Key Agreement Protocols Using Multivariate Equations on Non-commutative Ring

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

SUMMARY: In this paper we propose two KAP(key agreement protocols) using multivariate equations. As the enciphering functions we select the multivariate functions of high degree on non-commutative ring ***H*** over finite field ***Fq***. Two enciphering functions are slightly different from the enciphering function previously proposed by the present author. In proposed systems we can adopt not only the quaternion ring but also the non-associative octonion ring as the basic ring. Common keys are generated by using the enciphering functions. Proposed systems are immune from the Gröbner bases attacks because obtaining parameters of the enciphering functions to be secret keys arrives at solving the multivariate algebraic equations, that is, one of NP complete problems .Our protocols are also thought to be immune from the differential attacks because of the equations of high degree.

We can construct our system on the some non-commutative rings, for example quaternion ring, matrix ring or octonion ring.
.

key words: key agreement protocol, multivariate equations, Gröbner bases, NP complete problems, non-commutative ring

1. Introduction

In this paper we propose two KAP(key agreement protocols) using multivariate equations which have slightly different enciphering functions from the enciphering function of previously proposed KAP by the present auther[10].

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

Typical examples of KAP are almost based on the discrete logarithm problem over finite fields. Typical examples of PKC are classified as follows.

1) RSA cryptosystem[2] based on factoring problem ,
2) ElGamal cryptosystem[3] based on the discrete logarithm problem over finite fields ,
3) the elliptic curve cryptosystem[4] based on the discrete logarithm problem on the elliptic curve[5],[6],
4) multivariate public key cryptosystem (MPKC)[7],
and so on.

It is said that the problem of factoring large integers, the problem of solving discrete logarithms and the problem of computing elliptic curve discrete logarithms are efficiently solved in a polynomial time by the quantum computers.

It is thought that MPKC is immune from the attack of quantum computers. But MPKC proposed until now almost adopts multivariate quadratic equations because of avoiding the explosion of key length.

In the current paper, we propose two KAP using multivariate equations on non-commutative ring ***H*** over finite fields ***Fq*** without the explosion of key length. We choose the quaternion[8] ring as the non-commutative ring. The security of these systems is based on the computational difficulty to solve the multivariate algebraic equations of high degree.

To break these cryptosystems it is thought that we probably need to solve the multivariate algebraic equations of high degree that is equal to solving the NP complete problem. Then it is thought that our systems are immune from the attacks by quantum computers.

In the next section, we define multiplication on quaternion ring over ***Fq***.

In section3 we begin with generating the first multivariate function of high degree on the quaternion ring as the enciphering function. We construct the KAP by the first enciphering function.

In section4 we generate the second multivariate function of high degree on the quaternion ring. This multivariate function is slightly different from one in section 3. We construct second KAP using the second enciphering function by the same way in section3.

In these systems we can adopt not only the quaternion ring but also the non-associative octonion ring as the basic ring. In the last section, we provide concluding remarks.

2. The multiplication on quaternion ring

Let q be an odd prime. Let ***H*** be the quaternion ring over the finite field ***Fq*** as follows;

$$\boldsymbol{H}=\{(a_0,a_1,a_2,a_3)|\ a_i \in \boldsymbol{Fq}\ (i=0,1,2,3)\}. \quad (1)$$

In case of selecting the quaternion ring or octonion ring as the non-commutative ring, the modulus q needs to be more than 2 to keep non-commutative.

Here we define the product AB of $A=(a_0,a_1,a_2,a_3)$ and $B=(b_0,b_1,b_2,b_3)$ on quaternion ring ***H*** over ***Fq*** such that

$$AB = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 \bmod q,\ a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 \bmod q,\ a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 \bmod q,\ a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 \bmod q), \quad (2)$$

where $A,B \in \boldsymbol{H}$.

3. Proposition of the first KAP

3.1 The first enciphering function $F(X_1,..,X_d)$

Let m and d be positive integers .

Let S_1 be system parameters such that

$S_1=[q,d,m]$. (3)

As secret keys SK_1 ,we choose arbitrary parameters $A_{ij} \in \boldsymbol{H}$ $(i=1,..,m;j=1,..,d)$,that is,

$SK_1=[A_{ij}](i=1,..,m;j=1,..,d)$. (4)

We define the multivariate function $F(X_1,..,X_d)$ of high degree as the enciphering function such that

$$F(X_1,..,X_d) = \sum_{i=1}^{m} [\prod_{j=1}^{d} X_j A_{ij}]. \quad (5)$$

We determine the values of m and d later so that the number of variables(i.e secret keys) is nearly equal to the number of equations .

Although we adopt the quaternion ring as the basic ring $\boldsymbol{H}$, we can discuss in the same way on the matrix ring or the octonion[8] ring.

3.2 The element expression of $F(X_1,..,X_d)$

Let (f_0,f_1,f_2,f_3) be the element expression of $F(X_1,..,X_d)$. From (5), f_j $(j=0,..,3)$ is given as follows;

$$F(X_1,..,X_d)=(f_0,f_1,f_2,f_3), \quad (6)$$

$$f_j = \sum_{e_{10},..,e_{d3}} f_{je_{10}..e_{d3}} x_{10}^{e10}..x_{13}^{e13}..x_{d0}^{ed0}..x_{d3}^{ed3} \bmod q \quad (7)$$

with the coefficients $f_{je^{10}..e^{d3}} \in \boldsymbol{Fq}$ to be published , where

$$X_i = (x_{i0}, x_{i1}, x_{i2}, x_{i3}) \in \boldsymbol{H},$$
$$x_{ij} \in Fq, (i = 1,.., d; j = 0,.., 3).$$

$e_{ij} \in \{0,1\}(i=1,..,d;j=0,..,3)$ which satisfy $e_{i0}+..+e_{i3}=1$ $(i=1,..,d)$.

Then the number n of $f_{je^{10}..e^{d3}}$ is

$$n=4(4^d)=4^{d+1}. \quad (8)$$

Let $\{ f_{je^{10}..e^{d3}} \}$ be the set that includes all $f_{je^{10}..e^{d3}}$.

3.3 Construction of the first KAP

Let's describe the procedure that user U and user V obtain the common keys by using $F(X_1,..,X_d)$ and $T(X_1,..,X_d)$ as follows.

1) The set of system parameters $S_1=[q,d,m]$ is published by the system center which is trusted third party(TTP).

2) User U chooses randomly parameters $A_{ij} \in \boldsymbol{H}$ $(i=1,..,m;j=1,..,d)$.
The secret key of user U is

$SK_1=[A_{ij}]$ $(i=1,..,m;j=1,..,d)$.

3) User U generates $F(X_1,..,X_d)$ such that

$$F(X_1,..,X_d) = \sum_{i=1}^{m} [\prod_{j=1}^{d} X_j A_{ij}]. \quad (9)$$

4) User U calculates the set of coefficients $\{f_{je^{10}..e^{d3}}\}$ from (9) which consists of n parameters in $\boldsymbol{Fq}$.

5) Let PK_1 be the public key of user U such that

$$PK_1=\{ f_{je^{10}..e^{d3}} \}. \quad (10)$$

Beforehand user U publishes PK_1 which consists of n parameters in $\boldsymbol{Fq}$.

6) User V chooses randomly parameters $B_{ij} \in \boldsymbol{H}$ $(i=1,..,m;j=1,..,d)$.

7) User V generates $T(X_1,..,X_d)$ such that

$$T(X_1,..,X_d) = \sum_{i=1}^{m} [\prod_{j=1}^{d} X_j B_{ij}]. \quad (11)$$

8) Let (t_0,t_1,t_2,t_3) be the element expression of $T(X_1,..,X_d)$. From (11) user V calculates the set of coefficients $\{t_{je^{10}..e^{d3}}\}$ which consists of n parameters in $\boldsymbol{Fq}$.

t_j $(j=0,..,3)$ is given such that

$$T(X_1,..,X_d)=(t_0,t_1,t_2,t_3), \quad (12)$$

where

$$t_j = \sum_{e_{10}\cdots e_{d3}} t_{je_{10}..e_{d3}} x_{10}^{e10}..x_{13}^{e13}..x_{d0}^{ed0}..x_{d3}^{ed3} \bmod q \quad (13)$$

with the coefficients $t_{je^{10}..e^{d3}} \in \boldsymbol{Fq}$, where $e_{ij} \in \{0,1\}$ which satisfy

$e_{i0}+..+e_{i3}=1.$ $(i=1,..,d)$.

Then the number n' of $t_{je^{10}..e^{d3}}$ is $n'=4(4^d)=4^{d+1}$.

Let $\{ t_{je^{10}..e^{d3}} \}$ be the set that includes all $t_{je^{10}..e^{d3}}$.

9) User V sends $\{ t_{je^{10}..e^{d3}} \}$ to user U .

10) User V calculates common keys $Kv0$ and $Kv1$ as follows.

Let $Kv0$ be

$$Kv0=(Kv0_0,Kv0_1,Kv0_2,Kv0_3)$$
$$= \sum_{i=1}^{m} F(B_{i1},..,B_{id})$$
$$= \sum_{i=1}^{m} [\sum_{r=1}^{m} \prod_{j=1}^{d} B_{ij} A_{rj}]. \quad (14)$$

Then $Kv0_j(j=0,1,2,3)$ are obtained from (7) such that

$$Kv0_j = \sum_{i=1}^{m} \sum_{e_{10}..e_{d3}} f_{je_{10}..e_{d3}} v_{i10}^{e10}..v_{i13}^{e13}..v_{id0}^{ed0}..v_{id3}^{ed3} \bmod q \quad (15)$$

where

$(v_{ij0},v_{ij1},v_{ij2},v_{ij3})=B_{ij},(i=1,..,m;j=1,..,d)$,

$e_{ij} \in \{0,1\}(i=1,..,d;j=0,..,3)$ which satisfy

$e_{i0}+\ldots+e_{i3}=1\ (i=1,..,d)$.

Next let $Kv1$ be

$$Kv1=(Kv1_0,Kv1_1,Kv1_2,Kv1_3)$$

$$= \sum_{i=1}^{m} F(1, B_{i1},..., B_{id-1}) B_{id} \quad (16)$$

$$= \sum_{i=1}^{m} \sum_{r=1}^{m} [1 \cdot \prod_{j=1}^{d-1} A_{rj} B_{ij}] A_{rd} B_{id}$$

$$= \sum_{i=1}^{m} \sum_{r=1}^{m} \prod_{j=1}^{d} A_{rj} B_{ij} \quad (17)$$

Then $Kv1_j(j=0,1,2,3)$ are obtained from (7) and (16) such that

$$Kv1_j = \sum_{i=1}^{m} \sum_{e_{10}..e_{d3}} f'_{je_{10}..e_{d3}} v_{i10}^{e10}..v_{i13}^{e13}..v_{id0}^{ed0}..v_{id3}^{ed3} \bmod q \quad (18)$$

with the coefficients $f'_{je^{10}..e^{d3}} \in Fq$,
where

$(v_{ij0},v_{ij1},v_{ij2},v_{ij3})=B_{ij},(i=1,..,m;j=1,..,d)$.

$e_{ij} \in \{0,1\}(i=1,..,d;j=0,..,3)$ which satisfy

$e_{i0}+\ldots+e_{i3}=1\ (i=1,..,d)$.

11) User U calculates common keys $Ku0$ and $Ku1$ as follows.

Let $Ku0$ be

$$Ku0=(Ku0_0,Ku0_1,Ku0_2,Ku0_3)$$

$$= \sum_{i=1}^{m} T(1, A_{i1},..., A_{id-1}) A_{id} \quad (19)$$

$$= \sum_{i=1}^{m} \sum_{r=1}^{m} [1 \cdot \prod_{j=1}^{d-1} B_{rj} A_{ij}] B_{rd} A_{id}$$

$$= \sum_{i=1}^{m} \sum_{r=1}^{m} \prod_{j=1}^{d} B_{rj} A_{ij} . \quad (20)$$

$Ku0_j(j=0,1,2,3)$ are obtained from (13) and (19) such that

$$Ku0_j = \sum_{i=1}^{m} \sum_{e_{10}..e_{d3}} t'_{je_{10}..e_{d3}} u_{i10}^{e10}..u_{i13}^{e13}..u_{id0}^{ed0}..u_{id3}^{ed3} \bmod q \quad (21)$$

with the coefficients $t'_{je^{10}..e^{d3}} \in Fq$,
where
$(u_{ij0},u_{ij1},u_{ij2},u_{ij3})=A_{ij},(i=1,..,m;j=1,..,d)$,

$e_{ij} \in \{0,1\}(i=1,..,d;j=0,..,3)$ which satisfy

$e_{i0}+\ldots+e_{i3}=1\ (i=1,..,d)$.

Next let $Ku1$ be

$$Ku1=(Ku1_0,Ku1_1,Ku1_2,Ku1_3)$$

$$= \sum_{i=1}^{m} T(A_{i1},..., A_{id})$$

$$= \sum_{i=1}^{m} [\sum_{r=1}^{m} \prod_{j=1}^{d} A_{ij} B_{rj}]. \quad (22)$$

$Ku1_j(j=0,1,2,3)$ are obtained from (13) such that

$$Ku1_j = \sum_{i=1}^{m} \sum_{e_{10}..e_{d3}} t_{je_{10}..e_{d3}} u_{i10}^{e10}..u_{i13}^{e13}..u_{id0}^{ed0}..u_{id3}^{ed3} \bmod q \quad (23)$$

where

$(u_{ij0},u_{ij1},u_{ij2},u_{ij3})=A_{ij},(i=1,..,m;j=1,..,d)$,

$e_{ij} \in \{0,1\}(i=1,..,d;j=0,..,3)$ which satisfy

$e_{i0}+\ldots+e_{i3}=1\ (i=1,..,d)$.

From (14) ,(20)and (17),(22) we can confirm that

$$Ku0=Kv0, \quad (24)$$

and

$$Ku1=kv1. \quad (25)$$

The common key of user U and user V is $[Ku0,Ku1]$ or $[Kv0,Kv1]$.

3.4 Verification of the strength of the first KAP

Let's examine the strength of the first KAP. The strength of the first KAP depends on the strength of the multivariate functions described in section 3.1 In other words, we mention the difficulty to obtain A_{ij} $(i=1,..,m; j=1,..,d)$ from the set of coefficients $\{f_{je^{10}..e^{d3}}\}$ of $F(X_1,..,X_d)$ to be the public keys .

3.4.1 Multivariate algebraic equations from $F(X_1,..,X_d)$

Let A_{ij} be

$$A_{ij}=(A_{ij0},A_{ij1},A_{ij2},A_{ij3}) \in \boldsymbol{H},(i=1,..,m:j=1,..,d). \quad (26)$$

From (5) all $f_{je^{10}..e^{d3}}$ have the form such that

$$f_{je_{10}..e_{d3}} = \sum_{i=1}^{m} h_{ji,b_{10}..b_{d3}} A_{i10}^{\ b_{10}}..A_{i13}^{\ b_{13}}..A_{id0}^{\ b_{d0}}..A_{id3}^{\ b_{d3}} \bmod q \quad (27)$$

$(j = 0,..,3)$

with the coefficients $h_{ji,b10..bd3} \in \boldsymbol{Fq}$
where $b_{ij} \in \{0,1\}(i=1,..,d;j=0,..,3)$ which satisfy

$b_{i0}+\ldots+b_{i3}=1\ (i=1,..,d).$

From (27) we obtain $n(=4^{d+1})$ multivariate algebraic equations over $\boldsymbol{Fq}$ where A_{ijr} $(i=1,..,m;j=1,..,d;r=0,..3)$ are the variables i.e. unknown numbers.

3.4.2 Cryptanalysis using Gröbner bases

It is said that the Gröbner bases attacks is efficient for solving multivariate algebraic equations .We calculate the complexity G[9] to obtain the Gröbner bases for our multivariate algebraic equations on quaternion ring so that we confirm immunity of our KAP to the Gröbner bases attack .

We describe in case of $d=4$ and $q=O(10^{10})$ as samples of lower degree equations.
*s:*degree of equations $=d=4$.
n :the number of equations $=4(4^d)=1024$.
We select *m* so that the number of variables(i.e secret keys) is nearly equal to *n* , that is ,as $d=4$,
$m=\lfloor(4*4^d)/(4d)\rfloor=64$,
where $\lfloor*\rfloor$ means the largest integer less than or the integer equal to *.
z :the number of variables $=4dm=1024$
$d_{reg}=s+1=5$
$G=O((_nG_{dreg})^w)=O(2^{102})$ is more than 2^{80} which is the standard for safety where $w=2.39$.

So our KAP is immune from the Gröbner bases attacks and is immune from the differential attacks because of the equations of high degree in (27).

It is thought that the polynomial-time algorithm to break our first KAP does not exist probably.

3.5 The size of the keys of the first KAP

We consider the size of the system parameter *q* . We choose $q=O(2^{10})$ so that the size of the space of *Ku1* and *Ku2* is more than $O(2^{80})$.
In the case of $d=4$, the size of PK_1 and SK_1 is *11kbits* , *11kbits* each.

4. Proposition of the second KAP

4.1 The second enciphering function

Let *m* and *d* be positive integers .
Let S_2 be system parameters such that

$$S_2=[q,d,m] \quad . \quad (28)$$

As secret keys SK_2 ,we choose arbitrary parameters $A_i=(a_{i0},a_{i1},a_{i2},a_{i3}) \in \boldsymbol{H}\ (i=1,..,m)$,

$$SK_2=[A_i](i=1,..,m) \quad . \quad (29)$$

We define the multivariate function $F(X)$ of high degree such that

$$F(X)=\sum_{i=1}^{m}(a_{i0}x_0,a_{i1}x_1,a_{i2}x_2,a_{i3}x_3)^d \quad (30)$$

where

$X = (x_0, x_1, x_2, x_3) \in \boldsymbol{H}$,
$x_j \in Fq, (j = 0,.., 3)$.

We determine the value of *m* later so that the number of variables(i.e secret keys) is nearly equal to the number of equations .

Although we adopt the quaternion ring as the basic ring $\boldsymbol{H}$, we can discuss in the same way on the matrix ring or the octonion ring.

4.2 The element expression of $F(X)$

Let (f_0,f_1,f_2,f_3) be the element expression of $F(X)$. From (30), $f_j(j=0,..,3)$ is given as follows;

$$F(X)=(f_0,f_1,f_2,f_3), \quad (31)$$

$$f_j = \sum_{e_0+..+e_3=d} f_{je_0e_1e_2e_3} x_0^{e_0} x_1^{e_1} x_2^{e_2} x_3^{e_3} \bmod q \quad (32)$$

with the coefficients $f_{je0e1e2e3} \in \boldsymbol{Fq}$ to be published , where
$e_i(i=0,..,3)$ are non-negative integers which satisfy $e_0+..+e_3=d$.
Then the number *n* of $f_{je0e1e2e3}$ is

$$n=4(_4H_d)=4(_{3+d}C_3) \quad (33)$$

Let $\{ f_{je0e1e2e3} \}$ be the set that includes all $f_{je0e1e2e3}$.

4.3 Construction of the second KAP

Let's describe the procedure that user U and user V obtain the common keys using $F(X)$ as follows.

1) The set of system parameters $S_2=[q,d,m]$ is published by the system center which is trusted third party(TTP).

4) User U chooses randomly parameters $A_i=(a_{i0},a_{i1},a_{i2},a_{i3}) \in \boldsymbol{H}\ (i=1,..,m)$.
The secret key of user U is

$SK_2=[A_i]$ $(i=1,..,m)$.

5) User U generates $F(X)$ such that

$$F(X)=\sum_{i=1}^{m}(a_{i0}x_0,a_{i1}x_1,a_{i2}x_2,a_{i3}x_3)^d . \quad (34)$$

6) From (34) user U calculates the set of coefficients $\{f_{je0e1e2e3}\}$ which consists of n parameters in $\boldsymbol{Fq}$.

7) Let PK_2 be the public key of user U such that

$$PK_2=\{f_{je0e1e2e3}\}. \quad (35)$$

Beforehand user U publishes PK_2 which consists of n parameters in $\boldsymbol{Fq}$.

8) User V chooses randomly parameters $B_i=(b_{i0},b_{i1},b_{i2},b_{i3}) \in \boldsymbol{H}$ $(i=1,..,m)$.

7) User V generates $T(X)$ such that

$$T(X)=\sum_{i=1}^{m}(b_{i0}x_0,b_{i1}x_1,b_{i2}x_2,b_{i3}x_3)^d . \quad (36)$$

8) Let (t_0,t_1,t_2,t_3) be the element expression of $T(X)$. From (36) user V calculates the set of coefficients $\{t_{je0e1e2e3}\}$ which consists of n parameters in $\boldsymbol{Fq}$.

t_j $(j=0,..,3)$ is given such that

$$T(X)=(t_0,t_1,t_2,t_3), \quad (37)$$

where

$$t_j=\sum_{e0+..+e3=d} t_{je0e1e2e3}x_0^{e0}x_1^{e1}x_2^{e2}x_3^{e3} \bmod q \quad (38)$$

$e_i(i=0,..,3)$ are non-negative integers which satisfy $e_0+..+e_3=d$.

Then the number n' of $t_{je0e1e2e3}$ is $n'=4({}_4H_d)=4({}_{3+d}C_3)$.

Let $\{t_{je0e1e2e3}\}$ be the set that includes all $t_{je0e1e2e3}$.

11) User V sends $\{t_{je0e1e2e3}\}$ to user U .

12) User V calculates common keys Kv as follows.

Let Kv be

$$Kv=(Kv_0,Kv_1,Kv_2,Kv_3)$$

$$=\sum_{r=1}^{m}F(b_{r0},b_{r1},b_{r2},b_{r3})$$

$$=\sum_{r=1}^{m}[\sum_{i=1}^{m}(a_{i0}b_{r0},a_{i1}b_{r1},a_{i2}b_{r2},a_{i3}b_{r3})^d]. \quad (39)$$

Then $Kv_j(j=0,1,2,3)$ are obtained such that

$$Kv_j=\sum_{r=1}^{m}\sum_{e0+..+e3=d} f_{je0e1e2e3}b_{r0}^{e0}b_{r1}^{e1}b_{r2}^{e2}b_{r3}^{e3} \bmod q \quad (40)$$

where

$e_i(i=0,..,3)$ are non-negative integers which satisfy $e_0+..+e_3=d$.

11) User U calculates common keys Ku as follows.

Let Ku be

$$Ku=(Ku_0,Ku_1,Ku_2,Ku_3)$$

$$=\sum_{r=1}^{m}T(a_{r0},a_{r1},a_{r2},a_{r3})$$

$$=\sum_{r=1}^{m}[\sum_{i=1}^{m}(b_{i0}a_{r0},b_{i1}a_{r1},b_{i2}a_{r2},b_{i3}a_{r3})^d]. \quad (41)$$

$Ku_j(j=0,1,2,3)$ are obtained such that

$$Ku_j=\sum_{r=1}^{m}\sum_{e0+..+e3=d} t_{je0e1e2e3}a_{r0}^{e0}a_{r1}^{e1}a_{r2}^{e2}a_{r3}^{e3} \bmod q \quad (42)$$

where

$e_i(i=0,..,3)$ are non-negative integers which satisfy $e_0+..+e_3=d$.

From (39) and (41) we can confirm that

$$Ku=Kv. \quad (43)$$

The common key of user U and user V is $[Ku]$ or $[Kv]$.

4.4 Verification of the strength of the second KAP

Let's examine the strength of the second KAP. The strength of the second KAP depends on the strength of the multivariate functions described in section 4.1. In other words, we mention the difficulty to obtain A_i $(i=1,..,m)$ from the set of coefficients $\{f_{je0e1e2e3}\}$ of $F(X)$ to be the public keys .

4.4.1 Multivariate algebraic equations from $F(X)$

Let A_i be

$$A_i=(a_{i0},a_{i1},a_{i2},a_{i3}) \in \boldsymbol{H},(i=1,..,m).$$

From (30) all $f_{je0e1e2e3}$ have the form such that

$$f_{je0e1e2e3}=\sum_{i=1}^{m}h_{ji,c0c1c2c3}a_{i0}^{c0}a_{i1}^{c1}a_{i2}^{c2}a_{i3}^{c3} \quad (44)$$

$$(j=0,..,3)$$

with the coefficients $h_{ji,c0c1c2c3} \in \boldsymbol{Fq}$

where $c_i(i=0,..,3)$ are non-negative integers which satisfy

$$c_0+\ldots+c_3=d.$$

From (44) we obtain n multivariate algebraic equations over $\boldsymbol{Fq}$ where a_{ir} $(i=1,..,m;r=0,..3)$ are the variables i.e. unknown numbers.

4.4.2 Cryptanalysis using Gröbner bases

It is said that the Gröbner bases attacks is efficient for solving multivariate algebraic equations .We calculate the complexity G[9] to obtain the Gröbner bases for our multivariate algebraic equations on quaternion ring so that we confirm immunity of our second KAP to the Gröbner bases attack .

We describe in case of $d=6$ and $q=O(10^{20})$ as samples of lower degree equations.

*s:*degree of equations $=d=6$.

n :the number of equations $=4({}_4H_d) =4({}_{3+d}C_3)=336$.

We select *m* so that the number of variables(i.e secret keys) is nearly equal to *n* , that is,

$m=\lceil n/4 \rceil=84$,

where $\lceil * \rceil$ means the largest integer less than or the integer equal to *.

z :the number of variables $=4m=336$

$d_{reg}=s+1=7$

$G=O(({}_nG_{dreg})^w)=O(2^{110})$ is more than 2^{80} which is the standard for safety where $w=2.39$.

So the second KAP is immune from the Gröbner bases attacks and is immune from the differential attacks because of the equations of high degree in (44).

It is thought that the polynomial-time algorithm to break the second KAP does not exist probably.

4.5 The size of the keys of the second KAP

We consider the size of the system parameter *q* . We choose $q=O(2^{20})$ so that the size of the space of *Ku* or *Kv* is more than $O(2^{80})$.

In the case of $d=6$, the size of PK_2 and SK_2 is *7kbits* , *7kbits* each.

5. Conclusion

We proposed two KAP using multivariate functions on non-commutative quaternion ring over $\boldsymbol{F_q}$**.** It is a computationally difficult problem to obtain the secret keys from the public keys because the problem is one of NP complete problems. In order to ensure the safety, the size of *q* is to be more than *10* bits in the first KAP and to be more than *20* bits in the second KAP.

We can construct two KAP on the other non-commutative ring ,for example matrix ring or octonion ring.

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]Fujita , "EC in cryptography", NEC Technical Journal, Vol.50, No.11, pp.72-78, 1997.11.

[6] IEEE P1363/D9 (Draft Version 9) Standard Specifications for Public Key Cryptography.1998.

[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] John H. Conway, Derek A. Smith co-authored, translated by Syuuji Yamada, " On Quaternions and Octonions " Baifuukan Publication Center, Tokyo, .2006, pp.79-95.

[9] 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.

[10] Masahiro Yagisawa, " Key Agreement Protocols Based on Multivariate Algebraic Equations on Quaternion Ring ",Cryptology ePrint Archive,Report 2010/377,(2010-07).