Attribute-Based Fine-Grained Access Control with User Revocation

Jun Ye, Wujun Zhang, Shu-Lin Wu, Yuan-Yuan Gao, Jia-Tao Qiu

Attribute-based Fine-grained Access Control with User Revocation

Jun Ye[1,2⋆], Wujun Zhang[2], Shu-lin Wu[1], Yuan-yuan Gao[1], and Jia-tao Qiu[3]

[1] School of Science
Sichuan University of Science & Engineering, Sichuan, 643000, China
yejun@suse.edu.cn, wushulin_sh@163.com, gaoyuanyuan@iie.ac.cn
[2] School of Telecommunication Engineering
Xidian University, Shanxi, 710071, China
yejun@suse.edu.cn, wjzhang@xidian.edu.cn
[3] School of Automation and Electronic Information
Sichuan University of Science & Engineering, Sichuan, 643000, China
yhuiqiu@126.com

Abstract. Attribute-based encryption brings a lot of convenience for access control. But it introduces several challenges with regard to the user revocation. In this paper, we propose an access control mechanism using new key update technology to enforce access control policies with efficient user revocation capability. The access control can be achieved by efficient key update technology which takes advantage of the attribute-based encryption and key distribution. We demonstrate how to apply the proposed mechanism to securely manage the cloud data. The analysis results indicate that the proposed scheme is efficient and secure in user revocation.

Key words: Attribute-Based Encryption, Security, Efficient Revocation.

1 Introduction

In cloud computing, data owner outsources sensitive data to cloud server, which is shared with the users whose attributes satisfy the specific access privilege. It is widely applied to the Internet of Things. In the field of access control system, especially under the background of cloud computing, in order to optimize resources and management, more and more businesses and individuals store the data resources in third-party servers. So to provide effective access control [8, 16] of data resources is very necessary. The basic security requirement is to provide the data resources confidentiality. Attribute encryption system has many advantages compared with the traditional method in access control system, but access control has a new challenge in cloud environment.

In this case attribute-based encryption [11, 12, 14] (ABE) offers many convenient. ABE allows for a encrypter to encrypt a message to series of users who

⋆ Corresponding author

have such attributes, without access to a public key certificate. In ABE all the entities are uniformly described in the same way, but the attribute authority of different entities may be different from each other. This makes the decision function of access control may be able to adopt a uniform treatment according to the basis of determination. The ability to do public key encryption without certificates has many practical applications.

1.1 Related Work

Sahai proposed an private key-policy attribute-based encryption scheme by using secret sharing scheme. Goyal [5] proposed a key-policy scheme with a tree access structure where the interior nodes consist of AND and OR gates and the leaves consist of different parties. This scheme can be used to construct fine-grained access control. subsequently, Ostrovsky [13] proposed a non-monotonic ABE. The first ciphertext-policy ABE scheme is proposed by Bethencourt [2]. The ciphertext-policy is defined through the tree access structure and can deal with And an OR gates. On the construct of ABE scheme key-policy scheme is not convenient with the ciphertext-policy scheme, and scalability cannot be achieved. So most attribute-based encryption schemes are ciphertext-policy scheme. Many ABE scheme are proposed in different application fields. Sometimes besides the confidentiality of documents we also need to protect attribute in the ciphertext and the related policy. Anonymous ABE [11, 6, 7] is proposed to solve this problem. In order to disperse the right of authorized center, Chase and Lin [4, 9] proposes an multi-authority ABE scheme. For the purpose of improve the efficiency of user management in broadcast encryption based on public key encryption, Lubicz [10] proposes attribute-based broadcast encryption system. Recently, some ABE schemes with attributes and user revocation [3] have been proposed. And there are two main problems comes out, the backward security and the key updating.

Attribute revocation and user revocation is an essential mechanism in many applications. Attrapadung and Imai [1] proposed an user revocable ABE schemes, but to enable the direct user revocation, the data owner should take charge of all the membership. But the data owner can not directly control the data distribution when the data is outsourced. An efficient user revocation scheme is needed.

1.2 Our Contributions

An attribute-based access control scheme with efficient user revocation is proposed in this paper. An improved ABE model is established, in which the users has two classed of keys. One is the attribute keys and the other is private keys. Attribute keys can be used to get the part of deception key, K. The decryption key is generated by K and the users private keys. This scheme can easily to add and remove users. At last we give the rigorous security proof of our schemes.

The organization of this paper is as follows. Some preliminaries are given in Section 2. The improved attribute-based encryption model is given in Section 3.

Table 1. Notations

k:	security parameters
ω':	set of attributes needed for decryption
ω:	set of user's attributes
$E(\cdot)$:	encryption algorithm
$D(\cdot)$:	decryption algorithm
sk:	private key
pk:	public key
$R(\cdot,\cdot)$:	matching relation of tow elements
f:	key generation algorithm
s:	side information

The secure ABE scheme with efficient user revocation and the security analysis is given in Section 4. Finally, conclusion will be made in Section 5.

2 Preliminaries

2.1 Bilinear Maps

Let $\mathbb{G}_1, \mathbb{G}_2$ be the cyclic groups of prime order p, let g be a generator of $\mathbb{G}_1$, and $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a map with the following properties.

1. Bilinearity: $e(g^a, g^b) = e(g, g)^{ab}$, $a, b \in \mathbb{Z}_p$.
2. Non-degeneracy: There exist $x, y \in \mathbb{G}_1$ such that $e(x, y) \neq 1$.
3. Computable: For all $x, y \in \mathbb{G}_1$, $e(x, y)$ has to be computable in an efficient manner.

2.2 Complexity Assumption

Decisional Modified Bilinear Diffie-Hellman (MBDH) Assumption.

Given $g, g^x, g^y, g^z \in \mathbb{G}_1$ for unknown random $x, y, z, r \in \mathbb{Z}_p^*$. The MDBDH assumption is that no polynomial-time adversary is to be able to distinguish the tuple $(g^x, g^y, g^y, e(g, g)^{\frac{xy}{z}})$ from a random tuple $((g^x, g^y, g^y, e(g, g)^r)$ with more than a negligible advantage.

$$|Pr[\mathcal{A}(g^x, g^y, g^y, e(g, g)^{\frac{xy}{z}}) = 1] - Pr[\mathcal{A}((g^x, g^y, g^y, e(g, g)^r))] = 1| \leq \epsilon$$

3 Improved ABE Model

Some notations are list in table 1.

Setup: Encrypter generates different private key $sk^{(2)}$ for every user, and sends to every user by a secure channel. Then generates a secret key x which is used to encrypt the message, and another private key $sk^{(1)}$ which satisfies $x = f(sk^{(1)}, sk^{(2)})$ for every different $sk^{(2)}$.

Authority generates pk, and for every user, generates different $sk^{(3)}$ and s, user's attributes ω. Then sends to users.

Encryption: Encrypter encrypts the message M with x by computing $C = E(M, x)$, and encrypts $sk^{(1)}$ with pk, then gets a new key $sk^{(4)} = E(sk^{(1)}, s, pk)$. So the ciphertext is $\{\omega', C = E(M, x), s, sk^{(4)}\}$.

Decryption: If $R(\omega, \omega') = 0$, then $sk^{(1)} \neq D(sk^{(4)}, sk^{(3)}, s, pk)$, $x \neq f(sk^{(1)}, sk^{(2)})$. If $R(\omega, \omega') = 1$, user can get $sk^{(1)}$ by computing $sk^{(1)} = D(sk^{(4)}, sk^{(3)}, s, pk)$. Then user computes $x = f(sk^{(1)}, sk^{(2)})$, and recovers message $M = D(M, x)$. Where

$$R(\omega, \omega') = \begin{cases} 1\,, \text{the relation of } \omega \text{ and } \omega' \text{ satisfies decryption conditions} \\ 0\,, \text{else} \end{cases}$$

A schematic diagram of our model are as Fig. 1.

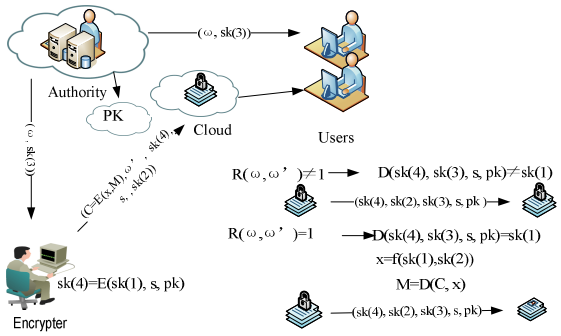

Fig. 1. Improved ABE Model

In this improved ABE model, to achieve user revocation efficiently, the key to encrypt M is divided into tow parts. One part is as a part of user's private key, the other part is used in the attributes policy.

4 Secure ABE Scheme with Efficient User Revocation

We now informally specify an improved threshold Attribute-Based Encryption system as a collection of four algorithms:

Setup (k): Authority generates an algorithm1 which takes a threshold value d as input and outputs a master key MK and a set of public parameters PK. Encrypter chooses a secret key K_1, and generates tow algorithms. One is a key generation algorithm2 with the security parameter k. The other is algorithm3 with which the private keys generated from algorithm2 achieve K_1.

Key Generation (S, MK): The authority executes the Key-Gen algorithm for the purpose of generating a new secret key SK. The algorithm takes as input

the user's identity S, as a set of strings representing a user's attributes and the master-key MK and outputs the secret key SK related to S. And encrypter run algorithm3 generates different secret private key K_2 for users and K_3, then sends the different K_2 to every user through a secure channel and publish algorithm3. And sends K_3 to authority.

Encryption (M, S', PK, K_1, K_3): Encrypter to encrypt a message M with K_1, outputs a ciphertext C. Encrypter encrypts K_3 with a target set S', out put K^*, and sends K^*, C and public parameters to users.

Decryption (C, S', S, SK, K^*, K_2): The decrypt algorithm is run by a user with identity S and secret key SK to attempt to decrypt K^* that has been encrypted with S'. If the set overlap $|S \bigcap S'|$ is greater than or equal to d the algorithm can decrypt K^* and output K. Along with K_3, users can compute the secret key K_1 with his/her own secret private key K_2 to recover M.

Here we give a secure ABE scheme in the improved ABE model. In this scheme authority can not recover M and it is easy to add and remove users.

A detailed description of our scheme is as follows.

4.1 Description

Initialization Assume there are n users in this system, authority chooses $m \times m$ full rank matrix A ($m > n$) and a random number $y \in \mathbb{Z}_p^*$. Authority generates a new m-dimensional vector Y with y,

$$Y = (y, y, \ldots, y)^T$$

and computes X from the linear equations $AX = Y$.

In this way y is used to encrypt the message M. X is as a part of private key. And athority chooses n vectors $\{a_1, a_2, \ldots, a_n\}$ from matrix A ($a_i = (a_{i1}, a_{i2}, \ldots, a_{im})$)as the secret private keys of n users, and sends a_i to each user U_i. (For the security of our scheme, we will give a method to generate X an Y, see the proof of Proposition 2 in this section).

We now create an scheme for authority in which a encryption of X created using attributes ω, can be decrypted only by users whose attributes ω' satisfied $|\omega \bigcap \omega'| \geq d$.

Let $\mathbb{G}_1$ be a bilinear group of prime order p, let g be a generator of $\mathbb{G}_1$, and let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ denote the bilinear map.

We also define the Lagrange coefficient $\Delta_{i,s}$ for $i \in \mathbb{Z}_p$ and a set S of elements in $\mathbb{Z}_p$:

$$\Delta_{i,s(x)} = \prod_{j \in S, j \neq i} \frac{x - j}{i - j}.$$

Identities will be element subsets of universe μ, of size $|\mu|$. And the attributes will be associated with the elements of μ. Our construction is as follows:

Setup(d) For simplicity, we can take the first $|\mu|$ elements of $\mathbb{Z}_p^*$ to be the universe of elements. Then authority chooses $t_1, \ldots, t_{|\mu|}$ and r uniformly from $\mathbb{Z}_p^*$. The published public parameters are:

$$T_1 = g^{t_1}, \ldots, T_{|\mu|} = g^{t_{|\mu|}}, Y = e(g, g)^r.$$

The master key is:

$$t_1, \ldots, t_{|\mu|}, r.$$

Key Generation A $d-1$ degree polynomial q is randomly chosen by autyority such that $q(0) = r$. The private key consists of components, $(D_i)_{i\in\omega}$, where $D_i = g^{q(i)/t_i}$ for every $i \in \omega$.

Encryption First, a random value $a, t, s \in \mathbb{Z}_p^*$ is chosen by encrypter, and encrypter computes b satisfies $ab = 1 \mod p$. The ciphertext is the published as:

$$E = (\omega', C = tyM, (tX)^a = ((tx_1)^a, (tx_2)^a, \ldots, (tx_m)^a)^T, E' = bY^s, \{E_i = T_i^s\}_{i\in\omega'}).$$

Decryption Some parts of ciphertext E is encrypted with a key associated with ω', where $|\omega \bigcap \omega'| \geq d$. User chooses an arbitrary subset of $\omega \bigcap \omega'$ with d elements. Then, the ciphertext can be decrypted as follows:

First, user U_j computes $E'/\prod_{i\in S} e(D_i, E_i)^{\Delta_{i,s}(0)}$ and gains b.

$$\begin{aligned} E'/\prod_{i\in S} e(D_i, E_i)^{\Delta_{i,s}(0)} &= be(g,g)^{sy}/\prod_{i\in S}(e(g^{q(i)/t_i}, g^{st_i}))^{\Delta_{i,s}(0)} \\ &= be(g,g)^{sy}/\prod_{i\in S}(e(g,g)^{sq(i)})^{\Delta_{i,s}(0)} \\ &= b. \end{aligned}$$

Second, user U_j computes

$$tX = (tX)^{ab} = ((tx_1)^{ab}, (tx_2)^{ab}, \ldots, (yx_m)^{ab})^T \mod p$$

and gets $tX = (tx_1, tx_2, \ldots, tx_m)^T$. Then U_j can get ty by the equation

$$ty = a_i tX \mod p$$

Last, user U_j can recover the message M by computing $M = C/ty$.

4.2 Security Analysis

Proposition 1. *The adversary whose attributes are not satisfied $|\omega \bigcap \omega'| \geq d$, can get y with the probability $\frac{1}{p} + \epsilon$. (ϵ is negligible).*

Proof. From the security of Decisional Modified Bilinear Diffie-Hellman (DMBDH) Assumption in [15], we know the probability with which the adversary can get the vector X which is used to compute ty is ϵ_1 (ϵ_1 is negligible).

The other way, adversary can just to guess ty. For ty is randomly chosen in $\mathbb{Z}_p$ by encrypter, the only information of ty adversary can get is ty is different from the other data which is used before. So the probability which adversary can guess ty is $\frac{1}{p} + \epsilon_2$, where ϵ_2 is negligible.

Therefore, the adversary whose attributes are not satisfied $|\omega \bigcap \omega'| \geq d$, can get ty with the probability $\frac{1}{p} + \epsilon_1 + \epsilon_2 = \frac{1}{p} + \epsilon$, where $\epsilon = \epsilon_1 + \epsilon_2$.

Proposition 2. *The probability which curious user can get other user's secret private key is at most* $\frac{1}{p}$.

Proof. With out loss of generality we assume U_1 is curious. When U_1 recover enough M, he/she would get enough pairs of X and Y. The original linear equations are

$$A_{m\times m}X_{m\times 1} = Y_{m\times 1} \mod p.$$

If there are m vectors of X which are linearly independent, U_1 can construct the following equations with the corresponding vectors of Y.

$$A(X_1, X_2, \ldots, X_m) = (Y_1, Y_2, \ldots, Y_m) \mod p$$

Generation of X and Y: Here we give a method to generate X and Y, which leads the curious user can not get other user's secret private key. By using this generation of X, encrypter would not reveal the private key a_i.

Encrypter can generate small amounts of X, i.e.$(X_1, X_2, \ldots, X_l), l \ll m$, and use the linear combination of vectors $(X_1, X_2, \ldots, X_l)$ to generate other X_j and get corresponding Y_j $(l \le j \le m)$.

$$X_j = k_{1j}X_1 + k_{2j}X_2 + \cdots + k_{lj}X_l \mod p(k_{ij} \in \mathbb{Z}_p^*, 1 \le i \le l)$$

and corresponding m-dimensional vector

$$Y_j = (\sum_{i=1}^{l} k_{ij}y_i, \sum_{i=1}^{l} k_{ij}y_i, \ldots, \sum_{i=1}^{l} k_{ij}y_i) \mod p.$$

Correctness of operation: X_j and Y_j generate from this way can make our scheme execute correctly. The correctness is as follows.

$$\begin{aligned} AX_j &= \left(a_1, a_2, \ldots, a_m\right)^T (k_{1j}X_1 + k_{2j}X_2 + \cdots + k_{lj}X_l) \\ &= \begin{pmatrix} k_{1j}a_1X_1 + k_{2j}a_1X_2 + \cdots + k_{mj}a_1X_m \\ k_{1j}a_2X_1 + k_{2j}a_2X_2 + \cdots + k_{mj}a_2X_m \\ k_{1j}a_mX_1 + k_{2j}a_mX_2 + \cdots + k_{mj}a_mX_m \end{pmatrix} \\ &= \begin{pmatrix} k_{1j}y_1 + k_{2j}y_2 + \cdots + k_{mj}y_m \\ k_{1j}y_1 + k_{2j}y_2 + \cdots + k_{mj}y_m \\ k_{1j}y_1 + k_{2j}y_2 + \cdots + k_{mj}y_m \end{pmatrix} \\ &= \left(\sum_{i=1}^{l} k_{ij}y_i, \sum_{i=1}^{l} k_{ij}y_i, \ldots, \sum_{i=1}^{l} k_{ij}y_i\right) \mod p. \end{aligned}$$

In this way the rank of the matrix which is consist of any combination of m vectors is less than l, so there are at least p^{m-l} vectors satisfies $AX = Y$. So the probability U_1 can get other user's secret private key is at most $\frac{1}{p^{m-l}}$.

Every user's secret private key (a m-dimensional vector) a satisfies $aX = Y \mod p$. There are P^{m-1} m-dimensional vectors a satisfies $aX = Y$ in $\mathbb{Z}_p$, but there are p^m m-dimensional vectors in $\mathbb{Z}_p$. So the probability U_1 can get other user's secret private key is $\frac{1}{p}$.

Hence, the probability the other user's key a_i can be gained is at most $\frac{1}{p}$.

4.3 User Addition and Revocation

User addition: When U_{n+1} join in, encrypter will give him/her a_{n+1} as the secret private key from the matrix $A_{m\times m}$ through a secure channel, and authority give him/her the corresponding private key according to his/her attributes. It is very easy to implement. Because a_{n_1} is the n_1th vector of A, so for all X used before, U_{n+1} can compute $a_{n+1}X = y$. In this way U_{n+1} can recover the message which encrypt before his/her join.

User revocation: When U_i is removed, the secret private key a_i is not available and the message M which is recovered by U_i should be re-encrypted by encrypter. Encrypter use a new vector a_i' which is the linear combination of vectors in A to instead of a_i, and get the new matrix A'.

$$a_i' = h_1a_1 + h_2a_2 + \cdots + h_ia_i + \cdots + h_ma_m \mod p$$

Where $h_j \in \mathbb{Z}_p, (1 \le j \le m)$, $\sum_{j=1}^m h_j \neq 1$ (If $\sum_{j=1}^m h_j = 1$, then $a_i'X = y$ and $a_iX = y$, so U_i can recover M). A is still full rank, X is uniquely determined.

U_j re-encrypt M, and computes the new $y' = a_jX'$ from the equation $A'X' = Y$ (where the vector a_i is replace by a_i'), then $C' = y'M \mod p$.

Proposition 3. *The probability the removed user can get the new y' is $\frac{1}{p}$.*

Proof. Even the new X' is gained, the removed user U_i uses his/her original secret private key a_i can not get y' yet. We assume $y' = a_i'X'$, here

$$a_i' = h_1a_1 + h_2a_2 + \cdots + h_ia_i + \cdots + h_ma_m \mod p,$$

and $\sum_{j=1}^m h_j \neq 1$. So

$$y' = \sum_{j=i}^m h_ja_jX' = \sum_{j=1,j\neq i}^m h_ja_jX' + h_ia_iX' = \sum_{j=1,j\neq i}^m h_jy' + h_ia_iX'.$$

If $a_iX' = y'$, then

$$y' = \sum_{j=i}^m h_ja_jX' = \sum_{j=1,j\neq i}^m h_jy' + h_iy' = \sum_{j=1}^m h_jy'$$

but $\sum_{j=1}^m h_j \neq 1$, then $a_iX' \neq y'$. So U_i can not get the new y'.

The another way to get y' is that U_i guess it from $\mathbb{Z}_p$. For y' is chosen form $\mathbb{Z}_p$ randomly, so the probability is $\frac{1}{p}$.

Therefore, the probability which the removed user can get the new y' is $\frac{1}{p}$.

Efficiency: When some member is removed, sever should update other members' secret private keys, which is efficient for small group by using the above technology.

The time cost of secret private keys update is as Fig. 2. We implement our mechanism using MATLAB language with a version of R2012b. The process is conducted on a computer with Intel(R) Core(TM)i3-3230 CPU processor running at 2.60 GHz, 4 GB RAM.

The time cost is related to the number of members, has nothing to do with the number of deleted members.

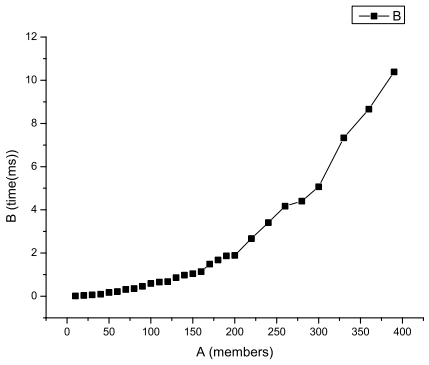

Fig. 2. Time Cost of User Revocation

5 Conclusion

In order to easily achieve user revocation, an improved ABE model is proposed in this paper. The improved scheme building on the proposal of fuzzy IBE from [15] is as examples of schemes in our model. The method that the keys which can recover messages are divided into tow parts are very effective to achieve user revocation. And a key updating method and a re-encryption method are proposed for the security of user revocation. The security of our schemes are strictly proved.

Acknowledgements

The work described in this paper is supported by the Science Founding of Artificial Intelligence Key Laboratory of Sichuan Province (2014RYJ06, 2012RYJ05); The Scientific Research Fund Project of Sichuan University of Science & Engineering (2013KY02); NSFC (No.11301362); Project of Innovative Research Team in University of Sichuan (NO.13TD0017); The talent project of Sichuan University of Science & Engineering (2013RC13).This work was supported by the high-quality goods resource sharing courses "mathematical modeling" of Sichuan province (2012-57); Science Founding of Science School of Sichuan university of science & engineering(10LXYB05); "mathematical modeling teaching group" of Sichuan University of Science & Engineering (2009-142-01).

References

1. N. Attrapadung and H. Imai. Conjunctive broadcast and attribute-based encryption. volume 5067, pages 248–265. Springer-Verlag, August 2009.
2. J. Bethencourt, A. Sahai, , and B. Waters. Ciphertext-policy attribute-based encryption. volume 3494, pages 321–334. Springer-Verlag, May 2007.

3. A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. pages 417–426, October 2008.
4. M. Chase and S.S.M. Chow. Privacy-aware attribute-based encryption with user accountability. pages 121–130. Springer-Verlag, November 2009.
5. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. volume 3494, pages 89–98, October 2006.
6. A. Kapadia, P.P. Tsang, and S.W. Smith. Attribute-based publishing with hidden credentials and hidden policies. pages 179–192, 2007.
7. J. Li, K. Ren, B. Zhu, and Z. Wan. Privacy-aware attribute-based encryption with user accountability. volume 5735, pages 347–362. Springer-Verlag, September 2009.
8. J.W. Li, J. Li, X.F. Chen, C.F. Jia, and Z.L. Liu. Efficient keyword search over encrypted data with fine-grained access control in hybrid cloud. volume 7645, pages 490–502. Springer-Verlag, November 2012.
9. H. Lin, Z. Cao, X. Liang, and J. Shao. Secure threshold multi-authority attribute based encryption without a central authority. *Information Sciences*, 180(13):2618–2632, 2010.
10. D. Lubicz and T. Sirvent. Attribute-based broadcast encryption scheme made efficient. volume 5023, pages 325–342. Springer-Verlag, June 2008.
11. T. Nishide, K. Yoneyama, and K. Ohta. Attribute-based encryption with partially hidden encryptor-specified access structures. volume 5037, pages 111–129. Springer-Verlag, June 2008.
12. T. Okamoto, K. Takashima, and M. Electric. Adaptively attribute-hiding (hierarchical) inner pro duct encryption. volume 7237, pages 591–608. Springer-Verlag, April 2012.
13. R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. pages 195–203, October 2007.
14. B. Parno, M. Raykova, and V. Vaikuntanathan. How to delegate and verify in public: Verifiable computation from attribute-based encryption. volume 7194, pages 422–439. Springer-Verlag, March 2012.
15. A. Sahai and B. Waters. Fuzzy identity-based encryption. volume 3494, pages 457–473. Springer-Verlag, May 2005.
16. X.X. Xie, H. Ma, J. Li, and X.F. Chen. New ciphertext-policy attribute-based access control with efficient revocation. volume 7804, pages 373–382. Springer-Verlag, March 2013.