Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):611-620

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Verifiable multi-authority attribute based encryption scheme with different permissions

Xueyan Liu[1,2], Zhanming Li[1], Zhanjun Hao[3] and Qiang Zhang[3]

[1]*College of Telecom Engineering and Information Engineering, Lanzhou University of Technology, Lanzhou; China*
[2]*College of Mathematics and Statistics, Northwest Normal University, Lanzhou, China*
[3]*College of Computer Science and Engineering, Northwest Normal University, Lanzhou, China*

ABSTRACT

In this paper, we study the traffic information granular computing theory and build traffic information fusion model, framework and implementation program based on granular computing. We raise uncertainty reduction algorithms for traffic flow prediction and congestion recognition algorithms based on granular computing theory, which will provide new ideas and methods in the complex decision making under uncertainty problems of the transportation systems. In an attribute based encryption scheme, each user is identified by a set of attributes, which are used to determined ecryption ability for each ciphertext. On the base of attribute based encryption and symmetric encryption algorithm, it proposes a verifiable multi-authority attribute based encryption scheme. In our scheme, access control permission is divided into two kinds: Read and Write for the first time. An encryptor can easily deal with this problem by using two different secret keys. When a user wants to get Read permission, he just needs to go to some authorities, yet not all. We also provide a verification scheme that ensures the integrity of data and realness of data sources. The encryptor generates a signature while encryption, the user carries out verification with given signature and the decrypted message. The scheme not only enhances the confidentiality of data, but also supports more flexible and more fine-grained access control strategy.

Key words: Multiple authorities, Attribute based encryption, Identity based encryption, Permission , Pseudorandom function(PRF)

INTRODUCTION

In 2005, Sahai and Waters introduced Fuzzy Identity-basedEncryption(Fuzzy-IBE) firstly[1].In the scheme, theidentity of user was described as a set of attribute, while thematching relation of identity was transited from the original“match” into“similarity matching”. 2006, Fuzzy-IBE is extended tothe attribute based encryption(ABE) by Goyal, Sahai and Waters etal.[2], they also expounded the concept and significance ofattribute based encryption. In attribute based encryptionmechanism, the user identity information was generalized asrelated attributes, and they divided ABE scheme into twotypes:*Ciphertext-Policy ABE*(CP-ABE) and*Key-PolicyABE* (KP-ABE) based on differentapplication.

With some basic schemes[3,4,5] proposed,researchers put forward the deep research work and researchdirection on attribute cryptography. Emura[6] and Chen etal. [7] considered the c“and” gate access structure. Attrapadung and Libert[8] constructed a ABE scheme supporting general access structure. Thelength of ciphertext and the encryption or decryption cost wasconstant in this scheme. Based on LWE problem, Agrawal etal. [9] has presented a new ABE scheme, in which accesspolicy was threshold, it also discussed the difficulty of generalaccess structure based on lattice. Maji et al. [10] firstpresented the concept and safety definition on attribute basedsignature(ABS). In ABS, the signer generates a signature whengiven a message and a policy, the verifier can ensure whether thesignature has been generated by the user who satisfying attributepolicy.Ateniese et al. [11] first proposed an attributebased secret handshakes scheme, which opened the research ofattribute based security protocol.Chase et al. [12,13] solved a single authority corrupted problem by employing multipleauthorities, and prevent the collusion between users by adopting aglobal identity GID for each user. Lewko et al. [14] present another multi-authority scheme, in which any party canbecome an authority and does not require any"central authority".

Attribute based encryption has been rapid developed since it wasborn,and it is a hot direction in cryptograph recently, whichrealizes non interactive fine-grained access control mechanism,expands one-to-one model to one to many model on encryption anddecryption, greatly enriches the flexibility of encryption policyand description of user permissions. Hence, it has a goodapplication prospects in distributed file management, third partydata storage, pay TV system and other fields[15,16].

However, in all existing ABE schemes, all users can only get onesame kind of permission if satisfying access policy. With therapid development of network, the rise of cloud computing anddifferent demand growth of large-scale user, it is necessary togive users different permissions. For example:there are fourattribute authorities monitoring four attribute sets $\mathrm{A}_1=\{a_1,a_2,a_3\}$, $\mathrm{A}_2=\{a_4,a_5\}$, $\mathrm{A}_3=\{a_6,a_7,a_8\}$, $\mathrm{A}_4=\{a_9,a_{10},a_{11},a_{12}\}$,the minimalrequirement are $d_1=2$, $d_2=1$, $d_3=2$, $d_4=2$. u_1, u_2, u_3 arethree users and C_1,C_2,C_3 are ciphertexts, the relatedattributes sets are $\mathrm{A}_{u1}=\{a_1,a_2,a_4,a_6,a_8,a_9,a_{10}\}$, $\mathrm{A}_{u2}=\{a_1,a_4,a_7,a_8\}$, $\mathrm{A}_{u3}=\{a_1,a_2,a_4, \quad a_7,a_8,a_{10},a_{12}\}$, $\mathrm{A}_{C1}=\{a_1,a_2,a_4,a_6,a_7,a_8\}$, $\mathrm{A}_{C2}=\{a_6,a_8,a_9,a_{10}\}$, $\mathrm{A}_{C3}=\{\{a_1,a_2,a_4,a_6,a_8\},\{a_1,a_2,a_4,a_6,a_8,a_{10},a_{11},a_{12}\}\}$.

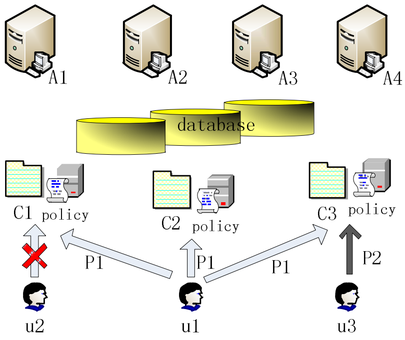

Fig. 1:More Fine-grained Access control From ABE

In Fig 1, 1) u_1 can decrypt C_1,while u_2 can't.And u_1 only goes to attribute authority A_1, A_2 and A_3,not to A_4;2) u_1 can decrypt C_1 and C_2,but referring differentauthorities set $\{\mathrm{A}_1,\mathrm{A}_2,\mathrm{A}_3\}$ and $\{\mathrm{A}_3,\mathrm{A}_4\}$, the number ofauthorities is different,too;3) u_1 gets P_1 permission bygoing to $\{\mathrm{A}_1,\mathrm{A}_2,\mathrm{A}_3\}$, but u_3 gets P_2 permission bygoing to all authorities.

From the example,we can see that:1)in differentapplications,there are many permissions,such as*Read*, *Copy*, *Reference* and*Write*. Therefore, permission problem should be consideredwhile designing access control policy. The basic operation of useris*Read* or *Write*. Of course, one also has*Read* permission if he has*Write* permission; 2) auser can get one permission while only going to some authorities.We also provide a verification scheme by a signature. Hence, inthis paper,in order to present *Read* Permission and*Write*Permission, we select two different key to controlthe two permissions,and the access policy is generated byencryptor.

The remainder of this paper is organized as follows: We discussthe novelty and contributions of this paper in Section II. InSection III, definitions and preliminaries are presented. In Section IV, the proposed verifiable multi-authority attribute basedencryption scheme with different permission is presented, and thesecurity analysis of the proposed scheme is discussed. In Section V, performance discussion is presented. Finally, conclusions andpossible future research directions are presented in Section VI.

OUR CONTRIBUTIONS

The object of our proposal is to present a verifiablemulti-authority ABE Scheme and resolve following problems:

- Many scholars have applied ABE to access control, but theissue of different permissions in one system has been ignored.Forexample,some users can read,others can copy.
- In the previous multi-authority schemes,the user mustsatisfy the attributes requirement of each authority to getdecryption ability. It is to say that the user must go to allauthorities.The author of [12] referred the problem inextensions,but there was some limit,which will be discusseddetailed in section V.B.
- In existing attribute based encryption scheme,the attention is focused on decryptor,while the honesty of encryptorand the integrity of data are ignored. For example,a user meetingthe attribute requirement got a message while the message has beencorrupted before encrypted.

To overcome these problems,we propose a verifiable multi-authorityattribute based encryption scheme with different permissions. Thescheme works as follows:First,the central authority setup thesystem parameters, and all authorities generate public keys andsecret keys for user u. Second,a sender encrypts a message M with a symmetric key K_{read} ,which only provides *Read* permission.Then K_{read} and *Write*permission K_{write} are encrypted respectively. In the process theencryptor generates access control policy for users and generatesa signature on M . Third, the user gets *Read*permissionand M , just meeting some authorities requirement,or even one.After, the user can verify the integrity of M and authenticityof the encryptor by offered signature. Moreover,if the user wantsto obtain*Write* permission, he should meet all attributerequirements of all authorities including the central authority.

The contributions of this paper are as follows:

- In the scheme, we realize the permission distinguishthat let user get *Read* Permission or *Write*Permission based on having attributes. The access control policyis generated by the encryptor, so the encryptor has more choicerights, which is more friendly to users. On the premise of theprotection of data confidentiality, the scheme provides differentpermissions for users having different attributes.
- To obtain *Read* permission, just some authority are involved,even only one. This scheme avoids the shortcomings that onemust go to all attribute authorities.
- There generates a BLS short signature[17] formessage M while encryption to present verification, whichensures the confidentiality, integrity of data and non-repudiationof encryptor.

PREMINARY

In our ABE scheme,we assume that:1) there are K attributeauthorities and a trusted central authority.2) the universe ofattributes can be partitioned into K attribute sets. Eachattribute authority will monitor one attribute set while thecentral authority will not monitor any attributes.The notations referred in the paper will be shown in Table I.

Table.1 Notation

Item	Description
A_u	the attribute set of user u
A_C	the attribute set of a ciphertext
A_u^k	attributes of u handled by authority k
A_C^k	attributes of ciphertext handled by authority k
GID	the global identity of each u
d_k	the required minimum number of $\mid \mathrm{A}_u^k \cap \mathrm{A}_C^k \mid$

A. BILINEAR MAPS AND COMPLEXITY ASSUMPTION

Let $\mathbf{G}_1$ and $\mathbf{G}_2$ be two cyclicmultiplicative groups of the same large prime order p .

Definition 1 *(Bilinear Maps)* A bilinear pairing is a computable bilinear map between two groups e: $\mathbf{G}_1 \times \mathbf{G}_1 \to \mathbf{G}_2$ .It is the modified Weil pairing or Tatepairing which has the following properties:

1).*Bilinear*: For any $g^a, g^b \in \mathbf{G}_1$, $e(g^a, g^b) = e(g, g)^{ab}$;

2).*Non-degenerate*: There exists $P, Q \in \mathbf{G}_1$, such that $e(P, Q) \neq 1$;

3).*Efficient*: There exists an efficient algorithm to compute the map.

Definition 2 *(Decisional Bilinear Diffie-Hellman (BDH) Assumption)*Suppose a challenge chooses a, b, c, R from $\mathbf{Z}_p^*$ randomly. The decisional BDH Assumption is that no polynomial-timeadversary is to be able to distinguish the tuple $< g, g^a, g^b, g^c, e(g,g)^{abc} >$ from the tuple $< g, g^a, g^b, g^c, e(g,g)^R >$ with more than a negligible advantage.

Definition 3 *(Decisional Modified Bilinear Diffie-Hellman (MBDH) Assumption)*Suppose a challenger chooses a,b,c,R from $\mathbf{Z}_p^*$ randomly. The decisional MBDH Assumption is that no polynomial-timeadversary is to be able to distinguish the tuple $< g, g^a, g^b, g^c, e(g,g)^{\frac{ab}{c}} >$ from the tuple $< g, g^a, g^b, g^c, e(g,g)^R >$ with more than a negligible advantage.

B.VERIFIABLE MULTI-AUTHORITY ABE SCHEME WITH DIFFERENT PERMISSIONS(VMA-ABE-DP)

The proposed scheme of verifiable multi-authority ABE scheme withdifferent permissions consisting of four phases: **Setup**,**KeyGen**, **EncSig** and**DecVer**, are shown as follows.

- **Setup**: Given a security parameter, thetrusted central authority runs a randomized algorithm whichoutputs a public key, secret key pair for each of the attributeauthorities, and also outputs a system public key and mastersecret key for himself.
- **KeyGen**:In this phase,there are two types of key:Attribute Key Generation and Central key Generation.

-**Attribute Key Generation**:A randomized algorithm run byan attribute authority.Takes as input the authority's secretkey,the authority's value d_k, a user's **GID**,and a set of attributes in the authority's domain.Outputs secretkey for the user.

-**Central Key Generation**:A randomized algorithm run by the central authority.Input the master secret key and a user's**GID**,then output secret key for the user.

- **EncSig**: The sender carries out two work:Encrypt and Signature

-**Encryption**:A randomized algorithm run by aencryptor. Input a set of attributes for some or all authorities,a message,and the system public key.Outputciphertext.

-**Signature**:A randomized algorithm run bya encryptor. Input a message and the signature key.Output signature.

- **DecVer**: The user carries out two work:Decrypt and Verification

-**Decryption**:A deterministic algorithm run by a user. Takes as input a ciphertext, which is encrypted under attribute set A_C and decryption keys for an attribute set A_u .Outputs a message M if $|\mathrm{A}_C^k \cap \mathrm{A}_u^k| \geq d_k$ for a certain number of authorities or all authorities k .

-**Verification**:A verification algorithm run by a user.Takes as input a signature, the system public key and the decrypted M .Outputs *Yes* or *No*.

C. SECURITY MODEL

To prove confidentiality of the proposed scheme,consider theselective identity(sid) attack model,the prototype scheme isselective identity security model in[1,12]. The game is followed.

- **Setup**

-The adversary sends a list of attribute sets $\mathrm{A}_C = \mathrm{A}_C^1 \cdots \mathrm{A}_C^l, l \leq K$, onefor each authority.He also sends a list of corrupted authoritieswhich cannot include the central authority.

-The challenger generates parameters for the system and sends to the adversary.This means the system public key,public keys for all honest authorities, and secret keys for all corrupted authorities.

- **Queries**: The adversary can make as many secret key queries as he wants to the attribute authorities or to the central authority. The only requirements are same as in [12].
- **Challenge**: The adversary sends two messages M_0 and M_1.The challenger chooses a bit b , computes the encryption of M_b under symmetric key which is encrypted for attribute set A_C, and sends these ciphertexts to the adversary.

- **More Queries**: The adversary may make more secret key queries subject to the requirements described above.

- **Guess**: The adversary outputs a guess b'

The adversary is said to succeed if $b = b'$.

***Definition 4** (Selective ID Secure)}*The verifiablemulti-authority attribute scheme with different permissions issid-secure if there exists a negligible function ν such that,in above game any adversary will succeed with probability at most $\frac{1}{2} + \nu(k)$.

D. BLS SIGNATURE

The signature scheme comprises three algorithms, **KeyGen**,**Sign**, and **Verify**. It makes use of a full-domainhash function $H : \{0,1\}^* \to \mathrm{G}_1$.

KeyGen:Pick $x \in_R \mathbf{Z}_p^*$, compute $PK = g^x$.The public key is PK, the secret key is x.

Sign:Given the secret key x and a message M, compute $h = H(M)$ and $\sigma = h^x$. The signature is σ.

Verify:Given a public key PK, a message M and asignature σ, compute $h = H(M)$. Then verify $e(g,\sigma) = e(PK, h)$.

VERIFIABLE MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION SCHEME WITH DIFFERENT PERMISSIONS(VMA-ABE-DP)

We now present our verifiable multi-authority attribute basedencryption scheme with different permissions. We use mixedencryption mechanism, where a symmetric key K_{read} is used toencrypt a message, then K_{read} and K_{write} are encryptedwith the public key cryptosystem. In order to preventcollusion,the scheme uses the global identity **GID** foreach user,and which is tied with his attributes and his publickey.There is also a BLS short signature to monitor the encryptor.

A. CONSTRUCTION

The proposed verifiable multi-authority attribute based encryptionscheme with different permissions vMA-ABE-DP, consisting of fourphases: **Setup**, **KeyGen**,**EncSig**and**DecVer**, are shown as follows.

- **Setup**: Let $\mathbf{G}_1$, $\mathbf{G}_2$ be twocyclic group of prime order p and generator $g \in \mathbf{G}_1$, $e : \mathbf{G}_1 \times \mathbf{G}_1 \to \mathbf{G}_2$.Select seeds $s_1, \cdots, s_K$ for all authorities.Also select $y_0, \{t_{k,i}\}_{k=1,\cdots,K; i=1,\cdots,n}$ from $\mathbf{Z}_q$. H isa hash function, $H : \{0,1\}^* \to \mathbf{G}_1$.

System Public Keyis $Y_0 = e(g,g)^{y_0}$.

- **KeyGen**:

-Attribute Authority k

Authority Secret Key $s_k, t_{k,1}, \cdots, t_{k,n}$

Authority Public Key $T_{k,1}, \cdots, T_{k,n}$ where $T_{k,i} = g^{t_{k,i}}$, $Y_{k,u} = e(g,g)^{y_{k,u}}$.

Authority Key for User u Let $y_{k,u} = F_{s_k}(u)$.Select random $d_k - 1$ degree polynomial p with $p(0) = y_{k,u}$.Secret key: $\{D_{k,i} = g^{\frac{p(i)}{t_{k,i}}}\}_{i \in \mathrm{A}_u}$.

- Central Authority k

Central Authority Secret Key y_0

Secret Key for User u Let $y_{k,u} = F_{s_k}(u)$.Secret key : $D_{CA} = g^{(y_0 - \sum_{k=0}^{K} y_{k,u})}$.

- **EncSig**:The user whose identifier is**GID**, randomly selects $s \in_R \mathbf{Z}_q$, $P_u = g^s$, $\{E_{k,i} = T_{k,i}^s\}_{i \in \mathrm{A}_u, \forall k}$. M is a message with a symmetric key K_{read} (such as AES),which control *ReadPermission*,and *WritePermission* key: K_{write} .

-**Encryption**: $C_r = E_{K_{read}}(M)$, $E = Y_0 K_{write}$ .Theuser generates a set $LEB = \{k \,||\, \mathrm{A}_C \cap \mathrm{A}_u \,| \geq d_k\}$ and K_{read} is partitioned into $|LEB|$ parts: $K_{r1}, \cdots, K_{r|LEB|}$,where $K_{read} = K_{r1} \| \cdots \| K_{r|LEB|}$ .Then $\{EE_k = Y_{k,u}^s K_{rk}\}_{k \in LEB}$.

-**Signature**:Compute $h = H(M)$ and $\sigma = h^s$ .The signature is σ .

The ciphertextis:
$C = < C_r, E, P_u, \{E_{k,i}\}_{i \in \mathrm{A}_u, \forall k}, \{EE_k\}_{k \in LEB}, \sigma >$.

- **DecVer**:

-**Compute** K_{read} :For each authority $k \in LEB$, for d_k attributes $i \in \mathrm{A}_C^k \cap \mathrm{A}_u^k$,compute $e(E_{k,i}, D_{k,i}) = e(g,g)^{p(i)s}$ .Interpolate to find $Y_{k,u}^s = \prod e(g,g)^{p(i)s\Delta_{i,S}(0)} = e(g,g)^{p(0)s} = e(g,g)^{y_{k,u}s}$,then compute $\{K_{rk} = EE_k / Y_{k,u}^s\}_{k \in LEB}$ to get $K_{read} = K_{r1} \| \cdots \| K_{r|LEB|}$, so

$$M' = D_{K_{read}}(C_r) \qquad (1)$$

-**Verification**:First,the user computes $h = H(M)$ .Then verifies

$$e(g,\sigma) = e(P_u, h) \qquad (2)$$

If (2) is established, M and the encryptor are not corrupted;else, M is corrupted or the signer is not the right one.

-**Compute** K_{write} :For each authority k and d_k attributes $i \in \mathrm{A}_C^k \cap \mathrm{A}_u^k$, compute $e(E_{k,i}, D_{k,i}) = e(g,g)^{p(i)s}$. Interpolate to find $Y_{k,u}^s = e(g,g)^{p(0)s} = e(g,g)^{y_{k,u}s}$ for each k .Compute $Y_{CA}^s = e(E_{CA}, D_{CA})$,combine these values to obtain $Y_{CA}^s \square \prod_{k=1}^{K} Y_{k,u}^s = Y_0^s$,then

$$K_{write} = E / Y_0^s \qquad (3)$$

B. CORRECTNESS

Now gives the correctness verification.

(1) $EE_k / Y_{k,u}^s = EE_k / e(g,g)^{p(0)s} = Y_{k,u}^s \square K_{rk} / \prod e(g,g)^{p(i)s\Delta_{i,S}(0)} = K_{rk}$

$K_{read} = K_{r1} \| \cdots \| K_{r|LEB|}, M = D_{K_{read}}(C_r)$.

(2) $e(g,\sigma) = e(g,h^x) = e(g^x,h) = e(P_u,h)$

(3) $$\begin{aligned} E / Y_0^s &= E / (Y_{CA}^s \square \prod_{k=1}^{K} Y_{k,u}^s) \\ &= E / (e(E_{CA}, D_{CA}) \square \prod_{k=1}^{K} e(g,g)^{p(i)s\Delta_{i,S}(0)}) \\ &= K_{write} \end{aligned}$$

C.SECURITY

In vMA-ABE-DP, not only the confidentiality of data is guaranteed,but the integrity of data and authenticity of data sources areverified. So the security of the scheme includes two parts:dataconfidentiality and signature unforgeability. Data confidentialitywill be proved under selective-ID model, and signatureunforgeability will be proved under adaptive selective-messageattack.

Theorem 1.This scheme is sid-secure according todefinition 4.

First we give some explain about behind proof. Then we follow witha detail proof.

About confidentiality: In our scheme, there are two kinds of permissions, which have been obtained by two different decryptionrespectively, the attribute authority number of the user must go to isdifferent,too. Especially,the central authority need not take part in the first kind of decryption. The two processes involve the confidentiality, but the details are different, we will give proofsdistinctly.

About Read Permission: Getting this kind of permission only need some authority,at least one. The adversary is allowedto request secret key for a given user u and attribute set A_u as long as there remains one honest authority k such that $|\mathrm{A}_C^k \cap \mathrm{A}_u^k| < d_k$. Thus, in the worst case,forall but one authority k, the adversary will be able to compute $Y_{k,u}^s = e(g,g)^{y_{k,u}s}$ for additive share $y_{k,u}$. We need $K_{rk} = EE_k / Y_{k,u}^s$ to be something which the adversary cannot compute($e(g,g)^{\frac{ab}{c}}$ is indistinguishable from random). Thus, we must "embed" this incomputable value in the share $y_{k,u}$ for the authority from which the adversary does nothave sufficient attributes. Since, in the process of decryption K_{rk}, only need to meet the requirements of one authority,so the prove process may look on as a single authority scheme.

About Write Permission: The process of encryption anddecryption is same as Chase's, so the detailed proof seeliterature[12].

Proof:The confidentiality proof of the scheme comprises twostages,one is to get K_{read} to decrypt the encrypted message,the other is to get K_{write}.

The first stage): Suppose there exists a polynomial-timeadversary, A,that can attack our scheme in theSelective-ID model with advantage ε. The challenge C that can play the Decisional MBDH game withadvantage $\frac{\varepsilon}{2}$.The simulation proceeds as follows:

The challenger sets the groups G_1 and G_2 with an efficient bilinear map, e and generator g. The challenger flips a fair binary coin, μ ,outside of C's view. If $\mu = 0$,the challenger sets $(A,B,C,Z) = (g^a, g^b, g^c, e(g,g)^{\frac{ab}{c}})$; otherwise it sets $(A,B,C,Z) = (g^a, g^b, g^c, e(g,g)^R)$ for random a,b,c,R.

SetupThe adversary sends an attribute set A_C^k for an honest authority.The challenge generatesthe public key parameters as follows.Given $Y_k = e(g,A) = e(g,g)^a$, chosen random $\beta_{k,i} \in \mathbf{Z}_p$, $\{T_{k,i} = g^{c\beta_{k,i}}\}_{i\in \mathrm{A}_C^k}$, and $\omega_{k,i} \in \mathbf{Z}_p$, $\{T_{k,i} = g^{\omega_{k,i}}\}_{i\in \mathrm{A}_u^k - \mathrm{A}_C^k}$.

Secret Key Queries The adversary A requestsfor private keys where the attribute set A_u^k satisfied $|\mathrm{A}_C^k \cap \mathrm{A}_u^k| < d_k$. We firstdefine three sets Γ, Γ', S in the following manner:

$$\Gamma = \mathrm{A}_C^k \cap \mathrm{A}_u^k$$
$$\Gamma \subseteq \Gamma' \subseteq \mathrm{A}_u^k \text{and} |\Gamma'| = d-1$$
$$S = \Gamma' \cup \{0\}$$

Now,we define the decryption key components $D_{k,i}$ for $i \in \Gamma'$ as:

If $i \in \Gamma : D_{k,i} = g^{s_i}$, where $s_i \in_R \mathbf{Z}_p$

If $i \in \Gamma' - \Gamma : D_{k,i} = g^{\frac{\lambda_i}{\omega_{k,i}}}$, where $\lambda_i \in_R \mathbf{Z}_p$

The intuition behind these assignments is that we are implicitly choosing a random $d-1$ degree polynomial $p(x)$ by choosing itsvalue for the $d-1$ points randomly in addition to having $p(0)=a$. For $i \in \Gamma$ we have $p(i) = c\beta_{k,i}s_i$ andfor $i \in \Gamma' - \Gamma$ we let $p(i) = \lambda_i$.

The challenge C can calculate the other $D_{k,i}$ values where $i \notin \Gamma'$ since the challenger knows the discrete log of $T_{k,i}$ for all $i \in \mathrm{A}_u^k - \mathrm{A}_C^k$. The challenger makes the assignments sa follows:
If $i \notin \Gamma'$:

$$D_{k,i} = (\prod_{j\in\Gamma} C^{\frac{\beta_{k,j}s_j\Delta_{j,S}(i)}{\omega_{k,j}}})(\prod_{j\in\Gamma'-\Gamma} g^{\frac{\lambda_j\Delta_{j,S}(i)}{\omega_{k,j}}})Y^{\frac{\Delta_{0,S}(i)}{\omega_i}}$$

Using interpolation C is able to calculate $D_{k,i} = g^{\frac{p(i)}{t_i}}$ for $i \notin \Gamma'$ where $p(x)$ was implicitly defined by the random assignment of the other $d_k - 1$ variables $D_{k,i} \in \Gamma'$ and $Y_{k,u}$ .Therefore ,thesimulator is able to construct a private key for the attribute set A_u^k .

ChallengeThe adversary A submits two challenge messages M_0 and M_1 to the challenger.The challenger flips a fair binary coin, b , and returns an encryption of M_b . The ciphertext is output as:

$$C_{rb} = E_{K_{read}}, \{E_{k,i} = B^{\beta_i}\}_{i\in \mathrm{A}_C}, EE_k = e(g,A)^{\frac{s_i}{c\beta_{k,i}}} \cdot K_{rk}$$

If $\mu = 0$, then $Z = e(g,g)^{\frac{ab}{c}}$ .If we let $r' = \frac{b}{c}$, then we have $E_0 = e(g,g)^{\frac{ab}{c}} \cdot K_{rk} = e(g,g)^{ar'} \cdot K_{rk} = Y_k^{ar'} \cdot K_{rk}$ and $E_{k,i} = B^{\beta_{k,i}} = g^{b\beta_{k,i}} = g^{\frac{bc\beta_{k,i}}{c}} = g^{r'c\beta_{k,i}} = (T_{k,i})^{r'}$ .Therefore,the ciphertext is a random encryption of the message M_b under A_C .

Otherwise, if $\mu = 1$, then $Z = e(g,g)^R$. We then have $E_1 = e(g,g)^R \cdot K_{rk}$, since R is random, E' will be arandom element of G_2 from the adversaries view and themessage contains no information about M_b .

More Secret Key Queries The challenger acts exactly as itdid above.

Guess A will submit a guess b' of b . If $b = b'$ the challenger will output $\mu' = 0$ to indicate that it wasgiven a MBDH-tuple,otherwise it will output $\mu' = 1$ to indicateit was given a random 4-tuple.

In the case where $\mu = 1$ the adversary gains no information about b . Therefore, we have $\Pr[\nu \neq \nu' \mid \mu = 1] = \frac{1}{2}$. Sincethe challenger guesses $\mu' = 1$ when $b \neq b'$, we have $\Pr[\mu' = \mu \mid \mu = 1] = \frac{1}{2}$. If $\mu = 0$ then the adversarysees an encryption of M_v . The adversary's advantage in thissituation is ε by definition. Therefore, we have $\Pr[b = b' \mid \mu = 0] = \frac{1}{2} + \varepsilon$. Since the challenger guesses $\mu' = 0$ when $b = b'$,we have $\Pr[\mu = \mu' \mid \mu = 0] = \frac{1}{2} + \varepsilon$ .The overall advantage of the challenger in the decisional MBDHgame is

---

$\frac{1}{2}\Pr[\mu'=\mu\mid\mu=0]+\frac{1}{2}\Pr[\mu'=\mu\mid\mu=1]-\frac{1}{2}=\frac{1}{2}(\frac{1}{2}+\varepsilon)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{1}{2}\varepsilon$ *The second stage)*: The same as in [12].

Theorem 2.The signature scheme in vMA-ABE-DP is secure against existential forgery on adaptive chosen-message attacks in Random Oracle Modelif BLS signature is secure against existential forgery on adaptivechosen-message attacks.

Proof: The signature of the scheme is BLS shortsignature.Since BLS signature is secure against existentialforgery on adaptive chosen-message attacks,so ours is.

DISCUSSION

A. DISCUSSION

In the scheme,we encrypt secret keys K_{read} instead ofmessage M ,alleviating the burden of encryption. K_{read} is dividedinto LEB parts and encrypted,which avoiding an adversary obtains M with $l < LEB$ parts and enhancing the security of the scheme.

We combine thesymmetric and asymmetric key system effectively.The mixedencryption mechanism(To ensure efficient encryption usingsymmetric key encryption of data, the encryption key is encryptedwith the public key cryptosystem), ensure illegal users not toget encryption key.

Prevent illegal users and malicious users destroying informationof the legitimate and honest users in the system. One side, thesignature can be used to verify the message sources; on the otherside, even if illegal users can crack encrypted data, they can notwrite data to the legitimate user message for not knowing K_{write} , illegally modified data can also be checked out.

B. COMPARISON

About the number problem of authorities, which the user must go tobefore he can decrypt a message,was discussed in our scheme andChase's,but there was some limit in Chase's.Now we will give somecomparison followed.

1)We remove this problem by increasing a public key $Y_{k,u}=e(g,g)^{y_{k,u}}$ by each attribute authority. Theencryptor include $EE_k=Y_{k,u}^{s}\cdot K_{rk}$ in the encryptionbased on $LEB=\{k \,||\, \mathrm{A}_C\cap\mathrm{A}_u \,|\geq d_k\}$ .Todecrypt a message without to go to authorities that not in LEB .In Chase's scheme,he added one "authority attribute k " foreach authority and a corresponding $T_{Nk}=g^{t_{Nk}}$ to thepublic key,the central authority gave every user a secret key foreach authority: $D_{Nk}=g^{y_{k,u}/t_{Nk}}$ .The encryptor wouldinclude T_{Nk}^{s} in the encryption for these authorities withoutrequired any attributes and a user would combine T_{Nk}^{s} and D_{Nk} while decryption. We can make a conclusion that thecentral authority and the encryptorare involved as generating accesspolicy in Chase's while only encryptor did in ours, which reducesthe dependenceon the central authority's, more easilyextended to semi-trusted authority or no trusted authorityscheme.

2)Chase et.al. made an extension to let the user to go to at least D authorities while decryption,yet in our scheme,it can bearbitrary number authority specified by encryptor. As aresult,ours is more flexible in application.

3) In the above process, there is added some information in both schemes. We assume that there is only a user, K attribute authorities, x attribute authorities without required any attribute in [12], $|LEB|$ attribute authorities involved while decryption in our scheme. The comparison of added information is shown in Table II. In [12], increased one authority attribute k and one public key for each attribute authority, increased every user a secret key D_{Nk} foreach attribute authority, increased T_{Nk}^{s} in the encryption for x authorities withoutrequired any attributes, the total increased communication is $K|k|+2K|p|+x|p|$. Yet, in our scheme, increased a public key for each attribute authority and $|LEB|$ EE_k , the total increased communication is $(K+|LEB|)|p|$. While decryption, there still needs to compute K $e(g,g)^{y_{k,u}s}$ in [12], the amount of computation does not increase nor decrease.

However, it only needs to compute $\lvert LEB \rvert\, e(g,g)^{y_{k,u}s}$ in our scheme, where $1 \leq \lvert LEB \rvert \leq K$, so the amount of computation reduced at least $K - \lvert LEB \rvert$. Thus, from the analysis of increased communication and computation, our scheme is significantly better.

Table.2Additional Information

Item	**[12]scheme**	**Our scheme**
Each attribute authority	a authority attribute k a public key T_{Nk}	a public key
Central authority	K secret key D_{Nk}	0
ciphertext	$x\ T_{Nk}^{s}$	$\lvert LEB \rvert EE_{k}$
decryption	0 computational cost	$-(K - \lvert LEB \rvert)$ computational cost

CONCLUSION

We create a novel scheme of verifiable multi-authority attributebased encryption. Our scheme allows users having differentattributes to obtain different access permissions.In the process, thenumber of authority is not fixed. All these are done by encryptoreasily. Our system allows decryptorto verify the integrity of dataand realness of encryptor who provided a signature on message.

Next, it would be interesting to consider much more accesspermission in attributes based encryption scheme. With the rapiddevelopment of cloud compute,we will apply it in cloud storage.

Acknowledgments
The authors wish to thank the anonymous referees for their patiencein reading this manuscript and their invaluable comments andsuggestions.

The work was supported by the National Natural Science Foundationof China under grant (61163038, 71263045);The Ministry ofeducation of Humanities and social science research projects (12YJCZH282)；The Ministry of education program for New Century Excellent Talents (ncet-12-0620).

REFERENCES

[1] A.Sahai, B.Waters. *Advances in Cryptology*, **2005,**3494(5),457-473.
[2] V. Goyal, O. Pandey, A. Sahai, et al. Attribute-based encryption for fine-grained access control of encrypted data, *Proceedings of the 13th ACM Conference on Computer and Communications Security*,**2006,**3(10),89-98.
[3] J. Bethencourt, A.Sahai, B. Waters. *IEEE Symposium on Security and Privacy*, **2007,**6571 (3),321-334.
[4] L. Cheung, C. Newport. Provably secure ciphertext-policy ABE, *Proceedings of the 14th ACM Conference on Computer and Communications Security*, **2007**,5932(8),456-465.
[5] B. Waters. *PublicKey Cryptography-PKC 2011*, **2011**,6571(3),53-70.
[6] K.Emura, A. Miyaji, A. Nomura, et al. *Information Security Practice and Experienc*e, **2009**,5451(4),13-23.
[7] C. Chen, Z. F. Zhang, D. G. Feng. *Provable Security*, **2011**,6980(10),84-101.
[8] N. Attrapadung, B.Libert, E. De Panafieu. *Public Key Cryptography-PKC 2011*,**2011**,6571(3), 90-108.
[9] S. Agrawal,X.Boyen,V.Vaikuntanathan, et al. *Public Key Cryptography-PKC 2012*,**2012**,7293(5),280-297.
[10] H. K.Maji, M.Prabhakaran, M .Rosulek. Attribute-based signatures, *Topics in Cryptology-CT-RSA 2011*,**2011**, 376-392.
[11] G. Ateniese, J. Kirsch, M. Blanton. *Theory of Cryptography*, **2007**,4392(2),515-534.
[12] M. Chase, S.S. M. Chow. Improving privacy and security inmulti-authority attribute-based encryption, *Proceedings of the 16th ACM Conference on Computer and Communications Security*.ACM, **2009**,121-130.
[13] A. Lewko, B. Waters. *Advances in Cryptology-EUROCRYPT* 2011, **2011**,6632(5),568-588.
[14] M. Pirretti, P. Traynor, P.Mc Daniel, et al. Secure attribute-based systems, *ACM Conference on Computer and Communications Security-CCS 2006*. **2006**,18(5),99-112.
[15] Qinlong Huang, Zhaofeng Ma, Jingyi Fu et al. *Journal of computers*,**2013**,8(11),2776-2780.
[16] D.Boneh, B. Lynn, H.Shacham. *Advances in Cryptology—ASIACRYPT* 2001, **2001**,2248(9),514-532.