A Digital Signature Using Multivariate Functions on Quaternion Ring

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

SUMMARY: We propose the digital signature scheme on non-commutative quaternion ring over finite fields in this paper. We generate the multivariate function of high degree *F(X)* . We construct the digital signature scheme using *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 .
key words: digital signature, multivariate algebraic equations, Gröbner bases attacks , quaternion, NP complete problems.

1. Introduction

Since Diffie and Hellman proposed the concept of the public key cryptosystem in 1976[1], various digital signature schemes were proposed.

Typical examples of digital signature are as follows.

1)The digital signature using RSA cryptosystem[2] based on factoring problem ,
2)the ElGamal signature scheme [3] based on the discrete logarithm problem over finite fields ,
3)the digital signature using elliptic curve cryptosystem[4] based on the discrete logarithm problem on the elliptic curve[5],[6],
4)the digital signature scheme based on multivariate public key cryptosystem (MPKC), such as the digital signature scheme using stepwise triangular scheme (STS), which is one of the basic trapdoors of MPKC[11], and so on.

Sato and Araki proposed a digital signature using non-commutative quaternion ring[7] which has been broken[8].

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 the digital signature scheme using multivariate functions of high degree on non-commutative quaternion[9] 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 digital signature scheme. In section 6, we verify the strength of our digital signature. We consider the size of the keys for our digital signature in section 7. In the last section, we provide concluding remarks.

2. The definition of the product AB

Let ***H*** be the quaternion ring over ***Fq***. 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

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

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.

3. Multivariate functions of high degree

Let q be an odd prime. Let m, d and r be positive integers . We choose arbitrary parameters $k_i \in$ ***Fq*** and $A_j \in$ ***H***$(i=1,..,m)$ as secret keys . We define the multivariate function $F(X)$ of high degree such that

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

where $X \in$ ***H*** is a variable. We determine the value of m later.

Next we choose an arbitrary element $R \in$ ***H*** to be non-commutative to A_j $(j=1,..,m)$ .We define a temporary multivariate function $T(X)$ such that

$$T(X)=\sum_{i=1}^{m}[k_i\prod_{j=0}^{d}A_i^{r^j}R^{r^j}X^{r^j}]. \tag{2}$$

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

Let s be

$s=1+r+r^2+..+r^d$. (3)

Let $F(X)$ be

$F(X)=(f_0,f_1,f_2,f_3)$, (4)

$$f_j = \sum_{e_0+..+e_3=s} f_{je_0e_1e_2e_3} x_0^{e_0} x_1^{e_1} x_2^{e_2} x_3^{e_3} \mod q \quad (5)$$

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

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 $f_{je_0e_1e_2e_3}$ is

$n={}_4H_s={}_{s+3}C_3$. (6)

Let $\{ f_{je_0e_1e_2e_3} \}$ be the set that includes all $f_{je_0e_1e_2e_3}$.

Let $T(X)$ be

$T(X)=(t_0,t_1,t_2,t_3)$, (7)

$$t_j = \sum_{e_0+..+e_3=s} t_{je_0e_1e_2e_3} x_0^{e_0} x_1^{e_1} x_2^{e_2} x_3^{e_3} \mod q \quad (8)$$

(j=0,1,2,3)

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

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

5. Proposed digital signature scheme

We construct the digital signature scheme using $F(X)$ and $T(X)$ as follows.

Let $[q,d,r,m]$ be the system parameters.

Let's describe the procedure that user U sends to user V a signature S.

1) User U selects $A_i \in \boldsymbol{H}$ $(i=1,..,m)$ *and* $R \in \boldsymbol{H}$ randomly,

where R is non-commutative to $A_i \in \boldsymbol{H}$ $(i=1,..,m)$.

2) User U calculates g as follows.

Let message E be

$E= (E_0,E_1,E_2,E_3) \in \boldsymbol{H}$, (9)

where E is non-commutative to $R,A_i \in \boldsymbol{H}$ $(i=1,..,m)$.

Let g be

$g=E_0+E_1+E_2+E_3$. (10)

3) User U generates $F(X)$ and $T(X)$ such that

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

$$T(X) = \sum_{i=1}^{m} [k_i \prod_{j=0}^{d} A_i^{r^j} R^{(g-1)r^j} X^{r^j}]. \quad (12)$$

4) User U calculates $\{f_{je0e1e2e3}\}$ and $\{t_{je0e1e2e3}\}$ from (11) and (12).

5) User U publishes the set of coefficients $\{f_{je0e1e2e3}\}$ as user U's public keys beforehand.

6) User U sends S to User V such that

$S=[\{t_{je_0e_1e_2e_3}\},R,E]$. (13)

7) User V calculates g as follows.

$g=E_0+E_1+E_2+E_3$.

8) User V confirms that $F(R^gE) \neq T(RE)$ by using $\{f_{je0e1e2e3}\}$ and $\{t_{je0e1e2e3}\}$ as follows.

Let R^gE be

$R^gE= (b_0,b_1,b_2,b_3)$.

$$F(R^g E) = \sum_{i=1}^{m} [k_i \prod_{j=0}^{d} A_i^{r^j} (R^g E)^{r^j}]$$

$$= F((b_0, b_1, b_2, b_3)) = (f_0', f_1', f_2', f_3') \quad (14)$$

where

$$f_j' = \sum_{e_0+..+e_3=s} f_{je_0e_1e_2e_3} b_0^{e_0} b_1^{e_1} b_2^{e_2} b_3^{e_3} \mod q, \quad (15)$$

$(j=0,1,2,3)$. e_0,e_1,e_2 and e_3 are non-negative integers which satisfy $e_0+\ldots+e_3=s$.

We can obtain $T(RE)$ using $\{ t_{je0e1e2e3} \}$ in the same way.

If $F(R^gE)=T(RE)$,then user V decides S to be not user U's signature.

The reason is given as follows.

The adversary can easily generate $F(R^{g-1}X)$ such that

$$F(R^{g-1}X) = \sum_{i=1}^{m} [k_i \prod_{j=0}^{d} A_i^{r^j} (R^{g-1}X)^{r^j}]. \quad (16)$$

$F(X)$ satisfies $F(R^gE)= F(R^{g-1}(RE))$.

Then user V needs to confirm that $F(R^gE) \neq T(RE)$ to prevent the adversary from disguising $F(R^{g-1}X)$ in $T(X)$.

9) User V selects a random integer p.

User V calculates $F(R^{g+p})$ and $T(R^{p+1})$ in the same way as 8).

10) If $F(R^{g+p})=T(R^{p+1})$ is true, user V considers S as user U's signature .

The system parameter is $[q,r,d,m]$.The public key is $PK=[\{f_{je_0e_1e_2e_3}\}$ $(j=0,..,3{:}0 \leqq e_0,..,e_3 \leqq s)]$ and the secret key is $SK=[k_i,A_i$ $(i=1,..,m)]$ in our digital signature sheme.

We recommend the size of p to be $O(q^2)$.

6. Verification of the strength of our digital signature

Let's examine the strength of our digital signature. The strength of our digital signature depends on the strength of the multivariate functions described in section 3. In other words, we mention the difficulty to obtain $k_i \in \boldsymbol{Fq}$ and $A_i \in \boldsymbol{H}$ $(i=1,..,m)$ from the value 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_j be

$A_i=(A_{i0},A_{i1},A_{i2},A_{i3})$ $(i=1,..,m)$. (19)

All $f_{je_0e_1e_2e_3}$ have the form

$$f_{je_0e_1e_2e_3} = \sum_{i=1}^{m} k_i \sum_{c_{ij0}+..+c_{ij3}=s} h_{ije_0..e_3c_{ij0}..c_{ij3}} A_{i0}^{c_{ij0}} .. A_{i3}^{c_{ij3}} \mod q \quad (20)$$

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

with the coefficients $h_{ije_0..e_3c_{ij0}..c_{ij3}} \in \boldsymbol{F_q}$ where $c_{ij0}, c_{ij1}, c_{ij2}$ and c_{ij3} are non-negative integers which satisfy $c_{ij0}+\dots+c_{ij3}=s$.

From (20) we obtain n multivariate algebraic equations over $\boldsymbol{F_q}$ where k_i and $A_{ij} \in \boldsymbol{F_q}$ $(i=1,..,m; j=0,..,3)$ 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[10] to obtain the Gröbner bases for our multivariate algebraic equations on quaternion ring so that we confirm immunity of our digital signature scheme 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 $=s+1=1+3+3^2+1=14$.

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

$m=\lfloor (4_{s+3}C_3)/(4+1) \rfloor=448$,

where $\lfloor * \rfloor$ means the largest integer less than or the integer equal to $*$.

v :the number of variables $=5m=2240$

$d_{reg}=s'+1=15$

$G=O(({}_nG_{dreg})^w)=O(2^{302})$ is more than 2^{80} which is the standard for safety where $w=2.39$.

Our digital signature scheme is immune from the Gröbner bases attacks and from the differential attacks because of the equations of high degree in (20).

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

7. The Size of the keys

We consider the size of the system parameter q . We choose $q=O(2^{20})$ so that the size of the space of $F(R^{g+p})$ or $T(R^{p+1})$ is more than $O(2^{80})$.

In the case of $d=2$ and $r=3$, the size of PK , SK and S is *45kbits* , *45kbits* ,*45kbits* each.

8. Conclusion

We proposed the digital signature scheme using multivariate functions on non-commutative quaternion ring over $\boldsymbol{F_q}$. It is a computationally difficult problem to obtain the secret key $[k_i, A_i \ (i=1,..,m)]$ from the public key $[\{f_{je_0e_1e_2e_3}\} \ (j=0,..,3: 0 \leqq e_0,..,e_3 \leqq s)]$ because the problem is one of NP complete problems. In order to ensure the safety, the size of q is to be more than *20* bits .

We can construct the same schemes 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] Satoh and Araki, "On Construction of Signature Scheme over a Certain Non-commutative ring ", IEEE Trans. Fundamentals , Vol.E80-A, No.1 January, 1997.

[8] Don Coppersmith, "Weakness in Quaternion Signatures", Journal of Cryptology , Vol.14, i2, pp77-85 (2001).

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

[10] 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.

[11] Shigeo Tsujii, Masahito Gotaishi and Kohtaro Tadaki, "Proposal on Multivariate Public Key Signature Scheme Applying the STS cryptosystem," IEICE Tech. Rep., vol. 109, no. 271, ISEC2009-59, pp. 55-60, Nov. 2009.