host key MK and the user's attribute weights set S as input, and the user's private key SK is output, assuming $S \in P$ is a weighted set of authorizations.

4) $Tp - Decrypt(SK, CT \rightarrow CT')$: In order to reduce the computational pressure when decrypting the user, the user submits the private key SK to the trusted third party agent decrypts the ciphertext and decrypts the ciphertext CT' which the proxy decrypts to the user, for the next step.

5) $Decrypt(SK, CT' \rightarrow MSG)$: The encrypted data holding user uses the private key SK and the ciphertext CT' as the input for the system, and the system will judge the information provided by the user to run the decryption algorithm. If the user complies with the access policy output MSG, the $\perp$ will be output and the system will be terminated.

3.2 Security Model

In the security confirmation process, a Challenger B and an Adversary A are defined. The Adversary chooses and challenges a Challenger, and the chosen Challenger accepts this challenge to play an indistinguishable under chosen plaintext attack (IND-CPA) game. The rules of an IND-CPA game are as follows:

System Initialization: A challenger inputs a stochastic parameter λ, and then the system's public parameter δ and master key parameter MK are generated.

Phase 1: The Adversary chooses the attribute set to be asked $U_i = \{u_{i,j}, u_{i,t}\}_{U_i \in U}$ submitted to the Challenger, and then the Challenger generates the corresponding private attribute key by operating the key generation algorithm and presents them to the Adversary.

Challenge: The Adversary chooses and presents to the Challenger two messages MSG_0 and MSG_1 with the same length and an authorized access set Q, which he wants to challenge. $U_{i,U_i \in U} \cap Q = \phi$ is worthy of note. The Challenger randomly chooses $\sigma \in \{0, 1\}$, computes the ciphertext $CT_\sigma = Encrypt(\delta, MSG, Q)$, and presents the latter to the Adversary.

Phase 2: The Adversary repeats the work in Phase 1 and continues to inquire the private attribute key of an attribute set $O_i = \{u_{i,j}, u_{i,t}\}_{O_i \in U}$. $O \cap Q = \phi$ is worthy of note. The Challenger computes the private attribute key according to the attribute value in the attribute set O and presents this attribute key to the Adversary.

Guess: The Adversary inputs his conjecture about $\sigma' \in \{0, 1\}$ according to the information in hand. If $\sigma = \sigma'$, then the Adversary wins. The advantage probability of the Adversary's winning is defined as $Adv_A := |Pr[\sigma = \sigma'] - \frac{1}{2}|$.

4 Design of the Scheme Algorithm

In the access structure of this paper, users can submit a monotonic access structure with (t, n) threshold, etc. In the access structure, the user can specify the weight range of the attribute, and only the user who satisfies the access structure and satisfies the weight range of the specified attribute in the access structure can complete the decryption operation. Next, the program execution process is described as follows:

$setup(\lambda, U)$: Enter a security parameter λ in the system, and the system call group generation algorithm generates the multiplication cycle group G and G_T of the two order P, group G generated by g, existing map $e : G \times G \rightarrow G_T$; Select the random number α, β, $\phi \in Z_p$, and select two parameters $\{\theta_i, \mu_i\}_{U_i \in U}$ for each property. Get the open parameter $PK = \{g, e(g, g)^\alpha, g^\alpha, \phi, \{\theta_i, \mu_i\}_{U_i \in U}, h_1, h_2, \cdots, h_m\}$, master key $MK = g^\alpha$.

$Encrypt(\delta, MSG, T \rightarrow CT)$: Input message MSG, global open parameter δ and user specified access structure T as input. Assuming that the attribute U_i sets the range $P_i = \{\tau_i, \tau_i'\}_{U_i \in U}$, $\{\tau_i, \tau_i'\}$ is the interval $[u_{i,j}, u_{i,k}]$ used for the attribute in the attribute access policy. Therefore, $V_{p_i} = V_{\{\rho_i, \rho_i'\}_{U_i \in U}} = \varphi^{\theta_i^{\tau_i} \mu_i^{Z - \tau_i'}}$ exists. The data receiver not only needs to satisfy the attribute access structure specified by the user, but also satisfy the specific attribute of the

range. The monotonic access structure T conversion generates a linear secret sharing matrix (M, ρ), which ρ_i maps M_i to specific attributes, and M_i represents the i-th row of M. The algorithm randomly selects the vector $v = (s, v_2, v_3, \cdots, v_n)$, $s \in Z_p$ for the required shared secret; randomly selects $r_x \in Z_p$.

Output the ciphertext:
$CT = \{C = MSG \cdot e(g,g)^{\alpha s}, (M,\rho), C' = g^s, C_{i(i\in\{1,2,\cdots,m\})}, C'_{i(i\in\{1,2,\cdots,m\})}\}$. Among them,

$$\begin{aligned} C_i &= \varphi^{\theta_i^{\rho_i}} \mu^{Z-\rho'_i} \cdot g^{\alpha\lambda_i} h_i^{-r_i} \\ C'_i &= g^{r_i}, \quad i \in \{1,2,\cdots,m\}. \end{aligned}$$

$KeyGen(MK, S \rightarrow SK)$: The $r \in Z_p$ is randomly selected by the master key MK and the user's weight set S as input, and the weight order value $U_{i,user(U_i\in S)} := V_{\{u_{i,user,j'}, u_{i,user,t'}\}_{u_i\in U_i\in S}} = \varphi^{\theta_i^{\tau_i}} \mu_i^{Z-\tau'_i}$ of the user attribute is calculated; the private key $SK = \{V_{\{u_{i,user,j'}, u_{i,user,t'}\}_{u_i\in U_i\in S}}, K = g^{\alpha} g^{\alpha r}, L = g^r, K_{U_i} = h'_{U_i}, \forall U_i \in S\}$ of the user is output, assuming that $S \in U$ is a weighted set of authorizations.

$Tp - Decrypt(SK, CT \rightarrow CT')$: The user submits the private key SK to the trusted third party agent decrypts the ciphertext and then trusts the third party to run the policy recovery (check) algorithm (Υ), which is calculated by replacing it with the user:

$$\begin{aligned} \widehat{C_1} &= C_1 / \psi(\{\mu_{i,j}, \mu_{i,t}\}_{U_i\in U}) \\ &= \varphi^{\theta_1^{\rho_1}} \mu^{Z-\rho'_1} \cdot g^{\alpha\lambda_1} T^{-r_1} / \varphi^{\theta_i^{\mu_{i,user,j'}} \mu_i^{Z-\mu_{i,k}}} \end{aligned}$$

So $CT' = \{C = MSG \cdot e(g,g)^{\alpha s}, (M,\rho), C' = g^s, \widehat{C}_{i(i\in\{1,2,\cdots,m\})}, C'_{i(i\in\{1,2,\cdots,m\})}\}$ gives the user the next step of decryption.

$Decrypt(SK, CT' \rightarrow MSG)$: The encrypted data holding user uses the private key SK and the encrypted ciphertext CT' issued by the system as input, and the calculation constant $w_i \in Z_p$ satisfies $\sum_{\rho_i\in S} w_i M_i = (1, 0, \cdots, 0)$. Decryption first calculated: $B = \frac{e(C',K)}{\Delta} = e(g,g)^{\alpha s}$, among $\Delta = \prod_{\rho_i\in S}(e(\widehat{C}_{i(i\in\{1,2,\cdots,m\})}, L) \cdot e(\widehat{C}'_{i(i\in\{1,2,\cdots,m\})}, K_{U_i} = T'_{U_i}))^{w_i}$. Finally, it can be concluded that $MSG = C/B$.

5 Security Confirmation and Comparison

5.1 Security Analysis

Theorem 1. *In the selected model, if there is an adversary A in the probabilistic polynomial time can't ignore the advantages of breaking the program, you can solve the q-parallel BDHE difficult assumptions.*

Proof. The challenger sets the random parameter y by Definition 1, selects a random parameter $\sigma \rightarrow_R \{0,1\}$, and if $\sigma = 0$, there is $Z = e(g,g)^{\alpha^{q+1}}$; Otherwise $Z \rightarrow G_T$. Before the game begins, A will declare to the B, the access structure $M^*, \rho^*)$ to challenge, where the number of M^* columns is n^*.

Initially. B first randomly selected $\alpha' \in Z_p$, and $\alpha = \alpha' + \alpha^{q+1}$, there is $e(g,g)^{\alpha} = e(g,g)^{\alpha'} \cdot e(g^{\alpha}, g^{\alpha^{q+1}})$. B build parameter $h_1, h_2, \cdots, h_m$, for each $x(1 \le x \le m)$ corresponds to a random parameter $z_x \in Z_p$, if there is a set of $\rho^*(i) = x$ for the index i, then $h_x = g^{z_x} \cdot g^{\alpha M^*_{i,1}/b_i}, g^{\alpha^2 M^*_{i,2}/b_i}, \cdots, g^{\alpha^{n^*} M^*_{i,n^*}/b_i}$; otherwise, $h_x = g^{z_x}$.

Phase 1: A Queries an access set S, where S does not satisfy the access structure M^*. B randomly selected $r \in Z_p$, seeking vector $\overrightarrow{w} = (w_1, w_2, \cdots, w_{n^*}) \in Z_p^{n^*}$ to make $w_1 = -1$, and for all i have $\rho^*(i) \in S$, $w \cdot M_i^* = 0$. Define $t = r + w_1\alpha^q + w_2\alpha^{q-1} + \cdots + w_{n^*}\alpha^{q-n^*+1}$, so $L = g^t = g^r \cdot g^{w_1\alpha^q} \cdot g^{w_2\alpha^{q^1}} \cdots g^{w_{n^*}\alpha^{q-n^*+1}}$; now calculate K_x, $\forall (x = U_i) \in S$. First consider the case for all i no $\rho^*(i) = x$, so $K_{U_i} = L^{z_x}$; when there are multiple i makes $\rho^*(i) = x$, because it is not allowed to simulate $g^{\alpha^{q+1}}$, K_x does not allow similar to $g^{\alpha^{q+1}}$ items. Because of $w \cdot M_i^* = 0$, all of the indices including α^{q+1} are going to cancel out. As a result, $K_x = L^{z_x} \cdot \prod_{j=1,2,\cdots,n^*}(g^{(\alpha^j/b_i)r} \prod_{k=1,2,\cdots,n,k\neq j}(g^{\alpha^{q+1+j-k}/b_i})^{w_k}) M^*_{i,j}$.

Challenge: A sends two lengths of the same message to B as MSG_0 and MSG_1. B randomly selects $\sigma \rightarrow_R \{0,1\}$, encrypts MSG_σ, calculates $C = MSG_\sigma \cdot Z \cdot e(g,g)^{s\alpha'}$ and $C' = g^s$, and then randomly selects $v'_2, v'_3, \cdots, v'_{n^*}$ from B to get $v = (s, s\alpha + v'_2, s\alpha^2 + v'_3, \cdots, s\alpha^{n^*-1} + v'_{n^*}) \in Z_p^{n^*}$; B randomly selected $r'_i \in Z_p$, $i = 1, 2, \cdots, n^*$, available $C_i = \varphi^{\theta_i^{\rho_i}} \mu^{Z-\rho'_i} \cdot h^{-r'_i}_{\rho^*(i)} \cdot \sum_{j=1}^{n^*} (g^{\alpha})^{M^*_{i,j} y'_j} \cdot (g^{b_i \cdot s})^{-z_{\rho^*(i)}} \cdot \prod_{k=1,2,\cdots,n^*,k\neq j}(g^{\alpha^j \cdot s(b_i/b_k)})^{M^*_{i,j}}$ and $C'_i = g^{r'_i} g^{sb_i}$.

Phase 2: The same as Phase 1.

Guess: A output on the σ speculation, if $\sigma = 0$, there are $Z = e(g,g)^{\alpha^{q+1}}$; otherwise $Z \rightarrow G_T$. If B can win this game, it can also win the Definition 1 by the same advantage.

□

5.2 Scheme Comparison

In this section, we compare the aspects of security assumptions, access strategies and policy development flexibility, ciphertext length and fine-grained access control with [21, 23, 29]. In the ciphertext length, assume that the attribute set is I; access strategy and strategy development flexibility to compare its access control and other flexibility level, the contrast index for the development of

Table 1: Scheme comparison

Scheme	Ciphertext Size	Assumptions	Access Strategy and Flexibility	Fine-grained Access Control
[21]	$O(n^m)$	q-parallel BDHE	Medium	Yes
[23]	$O(n^m)$	–	Low	Yes
[29]	$O(n)$	l-w BDHI	Medium	No
Our	$O(n^m)$	q-parallel BDHE	High	Yes

a variety of policies can be developed access control structure; the main contrast indicator of fine-grained access control is whether the comparison of attribute weights and the comparison of attribute weights can be achieved in the scheme strategy, such as whether to control the scope of the attribute weight. The specific scheme is shown in Table 1.

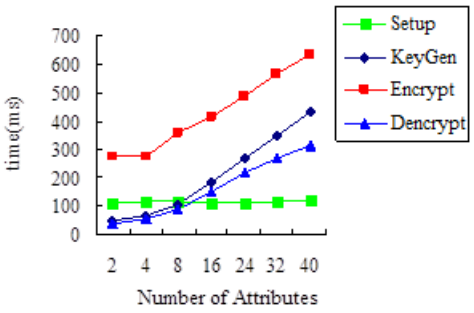

Figure 2: Simulation diagram

Analysis of Table 1, we can see that the proposed scheme has better performance in the scheme proposed in other literatures. In order to further illustrate the program can meet the needs of social networks in terms of performance, this paper simulates the environment i5-4590 3.3MHz, 4G RAM running under Windows 10 Professional; written in eclipse tools using Java, using the JPBC 1.2. 0, in order to facilitate comparison, each attribute is divided into eight sub-attributes for verification, a specific description as shown in Figure 2. The number of attributes increases exponentially from 2 to 8, and linearly increases from 8 (increasing by 8 each time). In order to show the relationship between the number of attributes and program run time. By calculating the time can be drawn that the program consumed by the time can be applied to multimedia social networks.

6 Conclusion

According to the characteristics of the property, this paper found that the previous ABE schemes seldom pay attention to the issue of attribute level. Therefore, this paper proposes an encryption scheme based on attribute weight order, and applies it to multimedia social network to solve the problem of user privacy data protection and authorization sharing. The program has the following two characteristics: 1) the data owner can make more fine-grained access control strategy according to the requirements, in order to meet the more detailed requirements of the same attribute; 2) this paper not only consider the sequence attribute weights, but also make a simple comparison and set the attribute authorization interval (range), increase the flexibility of the program and also make it more suitable for practical application scenarios. Through the comparative analysis of this scheme and other programs, experiments show that the system of this solution can be better adapted to the real application scenarios. In the future work, in order to improve the user experience, you can consider ways to use crowdsourcing [30, 31] to improve system efficiency.

Acknowledgments

The work was sponsored by National Natural Science Foundation of China Grant No.61772174 and 61370220, Plan For Scientific Innovation Talent of Henan Province Grant No.174200510011, Program for Innovative Research Team (in Science and Technology) in University of Henan Province Grant No.15IRTSTHN010, Program for Henan Province Science and Technology Grant No.142102210425, Natural Science Foundation of Henan Province Grant No.162300410094, Project of the Cultivation Fund of Science and Technology Achievements of Henan University of Science and Technology Grant No.2015BZCG01.

References

[1] A. Sahai, B. Waters, "Fuzzy identity-based encryption," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, *et al.*, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.

[3] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy (SP'07)*, pp. 321–334, 2007.

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

[5] Z. Liu, Z. L. Jiang, X. Wang, *et al.*, "Offline/online attribute?based encryption with verifiable outsourced decryption," *Concurrency and Computation: Practice & Experience*, vol. 29, no. 7, pp. 1–17, 2016.

[6] Y. Wu, Z. Wei, R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," *IEEE Transactions on Multimedia*, vol. 15, no. 4, pp. 778–788, 2013.

[7] Z. Zhang, B. B. Gupta, "Social media security and trustworthiness: overview and new direction," *Future Generation Computer Systems*, 2016. (DOI:10.1016/j.future.2016.10.007)

[8] M. Y. Shabir, A. Iqbal, Z. Mahmood, *et al.*, "Analysis of classical encryption techniques in cloud computing," *TsingHua Science and Technology*, vol. 21, no. 1, pp. 102–113, 2016.

[9] J. Han, W. Susilo, Y. Mu, *et al.*, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 665–678, 2015.

[10] C. C. Lee, P. S. Chung, M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231–240, 2013.

[11] H. Wang, Z. Zheng, L. Wu, *et al.*, "New directly revocable attribute-based encryption scheme and its application in cloud storage environment," *Cluster Computing*, vol. 20, no. 3, pp. 2385–2392, 2017.

[12] Y. Zhao, P. Fan, H. Cai, *et al.*, "Attribute-based encryption with non-monotonic access structures supporting fine-grained attribute revocation in m-healthcare," *International Journal of Network Security*, vol. 19, no. 6, PP. 1044–1052, 2017.

[13] Y. S. Rao, "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing," *Future Generation Computer Systems*, vol. 67, pp. 133–151, 2017.

[14] W. Sun, S. Yu, W. Lou, *et al.*, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 4, pp. 1187–1198, 2016.

[15] H. Zheng, J. Qin, J. Hu, *et al.*, "Threshold attribute?based signcryption and its application to authenticated key agreement," *Security & Communication Networks*, vol. 9, no. 18, pp. 4914–4923, 2016.

[16] W. Li, K. Xue, Y. Xue, *et al.*, "Tmacs: A robust and verifiable threshold multi-authority access control system in public cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 5, pp. 1484–1496, 2016.

[17] Z. W. Wang, Z. Z. Chu, "Efficient mediated ciphertext-policy attribute-based encryption for personal health records systems," *Journal of Internet Technology*, vol. 16, no. 5, pp. 877–883, 2015.

[18] L. Zhen, Z. Cao, D. S. Wong, "Efficient generation of linear secret sharing scheme matrices from threshold access trees," *Cryptology ePrint Archive*, Report 2010/374. (`http://eprint.iacr.org/2010/374`)

[19] A. Lewko, B. Water, "Decentralizing attribute-based encryption," in *Advances in Cryptology (EUROCRYPT'11)*, pp. 568–588, 2011.

[20] Y. Zhu, H. Hu, G. J. Ahn, *et al.*, "Comparison-based encryption for fine-grained access control in clouds," in *ACM Conference on Data and Application Security and Privacy*, pp. 105–116, 2012.

[21] X. Liu, J. Ma, J. Xiong, *et al.*, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," *International Journal of Network Security*, vol. 16, no. 6, pp. 437–443, 2014.

[22] S. Wang, K. Liang, J. K. Liu, *et al.*, "Attribute-based data sharing scheme revisited in cloud computing," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 8, pp. 1661–1673, 2016.

[23] Z. Wang, D. Huang, Y. Zhu, *et al.*, "Efficient attribute-based comparable data access control," *IEEE Transactions on Computers*, vol. 64, no. 12, pp. 3430–3443, 2015.

[24] K. Xue, J. Hong, Y. Xue, *et al.*, "CABE: A new comparable attribute-based encryption construction with 0-encoding and 1-encoding," *IEEE Transactions on Computers*, vol. 66, no. 9, pp. 1491–1503, 2017.

[25] T. Okamoto, T. Okamoto, K. Takashima, *et al.*, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *International Conference on Theory and Applications of Cryptographic Techniques*, pp. 62–91, 2010.

[26] Z. Liu, Z. Cao, Q. Huang, *et al.*, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in *European Symposium on Research in Computer Security*, pp. 278–297, 2011.

[27] H. Deng, Q. Wu, B. Qin, *et al.*, "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," *Information Sciences*, vol. 275, no. 11, pp. 370–384, 2014.

[28] C. C. Lee, M. S. Hwang, S. F. Tzeng, "A New Convertible Authenticated Encryption Scheme Based on the ElGamal Cryptosystem," *International Journal of Foundations of Computer Science*, vol. 20, no. 2, pp. 351–359, 2009.

[29] J. Li, Q. Wang, C. Wang, *et al.*, "Enhancing attribute-based encryption with attribute hierarchy," *Mobile Networks & Applications*, vol. 16, no. 5, pp. 553–561, 2011.

[30] Z. Zhang, R. Sun, X. Wang, *et al.*, "A situational analytic method for user behavior pattern in multi-

media social networks," *IEEE Transactions on Big Data*, 2017. (DOI:10.1109/TBDATA.2017.2657623)

[31] Z. Zhang, K. K. R. Choo, A. K. Sangaiah, *et al.*, "Crowd computing for social media ecosystems," *Applied Soft Computing*, vol. 66, pp. 492–494, 2018.

Biography

Cheng Li is currently a postgraduate majoring in Computer Science, Information Engineering College, Henan University of Science & Technology. His research interest focuses on information security, applied cryptography and multimedia social networks security.

Zhiyong Zhang, born in 1975 October, earned his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, P. R. China, respectively. He was post-doctoral fellowship at School of Management, Xi'an Jiaotong University, China. Nowadays, he is a full-time Henan Province Distinguished Professor, Ph.D. Supervisor and Dean with Department of Computer Science, Information Engineering College, Henan University of Science & Technology. He was also a visiting professor of Computer Science Department of Iowa State University. Prof. Zhang and research interests include multimedia content security and soft computing, social big data analytics, digital rights management, and so on. He is IEEE Senior Member (06'M, 11'S), ACM Senior Member (08'M, 13'S), IEEE Systems, Man, Cybermetics Society Technical Committee on Soft Computing. And also, he is Editorial Board Member of Multimedia Tools and Applications (Springer, SCI), Neural Network World (Czech Republic, SCI), Journal on Big Data (Springer) and EURASIP Journal on Information Security (Springer), Associate Editor of Human-centric Computing and Information Sciences (Springer), Leading Guest Editor/Co-Guest Editor of Applied Soft Computing (Elsevier, SCI), Computer Journal (Oxford, SCI), Future Generation Computer Systems (Elsevier, SCI), as well as International Advisory Board Member of International Journal of Cloud Applications and Computing (IGI Global). Recent years, he has published over 120 scientific papers and edited 6 books in the above research fields, and also holds 10 authorized patents.

Guoqin Chang, is a postgraduate student of Laboratory of Intelligent Computing & Application Technology for Big Data, Henan University of Science and Technology. Her research interests in intelligent information processing and data mining.