Attribute-Based Certificateless Cryptographic System

Guoyan Zhang
1. School of Computer Science and Technology, Shandong University
2. Cryptologic Technology and Information Security, Ministry of Education, Shandong University,
3. Institute of Information Science and Technology, Shandong University of Political Science and Law,
Jinan, China
Email: guoyanzhang@sdu.edu.cn

***Abstract*—As an extension of identity-based encryption scheme, attribute-based encryption scheme also has the key escrow problem. Multi-authority attribute-based encryption schemes are principal solution, but it is at the cost of the introducing extra infrastructure and communication.**
This paper introduces the concept of attribute-based certificatless encryption system (ABCE), which is a new approach to mitigate the key escrow problem in attribute-based encryption scheme. In ABCE, the user can choose his own secret key that the KGC cannot obtain. In contrast to attribute-based encryption scheme under multiple authorities, our approach needs less extra cost. Following, we give a generic construction and an improvement in the efficiency.

***Index Terms*—certificateless cryptography, attribute-based encryption, k -sibling interactive function family, one-way function.**

I. Introduction

Sahai and Waters [2] introduced the concept of attribute-based encryption (ABE). Two variants of ABE were subsequently proposed. In the key-policy variant (KP-ABE) of Goyal, Pandey, Sahai and Waters (GPSW)[3], every ciphertext is associated with a set of attributes, and every user secret key is associated with a threshold access structure on attributes. Decryption is enabled if and only if the ciphertext attribute set satisfies the access structure on the user secret key. In the ciphertext-policy variant (CP-ABE) of Bethencourt, Sahai and Waters (BSW) [4], the situation is reversed: attributes are associated with user secret keys and access structures with ciphertexts. Following, in order to make the access structure more expressive, many schemes have been presented [2, 3, 5, 6, 7, 8, 9, 10]. Simultaneously, schemes [7, 11, 12, and 13] are devoted to get constant-size ciphertexts.

Similar to identity-based encryption schemes, the KGC is able to compute the private key corresponding to any attribute, and he is free to engage in malicious activities without any risk of being confronted in a court of law. The malicious activities could include: decrypting and reading messages meant for any user, which is called the key escrow problem. One approach to mitigate the key escrow problem is to employ multi-authority attribute-based encryption, which allow the sender to specify for each authority k a set of attributes monitored by that authority and a number d_k so that the message can be decrypted only by a user who has at least d_k of the given attributes from every authority. Multi-authority attribute-based encryption is an attractive solution and successfully avoids placing trust in a single entity by making the system distributed. However, it is burdensome for a user to go to several key authorities, prove his attributes to each of them and get the corresponding private key component (which has to be done over a secure channel). Building on the ideas from [14], Chase proposed a solution for multi-authority attributes-based encryption, provided that a trusted central authority is available [15], but a global identifier is a "linchpin" for tying users' keys together. Her system relied on a central authority and was limited to expressing a strict “AND” policy over a pre-determined set of authorities. M$\ddot{u}$ller, Katzenbeisser, and Eckert [16, 17] give a system with a centralized authority that realizes any LSSS access structure. Their construction builds on the Waters system; their proof is limited to non-adaptive queries. The system achieves roughly the same functionality as the engineering approach above, except one can still acquire attributes from additional authorities without revisiting the central authority. The scheme [18] removed the central authority using a distributed PRF; However, the same limitations of an AND policy of a determined set of authorities remained. Lin ET. al. [17] gives a threshold-based scheme that is also somewhat decentralized. The set of authorities is fixed ahead of time, and they must interact during the system setup. The system is only secure up to collusions of m users, where m is a system parameter chosen at setup such that the cost of operations and key storage scales with m . Scheme [19] proposes a new multi-authority attribute-based encryption system. In their system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. Reference [20] gave attribute- based threshold signature scheme without a trusted central authority.

doi:10.4304/jcp.9.1.72-77

II. PRELIMINARIES

In this section, we give the related preliminaries:

Definition. *k* ***-Sibling Intractable Function Families***

Let $k = k(n)$ be a polynomial with $k \geq 1$. Let $H = \{H_n, n \in N\}$, where $H_n = \{h_n \mid h_n : \sum^{l(n)} \to \sum^{m(n)}\}$, be a family of functions that is one-way, polynomial time computable and samplable, and that has the collision accessibility property. Also let $X = \{x_1, x_2, \ldots, x_i\}$ be any set of i initial strings, where $1 \leq i \leq k$. H is a k-sibling intractable function family, or simply k-SIFF, if for each $1 \leq i \leq k$, for each sibling finder F, for each polynomial Q, and for all sufficiently large n,

$$\Pr\{F(X,h) \neq ?\} < \frac{1}{Q(n)} \quad (1)$$

Where h is chosen randomly and uniformly from $H_n^X \subset H_n$ the set of all functions in H_n that map $x_1, x_2, \ldots, x_i$ to the same strings in $\sum^{m(n)}$, and the probability $\Pr\{F(X,h) \neq ?\}$ is computed over H_n^X and the sample space of all finite strings of coin flips that F could have tossed.

To figure axis labels, use words rather than symbols. Do not label axes only with units. Do not label axes with a ratio of quantities and units. Figure labels should be legible, about 9-point type.

Color figures will be appearing only in online publication. All figures will be black and white graphs in print publication.

III. DEFINITION AND SECURITY MODEL

A. Definition

Refer to certificateless public key cryptography introduced by Al-Riyami and Paterson [1], we give two definitions about the vary types of attribute-based encryption :

Definition 1. Ciphertext-Policy Attribute-Based Certificateless Encryption Scheme.

A generic ciphertext-policy attribute-based certificateless encryption scheme consists of the following seven algorithms:

-SetUp: a probabilistic polynomial time (PPT) algorithm run by a key generation center (KGC) given a security parameter k and a universe of attributes U as input which outputs a randomly chosen master secret key *msk* and master public key *mpk* . The master public key *mpk* includes a description of the message space M and ciphertext space C.

-PartialPrivateKeyExtract: given the master public key *mpk* , master secret key *msk* and an attributes set $S \in U$ for entity A, the KGC runs this PPT algorithm to generate the partial private key d_A for the attributes set S ,Then the partial private key d_A is transported to entity A over a confidential and authentic channel.

-SetSecretValue: a PPT algorithm runs by the entity A given master public key *mpk* and his attributes set $S \in U$ as inputs which output a secret value x_A.

-SetPrivateKey: given master public key *mpk* , the entity A's secret value x_A, and the entity A's partial private key d_A as input, the entity runs this PPT algorithm to generate a private key SK_A.

-SetPublicKey: given master public key *mpk* and the entity A's secret value x_A , and output a public key PK_A for the entity A.

-Encrypt: given a plaintext $m \in M$, master public key *mpk* , an access tree T over the universe of attributes U and public keys list $PK_{A_1}, PK_{A_2}, \cdots, PK_{A_n}$ for an entity $A_1, A_2, \cdots, A_n$ as inputs, a sender runs this PPT algorithm to create a ciphertext $c \in C$ or the null symbol $\perp$ indicating an encryption failure.

-Decrypt: given master public key *mpk* , the entity's private key SK_A , and the ciphertext $c \in C$ that was encrypted under the access tree T as inputs, the entity as a recipient runs this deterministic algorithm to get a decryption δ , which is a plaintext message if the set S of attributes satisfies the access tree T .

Definition 2. Key-Policy Attribute-Based ertificateless Encryption

The definition is similar to the ciphertext-policy attribute-based certificateless encryption scheme, and we omit here.

B. Security Model

The following gives the security model for attribute-based certificateless encryption scheme:

In order to simulate the attack environment conveniently, we adopt the challenger C and adversary A model. Two kinds of adversaries are considered in the model. One is Type I adversary who cannot know the KGC's master secret key, but can replace any public key in publickeylist with other public keys he chooses. Another is Type II adversary who knows the KGC's master secret key and may still obtain full private keys for arbitrary attributes sets, but is disallowed to replace public key during the game.

In order to simulate the attack environment conveniently, we adopt the challenger C and adversary A model. Two kinds of adversaries are considered in the model. One is Type I adversary who cannot know the KGC's master secret key, but can replace any public key in publickeylist with other public keys he chooses. Another is Type II adversary who knows the KGC's master secret key and may still obtain full private keys for arbitrary attributes sets, but is disallowed to replace public key during the game.

Definition 3. IND-CPA Secure against Type I Adversary for Ciphertext-Policy Attribute-Based Certificateless Encryption.

A ciphertext-policy attribute-based certificateless encryption scheme is IND-CPA secure against Type I adversary if no PPT adversary A of Type I has a non-negligible advantage in the following game played against the challenger:

- A is a Type I attacker, the challenger takes a security parameter k and runs the setup algorithm. It gives A the master public key mpk, and keeps the master secret key msk to itself.
- A is given access to the following oracles:

-Public-Key-Request-Oracle: with master public key mpk as input, C chooses a random PK in publickeylist and returns it.

-Public-Key-Replace-Oracle: with a valid public key PK as input, C replaces any one of the public key in publickeylist with PK.

-Partial-Private-Key-Extract-Oracle: with attributes set S, master public key mpk, and master secret key msk as input, C searches the PartialPrivateKeylist, and returns d_S, if S is in the list. Else, he computes d_S = PartialPrivateKeyExtract (mpk, msk, S), adds $< S, d_S >$ to PartialPrivateKey list and returns it to A.

-Secret-Value-Extract-Oracle: with a public key PK as input, C returns the corresponding secret value x.

- After making the oracle queries a polynomial number of times, A outputs and submits two messages (M_0, M_1), together with a challenge access tree T. The challenger C picks a random bit $b \in \{0,1\}$ and computes c, the encryption of M_b, for the current publickeylist and access tree T. If the output of the encryption is $\perp$, then A immediately losses the game. Otherwise C is delivered to A.
- A makes a new sequence of queries as in step 2.
- A outputs a bit b. It wins if $b' = b$ and fulfills the following conditions:

- At any time, the set S satisfying the access tree T has not been queried in -Partial-Private-Key-Extract-Oracle with any query of -Public-Key-Replace-Oracle.

Define the guessing advantage of A as

$$Adv_{ABCE}^{IND-CPA}(A) \mid \Pr[b' = b] - \frac{1}{2} \mid \qquad (2)$$

A Type I adversary A breaks an IND-CPA secure ABCE scheme with $(t, q_{par}, q_{pub}, q_{sv}, q_{pp}, \varepsilon)$ if and only if the guessing advantage of A that accesses q_{par} times Partial-Private-Key-Extract-Oracle, q_{pub} times Public-Key-Request-Oracle, q_{sv} times Secret-Value-Extract-Oracle and q_{pp} times Public-Key-Replace-Oracle is greater than ε within running time t. The scheme is said to be $(t, q_{par}, q_{pub}, q_{sv}, q_{pp}, \varepsilon)$ -IND-CPA secure against Type I adversary if there is no adversary A that can break the IND-CPA secure with $(t, q_{par}, q_{pub}, q_{sv}, q_{pp}, \varepsilon)$.

Definition 4. IND-CPA Security against Type II Adversary for Ciphertext-Policy Attribute-Based Certificateless Encryption.

A ciphertext-policy attribute-based certificateless encryption scheme is IND-CPA secure against Type II adversary if no PPT adversary A of Type II has a non-negligible advantage in the following game played against the challenger:

- A is a Type II adversary, the challenger C run A with a security parameter k to get the master public key mpk and the master secret key msk to itself.
- A is given access to the following oracles:

-Public-Key-Request-Oracle: with master public key mpk as input, C chooses a random PK in publickeylist and returns it.

-Secret-Value-Extract-Oracle: with a public key PK as input, C returns the corresponding secret value x.

- After making the oracle queries a polynomial number of times, A outputs and submits two messages (M_0, M_1), together with a challenge access tree T. The challenger C picks a random bit $b \in \{0,1\}$ and computes the encryption of M_b for the current publickeylist and access tree T. If the output of the encryption is $\perp$, then A immediately losses the game. Otherwise c is delivered to A.
- A makes a new sequence of queries as in step 2.
- A outputs a bit b. It wins if $b' = b$ and fulfills the following conditions:

- At any time, any public key in the current publickeylist has not been submitted to the Secret-Value-Extract-Oracle.

Define the guessing advantage of A as

$$Adv_{ABCE}^{IND-CPA}(A) \mid \Pr[b' = b] - \frac{1}{2} \mid \qquad (3)$$

A Type II adversary A breaks an IND-CPA secure ABCE scheme with $(t, q_{pub}, q_{sv}, \varepsilon)$ if and only if the guessing advantage of A that accesses q_{pub} times Public-Key-Request-Oracle, q_{sv} times Secret-Value-Extract-Oracle and is greater than ε within running time t. The scheme is said to be $(t, q_{pub}, q_{sv}, \varepsilon)$ -IND-CPA secure against Type II adversary if there is no adversary A that can break the IND-CPA secure with $(t, q_{pub}, q_{sv}, \varepsilon)$

IV. A Generic Construction

A. The Construction

Let $(Setup'; Privatekey'; Encrypt'; Decryption')$ be an IND-CPA secure attribute-based encryption scheme, and (G, E, D) is an IND-CPA secure public key encryption scheme. Let (*SetUp; PartialPrivateKeyExtract; SetSec; SetPriv; SetPub; Encrypt; Decrypt*) be the attribute-based

certificateless encryption scheme from the above attribute-based encryption scheme and the public key encryption scheme , and the construction is as follows:

-SetUp: run *Setup'* of attribute-based encryption scheme to get the master secret key *msk* and master public key *mpk* . The master public key *mpk* includes a description of the ciphertext space C .

-PartialPrivateKeyExtract: given the master public key *mpk* , master secret key *msk* and an attributes set $S \in U$ for entity A , the KGC runs this PPT algorithm *Privatekey'* to generate the partial private key d_A for the attributes set. Then the partial private key d_A is transported to entity A over a confidential and authentic channel.

-SetSec: run G n times to get the corresponding secret values $x_1, x_2, \ldots, x_n$ and public keys $pk_1, pk_2, \ldots, pk_n$, assuming that there are n users. Especially, pk_i includes a description of the message space M .

-SetPriv: the private key SK_A for entity A is composed of the secret value x_A , and the entity A 's partial private key d_A .

-SetPub: The public key PK_A for the entity A is obtained from scheme of SetSec. The system public key is composed of （ *mpk* ， $pk_1, pk_2, \ldots, pk_n$ ）.

-Encrypt: given a plaintext $m \in M$, the ciphertext is

$$c = Encryption'(E_{pk_1}(m) \| E_{pk_2}(m) \| \cdots \| E_{pk_n}(m)) \quad (4)$$

-Decrypt: given master public key *mpk* , the entity's private key $SK_A = (d_A, x_A)$, and the ciphertext $c \in C$, if entity's attributes set satisfying the access tree T related with c (ciphertext-policy attribute-based encryption scheme), or the attributes related with c satisfies the access tree T (key-policy attribute-based encryption scheme), and then he can get the message as follows:

$$m = D_{x_A}(Decryption'_{d_A}(c)) \quad (5)$$

Otherwise outputs $\perp$.

B. Security Analysis

Theorem 1. Our ciphertext-policy attribute-based certificateless encryption scheme is at least as secure as the attribute-based encryption scheme or the public key encryption scheme considering Type I adversary.

Proof: Assuming A_1 is the Type I adversary, and then we can construct an attacker B_1 for attribute-based encryption scheme or an attacker B_2 for public key encryption scheme. Our idea is as follows: B_1 or B_2 simulates the attack environment of A_1 until he attacks attribute-based encryption scheme or public key encryption scheme successively by running A_1 .

Case 1: Attribute-based encryption scheme is IND-CPA secure.

Setup: Given the master public keys, B_1 runs public key scheme n times to get n public-secret key pairs $(pk_i, sk_i), (i = 1, 2, \cdots, n)$, and sends pk_i , with the master public keys *mpk* to A_1 ,

Phase 1. B_1 answers the queries of A_1 as follows:

-Public-Key-Request-Oracle: On receiving the query:

1. B_1 firstly searches PublicKeylist for a public key and returns it.
2. Else, he runs public key scheme to get public-secret key pair (pk_i, sk_i) and returns pk_i as answer.

-Public-Key-Replace-Oracle: On receiving a query pk , B_1 replaces any public key in publickeylist with pk

-Partial-Private-Key-Request-Oracle: On receiving a query $S \in U$:

1. B_1 Searches the PartialPrivateKey List for a tuple $< S, d_A >$ If exist, he returns d_A as answer.
2. Otherwise, B_1 queries the challenge C for S in partial-private-key-request-oracle to get d_A and returns it.

-Secret-Value-Extract-Oracle: with a public key pk as input, C returns the corresponding secret value x .

-Challenge: After making the oracle queries a polynomial number of times, A_1 outputs and submits two messages (M_0, M_1) , together with a challenge access tree T , B_1 sends $M_0 = (E_{pk_1}(m_0) \| E_{pk_2}(m_0) \| \cdots \| E_{pk_n}(m_0))$ $M_1 = (E_{pk_1}(m_1) \| E_{pk_2}(m_1) \| \cdots \| E_{pk_n}(m_1))$ to challenger C , C picks a random bit $b \in \{0,1\}$ and computes c , the encryption of M_b for the current publickeylist and access tree T. If the output of the encryption is $\perp$, then B_1 immediately losses the game. Otherwise c is delivered to B_1 and B_1 returns it to A_1 .

Phase 2. A_1 makes a new sequence of queries as in step 2, and B_1 answer it as phase 1.

A_1 outputs a bit b and B_1 outputs b . It wins if $b' = b$ and fulfills the following conditions:

- At any time, the set S satisfying the access tree T has not been queried in -Partial-Private-Key-Extract-Oracle with any query of -Public-Key-Replace-Oracle.

From the above analysis, we found, the successful probability of B_1 is at least the same to the successful probability of A_1 .

Case 2. If public key encryption scheme is IND-CPA secure, and the attribute-based encryption scheme is not IND-CPA secure. We can prove the successful probability of B_2 attacking the public key encryption is at least the same to A_1 in the light of the above proof method.

The attribute-based certificateless encryption scheme is IND-CPA secure against type $I\!I$ adversary can be proved by the following theorem.

Theorem 2. If the public key encryption scheme is IND-CPA secure, then our ciphertext-policy attribute-based certificateless encryption scheme is IND-CPA secure against Type $I\!I$ adversary.

The security analysis for key-policy attribute-based certificateless encryption scheme is similar to the one of ciphertext-policy attribute-based certificateless encryption scheme.

V. IMPROVEMENT

The scheme from the above section is fit for the small universe of attributes or small group of users. If there are lager universe of attributes or more potential users, the scheme has lower efficiency due to the encryption scheme and more public keys. In this section, we improve on the above attribute-based certificateless encryption scheme by using of k -sibling intractable function families and one-way trapdoor function family.

Let ($(Setup'; Privatekey'; Encryption'; Decryption')$ be an IND-CPA secure attribute-based encryption scheme, $H = \{H_n, n \in N\}$ be a k -sibling intractable function family, where $H_n = \{h_n \mid h_n : \sum^{l(n)} \to \sum^{m(n)}\}$. $G = \{G_n, n \in N\}$ be a pseudo-random function families, where $G_n = \{g_n \mid g_n : \sum^{l(n)} \to \sum^{m(n)}\}$ and $F = \{F_n, n \in N\}$ be a one-way trapdoor function family, where $F_n = \{f_n \mid f_n : \sum^{l(n)} \to \sum^{m(n)}\}$. Let (Setup; PartialPrivateKeyExtract; SetSec; SetPriv; SetPub; Encrypt; Decrypt) be the attribute-based certificateless encryption scheme from the above attribute-based encryption scheme , k-sibling intractable function families and one-way trapdoor function, and the construction is as follows:

-SetUp: run $Setup'$ of attribute-based encryption scheme to get the master secret key msk and master public key mpk . The master public key mpk includes a description of the ciphertext space C .

-PartialPrivateKeyExtract: given the master public key mpk , master secret key msk and an attributes set $S_i \in U$ for entity A_i , the KGC runs this PPT algorithm $Privatekey'$ to generate the partial private key d_{A_i} for the attributes set. Then the partial private key d_{A_i} is transported to entity A_i over a confidential and authentic channel.

-SetSec: given master public key mpk and his attributes set $S_i \in U$ as inputs, entity A_i outputs a secret value x_{A_i} . For all A_i , $(i = 1, 2, \cdots, n)$ he computes $y_i = g_{x_{A_i}}(S_i)$, $(i = 1, 2, \cdots, n)$, then all the entities jointly get a k -sibling intractable function h satisfying $h(y_i) = x$, $(i = 1, 2, \cdots, n)$.

-SetPriv: given master public key mpk , the entity A_i 's secret value x_{A_i} and temporary secret key x , and the entity x_{A_i} 's partial private key d_{A_i} as input, the entity runs this PPT algorithm to generate a private key SK_{A_i} .

-SetPub: given master public key mpk and the entity A_i 's secret value x_{A_i} , one-way trapdoor function f f with x as its trapdoor is returned.

-Encrypt: given a plaintext $m \in M$, the ciphertext is

$$c = Encrypt'(f(m)) \tag{6}$$

-Decrypt: given master public key mpk , the entity's Private Key $SK_{A_i} = (d_{A_i}, x_{A_i})$ and the ciphertext $c \in C$. If entity's attributes set satisfying the access tree T related with c (ciphertext-policy attribute-based encryption scheme), or the attributes related with c satisfies the access tree T (key-policy attribute-based encryption scheme), and then he can get the message as follows:

$$m = f_x^{-1}(Decryption'_{d_A}(c)) \tag{7}$$

Otherwise outputs $\perp$.

VI. CONCLUSIONS

In this paper, we give the new definition for attribute-based certificateless encryption scheme, and a generic construction is presented. The security of the generic construction is at least the same as the attribute-based encryption scheme. Of course, in order to give IND-CCA secure scheme, we can depend on weaker attribute-based encryption scheme, which is our further research. In order to improve the efficiency of attribute-based certificateless encryption scheme, we get an improvement by using a k-sibling intractable function family, and the improvement has shorter public key and efficient encryption and decryption scheme. Furthermore, our scheme is fit for key updating when there are users changed.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (No.61173139), the National Natural Science Foundation of China (No.61272091), Key Project of National Natural Science Foundation of Shandong Province under Grant (No.ZR2011FZ005), and Shandong Natural Science Foundation (No. ZR2012FQ028), Independent Innovation Foundation of Shandong University (No. 2012TS070), and Research Fund for the Doctoral Program of Higher Education of China (No. 20100131120015).

REFERENCES

[1] Sattam S. Al-Riyami, Kenneth G. Paterson, “Certificateless public key cryptography”, in: ASIACRYPT, Chi-Sung Laih, editor, 2003, LNCS 2894, pp. 452-473.

[2] A. Sahai and B. Waters, “Fuzzy identity based encryption”, in Advances in Cryptology-Eurocrypt, 2005, LNCS 3494, pp. 457–473.
[3] 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), 2006, pp. 89–98.
[4] J. Bethencourt, A. Sahai, and B, “Waters. Ciphertext-policy attribute-based encryption”, in Proceedings of the 28th IEEE Symposium on Security and Privacy (Oakland), 2007, pp. 321-334.
[5] Rafail Ostrovsky, Amit Sahai, and Brent Waters, “Attribute-based encryption with non-monotonic access structures”, in ACM Conference on Computer and Communications Security. 2007, pp. 195-203.
[6] Lewko, A., Sahai, A., Waters, B, “Revocation Systems with Very Small Private Keys”, in: IEEE Symposium on Security and Privacy (S&P) , 2010, pp.273-285.
[7] Nuttapong Attrapadung, Benoit Libert, and Elie de Panafieu, “Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts”, in PKC 2011, 2011, LNCS 6571, pp. 90-108.
[8] Ling Cheung and Calvin C. Newport, “Provably secure ciphertext policy abe”, in ACM Conference on Computer and Communications Security, 2007, pp. 456-465.
[9] Vipul Goyal, Abishek Jain, Omkant Pandey and Amit Sahai, “Bounded ciphertext policy attribute-based encryption”, in ICALP, 2008, LNCS 5126, pp. 579-591.
[10] Zhengqiu He, Lifa Wu, Huabo Li, Haiguang Lai, Zheng Hong, “Semantics-based Access Control Approach for Web Service,” in Journal of Computers, Vol 6, No 6 2011, 1152-1161.
[11] Daza, V., Herranz, J., Morillo, P., R`afols, C, “Extended access structures and their cryptographic applications”, To appear in Applicable Algebra in Engineering, Emura, K.,
[12] Miyaji, A., Nomura, A., Omote, K., Soshi, M, “A ciphertextpolicy attribute-based encryption scheme with constant ciphertext length”, in: ISPEC 2009, 2009, LNCS 5451, pp. 13-23.
[13] J. Herranz, F. Laguillaumie, C. R_afols, “Constant-Size Ciphertexts in Threshold Attribute-Based Encryption”, in PKC'2010, 2010, LNCS 6056 , pp. 19-34.
[14] M. Chase, “Multi-authority Attribute Based Encryption”, in S.P. Vadhan, editor, Theory of Cryptography – TCC 2007, LNCS 4392, 2007, pp. 515–534.
[15] S. Müller, S. Katzenbeisser, and C. Eckert, “Distributed attribute-based encryption”, in ICISC, 2008, pp. 20-36.
[16] S. Müller, S. Katzenbeisser, and C. Eckert, “On multi-authority ciphertext-policy attributebased encryption”, in Bulletin of the Korean Mathematical Society 46, 4, 2009, pp. 803-819.
[17] H. Lin, Z. Cao, X. Liang, and J. Shao, “ Secure threshold multi authority attribute based encryption without a central authority”, in INDOCRYPT, 2008, pp.426-436.
[18] Allison B. Lewko, Brent Waters, “Decentralizing Attribute-Based Encryption”, in EUROCRYPT 2011, 2011, pp. 568-588.
[19] M. Chase and S. Chow, “Improving privacy and security in multi-authority attribute-based encryption”, in ACM Conference on Computer and Communications Security, 2009, pp. 121-130.
[20] Changxia Sun, Wenping Ma, “Secure Attribute-based Threshold Signature without a Trusted Central Authority”, in Journal of Computers, Vol 7, No 12, 2012, 2899-2905.

Guoyan Zhang born in Shandong of China in 1977, and received the Ph.D. degree in information security from Shandong University, Jinan, Shandong, China, in 2008. Her research interests include attribute-based cryptography system and certificateless encryption scheme.

She is currently a lecturer in school of computer science and technology of Shandong University.