Fully secure non-monotonic access structure CP-ABE scheme

Dan Yang[1], BaocangWang[1,2*], Xuehua Ban[1]
[1]State KeyLaboratory of Integrated Service Networks, Xidian University
Xi'an 710071,China
[2]Key Laboratory of Cognitive Radio and Information Processing
Ministry of Education(Guilin University of Electronic Technology)
Guilin, Guangxi 541004, China
[e-mail: ydyk121@163.com, bcwang79@aliyun.com, banxuehua@163.com]
*Corresponding author: Baocang Wang

Received July 31, 2017; revised October 13, 2017; accepted October 26, 2017; published March 31, 2018

Abstract

Ciphertext-policy attribute-based encryption (CP-ABE) associates ciphertext with access policies. Only when the user's attributes satisfy the ciphertext's policy, they can be capable to decrypt the ciphertext. Expressivity and security are the two directions for the research of CP-ABE. Most of the existing schemes only consider monotonic access structures are selectively secure, resulting in lower expressivity and lower security. Therefore, fully secure CP-ABE schemes with non-monotonic access structure are desired. In the existing fully secure non-monotonic access structure CP-ABE schemes, the attributes that are set is bounded and a one-use constraint is required by these projects on attributes, and efficiency will be lost. In this paper, to overcome the flaw referred to above, we propose a new fully secure non-monotonic access structure CP-ABE. Our proposition enforces no constraints on the scale of the attributes that are set and permits attributes' unrestricted utilization. Furthermore, the scheme's public parameters are composed of a constant number of group elements. We further compare the performance of our scheme with former non-monotonic access structure ABE schemes. It is shown that our scheme has relatively lower computation cost and stronger security.

Keywords: Ciphertext-policy attribute based encryption, Non-monotonic access structure, Full security, Access control

1. Introduction

The fundamental lineaments making the cloud so attracting today is the grand accessibility it supplies: users can access their data by means of the Internet from anywhere, whereas unauthorized receivers can not access the data. One possible approach to support this feature is to encrypt stored data. Conventional public-key encryption mechanisms, nevertheless, were formulated to encode data confidentially to a objective receiver, which appears to limit the scope of possibilities and flexibility provided by the cloud environment.

To solve this problem, The fuzzy identity-based scheme was proposed by Sahai and Waters [1], then the concept of attribute-based encryption (ABE) was foremost presented. This scheme is restricted therein it allows an authority merely to issue private keys expressing threshold policies. Since then, several works [2-17] proposed different ABE systems and applications, among which two worksare remarkable. Goyal et al. [6] propounded a fine-grained access constraint for attribute-based encryption. Their constructure supplies a mechanism to create secret key with a fine grained access tree policy built up through AND, OR, and threshold gates. Such scheme as key-policy attribute-based encryption(KP-ABE) was called by researchers. Contrary to [6], Bethencourt et al. [2] proposed a scheme, which the access policy imbeded in ciphertext instead of in secret key. The scheme was entitled as ciphertext-policy attribute-based encryption (CP-ABE). In recent years, Li [14] propounded a hidden access policy CP-ABE scheme, which can protect the privacy of the encryptor and decryptor. Guan [16] proposed a conditional CP-ABE which enables data owner to add extra access trees and the corresponding conditions. Jiang [15] proposed a flexible CP-ABE supporting AND-gate and threshold with short ciphertexts.

The research on ABE focus on two subjects: one is to raise its expressivity; the other is to reach stronger security. An extensive rank of access structures can be expressed by the above schemes, but they are still restricted since they support a monotonic access structure only. For example, we merely want to authorize the set $\{a_1, a_2\}$ or $\{a_3, a_4\}$, but the authorized sets can be expressed in $(a_1 \wedge a_2 \wedge \neg a_3 \wedge \neg a_4) \vee (\neg a_1 \wedge \neg a_2 \wedge a_3 \wedge a_4)$ only, no monotonic access structure can fulfill such demand. Ostrovsky [18] proposed the first KP-ABE scheme with non-monotone access structure to address this problem. The scheme adopts the idea from the Naor-Pinkas revocation scheme [19] to obtain the selective security and fixed size of attributes set. Cheung [4] propounded an ABE scheme with non-monotonic access structure, according to doubling attributes universe's size. A bounded CP-ABE was proposed by Vipul Goyal [5], in which attributes should be mapped to three values: Non-Negated, Negated and Ignorable. Sadikin [20] propounded a non-monotonic access structure CP-ABE using the real NOT gate in the access structure. Yamada [21] proposed a new non-monotonic ABE schemes with compact parameters. Conditional CP-ABE was broadened by Wang [22] to give support to XACML (eXtensible Access Control Markup Language) based policy transformation and to support logical NOT in policies by means of De Morgan's Laws. Unfortunately, all these schemes were proved to be secure under Selective-ID model. The attacker ought to announce the access structure he will attack prior to getting public parameters of the system. This is apparently not acceptable for the security requirements in practice.

Some works have presented fully secure schemes to enhance the security. Waters [23] proposed a fully secure IBE scheme using what they called dual system encryption. Okamoto [24] proposed a fully secure functional encryption (FE) scheme with non-monotonic access

structure. Lewko [25] provided an ABE scheme with the inaugural proof of full security in the standard model through exploiting the dual system encryption. Nevertheless, the attributes in these schemes needing a one-use constraint, a loss will be incurred by such mechanism in efficiency. To obviate the efficiency loss, a fully secure monotonic access structure CP-ABE scheme was propounded by Lewko and Waters [26], which full security is reached by using selective methods. This work permits attributes' unrestricted use when even proving to be fully secure in the standard model. Yang [27] proposed a fully secure non-monotonic access structure KP-ABE by making use of the new proof methods, but the number of attributes was fixed. Yuan [13] propounded a fine-grained access control based on non-monotonic CP-ABE without proving the security. Yet fully secure non-monotonic access structure ABE schemes are still desired.

In this paper, to conquer the deficiency mentioned above, we propose a new fully secure non-monotonic access structure CP-ABE. The size of the attributes that are set is not restricted by our construction and our construction allows unrestricted use of attributes. Furthermore, the scheme's public parameters comprise a constant number of group elements. We further compare our scheme with former non-monotonic access structure ABE schemes. The results show that our scheme has relatively lower computation cost and stronger security.

The remainder of the article was organized as follows. In Section 2, we present the principal theoretic background we utilize later on. In Section 3, our construction is explained in particular. In Section 4, we prove its full security in the standard model. In Section 5, we compare our work with former works in the literature. In Section 6, we conclude the article.

2. Preliminaries

2.1 Composite Order Bilinear Groups

We define composite order bilinear groups as follows [26].

We let G denote a group generator, an algorithm which takes a security parameter λ as input and outputs a description of a bilinear group G. We define $G's$ output as (N, G, G_T, e), where $N = p_1 p_2 p_3$ is a product of three distinct primes, G and G_T are cyclic groups of order N, and $e: G^2 \to G_T$ is a map such that:

(1) (Bilinear) $\forall a, b \in Z_N, e(g^a, g^b) = e(g, g)^{ab}$

(2) (Non-degenerate) $\exists g \in G$ such that $e(g, g)$ has order N in G_T

We refer to G as the source group and G_T as the target group. We assume that the group operations in G and G_T and the map e are computable in polynomial time with respect to λ, and the group descriptions of G and G_T include a generator of each group.

2.2 Access Structure

The definition of Access Structure is defined as follows [27].

Let $U = \{U_1, U_2, ..., U_n\}$ be a set of parties. $AS \subseteq 2^U$ is a subset of 2^U and 2^U denoted the set of all the subset of U. The collection AS is called an access structure. The sets in AS are called the authorized sets, and the sets not in AS are called the unauthorized sets. The access structure is monotone if $\forall A, A', A \in AS$ and $A \subseteq A'$, then $A' \in AS$.

2.3 Linear Secret Sharing Scheme

We define linear Secret Sharing Scheme as follows [21].

Let P be a set of parties. Let L be an $l \times m$ matrix. Let $\pi : \{1,\cdots,l\} \to P$ be a function that maps a row to a party for labeling. A secret sharing scheme π for access structure Γ over a set of P is a linear secret-sharing scheme (LSSS) in Z_p and is represented by (L,π) if it consists of two efficient algorithms:

$Share_{L,\pi}$. There exists an efficient algorithm that takes as input a value to be shared $s \in Z_p$. It chooses $s_2,\cdots,s_m \leftarrow Z_p$ and let $\vec{s} = (s,s_2,\cdots,s_m)$. It outputs $L \cdot \vec{s}$ as the vector of l shares. The share $\lambda_i = (\vec{L_i},\vec{s})$ belongs to party $\pi(i)$, where $\vec{L_i}$ denotes the i^{th} row of L.

$Recon_{L,\pi}$. The algorithm takes as input an access set $S \in \Gamma$. Let $I = \{i \mid \pi(i) \in S\}$. It outputs a set of constants $\{(i,\mu_i)\}_{i\in I}$ which has a linear reconstruction property: $\sum_{i\in I} \mu_i \lambda_i = s$.

2.4 CP-ABE Definition

A CP-ABE system consists of four algorithms:

Setup: This is a probabilistic algorithm that takes no input other than the implicit security parameter. It outputs the public parameters PP and a master secret key MSK.

Encryption: This is a probabilistic algorithm that takes as input a message M, an access structure $\mathbb{A}$, and the public parameters PP. It outputs the ciphertext CT.

Key Generation: This is a probabilistic algorithm that takes as input a set of attributes w, the public parameters PP, and the master secret key MSK. It outputs a decryption key SK.

Decryption: This algorithm takes as input the ciphertext CT that was encrypted under an access structure $\mathbb{A}$, the decryption key SK for a set of attributes w, and the public parameters PP. It outputs the message M if $w \in \mathbb{A}$.

2.5 Complexity Assumptions

Assumption 1. [26] Given a group generator $\mathcal{G}$, we define the following distribution:

$$\mathbb{G} = \left(N = p_1 p_2 p_3, G, G_T, e\right) \xleftarrow{R} \mathcal{G},$$

$$g_1 \xleftarrow{R} G_{p_1}, g_2, X_2, Y_2 \xleftarrow{R} G_{p_2}, g_3 \xleftarrow{R} G_{p_3}, \alpha, s \xleftarrow{R} Z_N,$$

$$D = \left(\mathbb{G}, g_1, g_2, g_3, g_1^{\alpha} X_2, g_1^{s} Y_2\right), T_0 = e\left(g_1, g_1\right)^{\alpha s}, T_1 \xleftarrow{R} G_T.$$

We define the advantage of an algorithm $\mathcal{A}$ in breaking this assumption to be:

$$Adv^1_{\mathcal{G},\mathcal{A}}(\lambda) := \left|\Pr\left[\mathcal{A}\left(D, T_0\right) = 1\right] - \Pr\left[\mathcal{A}\left(D, T_1\right) = 1\right]\right|$$

Assumption 2. (The General Subgroup Decision Assumption [26]) We let G denote a group generator and $Z_0, Z_1, ..., Z_k$ denote a collection of non-empty subsets of $\{1,2,3\}$ where each Z_i for $i \geq 2$ satisfies either $Z_0 \cap Z_i \neq \varnothing \neq Z_1 \cap Z_i$ or $Z_0 \cap Z_i = \varnothing = Z_1 \cap Z_i$. We define the following distribution:

$$\mathbb{G} = \left(N = p_1 p_2 p_3, G, G_T, e\right) \xleftarrow{R} \mathcal{G},$$

$$gz_2 \xleftarrow{R} G_{Z_2}, ..., gz_k \xleftarrow{R} G_{Z_k},$$

$$D = \left(\mathbb{G}, gz_2, ..., gz_k\right), T_0 \xleftarrow{R} G_{Z_0}, T_1 \xleftarrow{R} G_{Z_1}.$$

Fixing the collection of sets $Z_0, Z_1, ..., Z_k$, we define the advantage of an algorithm $\mathcal{A}$ in

breaking this assumption to be:

$$Adv_{\mathcal{G},\mathcal{A}}^{SD}(\lambda) := \left|\Pr\left[\mathcal{A}(D,T_0)=1\right]-\Pr\left[\mathcal{A}(D,T_1)=1\right]\right|$$

Assumption 3. (The Three Party Diffie-Hellman Assumption in a Subgroup [26]) Given a group generator $\mathcal{G}$,we define the following distribution:

$$\mathbb{G}=\left(N=p_1p_2p_3,G,G_T,e\right)\xleftarrow{R}\mathcal{G},$$

$$g_1\xleftarrow{R}G_{p_1},g_2\xleftarrow{R}G_{p_2},g_3\xleftarrow{R}G_{p_3},x,y,z\xleftarrow{R}Z_N,$$

$$D=\left(\mathbb{G},g_1,g_2,g_3,g_2^x,g_2^y,g_2^z\right),T_0=g_2^{xyz},T_1\xleftarrow{R}G_{p_2}.$$

We define the advantage of an algorithm $\mathcal{A}$ in breaking this assumption to be:

$$Adv_{\mathcal{G},\mathcal{A}}^{3DH}(\lambda) := \left|\Pr\left[\mathcal{A}(D,T_0)=1\right]-\Pr\left[\mathcal{A}(D,T_1)=1\right]\right|$$

Assumption 4. (The Source Group q-Parallel BDHE Assumption in a Subgroup [26]) Given a group generator $\mathcal{G}$ and a positive q , we define the following distribution:

$$\mathbb{G}=\left(N=p_1p_2p_3,G,G_T,e\right)\xleftarrow{R}\mathcal{G},$$

$$g_1\xleftarrow{R}G_{p_1},g_2\xleftarrow{R}G_{p_2},g_3\xleftarrow{R}G_{p_3},c,d,f,b_1,\cdots,b_q\xleftarrow{R}Z_N,$$

$$D=(\mathbb{G},g_1,g_2,g_3,g_2^f,g_2^{df},g_2^c,g_2^{c^2},\cdots,g_2^{c^q},g_2^{c^{q+2}},\cdots,g_2^{c^{2q}},$$

$$g_2^{c^i/b_j}\ \forall i\in[2q]\setminus\{q+1\},j\in[q],$$

$$g_2^{dfb_j}\ \forall j\in[q],g_2^{dfc^ib_{j'}/b_j}\ \forall i\in[q],j,j'\in[q]\ s.t.\ j\neq j')$$

$$T_0=g_2^{dc^{q+1}},T_1\xleftarrow{R}G_{p_2}.$$

We define the advantage of an algorithm $\mathcal{A}$ in breaking this assumption to be:

$$Adv_{\mathcal{G},\mathcal{A}}^{q}(\lambda) := \left|\Pr\left[\mathcal{A}(D,T_0)=1\right]-\Pr\left[\mathcal{A}(D,T_1)=1\right]\right|$$

2.6 Non-monotonic Access Structure

We recall a technique proposed by Ostrovsky, Sahai, and Waters [18] to move from monotonic access structures to non-monotonic access structure. Denoted A as a collection of monotonic access structures for a set of parties P , the parties in P has the following properties: either the name is normal (like x) or it is primed (like x'), and if $x\in P$ then $x'\in P$ and vice versa. Conceptually, prime attributes are associated with negation of unprimed attributes.

We define the family of non-monotonic access structure $\widetilde{A}$: For each monotonic access structure A, the corresponding non-monotonic access structure is $NM(\mathrm{A})$ over a set of parties $\widetilde{P}$, where $\widetilde{P}$ is a set of all the unprimed parties in P. For every set $\tilde{S}\subset\widetilde{P}$, $N(\tilde{S})$ is defined as $N(\tilde{S})=\tilde{S}\cup\{x'\mid x\in\widetilde{P}\setminus\tilde{S}\}$. Then $NM(\mathrm{A})$ is defined by saying that $\tilde{S}$ is authorized in $NM(\mathrm{A})$ if and only if $N(\tilde{S})$ is authorized in A. For each access set $X\in NM(\mathrm{A})$, there is a set in A containing the elements in X and primed elements for each party not in X.

3. Main Construction

$Setup(\lambda)$: The setup algorithm executes as follows. It selects a bilinear group G of order $N = p_1 p_2 p_3$ (3 different primes). We let G_{p_i} denote the subgroup of order p_i in G. It then selects random exponents $\alpha, a, k \in Z_N$ and a random group element $g \in G_{p_1}$. Finally the public parameters: $PP=(N, g, g^a, g^k, e(g,g)^\alpha)$. The master secret key: $MSK=(g^\alpha, g_3)$, g_3 is a generator of G_{P_3}.

$KeyGen(MSK, PP, \gamma)$: Given a set of attributes $\gamma = \{\gamma_1, \cdots, \gamma_f\} \subset Z_N$, the key generation algorithm chooses random exponents $b, c, d \in Z_N$, and random elements $R, R', \{W_i, V_i\}, \{W_i', V_i'\}_{i \in f} \in G_{p_3}$. It then chooses $r, r_1, \cdots, r_f \leftarrow Z_N$ and $r_1', \cdots, r_f' \in Z_N$ randomly such that $r_1' + \cdots + r_f' = r$. The secret key is $K = g^\alpha g^{dr} R$, $K_{i,1} = g^{-cr}(g^{k\gamma_i} g^a)^{r_i} W_i$, $K' = g^r R'$, $K_{i,2} = g^{r_i} V_i$, $K_{i,1'} = (g^{kb\gamma_i} g^{ab})^{r_i'} W_i'$, $K_{i,2'} = g^{br_i'} V_i'$, $\forall i \in [f]$.

The final output is $SK = (K, K', \{K_{i,1}, K_{i,2}, K_{i,1'}, K_{i,2'}, \forall i \in [f]\})$.

$Encrypt(PP, M, \tilde{\Gamma})$: A ciphertext satisfying the non-monotonic access structure $\tilde{\Gamma}$ will be computed by the encryption algorithm. As presented in Part 2.6, there is a monotonic access structure Γ and linear secret sharing scheme (L, π) over P corresponding to $\tilde{\Gamma}$. First, the algorithm chooses randomly $\vec{s} = (s, s_2, \cdots, s_m) \leftarrow Z_N^m$ and for each $\pi(i)$, $i = 1, \cdots, l$ computes share $\lambda_i = (L_i \cdot s)$. It then computes $C_0 = M \cdot e(g,g)^{\alpha \cdot s}$, $C_1 = g^s$.

If $\tilde{x}_i$ is not primed, we have

$$C_i = (C_i^1 = g^{d\lambda_i} g^{ct_i}, C_i^2 = (g^{kx_i} g^a)^{-t_i}, C_i^3 = g^{t_i}) \tag{1}$$

If $\tilde{x}_i$ is primed, we have

$$C_i = (C_i^4 = g^{d\lambda_i} g^{(kb)t_i}, C_i^5 = (g^{kx_i} g^a)^{-t_i}, C_i^6 = g^{t_i}) \tag{2}$$

$Decrypt(PP, CT, SK)$: First the decryption algorithm checks whether $\gamma \in \tilde{\Gamma}$, if not it outputs $\perp$. If $\gamma \in \tilde{\Gamma}$, we can get $\tilde{\Gamma} = NM(\Gamma)$ and corresponding linear secret sharing scheme (L, π). For $I = \{i \mid \pi(i) \in \gamma'\}$, $\gamma' = N(\gamma) \in \Gamma$, if the attributes set γ' satisfy Γ, a set of coefficients $\{(i, \mu_i)\}_{i \in I}$ can be computed by the receiver such that $\sum_{i \in I} \lambda_i \cdot \mu_i = s$.

Next, for every positive attribute $x_i \in \gamma$, the decrypt procedure computes:

$$\begin{aligned} & e(C_i^1, K') \cdot e(C_i^2, K_{i,2}) \cdot e(C_i^3, K_{i,1}) \\ &= e(g^{d\lambda_i} g^{ct_i}, g^r) \cdot e((g^{kx_i} g^a)^{-t_i}, g^{r_i}) \cdot e(g^{t_i}, g^{-cr}(g^{k\gamma_i} g^a)^{r_i}) \\ &= e(g,g)^{d\lambda_i r} \cdot e(g,g)^{crt_i} \cdot e(g,g)^{-kt_i x_i r_i} \cdot e(g,g)^{-at_i r_i} \cdot e(g,g)^{-crt_i} \\ &= e(g,g)^{d\lambda_i r} \end{aligned} \tag{3}$$

For every negated attribute $x_i \in \gamma$, the decrypt procedure computes:

$$
\begin{aligned}
& e(C_i^4, K') \cdot \prod_{j \in [f]} (e(C_i^6, K_{j,1'}) \cdot e(C_i^5, K_{j,2'}))^{\frac{1}{x_i - \gamma_j}} \\
&= e(g,g)^{d\lambda_i r} \cdot e(g,g)^{kbrt_i} \cdot \prod_{j \in [f]} (e(g,g)^{kb\gamma_i t_i r_j'} \cdot e(g,g)^{-kx_i t_i b r_j'})^{\frac{1}{x_i - \gamma_j}} \\
&= e(g,g)^{d\lambda_i r} \cdot e(g,g)^{kbrt_i} \cdot e(g,g)^{-kbrt_i} \\
&= e(g,g)^{d\lambda_i r}
\end{aligned} \tag{4}
$$

Finally the message can be obtained by computing:

$$
\begin{aligned}
M &= \frac{C_0}{e(C_1, K) \cdot \prod_{i \in I} (e(g,g)^{dr\lambda_i})^{-\mu_i}} \\
&= \frac{C_0}{e(g^s, g^{\alpha} g^{dr}) \cdot \prod_{i \in I} (e(g,g)^{-dr\lambda_i \mu_i})} \\
&= \frac{C_0}{e(g,g)^{\alpha s}}
\end{aligned} \tag{5}
$$

4. Proof of Security

Our scheme's security is now proven as follows:

Theorem 1. Under Assumption 1, the General Subgroup Decision Assumption, the Three Party Diffie-Hellman Assumption in a Subgroup, and the Source Group q-Parallel BDHE Assumption in a Subgroup defined in Section 2.5, our scheme defined in Section 3 is fully secure.

The security proof is acquired via a hybrid argument by means of a sequence of games,. We let g_2 : a fixed generator of the subgroup G_{p_2}.

Semi-functional keys: In order to generate a semi-functional key for an attribute set γ, one first calls the normal key generation algorithm to create the normal key: $K, K', \{K_{i,1}, K_{i,2}, K_{i,1}', K_{i,2}'\}_{i \in f}$, then a random element $W \in G_{p_2}$ is chosen, and gets the semi-functional key: $KW, K', \{K_{i,1}, K_{i,2}, K_{i,1}', K_{i,2}'\}_{i \in f}$.

Semi-functional ciphertext: In order to generate a semi-functional ciphertext for the non-monotonic access structure $\tilde{\Gamma}$, one first runs the normal encryption algorithm to create the normal ciphertext, then randomly chooses $a', b', d', c', k' \in Z_N$, random exponent $\eta_i \in Z_N$ and $\theta_i \in Z_N$ for each $i \in l$, a random exponent $\psi_i \in Z_N$ for each attribute i.The semi-functional ciphertext is: C_0, $C_1 g_2^{s'}$, if ψ_i is a positive attribute: $C_{i,1} g_2^{d'\theta_i + c'\eta_i}$, $C_{i,2} g_2^{-(k'\eta_i\psi_i + a'\eta_i)}$, $C_{i,3} g_2^{\eta_i}$; if ψ_i is a negated attribute: $C_{i,1}' g_2^{d'\theta_i\eta_i + k'b'\eta_i}$, $C_{i,2}' g_2^{-(k'\eta_i\psi_i + a'\eta_i)}$, $C_{i,3}' g_2^{\eta_i}$.

Nominal Semi-functional keys: The simulator first takes the normal keys using the normal key generation algorithm, then randomly chooses $r' \in Z_N$ and $\varphi_i \in Z_N$ for each $i \in [f]$. The nominal semi-functional key is: $K g_2^{d'r'}$, $K' g_2^{r'}$, $K_{i,1} g_2^{-c'r' + k'\psi_i r' + a'\varphi_i}$, $K_{i,2} g_2^{\varphi_i}$, $K_{i,1}' g_2^{k'b'\varphi_i\psi_i + a'b'\varphi_i}$, $K_{i,2}' g_2^{b'\varphi_i}$, $\forall i \in [f]$.

Temporary Semi-functional keys: The simulator randomly chooses $W \in G_{p_2}$ and creates the temporary semi-functional keys: KW, $K'g_2^{r'}$, $K_{i,1}g_2^{-c'r'+k'\psi_i r'+a'\varphi_i}$, $K_{i,2}g_2^{\varphi_i}$, $K_{i,1}^{'}g_2^{k'b'\varphi_i\psi_i+a'b'\varphi_i}$, $K_{i,2}^{'}g_2^{b'\varphi_i}$, $\forall i \in [f]$.

For each k from 1 to Q, the following games are defined:

$Game_{real}$: This is the actual security game, the ciphertext and keys are normal.

$Game_0$: The ciphertext that is supplied to the attacker is semi-functional, and the keys are normal.

$Game_k$: The ciphertext that is supplied to the attacker is semi-functional. The remaining keys are normal.

$Game_k^N$: This is similar to $Game_k$, apart from the fact that the k_{th} key supplied to the attacker is a nominal semi-functional key. The first $k-1$ keys are still semi-functional in the original sense, whereas the remaining keys are normal.

$Game_k^T$: This is similar to $Game_k$, apart from the fact that the k_{th} key supplied to the attacker is a temporary semi-functional key. The remaining keys are normal and the first $k-1$ keys are semi-functional in the original sense.

$Game_{final}$: This is similar to $Game_Q$, the only difference is that the ciphertext sent to an attacker is encrypted with random messages.

Our hybrid argument is completed in the following lemmas.

Lemma 1. Beneath Assumption 2, there is no polynomial time attacker can achieve a non-negligible difference in advantage between $Game_{real}$ and $Game_0$.

Proof. Assuming that a PPT attacker $\mathcal{A}$ achieving a non-negligible difference in advantage between $Game_{real}$ and $Game_0$, we can generate a PPT algorithm $\mathcal{B}$ to break the assumption 2 with sets: $Z_0 := \{1\}$, $Z_1 := \{1,2\}$, $Z_2 := \{1\}$, $Z_3 := \{3\}$. $\mathcal{B}$ is given g_1, g_3, T, where g_1 denotes a generator of G_{p_1}, g_3 denotes a generator of G_{p_3}, and T is either from G_{p_1} or $G_{p_1p_2}$. $\mathcal{B}$ will simulate either $Game_{real}$ or $Game_0$ with $\mathcal{A}$.

$\mathcal{B}$ randomly selects $\alpha, a, k \in Z_N$, then the public parameters: $PP = \{N, g = g_1, g^a = g_1^a, g^k = g_1^k, e(g,g)^\alpha = e(g_1,g_1)^\alpha\}$. It gives these to $\mathcal{A}$. $\mathcal{B}$ saves the MSK.

In some stage, $\mathcal{A}$ request a challenge ciphertext for non-monotonic access structures $\tilde{\Gamma}$ and message M_0, M_1. $\mathcal{B}$ first chooses a random bit b, then $\mathcal{B}$ chooses random exponents $\tilde{\lambda}_i \in Z_N$, $\tilde{t}_i \in Z_N$ for each i from 1 to l, It sets g_1^s equal to the G_{p_1} part of T and sets $\lambda_i = s\tilde{\lambda}_i$, $t_i = s\tilde{t}_i$, then outputs the challenge ciphertext: $C_0 = M_b e(g_1,T)^\alpha$, $C_1 = T$, if x_i is a positive attribute: $C_i^1 = T^{d\tilde{\lambda}_i + c\tilde{t}_i}$, $C_i^3 = T^{\tilde{t}_i}$, $C_i^2 = T^{-(kx_i\tilde{t}_i + a\tilde{t}_i)}$; if x_i is a negated attribute: $C_i^4 = T^{d\tilde{\lambda}_i + kb\tilde{t}_i}$, $C_i^5 = T^{-(kx_i\tilde{t}_i + a\tilde{t}_i)}$, $C_i^6 = T^{\tilde{t}_i}$.

If $T \in G_{p_1}$, this is a distributed normal ciphertext, and $\mathcal{B}$ has properly simulated $Game_{real}$ with $\mathcal{A}$. If $T \in G_{p_1p_2}$, this is a semi-functional ciphertext, and $\mathcal{B}$ has simulated $Game_{real}$ with $\mathcal{A}$. So $\mathcal{B}$ can break the assumption 2 with the same advantage if the adversary $\mathcal{A}$ can achieve a non-negligible difference in advantage between $Game_{real}$ and $Game_0$.

Lemma 2. Beneath Assumption 2, for any $1 \le k \le Q$, no polynomial time attacker can achieve a non-negligible difference in advantage between $Game_{k-1}$ and $Game_k^N$.

Proof. Assuming that there is a PPT attacker $\mathcal{A}$ achieving a non-negligible difference in advantage between $Game_{real}$ and $Game_0$, we can generate a PPT algorithm $\mathcal{B}$ to break the assumption 2 with sets: $Z_0 := \{1,3\}$, $Z_1 := \{1,2,3\}$, $Z_2 := \{1\}$, $Z_3 := \{3\}$, $Z_4 := \{1,2\}$, $Z_5 := \{2,3\}$. $\mathcal{B}$ is given $g_1, g_3, X_1X_2, Y_2Y_3, T$, where X_1 is a generator of group G_{p_1}, g_3 and X_3 are generator of group G_{p_3}, X_2 is a generator of group G_{p_2}, and T is either a random element of $G_{p_1p_3}$ or $G_{p_1p_2p_3}$. $\mathcal{B}$ will simulate either $Game_{k-1}$ or $Game_k^N$ with $\mathcal{A}$.

For the inaugural $k-1$ enquiries, $\mathcal{B}$ first announces the normal key generation algorithm to get K, K', $K_{i,1}$, $K_{i,2}$, $K_{i,1}'$, $K_{i,2}'$, then $\mathcal{B}$ selects $\tau \in Z_N$ randomly, and creates the semi-functional key: $K(Y_2Y_3)^\tau$, K', $K_{i,1}$, $K_{i,2}$, $K_{i,1}'$, $K_{i,2}'$.

To respond the enquiries of k key, $\mathcal{B}$ selects $R, R', \{W_i, V_i\}, \{W_i', V_i'\} \in G_{p_3}$ and a exponent $\tilde{b} \in Z_N$, then creates the key: $K = g_1^\alpha T^d R$, $K' = TR'$, $K_{i,1} = T^{-c+\tilde{k}w_i r_i + \tilde{a}r_i} W$, $K_{i,2} = T^{r_i} V_i$, $K_{i,1}' = T^{\tilde{b}r_i'(kw_i+a)} W_i'$, $K_{i,2}' = T^{\tilde{b}r_i'} V_i'$. In order to create the semi-functional challenge ciphertext for non-monotonic $\tilde{\Gamma}$ and message M_b, $\mathcal{B}$ outputs the semi-functional ciphertext: $C_0 = M_b e(g_1, X_1X_2)^\alpha$, $C_1 = X_1X_2$, if x_i is a positive attribute: $C_i^1 = X_1 X_2^{d\tilde{\lambda}_i + c\tilde{t}_i}$, $C_i^2 = X_1 X_2^{-(kx_i\tilde{t}_i + a\tilde{t}_i)}$, $C_i^3 = X_1 X_2^{\tilde{t}_i}$; if x_i is a negated attribute: $C_i^4 = X_1 X_2^{d\tilde{\lambda}_i + kb\tilde{t}_i}$, $C_i^5 = X_1 X_2^{-(kx_i\tilde{t}_i + a\tilde{t}_i)}$, $C_i^6 = X_1 X_2^{\tilde{t}_i}$.

This is a properly distributed normal key if $T \in G_{p_1p_3}$, $\mathcal{B}$ simulated $Game_{k-1}$ with $\mathcal{A}$. This is a semi-functional key if $T \in G_{p_1p_2p_3}$, $\mathcal{B}$ simulated $Game_k^N$ with $\mathcal{A}$. So $\mathcal{B}$ can break the assumption 2 with the same advantage if the adversary $\mathcal{A}$ can achieve a non-negligible difference in advantage between $Game_{k-1}$ and $Game_k^N$.

Lemma 3. Beneath Assumption 3, no polynomial time attacker can achieve a non-negligible difference in advantage between $Game_k^T$ and $Game_k^N$, $k = 1, \cdots, Q_1$.

Proof. Assuming that there is a PPT attacker $\mathcal{A}$ achieving a non-negligible difference in advantage between $Game_k^T$ and $Game_k^N$, we can generate a PPT algorithm $\mathcal{B}$ to break the assumption 3. $\mathcal{B}$ is given $g_1, g_2, g_3, g_2^x, g_2^y, g_2^z, T$, where T is either g_2^{xyz} or a random element of G_{p_2}. $\mathcal{B}$ will simulate either $Game_k^T$ or $Game_k^N$ with $\mathcal{A}$ depending on the nature of T.

For the first $k-1$ queries made by $\mathcal{A}$, $\mathcal{B}$ firstly runs the normal key generation algorithm to get $K, K', K_{i.1}, K_{i,2}, K_{i,1}', K_{i,2}'$, then $\mathcal{B}$ randomly chooses $W \in G_{p_2}$, and forms the semi-functional key as: $KW, K', K_{i,1}, K_{i,2}, K_{i,1}', K_{i,2}'$. To form the k^{th} key, $\mathcal{B}$ first calls the normal key generation algorithm, then randomly choose $r' \in Z_N$ and $\varphi_i \in Z_N$. It sets the key as $Kg_2^{d'r'}T$, $K' g_2^{r'}$, $K_{i,1} g_2^{-c'r' + k'\psi_i r' + a'\varphi_i}$, $K_{i,2} g_2^{\varphi_i}$, $K_{i,1}' g_2^{k'b'\varphi_i\psi_i + a'b'\varphi_i}$, $K_{i,2}' g_2^{b'\varphi_i}$.

If $T = g_2^{xyz}$, this is a properly distributed nominal semi-functional key, and if T is a random in G_{p_2}, this is a properly distributed temporary semi-functional key.

To create the semi-functional challenge ciphertext for non-monotonic access structures $\tilde{\Gamma}$ and message M_b, $\mathcal{B}$ first runs the normal encryption algorithm to produce a normal ciphertext. Then finds the monotonic access structure Γ and linear secret sharing scheme Π over P corresponding to $\tilde{\Gamma}$. For every attribute $\tilde{x}_i$ corresponding to Γ, where $\tilde{x}_i \in P$, let $\gamma' = N(\gamma) \in \Gamma$. Let M be the share-generating matrix for linear secret sharing scheme. $\mathcal{B}$ can efficiently find a vector $\tilde{w} \in Z_N^n$ such that $\tilde{w} \cdot M_i = 0$. Such a vector will exist as long as $(1,0,\cdots,0)$ is not in the span of $\{M_i\}_{\pi(\mathrm{i})\in\gamma}$ modulo each of p_1, p_2, p_3. $\mathcal{B}$ also chooses a random vector $w' \in Z_N^n$ with first entry equal to 0 and implicitly set $w = \tilde{w} + c \cdot w'$. For semi-functional ciphertext, $\mathcal{B}$ first computes C_0 and $C_1 g_2^{s'}$.

To compute the other part of semi-functional ciphertext, firstly, for the positive attributes $\tilde{x}_i = x_i$. If $x_i \in \gamma$, $\mathcal{B}$ selects $\eta_i \in Z_N$ and outputs: $C_i^1 g_2^{w\lambda_i} g_2^{c'\eta_i}$, $(C_i^2 g_2^{k'x_i} g_2^{a'})^{-\eta_i}$, $C_i^3 g_2^{\eta_i}$. If $x_i \notin \gamma$, it will implicitly set $\eta_i = (c')^{-1}\lambda_i \cdot \tilde{w} + \tilde{\eta}_i$ and outputs: $C_i^1 g_2^{w\lambda_i} g_2^{c'\tilde{\eta}_i}$, $(C_i^2 g_2^{k'x_i} g_2^{a'})^{-\tilde{\eta}_i}$, $C_i^3 g_2^{(c')^{-1}\lambda_i \cdot \tilde{w}} g_2^{\tilde{\eta}_i}$. For the negated attributes $\tilde{x}_i = x_i'$. If $x_i' \in \gamma$, then $x_i' \notin \gamma'$. $\mathcal{B}$ selects $\phi_i \in Z_N$ and setting $w = -\lambda_i + \phi_i$ randomly. $\mathcal{B}$ creates the semi-functional ciphertext: $C_i^4 g_2^{d'(-w+\phi_i)} g_2^{k'b'\phi_i}$, $C_i^5 g_2^{-(k'x_i\phi_i + a'\phi_i)}$, $C_i^6 g_2^{\phi_i'}$. If $x_i' \notin \gamma$, then $x_i' \in \gamma'$. $\mathcal{B}$ selects $\phi_i' \in Z_N$ and outputs the semi-functional ciphertext: $C_i^4 g_2^{d'\lambda_i} g_2^{k'b'\phi_i'}$, $C_i^5 g_2^{-(k'x_i\phi_i' + a'\phi_i')}$, $C_i^6 g_2^{\phi_i'}$.

If $T = g_2^{xyz}$, $\mathcal{B}$ simulates $Game_k^N$ with $\mathcal{A}$. If T is random in G_{p_2}, $\mathcal{B}$ simulates $Game_k^T$ with $\mathcal{A}$. So $\mathcal{B}$ can break the assumption 3 with the same advantage if the adversary $\mathcal{A}$ can achieve a non-negligible difference in advantage between $Game_k^T$ and $Game_k^N$.

Lemma 4. Beneath Assumption 4, no polynomial time attacker can achieve a non-negligible difference in advantage between $Game_k^T$ and $Game_k^N$.

Proof. Assuming that there is a PPT attacker $\mathcal{A}$ achieving a non-negligible difference in advantage between $Game_k^T$ and $Game_k^N$ for some k such that $Q_1 < k \le Q$, we can generate a PPT algorithm $\mathcal{B}$ to break the assumption 4. $\mathcal{B}$ is given $g_1, g_2, g_3, g_2^f, g_2^{df}, g_2^{c^i}, g_2^{c^i/b_j}$, $\forall i \in [2q]\backslash\{q+1\}, j \in [q]$, $g_2^{df b_j}, \forall j \in [q]$, $g_2^{df c^i b_{j'}/b_j}$, $\forall i \in [q]$, $j, j' \in [q]$ such that $j \ne j'$, and T is either equal to $g_2^{dc^{q+1}}$ or a random element of G_{p_2}. $\mathcal{B}$ will simulate either $Game_k^T$ or $Game_k^N$ with $\mathcal{A}$ depending on T.

$\mathcal{B}$ can firstly create a normal key and then multiply the K using a random element of G_{p_2} to create the first $k-1$ semi-functional keys. Because we are assuming the k^{th} key query is a Phase 2 key query, before requesting the k^{th} key, $\mathcal{A}$ will request the challenge ciphertext for non-monotonic access structures $\tilde{\Gamma}$. $\mathcal{B}$ first finds linear secret sharing scheme over P corresponding to $\tilde{\Gamma}$ and the monotonic access structures Γ. For every attribute $\tilde{x}_i$ corresponding to Γ, where $\tilde{x}_i \in P$, J_i is the set of indices j such that $\rho(j) = i$. $\mathcal{B}$ define $g_2^{\eta_i}$, $g_2^{\phi_i}$ as:

$$g_2^{\eta_i} = g_2^{\tilde{\eta}_i} \prod_{j \in J_i} (g_2^{c^q/b_j})^{M_{j,1}} \cdot (g_2^{c^{q-1}/b_j})^{M_{j,2}} \cdots (g_2^{c^{q-n+1}/b_j})^{M_{j,n}} \tag{6}$$

$$g_2^{\phi_i} = g_2^{\phi_i'} \prod_{j \in J_i} (g_2^{c^q/b_j})^{M_{j,1}} \cdot (g_2^{c^{q-1}/b_j})^{M_{j,2}} \cdots (g_2^{c^{q-n+1}/b_j})^{M_{j,n}} \tag{7}$$

Then $\mathcal{B}$ sets the sharing vector w : $w := (y_1(cd)^{-1}, y_2(cd)^{-1}, \cdots, y_n(cd)^{-1})$, $y_1, y_2, \cdots, y_n \in Z_N$, so we have $f'\lambda_i w = y_1\lambda_{i,1} + y_2\lambda_{i,2} + \cdots + y_n\lambda_{i,n}$. $\mathcal{B}$ finally creates the semi-functional ciphertext: C_0 , $C_1 g_2^f$. If $\widetilde{x_i}$ is a positive attribute: $C_i^1 g_2^{y'\lambda_i + c'\tilde{t_i}}$, $C_i^2 g_2^{-(dfx_i\tilde{t_i} + a'\tilde{t_i})}$, $C_i^3 g_2^{dfb_j} g_2^{\tilde{t_i}}$; If $\widetilde{x_i}$ is a negated attribute: $C_i^1 g_2^{y'\lambda_i + bdf\tilde{t_i}}$, $C_i^2 g_2^{-(dfx_i\tilde{t_i} + a'\tilde{t_i})}$, $C_i^3 g_2^{dfb_j} g_2^{\tilde{t_i}}$.

If $\mathcal{A}$ later asks the k^{th} key for attribute sets γ , $\mathcal{B}$ firstly calls the usual key generation algorithm to create a normal key. In order to create the semi-functional components, it firstly selects a vector $\theta = (\theta_1, \theta_2, \cdots, \theta_n) \in Z_N^n$ such that $\theta \cdot M_i = 0 \bmod N$. Such a vector will exist as long as $(1,0,\cdots,0)$ is not in the span of $\{M_i\}_{\rho(i)\in\gamma}$ modulo each of p_1 , p_2 , p_3 . $\mathcal{B}$ sets $d' = \theta_1 c^q + \theta_2 c^{q-1} + \cdots + \theta_n c^{q-n+1}$. Then $\mathcal{B}$ can form $g_2^{d'} = (g_2^{c^q})^{\theta_1} (g_2^{c^{q-1}})^{\theta_2} \cdots (g_2^{c^{q-n+1}})^{\theta_n}$ Since θ is orthogonal to M_i, we have:

$$d'\eta_i = d'\widetilde{\eta_i} + \sum_{i \in J_i} \sum_{\substack{m_1, m_2 = 1 \\ m_1 \neq m_2}}^{n} \theta_{m_1} M_{i,m_2} b_i^{-1} c^{q+1+m_2-m_1} \tag{8}$$

$\mathcal{B}$ can compute $g_2^{d'\eta_i}$ from the terms it is given in the assumption because of $q+1+m_2-m_1$ is in the set $[2q]\backslash\{q+1\}$. So $\mathcal{B}$ creates the semi-functional term for key component K : $T^{\theta_1} \cdot (g_2^{c^{q-1}})^{\theta_2} \cdots (g_2^{c^{q-n+1}})^{\theta_n}$.

$\mathcal{B}$ simulates $Game_k^N$ with $\mathcal{A}$ if $T = g_2^{dc^{q+1}}$. $\mathcal{B}$ simulates $Game_k^T$ with $\mathcal{A}$ if T is a random element of G_{p_2} . So $\mathcal{B}$ can break the assumption 4 with the same advantage if the adversary $\mathcal{A}$ can achieve a non-negligible difference in advantage between $Game_k^T$ and $Game_k^N$,.

Lemma 5. Beneath Assumption 2, for any k from 1 to Q , no polynomial time attacker can achieve a non-negligible difference in advantage between $Game_k^T$ and $Game_k$.

Proof. The proof of lemma 5 is similar to the proof of lemma 2, apart from that $\mathcal{B}$ takes Y_2Y_3 to create a semi-functional key.

Lemma 6. Beneath Assumption 1, no polynomial time attacker can achieve a non-negligible difference in advantage between $Game_Q$ and $Game_{final}$.

Proof. Assuming that there is a PPT attacker $\mathcal{A}$ achieving a non-negligible difference in advantage between $Game_Q$ and $Game_{final}$,then we can get a PPT algorithm $\mathcal{B}$ to break the Assumption 1. $\mathcal{B}$ is given $g_1, g_2, g_3, g_1^{\alpha} X_2, g_1^s Y_2, T$, where T is either $e(g_1, g_1)^{\alpha s}$ or a random element of G_T . $\mathcal{B}$ will simulate either $Game_Q$ and $Game_{final}$ with $\mathcal{A}$.

$\mathcal{B}$ chooses random exponent $\sigma \in Z_N$, if $\mathcal{A}$ requests a key for an attribute set γ . The key is: $K' = g_1^r R'$, $K = (g_1^{\alpha} X_2) g_1^{dr} R g_2^{\gamma}$, $K_{i,1} = g_1^{-cr} (g_1^{kw_i} g_1^a)^{r_i} W_i$, $K_{i,1}' = (g_1^{kbw_i} g_1^{ab})^{r_i'} W_i'$, $K_{i,2}' = g_1^{br_i'} V_i'$.

In order to create the semi-functional challenge ciphertext for non-monotonic $\tilde{\Gamma}$ and message M_b , $\mathcal{B}$ chooses randomly exponent $\widetilde{\lambda_i} \in Z_N$ and $\tilde{t_i} \in Z_N$, the ciphertext is formed

as: $C_0 = M_b T$, $C_1 = g_1^s Y_2$. if $\widetilde{x}_i$ is a positive attribute: $C_i^1 = (g_1^s Y_2)^{d\widetilde{\lambda}_i + c\widetilde{t}_i}$, $C_i^2 = (g_1^s Y_2)^{-(kx_i\widetilde{t}_i + a\widetilde{t}_i)}$, $C_i^3 = (g_1^s Y_2)^{\widetilde{t}_i}$; if $\widetilde{x}_i$ is a negated attribute: $C_i^4 = (g_1^s Y_2)^{d\widetilde{\lambda}_i + kb\widetilde{t}_i}$, $C_i^5 = (g_1^s Y_2)^{-(kx_i\widetilde{t}_i + a\widetilde{t}_i)}$, $C_i^6 = (g_1^s Y_2)^{\widetilde{t}_i}$.

This is semi-functional encryption of a random message and $\mathcal{B}$ simulated $Game_{final}$ if T is a random element of group G_T. If $T = e(g_1, g_1)^{\alpha s}$, this is semi-functional encryption of M_b and $\mathcal{B}$ simulated $Game_Q$ with $\mathcal{A}$. So, $\mathcal{B}$ can break Assumption 1 with the same advantage if the adversary $\mathcal{A}$ can achieve a non-negligible difference in advantage between $Game_Q$ and $Game_{final}$.

The proof of Theorem 1 is completed.

5. Comparisons

In this part, we compare our work with former works in the literature. We compare our work with [13, 20-22, 27] as they also constructed ABE with non-monotonic access structure. For convenience, PP, SK and CT are shortened from the size of the public parameters, the secret key, and the ciphertext length excluding the access policy respectively. $|G_1|, |G_2|$ denote the bit-length of the elements belongs to G_1, G_2. t denotes the attributes' number. n denotes the number of attributes appearing in an access policy.

Table 1. Size of each Value

Schemes	PP	SK	CT	Policy
YDW13[27]	$(t+3)\|G_1\|$	$(3n+2)\|G_1\|$	$(t+3)\|G_1\|$	Key
RSY 13[20]	$(t+2)\|G_1\|+\|G_2\|$	$(3t+3)\|G_1\|$	$(2n+1)\|G_1\|+\|G_2\|$	Ciphertext
SNG 14[21]	$(4t+1)\|G_1\|$	$(4t+2)\|G_1\|$	$(3n+1)\|G_1\|$	Ciphertext
YML15[13]	$(t+3)\|G_1\|+\|G_2\|$	$(3t+2)\|G_1\|$	$(3n+2)\|G_1\|+\|G_2\|$	Ciphertext
WWT17[22]	$(3t+1)\|G_1\|$	$(2t+1)\|G_1\|+\|G_2\|$	$(2n+3)\|G_1\|$	Ciphertext
Our scheme	$\|G_1\|$	$(4t+1)\|G_1\|$	$(3n+1)\|G_1\|$	Ciphertext

Table 2. Security Properties of ABE

Schemes	Security	Monotonic	Assumption	With testing	Attributes set
YDW13[27]	Fully	Non	q-parallel BDHE	Yes	Bounded
RSY13[20]	Fully	Non	Generic bilinear group	Yes	Bounded
SNG14[21]	Selective	Non	n-(B)	Yes	Unbounded
YML15[13]	Selective	Non	DBDH	No	Bounded
WWT17[22]	Selective	Non	DBDH	Yes	Bounded
Our scheme	Fully	Non	q-parallel BDHE	Yes	Unbounded

In **Table 1**, the size of PP and CT in our scheme is the shortest ones, and the size of SK of our scheme is short, so our scheme's communication cost is small. In **Table 2**, compared with YDW13, RSY13, WWT17 and YML15, the size of the attributes that are set is not restricted by our construction. Compared with SNG14, YML15 and WWT 17, our constructer

is fully secure in the standard model. In summary, our constructer has relatively lower computation cost and stronger security than existing ABE schemes.

6. Conclusion

We presented a non-monotonic access structure CP-ABE scheme and the security is proven in the adaptively model. The performance of our scheme compares favorably with previous ones. A safer and more expressive scheme in the future deserves to be put forward.

Acknowledgment

This work was supported by the National Key R&D Program of China under Grants No. 2017YFB0802000, the National Natural Science Foundation of China (No. 61572390, 61473029, 61672412), the Natural Science Foundation of Ningbo City under Grants No. 201601HJ-B01382, and the Open Foundation of Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education (Guilin University of Electronic Technology) under Grants No. CRKL160202.

References

[1] Sahai, A. and B. Waters., "Fuzzy identity-based encryption," in *Proc. of International Conference on Theory and Applications of Cryptographic Techniques*. 2005. Article (CrossRef Link).
[2] Bethencourt, J., A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *Proc. of IEEE Symposium on Security and Privacy*, 2007. Article (CrossRef Link).
[3] Chase, M., "Multi-authority attribute based encryption," in *Proc. of Conference on Theory of Cryptography*, 2007. Article (CrossRef Link).
[4] Cheung, L. and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. of ACM Conference on Computer and Communications Security*, 2007. Article (CrossRef Link).
[5] Goyal, V., et al., "Bounded Ciphertext Policy Attribute Based Encryption," *DBLP*, pp. 579-591, 2008. Article (CrossRef Link).
[6] Goyal, V., et al., "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. of CCS '06 Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89-98, 2006. Article (CrossRef Link).
[7] Han, J., et al., "Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption," *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 3, p. 665-678, 2015. Article (CrossRef Link).
[8] Horváth, M., "Attribute-Based Encryption Optimized for Cloud Computing," *Infocommunications Journal*, vol. 7, no. 2, pp. 1-9, 2014. Article (CrossRef Link).
[9] Lewko, A. and B. Waters, "Decentralizing Attribute-Based Encryption," in *Proc. of Advances in Cryptology - EUROCRYPT 2011 - International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*. 2011. Article (CrossRef Link).
[10] Longo, R., C. Marcolla, and M. Sala, "Key-Policy Multi-authority Attribute-Based Encryption," in *Proc. of International Conference on Algebraic Informatics*, vol. 9270, pp. 152-164, 2016. Article (CrossRef Link).
[11] Phuong, T.V.X., et al., "*Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key," Springer International Publishing*, 2015. Article (CrossRef Link).
[12] Rouselakis, Y. and B. Waters, "*Practical constructions and new proof methods for large universe attribute-based encryption,"* in *Proc. of ACM Sigsac Conference on Computer & Communications Security*, 2013. Article (CrossRef Link).

[13] Yuan, Q., C. Ma, and J. Lin, "*Fine-Grained Access Control for Big Data Based on CP-ABE in Cloud Computing," Springer Berlin Heidelberg*, pp. 344-352, 2015. Article (CrossRef Link).
[14] Li, J., et al., "Ciphertext-Policy Attribute-Based Encryption with Hidden Access Policy and Testing," *Ksii Transactions on Internet & Information Systems*, vol. 10, no. 7, 2016. Article (CrossRef Link).
[15] Jiang, Y., et al., "Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts," *International Journal of Information Security*, pp. 1-13, 2017. Article (CrossRef Link).
[16] Guan, Z., et al., "Conditional Ciphertext-Policy Attribute-Based Encryption Scheme in Vehicular Cloud Computing," *Mobile Information Systems*, pp. 1-10, 2016. Article (CrossRef Link).
[17] Malluhi, Q.M., V.C. Trinh, and V.C. Trinh, "A Ciphertext-Policy Attribute-based Encryption Scheme With Optimized Ciphertext Size And Fast Decryption," in *Proc. of ACM on Asia Conference on Computer and Communications Security*, 2017. Article (CrossRef Link).
[18] Ostrovsky, R., A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. of Ccs 07 Acm Conference on Computer & Communications Security*, 2007. Article (CrossRef Link).
[19] Naor, M. and B. Pinkas, "Efficient trace and revoke schemes," *International Journal of Information Security*, vol. 9, no. 6, pp. 411-424, 2010. Article (CrossRef Link).
[20] Sadikin, R., S.J. Moon, and Y.H. Park, "Ciphertext Policy-Attribute Based Encryption with Non Monotonic Access Structures," *Journal of The Institue of Elcetronic Engineers of Korea*, vol. 50, no. 9, p. 21-31, 2013. Article (CrossRef Link).
[21] Yamada, S., et al., "A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption," *2014: Springer Berlin Heidelberg*, p. 275-292, 2014. Article (CrossRef Link).
[22] Wang, Y., et al., "CP-ABE Based Access Control for Cloud Storage," *2017: Springer International Publishing*, 2017. Article (CrossRef Link).
[23] Waters, B., "Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions," in *Proc. of International Cryptology Conference on Advances in Cryptology*, 2009. Article (CrossRef Link).
[24] Okamoto, T. and K. Takashima, "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption," in *Proc. of CRYPTO*, 2010. Article (CrossRef Link).
[25] Lewko, A., et al, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *Proc. of Advances in Cryptology - EUROCRYPT 2010, International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, 2010. Article (CrossRef Link).
[26] Lewko, A. and B. Waters, "New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques," *2012: Springer Berlin Heidelberg*, p. 180-198, 2012. Article (CrossRef Link).
[27] Yang, X., et al, "Fully Secure Attribute-Based Encryption with Non-monotonic Access Structures," in *Proc. of International Conference on Intelligent NETWORKING and Collaborative Systems*, 2013. Article (CrossRef Link).

Dan Yang received B.S. degree in Information Security from Xi'an University of Posts & Telecommunications, Xi'an, China in 2014. She is currently pursuing M.S. degree in Cryptography in Xidian University, Xi'an, China. Her research interests include cryptography, information security and network security.

Professor Baocang Wang received his PhD from Xidian University in 2006. He is currently a full professor and PhD supervisor at Xidian University, Xi'an City, Shaanxi Province, China. His current research interest includes post-quantum cryptography, cloud and big data security, number-theoretic algorithms. He has published over 50 research papers.

Xuehua Ban received B.S. degree in Mathematics and Applied Mathematics from Ningxia University, Yinchuan, China in 2014. She is currently pursuing M.S. degree in Cryptography in Xidian University, Xi'an, China. Her research interests includeattribute-based encryption and obfuscation.