Key Agreement Protocols Based on Multivariate Algebraic Equations on Quaternion Ring

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

SUMMARY: In this paper we propose new key agreement protocols based on multivariate algebraic equations. We choose the multivariate function *F(X)* of high degree on non-commutative quaternion ring ***H*** over finite field ***Fq***. Common keys are generated by using the public-key *F(X).* Our system is immune from the Gröbner bases attacks because obtaining parameters of *F(X)* 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 and the rank attacks.

key words: key agreement protocol, multivariable algebraic equation, Gröbner bases, NP complete problems, quaternion,

1. Introduction

Since Diffie and Hellman proposed the concept of key agreement protocols (KAP) and the public key cryptosystem (PKC) in 1976[1], various KAP and the 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 KAP using multivariate functions of high degree on non-commutative quaternion[8] ring ***H*** over finite fields ***Fq*** without the explosion of key length. The security of this system is based on the computational difficulty to solve the multivariate algebraic equations of high degree.

To break this cryptosystem it is thought that we must probably solve the multivariate algebraic equations of high degree that is equal to solving the NP complete problem. Then it is thought that our system is immune from the attacks by quantum computers.

In the next section, we begin with the definition of the product AB between A and B on the non-commutative quaternion ring over ***Fq***. In section 3 ,we generate the multivariate functions of high degree on the ring. In section 4, we describe the element expression of the multivariate functions of high degree . In section 5,we construct proposed KAP. In section 6, we verify the strength of our KAP. We consider the size of the keys for our KAP in section 7. In the last section, we provide concluding remarks.

2. The definition of the product AB

Let *q* be an odd prime.Let ***H*** be the quaternion ring over ***Fq***. As we select the non-commutative quaternion ring as the basic 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

$$\begin{aligned} AB=(&a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 \bmod q,\\ &a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 \bmod q,\\ &a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 \bmod q,\\ &a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 \bmod q\ ). \end{aligned}$$

Let A^{-1} be the inverse of *A* such that

$$A^{-1}=(a_0I_s,-a_1I_s,-a_2I_s,-a_3I_s) \tag{1}$$

where

$$a_0^2+a_1^2+a_2^2+a_3^2 \neq 0 \quad mod\ q \tag{2}$$

$$I_s=1/(a_0^2+a_1^2+a_2^2+a_3^2)\ mod\ q. \tag{3}$$

3. Multivariate functions of high degree

Let *m, d* and *r* be positive integers . As secret keys we choose arbitrary parameters $A_i \in \boldsymbol{H}(i=1,..,m)$ which have the inverse A_i^{-1} . We define the multivariate function *F(X)* of high degree such that

$$F(X) = \sum_{i=1}^{m} [\ \prod_{j=0}^{d} A_i^{r^j} X^{r^j}]. \tag{4}$$

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 .

4. The element expression of *F(X)*

Let s be

$$s=1+r+r^2+\ldots+r^d. \quad (5)$$

Let (f_0,f_1,f_2,f_3) be the element expression of $F(X)$ .From (4), f_j $(j=0,..,3)$ is given such that

$$F(X)=(f_0,f_1,f_2,f_3) \quad , \quad (6)$$

$$f_j = \sum_{e_0+..+e_3=s} f_{je_0e_1e_2e_3} x_0^{e0} x_1^{e1} x_2^{e2} x_3^{e3} \bmod q \quad (7)$$

with $0 \leq e_0,e_1,e_2,e_3 \leq s$ and the coefficients $f_{je0e1e2e3}$ $\in \boldsymbol{Fq}$ to be published , where

$$X = (x_0, x_1, x_2, x_3) \in \mathbf{H},$$

$$x_i \in Fq, (i = 0,.., 3).$$

e_0,e_1,e_2 and e_3 are non-negative integers which satisfy $e_0+\ldots+e_3=s$.

Then the number n of $f_{je0e1e2e3}$ is

$$n={}_4H_s={}_{4_{s+3}}C_3. \quad (8)$$

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

5. Proposed key agreement protocol

Let's describe the procedure that user U and user V obtain the common keys using $F(X\ )$ and $T(X)$ as follows.

Let S be the set of system parameters

$$S=[q,d,r,m]. \quad (9)$$

1) User U selects randomly $A_i= (A_{i0}, A_{i1}, A_{i2}, A_{i3}) \in \boldsymbol{H}$ $(i=1,..,m)$.
   The secret key of user U is
   $SK=[A_i]\ (i=1,..,m)$ (10)
2) User U generates $F(X)$ such that

$$F(X) = \sum_{i=1}^{m} [\prod_{j=0}^{d} A_i^{r^j} X^{r^j}], \quad (11)$$

3) User U calculates $\{f_{je0e1e2e3}\}$ from (11) .
4) Let PK be the public key of user U such as
   $PK=\{f_{je0e1e2e3}\}$. (12)
   Beforehand user U publishes PK which consists of n parameters in $\boldsymbol{Fq}$.
5) User V selects randomly $R_i= (R_{i0}, R_{i1}, R_{i2}, R_{i3}) \in \boldsymbol{H}$ $(i=1,..,m)$
   which have the inverse R_i^{-1}.
6) User V generates $T(X)$ such that

$$T(X) = \sum_{i=1}^{m} [\prod_{j=0}^{d} R_i^{r^j} X^{r^j}]. \quad (13)$$

7) Let (t_0,t_1,t_2,t_3) be the element expression of $T(X)$. From (13) 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
   $T(X)=(t_0,t_1,t_2,t_3)$, (14)
   where

$$t_j = \sum_{e_0+..+e_3=s} t_{je_0e_1e_2e_3} x_0^{e0} x_1^{e1} x_2^{e2} x_3^{e3} \bmod q \quad (15)$$

with the coefficients $t_{je0e1e2e3} \in \boldsymbol{Fq}$. e_0,e_1,e_2 and e_3 are non-negative integers which satisfy $e_0+\ldots+e_3=s$.

Then the number n of $t_{je0e1e2e3}$ is

$$n={}_4H_s={}_{4_{s+3}}C_3.$$

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

8) User V sends $\{t_{je0e1e2e3}\}$ to user U .
9) User V calculates common keys $Kv1$ and $Kv2$ as follows.

Let $Kv1$ and $Kv2$ be

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

$Kv2=(Kv2_0,Kv2_1,Kv2_2,Kv2_3)$.

$$Kv1_j = \sum_{i=1}^{m} \sum_{e_0+..+e_3=s} f_{je_0e_1e_2e_3} R_{i0}^{e0} R_{i1}^{e1} R_{i2}^{e2} R_{i3}^{e3} \bmod q \quad (16)$$

$(j=0,1,2,3)$

e_0,e_1,e_2 and e_3 are non-negative integers which satisfy $e_0+\ldots+e_3=s$.

Let Rr_i and $Tv2_{ij}$ be

$$Rr_i = R_i^{r} = (Rr_{i0}, Rr_{i1}, Rr_{i2}, Rr_{i3}) \in \mathbf{H}, \quad (17)$$

$$Tv2_{ij} = \sum_{e_0+..+e_3=s} f_{je_0e_1e_2e_3} Rr_{i0}^{e0} Rr_{i1}^{e1} Rr_{i2}^{e2} Rr_{i3}^{e3} \bmod q. \quad (18)$$

$(i=1,..,m;j=0,1,2,3)$

e_0,e_1,e_2 and e_3 are non-negative integers which satisfy $e_0+\ldots+e_3=s$.

$$Kv2 = \sum_{i=1}^{m} R_i (Tv2_{i0},Tv2_{i1},Tv2_{i2},Tv2_{i3}) R_i^{-r^{d+1}} \in \mathbf{H}, \quad (19)$$

10) User U calculates common keys $Ku1,Ku2$ as follows.

Let $Ku1$ and $Ku2$ be

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

$Ku2=(Ku2_0,Ku2_1,Ku2_2,Ku2_3)$.

Let Ar_i and $Tu1_{ij}$ be

$$Ar_i = A_i^{r} = (Ar_{i0}, Ar_{i1}, Ar_{i2}, Ar_{i3}) \in \mathbf{H}, \quad (20)$$

$$Tul_{ij} = \sum_{e_0+..+e_3=s} t_{je_0e_1e_2e_3} Ar_{i0}^{e0} Ar_{i1}^{e1} Ar_{i2}^{e2} Ar_{i3}^{e3} \bmod q. \quad (21)$$

$(i=1,..,m;j=0,1,2,3)$

e_0,e_1,e_2 and e_3 are non-negative integers which satisfy $e_0+\ldots+e_3=s$.

$$Kul = \sum_{i=1}^{m} A_i (Tul_{i0},Tul_{i1},Tul_{i2},Tul_{i3}) A_i^{-r^{d+1}} \in \mathbf{H}, \quad (22)$$

$$Ku2_j = \sum_{i=1}^{m} \sum_{e_0+..+e_3=s} t_{je_0e_1e_2e_3} A_{i0}^{e0} A_{i1}^{e1} A_{i2}^{e2} A_{i3}^{e3} \bmod q \quad (23)$$

$(j=0,1,2,3)$

e_0,e_1,e_2 and e_3 are non-negative integers which satisfy $e_0+\ldots+e_3=s$.

We can confirm that

$Ku1=Kv1,$ (24)

$Ku2=Kv2$ (25)

as follows.

$$Kv1 = \sum_{y=1}^{m} F(R_y) = \sum_{y=1}^{m} \sum_{i=1}^{m} [\prod_{j=0}^{d} A_i^{r^j} R_y^{r^j}], \tag{26}$$

$$Ku1 = \sum_{y=1}^{m} A_y T(A_y^{r}) A_y^{-r^{d+1}}$$

$$= \sum_{y=1}^{m} A_y \{ \sum_{i=1}^{m} [\prod_{j=0}^{d} R_i^{r^j} A_y^{r^{j+1}}]\} A_y^{-r^{d+1}},$$

$$= \sum_{y=1}^{m} \{ \sum_{i=1}^{m} A_y \prod_{j=0}^{d} R_i^{r^j} A_y^{r^{j+1}} \} A_y^{-r^{d+1}}$$

$$= \sum_{y=1}^{m} \sum_{i=1}^{m} \prod_{j=0}^{d} A_y^{r^j} R_i^{r^j} = Kv1. \tag{27}$$

We can also confirm in the same way that
Ku2=Kv2.

The common keys of user U and user V are *[Ku1,Ku2]* or *[Kv1,Kv2].*

6. Verification of the strength of our KAP

Let's examine the strength of our KAP. The strength of our KAP depends on the strength of the multivariate functions described in section 3. In other words, we mention the difficulty to obtain $A_i \in \boldsymbol{H}$ $(i=1,..,m)$ from the set of coefficients $\{f_{je_0e_1e_2e_3}\}$ of $F(X)$ to be the public keys .

6.1 Multivariate algebraic equations from *F(X)*

Let A_i be

$$A_i=(A_{i0},A_{i1},A_{i2},A_{i3}) \quad (i=1,..,m) . \tag{28}$$

From (4) all $f_{je_0e_1e_2e_3}$ have the form

$$f_{je_0e_1e_2e_3} =$$

$$\sum_{i=1}^{m} \sum_{cij0+..+cij3=s} h_{ije_0...e_3c_{ij0}..c_{ij3}} A_{i0}^{c_{ij0}} ..A_{i3}^{c_{ij3}} \mod q \tag{29}$$

$$(j = 0,..,3;0 \le e_0 ,e_1 ,e_2 ,e_3 \le s)$$

with the coefficients $h_{ije0..e3cij0..cij3} \in \boldsymbol{Fq}$ where c_{ij0},c_{ij1},c_{ij2} and c_{ij3} are non-negative integers which satisfy $c_{ij0}+\ldots+c_{ij3}=s$.

From (29) we obtain n multivariate algebraic equations over $\boldsymbol{Fq}$ where $A_{ij} \in \boldsymbol{Fq}$ $(i=1,..,m;j=0,..,3)$ are the variables i.e. unknown numbers.

6. 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 the case of $d=2$ and $r=3$ as samples of lower degree equations.
s:degree of equations $=1+3+3^2=13.$
n :the number of equations $=4({}_{s+3}C_3)=2240.$
We select m so that the number of variables(i.e secret keys) is nearly equal to n , that is
$m=\lceil(4_{s+3}C_3)/4\rceil=560,$
where $\lceil * \rceil$ means the largest integer less than or the integer equal to *.
z :the number of variables $=4m=2240$
$d_{reg}=s+1=14$
$G=O(({}_nC_{dreg})^w)=O(2^{285})$ is more than 2^{80} which is the standard for safety where $w=2.39$.

Our KAP is immune from the Gröbner bases attacks and from the differential attacks because of the equations of high degree in (29).

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

7. The Size of the keys

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 $d=2$ and $r=3$, the size of *PK* ,and *SK* is *23kbits* , *23kbits* each.

8. Conclusion

We proposed the KAP using multivariate functions on non-commutative quaternion ring over $\boldsymbol{Fq}$**.** It is a computationally difficult problem to obtain the secret keys $[A_i]$ from the public keys $\{f_{je_0e_1e_2e_3}\}$ 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 .

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