Key distribution system and attribute-based encryption on non-commutative ring

Masahiro Yagisawa†
†Resident in Yokohama-shi
Sakae-ku , Yokohama-shi, Japan

SUMMARY:
I propose the new key distribution system and attribute-based encryption scheme on non-commutative ring where the complexity required for enciphering and deciphering is small. As in this system encryption keys and decryption keys involve the attributes of each user, the system is adaptive for cloud computing systems. The security of this system is based on the complexity for solving the multivariate algebraic equations of high degree over finite field, that is, one of NP complete problems. So this system is immune from the Gröbner basis attacks. The key size of this system becomes to be small enough to handle.
key words: key distribution, attribute-based encryption ,multivariate polynomial, Gröbner basis, NP complete problems

1. Introduction

Since Diffie and Hellman proposed the concept of the public key cryptosystem (PKC) and key agreement protocol (KAP) in 1976[1], various PKC and KAP were proposed [2],[3],[4].

Another new concept, attribute-based encryption (ABE) system was proposed in 2000's. As in ABE system encryption keys and decryption keys involve the attributes of each user, the system is adaptive for cloud computing systems. As almost all ABE systems proposed until now are based on the bilinear pairing, the complexity required for enciphering or deciphering is not small enough [5].

I propose the new key distribution system and attribute-based encryption system over non-commutative ring where the complexity required for enciphering and deciphering is small.

The security of our systems is based on the computational difficulty to solve the multivariate algebraic equations of high degree while the almost all multivariate public key cryptosystems[7],[8],[9],[10],[11] proposed until now are based on the quadratic equations avoiding the explosion of the coefficients. Because this system is based on multivariate algebraic equations of high degree, our scheme is against the Gröbner basis[6] attack, the differential attack, rank attack and so on.

Though I can construct this system over many non-commutative rings, I will adopt the ABE system based on the quaternion ring as the typical example for showing how this system is constructed.

In the next section, we begin with defining the multiplication and addition on quaternion ring H over finite field. In section 3, we describe the inverse of the element in H. In section 4, we classify users in cloud computing system. In section 5, we describe n-dimensional vector. In section 6, we describe the list of the n quaternions on the centre of cloud computing system. In section 7, we describe AND operation of enciphering keys. In section 8, we describe AND, OR and NOT operations of enciphering keys. In section 9, we describe the concrete method for enciphering/deciphering. In section 10, we describe cryptanalysis of the proposed system. In section 11, we show the numerical example for proposed system. In section 12, we describe the sizes of the keys and the complexity for enciphering/deciphering.

In the last section, we provide concluding remarks.

2. Multiplication and addition of $A,B \in H$

Let q be a prime. Let n, c, r and s be positive integers. Let SP be system parameters[q, n, c, r, s].The centre (trusted third party, TTP) chooses arbitrary parameters $Q(i)=(q_{i1},q_{i2},q_{i3},q_{i4}) \in H^*$, $(i=1,..,n)$, $q_{ij} \in Fq$ $(j=1,2,3,4)$ where H* is the set on the quaternion ring over finite field, Fq such that

$$H^* = \{(h_1,h_2,h_3,h_4) \mid h_1^2 + h_2^2 + h_3^2 + h_4^2 \neq 0 \bmod q, h_i \in Fq, (i = 1,2,3,4)\} \quad (1)$$
$$H = H^* \cup (0,0,0,0).$$

Let $A=(a_1,a_2,a_3,a_4) \in H, B=(b_1,b_2,b_3,b_4) \in H,$
We define $AB \bmod q$ such that
$AB \bmod q=(a_1b_1-a_2b_2-a_3b_3-a_4b_4 \bmod q,$
$a_1b_2+a_2b_1+a_3b_4-a_4b_3 \bmod q,$
$a_1b_3-a_2b_4+a_3b_1+a_4b_2 \bmod q,$
$a_1b_4+a_2b_3-a_3b_2+a_4b_1 \bmod q)$

$A+B \bmod q=(a_1+b_1 \bmod q,\ a_2+b_2 \bmod q,\ a_3+b_3 \bmod q,\ a_4+b_4 \bmod q)$.

3. Inverse of $Q(i)$

From (1) $Q(i)^{-1}$, the inverse of any $Q(i) \in H^*$ exists such that

$$Q(i)^{-1} = (h^{-1}q_{i1} \bmod q,\ h^{-1}q_{i2} \bmod q,\ h^{-1}q_{i3} \bmod q,\ h^{-1}q_{i4} \bmod q) \quad (2)$$
where
$$h = |Q(i)| = q_{i1}^2 + q_{i2}^2 + q_{i3}^2 + q_{i4}^2 \neq 0 \bmod q.$$

4. Classification of users in cloud computing system

We assign the class and rank to the user according to his/her attribute.
For example, when user A belongs to the class a and rank 3, use A is given three n-dimensional vectors mentioned in §5.

5. n-dimensional vector $V(a,j)$

We define the n-dimensional vector $V(a,j)$ as the encryption/decryption parameters such that

$$V(a,j)=(vaj_1, vaj_2, \ldots, vaj_n) \in Fq^n,\ vaj_k \in Fq \quad (a=1,..,c; j=1,..,r; k=1,..,n) \quad (3)$$
where
c is the number of the class of users in this system,
r is the number of the rank of users in this system.
User A is given $V(a,j), V(a,j-1),.., V(a,1)$ relating with his/her attribute i.e. class and rank.
Let (a,j) be the attribute where a is the name of class and j is the name of rank.
When user A belongs to the class a and rank 3,user A is given $V(a,1), V(a,2)$ and $V(a,3)$ from the supplier of information (SI).

6. List of n quaternions (LQ) to be non-commutative each other

The SI selects n quaternions such that

$$Q(i) \in H^*, (i = 1,\ldots n), \quad (4)$$
where
$$Q(i)Q(j) \neq Q(j)Q(i) \ (i \neq j),$$
$$(1 \leq i, j \leq n).$$

The SI publishes LQ, the list of the n quaternions, $Q(i)(i=1,..,n)$ on the centre of cloud computing system.

7. Basic method for enciphering/deciphering by only AND operation

SI distributes $V(a,j) \in Fq^n$ to user A who belongs to the class a and rank j through the secure communication line beforehand.

SI publishes cipher-text C corresponding to the message $M \in H$ on the centre of cloud computing system such that

$$E(a,i) = Q(Vai_1)Q(Vai_2)..Q(Vai_n) \bmod q, \quad (i=1,\ldots,j) \tag{5}$$

$$\left.\begin{array}{l} C=E(a,j)\cdot\cdot\cdot E(a,1)ME(a,1)^{-1}\cdot\cdot\cdot E(a,j)^{-1} \bmod q \in H \\ \text{where} \\ M=(M_1,M_2,M_3,M_4) \quad \in H \\ M_k \in Fq, \ (k=1,2,3,4) \end{array}\right\} \tag{6}$$

We consider that plaintext M is enciphered by using "AND" of enciphering keys $E(a,i)$ $(i=1,\ldots,j)$.

The user A downloads LQ and C from the centre of cloud computing system through the insecure communication line and deciphers C to obtain M' by calculating the decryption key $D(a,1),..,D(a,j)$ using $V(a,1),..,V(a,j)$ such that

$$D(a,i) = Q(Vai_1)Q(Vai_2)..Q(Vai_n) \bmod q, \quad (i=1,..,j) \tag{7}$$

$$M' = D(a,1)^{-1}..D(a,j)^{-1}CD(a,j)..D(a,1) \bmod q. \tag{8}$$

Since $E(a,i)=D(a,i)$ $(i=1,..,j)$, we obtain $M'=M$.

LQ is replaced at the every set of cipher-texts C or LQ is replaced periodically.

8. AND, OR, NOT operations

Here we define the AND, OR, NOT operations of encryption/decryption keys as follows.

8.1 AND operation of encryption keys

Let $E(a,j)$ and $E(b,k)$ be the encryption keys.

AND operation of $E(a,j)$ and $E(b,k)$, $AND[E(a,j),E(b,k)]$ is defined such that

$AND[E(a,j),E(b,k)]=E(a,j)E(b,k) \bmod q.$

Note that in general,

$AND[E(a,j),E(b,k)] \neq AND[E(b,k),E(a,j)]$.

8.2 OR operation of 2 encryption keys, (2-OR)

Let s be the positive integer to be published.

2-OR operation of $E(a,j)$ and $E(b,k)$, $OR[E(a,j),E(b,k),X]$ is defined such that

$$OR[E(a,j),E(b,k),X]=E(b,k)(1-E(a,j)^sE(b,k)^{-s})^{-1}(1-E(a,j)^sX)+ E(a,j)(1-E(b,k)^sE(a,j)^{-s})^{-1}(1-E(b,k)^sX) \bmod q.$$

If and only if (Iff) $X=E(a,j)^{-s}$,

$$OR[E(a,j),E(b,k),E(a,j)^{-s}]= 0+ E(a,j)(1-E(b,k)^sE(a,j)^{-s})^{-1}(1-E(b,k)^sE(a,j)^{-s}) =E(a,j) \bmod q$$

where $X \in H^*$, $0=(0,0,0,0) \in H$.

Iff $X=E(b,k)^{-s}$,

$$OR[E(a,j),E(b,k),E(b,k)^{-s}]=E(b,k)(1-E(a,j)^sE(b,k)^{-s})^{-1}(1-E(a,j)^sE(b,k)^{-s}) + 0=E(b,k) \bmod q.$$

(See <appendix> theorem 1)

8.3 OR operation of 3 encryption keys, (3-OR)

3-OR operation of $E(a,j),E(b,k)$ and $E(c,l)$, $OR[E(a,j),E(b,k),E(c,l),X]$ is given such that

$$\begin{aligned} OR[E(a,j),E(b,k),E(c,l),X]=&E(c,l)(1-E(a,j)^sE(c,l)^{-s})^{-1}(1-E(a,j)^sX)(1-E(b,k)^sE(c,l)^{-s})^{-1}(1-E(b,k)^sX) \\ &+ E(a,j)(1-E(b,k)^sE(a,j)^{-s})^{-1}(1-E(b,k)^sX)(1-E(c,l)^sE(a,j)^{-s})^{-1}(1-E(c,l)^sX) \\ &+ E(b,k)(1-E(c,l)^sE(b,l)^{-s})^{-1}(1-E(c,l)^sX)(1-E(a,j)^sE(b,k)^{-s})^{-1}(1-E(a,j)^sX) \bmod q \end{aligned}$$

where $X \in H^*$.
If $X=E(a,j)^{-s}$,
$OR[E(a,j),E(b,k),E(c,l),E(a,j)^{-s}]$
$=0+E(a,j)(1-E(b,k)^s E(a,j)^{-s})^{-1}(1-E(b,k)^s E(a,j)^{-s})(1-E(c,l)^s E(a,j)^{-s})^{-1}(1-E(c,l)^s E(a,j)^{-s})+0=E(a,j) \bmod q.$
If $X=E(b,k)^{-s}$,
$OR[E(a,j),E(b,k),E(c,l),E(b,k)^{-s}]$
$=0+0+E(b,k)(1-E(c,l)^s E(b,k)^{-s})^{-1}(1-E(c,l)^s E(b,k)^{-s})(1-E(a,j)^s E(b,k)^{-s})^{-1}(1-E(a,j)^s E(b,k)^{-s})=E(b,k) \bmod q.$
If $X=E(c,l)^{-s}$,
$OR[E(a,j),E(b,k),E(c,l),E(c,l)^{-s}]$
$=E(c,l)(1-E(a,j)^s E(c,l)^{-s})^{-1}(1-E(a,j)^s E(c,l)^{-s})(1-E(b,k)^s E(c,l)^{-s})^{-1}(1-E(b,k)^s E(c,l)^{-s})+0+0=E(c,l) \bmod q.$

As 3-OR operation has the second order polynomial of X, some values of X exist that satisfy the equation such that
$OR[E(a,j),E(b,k),E(c,l),X]=E(a,j) \bmod q.$
But the probability is very small that the value of X selected randomly satisfies the above equation because the value of modulus q is selected larger than $O(2^{20})$ as described in section 12.

t-OR operation is given by t-1 degree polynomials of X on H.

8.4 NOT operation of encryption key
NOT operation of $E(a,j)$, $NOT(E(a,j),X)$ is defined such that
$NOT[E(a,j),X]=(1-E(a,j)^s X)^{-1}(1-E(a,j)^s X) \bmod q,$
where we define
$(0 \bmod q)^{-1}=0 \bmod q.$
Then let $X=(0,0,0,0) \in H$,
$X^{-1}=(h^{-1}0 \bmod q, -h^{-1}0 \bmod q, -h^{-1}0 \bmod q, -h^{-1}0 \bmod q)=(0,0,0,0) \in H.$
where
$h=0^2+0^2+0^2+0^2=0 \bmod q,$
from definition
$h^{-1}=0 \bmod q.$
If $X=E(a,j)^{-s}$,
$NOT(E(a,j),X)=(1-E(a,j)^s E(a,j)^{-s})^{-1}(1-E(a,j)^s E(a,j)^{-s}) \bmod q=0^{-1}0 \bmod q=0.$
If $X=E(b,k)^{-s}$,
$NOT(E(a,j),X)=(1-E(a,j)^s E(b,k)^{-s})^{-1}(1-E(a,j)^s E(b,k)^{-s}) \bmod q=1 \bmod q=1.$

8.5 Complicated operations of AND and OR of encryption keys
Now we can calculate the logical expression of encryption keys as follows.
$R(X,Y)=AND[OR[E(c,l),E(d,m),X],OR[E(a,j),E(b,k),Y]]$
$=OR[E(c,l),E(d,m),X]\ OR[E(a,j),E(b,k),Y]=\{E(d,m)(1-E(c,l)^s E(d,m)^{-s})^{-1}(1-E(c,l)^s X)+$
$E(c,l)(1-E(d,m)^s E(c,l)^{-s})^{-1}(1-E(d,m)^s X)\}\{E(b,k)(1-E(a,j)^s E(b,k)^{-s})^{-1}(1-E(a,j)^s Y)+$
$E(a,j)(1-E(b,k)^s E(a,j)^{-s})^{-1}(1-E(b,k)^s Y)\} \bmod q.$
If $X=E(c,l)^{-s}$ and $Y=E(a,j)^{-s}$,
$R(X,Y)=E(c,l)E(a,j).$

We can also calculate the logical expressions of decryption keys, $D(a,j)$, $D(b,k)$ etc.

9. Proposed method of enciphering/deciphering

9.1 Key distribution system

1) The centre selects the system parameters SP=[q,n,c,r,s], and publishes them on the cloud computing system, where let q be the prime, n be the number of $Q(i)$, c be the number of the class, r be the number of the rank, s be the positive integer.
2) All users (including the supplier of information) download SP.
3) The supplier of information (SI) selects n-dimensional vector $V(a,i)$ ($a=1,..,c;i=1,..,r$) where SI is the centre or one of users in the cloud computing system.
4) SI classifies the users according to his/her attributes i.e. class and rank.
5) SI distributes the n-dimensional vector $V(a,d), V(a,d-1),.., V(a,1)$ to the users whose attribute is class a and rank d through the secure communication line beforehand, where $V(a,i)=(vai_1, vai_2, \cdots, vai_n) \in Fq^n$, $vai_k \in \{1,2,\cdots,n\}$, $(i=1,..,d; k=1,..,n)$.
6) SI selects $Q(i)(i=1,..,n)$ and publishes the list of $Q(i)$, LQ on the center of cloud computing system.
SI changes the LQ frequently.
7) The users with attribute (a,d) who received the n-dimensional vector $V(a,d), V(a,d-1),.., V(a,1)$ calculates the encryption keys $E(a,d),..,E(a,1)$ by using (5).

9.2 Attribute-based encryption (ABE)

For example, in case of $c=2$ and $r=3$ we show the enciphering/deciphering procedure.

8) SI who wants to send the massage M to the users with the attribute $(a,3)$ or the attribute $(b,2)$, enciphers the message M to cipher-text $C(X)$ as follows.

$K(X)=OR[AND[E(a,3),E(a2),E(a,1)],AND[E(b,2)E(b,1)],X]$

$=OR[E(a,3)E(a,2)E(a,1),E(b,2)E(b,1),X]$,

$C(X)=|K(X)|K(X)M(K(X))^{-1} \bmod q$,

where

let $K(X)=(k_1,k_2,k_3,k_4)$ and $|K(X)|=k_1^2+k_2^2+k_3^2+k_4^2 \bmod q$.

Then $C(X)=(k_1,k_2,k_3,k_4)M(k_1,-k_2,-k_3,-k_4)$

9) SI publishes $C(X)$ on the center of cloud computing system.
The user A with the attribute $(a,3)$ or the user B with attribute $(b,2)$ who want to obtain the message M accesses to the cloud computing system and download $C(X)$, LQ and decipher $C(X)$ to message M as follows.

10-1) The user A with the attribute $(a,3)$ calculates $E(a,1),..,E(a,3)$ from $V(a,1),..,V(a,3)$ and LQ.
10-2) The user B with the attribute $(b,2)$ calculates $E(b,1),E(b,2)$ from $V(b,1),V(b,2)$ and LQ.
11-1) The user A with the attribute $(a,3)$ deciphers $C(X)$ to obtain M as follows.
The following expression is obtained by substituting $(E(a,1)E(a,2)E(a,3))^{-s}$ to X of $C(X)$.

$CM=C((E(a,1)E(a,2)E(a,3))^{-s})$

$=|K((E(a,1)E(a,2)E(a,3))^{-s})|\ K((E(a,1)E(a,2)E(a,3))^{-s})M\{K((E(a,1)E(a,2)E(a,3))^{-s})\}^{-1}$

$=|E(a,1)E(a,2)E(a,3)|\ OR[E(a,3)E(b,2)E(a,1),\ E(b,2),E(b,1),\ (E(a,1)E(a,2)E(a,3))^{-s}]\ M$

$\{OR[E(a,3)E(b,2)E(a,1),\ E(b,2),E(b,1),\ (E(a,1)E(a,2)E(a,3))^{-s}]\}^{-1}$

$=|E(a,1)E(a,2)E(a,3)|\ E(a,3)E(a,2)E(a,1)M\{E(a,3)E(a,2)E(a,1)\}^{-1}$.

Then

$|D(a,1)D(a,2)D(a,3)|^{-1}D(a,1)^{-1}D(a,2)^{-1}D(a,3)^{-1}CMD(a,3)D(a,2)D(a,1)=M$

is obtained because that

$|D(a,1)D(a,2)D(a,3)|=|E(a,1)E(a,2)E(a,3)|$.

11-2) The user B with the attribute $(b,2)$ deciphers $C(X)$ to obtain M as follows.
The following expression is obtained by substituting $(E(b,2)E(b,1))^{-s}$ to X of $C(X)$.

$CM=C((E(b,1)E(b,2))^{-s})=|K((E(b,1)E(b,2))^{-s})|\ K((E(b,1)E(b,2))^{-s})M\{K((E(b,1)E(b,2))^{-s})\}^{-1}$

$=|E(b,1)E(b,2)|\ OR[E(a,3)E(a,2)E(a,1),\ E(b,2)E(b,1),\ (E(b,1)E(b,2))^{-s}]M$

$\{OR[E(a,3)E(a,2)E(a,1),\ E(b,2)E(b,1),\ (E(b,1)E(b,2))^{-s}]\}^{-1}$

$=|E(b,1)E(b,2)|\ E(b,2)E(b,1)M\{E(b,2)E(b,1)\}^{-1}$.

Then

$|D(b,1)D(b,2)|^{-1}D(b,1)^{-1}D(b,2)^{-1}CMD(b,2)D(b,1)=M$

is obtained because that

$|D(b,1)D(b,2)| = |E(b,1)E(b,2)|$.

10.Cryptanalysis of the current system

10.1 Solving M and $E(a,1)$ from $C=|E(a,1)|E(a,1)M\{E(a,1)\}^{-1}$

Cryptanalyst who tries to obtain $M=(m_1,m_2,m_3,m_4)$ and $E(a,1)$ from the value of C does not have the separate information on M or $E(a,1)$.

$C=|E(a,1)|E(a,1)M\{E(a,1)\}^{-1}$

is able to be transformed to

$C=|E(a,1)g|E(a,1)g(g^{-1}Mg)\{E(a,1)g\}^{-1}$ where $g \in H^*$ and $|g|=1$.

Then cryptanalyst cannot determine the value of M or $E(a,1)$ because many pairs of M and $E(a,1)$ exist.

10.2 Gröbner basis attacks for the proposed scheme

It is said that the Gröbner basis attacks is efficient for solving multivariate algebraic equations.

We calculate the complexity G to obtain the Gröbner basis for our multivariate algebraic equations over Fq so that we confirm immunity of our system to the Gröbner basis attack .

1) Method for obtaining $R(X,Y)$ from the expression of $C(X,Y)$

$C(X,Y)=|R(X,Y)|R(X,Y)M(R(X,Y))^{-1}$ is given

where $R(X,Y)=AND[OR[E(c,l),E(d,m),X],OR[E(a,j),E(b,k),Y]]$.

Then, we calculate the complexity required to obtain $R(X,Y)$ in case that $n=32$ and $s=O(2^{20})$.

$R(X,Y)$ has 100 coefficients because the i-th element of $R(X,Y)$, ri has the form such that

$r_i=e_{i0}+e_{i11}x_1+..+e_{i14}x_4+e_{i21}y_1+..+e_{i24}y_4+e_{i311}x_1y_1+..+e_{i344}x_4y_4$, $(i=1,..,4)$,

where $X=(x_1,..,x_4)$, $Y=(y_1,..,y_4)$ and $e_{i0},e_{ij},e_{ijk} \in Fq$.

$(R(X,Y))^{-1}$ is given such that

$(R(X,Y))^{-1}=(h^{-1}r_1, -h^{-1}r_2, -h^{-1}r_3, -h^{-1}r_4)$

where

$h=r_1^2+r_2^2+r_3^2+r_4^2 \bmod q$,

$|R(X,Y)| = r_1^2+r_2^2+r_3^2+r_4^2 \bmod q = h$.

Then $C(X,Y)=(c_1,c_2,c_3,c_4)$ has the form such that

$c_i=c_{i0}+c_{i11}x_1+..+c_{i14}x_4+c_{i21}y_1+..+c_{i24}y_4+c_{i311}x_1y_1+..+c_{i344}x_4y_4+C3(X,Y)+C4(X,Y)$,

$(i=1,..,4)$,

where $C3(X,Y)$ is polynomial of $x_1,..,x_4,y_1,..,y_4$ of 3 degree and $C4(X,Y)$ is polynomial of $x_1,..,x_4,y_1,..,y_4$ of 4 degree.

We try to obtain the coefficients, e_i,e_{ij},e_{ijk} of $R(X,Y)$ from $C(X,Y)$ by using Gröbner basis.

The number of variables is 104.

The number of equations is $900(=(1+8+36+80+100)*4)$.

The degree of equation is 4.

$G=({}_{104}C_5)^w=2^{63}$, $(w=2.39)$ is not enough large.

But $R(X,Y)$ and M is able to substitute for $R(X,Y)g$ and $g^{-1}Mg$ where $|g|=1$. Then cryptanalyst cannot determine the value of M or $R(X,Y)$ because $O(q^3)$ pairs of M and $R(X,Y)$ exist.

It is said that it is not efficient to obtain the coefficients, e_i,e_{ij},e_{ijk} of $R(X,Y)$ from $C(X,Y)$ by using Gröbner basis.

2) Method for obtaining $E(a,j),E(b,k),E(c,l)$ and $E(d,m)$ from the expression of $C(X,Y)$

$C(X,Y)=|R(X,Y)|R(X,Y)M(R(X,Y))^{-1}$ is given where

$R(X,Y)=AND[OR[E(c,l),E(d,m),X],OR[E(a,j),E(b,k),Y]]$.

Then, we calculate the complexity required to obtain $E(a,j),E(b,k),E(c,l)$ and $E(d,m)$ in case that $n=32$ and $s=O(2^{20})$.

Considering that $OR[E(a,j),E(b,k),Y]$ is polynomial of $E(a,j)$ and $E(b,k)$ of more than 3s-degree, we are not able to adopt Gröbner basis attack.

It is shown that this scheme is immune from the Gröbner basis attacks. Then it is said that the polynomial time algorithm to break our scheme does not exist probably.

11. Numerical example of key distribution and attribute-based encryption

We show the simple example of key distribution and attribute-based encryption in this section.

Centre of cloud computing system publishes the system parameters.

SI publishes ciphertext $C(X)$ on the center of cloud computing system which only user A with attribute $(a,1)$ or user B with attribute $(b,1)$ can deciphers.

User A or B download $C(X)$ from on the centre of cloud computing system and deciphers plaintext M by using his attribute $(a,1)$ or $(b,1)$ independently.

The procedure is shown as follows.

1.Centre selects system parameters such that

$q=5,\ n=5,\ c=2,\ r=1,\ s=1.$

Center publishes them on the centre of cloud computing system.

2.SI selects $LQ=\{Q(1),Q(2),Q(3),Q(4),Q(5)\}$ such that

$Q(1)=(4,1,2,4),\ Q(2)=(2,2,1,3),\ Q(3)=(2,3,4,0),\ Q(4)=(4,2,4,0),\ Q(5)=(0,3,2,2).$

SI publishes LQ on the center of cloud computing system.

3.SI selects $V(a,1)=(1,2,3,1,4)$ and $V(b,1)=(4,3,1,2,5)$.

SI sends $V(a,1)$, $V(b,1)$ to user A and user B through security communication line, respectively.

4.SI calculates $E(a,1)$ from LQ and $V(a,1)$ such that

$E(a,1)=Q(1)Q(2)Q(3)Q(1)Q(4)\ mod\ q=(1,2,3,3).$

5.User A downloads LQ from the center of cloud computing system.

User A calculates $E(a,1)$ from LQ and $V(a,1)$ such that

$E(a,1)=Q(1)Q(2)Q(3)Q(1)Q(4)\ mod\ q=(1,2,3,3).$

6.SI calculate $E(b,1)$ from LQ and $V(b,1)$ such that

$E(b,1)=Q(4)Q(3)Q(1)Q(2)Q(5)\ mod\ q=(3,2,1,2).$

7. User B downloads LQ from the center of cloud computing system.

User B calculates $E(b,1)$ from LQ and $V(b,1)$ such that

$E(b,1)=Q(4)Q(3)Q(1)Q(2)Q(5)\ mod\ q=(3,2,1,2).$

8. SI publishes ciphertext $C(X)$ for plaintext M on the centre of cloud computing system as follows.

$K(X)=OR[E(a,1),E(b,1)]$

$=E(b,1)[1-E(a,1)E(b,1)^{-1}]^{-1}(1-E(a,1)X)+E(a,1)[1-E(b,1)E(a,1)^{-1}]^{-1}(1-E(b,1)X).$

$=(3,2,1,2)[1-(1,2,3,3)(3,2,1,2)^{-1}]^{-1}(1-(1,2,3,3)(x1,x2,x3,x4))+$

$(1,2,3,3)[1-(3,2,1,2)(1,2,3,3)^{-1}]^{-1}(1-(3,2,1,2)(x1,x2,x3,x4))$

$=(4+3x_1+0x_2+x_3+3x_4,1+0x_1+3x_2+3x_3+4x_4,1+4x_1+2x_2+3x_3+0x_4,1+2x_1+x_2+0x_3+3x_4)$

$=(k_1,k_2,k_3,k_4),$

Let M the plaintext $(4,3,1,1)$.

$C(X)=|K(X)|K(X)M(K(X))^{-1}$

$=(k_1,k_2,k_3,k_4)M(k_1,-k_2,-k_3,-k_4)$

$=(4+3x_1+0x_2+x_3+3x_4,1+0x_1+3x_2+3x_3+4x_4,1+4x_1+2x_2+3x_3+0x_4,1+2x_1+x_2+0x_3+3x_4)(4,3,1,1)$

$((4+3x_1+0x_2+x_3+3x_4),-(1+0x_1+3x_2+3x_3+4x_4),-(1+4x_1+2x_2+3x_3+0x_4),-(1+2x_1+x_2+0x_3+3x_4))$

$=(1+4x_1+3x_2+0x_3+2x_4+x_1^2+x_2^2+x_3^2+x_4^2+0x_1x_2+0x_1x_3+0x_1x_4+0x_2x_3+0x_2x_4+0x_3x_4,$

$4+4x_1+1x_2+1x_3+1x_4+4x_1^2+0x_2^2+2x_3^2+4x_4^2+2x_1x_2+4x_1x_3+0x_1x_4+1x_2x_3+2x_2x_4+4x_3x_4,$

$4+4x_1+2x_2+0x_3+2x_4+3x_1^2+4x_2^2+4x_3^2+4x_4^2+0x_1x_2+3x_1x_3+2x_1x_4+0x_2x_3+0x_2x_4+4x_3x_4,$

$2+1x_1+3x_2+3x_3+0x_4+1x_1^2+0x_2^2+x_3^2+3x_4^2+2x_1x_2+0x_1x_3+4x_1x_4+3x_2x_3+4x_2x_4+1x_3x_4).$

9. User A downloads $C(X)$ from the centre of cloud computing system.

User A calculates $E(a,1)^{-1}$ and $C(E(a,1)^{-1})$ such that

$E(a,1)^{-1}=(1,2,3,3)^{-1}=(1+4+4+4)^{-1}(1,-2,-3,-3)=(2,1,4,4).$

$C(E(a,1)^{-1})=C((2,1,4,4))=(2,0,0,2).$

User A deciphers M such that

$|E(a,1)|^{-1}E(a,1)^{-1}C(E(a,1)^{-1})E(a,1)=|(1,2,3,3)|^{-1}(2,1,4,4)(2,0,0,2)(1,2,3,3)=(4,3,1,1)=M.$

User A obtains plaintext M.

10. User B downloads $C(X)$ from the center of cloud computing system.
User B calculates $E(b,1)^{-1}$ and $C(E(b,1)^{-1})$ such that
$E(b,1)^{-1}=(3,2,1,2)^{-1}=(4+4+1+4)^{-1}(3,-2,-1,-2)=(1,1,3,1)$.
$C(E(b,1)^{-1})=C((1,1,3,1))=(2,0,2,0)$.
User B deciphers M such that
$|E(b,1)|^{-1}E(b,1)^{-1}C(E(b,1)^{-1})E(b,1)=|(3,2,1,2)|^{-1}(1,1,3,1)\ (2,0,2,0)\ (3,2,1,2)=(4,3,1,1)=M$.
User B obtains plaintext M.

12. The size of the keys and the complexity for enciphering/deciphering

We consider the size of the system parameter q. We select the size of q such that the size of the order of H, $O(q^4)$ is larger than $O(2^{80})$. And we select the size of n such that (n^n) is larger than $O(2^{80})$. Then we need to select modulus $q \geqq O(2^{20})$ and $n \geqq 19$.

In case of $n=32, c=128, r=8, O(s)=O(2^{20})$ and $O(q)=O(2^{20})$, the size of $LQ, SV=\{V(1,1),..,V(c,r)\}$, $SE=\{E(1,1),\ldots,E(c,r)\}$, $SD=\{D(1,1),..,D(c,r)\}$, SP are about 2.56kbits, 164kbits, 82kbits, 82kbits, 55bits respectively.

The complexity to obtain SE and SD is $O(2^{28})$ bit-operations each. The complexity to obtain the cipher-text $C=|K|KMK^{-1}$ where $K=AND[E(a,1),..,E(a,32)]$ is $O(2^{18})$ bit-operations.

The complexity to obtain the plaintext $M=|K|^{-1}K^{-1}CK$ where $K=AND[D(a,1),..,D(a,32)]$ is $O(2^{18})$ bit-operations.

The complexity to obtain the cipher-text $C(X)=|K(X)|K(X)MK(X)^{-1}$ where $K(X)=OR[E(a,1),..,E(a,16),E(a,17),..,E(a,32),X]$ is $O(2^{21})$ bit-operations.

On the other hand the complexity of the enciphering and deciphering in RSA scheme is $O(2(\log n)^3)=O(2^{34})$ where the size of modulus n is 2048bits.

Then our invention requires small memory space and complexity to encipher and decipher so that we are able to implement our scheme to the mobile devices.

13.Conclusion

We proposed the key distribution system and attribute based encryption. It was shown that our system is immune from the Gröbner basis attacks by calculating the complexity to obtain the Gröbner basis for solving the multivariate algebraic equations.

References

[1]W. Diffie and M. Hellman, "New Directions in Cryptography",
IEEE Transactions on Information Theory, IT-22, 6 , pp.644-654 (Nov.1976)

[2] R. L. Rivest , A. Shamir , and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems, ", Comm., ACM, Vol.21, No.2, pp.120-126, 1978.2.

[3] T. E. ElGamal, "A public key Cryptosystem and a Signature Scheme Based on Discrete Logarithm ", Proceeding Crypto 84 (Aug.1984).

[4]N, Koblitz , Translated by Sakurai Kouiti , "A Course in Number Theory and Cryptography ", Springer-Verlag Tokyo, Inc., Tokyo, 1997.

[5] Tatsuaki Okamoto and Katsuyuki Takashima, “Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption,” Cryptology ePrint Archive, Report 2010/563, 2010.

[6] M. Bardet , J. C. Faugere, and B. Salvy, "On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations," Proceeding of the International Conference on Polynomial System Solving(ICPSS2004),pp.71-75,November 2004.

[7] Shigeo Tsujii , Kohtaro Tadaki , Masahito Gotaishi ,Ryo Fujita ,and Masao Kasahara ,"Proposal Integrated MPKC:PPS—STS Enhanced Perturbed Piece in Hand Method---," IEICE Tech. Rep.ISEC2009-27,SITE2009-19,ICSS2009-41(2009-07),July 2009.

[8] T. Matsumoto, H. Imai, H. Harashima, and H. Miyakawa, “A class of asymmetric cryptosystems using obscure representations of enciphering functions, ” in 1983 National Convention Record on Information Systems, IECE Japan, 1983.

[9] T. Matsumoto, and H. Imai, “Public quadratic polynomial-tuples for efficient signature verification and message-encryption,” Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT’88, pp.419–453, New York, NY, USA, 1988, Springer-Verlag New York, Inc.

[10] S. Tsujii, K. Tadaki, and R. Fujita, “Piece in hand concept for enhancing the security of multivariate type public key cryptosystems: Public key without containing all the information

of secret key," Cryptology ePrint Archive, Report 2004/366, 2004.
[11] C.Wolf, and B. Preneel, "Taxonomy of public key schemes based on the problem of multivariate quadratic equations," Cryptology ePrint Archive, Report 2005/077, 2005, http://eprint.iacr.org/.
[12] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Press, Los Alamitos(2007)
[13] Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption scheme. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455–470. Springer, Heidelberg(2008)
[14] Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer, Heidelberg (2007)
[15] Boneh, D., Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
[16] Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004)
[17] Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext.In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005).

<Appendix>
Theorem 1
Let $OR[E(a,j),E(b,k),X]$ be
$E(b,k)(1-E(a,j)^{s}E(b,k)^{-s})^{-1}(1-E(a,j)^{s}X) + E(a,j)(1-E(b,k)^{s}E(a,j)^{-s})^{-1}(1-E(b,k)^{s}X) \bmod q$.

If and only if (Iff) $X=E(a,j)^{-s}$,
$OR[E(a,j),E(b,k),E(a,j)^{-s}]=E(a,j) \bmod q$
where $E(a,j)\neq E(b,k)$, $X\in H^{*}$, $0=(0,0,0,0)\in H$.

Proof:
If $X=E(a,j)^{-s}$,
$OR[E(a,j),E(b,k),E(a,j)^{-s}]= 0+ E(a,j)(1-E(b,k)^{s}E(a,j)^{-s})^{-1}(1-E(b,k)^{s}E(a,j)^{-s}) =E(a,j) \bmod q$
where $0=(0,0,0,0)\in H$.

If
$E(b,k)(1-E(a,j)^{s}E(b,k)^{-s})^{-1}(1-E(a,j)^{s}X) + E(a,j)(1-E(b,k)^{s}E(a,j)^{-s})^{-1}(1-E(b,k)^{s}X)=E(a,j)$ ・・・①,
$E(b,k)(1-E(a,j)^{s}E(b,k)^{-s})^{-1}(1-E(a,j)^{s}X') + E(a,j)(1-E(b,k)^{s}E(a,j)^{-s})^{-1}(1-E(b,k)^{s}X') =E(a,j)$ ・・・②,
Calculating ①－② ,
$E(b,k)(1-E(a,j)^{s}E(b,k)^{-s})^{-1}(-E(a,j)^{s}(X-X')) + E(a,j)(1-E(b,k)^{s}E(a,j)^{-s})^{-1}(-E(b,k)^{s}(X-X'))=0$
$E(b,k)(E(a,j)^{-s}-E(b,k)^{-s})^{-1}(-(X-X')) + E(a,j)(E(b,k)^{-s} -E(a,j)^{-s})^{-1}(-(X-X'))=0$
$(E(b,k)- E(a,j))(E(a,j)^{-s}-E(b,k)^{-s})^{-1}(-(X-X')) =0$
$(E(b,k)- E(a,j))(E(a,j)^{-s}-E(b,k)^{-s})^{-1}(X-X') =0$
From $E(a,j)\neq E(b,k)$, then $E(a,j)^{-s}\neq E(b,k)^{-s}$.
We obtain
$X=X'$. q.e.d.