Improving Security in Ciphertext-Policy Attribute-Based Encryption with Hidden Access Policy and Testing

Hongjian Yin, Leyou Zhang*, Yilei Cui
School of Mathematics and Statistics, Xidian University
Xi'an, Shaanxi 710171 - China
[e-mail: honjanyin@163.com, lyzhang@mail.xidian.edu.cn, CYL_Study@163.com]
*Corresponding author: Leyou Zhang

Received February 28, 2018; revised September 20, 2018; accepted November 3, 2018; published May 31, 2019

Abstract

Ciphertext-policy attribute-based encryption (CP-ABE) is one of the practical technologies to share data over cloud since it can protect data confidentiality and support fine-grained access control on the encrypted data. However, most of the previous schemes only focus on data confidentiality without considering data receiver privacy preserving. Recently, Li et al.(in TIIS, 10(7), 2016.7) proposed a CP-ABE with hidden access policy and testing, where they declare their scheme achieves privacy preserving for the encryptor and decryptor, and also has high decryption efficiency. Unfortunately, in this paper, we show that their scheme fails to achieve hidden access policy at first. It means that any adversary can obtain access policy information by a simple decisional Diffie-Hellman test (DDH-test) attack. Then we give a method to overcome this shortcoming. Security and performance analyses show that the proposed scheme not only achieves the privacy protection for users, but also has higher efficiency than the original one.

Keywords: CP-ABE, anonymity, hiding access policy, decrypt testing

This work was supported in part by the Nature Science Foundation of China under Grant (NO. 61472307, 61402112, 61100165 and 61100231), the Natural Science Basic Research Plan in Shaanxi Province of China (NO. 2016JM6004), the National Key Research and Development Program of China (NO. 2017YFB0802002), and the National Cryptography Development Fund under Grant (NO. MMJJ20180209).

http://doi.org/10.3837/tiis.2019.05.029 **ISSN : 1976-7277**

1. Introduction

As one of the research hotspots of public key encryption, attribute-based encryption (ABE) [1] is considered an effective way to achieve fine-grained access control of encrypted data in Cloud storage. In ABE schemes, access policies are represented by attribute sets, and it can be specified by data owners to allow those users whose attribute set satisfies the specified policy to access the encrypted data.

Generally speaking, the ABE schemes can be divided into two types: key-policy attribute-based encryption and ciphertext-policy attribute-based encryption, abbreviated as CP-ABE and KP-ABE respectively. In the KP-ABE schemes [2-4], ciphertexts are associated with attributes set, and users' secret keys are related to access structures. Conversely, in the CP-ABE schemes [5-7], attributes are associated with secret keys and access structures are related to the ciphertexts. In particular, this paper only focus on CP-ABE.

In traditional CP-ABE schemes [5-7], access policies are sent to users as a part of the ciphertext. It means that any user, whether he/she is legal or not, can know the access policy as long as he/she gets the ciphertexts. In some cases, however, the access policy itself is the sensitive information. For instance, Alice shares her encrypted data and sets the access policy so that the mental health counselor will be able to decrypt her health records. So, the attributes "mental health" and "counselor" included in the access policy. And anyone, although he or she cannot decrypt the ciphertext, may guess that Alice is suffering some mental health problems.

In order to further prevent users from revealing their privacy, the concept of ABE with partially hidden policy was introduced by Nishide et al. in [10]. They presented two schemes to hide the policy of CP-ABE. In these schemes, a decryptor neither decrypt the data nor guess the access policy information, if the decryptor's attributes set do not satisfy the ciphertext policy. In addition, their schemes have proved to be selective security. Since then, some other CP-ABE schemes with policy hidden have been proposed one after another. In [11], under composite order group, the authors constructed a ciphertext-policy hiding CP-ABE scheme. This scheme is fully security and supports AND-gate access policy. In order to enhance the flexibility of access policy, Wang and He [12] proposed a hidden policy scheme with LSSS matrix access structure. Recent works in this area focused on constructing more efficient ciphertext-policy hidden CP-ABE with short ciphertext size [13-14], developing schemes with additional applications such as keyword search [15-16].

However, in the ciphertext-policy hiding CP-ABE proposals, users need to do excessive calculation for decryption no matter their attribute sets match the ciphertext-policy or not, which makes the users do too many useless computations when their attribute sets do not match the hidden policy. To enhance the efficiency of previous schemes, a novel access policy hidden CP-ABE scheme was introduced in [17]. In their scheme, users can test whether their attributes match the ciphertext-policy or not before performing the decryption operation. Furthermore, the consumption of test operation is much less than that of decryption calculation. Unfortunately, we found that their scheme cannot hide the access policy. In particular, any adversary can use public parameters, such as public keys and ciphertexts, to get attribute information about access policy, easily.

1.1 Our Contributions

In this paper, there are two main contributes. Firstly, a detailed security analysis of the literature [17] is given to illustrate that access policy hidden cannot be realized in this scheme.

Secondly, an improved access policy hidden scheme is constructed to solve the shortcomings of literature [17]. In our scheme, the problem of user privacy leakage can be avoided by hiding the access policy. In addition, the security of the proposed scheme is reduced to DBDH assumption under the standard model. Security analyses and performance comparison show that our scheme not only realizes users' privacy protection, but also has higher efficiency than the original one.

1.2 Organization

Some preliminaries are given in section 2. The security analysis of the scheme in [17] is given in section3. Section 4 proposes the improved CP-ABE with policy hidden. Security proof and some comparisons between our scheme and previous works are introduced in section 5 and 6, respectively. The conclusions are given in section 7 finally.

2. Preliminaries

2.1 Bilinear Mapping

Let G and G_T be cyclic groups of prime order p. g is the random generator of the group G. $e: G \times G \to G_T$ is called a bilinear mapping if the following properties are satisfied:

(i) Bilinearity: for all $g, h \in G$ and $a, b \in Z_N$, $e(g^a, h^b) = e(g, h)^{ab}$;

(ii) Non-degeneracy: $e(g, g) \neq 1$;

(iii) Computability: $\forall g, h \in G$, there are efficient algorithms to compute $e(g, h)$.

2.2 Hardness Assumption

Let $a, b, c, z \in_R Z_p$, and $g \in_R G$ be a generator. The decisional bilinear Diffie-Hellman (DBDH) assumption holds in group G: if no probabilistic polynomial-time algorithm can distinguish the tuple $[g, g^a, g^b, g^c, e(g, g)^{abc}]$ from $[g, g^a, g^b, g^c, e(g, g)^z]$ with non-negligible advantage.

2.3 Access Policy

Following [11], the access structure type of our construction is AND-gate with multi-valued attributes. This access policy is described as follows.

Let $\widetilde{U} = \{att_1, att_2, \cdots, att_n\}$ be an attributes set. $S_i = \{v_{i,1}, v_{i,2}, \cdots, v_{i,n_i}\}$ are all possible values of attribute $att_i \in \widetilde{U}$. Let $L = [L_1, L_2, \cdots, L_n]$ be user's attribute list where $L_i \in S_i$. The access policy $W = [W_1, W_2, \cdots, W_n]$, where $W_i \in S_i$. In this paper, we use $L \models W$ to represent that L satisfies W, and $\models$ indicates unsatisfactory symbol.

2.4 Definition of CP-ABE with Hidden Access Policy and Testing

The formal definition of CP-ABE with hidden access policy and testing scheme is given as follows. There are four algorithms in this scheme.

-Setup(1^λ): Taking security parameter 1^λ as inputs, then this algorithm generates public key PK and master secret key MSK.

-KeyGen(PK, MSK, L): The KeyGen takes as inputs PK, MSK as well as user attribute set L, and generates the attribute list L's auxiliary information and some other secret keys.

-Encrypt(PK, M, W): It inputs the message M, public parameter PK and policy W and outputs the corresponding ciphertexts CT_W. Here the access policy W's auxiliary information

is a part of the ciphertext CT_W.

-Decrypt(PK, CT_W, SK_L): This algorithm consists of two phases: access policy testing and decryption phase. This algorithm takes as inputs the public parameter PK, ciphertexts CT_W as well as the secret key SK_L. It first runs the *Testing phase* to check whether user attributes set satisfies the ciphertext- policy about CT_W or not. If the testing matches well, this algorithm runs the *Decryption phase* and outputs M.

2.5 Security Model

Similar to literature [21], the following is the definition of the indistinguishability against selective ciphertext-policy and chosen-plaintext attacks (IND-sCP-CPA) model. This model is simulated between adversary $\mathcal{A}$ and a challenger $\mathcal{B}$.

Initial: $\mathcal{A}$ chooses challenge policies W_0^* and W_1^* and submits them to $\mathcal{B}$.

Setup: The challenger picks a security parameter 1^λ, and runs Setup algorithm to get a master secret key MSK and public parameter PK. The challenger reserves MSK and sends PK to the adversary.

Phase 1: $\mathcal{A}$ submits an attribute list L for the KeyGen query. $\mathcal{B}$ returns SK_L to $\mathcal{A}$ only if $L \not\models W_0^* \wedge L \not\models W_1^*$. Otherwise, it outputs $\perp$.

Challenge: $\mathcal{A}$ submits two equal length messages M_0^* and M_1^* to the challenger on which it wishes to challenge with respect to W_0^* and W_1^*. $\mathcal{B}$ picks a random bit $\rho \in \{1,0\}$ and sends CT = *Encrypt*(PK, M_ρ^*, W_ρ^*) to $\mathcal{A}$.

Phase 2: It is similar to Phase 1.

Guess. Finally, the adversary outputs its guess $\rho' \in \{1,0\}$, and wins the game if $\rho' = \rho$.

The advantage of adversary in this game can be defined $\left|Pr[\rho' = \rho] - \frac{1}{2}\right|$.

Definition 1. A hidden access policy CP-ABE scheme is secure against selectively chosen plaintext attack if all polynomial time adversaries have a negligible advantage in the above game.

3. Review and Security Analysis of Li et al.'s Scheme

3.1 Review of Li et al.'s Scheme

The following is a brief review of the scheme in [17], and it contains four algorithms as follows.

-Setup(1^λ): It takes as inputs the security parameter 1^λ and outputs a bilinear mapping e and two cyclic groups G and G_T. The trusted authority (TA) picks $\alpha, \beta \in_R Z_p$ and $a_{i,j} \in_R Z_p$ where $i \in [1,n]$, $j \in [1,n_i]$. TA computes $Y = e(g,g)^\alpha$, $X = g^\beta$ and $T_{i,j} = g^{a_{i,j}}$, where $i \in [1,n]$, $j \in [1,n_i]$. The public parameters PK and the master secret key MSK are are published as follows:

$$PK = \langle e, G, G_T, g, Y, X, \{T_{i,j}\}_{i\in[1,n], j\in[1,n_i]}\rangle,$$

$$MSK = \langle \alpha, \beta, \{a_{i,j}\}_{i\in[1,n], j\in[1,n_i]}\rangle.$$

-KeyGen(PK, MSK, L): Taking the master secret key MSK, public key PK, and a set of attributes $L = [L_1, L_2, \cdots, L_n]$ as inptus, this algorithm performs the following computing: The trusted authority chooses $u, r^* \in_R Z_p$, and $\lambda_i \in_R Z_p$ for the user, where $1 \le i \le n$. Then

trusted authority computes $D_0 = g^{\alpha+\beta u}$, $D_{i,1} = g^{u+a_{i,j}\lambda_i}$, $D_{i,2} = X^{\lambda_i}$ for decryption. Furthermore, the trusted authority computes $D_i^* = T_{i,j}^{r^*}$, $i \in [1,n]$, $D_0^* = g^{r^*}$, which are used to test whether users' attribute set L satisfies the policy W or not. Finally, this algorithm delives the secret key SK_L to user.

$$SK_L = \langle D_0, \{D_{i,1}, D_{i,2}, D_i^*\}_{1\le i\le n}, D_0^* \rangle.$$

-Encrypt(PK, M, W): This algorithm takes as inputs the public key PK, a message $M \in G_T$ and access policy $W = [W_1, W_2, \cdots W_n]$. The encryptor randomly chooses $s, s^* \in Z_p$, then it computes $\tilde{C} = MY^s$, $C_0 = g^s$, $C_0^* = g^{s^*}$. The encryptor picks up random values $s_i \in Z_p$ such that $s = \sum_1^n s_i$ and computes $C_{i,1} = X^{s_i}$ where $i \in [1,n]$. If $v_{i,j} \in W_i$, the encryptor computes $C_{i,j,2} = T_{i,j}^{s_i}$ and $C_{i,j}^* = T_{i,j}^{s}$; else $v_{i,j} \notin W_i$, $C_{i,j,2}$ and $C_{i,j}^*$ are randomly chosen elements in group G. Finally, this algorithm outputs the corresponding ciphertext CT_W,

$$CT_W = \langle \tilde{C}, C_0, C_0^*, \{\{C_{i,1}\}, \{C_{i,j,2}, C_{i,j}^*\}_{j\in[1,n_i]}\}_{i\in[1,n]} \rangle.$$

-Decrypt(PK, CT_W, SK_L): Taking PK, CT_W, and SK_L as inputs, the decryptor runs the following operations:

(i) **Testing phase:** The user checks whether attribute list L satisfies policy W or not. $L \models W$ if and only if $e(C_0^*, \prod_{i=1}^n D_i^*) = e(D_0^*, C_{i,j}^*)$ holds. If $L \not\models W$, it returns $\perp$ and terminates. If $L \models W$, it enters into the decryption operation.

(ii) **Decryption phase:** Users decrypt the ciphertext to get the massage M by the following eqution.

$$M = \frac{\tilde{C} \prod_{i=1}^n e(C_{i,1}, D_{i,1})}{e(C_0, D_0) \prod_{i=1}^n e(C_{i,j,2}, D_{i,2})}$$

3.2 Security Analysis of Li et al.'s Scheme

In literature [17], authors have introduced a CP-ABE scheme, in which the policy is hidden. In order to enhance the decryption efficiency, their scheme adds the testing phase before the decryption procedure. However, we found that the ciphertext components used for testing phase disclose the underlying ciphertext access policy, in other words, their scheme will leak ciphertext receivers' identity privacy. Next, we explain why the above scheme cannot realize access policy hidden.

Suppose there is an adversary who has knowledge of universe of attributes. The adversary can employ some parts of public parameters and ciphertexts to check if a guess access policy is encrypted in ciphertext, successfully. More concretely, let $T_{i,j}$, X, $C_{i,1}$ and $C_{i,j}^*$ be a decisional Diffie-Hellman (DDH) tuple, the adversary runs the following DDH test attack to determine whether the guess policy W^* is same as the access policy W used in ciphertext or not.

$$e(C_{i,1}, \prod_{W^*} T_{i,j}) \stackrel{?}{=} e(X, \prod_W C_{i,j}^*)$$

If the above equation holds, the adversary can conclude that $W^* = W$. That is to say, the DDH test attack works successfully due to ciphertext components $C_{i,1}$ and $C_{i,j}^*$.

4. The Proposed Scheme

This section will present a novel ciphertext-policy hidden CP-ABE scheme.

4.1 Construction

-Setup(1^λ): To generate the system parameters, the setup algorithm takes the security parameters 1^λ as inputs and outputs a bilinear mapping e as well as two cyclic groups of prime order p, G and G_T. This algorithm randomly chooses a generator g in group G, and elements $\alpha, \tau \in_R Z_p$ and $a_{i,j} \in_R Z_p$ where $i \in [1,n], j \in [1,n_i]$. Finally, it computes $g_1 = g^\tau$, $Y = e(g,g)^\alpha$ and $T_{i,j} = g^{a_{i,j}}$, where $i \in [1,n], j \in [1,n_i]$.

$$PK = \langle e, G, G_T, g, g_1, Y, \{T_{i,j}\}_{i\in[1,n],j\in[1,n_i]}\rangle,$$
$$MSK = \langle \alpha, \tau, \{a_{i,j}\}_{i\in[1,n],j\in[1,n_i]}\rangle.$$

-KeyGen(PK, MSK, L): To get the secret keys, user U submits his/her attribute list $L = [L_1, L_2, \cdots, L_n]$. This algorithm inputs PK, MSK as well as the user attributes set L. Then it outputs secret keys fou U as follows.

Firstly, the KeyGen algorithm randomly picks $\beta \in Z_p$ and $\alpha_k, \beta_k \in_R Z_p$ $(k \in [1,t])$. This algorithm computes $D_0 = g^{\alpha-\beta}$ and $D_{i,j} = g^{\frac{\beta}{a_{i,j}}}$. Furthermore, for all $L_i \in L$, we assume that $L_i = L_{i,1}L_{i,2}\cdots L_{i,l}$ where each $L_{i,m} \in \{0,1\}$ $(m \in [1,l])$. Therefore, the user attributes list $L = [L_1, L_2, \cdots, L_n]$ can be described by a binary array $L = [L_{1,1}\cdots L_{1,l}\cdots L_{n,1}\cdots L_{n,l}]$. For convenience, we set $L = [l_1 l_2 \cdots l_t]$ $(l_k \in \{0,1\})$. Let $h_0 = g$, for $i = 1$ to t, and the KeyGen algorithm computes $h_i = (h_{i-1})^{\alpha_i^{l_i}\beta_i^{1-l_i}}$ and sets the attribute list L's auxiliary information $h_L = h_t$. Finally, this algorithm computes $D^* = h_L^\tau$ and outputs user $U's$ secret keys SK_L,

$$SK_L = \langle D_0, \{D_{i,j}\}_{v_{i,j}\in L}, D^*\rangle.$$

-Encrypt(PK, M, W): Firstly, the data owner randomly selects $r \in Z_p$, $s_i \in Z_p$ and sets $s = \sum_1^n s_i$. Then he/she runs the encrypt algorithm and encrypts the message $M \in G_T$ with aeecss policy $W = [W_1, W_2, \cdots W_n]$ as follows:

$$\tilde{C} = MY^s, C_0 = g^s, C_0^* = g^r \text{ and } C_1^* = e(g_1, h_W)^r.$$

And for $v_{i,j} \in W$, the encryptor computes $C_{i,j} = T_{i,j}^{s_i}$. Finally he outputs the ciphertexts as

$$CT_W = \langle \tilde{C}, C_0, C_0^*, C_1^*, \{C_{i,j}\}_{v_{i,j}\in W}\rangle.$$

-Decrypt(PK, CT_W, SK_L): To decrypt the ciphertext, decryptor inputs its secret key SK_L and some other public parameters and runs the following operations.

(i) Testing phase: The decryptor computes the following equation to check whether its attirbutes satisfy the ciphertext policy.

$$e(C_0^*, D^*) \stackrel{?}{=} C_1^* \quad (1)$$

If the above equation does not hold, then the decryption calculations terminate. Otherwise, the decryptor continues the next phase.

(ii) Decryption phase: The decryptor recovers the message M as follows.

$$M = \frac{\tilde{C}}{e(C_0, D_0) \cdot \prod_{a_{i,j} \in L} e(C_{i,j}, D_{i,j})} \tag{2}$$

4.2 Correctness of the Proposed Construction

If attribute list L satisfies the ciphertext-policy, it means that $L_i = W_i$ and $h_L = h_W$ hold. We first show that the Eq.(1) holds as follows.

$$\begin{aligned} & e(C_0^*, D^*) \\ &= e(g^r, h_L^\tau) \\ &= e(g_1, h_L)^r \\ &= e(g_1, h_W)^r = C_1^* \end{aligned}$$

Then the message M can be computed by the following equation.

$$\begin{aligned} & \frac{\tilde{C}}{e(C_0, D_0) \cdot \prod_{a_{i,j} \in L} e(C_{i,j}, D_{i,j})} \\ &= \frac{M \cdot e(g,g)^{\alpha s}}{e(g^s, g^{\alpha-\beta}) \cdot \prod_{a_{i,j} \in L} e\left(g^{a_{i,j} s_i}, g^{\frac{\beta}{a_{i,j}}}\right)} \\ &= \frac{M \cdot e(g,g)^{\alpha s}}{e(g,g)^{\alpha s} \cdot e(g,g)^{-\beta s} \cdot \prod_{a_{i,j} \in L} e(g,g)^{\beta s_i}} \\ &= \frac{M}{e(g,g)^{-\beta s} \cdot e(g,g)^{\beta \sum_{i=1}^{n} s_i}} = M \end{aligned}$$

4.3 Access Policy Hiding

Next, we will expound that the proposed scheme achieves access policy hiding. Suppose there is an adversary who has knowledge of universe of attributes. The adversary wants to employ public parameters and ciphertexts to check whether a guess access policy is encrypted in ciphertexts or not.

Suppose the adversary is given ciphertexts $CT_W = \langle \tilde{C}, C_0, C_0^*, C_1^*, \{C_{i,j}\}_{v_{i,j} \in W} \rangle$, which is the outputs of the encryption algorithm under an access policy W. Then it makes a guess W^* of W. The DDH-like test is $e(C_0^*, h_{W^*}) \stackrel{?}{=} C_1^*$, it can also be represented as $\frac{e(C_0^*, h_{W^*})}{C_1^*} \stackrel{?}{=} 1$. Because

$\frac{e(C_0^*,h_{W^*})}{C_1^*} = \frac{e(g^r,h_{W^*})}{e(g^\tau,h_W)^r} = \frac{e(g,h_{W^*})^r}{e(g,h_W)^{\tau \cdot r}}$, and τ is one of the master secret key in the scheme. In this case, no matter whether $W^* = W$ or not, $\frac{e(C_0^*,h_{W^*})}{C_1^*} \neq 1$. Thus, the adversary can not determine which access policy is used in the ciphertexts and our proposed construction preserves access policy hiding.

5. Security Analysis

This section will prove that the proposed scheme is selective security under the DBDH assumption.

Game_0 is the original game. Game_1 is like Game_0 expect the challenge ciphertexts. In this game, $\tilde{C}$ is selected randomly from G_T when the attribute list $L \not\models W_0^* \wedge L \not\models W_1^*$, and the other ciphertexts are created normally. When $L \models W_0^* \wedge L \models W_1^*$, the challenge ciphertexts are generated correctly. That is, $\text{Game}_0 = \text{Game}_1$ in this case.

Theorem 1. If there is an adversary that is able to distinguish Game_0 and Game_1 with the advantage ε, then we can simulate an algorithm that can solve the DBDH assumption with the advantage ε.

Proof:

Init: $\mathcal{A}$ submits two challenge policies W_0^* and W_1^*, and the challenger $\mathcal{B}$ chooses a random bit $\rho \in \{1,0\}$.

Setup: To generate PK, the challenger picks $x^* \in_R Z_p$ at random sets $\alpha = ab + x^*$, then $Y = e(g,g)^{ab}$. The challenger $\mathcal{B}$ picks $\tau \in_R Z_p$ at random and computes $g_1 = g^\tau$. For any attributr $v_{i,j}$, $\mathcal{B}$ picks random elements $k_{i,j} \in_R Z_p$ where $i \in [1,n], j \in [1,n_i]$. If $v_{i,j} \in W_{\rho,i}^*$, then $a_{i,j} = k_{i,j}$, $T_{i,j} = g^{a_{i,j}}$; if $v_{i,j} \notin W_{\rho,i}^*$, then $a_{i,j} = \frac{b}{k_{i,j}}$, $T_{i,j} = g^{\frac{b}{k_{i,j}}}$. Finaly, the challenger sends the $PK = \langle e, G, G_T, g, g_1, Y, \{T_{i,j}\}_{i\in[1,n], j\in[1,n_i]} \rangle$ to $\mathcal{A}$.

Phase 1: Firstly, the adversary $\mathcal{A}$ with an attribute set $L = [L_1, L_2, \cdots, L_n]$ makes the secret key query. In this Here, the case $L \not\models W_0^* \wedge L \not\models W_1^*$ is only consided. Because, by our definition, if $L \models W_0^* \wedge L \models W_1^*$, then $\text{Game}_0 = \text{Game}_1$. Therefore, in this case, $\mathcal{B}$ terminates the game and takes a random guess. When $L \not\models W_0^* \wedge L \not\models W_1^*$, there must be $i^* \in \{1, \cdots, n\}$ such that $L_{i^*}(v_{i^*,j_{i^*}}) \notin W_{\rho,i^*}^*$. The challenger random selects $\beta, \alpha_k, \beta_k \in_R Z_p$ $(k \in [1,t])$.

The component D_0 and D^* are computed as $D_0 = g^{\alpha-\beta}$ and $D^* = h_L^\tau$. For $i = i^*$, the challenger random picks $\beta^* \in_R Z_p$ and sets $\beta = ab + \beta^* b$, then it computes $D_0 = g^{x^*-\beta^* b} = g^{\alpha-ab-\beta^* b}$ and $D_{i,j} = T_{i,j}^a \cdot g^{\beta^* k_{i,j}} = g^{(a+\beta^*)k_{i,j}} = g^{\frac{ab+b\beta^*}{a_{i,j}}}$; for $i \neq i^*$, $\mathcal{B}$ computes $D_0 = g^{\alpha-\beta}$ and $D_{i,j} = g^{\frac{\beta}{a_{i,j}}}$.

Challenge: After receiving two equal length messages M_0^* and M_1^* from $\mathcal{A}$, the challenger sets $C_0 = g^c$ and $\tilde{C} = M_\rho^* \cdot e(g,g)^{\alpha c}$ which implies $s = c$. In addition, the challenger picks randomly $r \in_R Z_p$ and computes $C_0^* = g^r$ and $C_1^* = e(g_1, h_{W_\rho^*})^r$. For $\forall i \in [1,n], i \neq i^*$, the challenger selects randomly $s_i \in_R Z_p$; for $i = i^*$, the challenger computes $s_{i^*} = c - \sum_{i=1, i\neq i^*}^n s_i$. The rest of ciphertexts is generated as follows.

- For $i = i^*$, the challenger computes $C_{i^*,j} = T_{i,j}^{s_i} = g^{\frac{bs_{i^*}}{k_{i,j}}}$.

- For $i \neq i^*$, the challenger computes $C_{i,j} = T_{i,j}^{s_i} = g^{a_{i,j}s_i}$.

Finally the challenger sends the challenge ciphertext $CT_{W_\rho^*} = \langle \tilde{C}, C_0, C_0^*, C_1^*, \{C_{i,j}\}_{v_{i,j} \in W} \rangle$ to the adversary $\mathcal{A}$.

Phase 2: It is similar to Phase 1.

Guess: $\mathcal{A}$ outputs a guess ρ' of ρ. Then the challenger $\mathcal{B}$ outputs 1 if $\rho' = \rho$ and 0 otherwise.

When $Z = e(g,g)^{abc}$, $\mathcal{A}$ is in Game_0; when Z is random, $\mathcal{A}$ is in Game_1. Therefore, challenger has advantage ε in the DBDH game.

6. Performance Comparison

Some comparisons between our scheme and some previous schemes will be given in this section, all of them are ciphertext-policy hiding CP-ABE schemes.

Some previous policy hiding CP-ABE schemes are compared with ours in storage cost, computational cost and security properties in **Table 1**, **2** and **3**, respectively. For convenience, let $\widetilde{U} = \{att_1, att_2, \cdots, att_n\}$ be a attributes set, and n is the number of attributes in universe. n_i is the number of att_i. Set $N = \prod_{i=1}^{n} n_i$ and let it expresse the total number of possible values of all attributes. $|PK|$, $|SK|$ and $|CT|$ are used to denote the length of publick parameter, secret key and ciphertext. Let the notation $k\text{TE}_\text{G}$ and $k\text{TE}_\text{GT}$ be k-times calculations over the group G and group G_T. TP means the time for one pairing.

From **Table 1**, **2** and **3**, it is easy to see that the proposed scheme is efficient in the size of public parameters, secret keys and ciphertexts. Although the efficiency of scheme in [11] looks just as good as ours, there is no testing phase in their scheme and it is constructed in groups of composite order.

In particular, the computation cost of our testing phase is just $\text{TP}+\text{TE}_\text{GT}$, which means that the user only needs to perform one pairing computation if his/her attribute list does not satisfy the ciphertext-policy. It is an efficient way to avoid excessive computations before decryption and improve the efficiency for the decryptor.

Table 1. Storage Cost of Different Schemes

Scheme	$\|PK\|$	$\|SK\|$	$\|CT\|$	Pairing	
				Testing Phase	Decryption Phase
Nishide et al. [10]	O(2N)	O(3n)	O(2n)	—	O(3n)
Lai et al. [11]	O(N)	O(n)	O(n)	—	O(n)
Phuong et al. [20]	O(8n)	O(4n)	O(4n)	—	O(n)
Ours	O(N)	O(n)	O(n)	O(1)	O(n)

Table 2. Computational Cost of Different Schemes

Scheme	Setup	KeyGen	Encryption	Decryption	
				Testing Phase	Decryption Phase
Nishide et al. [10]	$(2N)TE_G$ $+TP+TE_{GT}$	$(5n+1)TE_G$	$(2n+1)TE_G$ $+2TE_{GT}$	—	$(3n+1)TP$ $+(3n+3)TE_{GT}$
Lai et al. [11]	$(2N+1)TE_G$ $+TP+TE_{GT}$	$(n+1)TE_G$	$(2n+2)TE_G$ $+2TE_{GT}$	—	$(n+1)TP$ $+(n+2)TE_{GT}$
Phuong et al. [20]	$(8n+4)TE_G$ $+TP$	$(21n+1)TE_G$	$(20n+2)TE_G$ $+2TE_{GT}$	—	nTP $+(n+3)TE_{GT}$
Ours	$(2N+1)TE_G$ $+TP+ TE_{GT}$	$(2n+2)TE_G$	$TP+3TE_{GT}$ $+(n+2)TE_G$	$TP+TE_{GT}$	$(n+1)TP$ $+(n+2)TE_{GT}$

Table 3. Security Comparison among Different Schemes

Scheme	Order of Bilinear Groups	Security Model	Hardness	With Testing
Nishide et al. [10]	p	Selective	DBDH D-Linear	No
Lai et al. [11]	pqr	Full	Subgroup Assumption	No
Phuong et al. [20]	p	Selective	DBDH D-Linear	No
Ours	p	Selective	DBDH	Yes

7. Conclusion

This paper, firstly expounds that Li's scheme has disadvantages under the DDH-test attack, and their scheme cannot realize access policy hidden. Subsequently, a novel and improved scheme is proposed to resist the DDH-test attack. In this novel scheme, a testing phase is added before decryption. The cost of its testing phase is only one pairing. In addition, our scheme can be reduced to the standard assumptions.

References

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. of 24th annual international conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05)*, pp. 457-473, May 22-26, 2005. Article (CrossRef Link)

[2] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. of 13th ACM conference on Computer and Communications Security (CCS'06)*, pp. 89-98, October 30 - November 03, 2006. Article (CrossRef Link)
[3] N. Attrapadung, B. Libert and E.D. Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in *Proc. of 14th international conference on Practice and theory in public key cryptography conference on Public key cryptography (PKC'11)*, pp. 90-108, March 06-09, 2011. Article (CrossRef Link)
[4] C. Ge, W. Susilo, J. Wang, Z. Huang, L. Fang and Y. Ren, "A key-policy attribute-based proxy re-encryption without random oracles," *Computer Journal*, vol. 59, no. 7, pp. 970-982, July, 2016. Article (CrossRef Link)
[5] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. of 2007 IEEE Symposium on Security and Privacy (SP'07)*, pp. 321-334, May 20-23, 2007. Article (CrossRef Link)
[6] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *Proc. of 14th international conference on Practice and theory in public key cryptography conference on Public key cryptography (PKC'11)*, pp. 53-70, March 06-09, 2011. Article (CrossRef Link)
[7] L. Zhang and Y. Hu, "New constructions of hierarchical attribute-based encryption for fine-grained access control in cloud computing," *Ksii Transactions on Internet and Information Systems*, vol. 7, no. 5, pp. 1343-1356, May, 2013. Article (CrossRef Link)
[8] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," in *Proc. of 26th Annual International Cryptology Conference (CRYPTO'06)*, pp. 290-307, August 20-24, 2006. Article (CrossRef Link)
[9] L. Zhang, Y. Mu and Q. Wu, "Compact anonymous hierarchical identity-based encryption with constant size private keys," *Computer Journal*, vol. 59, no. 4, pp. 452–461, April, 2016. Article (CrossRef Link)
[10] T. Nishide, K. Yoneyama and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Proc. of 6th international conference on Applied cryptography and network security (ACNS'08)*, pp. 111-129, June 03-06, 2008. Article (CrossRef Link)
[11] J. Lai, R.H. Deng and Y. Li, "Fully secure cipertext-policy hiding CP-ABE," in *Proc. of 7th international conference on Information security practice and experience (ISPEC'11)*, pp. 24-39, May 30 - June 01, 2011. Article (CrossRef Link)
[12] Z. Wang and M. He, "CP-ABE with hidden policy from Waters efficient construction," *International Journal of Distributed Sensor Networks*, vol. 12, no. 1, pp. 1-8, January, 2016. Article (CrossRef Link)
[13] N. Doshi and D. Jinwala, "Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext," in *Proc. of 2011 international conference on Advanced Computing, Networking and Security (ADCONS'11)*, pp. 515-523, December 16-18, 2011. Article (CrossRef Link)
[14] C. Jin, X. Feng and Q. Shen, "Fully secure hidden ciphertext policy attribute-based encryption with short ciphertext size," in *Proc. of 6th International Conference on Communication and Network Security (ICCNS '16)*, pp. 91-98, November 26-29, 2016. Article (CrossRef Link)
[15] P. Xu, Q. Wu, W. Wang, W. Susilo, J. Domingo-Ferrer and H. Jin, "Generating searchable public-key ciphertexts with hidden structures for fast keyword search," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1993-2006, September, 2015. Article (CrossRef Link)
[16] S. Qiu, J. Liu, Y. Shi and R. Zhang, "Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack," *Science China Information Sciences*, vol. 60, no. 5: 052105, May, 2017. Article (CrossRef Link)
[17] J. Li, H. Wang, Y. Zhang and J. Shen, "Ciphertext-policy attribute-based encryption with hidden access policy and testing," *Ksii Transactions on Internet and Information Systems*, vol. 10, no. 7, pp. 3339-3352, July, 2016. Article (CrossRef Link)

[18] J. Lai, R.H. Deng and Y. Li, "Expressive CP-ABE with partially hidden access structures," in *Proc. of 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS '12)*, pp. 18-19, May 02-04, 2012. Article (CrossRef Link)
[19] X. Li, D. Gu, Y. Ren, N. Ding and K. Yuan, "Efficient ciphertext-policy attribute based encryption with hidden policy," in *Proc. of 5th international conference on Internet and Distributed Computing Systems (IDCS'12)*, pp. 146-159, November 21-23, 2012. Article (CrossRef Link)
[20] T.V.X. Phuong, G. Yang and W. Susilo, "Hidden ciphertext policy attribute-based encryption under standard assumptions," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 35-45, January, 2016. Article (CrossRef Link)
[21] M. Padhya and D. Jinwala, "A novel approach for searchable CP-ABE with hidden ciphertext-policy," in *Proc. of 10th International Conference on Information Systems Security (ICISS'14)*, pp. 167-184, December 16–20, 2014. Article (CrossRef Link)
[22] K. Emura, A. Miyaji, A. Nomura, K. Omote and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," *International Journal of Applied Cryptography*, vol. 2, no. 1, pp. 46-59, July 2010. Article (CrossRef Link)
[23] S. Liu, W. Fu, L. He, J, Zhou and M. Ma, "Distribution of primary additional errors in fractal encoding method," *Multimedia Tools & Applications*, vol. 76, no. 4, pp. 5787-5802, February, 2017. Article (CrossRef Link)
[24] M. Abdalla, D. Catalano and D. Fiore, "Verifiable random functions from identity-based key encapsulation," in *Proc. of 28th Annual International Conference on Advances in Cryptology: the Theory and Applications of Cryptographic Techniques (EUROCRYPT '09)*, pp. 554-571, April 26-30, 2009. Article (CrossRef Link)
[25] L. Zhang, Q. Wu, Y. Mu and J. Zhang, "Privacy-preserving and secure sharing of PHR in the cloud," *Journal of Medical Systems*, vol. 40, no. 12, pp. 1-13, December, 2016. Article (CrossRef Link)
[26] S. Liu, Z. Pan and X. Cheng, "A novel fast fractal image compression method based on distance clustering in high dimensional sphere surface," *Fractals-Complex Geometry Patterns and Scaling in Nature and Society*, vol. 25, no. 4, pp. 1740004, June, 2017. Article (CrossRef Link)
[27] K. Yang, Q. Han, H. Li, K. Zheng, Z. Su and X. Shen, "An efficient and fine-grained big data access control scheme with privacy-preserving policy," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 563-571, April, 2017. Article (CrossRef Link)
[28] H. Yin and L. Zhang, "Security analysis and improvement of an anonymous attribute-based proxy re-encryption," in *Proc. of 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS'17)*, pp. 344-352, December 12-15, 2017. Article (CrossRef Link)
[29] M. Hattori, T. Hirano, T. Ito, N. Matsuda, T. Mori, Y. Sakai and K. Ohta, "Ciphertext-policy delegatable hidden vector encryption and its application to searchable encryption in multi-user setting," in *Proc. of 13th IMA international conference on Cryptography and Coding (IMACC'11)*, pp. 190-209, December 12-15, 2011. Article (CrossRef Link)
[30] J. Li, W. Yao, Y. Zhang, H Qian and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 785-796, September-October, 2017. Article (CrossRef Link)
[31] S. Liu, Z. Pan and H Song, "Digital image watermarking method based on DCT and fractal encoding," *Iet Image Processing*, vol. 11, no. 10, pp. 815-821, October, 2017. Article (CrossRef Link)

Hongjian Yin received the master degree in applied mathematics from Xidian University, China, in 2018. He is currently working toward the Ph.D. degree in University of Science and Technology Beijing, China. His current research interests include information security and cryptography.

Leyou Zhang is a professor in the school of mathematics and statistics at Xidian University, Xi'an China. He received his Ph.D. from Xidian University in 2009. From Dec. 2013 to Dec. 2014, he is a research fellow in the school of computer science and software engineering at the University of Wollongong. His current research interests include network security, computer security, and cryptography.

Yilei Cui received the BS degree in mathematics in 2016 from the Henan Normal University, China. Currently, he is working toward the Ph.D. degree in Applied Mathematics in Xidian University, China. His current interests include applied cryptography and cloud security.