Efficient Cryptographic Access Control Protocol for Sensitive Data Management

Xixi Yan
School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan, China
Email: yanxixi0326@163.com

Tao Geng
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
Email:taogeng@yahoo.com.cn

Haiyang Ding
College of Information Engineering, Beijing Institute of Graphic Communication, Beijing, China
Information Security Center, Beijing University of Posts and Telecommunications, Beijing, China
Email: o_dhy@163.com

***Abstract*---In view of sensitive data management, an efficient cryptographic access control scheme is proposed. Based on attribute-based encryption, the proposed scheme not only inherits flexibility and fine-grained access control for users, but also realizes cryptographic management for servers. In additional, the scheme alleviates the administering burdens on the server, and handle dynamic access policies in a more efficient and cryptographic way. Compared with the existing system, the scheme relieves the server from intense encryption /decryption processing, and achieves reliable decentralized encryption /decryption with good scalability and efficiency.**

***Index Terms*---Senstive data sharing, Access control, Attribute-based encryption**

I. Introduction

Along with the popularization of Internet, the demand for sharing sensitive data resources becomes more and more stronger in the distributed computing environment. The provider of resources needs to control sensitive data sharing range by developing flexible extensible access control strategy. Therefore, an efficient cryptographic access control protocol for sensitive data management is of increasingly great importance.

Traditional access control architectures usually assume the data owner and sever storing the data in the same trusted domain. When user wants to access data, he must get the authorization through submitting his identity information. In other words, only an authorized user is permitted to access the sensitive data. However, it can't meet the demand for sharing sensitive data resources, and there are a lot of security problems during the period of storage, transmission and usage including as: (I) because all of E-document is often stored with the plaintext in the server, once sever is under attack, the sensitive data will be leaked out; (II) sever must be trusted to preventing the collusion between the user and sever because it need to record when and where the user accesses the data; (III) server must take measure to ensure secure transmission between sender and receiver, even if the receiver is authorized.

One method for alleviating some of these problems is to store data in encrypted form. Thus, if the server is attacked, the amount of sensitive information loss will be limited. However, how to store and share the encrypted data selectively at a fine-grained level is one of the urgent problems to be solved. In this paper, an efficient cryptographic access control for sensitive data management which is based on attributed –based encryption will be proposed.

The rest of this paper is organized as follows: Section II provides an overview on related work. Then we present an efficient cryptographic access control protocol for sensitive data management in Section III. In Section IV, we prove the security of protocol, analyze its efficiency and evaluate its performance based on real implementation. Lastly, we conclude the paper in Section V.

II. Related Work

A. Attributed-Based Encryption (ABE)

The concept of Attributed-Based Encryption (ABE) was first introduced by Sahai and Waters in 2005 [1], which refines identity-based encryption by associating ciphertext and private keys with sets of descriptive attributes. Then a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key. In 2006, two categories of ABE including ciphertext policy and key policy are presented in Reference [2]. In CP-ABE [2] (Ciphertext policy attribute based encryption, CPABE), the user secret key is associated with a set of attributes and a ciphertext is associated with an access control policy over a list of attributes. The decrtyptor can decrypt

doi:10.4304/jcp.9.1.222-227

the ciphertext if the list of attributes associated with the secret key satisfies the access policy. In KP-ABE [2] (Key policy attribute based encryption), the secret key is associated with an access control policy over a list attributes and the ciphertext is associated with a set of attributes. The decryptor can decrypt the ciphertext if the list of attributes associated with the ciphertext satisfies the access policy associated with the secret key. The first KP-ABE scheme [2] can realize the monotonic access structures for key policies. To enable more flexible access policy, Ostronsky et al. [3] consequently presented a fine-grain non-monotonic access structure in KP-ABE. The first CP-ABE scheme [4] which is only proved under the generic group model was proposed by Bethencourt et al. Consequently, Cheung and Newport [5] presented another construction which only permits AND gates while the first expressive construction is proved to be secure under the standard model. Later, Goyal et al. [6] gave another construction which is based on number theoretic assumption and supports threshold gates in access tree.

B. Existing Access Control Scheme for Sensitive Data Management

Obviously, traditional access control scheme has shown limitations to cover modern digital environment and it can’t meet the demand for the security of sensitive data management. The emergence of DRM (Digital rights management) technology provides a foundation for more trusted and secure computing environment. Adolf Honl and Alf Zugenmaier [10] present an approach to solve privacy about personal data in a smart hospital environment based on DRM technology. However, today’s DRM technology requires well–defined policies and models that can express usage decisions more comprehensively [11-12]. UCON (usage control) technology encompasses these areas including traditional access control, DRM and trust management and goes beyond in its definition and scope. UCON technology can achieve fine-grained control on digital resources and provide for reliable and trusted controls on the usages of digital resources throughout their life cycle [13]. The concept of proxy re-encryption(PRE) was introduced by Blaze, Bleumer and Strauss [14].In this scheme, a semi-trust proxy will transform a ciphertext originally intended for Alice into an encryption of the same message intended for Bob, and the proxy can’ t acquire any plaintext. In a PRE scheme, data m encrypted under pk_A can be eventually changed to being encrypted under a different key pk_B , which made the server avoid storing the plaintext. Behzad Malek and Ali Miri design a balanced access control system [17] that policies are integrated into private keys of users. At present, most existing access control schemes pay attention to control usage on plaintext data, but it is not secure to store and transmit sensitive data. Therefore, how to realize cryptographic access control is the main problem to be solved in the paper.

III. NEW CONSTRUCTIONS

A. Ciphertext-Policy Attribute-based Encryption Scheme

An CP-ABE scheme is a tuple of probalistic polynomial time algorithms(SETUP, KEYGEN, ENC, DEC).

- $SETUP\left(1^k\right)$: On input a security parameter 1^k , the setup algorithm SETUP outputs a system public parameter pk and a master key mk ;
- $KEYGEN\left(A_u, mk\right)$: On input a set of attributes A_u identifying the user and a master key mk , the key generation algorithm KEYGEN outputs a secret key usk associated with the set of attributes A_u ;
- $ENC\left(m, A_c, pk\right)$: On input an access policy A_c , a message to be encrypted m and the system public key pk , the algorithm ENC outputs the ciphertext C associated with the access policy A_c ;
- $DEC\left(usk, C_i\right)$: on input a secret key usk and the ciphertext C , the decryption algorithm DEC first checks if the attribute A_u satisfies the access structure of A_c . Then, if check passes, it outputs a message m .

B. Main Idea

The composition of the scenario is shown in Fig.1. After creating sensitive data, the creator encrypts the data with Symmetrical cryptographic algorithm (AES, DES, etc). Then the Symmetric key will be encrypted with ABE scheme, so that the use can decrypt the key ciphertext if the attributes associated with the user secret key satisfies the access policy. After that, the ciphertext will be stored and managed by system server who is in possession of a master key which is used to generate secret keys of users. In this way, it provides an efficient cryptographic access control protocol for sensitive data management which can also handle dynamic access policies.

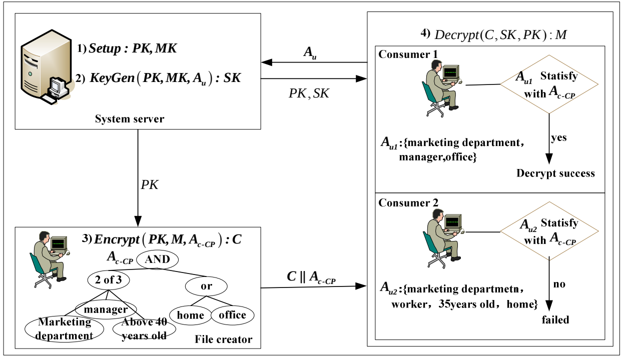

1) $Setup : PK, MK$
2) $KeyGen(PK, MK, A_u) : SK$
System server
A_u
PK, SK
PK
3) $Encrypt(PK, M, A_{c\text{-}CP}) : C$
$A_{c\text{-}CP}$
AND
2 of 3
or
manager
Marketing department
Above 40 years old
home
office
File creator
$C \| A_{c\text{-}CP}$
4) $Decrypt(C, SK, PK) : M$
Consumer 1
A_{u1} Statisfy with $A_{c\text{-}CP}$
yes
A_{u1}:{marketing department, manager,office}
Decrypt success
Consumer 2
A_{u2} Statisfy with $A_{c\text{-}CP}$
no
A_{u2}:{marketing departmetn, worker, 35years old, home}
failed

Figure 1. The model for proposed scheme in sensitive data management

C. Proposed Access Control Protocol Based on ABE for Sensitive Data Management

An efficient cryptographic access control protocol based on CP-ABE [3] scheme for sensitive data management will be shown as follows.

(I) Notations

The description of notations is shown as follows.

TABLE1.
THE DESCRIPTION OF NOTATIONS

Notations	description
PK	System public key
MK	master key
SK_u	The secret key of user
A_u	A set of attributes for user
A_c	A set of attributes for encrypting k
k	Symmetric key for encrypting the data plaintext
C_k	Symmetric key ciphertext
$Enc_k(X)$	Encrypting X with key k
$Dec_k(X)$	Decrypting X with key k

(II) Setup and initialization

A)The system server chooses a bilinear group G_0 of prime order p with generator g, and then it chooses two random exponents $\alpha, \beta \in Z_p$. So the system generates public key PK and master key MK using $SETUP\left(1^k\right)$ algorithm as follows.

$$S: PK = G_0, g, h = g^{\beta}, f = g^{1/\beta}, e(g,g)^{\alpha} \quad (1)$$

$$S: MK = \left(\beta, g^{\alpha}\right) \quad (2)$$

B)The system server defines a set of attributes A, and choose a random $r \in Z_p$, and then random $r_u \in Z_p$ for each attribute $j \in A$.

$$S: SK = \left(D = g^{(\alpha+\gamma)/\beta}, D_j = g^r \bullet H(j)^{r_u}, D_j' = g^{r_u}, \forall u \in A\right) (3)$$

(III) New user grant

When a new user wants to join the system, sever will assign an access structure and the corresponding secret key to this user.

A)According to the unique identity of each user A_u ($A_u \subseteq A$), server choose random r' and r_u' $(\forall u \in A_u)$. Then it creates a secret key as

$$SK_u = \left(D' = Df^{r'}, \forall u \in A_u : D_u' = D_u g^{r'} H(u)^{r_u'}, D_u'' = D_u' g^{r_u'}\right) (4)$$

B)Send the public key PK and user attribute secret key to the user.

$$S \rightarrow U : PK, SK_u$$

(IV) New file creation

In the multi-domain environment, the data creator can also be outside user as inside user. Therefore, the data creator must submit the file ciphertext and key ciphertext to domain server which manages the file uniformly.

A)The file creator O creates a new file F and selects a unique ID for this data file.

B)Randomly select a symmetric data encryption key k and encrypt the data file using k with AES algorithm.

$$O : F' = Enc_k(F) \quad (5)$$

C)The file creator encrypts symmetric data encryption key k under a tree access structure A_c for the data file.

a) Choose a polynomial q_x for each node x in the tree A_c. For each node x in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node ($d_x = k_x - 1$).

b) Start with the root node R and choose a random $s \in Z_p$ and set $q_R(0) = s$. Choose d_R other points of the polynomial q_R randomly to define it completely. For any other node x, set $q_x(0) = q_{parent(x)}(index(x))$ and choose d_x other points randomly to completely it completely.

c) Let Y be the set of leaf nodes in A_c. Therefore, the symmetric data encryption key ciphertext is computed as:

$$O : C_k = \begin{pmatrix} A_c, C' = ke(g,g)^{\alpha s}, C'' = h^s, \\ \forall y \in Y : \quad C_y = g^{q_y(0)}, C_y' = H(att(y))^{q_y(0)} \end{pmatrix} \quad (6)$$

D)Finally, the creator O sends the file ciphertext F' and key ciphertext C_k to domain severs.

$$O \rightarrow S : F' \| C_k$$

(V)The file access

A)The user submits the file ID and applies for accessing.

$$U \rightarrow S : \text{Document Request}$$

B)Sever S verify if the requesting user is a valid system user in user list. If true, it sends the file ciphertext F' as well as ciphertext of the key C_k to the user.

$$S \rightarrow U : F' \| C_k$$

(VI) The file decryption

A)On receiving the response from DS, the user first verifies if the data owner's signatures on the attribute information and the corresponding public key components.

$$U : Verify\left(\mathrm{si}\,g\left(F'\right)\right)$$

B)The user decrypts the content key C_k with his attribute secret key SK_u.

$$U : k = Dec_{sk}\left(C_k\right) \tag{7}$$

a) If the node x is a leaf node, with the algorithm $DecryptNode\left(C_k, SK_u, x\right)$, let $i = att\left(x\right)$ and computes:

$$DecryptNode\left(C_k, SK_u, x\right) = \begin{cases} \dfrac{e\left(D_i, C_x\right)}{e\left(D_i', C_x'\right)} = e\left(g,g\right)^{rq_x(0)} & i \in A \\ \perp & i \notin A \end{cases} \tag{8}$$

b) If the node x is not a leaf node, nodes z are children of x. Let S_x be an arbitrary k_x-sized set of child nodes z such that $F_Z \neq \perp$. If no such set exists then the node was not satisfied and the function returns $\perp$. Otherwise, then compute:

$$\begin{aligned} & F_x \\ & = \prod_{z \in S_x} F_Z^{\Delta_{i,S_x'(0)}} \quad \left(i = index\left(z\right), S_x' = \left\{index\left(z\right) : z \in S_x\right\}\right) \\ & = \prod_{z \in S_x} \left(e\left(g,g\right)^{r \cdot q_z(0)}\right)^{\Delta_{i,S_x'(0)}} \\ & = \prod_{z \in S_x} e\left(g,g\right)^{r \cdot q_x(i) \cdot \Delta_{i,S_x'(0)}} \\ & = e\left(g,g\right)^{r \cdot q_x(0) \cdot} \end{aligned} \tag{9}$$

c) At last, decrypts C_k by computing:

$$\begin{aligned} & C' \Big/ \left(e\left(C'', D\right) \big/ e\left(g,g\right)^{rq_R(0)}\right) \\ & = C' \Big/ \left(e\left(h^s, g^{(\alpha+\gamma)/\beta}\right) \Big/ e\left(g,g\right)^{rs}\right) \\ & = k \end{aligned} \tag{10}$$

C)The user decrypts data files using k with AES.

$$U : F = Dec_k\left(F'\right) \tag{11}$$

IV. Analysis of Our Proposed Scheme

A. Security Analysis

From the following immediately available prosperities, we first analyze security analysis of our proposed scheme.

(I)Content key confidentiality: This property can be immediately achieved by using the enhanced construction of CP-ABE [3] which can be used to disclose the identities of key abusers. Content key is encrypted under an attribute access tree structure, and the ciphertext contains an access policy. If the set S of attributes which is represented by user' s secret key satisfies the access structure A, the user will decrypt the ciphertext and return content key.

(II) Sensitive data confidentiality: In our proposed scheme, data owner encrypts the file under k with AES algorithm, and k was encrypted with ABE algorithm. Then, the ciphertext was sent to system server. Assuming AES algorithm is secure, security of this scheme is merely relied on the security of ABE. In ABE scheme, private key was identified with a set S of descriptive attributes. The server or consumer that wants to decrypt a message will specify an access policy through access tree that private keys must satisfy in order to decrypt. A user will be able to decrypt a ciphertext with a given key if and only if there is an assignment of attributes from the secret key to nodes of the tree such that the tree is satisfied. Therefore, the sensitive data is in the form of ciphertext in the lifetime. Even though sever is not trusted or attacked, the sensitive data can't be leak out.

(III)Cryptographic access control: In our proposed scheme, we guarantee cryptographic and fine-grained access control by ABE. The data owner defines flexible access structure for each user, so the consumer was delegated according to attributes set by the data owner selectively. Only user secret key satisfies with access structure, can he operate the file after receiving data ciphertext.

B. Efficiency Analysis

We will analyze the efficiency between traditional management and our scheme as follows.

(I)System Function. In the traditional management of sensitive data, all of E-document is often stored with the plaintext in the server, once sever is under attack, the sensitive data will be leaked out. Also, sever must be trusted to preventing the collusion between the user and sever because it need to record when and where the user accesses the data. An efficient cryptographic access control scheme for sensitive data management is proposed to solve these problems.

TABLE2.
COMPARISON OF SYSTEM FUNCTION

comparison	Traditional management scheme	Our scheme
server	trusted	untrusted
The form of sensitive data stored by server	ciphertext	ciphertext
Server can decrypt the ciphertext	yes	no
update authority	no	yes
Access control	plain	cryptographic

(II) User authority grant. In this operation, a user authority is associated with an attribute set, which relate to his secret key. The main computation overhead of this operation is distributing the key. The computation complexity is $O(1)$ in our scheme. However, the computation complexity is $O(n)$, where n is the number of user. The comparison is shown at Tab.3.

(III) Sensitive data access. In the traditional management, when the consumer applies for the access of sensitive data, server needs to decrypt the data ciphertext firstly, and then encrypt the data ciphertext with the consumer's public key. So the computation complexity is $O(1T_E + 1T_D)$, where T_E is the number of encryption, and T_D is the number of decryption. In our scheme, there is nothing to do in this operation.

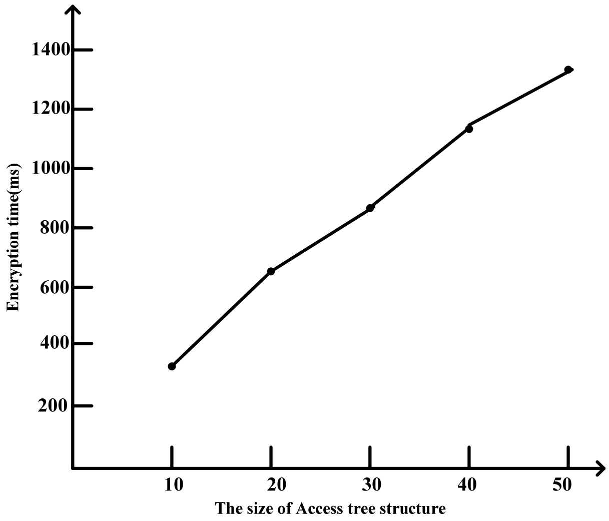
TABLE3.
COMPARISON OF COMPUTATION COMPLEXITY

operation	Traditional management scheme	Our scheme
Key distribution	$O(n)$	$O(1)$
Sensitive data encryption for owner	$O(1)$	$O(1)$
Sensitive data access	$O(1T_E + 1T_D)$	0

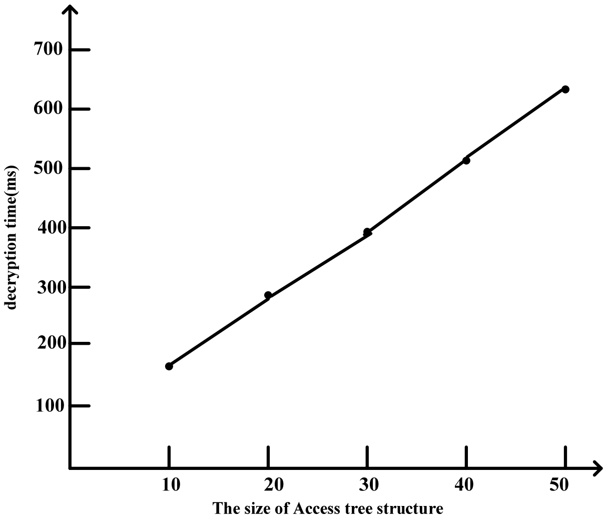
C. Implementation

In a real scenario, the number of attributes of every user is limited, and the number of subsets and attributes in access control tree is determined by the file control policy. Therefore, assume that the number of attributes for use is 5, and the number of attributes in access control structure if fixed to be 50.

The comprehensive experiments are conducted on a laptop with dual core 2.4GHz and 2GB RAM. We make an analysis on the experimental data with 1MB size, and encrypt the sensitive data with AES algorithm under 192bits symmetric key. We can see the time for encrypting the file depends on the access tree structure. According to the number of the access tree policy, the time required to encrypt the file is shown in Fig.2.



(a) New file creation and encryption



(b) File access and decryption (there is 1subset with 50 attributes in the private key)

Figure1. Experiments on file creation and encryption

V. CONCLUSIONS

To assure sensitive resource sharing and distribution with high efficiency and good scalability, an efficient cryptographic access control protocol will be proposed in the paper. Comparing with the traditional access control scheme, there are several advantages as follows: (I)Even if system server is attacked, sensitive resource can't be decrypted by the attacker, because sensitive resource is transmit and stored in the form of ciphertext during the lifetime.(II)The scheme alleviates the administering burdens on the server, and handle dynamic access policies in a more efficient and cryptographic way, so the server need not to be trusted by sensitive owner and consumer. (III)The data owner defines flexible access structure for each user, so the consumer was delegated according to attributes set by the data owner selectively. Only user secret key satisfies with access structure, can he operate the file after receiving data ciphertext. (IV)The scheme relieves the server from intense encryption /decryption processing, and achieves reliable decentralized encryption /decryption with good scalability and efficiency.

ACKNOWLEDGMENT

This work has been supported by the National Natural Science Foundation of China (No.61272519), IIE's Research Project on Cryptography (No.Y3Z0032104).

REFERENCES

[1] Amit Sahai and Brent Waters, "Fuzzy identity-based encryption", In EUROCRYPT2005, LNCS3494, pp.457-473, 2005.

[2] Vipul Goyal, Omkant Pandey, Amit Sahai,etc, "Attributed-based encryption for fine-grained access control of encrypted data", In: ACM Conference on Computer and Communications Security, pp.89-98, 2006.

[3] Rafail Ostrovsky, Amit Sahai and Brent Waters, "Attribute-based encryption with non-monotonic access structures", In: ACM Conference on Computer and

Communications Security, pp.195-203, 2007.

[4] John Bethencourt, Amit Sahai, and Brent Waters, “Ciphertext-policy attribute-based encryption”, In: IEEE Symposium on Security and Privacy, pp.321-334, 2007.

[5] Ling Cheung, Calvin Newport, “Provably secure ciphertext policy ABE”, In: ACM Conference on Computer and Communications Security, pp.456-465, 2007.

[6] Vipul Goyal, Abhishek Jain, Omkant Pandey, et al, “Bounded ciphertext policy attribute based encryption”, In: ICALP’08, LNCS 5126, PP.579-591, 2008.

[7] Li Jin, Wang Qian, Wang Cong, et al, “Enhancing attribute-based encryption with attribute hierarchy”, In: Mobile networks and applications, Vol.16, No.5, pp.553-361, 2011.

[8] Wan Zhiguo, Liu Jun’e, Robert H.Deng, et al, “HASBE: A Hierarchical attribute-based solution for flexible and scalable access control in cloud computing”, In: transactions on information forensics and security, Vol.7, No.2, pp.743-754, 2012.

[9] Yan Xixi, Ma Zhaofeng, Yang Yixian, et al, “A CCA-secure and interoperable cross-domain distribution protocol for E-document”, In: Advances information sciences and service sciences (AISS), Vol.4, No.1, pp.311-319, 2012

[10] Adolf Hohl , Alf Zugenmaier, “Safeguarding personal data with DRM in pervasive computing”, In: Security and privacy workshop at pervasive, 2004.

[11] Sangho L, Heejin P, Jong K. “A secure and mutual-profitable DRM interoperability scheme”. In: Computers and Communications (ISCC), pp.75-80, 2010.

[12] Qin Q, Zhi T, Yinyan Y. “A decentralized authorization scheme for DRM in P2P file-sharing systems”. In: Consumer Communications and Networking Conference (CCNC), pp.136-140, 2011.

[13] Jaehong Park, “The UCON usage control model”, In: ACM transactions on information and system security, Vol.7, No.1, pp.128-174, 2004.

[14] M.Blaze, G.Bleumer, and M.Strauss, “Divertible protocols and atomic proxy cryptography”, In EUROCRYPT1998, LNCS1403, pp.127-144, 1998.

[15] Yan Xixi, Ma Zhaofeng, “Identity-based domain key distribution protocol in the E-document security management”. In: Journal on communications, Vol.33, No.5, PP.12-20, 2012.

[16] Yan Xixi, Ma Zhaofeng, “A distribution protocol based on proxy Re-encryption in domain environment of E-document management”. In: Journal of Beijing University of Posts and Telecommunications, Vol.35, No.5, PP.81-84, 2012.

[17] Behzad, A. Miri, “Combining attribute-based and access systems”. In:Muzio JC,Brent RP,eds.Proc.IEEE CSE 2009,12th IEEE Int’l Conf.on Computational Science and Engineering.IEEE Computer Society, pp.305-312,2009.

[18] Zhang Jindan, Wang xuan. Yang Xiaoyuan, “Identity based proxy re-encryption from BB1 IBE”. Journal of computers, Vol 8, No.6, pp.1618-1626, 2013.

[19] Wang Xiaoming, Lin Yanchun, “An efficient access control scheme for outsourced data”, Journal of computers, Vol 7, No.4, pp.918-922, 2012.

[20] Wu Qing, Wang Wenqing, “New identity-based broadcast encryption with constant ciphertext in the standard model”, Journal of software, Vol 6, No.10, pp.1929-1936, 2011.

[21] Li Hengjian, Wang Lianhai, Zhang Ruichao, Wu Lu, “A high performance and secure palmprint template protection scheme”, Journal of software, Vol 7, No.8, pp.1827-1834, 2012.

Xixi Yan was born in 1985. She received the Ph.D. degree in Cryptography from Beijing University of Posts and Telecommunications, Beijing, China in 2012. Now she is working at School of Computer Science and Technology, Henan Polytechnic University, Henan, China. Her research interests include digital right management (DRM), data security, etc.

Tao Geng was born in 1983.He received the Ph.D degree in Cryptography from Beijing University of Posts and Telecommunications,Beijing,China in 2012.Now,he is working at Institute of Information Engineering, Chinese Academy of Sciences,Beijing.His interests include information security, secure multi-party computation,etc.

Haiyang Ding received his M.S. degree in signal and information processing from Beijing Jiaotong University, Beijing in 2004, and his B.S. degree in electronics and information technology from Beijing Jiaotong University, Beijing in 2001. He is currently a Ph.D. candidate at Beijing University of Posts and Telecommunications, Beijing, China. His current research interests include information security, digital image processing, DSP technology.