A Key-Policy Attribute-based Encryption Scheme for General Circuit from Bilinear Maps

Peng Hu and Haiying Gao
(Corresponding author: Haiying Gao)
Information and Technology Institute
No.62, Science Avenue, National High and New Technology
Industries Development Zone, Zhengzhou, Henan 450001, P. R. China
(Email: hupeng007@126.com)
(Received Oct. 6, 2016; revised and accepted Feb. 1 & Feb. 19, 2017)

Abstract

By access structure and attribute set, attribute-based encryption realizes fine-grained access control and one to many encryption. The expression of access structure directly decides the application range of one scheme and the general circuit reaches the best form. Since the safety of multilinear maps is suffered question, using relatively efficient and safe bilinear maps to construct circuit attribute-based encryption becomes popular. In this paper, we first propose a method that can convert any monotone circuit to an equivalent access tree. Then based on it, we propose a key-policy attribute-based encryption for general circuit from bilinear maps. Moreover, combining exiting method that can convert any access tree into LSSS structure and plenty of well-developed LSSS schemes, we can directly obtain corresponding circuit schemes. Compared with currently scheme from bilinear maps, our work is more efficient and expandable. In the standard model, selective security of our scheme is proved under the decisional bilinear Diffie-Hellman assumption.

Keywords: Attribute-based Encryption; Access Tree; Bilinear Maps; General Circuit; Selective Security

1 Introduction

With the Internet more and more developed, the application of cloud storing and cloud computing are more and more widely. And the security problem also becomes more and more serious [3, 21]. In traditional public key encryption, the message is encrypted to a specific individual. The efficiency becomes extremely low when sharing a message with multi users. Attribute-Based Encryption (ABE) as a new type public key primitive realizes one to many encryption and fine grand access control.

Sahai and Waters [18] proposed the concept of ABE in EUROCYPT 2005. Different with traditional public key encryption, there are attribute set and access structure in encryption and key generation phase. And according to the position, the ABE can be divided into two types: when attribute set associate with ciphertext and access structure associate with private key, it is called Key-Policy ABE (KP-ABE); when attribute set associate with private key and access structure associate with ciphertext, it is called Ciphertext-Policy ABE (CP-ABE). Only when attribute set satisfy access structure, the user can decrypt the encrypted message. In 2006, Goyal et al. [10] proposed the first KP-ABE scheme, and the access structure of this scheme is access tree with highly efficient secret sharing approach.

How to improve the expression of the access structure is an important research field in ABE, and the progress of the improvement is really slow. After first access tree ABE was proposed in 2006, Lewko and Waters [12] converted it into Linear Secret Sharing Scheme (LSSS) as access structure until 2011. In 2013, Garg et al. [9] utilized the multilinear maps [8] built in ideal lattice to construct a KP-ABE scheme that supported general circuit as access structure. The general circuit can express any fixed running time program and reach the strongest expression in ABE [23]. After that, Tiplea et al. [20] proposed the first circuit KP-ABE scheme from bilinear maps. Until now, it is still the only one work that achieves the general circuit by bilinear maps. Recently, Hu and Jia [11] pointed out that the multilinear maps they used are not safe and gave a valid attack. Therefore, we build the scheme on mature bilinear maps and its assumption.

2 Related Work

Unlike other fast developing branches in the ABE system, the most important one which aim to achieve better expression improves really slowly. The first KP-ABE [10] scheme used access tree as structure in 2006. The access tree can be used to represent any monotone Boolean formulas which is a special case in mono-

tone circuit with limitation of fan-out one for every node. In 2011, [12] proposed a KP-ABE scheme with LSSS as structure, and in their scheme, they proposed a method that can convert any access tree into a LSSS matrix. Due the flexible and efficiency of LSSS, many schemes [1, 7, 13, 14, 15, 16, 17, 22] used LSSS structure to achieve additional property based on [12]. In 2013, [9] explained that the "backtracking attack" was the main barrier to extent access tree's single fan-out into circuit's multi fan-out. And they used level multilinear maps to prevent the attack, but the private key size and computation complexity of paring is extremely high. After that, there appeared many optimization and extensions schemes [4, 5, 6] based on [9]. However, [11] found a weakness on the multilinear maps they used and give a valid attack, leading their scheme unsafe. As for now, there is only one scheme achieved circuit ABE from bilinear maps. But its complexity is still high and has limitation on extension.

In this work, we propose a method that can converts any monotone circuit into a corresponding access tree, and then use the secret sharing method in [10] to construct a KP-ABE scheme. Selective security of our scheme in the standard model is proved under the decisional bilinear Diffie-Hellman assumption. Compared with [20], our scheme do not have extra gate (FANOUT gate) and its components, therefore our scheme is more efficient. More important, combining with the method proposed in [22] that converts any access tree into a corresponding LSSS, we can directly get plenty of circuit schemes with additional property based on current schemes like CP-ABE [24], private key tracing [14, 15], revoke [16], large universe [17], etc.

3 Preliminary

Definition 1. *Access Structure [19]: For a given non-empty finite set U, any non-empty subset S of U is called an access structure definite on U. S is called monotone if for $\forall B \in S$ satisfies:*

$$(\exists A \in S)(A \subseteq B) \Rightarrow B \in S.$$

If a subset of U also belongs to S, it is called authorized set; otherwise, it is called unauthorized set. In ABE scheme, we call the elements of U as attributes.

Definition 2. *Access Tree: An access tree is combined by leaf nodes and gates. Each leaf node has one outgoing wire and associates with one attribute. The gate type is either OR gate (1 of 2 threshold gate) or AND gate (2 of 2 threshold gate) which has two incoming wires and one out going wire.*

Definition 3. *General Circuit [9]: A general circuit is combined by input nodes and gates. Each input node has arbitrary numbers outgoing wires (at least one) and associates with one attribute. The gate type is either OR gate, AND gate which has two incoming wires, or NOT gate which has one incoming wire and one outgoing wire, and those gates can have arbitrary numbers outgoing wires (at least one).*

In our scheme, we use notation $C_x(\Gamma_x)$ to represent a sub-circuit (sub-tree) with root node x, and abuse the subscript r to express entire circuit (tree). For input attribute set A, we use $C_x(A) = 1$ ($\Gamma_x(A) = 1$) to represent A satisfy sub-circuit (sub-tree) $C_x(\Gamma_x)$, and $C_x(A) = 0(\Gamma_x(A) = 1)$ to represent it is not. We use tuple (w, w_1, w_2) to represent a node w and its left and right child nodes w_1, w_2, and use $S(w), R(w)$ to represent the sharing attaches and recovery value to outgoing wires of node w respectively.

Definition 4. *Monotone Circuit [9]: A general circuit is monotone if it does not have any NOT gate.*

Like [9] said, we can use De Morgan's rule to convert any general circuit into an equivalent circuit with NOT gates only appear at input level, and above is a monotone one. Then we combine those NOT gates with attributes associated in input nodes. Therefore, we just consider monotone circuit in the scheme. In circuit or access tree, if the number of a node's outgoing wire is one, we call it a single fan-out node; otherwise we call it a multi fan-out node.

3.1 Definition for Circuit KP-ABE

There are four algorithms in a KP-ABE scheme for circuit, including three probabilistic polynomial-time (PPT) algorithms and one deterministic polynomial-time (DPT) algorithm as follows:

Setup$(\lambda, n) \rightarrow (PP, MSK)$**:** The setup is a PPT algorithm. It inputs the security parameter λ and number of system attribute n. It outputs the public parameters PP and master secret key MSK.

Encrypt$(PP, A, m) \rightarrow CT$**:** The encryption is a PPT algorithm. It inputs the public parameters PP, an attribute set A and a message m. It outputs ciphertext CT.

KeyGen$(MSK, C) \rightarrow PK$**:** The key generation is a PPT algorithm. It inputs the master secret key MSK and a circuit C. It outputs private key PK.

Decrypt$(PK, E) \rightarrow m/\perp$ **:** The decryption is a DPT algorithm. It inputs private key PK and a ciphertext CT. It outputs a message m or the special symbol $\perp$.

3.2 Security Model for Circuit KP-ABE

The selective security model of circuit KP-ABE can be seen as a game between a challenger and an attacker. At the end, the attacker will give a guess. If the guess is right, the attacker wins the game; otherwise, the challenger wins.

Init. The attacker declares the attribute set A^*.

Setup. The challenger runs the Setup algorithm, then publishes the public parameters PP, and keeps the master secret key MSK.

Phase 1. The attacker requests any polynomial number times private key queries for any circuit C under the limitation that $C(A^*) = 0$, and the challenger return the corresponding private key to the attacker.

Challenge. The attacker issues two equal length messages m_0, m_1, then challenger flips a random bit $b \in \{0, 1\}$, and return the corresponding ciphertext to the attacker.

Phase 2. Same as the **Phase 1**.

Guess. The attacker gives a guess b' of b. The advantage of the attacker in the game is defined by $\Pr[b = b'] - \frac{1}{2}$.

Definition 5. *Selective Security: If for all PPT attackers at most have a negligible advantage in above game, we call this circuit KP-ABE scheme is selective secure.*

3.3 Bilinear Maps and Assumption

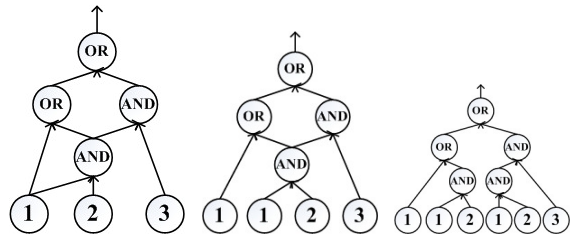
Definition 6. *Bilinear Maps [2]: For two multiplicative cyclic group of prime order p G_1, G_2 with generator g of G_1 and a map $e : G_1 \times G_1 \to G_2$. We call e is a bilinear map and G_1 is bilinear group if they satisfy:*

1) *Bi-linearity: for all $u, v \in G_1$ and $a, b \in Z_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$;*
2) *Non-degeneracy: $e(g, g) \neq 1$;*
3) *Computable: the group operation in G_1 and map e are both efficiently computable.*

Definition 7. *Decisional Bilinear Diffie-Hellman (DBDH) Assumption: Given two bilinear groups G_1, G_2 and $g, g^a, g^b, g^c, e(g, g)^{abc}, e(g, g)^z$ (a, b, c, z are randomly chosen from Z_p), there is no polynomial-time algorithm can distinguish $e(g, g)^{abc}$ and a random element $e(g, g)^z$ in G_1.*

4 Circuit Conversion

The secret sharing of our scheme is based on [10]. But because of "backtracking attack", it cannot directly used in circuit. Therefore, our idea is to convert each multi fan-out node into equivalent form of several single fan-out nodes, and then use the method in [10] to build a KP-ABE scheme while still resists attack. Our conversion's direction is in a bottom up direction in circuit. For a node x with fan-out $l (l \geq 2)$, we use l copies of sub-circuits C_x but only has single fan-out for root node, to replace the original sub-circuit C_x. Then move to the next node. For better understanding, we give a simple example in Figure 1(abc). As shown in Figure 1(a), there are two multi fan-out nodes, and we first use two nodes 1 with single fan-out to link its two parents which turns into Figure 1(b). Then we use same method to convert AND gate in upper level and get circuit in Figure 1(c). We can easily find that Figure 1(a) and 1(c) are equivalent.



(a) Original circuit (b) Step 1 (c) Step 2

Figure 1: Circuit conversion

Here we explain why our scheme can resist the "backtracking attack". The attack only takes place in multi fan-out gate that its outgoing wire links to an OR gate. As we can see in Figure 2, due to the sharing of incoming wires in OR gate and outgoing wires in multi fan-out gate (marked as X) are equal. When someone knows the left wire's sharing of OR gate, it can directly know the left wire's sharing of AND gate even though the multi fan-out gate is not satisfied and its sharing of outgoing wires is not supposed to know. In our scheme, we convert all multi fan-out gates to single fan-out. And in secret sharing phase, we attach different sharing to those wires; therefore the attacker cannot use the multi fan-out as bridge to attack other gates.

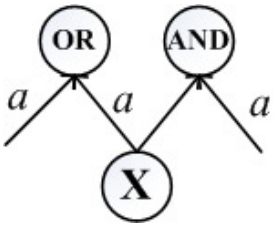


Figure 2: Backtracking attack

5 Our Construction

Setup(λ, n)**:** In system setup phase, it inputs the security parameter λ to choose prime p and number of attributes n to choose attribute universe $U = \{1, \cdots, n\}$. Then it generates two bilinear groups G_1, G_2 with order p and a bilinear map $e : G_1 \times G_1 \to G_2$. Suppose the generator of G_1 is g. At last, it randomly chooses $y \in Z_p$, $t_i \in Z_p$ for every $i \in U$ and publishes the public parameters:

$$PP = \left(Y = e(g, g)^y, \left(T_i = g^{t_i} | i \in U\right)\right) \quad (1)$$

keeps the master secret key:

$$MSK = (y, t_1, \cdots, t_n) \quad (2)$$

Encrypt(m, A, PP)**:** In encryption phase, it inputs the public parameters PP, an attribute set $A \subseteq U$ and a message $m \in G_2$. Then it randomly chooses $s \in Z_p$ and outputs the ciphertext:

$$\begin{aligned} CT &= (A, g^s, E', E_i) \\ E' &= me(g,g)^{ys} \\ E_i &= T_i^s = g^{st_i} | i \in A. \end{aligned}$$

KeyGen(C, MSK)**:** In key generation phase, it inputs the master secret key MSK and a circuit C. Then it converts the circuit C into an equivalent access tree. After that, it sets $S(r) = y$ for the root node and shares the y in a top down manner as follows:

OR gate (w, w_1, w_2)**:** If $S(w) = \delta$, then it sets:

$$S(w_1) = S(w_2) = \delta.$$

AND gate (w, w_1, w_2)**:** If $S(w) = \delta$, then it randomly chooses $\varphi \in Z_p$ and sets:

$$\begin{aligned} S(w_1) &= \varphi, \\ S(w_2) &= \delta - \varphi. \end{aligned}$$

Finally, it generates the private key at each leaf node by the sharing it gets. For each leaf node x and its attached attribute t_x, it outputs the private key:

$$SK = \{SK_x = g^{S_x/t_x}\}.$$

Decryption(CT, PK)**:** In decryption phase, it inputs the ciphertext CT with structure Γ and user's private key PK with attribute set A. Then it does the follow to calculate the message:

Leaf node (w)**:** If $\Gamma_w(A) = 1$, it calculates:

$$\begin{aligned} R(w) &= e(SK_x, E_x) \\ &= e\left(g^{S_x/t_x}, g^{st_x}\right) \\ &= e(g,g)^{sS_x}. \end{aligned}$$

AND gate (w, w_1, w_2)**:** If $\Gamma_w(A) = 1$, it calculates:

$$\begin{aligned} R(w) &= R(w_1) \cdot R(w_2) \\ &= e(g,g)^{\varphi s} e(g,g)^{\delta s - \varphi s} \\ &= e(g,g)^{\delta s}. \end{aligned}$$

OR gate (w, w_1, w_2)**:** If $\Gamma_w(A) = \Gamma_{w_1}(A) = 1$, it sets:

$$R(w) = R(w_1).$$

Or if $\Gamma_w(A) = \Gamma_{w_2}(A) = 1$, it sets:

$$R(w) = R(w_2).$$

Finally, it will get $Y = e(g,g)^{ys}$ at the root node if $\Gamma(A) = 1$, and get message $m = E'/Y$.

6 Security Proof

In this section, we give the security proof of our KP-ABE scheme by DBDH assumption under the standard model. As described in Section 3.2, it is a game between a poly-time attacker and a challenger.

Theorem 1. *If there exists a poly-time attacker who can break our KP-ABE scheme with advantage ε, the challenger can solve the DBDH problem with advantage $\varepsilon/2$.*

Proof. The challenger first receives an instance of a BDHE assumption, which includes (g^a, g^b, g^c, T) and the challenger will decide whether $T = e(g,g)^{abc}$ or $T = e(g,g)^z$. Next it will use the attacker's ability to solve the problem.

Init. The attacker announces the challenge attribute set A^*.

Setup. The challenger sets $Y = e(g^a, g^b) = e(g,g)^{ab}$, then it randomly chooses r_i for all $i \in U$ and sets:

$$T_i = \begin{cases} g^{r_i}, i \in A^* \\ g^{br_i}, i \notin A^* \end{cases}$$

Finally it publishes the public parameters:

$$\begin{aligned} PP &= (p, G_1, G_2, g, e, n, Y, T_i) \\ Y &= e(g,g)^y \\ T_i &= g^{t_i} | i \in U. \end{aligned}$$

Phase 1. The attacker can submit any poly numbers circuits with limitation $C(A^*) = 0$. After receiving the circuit, the challenger converts it into access tree Γ and starts the secret sharing procedure.

The challenger first implicitly sets $y = S(r) = ab$ for the root node and sharing y by access tree in a top down manner as following (note that for a node w, if $\Gamma_w(A^*) = 0$, the sharing form of its outgoing wire would be an element in Z_p; otherwise it would be an element in G_1).

OR gate (w, w_1, w_2)**:** Suppose $S(w) = L$, it sets:

$$S(w_1) = S(w_2) = \delta.$$

AND gate (w, w_1, w_2)**:** Suppose $S(w) = L$, it first randomly chooses $K \in Z_p$. Then if $\Gamma_w(A^*) = \Gamma_{w_1}(A^*) = \Gamma_{w_2}(A^*) = 1$, it sets:

$$\begin{aligned} S(w_1) &= K, \\ S(w_2) &= L - K. \end{aligned}$$

If $\Gamma_w(A^*) = 0, \Gamma_{w_1}(A^*) = 1, \Gamma_{w_2}(A^*) = 0$, it sets:

$$\begin{aligned} S(w_1) &= K, \\ S(w_2) &= L/g^K. \end{aligned}$$

If $\Gamma_w(A^*) = 0, \Gamma_{w_1}(A^*) = 0, \Gamma_{w_2}(A^*) = 1$, it sets:

$$\begin{aligned} S(w_1) &= L/g^K \\ S(w_2) &= K. \end{aligned}$$

If $\Gamma_w(A^*) = \Gamma_{w_1}(A^*) = \Gamma_{w_2}(A^*) = 0$, it sets:

$$\begin{aligned} S(w_1) &= g^K, \\ S(w_2) &= L/g^K. \end{aligned}$$

For each leaf node, it sets:

$$SK_x = \begin{cases} (g^b)^{S(x)/r_i}, x \in A \\ S(x)^{1/r_i}, x \notin A \end{cases}$$

At last, the challenger sends the private key $SK = \{SK_x\}$ to the attacker.

Challenge. The attacker submits two equal length messages m_0, m_1 to the challenger. Then the challenger flips a random coin $b \in \{0,1\}$ and outputs the following ciphertext to the attacker:

$$E = (A^*, E' = m_v T, \{E_i = g^{cr_i}\}_{i \in A^*}).$$

Phase 2. This phase is same as **Phase 1**.

Guess. The attacker gives a guess b' about b. If $b' = b$, the challenger decides $T = e(g,g)^{abc}$; otherwise, it decides $T = e(g,g)^z$.

Next, we calculate the advantage that challenger has. We use $\Pr[C]$ to represent the probability that the challenger's decision is right, use $\Pr[C_{abc}]$ to represent the probability that the challenger decide $T = e(g,g)^{abc}$ and use $\Pr[C_z]$ to represent the probability that challenger decides $T = e(g,g)^z$. Suppose the attacker can break this scheme with advantage ε, then:

$$\begin{aligned} \Pr[C] &= \Pr[C_{abc}|T = e(g,g)^{abc}] \\ &\quad \cdot \Pr[T = e(g,g)^{abc}] \\ &\quad + \Pr[C_z|T = e(g,g)^z] \cdot \Pr[T = e(g,g)^z] \\ &= \Pr[b' = b|T = e(g,g)^{abc}] \\ &\quad \cdot \Pr[T = e(g,g)^{abc}] \\ &\quad + \Pr[b \neq b|T = e(g,g)^z] \cdot \Pr[T = e(g,g)^z] \\ &= \frac{1}{2}\left(\frac{1}{2} + \varepsilon\right) + \frac{1}{2} \times \frac{1}{2} \\ &= \frac{1}{2} + \frac{\varepsilon}{2}. \end{aligned}$$

□

7 Efficiency Analysis

In this section, we give the efficiency analysis by comparing our scheme with [20] since it is the only one work that achieved circuit ABE from bilinear maps. The efficiency of [20] and our scheme both rely on the distribution and numbers of multi fan-out nodes in circuit. Therefore, we give the comparison in a more concrete circuit as follows.

Table 1: Private key size in [20] and our scheme

Scheme	Worst case	Best case
[20]	$nj + n + j^r$	$nj + n + r\,(j-1)$
Our	$n + j^r$	$n + r\,(j-1)$

Suppose there are n input nodes, r multi fan-out nodes all with j outgoing wires. The best case in both [20] and our is that there is no path between any two multi fan-out nodes, and the private key size of [20] is $nj + n + r\,(j-1)$ and our is $n + r\,(j-1)$. The worst case is that there is a path through all multi fan-out nodes, and the private key size of [20] is $nj + n + j^r$ and our is $n + j^r$. The private key size is between this two in other cases. We give a summary in the Table 1. The private key size also means the paring times in decryption phase, therefore our scheme is more efficiency than [20].

8 Conclusion

In this work, we first propose a method that can convert any monotone circuit into an equivalence access tree, and then based on that, we propose a KP-ABE scheme for general circuit from bilinear maps that can resist "backtracking attack", and prove its selective security under DBDH assumption in standard model. Compared with the only one circuit KP-ABE from bilinear, our scheme is more efficient than that. More important, based on existing method that can convert any access tree into LSSS matrix and plenty of efficient LSSS ABE schemes with different additional property, we can directly obtain the corresponding circuit ABE schemes.

Currently, multilinear maps are not safe and the complexity of circuit ABE from bilinear maps are still too high for practical use. How to optimize the secret sharing procedure for circuit still need further research.

Acknowledgments

The authors would like to thank the anonymous reviewers of this paper for their valuable comments and suggestions. This work was sponsored in part by the National Natural Science Foundation of China [Grant No.61272041, Grant No.61601515], Foundation of Science and Technology on Information Assurance Laboratory [Grant No.KJ-15-006] and Fundamental and Frontier Technology Research of Hennan Province (Grant No.162300410192).

References

[1] B. Balusamy, P. V. Krishna, G. S. T. Arasi, and V. Chang, "A secured access control technique for cloud computing environment using attribute based hierarchical structure and token granting system," *International Journal of Network Security*, vol. 19, no. 4, pp. 559–572, 2017.

[2] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (CRYPTO'01)*, pp. 213–229, California, USA, Aug. 2001.

[3] Z. Cao, C. Mao, L. Liu, "Analysis of one secure anti-collusion data sharing scheme for dynamic groups in the cloud," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 68–72, 2016.

[4] P. Datta, R. Dutta, and S. Mukhopadhyay, "Compact attribute-based encryption and signcryption for general circuits from multilinear maps," in *Progress in Cryptology (INDOCRYPT'15)*, pp. 3–24, India, Dec. 2015.

[5] P. Datta, R. Dutta, and S. Mukhopadhyay, "General circuit realizing compact revocable attribute-based encryption from multilinear maps," in *18th International Conference on Information Security (ISC'15)*, pp. 336–354, Norway, Sept. 2015.

[6] C. C. Dragan and F. L. Tiplea, "Key-policy attribute-based encryption for general boolean circuits from secret sharing and multi-linear maps," in *Second International Conference on Cryptography and Information Security in the Balkans*, pp. 112–133, Slovenia, Sept. 2015.

[7] X. B. Fu, S. K. Zeng, and F. G. Li, "Blind expressive ciphertext policy attribute based encryption for fine grained access control on the encrypted data," *International Journal of Network Security*, vol. 17, no. 6, pp. 661–671, 2015.

[8] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices," in *Advances in Cryptology (EUROCRYPT'13)*, pp. 1–17, Greece, May 2013.

[9] S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters, "Attribute-based encryption for circuits from multilinear maps," in *Advances in Cryptology (CRYPTO'13)*, pp. 479–499, CA, USA, Aug. 2013.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06)*, pp. 89–98, Alexandria, VA, USA, 2006.

[11] Y. P. Hu and H. W. Jia, "Cryptanalysis of GGH map," in *Advances in Cryptology (EUROCRYPT'16)*, pp. 537–565, Vienna, Austria, May 2016.

[12] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology (EUROCRYPT'11)*, pp. 568–588, Tallinn, Estonia, May 2011.

[13] Q. Y. Li and F. L. Zhang, "A fully secure attribute based broadcast encryption scheme," *International Journal of Network Security*, vol. 17, no. 3, pp. 255–263, 2015.

[14] Z. Liu, Z. F. Cao, and D. S. Wong, "Fully collusion-resistant traceable key-policy attribute-based encryption with sub-linear size ciphertexts," in *10th International Conference on Information Security and Cryptology*, pp. 403–423, Beijing, China, Dec. 2014.

[15] J. T. Ning, X. L. Dong, Z. F. Cao, L. F. Wei, and X. D. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1274–1288, 2015.

[16] T. Okamoto and K. Takashima, "Fully secure unbounded inner-product and attribute-based encryption," in *Advances in Cryptology (ASIACRYPT'12)*, pp. 349–366, Beijing, China, Dec. 2012.

[17] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in *ACM SIGSAC Conference on Computer and Communications Security (CCS'13)*, pp. 463–474, Berlin, Germany, Nov. 2013.

[18] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology (EUROCRYPT'05)*, pp. 457–473, Aarhus, Denmark, May 2005.

[19] D. R. Stinson, *Cryptography: Theory and Practice.(3ed, in English)*, Britain: Chapman and Hall, 2005.

[20] F. L. Tiplea and C. C. Dragan, "Key-policy attribute-based encryption for boolean circuits from bilinear maps," in *First International Conference on Cryptography and Information Security in the Balkans*, pp. 175–193, Istanbul, Turkey, Oct. 2014.

[21] Z. Wang, Y. Lu, G. Sun, "A policy-based deduplication mechanism for securing cloud storage," *International Journal of Electronics and Information Engineering*, vol. 2, no. 2, pp. 70–79, 2015.

[22] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *14th International Conference on Practice and Theory in Public Key Cryptography (PKC'11)*, pp. 53–70, Taormina, Italy, Mar. 2011.

[23] B. Waters, "Functional encryption: Origins and recent developments," in *16th International Conference on Practice and Theory in Public-Key Cryptography (PKC'13)*, pp. 51–54, Nara, Japan, Feb. 2013.

[24] J. Xu, Q. Y. Wen, W. M. Li, and Z. P. Jin, "Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing," *IEEE Transactions on Parallel Distributed Systems*, vol. 27, no. 1, pp. 119–129, 2016.

Biography

Peng Hu received his BS degree in information security from Zhengzhou Information and Technology Institute, Hennan, China, in 2014. He is currently a postgraduate student in Zhengzhou Information and Technology Institute. His current research interests include cryptography and information security.

Haiying Gao received her BS degree in mathematics from Hennan university, Hennan, China, in 1999. She received her MS degree in information security from Zhengzhou Information and Technology Institute, Hennan, China, in 2003, and her PhD from Xidian University, Shanxi, China, in 2006. She is currently a professor with the Zhengzhou Information and Technology Institute, Hennan, China. Her research interest focuses on cryptology theory.