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 \( F_q \). 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
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 \( F_q \) 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 \( F_q \). 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 \( F_q \). 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 \( F_q \) such that

\[
AB = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 \mod q,
\]

\[
a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 \mod q,
\]

\[
a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 \mod q,
\]

\[
a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 \mod q.
\]

Let \( A^t \) be the inverse of A such that

\[
A^t = (a_0 I_0 - a_1 I_1 - a_2 I_2 - a_3 I_3)
\] where

\[
a_0^2 + a_1^2 + a_2^2 + a_3^2 \neq 0 \mod q
\]

\[
I_i = I/(a_0^2 + a_1^2 + a_2^2 + a_3^2) \mod q.
\]

3. Multivariate functions of high degree

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

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

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
\[
s = 1 + r + r^2 + \ldots + r^d,
\]
(5)

Let \((f_0, f_1, f_2, f_3)\) be the element expression of \( F(X) \). From (4), \( f_j (j = 0, \ldots, 3) \) is given such that
\[
F(X) = (f_0, f_1, f_2, f_3)
\]
(6)

with \( 0 \leq e_0, e_1, e_2, e_3 \leq s \) and the coefficients \( f_{j e_0 e_1 e_2 e_3} \) of \( F(X) \) to be published, where
\[
X = (x_0, x_1, x_2, x_3) \in H,
\]
\[
x_j \in F_q, \quad (i = 0, \ldots, 3),
\]
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 \( f_{j e_0 e_1 e_2 e_3} \) is
\[
n = 4H_s = 4s + 3C_3
\]
(8)

Let \( \{ f_{j e_0 e_1 e_2 e_3} \} \) be the set that includes all \( f_{j e_0 e_1 e_2 e_3} \).

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 \( S = \{ q, d, r, m \} \).

1) User U selects randomly \( A_i = (A_{i0}, A_{i1}, A_{i2}, A_{i3}) \in H \) \((i = 1, \ldots, m)\).

The secret key of user U is
\[
SK = [q, d, r, m]
\]
(10)

2) User U generates \( F(X) \) such that
\[
F(X) = \sum_{i=1}^{m} \prod_{j=0}^{d} A_{ij}^{e_i} x_i^{r_i}
\]
(11)

3) User U calculates \( f_{j e_0 e_1 e_2 e_3} \) from (11).

4) Let \( PK \) be the public key of user U such as
\[
PK = \{ f_{j e_0 e_1 e_2 e_3} \}
\]
(12)

Beforehand user U publishes \( PK \) which consists of \( n \) parameters in \( F_q \).

5) User V selects randomly \( R_i = (R_{i0}, R_{i1}, R_{i2}, R_{i3}) \in H \) \((i = 1, \ldots, m)\) which have the inverse \( R_i^{-1} \).

6) User V generates \( T(X) \) such that
\[
T(X) = \sum_{j=0}^{2} \prod_{i=0}^{d} R_{ij}^{e_i} x_i^{r_i}
\]
(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 \( \{ t_{j e_0 e_1 e_2 e_3} \} \) which consists of \( n \) parameters in \( F_q \).

\( t_j (j = 0, \ldots, 3) \) is given such that
\[
T(X) = (t_0, t_1, t_2, t_3)
\]
(14)

where
\[
t_j = \sum_{e_0 + \ldots + e_3 = s} f_{j e_0 e_1 e_2 e_3} x_0^{e_0} x_1^{e_1} x_2^{e_2} x_3^{e_3} \mod q
\]
(15)

with the coefficients \( f_{j e_0 e_1 e_2 e_3} \) of \( F_q \). \( e_0, e_1, e_2, e_3 \) are non-negative integers which satisfy \( e_0 + \ldots + e_3 = s \).

Then the number \( n \) of \( f_{j e_0 e_1 e_2 e_3} \) is
\[
n = 4H_s = 4s + 3C_3
\]
Let \( \{ f_{j e_0 e_1 e_2 e_3} \} \) be the set that includes all \( f_{j e_0 e_1 e_2 e_3} \).

8) User V sends \( \{ f_{j e_0 e_1 e_2 e_3} \} \) to user U.

9) User V calculates common keys \( K_{u1}, K_{v1} \) as follows.

Let \( K_{u1}, K_{v1} \) be
\[
K_{u1} = (K_{u10}, K_{u11}, K_{u12}, K_{u13}) \in H
\]
and
\[
K_{v1} = (K_{v10}, K_{v11}, K_{v12}, K_{v13}) \in H
\]
(17)

\[
K_{v2} = \sum_{i=1}^{m} \sum_{j=0}^{d} f_{j e_0 e_1 e_2 e_3} R_{0i}^{e_0} R_{1i}^{e_1} R_{2i}^{e_2} R_{3i}^{e_3} \mod q
\]
(18)

\[
K_{u2} = \sum_{i=1}^{m} \sum_{j=0}^{d} f_{j e_0 e_1 e_2 e_3} A_{0i}^{e_0} A_{1i}^{e_1} A_{2i}^{e_2} A_{3i}^{e_3} \mod q
\]
(21)

10) User U calculates common keys \( K_{u2}, K_{v2} \) as follows.

Let \( K_{u2}, K_{v2} \) be
\[
K_{u2} = (K_{u20}, K_{u21}, K_{u22}, K_{u23})
\]
and
\[
K_{v2} = (K_{v20}, K_{v21}, K_{v22}, K_{v23})
\]
(19)

\[
K_{u1} = K_{v1},
\]
(24)

\[
K_{u2} = K_{v2}
\]
(25)
\[
Kv_l = \sum_{y=1}^{m} F(R_y) = \sum_{y=1}^{m} \sum_{i=1}^{m} \left( \prod_{j=0}^{\ell-1} A_{y_j}^{r_j} R_{y_j}^{r_j} \right), 
\]
(26)

\[
Ku_l = \sum_{y=1}^{m} A_y \sum_{i=1}^{d} A_y^{r_i} \prod_{j=0}^{\ell-1} A_{y_j}^{r_j} = \sum_{y=1}^{m} A_y \sum_{i=1}^{d} \prod_{j=0}^{\ell-1} A_{y_j}^{r_j}.
\]

\[
\sum_{y=1}^{m} \sum_{i=1}^{m} \prod_{j=0}^{\ell-1} A_{y_j}^{r_j} \cdot A_{y}^{r_i} = \sum_{y=1}^{m} \sum_{i=1}^{m} \prod_{j=0}^{\ell-1} A_{y_j}^{r_j} R_i^{r_i} = Ku_l. 
\]
(27)

We can also confirm in the same way that \( Ku_2 = Ku_2 \).

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 \( f_{j(e^j e^j e^j)} \) from the set of coefficients \( \left\{ f_{j(e^j e^j e^j)} \right\} \) of \( F(X) \) to be the public keys.

6.1 Multivariate algebraic equations from \( F(X) \)

Let \( A_i \) be
\[
A_i = (A_{i_0}, A_{i_1}, A_{i_2}, A_{i_3}) \quad (i=1,\ldots,m). 
\]
(28)

From (4) all \( f_{j(e^j e^j e^j)} \) have the form
\[
f_{j(e^j e^j e^j)} = \sum_{i=1}^{m} \sum_{c_{i_0}, c_{i_1}, c_{i_2}, c_{i_3}} h_{i_0, i_1, i_2, i_3} A_{i_0}^{c_{i_0}} A_{i_1}^{c_{i_1}} A_{i_2}^{c_{i_2}} A_{i_3}^{c_{i_3}} \mod q 
\]
(29)

with the coefficients \( h_{i_0, i_1, i_2, i_3} \in F_q \) where \( c_{i_0} c_{i_1} c_{i_2} c_{i_3} \) are non-negative integers which satisfy \( c_{i_0} + c_{i_1} + c_{i_2} + c_{i_3} \leq s \).

From (29) we obtain \( n \) multivariate algebraic equations over \( F_q \) where \( A_{i_j} \in F_q \) \( (i=1,\ldots,m; j=0,\ldots,3) \) 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(\( s_{e} C_{3} \)) = 2240.

We select \( m \) so that the number of variables (i.e. secret keys) is nearly equal to \( n \), that is
\[
m = \left( 4(\sum_{i=0}^{e-1} C_{3}^i) \right) / 41 = 560.
\]

where \( i \neq 1 \) is the largest integer less than or the integer equal to *. \( z: \) the number of variables = 4\( m = 2240 \)
\[
d_{eq} = s + l = 14 
\]
\[
G = O(s C_{dreg}) \approx O(2^{385}) \quad \text{is more than} \quad 2^{90} \quad \text{which is the standard for safety where} \quad w = 2.39.
\]

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 \( Ku_1 \) and \( Ku_2 \) is more than \( O(2^{90}) \).

In the case of \( d=2 \) and \( r=3 \), the size of \( PK \) and \( SK \) is \( 23 \text{bits} \), \( 23 \text{bits} \) each.

8. Conclusion

We proposed the KAP using multivariate functions on non-commutative quaternion ring over \( F_q \). It is a computationally difficult problem to obtain the secret keys \( \{ A_i \} \) from the public keys \( \{f_{j(e^j e^j e^j)}\} \) 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


[7] Shigeo Tsuji, Kohtaro Tadaki, Masahito Gotaishi ,Ryo
