A Digital Signature Based on Multivariate Polynomials over Fq

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

SUMMARY: We propose the digital signature scheme based on multivariate polynomials over finite fields in this paper. We generate the multivariate a polynomial 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 polynomial , multivariate algebraic equation, Gröbner bases attacks , 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)[11],[12],

and so on.

Sato and Araki proposed a digital signature[7] using non-commutative quaternion ring 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 except [12] 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 polynomials of high degree over finite fields ***Fq***. 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 generate the multivariate polynomial of high degree over ***Fq***. In section 3, we describe the expansion of the multivariate polynomial of high degree . In section 4,we construct proposed digital signature scheme. In section 5, we verify the strength of our digital signature. We consider the size of the keys for our digital signature in section 6. In the last section, we provide concluding remarks.

2. Multivariate polynomial of high degree

Let q be a prime. Let n,d and m be positive integers . We choose arbitrary parameters $k_i\,,a_{ij} \in \boldsymbol{Fq}$ $(i=1,..,m;j=1,..,n)$ as secret keys . We define the multivariate polynomial $F(X) \in \boldsymbol{Fq}[x_1,x_2,..,x_n]$ of high degree such that

$$F(X)=\sum_{i=1}^{m}[k_i(\sum_{\lambda=1}^{d}(\sum_{j=1}^{n}a_{ij}x_j)^{\lambda})], \tag{1}$$

$$\det(a_{ij})\neq 0 \mod q \tag{2}$$

where $X=(x_1,x_2,..,x_n)^T \in \boldsymbol{Fq}[x_1,x_2,..,x_n]^n$. We select the value of d and n arbitrarily ,but determine the value of m later.

Next we choose an arbitrary parameters $r_{ij} \in \boldsymbol{Fq}$ $(j=1,..,m;j=1,..,n)$ .We define a temporary multivariate polynomial $T(X) \in \boldsymbol{Fq}[x_1,x_2,..,x_n]$ such that

$$T(X)=\sum_{i=1}^{m}[k_i(\sum_{\lambda=1}^{d}(\sum_{j=1}^{n}r_{ij}x_j)^{\lambda})]. \tag{3}$$

3. Expansion of *F(X)*

From (1), the expansion of $F(X)$ is given such that

$$F(X)=\sum_{i=1}^{d}\sum_{e_{i1}+..+e_{in}=i} f_{ie_{i1}..e_{in}}x_1^{e_{i1}}....x_n^{e_{in}} \tag{4}$$

with the coefficients $f_{ie_{i1}..e_{in}} \in \boldsymbol{Fq}$ to be published , where $e_{ij}(i=1,..,d;j=1,..,n)$ are non-negative integers which satisfy $e_{i1}+..+e_{in}=i,(i=1,..,d)$.

Then the number N of $f_{ie_{i1}..e_{in}}$ is

$$N=\sum_{i=1}^{d}{}_nH_i=\sum_{i=1}^{d}{}_{n+i-1}C_i \tag{5}$$

Let B_f be the set $\{f_{ie_{i1}..e_{in}}\}$ that includes all $f_{ie_{i1}..e_{in}}$. $f_{ie_{i1}..e_{in}}$ in B_f is arranged according to some rule to be made public.

We determine the value of m as follows.

$$m=\lfloor N/(n+1)\rfloor, \tag{6}$$

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

From (3), the expansion of $T(X)$ is given such that

$$T(X) = \sum_{i=1}^{d} \sum_{e_{i1}+..+e_{in}=i} t_{ie_{i1}..e_{in}} x_1^{e_{i1}} \cdots x_n^{e_{in}} \tag{7}$$

with the coefficients $t_{ie_{i1}..e_{in}} \in \boldsymbol{Fq}$ to be published, where $e_{ij} (i=1,..,d; j=1,..,n)$ are non-negative integers which satisfy $e_{i1}+..+e_{in}=i, (i=1,..,d)$.

Then the number N' of $t_{ie_{i1}..e_{in}}$ is equal to N.
Let B_t be the set $\{t_{ie_{i1}..e_{in}}\}$ that includes all $t_{ie_{i1}..e_{in}}$.

4. Proposed digital signature scheme

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

Let's describe the procedure that user U sends a signature S and parameters W with B_t to user V and user V verifies S to be the signature of user A.
The trusted third party(TTP) make the integers $\{q,n,d,m\}$ public.

4.1 Procedure of digital signature

1) User U selects randomly $k_i, a_{ij} \in \boldsymbol{Fq}$, where $\det(a_{ij}) \neq 0 \bmod q$.
2) User U generates $F(X)$ such that

$$F(X) = \sum_{i=1}^{m} [k_i (\sum_{\lambda=1}^{d} (\sum_{j=1}^{n} a_{ij} x_j)^{\lambda})].$$

3) User U obtains the expansion of $F(X)$ as follows;

$$F(X) = \sum_{i=1}^{d} \sum_{e_{i1}+..+e_{in}=i} f_{ie_{i1}..e_{in}} x_1^{e_{i1}} \cdots x_n^{e_{in}}$$

with the coefficients $f_{ie_{i1}..e_{in}} \in \boldsymbol{Fq}$ to be published, where $e_{ij} (i=1,..,d; j=1,..,n)$ are non-negative integers which satisfy $e_{i1}+..+e_{in}=i, (i=1,..,d)$.
Let B_f be the set $\{f_{ie_{i1}..e_{in}}\}$ that includes all $f_{ie_{i1}..e_{in}}$.
4) User U send the B_f to TTP with ID of user U.
5) User U selects randomly $r_{ij} \in \boldsymbol{Fq}$.
6) User U generates $T(X)$ such that

$$T(X) = \sum_{i=1}^{m} [k_i (\sum_{\lambda=1}^{d} (\sum_{j=1}^{n} r_{ij} x_j)^{\lambda})].$$

7) User U obtains the expansion of $T(X)$ as follows;

$$T(X) = \sum_{i=1}^{d} \sum_{e_{i1}+..+e_{in}=i} t_{ie_{i1}..e_{in}} x_1^{e_{i1}} \cdots x_n^{e_{in}}$$

with the coefficients $t_{ie_{i1}..e_{in}} \in \boldsymbol{Fq}$, where e_{ij} $(i=1,..,d; j=1,..,n)$ are non-negative integers which satisfy $e_{i1}+..+e_{in}=i, (i=1,..,d)$.
Let B_t be the set $\{t_{ie_{i1}..e_{in}}\}$ that includes all $t_{ie_{i1}..e_{in}}$.

8) User U generates the parameters $W_i = (w_{i1}, w_{i2}, .., w_{in})^T$, $w_{ij} \in Fq$, $(i,j=1,..,n)$ from the message M.
Let W be $[w_1, w_2, .., w_n]$.
9) User U calculates z_h $(h=1,..,n)$ as follows;

$$z_h = T(W_h) \tag{8}$$
$$= \sum_{i=1}^{d} \sum_{e_{i1}+..+e_{in}=i} t_{ie_{i1}..e_{in}} w_{h1}^{e_{i1}} \cdots w_{hn}^{e_{in}} \bmod q,$$
$$(h=1,..,n).$$

10) User U calculates c_{ij} $(i,j=1,..,n)$ which satisfy the following equations.

$$\sum_{j=1}^{n} a_{ij} c_{j1} = \sum_{j=1}^{n} r_{ij} w_{j1} \bmod q = R_{i1}$$
$$\sum_{j=1}^{n} a_{ij} c_{j2} = \sum_{j=1}^{n} r_{ij} w_{j2} \bmod q = R_{i2}$$
$$\cdots\cdots\cdots \tag{9}$$
$$\sum_{j=1}^{n} a_{ij} c_{j(n-1)} = \sum_{j=1}^{n} r_{ij} w_{j(n-1)} \bmod q = R_{i(n-1)}$$
$$\sum_{j=1}^{n} a_{ij} c_{jn} = \sum_{j=1}^{n} r_{ij} z_j \bmod q = R_{in}$$
$$(i=1,\ldots,n).$$

Here we can express (9) as follows;

$$A(c_{11},..,c_{1n}, c_{21},..,\ldots, c_{n1},..,c_{nn})^T$$
$$= (R_{11},..,R_{1n}, R_{21},..,\ldots, R_{n1},..,R_{nn})^T, \tag{10}$$

where

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix}, \tag{11}$$

$$A_{ij} = \begin{pmatrix} a_{ij} & 0 & \cdots & 0 \\ 0 & a_{ij} & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & a_{ij} \end{pmatrix}; n \times n \quad matrix. \tag{12}$$

We can explain that we obtain $\{c_{ij}\}$, $(i,j=1,..,n)$, that is, $\det(A) \neq 0 \bmod q$ as follows.
At 1st step we interchange the columns i and $n(i-1)+1$ of A for $i=2,..,n$. Next we interchange the row i and $n(i-1)+1$ for $i=2,..,n$.
At 2nd step we interchange the columns $n+i$ and $n(i-1)+2$ for $i=3,..,n$. Next we interchange the row $n+i$ and $n(i-1)+2$ of A for $i=3,..,n$.

… …

… …

At (n-1)th step we interchange the columns $n(n-2)+i$ and $n(i-1)+n-1$ for $i=n$. Next we interchange the row $n(n-2)+i$ and $n(i-1)+n-1$ for $i=n$.

Then we obtain A' such that

$$A' = \begin{pmatrix} (a_{ij}) & 0 & \cdots & 0 \\ 0 & (a_{ij}) & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & (a_{ij}) \end{pmatrix} ; n^2 \times n^2 matrix,$$

where

(a_{ij}) is a $n \times n$ matrix such that

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} .$$

So we obain

$$det(A)=(-1)^{2(n-1)+2(n-2)+\ldots+2} det(A')$$
$$= det(A') =(det(a_{ij}))^n. \quad (13)$$

From (2)

$det(A) \neq 0 \bmod q$.

We can obtain $\{c_{ij}\}, (i,j=1,..,n)$ over $\boldsymbol{Fq}$.

11) User U makes $\{c_{ij}\}, (i,j=1,..,n)$ the signature S of user U.

12) User sends $[S,W, B_t]$ to User V .

13) User V calculates z_h $(h=1,..,n)$ by using W, B_t as follows;

$$z_h = \sum_{i=1}^{d} \sum_{e_{i1}+..+e_{in}=i} t_{ie_{i1}..e_{in}} w_{h1}^{e_{i1}} \ldots w_{hn}^{e_{in}} \bmod q \quad (14)$$

$(h = 1,..,n)$.

14) User V confirms $F(X)=T(Y)$ as follows;

$$X=(x_1,x_2,..,x_n)^T,$$
$$x_1=c_{11}g_1+c_{12}g_2+..+c_{1n}g_n$$
$$\ldots\ldots\ldots \quad (15)$$
$$x_n=c_{n1}g_1+c_{n2}g_2+..+c_{nn}g_n$$

where $g_i\,(i=1,..,n)$ is valiable.

User V expands $F(X)$ by using (15) where variables are $g_i\,(i=1,..,n)$.

$$Y=(y_1,y_2,..,y_n)^T,$$
$$y_1=w_{11}g_1+w_{12}g_2+..+w_{1(n-1)}g_{n-1}+z_1g_n$$
$$\ldots\ldots\ldots \quad (16)$$
$$y_n=w_{n1}g_1+w_{n1}g_2+..+w_{n(n-1)}g_{n-1}+z_ng_n$$

User V expands $T(Y)$ by using (16) where variables are $g_i\,(i=1,..,n)$.

15) User V compares the coefficients of $F(X)$ with those of $T(Y)$ .If all coefficients of $F(X)$ are equal to those of $T(Y)$, then user V considers S to be the signature of user U, else user V considers S not to be the signature of user U.

User V can also confirm $F(X)=T(Y)$ by another manner as follws;

16-1) User V selects random numbers $v_{ij}(i=1,..,2n;j=1,..,n)$ and substitutes v_{ij} for g_j $(i=1,..,2n;j=1,..,n)$ of $F(X)$ and $T(Y)$.Then user V confirms $F((v_{i1},..,v_{in})^T)=T((v_{i1},..,v_{in})^T), (i=1,..,2n)$.

16-2) User V repeats 16-1)step 2n times. If $F((v_{i1},..,v_{in})^T)=T((v_{i1},..,v_{in})^T)$ is true 2n times ,then user V considers S to be the signature of user U, else user V considers S not to be the signature of user U.

4.2 Proof of *F(X)=T(Y)*

We can prove that $F(X)=T(Y)$ as follows;

$$\sum_{j=1}^{n} a_{ij}x_j = \sum_{j=1}^{n} a_{ij} \sum_{k=1}^{n} c_{jk}g_k$$
$$= \sum_{k=1}^{n} (\sum_{j=1}^{n} a_{ij}c_{jk})g_k \quad (i = 1,..,n), \quad (17)$$

$$\sum_{j=1}^{n} r_{ij}y_j = \sum_{j=1}^{n} r_{ij}(\sum_{k=1}^{n-1} w_{jk}g_k + z_jg_n)$$
$$= \sum_{k=1}^{n-1} (\sum_{j=1}^{n} r_{ij}w_{jk})g_k + (\sum_{j=1}^{n} r_{ij}z_j)g_n \quad (18)$$

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

From (9) we obtain

$$\sum_{j=1}^{n} a_{ij}x_j = \sum_{j=1}^{n} r_{ij}y_j \quad (i = 1,.., n). \quad (19)$$

Then from (1) and (3) we obtain

$F(X)=T(Y)$.

5. 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 polynomials described in section 2. In other words, we mention the difficulty to obtain k_i and $a_{ij} \in Fq\ (i,j=1,..,m)$ from the value of coefficients $f_{ie_{i1}..e_{in}}$ of $F(X)$ to be the public keys .

5.1 Multivariate algebraic equations derivative from *F(X)*

All $f_{ie_{i1}..e_{in}}$ in (4) have the form

$$f_{ie_{i1}\cdots e_{in}} = \sum_{j=1}^{m} b_{ie_{i1}..e_{in}} k_j a_{j1}^{e_{i1}} \dots a_{jn}^{e_{in}} \mod q \tag{20}$$

with the coefficients $b_{iei1\ldots ein} \in \boldsymbol{Fq}$ where $e_{ij}(j=1,..,n)$ are non-negative integers which satisfy

$e_{i1}+..+e_{in}=i.\ (i=1,..,d).$

From (20) we obtain N multivariate algebraic equations over $\boldsymbol{Fq}$ where k_j and a_{jr} $(j=1,..,m;r=1,..n)$ are the variables i.e. unknown numbers.

$\{q,n,d,m\}$ are the system parameters.

The public keys are $PK=\{f_{ie_{i1}..e_{in}}\}$ and the secret keys are $SK=\{k_i,a_{ij}\}$ in our digital signature sheme.

5. 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 over $\boldsymbol{Fq}$ so that we confirm immunity of our digital signature scheme to the Gröbner bases attack .

We describe the complexity of our scheme in the case of $d=5,n=5$ as samples of lower degree equations.

s:degree of multivariate algebraic equations $=d+1=6$.

N :the number of equations $={}_5C_1+{}_6C_2+{}_7C_3+{}_8C_4+{}_9C_5 =251$.

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

$m=\lfloor N/(5+1)\rfloor=41$,

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

v :the number of variables $=6m=246$

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

$G=O(({}_nC_{dreg})^w)=O(2^{103})$ 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.

6. The Size of the keys and complexity to obtain keys

We consider the size of the system parameter q . We select the size of q such that the size of the space of $\{c_{ij}\}$ is larger than 2^{80} to be the standard for safety. Then we need to select the size of modulus q larger than 4bit.

In the case of $d=5$,$n=5$ and $q=13$, the size of PK , SK, S and W is about $1kbits$ each.

The complexity to obtain $\{f_{ie_{i1}..e_{in}}\}$ in (4) and $\{t_{ie_{i1}..e_{in}}\}$ in (7),is $O(2^{20})$ each. The complexity to obtain c_{ij} $(i,j=1,..,n)$ is $O(n^6(log_2q)^2)=O(2^{18})$.

7. Conclusion

We proposed the digital signature scheme using multivariate polynomials over $\boldsymbol{Fq}$. It is a computationally difficult problem to obtain the secret keys $\{k_i ,a_{ij}\}$ from the public keys $\{f_{ie_{i1}..e_{in}}\}$ because the problem is one of NP complete problems. In order to ensure the safety, the size of q is to be more than 4 bits .

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.

[12] Masahiro Yagisawa, " A Digital Signature Using Multivariate Functions on Quaternion Ring ",Cryptology ePrint Archive,Report 2010/352,(2010-06).