Key Agreement Protocols Based on Multivariate Polynomials over *Fq*

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

SUMMARY: In this paper we propose new key agreement protocols based on multivariate polynomials over finite field ***Fq***. We concretely generate the multivariate polynomial $F(\boldsymbol{X}) \in Fq[x_1, . . . , x_n]$ such that $F(\boldsymbol{X})= \Sigma_{i=1}{}^m k_i[A_i(\boldsymbol{X})^d + A_i(\boldsymbol{X})^{d-1} + .. + A_i(\boldsymbol{X})]$ where $A_i(\boldsymbol{X}) = a_{i1}x_1+\ldots+a_{in}x_n$,coefficients k_i , $a_{ij} \in Fq$ $(i=1,..,m:j=1,..,n)$ and variables $\boldsymbol{X}=(x_1,..,x_n)^T \in Fq[x_1, . . . , x_n]^n$. The common key $K(\boldsymbol{X})$ has the form such that $K(\boldsymbol{X})= \Sigma_{i=1}{}^m h_i\, F((b_{i1}x_1,...,b_{in}x_n)^T)$ where h_i ,$b_{ij} \in Fq$ $(i=1,..,m:j=1,..,n)$ to be the temporary secret keys of the partner . Our system is immune from the Gröbner bases attacks because obtaining coefficients of $F(\boldsymbol{X})$ 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 because of the equations of high degree.

key words: key agreement protocol, multivariate polynomials, Gröbner bases, NP complete problems, finite field

1. Introduction

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

Though typical examples of KAP are almost based on the discrete logarithm problem over finite fields ,some schemes of KAP based on the multivariate equations were proposed by the current auther[10],[11].

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 polynomials over finite field ***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 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 system is immune from the attacks by quantum computers.

In the next section, we begin with generating the multivariate polynomials of high degree over finite field. In section 3, we describe the expansions of the multivariate polynomials of high degree. In section 4, we construct proposed KAP. In section 5, we verify the strength of our KAP. We consider the size of the keys for our KAP in section 6. In the last section, we provide concluding remarks.

2. The multivariate polynomials of high degree

Let q be a prime. Let ***Fq*** be the finite field.
Let m ,n and d be positive integers .
Let S be system parameters such that

$$S=[q,d,m,n] \quad . \tag{1}$$

As secret keys SK ,we choose arbitrary parameters k_i and $a_{ij} \in Fq$ $(i=1,..,m;j=1,..,n)$.

Let $F(\boldsymbol{X})$ be the polynomials in $Fq[x_1, . . . , x_n]$ such that

$$F(X) = \sum_{i=1}^{m} \sum_{j=1}^{d} k_i \{A_i(X)\}^j , \tag{2}$$

where

$$A_i(\boldsymbol{X})=a_{i1}x_1+\ldots+a_{in}x_n \quad ,(i=1,..,m) \tag{3}$$

$$\text{variables;}\ \boldsymbol{X}=(x_1,..,x_n)^T \in \boldsymbol{Fq}[x_1,..,x_n]^n \tag{4}$$

$$SK=[\, k_i,a_{ij}](i=1,..,m;j=1,..,n). \tag{5}$$

We determine the value of m later so that the total number of coefficients k_i and a_{ij} (i.e secret keys) is nearly equal to the number of equations .

3. The expansion of *F(X)*

We obtain the expansion of $F(\boldsymbol{X})$ from (2) as follows;

$$F(X) = \sum_{i=1}^{d} \sum_{e_{i1}+..+e_{in}=i} f_{ie_{i1}..e_{in}} x_1^{e_{i1}} \ldots x_n^{e_{in}} \tag{6}$$

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 $e_{i1}+..+e_{in}=i$.

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

$$N=\sum_{i=1}^{d} {}_{n}H_{i}=\sum_{i=1}^{d} {}_{n+i-1}C_{i} \tag{7}$$

Let $\{f_{ie_{i1}..e_{in}}\}$ be the set that includes all $f_{ie_{i1}..e_{in}}$.

We determine the value of m as follows.

$$m=\lfloor (N)/(n+1) \rfloor, \tag{8}$$

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

4. Proposed key agreement protocol

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

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

2) User U chooses randomly parameters $k_i,a_{i1} \in Fq, (i=1,..,m:j=1,..,n)$.
The secret key of user U is
$SK=[k_i,a_{i1}](i=1,..,m;j=1,..,n)$.

3) User U generates $F(\boldsymbol{X})$ such that

$$F(X)=\sum_{i=1}^{m}\sum_{j=1}^{d} k_i \{A_i(X)\}^j . \tag{9}$$

4) User U calculates the set of coefficients $\{f_{ie_{i1}..e_{in}}\}$ from (9) .

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

$$PK=\{f_{ie_{i1}..e_{in}}\}. \tag{10}$$

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

6) User V chooses randomly parameters
$h_i,b_{i1} \in Fq, (i=1,..,m:j=1,..,n)$

7) User V generates the temporary polynomial $T(\boldsymbol{X})$ such that

$$T(X)=\sum_{i=1}^{m}\sum_{j=1}^{d} h_i \{B_i(X)\}^j , \tag{11}$$

where

$B_i(\boldsymbol{X})=b_{i1}x_1+\ldots+b_{in}x_n \quad ,(i=1,..,m)$.

8) From (11) user V calculates the set of coefficients $\{t_{ie_{i1}..e_{in}}\}$ which consists of N parameters in $\boldsymbol{Fq}$.

The expansion of $T(\boldsymbol{X})$ is given such that

$$T(X)=\sum_{i=1}^{d}\sum_{e_{i1}+..+e_{in}=i} t_{ie_{i1}..e_{in}} x_1^{e_{i1}} \ldots x_n^{e_{in}} \tag{12}$$

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 $e_{i1}+..+e_{in}=i$.

Then the number N' of $t_{ie_{i1}..e_{in}}$ is equal to N.

Let $\{t_{ie_{i1}..e_{in}}\}$ be the set that includes all $t_{ie_{i1}..e_{in}}$.

9) User V sends $\{t_{ie_{i1}..e_{in}}\}$ to user U .

10) User V calculates common keys Kv as follows.
Let Kv be

$$Kv(X)=\sum_{r=1}^{m} h_r F((b_{r1}x_1,\ldots,b_{rn}x_n)^T). \tag{13}$$

From (2) we obtain

$$Kv(X)=\sum_{r=1}^{m}\sum_{i=1}^{m}\sum_{j=1}^{d} h_r k_i (a_{i1}b_{r1}x_1+..+a_{in}b_{rn}x_n)^j . \tag{14}$$

From (6) we obtain

$$Kv(X)=\sum_{r=1}^{m}\sum_{i=1}^{d}\sum_{e_{i1}+..+e_{in}=i} h_r f_{ie_{i1}..e_{in}} (b_{r1}x_1)^{e_{i1}} \ldots (b_{rn}x_n)^{e_{in}} . \tag{15}$$

11) User U calculates common keys Ku as follows.
Let Ku be

$$Ku(X)=\sum_{r=1}^{m} k_r T((a_{r1}x_1,\ldots,a_{rn}x_n)^T). \tag{16}$$

From (11) we obtain

$$Ku(X)=\sum_{r=1}^{m}\sum_{i=1}^{m}\sum_{j=1}^{d} k_r h_i (b_{i1}a_{r1}x_1+..+b_{in}a_{rn}x_n)^j . \tag{17}$$

From (12) we obtain

$$Ku(X)=\sum_{r=1}^{m}\sum_{i=1}^{d}\sum_{e_{i1}+..+e_{in}=i} k_r t_{ie_{i1}..e_{in}} (a_{r1}x_1)^{e_{i1}} \ldots (a_{rn}x_n)^{e_{in}} . \tag{18}$$

From (14) and (17) we can confirm that

$Ku=Kv,$ (19)

The common key of user U and user V is *Ku* or *Kv*.

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

5.1 Multivariate algebraic equations from $F(X)$

From (6) all $f_{ie_{i1}..e_{in}}$ have the form such that

$$f_{ie_{i1}\dots e_{in}} = \sum_{j=1}^{m} c_{ie_{i1}..e_{in}} a_{j1}^{e_{i1}} \dots a_{jn}^{e_{in}} \quad (20)$$

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

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

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

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

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[9] to obtain the Gröbner bases for our multivariate algebraic equations over $\boldsymbol{Fq}$ so that we confirm immunity of our KAP to the Gröbner bases attack .

We describe the complexity in case of $d=6,n=6$ and $q=7$ as samples of lower degree equations.
s:degree of equations $=d+1=7$.
N :the number of equations $={}_6H_6+..+{}_1H_1=637$.
We select m so that $(n+1)m$,the number of variables(i.e secret keys) is nearly equal to N , that is
$m=\lceil(N)/(n+1)\rceil=\lceil(637)/7\rceil=91.$
z :the number of variables $=(n+1)m=7*91=637$
$d_{reg}=s+1=8$
$G=O(({}_zG_{dreg})^w)=O(2^{141})$ 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 (20).

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

6. The size of the keys

We consider the size of the system parameter q . As q is a prime ,we obtain $a^q=a \in \boldsymbol{Fq}$. Then we select the size of q such that the modulus q is larger than d, the degree of $F(\boldsymbol{X})$.
In the case of $d=6,n=6$ and $q=7$, the size of *PK* or *SK* is smaller than *2kbits* .

7. Conclusion

We proposed the key agreement protocols based on multivariate polynomials over finite field $\boldsymbol{Fq}$. It was shown that our system is immune from the Gröbner bases attacks by calculating the complexity to obtain the Gröbner bases for our 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]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).

[11] Masahiro Yagisawa, " Key Agreement Protocols Using Multivariate Equations on Non-commutative Ring ",Cryptology ePrint Archive,Report 2010/458,(2010-08).