Ciphertext-Policy Attribute-Based Encryption with Hidden Access Policy and Testing

Jiguo Li[1], Haiping Wang[1], Yichen Zhang[1], Jian Shen[2]
[1]College of Computer and Information, Hohai University, Nanjing 211100, China
[2]School of Computer and Software, Nanjing University of Information Science and Technology 210044, Nanjing, China
[e-mail: ljg1688@163.com, 761248339@qq.com, zyc_718@163.com,s_shenjian@126.com]
*Corresponding author: Jiguo Li

Received January 26, 2016; revised May 21, 2016; accepted June 17, 2016; published July 31, 2016

Abstract

In ciphertext-policy attribute-based encryption (CP-ABE) scheme, a user's secret key is associated with a set of attributes, and the ciphertext is associated with an access policy. The user can decrypt the ciphertext if and only if the attribute set of his secret key satisfies the access policy specified in the ciphertext. In the present schemes, access policy is sent to the decryptor along with the ciphertext, which means that the privacy of the encryptor is revealed. In order to solve such problem, we propose a CP-ABE scheme with hidden access policy, which is able to preserve the privacy of the encryptor and decryptor. And what's more in the present schemes, the users need to do excessive calculation for decryption to check whether their attributes match the access policy specified in the ciphertext or not, which makes the users do useless computation if the attributes don't match the hidden access policy. In order to solve efficiency issue, our scheme adds a testing phase to avoid the unnecessary operation above before decryption. The computation cost for the testing phase is much less than the decryption computation so that the efficiency in our scheme is improved. Meanwhile, our new scheme is proved to be selectively secure against chosen-plaintext attack under DDH assumption.

Keywords: Attribute-based encryption, hidden access policy, DDH assumption, chosen-plaintext attack

This research was supported by the National Natural Science Foundation of China (61272542), the Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions, the Fundamental Research Funds for the Central Universities (2016B10114), Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, and the Project of Scientific Research Innovation for College Graduate Student of Jiangsu Province (KYZZ15_0151).

http://dx.doi.org/10.3837/tiis.2016.07.026 **ISSN : 1976-7277**

1. Introduction

To provide fine-grained access control over encrypted data, Sahai and Waters [1] introduced a novel public key primitive namely attribute-based encryption (ABE). The ABE mechanism enables public key-based one-to-many encryption. A lot of ABE schemes [2-12] have been presented. Goyal et al. [2] further clarified the concept of ABE. The ABE schemes are divided into two kinds. One is key-policy ABE (KP-ABE), where key is associated with access policy and ciphertext is associated with attribute set. The other is ciphertext-policy ABE (CP-ABE), which was first proposed by Bethencourt et al. [3]. This scheme [3] is proved secure under the generic group model. Cheung and Newport proposed a CP-ABE scheme [4] which was secure in the standard model. Goyal et al. [6] presented a bounded CP-ABE scheme with expressive access policy using access tree with threshold gates as its nodes. The scheme was proved to be secure under the DBDH assumption. Recently, Li et al. [13] proposed a flexible and fine-grained attribute-based data storage in cloud computing, which can withstand collusion attack performed by revoked users cooperating with existing users. To improve the computation cost, they outsource high computation load to cloud service providers without leaking data content and secret keys.

All the constructions mentioned above share one fatal defect that their access policies have to be shown in the ciphertexts because the decryptors need to do their decryption with them. To protect user's privacy in an access policy, Kapadia et al. proposed a CP-ABE scheme with hidden ciphertext policies [14]. However, the scheme [14] cannot resist collusion attack. Later, Nishide et al. [15] presented two improved schemes with partially hidden ciphertext policies, which were proved secure under DBDH assumption and D-Linear assumption. Li et al. [16] presented an anonymous CP-ABE scheme which can prevent the problem of illegal key sharing among users. Müller and Katzenbeisser [17] provided a cryptographic access control with hidden access policy, which is selectively secure. Lai et al. [18, 19] proposed a fully secure CP-ABE with partially hidden access policy. Qian et al. [20,21] presented a privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure, which is applied in personal health record. Xhafa et al. [22] proposed a multi-authority anonymous ciphertext-policy ABE scheme with user accountability, which can be used to design an attribute-based PHR sharing system. Sabitha et al. [23] proposed a scheme which was able to ensure security, integrity, privacy of preserved fine-grained access control and prevent data mining attacks on shared data. However, all these extensional CP-ABE schemes realize the attribute matching detection only after decryption which is not practical due to large computation cost. As the amount of encrypted files stored in cloud are becoming very huge, which will hinder efficient query processing, keyword search and data auditing [24-27] have become an important and challenge issue in cloud storage. To solve above problem, Li et al. [28, 29] presented two attribute-based encryption schemes with keyword search function for cloud storage. In order to protect privacy, Padhya et al. [30] presented a searchable CP-ABE scheme with hidden ciphertext policy. In order to prevent key abuse problem, Liu et al. [31] provided a blackbox traceable CP-ABE scheme. Ning et al. [32] proposed a white-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes.

1.1 Our Motivations and Contributions

In CP-ABE scheme, the user is able to decrypt the ciphertext only if the attributes defined in the secret key satisfy the access policy specified in the ciphertext. The access policy should be sent to the user along with the corresponding ciphertext. However, the access policy may contain some sensitive information. Some CP-ABE schemes with hidden access policy were presented to protect the privacy for users. However, in the present CP-ABE schemes with hidden access policy, the users need to do excessive calculation for decryption whether their attributes match the access policy specified in the ciphertext or not, which makes the users do useless computation if the attributes don't match the hidden access policy. We present a CP-ABE scheme with hidden access policy and testing. Our scheme adds a test about whether the attribute lists matches the hidden attributes policy in ciphertexts or not before the decryption. The computation amount for the test is much less than the decryption. What's more, many present CP-ABE with hidden access policy can only use simple access policy such as one to one, which means that the attribute list of the decryptor must be as the same as the access policy hidden in the ciphertexts. Our scheme is based on AND-gates on multi-valued attributes with wildcards. We prove the security of our scheme under CDH assumption and D-Linear assumption.

1.2 Organization

We organize the rest of the paper as follows. In section 2, we review some preliminary knowledges used in our paper. In Section 3, we present a new CP-ABE scheme with hidden access policy and testing. We prove the security of our scheme in Section 4. In Section 5, we give some efficiency comparison with the existing schemes. Finally, we conclude the paper in Section 6.

2. Preliminaries

2.1 Bilinear maps

Let G and G_T be multiplicative cyclic groups of prime order p. g is a generator of G. Let $e: G \times G \rightarrow G_T$ be a bilinear map. The bilinear map satisfies following properties:

(1) Bilinearity: For all $u, v \in G$, and $a, b \in Z_p$ which is selected randomly, we have $e(u^a, v^b) = e(u, v)^{ab}$.

(2) Non-degeneracy: There exists $u, v \in G$ such that $e(u, v) \neq 1$.

(3) Computability: For all $u, v \in G$, there is an efficient algorithm to compute $e(u, v)$.

2.2 Complexity assumption

We state the complexity assumption below to be used in the paper.

Difinition 1 (The Decisional Diffie-Hellman Assumption[33]**).** Let $z_1, z_2 \in_R Z_p^*$, $Z \in G$ be chosen at random and $g \in G$ be a generator. The DDH assumption is that no probabilistic polynomial-time algorithm can distinguish the tuple $[g, g^{z_1}, g^{z_2}, g^{z_1 z_2}]$ from the tuple $[g, g^{z_1}, g^{z_2}, Z]$ with non-negligible advantage.

2.3 Access policy

In our context, the user's authority is expressed by the attributes. We use AND-gates on multi-valued attributes with wildcards as follows:

Definition 2 (Access policy[34]). Let $U=\{att_1,\ldots,att_n\}$ be a set of attributes. For $att_i \in U$, $S_i=\{v_{i,1},v_{i,2},\ldots,v_{i,n_i}\}$ is a set of possible values, where n_i is the number of possible values for att_i. $L=[L_1,L_2,\ldots,L_n]$ is an attribute list where $L_i=v_{i,t_i}\in S_i$ and $t_i\in\{1,2,\ldots,n_i\}$ for a user. $W=[W_1,W_2,\ldots,W_n]$ is an access policy where $W_i\subset S_i$. The notation that an attribute list L satisfies an access policy W means that $L_i\in W_i(\forall i=1,2,\ldots,n)$. $W_i=S_i$ means wildcard that plays the role of "don't care" value.

2.4 Definition of CP-ABE with Hidden Access Policy

There are three entities: a trusted authority (TA), an encryptor and a decryptor in CP-ABE scheme with hidden access policy. TA is responsible for the issue of attribute associated with private key of decryptors. The encryptor appoints the access policy that controls which ciphertexts a decryptor is able to decrypt. In order to represent simply, we use a function F with two inputs to describe whether the attribute list L satisfies access policy W. $F(L,W)=1$ means that the attribute list L satisfies access policy W and $F(L,W)=0$ means the opposite.

Our CP-ABE scheme with hidden access policy and testing consists of four algorithms based on [14], namely, *Setup*, *KeyGen*, *Encryption*, and *Decryption*, which are defined as follows:

- $Setup(1^\lambda)$: It is run by TA. It takes as input implicit security parameter 1^λ, generates a public parameter PK and a master secret key MSK.
- $KeyGen(MSK,PK,L)$: It is run by TA. It takes as input public parameter PK and master secret key MSK and the attribute set L for user, generates the secret key sk_L.
- $Encrypt(PK,M,W)$: It is run by encryptor. The encryption algorithm takes as input the message M, public parameter PK and access policy W over the universe of attributes. It outputs ciphertext CT_W.
- $Decrypt(PK,CT_W,sk_L)$: It is run by decryptor. It takes as input the public parameter PK, the ciphertext CT_W embedded in access policy W, and the secret key sk_L containing attribute set L.
  Testing Phase: If $F(L,W)=0$, it outputs an error symbol $\perp$. Otherwise, it runs the following *Decryption Phase*.
  Decryption Phase: It outputs M.

2.5 Security Model

The goals of an adversary $\mathcal{A}$ in an CP-ABE system with hidden access policy include extracting information of a plaintext from the ciphertext and distinguishing hidden access policy in ciphertexts. We call it IND-sCP-CPA. So the security model is described as a security game between a challenger $\mathcal{S}$ and an adversary $\mathcal{A}$ based on [30]. The game proceeds as follows:

Initial. The adversary $\mathcal{A}$ commits to the challenge ciphertext policies W_0^*, W_1^*. The challenger $\mathcal{S}$ chooses a sufficiently large security parameter 1^λ, and runs $Setup(1^\lambda)$ algorithm to get a master secret key MSK and public key PK. The challenger $\mathcal{S}$ reserves MSK and gives PK to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ submits the attribute list L for a *KeyGen* query. If $(F(L,W_0^*)=0 \wedge F(L,W_1^*)=0)$, the challenger $\mathcal{S}$ gives the adversary the secret key sk_L.

Challenge. $\mathcal{A}$ submits two equal length messages M_0^*, M_1^* to the challenger on which it wishes to challenge with respect to W_0^*, W_1^*. The challenger $\mathcal{S}$ flips a random coin $b \in \{0,1\}$ and passes the ciphertext $CT = Encrypt\left(PK,\ M_b^*,\ W_b^*\right)$ to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ continues to issue queries as *Phase* 1, with the same restriction that $(F(L,W_0^*)=0 \wedge F(L,W_1^*)=0)$.

Guess. Finally, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$ of b.

The advantage of an adversary in this game is defined as $|\Pr[b'=b]-\frac{1}{2}|$.

Definition 3. A hidden access policy CP-ABE scheme is secure against selectively chosen-plaintext attack if all polynomial time adversaries have at most a negligible advantage in the above game.

3. Construction for CP-ABE Scheme with Hidden Access Policy and Testing

In this section, we present the concrete CP-ABE scheme with hidden access policy and testing. Let $U=\{att_1,\ldots,att_n\}$ be a set of attributes. For $att_i \in U$, $S_i=\{v_{i,1},v_{i,2},\ldots,v_{i,n_i}\}$ is a set of possible values, where n_i is the number of possible values for att_i. $L=[L_1,L_2,\ldots,L_n]$ is an attribute list for a user, where $L_i \in S_i$. $W=[W_1,W_2,\ldots,W_n]$ is an access policy, where $W_i \subset S_i$.

$Setup(1^\lambda)$: The algorithm takes as input a security parameter 1^λ. TA obtains a bilinear group (p,G,G_T,e), where G and G_T are multiplicative cyclic groups of prime order p and $e: G\times G \to G_T$ is the bilinear map. TA chooses $\alpha,\beta \in_R Z_p$ and $a_{i,t} \in_R Z_p$ $(i\in[1,n], t\in[1,n_i])$. TA computes $Y=e(g,g)^\alpha$, $X=g^\beta$, and $T_{i,t}=g^{a_{i,t}}$ $(i\in[1,n], t\in[1,n_i])$. $PK=(e,G,G_T,g,Y,X,\{T_{i,t}\}_{i\in[1,n],t\in[1,n_i]})$ are published as the public parameters. The master secret key is $MSK=(\alpha,\beta,\{a_{i,t}\}_{i\in[1,n],t\in[1,n_i]})$.

$KeyGen(MSK,PK,L)$: The key generation algorithm takes as input the master secret key MSK, public key PK, and a set of attributes $L=[L_1,L_2,\ldots,L_n]$. The algorithm performs as follows:

TA chooses $u,r^* \in_R Z_p$ and $\lambda_i \in_R Z_p$ for the user, where $1\le i\le n$. TA computes

$D_0 = g^{\alpha+\beta u}$, $D_{i,1} = g^{u+a_{i,t}\lambda_i}$, $D_{i,2} = X^{\lambda_i}$ where $L_i = v_{i,t}$ for decryption. Furthermore, TA computes $D_i^* = T_{i,t}^{r^*}, i \in [1,n]$, where $L_i = v_{i,t}$, $D_0^* = g^{r^*}$ is used to test whether the user's attribute list L satisfies the access policy W. The secret key $sk_L =< D_0, \{D_{i,1}, D_{i,2}, D_i^*\}_{1\le i\le n}, D_0^* >$ is delivered to the user.

$Encrypt(PK, M, W)$: The encryption algorithm takes as input the public parameters PK, a message $M \in G_T$ and access policy $W = [W_1, W_2, \ldots, W_n]$. The encryptor randomly chooses $s, s^* \in Z_p$, and 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 $s = \sum_{i=1}^{n} s_i$ and computes $C_{i,1} = X^{s_i}$, where $1 \le i \le n$. If $v_{i,t} \in W_i$, the encryptor computes $[C_{i,t,2}, C_{i,t}^*] = [T_{i,t}^{s_i}, T_{i,t}^{s^*}]$, else $v_{i,t} \notin W_i$, $[C_{i,t,2}, C_{i,t}^*]$ are random elements in G. $CT_W =< \tilde{C}, C_0, C_0^*, \{\{C_{i,1}\}, \{C_{i,t,2}, C_{i,t}^*\}_{t\in[1,n_i]}\}_{i\in[1,n]} >$ is the ciphertext for M with respect to W.

$Decrypt(PK, CT_W, sk_L)$: Taking public key PK, ciphertext CT_W, and secret key sk_L as input, the decryptor proceeds as follows:

Testing Phase: The user checks whether $F(L,W) = 1$. $F(L,W) = 1$ if and only if $\frac{e(C_0^*, \prod_{i=1}^{n} D_i^*)}{e(D_0^*, \prod_{i=1}^{n} C_{i,t}^*)} = 1$ holds, where $L_i = v_{i,t}$. If $F(L,W) = 0$, it returns $\perp$ and terminates. If $F(L,W) = 1$, it enters into the *Decryption Phase*.

Decryption Phase: The user decrypts the ciphertext to get M by the following eqution.

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

If a user's attribute list L satisfies the access policy W, the correctness of the proposed scheme can be verified as follows:

$$\frac{e(C_0^*, \prod_{i=1}^{n} D_i^*)}{e(D_0^*, \prod_{i=1}^{n} C_{i,t}^*)} = \frac{e(g^{s^*}, \prod_{i=1}^{n} T_{i,t}^{r^*})}{e(g^{r^*}, \prod_{i=1}^{n} T_{i,t}^{s^*})} = \frac{e(g^{s^*}, \prod_{i=1}^{n} g^{a_{i,t} r^*})}{e(g^{r^*}, \prod_{i=1}^{n} g^{a_{i,t} s^*})} = \frac{e(g,g)^{s^* r^* \sum_{i=1}^{n} a_{i,t}}}{e(g,g)^{s^* r^* \sum_{i=1}^{n} a_{i,t}}} = 1$$

On the base of that, the user can decrypt the ciphertext:

$$\frac{\tilde{C}\prod_{i=1}^{n} e(C_{i,1}, D_{i,1})}{e(C_0, D_0)\prod_{i=1}^{n} e(C_{i,t,2}, D_{i,2})} = \frac{MY^s \prod_{i=1}^{n} e(X^{s_i}, g^{u+a_{i,t}\lambda_i})}{e(g^s, g^{\alpha+\beta u})\prod_{i=1}^{n} e(T_{i,t}^{s_i}, X^{\lambda_i})}$$

$$= \frac{Me(g,g)^{\alpha s}\prod_{i=1}^{n} e(g^{\beta s_i}, g^{u+a_{i,t}\lambda_i})}{e(g^s, g^{\alpha+\beta u})\prod_{i=1}^{n} e(g^{a_{i,t}s_i}, g^{\beta\lambda_i})} = \frac{M\prod_{i=1}^{n} e(g,g)^{\beta u s_i}}{e(g,g)^{\beta u s}}$$

$$= \frac{Me(g,g)^{\beta u\sum_{i=1}^{n} s_i}}{e(g,g)^{\beta u s}} = M$$

4. Security Proof

Our CP-ABE scheme with hidden access policy is proved selectively secure under the assumption. As for selectively secure, the adversary should commit to the challenge access policies W_0^*, W_1^* at the beginning of the game.

A sequence of hybrid games are used to argue that the adversary cannot win the security game denoted by *G* with non-negligible probability. Firstly, the original game *G* is modified into a game G_0, which is the same as *G* except how the challenge ciphertext is generated. In the game G_0, the part of the challenge ciphtertext $\tilde{C}$ is randomly selected from G_T regardless of the random coin *b* when the attribute list *L* satisfies that $F(L,W_0)=0 \wedge F(L,W_1)=0$. The adversary can get the rest of the ciphertext normally. As for $F(L,W_0)=1 \wedge F(L,W_1)=1$, G_0 is the same as *G* that the challenge ciphertext in G_0 is generated correctly. We use assumption to prove that game *G* and game G_0 is indistinguishable.

Theorem 1. If there exists an adversary $\mathcal{A}$ that can distinguish game *G* and game G_0 with the advantage ε, we can construct an algorithm $\mathcal{B}$ that can solve the DDH assumption with the advantage ε.

Proof: Given a DDH paradigm $(g, g^{z_1}, g^{z_2}, \mathrm{Z})$, the simulator $\mathcal{B}$ creates the following simulation.

Init: The simulator $\mathcal{B}$ runs $\mathcal{A}$. $\mathcal{A}$ gives $\mathcal{B}$ two challenge chiphertext policies $W_0^* = \left[W_{0,1}, \ldots, W_{0,n}\right]$, $W_1^* = \left[W_{1,1}, \ldots, W_{1,n}\right]$. Then $\mathcal{B}$ flips a random coin $b \in \{0, 1\}$.

Setup: $\mathcal{B}$ sets $Y = e(g, g)^{\alpha} = e(g, g^{z_1}) = e(g, g)^{z_1}$. This implies $\alpha = z_1$. $\mathcal{B}$ chooses $\beta \in_R Z_p$. For $\forall 1 \le i \le n$, $\mathcal{B}$ generates $\{T_{i,t}\}_{1\le t\le n_i}$ such that $T_{i,t} = g^{a_{i,t}}$, if $v_{i,t} \in W_{b,i}$, $T_{i,t} = g^{z_1 a_{i,t}}$, if $v_{i,t} \notin W_{b,i}$ with $\{a_{i,t} \in_R Z_p\}_{1\le t\le n_i}$. $\mathcal{B}$ publishes public parameters $PK = (e, G, G_T, g, Y, \{T_{i,t}\}_{i\in[1,n], t\in[1,n_i]})$ as in the real scheme.

Phase1: $\mathcal{A}$ submits an attribute list $L=[L_1,L_2,\ldots,L_n]$ in a secret key query. Considering $(F(L,W_0^*)=0\wedge F(L,W_1^*)=0)$, there must be $j\in\{1,\ldots,n\}$ such that $L_j(v_{j,t_j})\notin W_{b,j}$. $\mathcal{B}$ picks up $u,r^*\in_R Z_p$. For $1\le i\le n$, $\lambda_i\in_R Z_p$.

The component D_0 of the secret key sk_L can be computed as $D_0=g^{\alpha+\beta u}=g^{z_1+\beta u}$.

For $i=j$, $\mathcal{B}$ computes the components $[D_{j,1},D_j^*]$ as $D_{j,1}=T_{j,t}^{\lambda_j}g^u=(g^{z_1})^{a_{j,t}\lambda_j}g^u$, $D_j^*=T_{j,t}^{r^*}=(g^{z_1})^{a_{j,t}r^*}$.

For $i\ne j$, $\mathcal{B}$ computes the components $[D_{i,1},D_i^*]$ as $D_{i,1}=T_{i,t}^{\lambda_i}g^u=g^{a_{i,t}\lambda_i}g^u$, $D_i^*=T_{\mathrm{i},t}^{r^*}=g^{a_{i,t}r^*}$.

Challenge: $\mathcal{A}$ submits messages M_0^*, M_1^* to the challenger on which it wishes to challenge with respect to W_0^*, W_1^*. $\mathcal{B}$ sets $C_0=g^{z_2}$, $C_0^*=g^{s^*}$ and $\tilde{C}=M_b^*\cdot Y^s=M_b^*\cdot e(g,g)^{\alpha s}=M_b^*\cdot e(g,g)^{z_1z_2}$ which implies $s=z_2$. For $\forall 1\le i\le n, i\ne j$, $\mathcal{B}$ chooses $s_i\in_R Z_p$ and for $i=j$, $\mathcal{B}$ computes $s_j=z_2-\sum_{i=1,i\ne j}^{n}s_i$.

For $i=j$, the components $[C_{j,1},C_{j,t,2},C_{j,t}{}^*]$ of the ciphertext is computed as

$$C_{j,1}=g^{\beta s_j}=g^{\beta(z_1-\sum_{i=1,i\ne j}^{n}s_i)}=(g^{z_1})^{\beta}/g^{\beta\sum_{i=1,i\ne j}^{n}s_i},\ [C_{j,t,2},C_{j,t}^*]\in_R G^2.$$

For $i\ne j$, the components $[C_{i,1},C_{i,t,2},C_{i,t}{}^*]$ of the ciphertext is computed as $C_{i,1}=g^{\beta s_i}$, $C_{i,t,2}=T_{i,t}^{s_i}=g^{a_{i,t}s_i}$, $C_{i,t}{}^*=T_{i,t}^{s^*}=g^{a_{i,t}s^*}$.

Phase2: *Phase* 1 is repeated.

Guess: From the above considerations, the adversary can decide a guess b' of b when $Z=e(g,g)^{z_1z_2}$, $\mathcal{A}$ is in game *G*. Else $\mathcal{A}$ only makes a random guess because $\mathcal{A}$ is in game G_0 when Z is random. If $b'=b$, $\mathcal{B}$ outputs $\beta=1$ and otherwise outputs $\beta=0$. Therefore $\mathcal{B}$ can break the DDH problem with the probability ε.

Secondly, G_0 is modified by changing how to generate the ciphertext components $\{C_{i,1}\}_{i\in[1,n]}$ and define a sequence of games as follows.

If $v_{i,t}$ is $(v_{i,t}\in W_{0,i}\wedge v_{i,t}\in W_{1,i})$ or $(v_{i,t}\notin W_{0,i}\wedge v_{i,t}\notin W_{1,i})$, the ciphertext component $\{C_{i,1}\}_{i\in[1,n]}$ is obtained as in the real scheme through the sequence of all the games. But for $v_{i,t}$ such that $(v_{i,t}\in W_{0,i}\wedge v_{i,t}\notin W_{1,i})$ or $(v_{i,t}\notin W_{0,i}\wedge v_{i,t}\in W_{1,i})$, the ciphertext component $\{C_{i,1}\}_{i\in[1,n]}$ which is obtained normally in the game G_{l-1} is replaced by the random values in the new modified game G_l ignoring the random coin *b*. To be specific, we won't make a new game by replacing the ciphertext component $\{C_{i,1}\}_{i\in[1,n]}$ until there is no $v_{i,t}$ such that $(v_{i,t}\in W_{0,i}\wedge v_{i,t}\notin W_{1,i})$ or $(v_{i,t}\notin W_{0,i}\wedge v_{i,t}\in W_{1,i})$. We use DDH assumption to prove that the game G_l and G_{l-1} is indistinguishable.

Lastly, we can get the obvious conclusion that in the last game of the game sequence, the advantage of the adversary is 0 because the adversary is given a ciphertext chosen from the

same access policy regardless of the random coin *b*.

Theorem 2. If there exists an adversary $\mathcal{A}$ that can distinguish game G_{l-1} and game G_l with the advantage ε, we can construct an algorithm $\mathcal{B}$ that can solve the DDH assumption with the advantage ε.

Proof: Given a DDH paradigm $[g, g^{z_1}, g^{z_2}, Z]$, where Z is either $g^{z_1 z_2}$ or random with equal probability, the simulator $\mathcal{B}$ creates the following simulation.

As mentioned above, the ciphertext components $\{C_{i,1}\}_{i\in[1,n]}$ is generated as in the real scheme in game G_{l-1}. But in game G_l, the components are random regardless of the random coin b.

Init: The simulator $\mathcal{B}$ runs $\mathcal{A}$. $\mathcal{A}$ gives $\mathcal{B}$ two challenge chiphertext policies $W_0^* = \left[W_{0,1}, \ldots, W_{0,n}\right]$, $W_1^* = \left[W_{1,1}, \ldots, W_{1,n}\right]$. Then $\mathcal{B}$ flips a random coin $b \in \{0, 1\}$. When $v_{i_l,t_l} \in W_{1,i} \wedge v_{i_l,t_l} \in W_{0,i}$ or $v_{i_l,t_l} \notin W_{1,i} \wedge v_{i_l,t_l} \notin W_{0,i}$, game G_{l-1} is the same as game G_l according to the game definition. We can only need to consider the case when $v_{i_l,t_l} \in W_{1,i} \wedge v_{i_l,t_l} \notin W_{0,i}$ or $v_{i_l,t_l} \notin W_{1,i} \wedge v_{i_l,t_l} \in W_{0,i}$.

Setup: $\mathcal{B}$ sets $Y = e(g, g)^{\alpha}$ and $X = g^{\beta} = g^{z_1}$, which implies $\beta = z_1$. For $\forall 1 \le i \le n$, $\mathcal{B}$ generates $\{T_{i,t}\}_{1\le t\le n_i}$ such that $T_{i,t} = g^{a_{i,t}}$, if $v_{i,t} \in W_{b,i}$, $T_{i,t} = g^{z_1 a_{i,t}}$, if $v_{i,t} \notin W_{b,i}$ with $\{a_{i,t} \in_R Z_p\}_{1\le t\le n_i}$. $\mathcal{B}$ publishes public parameters $PK = (e, G, G_T, g, Y, \{T_{i,t}\}_{i\in[1,n],t\in[1,n_i]})$ as in the real scheme.

Phase1: $\mathcal{A}$ submits an attribute list $L = [L_1, L_2, \ldots, L_n]$ in a secret key query.

$\mathcal{B}$ chooses $u, r^* \in_R Z_p$ and $\lambda_i \in_R Z_p$ for the user, where $1 \le i \le n$. $\mathcal{B}$ computes the secret key components as follows $D_{i,1} = g^{u + a_{i,t}\lambda_i}$, $D_i^* = T_{i,t}^{r^*}$, $D_{i,2} = X^{\lambda_i} = (g^{z_1})^{\lambda_i}$ where $L_i = v_{i,t}$ for decryption. And then $D_0 = g^{\alpha+\beta u} = g^{\alpha + z_1 u} = (g^{z_1})^u g^{\alpha}$, $D_0^* = g^{r^*}$.

Challenge: $\mathcal{A}$ submits messages M_0^*, M_1^* to the challenger on which it wishes to challenge with respect to W_0^*, W_1^*. $\mathcal{B}$ sets $C_0 = g^{z_2}$ which implies $s = z_2$, and $\tilde{C} = M_b^* \cdot Y^s = M_b^* \cdot e(g,g)^{\alpha z_2} = M_b^* \cdot e(g, g^{z_2})^{\alpha}$, $C_0^* = g^{s^*}$ where $s^* \in_R Z_p$. For $1 \le i \le n, i \ne l$, $s_i \in_R Z_p$. For $i = l$, $s_l = z_2 - \sum_{i=1, i\ne l}^{n} s_i$.

For $i = l$, the components $[C_{l,1}, C_{l,t,2}]$ of the ciphertext is computed as $C_{l,1} = g^{\beta s_l} = g^{z_1(z_2 - \sum_{i=1,i\ne l}^{n} s_i)}$

$= (g^{z_1 z_2}) / g^{z_1 \sum_{i=1,i\ne l}^{n} s_i} = Z / g^{z_1 \sum_{i=1,i\ne l}^{n} s_i}$, $C_{l,t,2} = T_{l,t}^{s_l} = g^{a_{l,t}(z_1 - \sum_{i=1,i\ne l}^{n} s_i)} = (g^{z_1})^{a_{l,t}} / g^{a_{l,t}\sum_{i=1,i\ne l}^{n} s_i}$.

If $Z = g^{z_1 z_2}$, the components are well-formed and $\mathcal{A}$ is in game G_{l-1}. And if Z is random, $\mathcal{A}$ is in game G_l.

Phase2: Phase1 is repeated.

Guess: From the above considerations, the adversary can decide a guess b' of b when $Z = g^{z_1 z_2}$, $\mathcal{A}$ is in game G_{l-1}. Else $\mathcal{A}$ only makes a random guess when Z is random, $\mathcal{A}$ is in game G_l. Therefore $\mathcal{B}$ can break the DDH problem with the probability ε.

5. Performance Comparison

In this section, we compare our work with previous works which are all CP-ABE schemes with hidden access policy to expound our scheme's advantages. For convenience, PK, MSK, SK, CT are the shortened form for the size of the public key, the master secret key, the secret key, and the ciphertext length excluding the access policy respectively. What's more, $Enc.$ and $Dec.$ are the shortened form for the computational time of encryption and decryption respectively. $|G|$, $|G_T|$, $|Z_P|$ denote the bit-length of the elements belongs to G, G_T, Z_P. Let $U=\{att_1,...,att_n\}$ be the attribute universe. n is the number of all attributes in universe. n_i is the number of att_i. $N=\sum_{i=1}^{n} n_i$ expresses the total number of possible values of all attributes. Let the notation kG and kG_T be k-times calculations over the group G and group G_T, respectively. C_e means the time for one pairing.

Table 1. Size of each value

	PK	***MK***	***SK***	***CT***
NYO 08[15]	$(2N+1)\|G\|+\|G_T\|$	$(2N+1)\|Z_p\|$	$3(N+1)\|G\|$	$(2N+1)\|G\|+\|G_T\|$
Lai 11[19]	$(N+1)\|G\|+\|G_T\|$	$\|G\|+(N+1)\|Z_p\|$	$(N+1)\|G\|$	$(N+1)\|G\|+\|G_T\|$
Müller 12[17]	$(N+2)\|G\|+2\|G_T\|$	$(N+4)\|Z_p\|$	$(2n+2)\|G\|$	$(N+n)\|G\|+2\|G_T\|$
Our scheme	$(N+1)\|G\|+\|G_T\|$	$(N+2)\|Z_p\|$	$(2N+1)\|G\|$	$(N+n)\|\mathbb{G}\|+\|\mathbb{G}_T\|$

Table 2. Computational Cost of Encryption and Decryption

	Encryption	***Decryption***
NYO 08[15]	$(2N+1)G+G_T$	$(3n+1)C_e+(3n+1)G_T$
Lai 11[19]	$(2N+2)G+G_T$	$(n+1)C_e+(n+3)G_T$
Müller 12[17]	$(N+n)G+2G_T$	$(3n+2)C_e+(3n+2)G_T$
Our scheme	$(N+n)G+G_T$	$(2n+1)C_e+(2n+1)G_T$

Table 3. Security Properties of CP-ABE

	Order of Bilinear Groups	***Security Model***	***Assumption***	***With testing***
NYO 08[15]	$N=p$	*Selective*	*DBDH, D-Linear*	*No*
Lai 11[19]	$N=pqr$	*Fully*	*Non-standard*	*No*
Müller 12[17]	$N=p$	*Selective*	*DBDH*	*No*
Our scheme	$N=p$	*Selective*	*DDH*	*Yes*

Table 4. Expressiveness of Policy

NYO 08[15]	*AND-gates on multi-valued attributes with wildcards*
Lai 11[19]	*AND-gates on multi-valued attributes*
Müller 12[17]	*monotonic syntax tree*
Our scheme	*AND-gates on multi-valued attributes with wildcards*

Compared with the other schemes, our construction shows many merits (see **Table 1**- **Table 4**). Firstly, for the size of parameters, the size of the PK and MSK in our schem is the shortest ones, and the size of SK and CT of our scheme are relatively very short, so our scheme's communication cost is small. Secondly, our sheme's computation time of encryption is smaller than Müller's [17], but the efficiency of decryption in our scheme is high. Thirdly, our scheme is selectively secure with testing phase which can avoid excessive computaions before decryption and improve the efficiency for the decryptor. On the whole, our scheme has relatively lower communication and computaion cost than exsiting CP-ABE schemes.

As you can see from the tables above, the decryption cost of CP-ABE scheme with hidden access policy is always huge. If there is no testing, the decryptor may spend much time on pairing computaion because one pairing costs a lot of time. But in our scheme, we add a test before decryption. The decryptor then does decryption if she passes the testing. The time of one testing is $2C_e + 2nG$, which reduce the time for pairing computaion to a large extent. And our scheme shows a little advantage especially for public key and computational time of decryption.

6. Conclusion

In this paper, we propose a new CP-ABE scheme with hidden access policy. We prove the scheme is selectively secure in standard model. Security in our scheme is reduced to DDH assumption. The access policy is based on AND-gates on multi-valued attributes with wildcards, which is very expressive. Moreover, we add a testing phase before decryption. The cost of one test is small so it is effective.

References

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. of EUROCRYPT 2005*, LNCS 3494, pp. 457-473, 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 the 13th ACM Conf. on Computer and Communications Security*, pp. 89-98, 2006. Article (CrossRef Link)

[3] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. of IEEE Symposium on Security and Privacy*, pp. 321-334, May 20-23, 2007. Article (CrossRef Link)

[4] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. of the 14th ACM Conf. on Computer and Communications Security*, pp. 456-465, 2007. Article (CrossRef Link)

[5] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," *Theory of Cryptography*, LNCS 4392, pp. 535-554, 2007. Article (CrossRef Link)

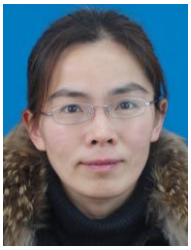
[6] V. Goyal, A. Jain, O. Pandey and A. Sahai, "Bounded ciphertext policy attribute based encryption," *Automata, Languages and Programming*, LNCS 5126, pp. 579-591, 2008. Article (CrossRef Link)

[7] A. Lewko, T. Okamoto, K. Takashima and B. Water, "Fully secure functional encryption: attributed-based encryption and (hierarchical) inner product encryption," *EUROCRYPT 2010*, LNCS 6110, pp. 62-91, 2010. Article (CrossRef Link)
[8] T. Okamato and K. Takashima, "Fully secure function encryption with general relations from the decisional linear assumption," in *Proc. of CRYPTO 2010*, LNCS 6223, pp. 191-208, 2010. Article (CrossRef Link)
[9] R. Ostrovsky, A. Sahai and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. of the 14th ACM Conf. on Computer and Communications Security*, pp. 195-203, 2007. Article (CrossRef Link)
[10] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," *PKC 2011*, LNCS 6571, pp. 53-70, 2011. Article (CrossRef Link)
[11] S. Yamada, N. Attrapadung, G. Hanaoka and N. Kunihiro, "Generic constructions for chosen-ciphertext secure attribute based encryption," *PKC 2011*, LNCS 6571, pp. 71-89, 2011. Article (CrossRef Link)
[12] S. Yu, K. Ren and W. Lou, "Attribute-based content distribution with hidden policy," in *Proc. of NPSEC 2008*, pp. 39-44, October 19-19, 2008. Article (CrossRef Link)
[13] J. G. Li, W. Yao, Y. C. Zhang, H. L. Qian, and J. G. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing*, DOI: 10.1109/TSC.2016.2520932, 2016. Article (CrossRef Link)
[14] A. Kapadia, P. P. Tsang and S. W. Smith, "Attribute-based publishing with hidden credentials and hidden policies," in *Proc. of NDSS 2007*, vol. 7, pp. 179-192, 2007. Article (CrossRef Link)
[15] T. Nishide, K. Yoneyama and K. Ohata, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Proc. of ACNS 2008*, LNCS 5037, pp. 111-129, 2008. Article (CrossRef Link)
[16] J. Li, K. Ren, B. Zhu and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in *Proc. of ISC 2009*, LNCS 5735, pp. 347-362, 2009. Article (CrossRef Link)
[17] S. Müller and S. Katzenbeisser, "Hiding the policy in cryptographic access control," *Security and Trust Management*, LNCS 7170, pp. 90-105, 2012. Article (CrossRef Link)
[18] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," in *Proc. of the 7th ACM Conf. on Information, Computer and Communications Security*, pp. 18-19, 2012. Article (CrossRef Link)
[19] J. Lai, R. H. Deng and Y. Li, "Fully secure ciphertext-policy hiding CP-ABE," in *Proc. of ISPEC 2011*, LNCS 6672, pp. 24-39, 2011. Article (CrossRef Link)
[20] H. L. Qian, J. G. Li and Y. C. Zhang, "Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure," in *Proc. of ICICS 2013*, LNCS 8233, pp. 363-372, 2013. Article (CrossRef Link)
[21] H. L. Qian, J. G. Li, Y. C. Zhang and J. G. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," *International Journal of Information Security*, vol. 14, no. 6, pp. 487-497, 2015. Article (CrossRef Link)
[22] F. Xhafa, J. Feng, Y. Zhang, X. Chen and J. Li, "Privacy-aware attribute-based PHR sharing with user accountability in cloud computing," *Journal of Supercomputing,* vol. 71, no. 5, pp. 1607-1619, 2015. Article (CrossRef Link)
[23] S. Sabitha and M. S. Rajasree, "Anonymous-CPABE: privacy preserved content disclosure for data sharing in cloud," in *Proc. of ARCS 2015*, LNCS 9017, pp. 146-157, 2015. Article (CrossRef Link)
[24] Z. J. Fu, X. M. Sun, Q. Liu, L. Zhou, and J. G. Shu, "Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, vol. E98-B, no. 1, pp.190-200, 2015. Article (CrossRef Link)
[25] Y. J. Ren, J. Shen, J. Wang, J. Han and S. Y. Lee, "Mutual verifiable provable data auditing in public cloud storage," *Journal of Internet Technology*, vol. 16, no. 2, pp. 317-323, 2015. Article (CrossRef Link)

[26] Z. H. Xia, X. H. Wang, X. M. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340-352, 2015. Article (CrossRef Link)
[27] Z. J. Fu, K. Ren, J. G. Shu, X. M. Sun, and F. X. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Transactions on Parallel and Distributed Systems*, DOI: 10.1109/TPDS.2015.2506573, 2015. Article (CrossRef Link)
[28] J. G. Li, X. N. Lin, Y. C. Zhang and J. G. Han, "KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Transactions on Services Computing*, DOI:10.1109/TSC.2016.2542813, 2016. Article (CrossRef Link)
[29] J. G. Li, Y. R. Shi and Y. C. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," *International Journal of Communication Systems*, DOI: 10.1002/dac.2942, 2015. Article (CrossRef Link)
[30] M. Padhya and D. Jinwala, "A novel approach for searchable CP-ABE with hidden ciphertext-policy," in *Proc. of International Conference on Information Systems Security*, LNCS 8880, pp. 167-184, 2014. Article (CrossRef Link)
[31] Z. Liu, Z. F. Cao, D. S. Wong, "Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on eBay," in *Proc. of the 20th ACM Symposium on Computer and Communications Security*, ACM, pp. 475-486, 2013. Article (CrossRef Link)
[32] J. T. Ning, X. L. Dong, Z. F. Cao, L. F. Wei, X. D. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," *IEEE Transactions Information Forensics and Security*, vol.10, no. 6, pp.1274-1288, 2015. Article (CrossRef Link)
[33] I. Shaparlinski, "Computational Diffie-Hellman problem," *Encyclopedia of Cryptography and Security*, pp. 240-244, 2011. Article (CrossRef Link)
[34] K. Emura, A. Miyaji, A. Nomura, K. Omote and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Proc. of ISPEC 2009*, LNCS 5451, pp. 13-23, 2009. Article (CrossRef Link)

Jiguo Li received his B.S. degree in mathematics from Heilongjiang University, Harbin, China in 1996, M.S. degree in mathematics and Ph.D. degree in computer science from Harbin Institute of Technology, Harbin, China in 2000 and 2003, respectively. During 2006.9-2007.3, he was a visiting scholar at Centre for Computer and Information Security Research, School of Computer Science & Software Engineering, University of Wollongong, Australia. During 2013.2-2014.1, he was a visiting scholar in Institute for Cyber Security in the University of Texas at San Antonio. He is currently a Professor with the College of Computer and Information, Hohai University, Nanjing, China. His research interests include cryptography and information security, cloud computing, wireless security and trusted computing etc. He has published over 100 research papers in refereed international conferences and journals. His work has been cited more than 1600 times at Google Scholar. He has served as program committee member in over 20 international conferences and served as the reviewers in over 50 international journals and conferences.

Haiping Wang received B.S. degree in computer science and technology from Hohai University, Nanjing, China in 2013. She received M.S. degree in computer science and technology from Hohai University, Nanjing, China in 2016. Her research interests include cryptography and information security, network security.



Yichen Zhang received her B.S. degree in computer science from the Qiqihar University, Qiqihar, China in 1995. She received her Ph.D. degree in computer science from Hohai University, Nanjing, China in 2015. She is currently an associate professor with the College of Computer and Information, Hohai University, Nanjing, China. Her research interests include cryptography, network security. She has published over 30 research papers in refereed international conferences and journals.

Jian Shen received the BE degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2007 and the ME and PhD degrees in Computer Science from Chosun University, Gwangju, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a full professor in the School of Computer and Software at Nanjing University of Information Science and technology, Nanjing, China. His research interests include information and network security, security systems, public-key cryptography, cloud computing and security, wireless networks and mobile computing.