FULLY HOMOMORPHIC ENCRYPTION WITHOUT BOOTSTRAPPING

Masahiro Yagisawa†
†Resident in Yokohama-shi
Sakae-ku, Yokohama-shi, Japan
tfkt8398yagi@hb.tp1.jp

SUMMARY: Gentry's bootstrapping technique is the most famous method of obtaining fully homomorphic encryption. In previous work I proposed a fully homomorphic encryption without bootstrapping which has the weak point in the plaintext [1],[18]. In this paper I propose the improved fully homomorphic encryption scheme on non-associative octonion ring over finite field without bootstrapping technique where the plaintext consists of a plaintext u and two random numbers v,w. The proposed fully homomorphic encryption scheme is immune from the "u and $-u$ attack". As the scheme is based on computational difficulty to solve the multivariate algebraic equations of high degree while the almost all multivariate cryptosystems [2],[3],[4],[5],[6],[7] proposed until now are based on the quadratic equations avoiding the explosion of the coefficients. Because proposed fully homomorphic encryption scheme is based on multivariate algebraic equations with high degree or too many variables, it is against the Gröbner basis [8] attack, the differential attack, rank attack and so on.

The key size of this system and complexity for enciphering /deciphering become to be small enough to handle.
keywords: fully homomorphic encryption, multivariate algebraic equation, Gröbner basis, octonion

§1. Introduction

A cryptosystem which supports both addition and multiplication (thereby preserving the ring structure of the plaintexts) is known as fully homomorphic encryption (FHE) and is very powerful. Using such a scheme, any circuit can be homomorphically evaluated, effectively allowing the construction of programs which may be run on encryptions of their inputs to produce an encryption of their output. Since such a program never decrypts its input, it can be run by an untrusted party without revealing its inputs and internal state. The existence of an efficient and fully homomorphic cryptosystem would have great practical implications in the outsourcing of private computations, for instance, in the context of cloud computing.

With homomorphic encryption, a company could encrypt its entire database of e-mails and upload it to a cloud. Then it could use the cloud-stored data as desired—for example, to calculate the stochastic value of stored data. The results would be downloaded and decrypted without ever exposing the details of a single e-mail.

In 2009 Gentry, an IBM researcher, has created a homomorphic encryption scheme that makes it possible to encrypt the data in such a way that performing a mathematical operation on the encrypted information and then decrypting the result produces the same answer as performing an analogous operation on the unencrypted data[9],[10].

But in Gentry's scheme a task like finding a piece of text in an e-mail requires chaining together thousands of basic operations. His solution was to use a second layer of encryption, essentially to protect intermediate results when the system broke down and needed to be reset.

Some fully homomorphic encryption schemes were proposed until now [11],[12],[13],[14],[15].

In this paper I propose a fully homomorphic encryption scheme on non-associative octonion ring over finite field which is based on computational difficulty to solve the multivariate algebraic equations of high degree while the almost all multivariate cryptosystems [4],[5],[6],[7] proposed until now are based on the quadratic equations avoiding the explosion of the coefficients. Our scheme is against the Gröbner basis [8] attack, the differential attack, rank attack and so on.

Organization of this paper is as follows. In Sec.2 preliminaries for octonion operation are described. In Sec.3 we construct proposed fully homomorphic encryption scheme. In Sec.4 the procedure for proposed fully homomorphic encryption scheme is described. In Sec.5 re-encryption scheme is described. In Sec.6 we analyse proposed scheme to show that proposed scheme is immune from the Gröbner basis attacks by calculating the complexity to obtain the Gröbner basis for the multivariate algebraic equations. In Sec.7 we describe the size of the parameters and the complexity for enciphering and deciphering. In Sec.8 we describe conclusion. In Sec.9 we consider the composition of plaintext.

§2. Preliminaries for octonion operation

In this section we describe the operations on octonion ring and properties of octonion ring.

§2.1 Multiplication and addition on the octonion ring *O*

Let q be a fixed modulus to be as large prime as $O(2^{10})$.

Let O be the octonion [16]ring over a finite field $\boldsymbol{Fq}$.

$$O=\{(a_0,a_1,\ldots,a_7) \mid a_j \in \boldsymbol{Fq}\ (j=0,1,\ldots,7)\} \tag{1}$$

We define the multiplication and addition of $A,B \in O$ as follows.

$$A=(a_0,a_1,\ldots,a_7),\quad a_j \in \boldsymbol{Fq}\ (j=0,1,\ldots,7), \tag{2}$$

$$B=(b_0,b_1,\ldots,b_7),\ b_j \in \boldsymbol{Fq}\ (j=0,1,\ldots,7). \tag{3}$$

$$\begin{aligned}
&AB \bmod q\\
&= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7 \bmod q,\\
&\quad a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3 \bmod q,\\
&\quad a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6 \bmod q,\\
&\quad a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1 \bmod q,\\
&\quad a_0b_4+a_1b_2 - a_2b_1 - a_3b_6+a_4b_0+a_5b_7+ a_6b_3 - a_7b_5 \bmod q,\\
&\quad a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4 \bmod q,\\
&\quad a_0b_6+a_1b_5 - a_2b_7+a_3b_4 - a_4b_3 - a_5b_1+a_6b_0 +a_7b_2 \bmod q,\\
&\quad a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0 \bmod q)
\end{aligned} \tag{4}$$

$$\begin{aligned}
&A+B \bmod q\\
&=(a_0+b_0 \bmod q,\ a_1+b_1 \bmod q,\ a_2+b_2 \bmod q,\ a_3+b_3 \bmod q\ ,\\
&\quad a_4+b_4 \bmod q,\ a_5+b_5 \bmod q,\ a_6+b_6 \bmod q,\ a_7+b_7 \bmod q\ ).
\end{aligned} \tag{5}$$

Let

$$|A|^2= a_0^2+a_1^2+\ldots+a_7^2 \bmod q. \tag{6}$$

If $|A|^2 \neq 0 \bmod q$, we can have A^{-1}, the inverse of A by using the algorithm **Octinv**(A) such that

$$A^{-1}= (a_0/|A|^2 \bmod q,\ -a_1/|A|^2 \bmod q,\ldots,\ -a_7/|A|^2 \bmod q) \leftarrow \textbf{Octinv}(A). \tag{7}$$

Here details of the algorithm **Octinv**(A) are omitted and can be looked up in the **Appendix A.**

§2.2 Order of the element in *O*

In this section we describe the order "J" of the element "A" in octonion ring, that is,

$$A^{J+1}=A \bmod q.$$

Theorem 1

Let $A:=(a_{10},a_{11},\ldots,a_{17})\in O,\ a_{1j}\in Fq \quad (j=0,1,\ldots,7)$.

Let $(a_{n0},a_{n1},\ldots,a_{n7}):=A^{n}\in O,\ a_{nj}\in Fq \quad (n=1,2,\ldots;j=0,1,\ldots,7)$.

a_{00}, a_{nj}'s($n=1,2,\ldots;j=0,1,\ldots$) and b_n's($n=0,1,\ldots$) satisfy the equations such that

$$N:=a_{11}^2+\ldots+a_{17}^2 \quad \bmod q$$

$$a_{00}:=1,\ b_0:=0,\ b_1:=1,$$

$$a_{n0}=a_{n-1,0}\,a_{10}-b_{n-1}N \bmod q,\ (n=1,2,\ldots), \tag{8}$$

$$b_n=a_{n-1,0}+b_{n-1}a_{10} \bmod q,\ (n=1,2,\ldots), \tag{9}$$

$$a_{nj}=b_na_{1j} \bmod q,\ (n=1,2,\ldots;j=1,2,\ldots,7). \tag{10}$$

(*Proof*:)

Here proof is omitted and can be looked up in the **Appendix B**.

Theorem 2

For an element $A=(a_{10},a_{11},\ldots,a_{17})\in O$,

$$A^{J+1}=A \bmod q,$$

where

$$J=\mathrm{LCM}\{q^2-1,\ q-1\}=q^2-1,$$

$$N:=a_{11}^2+a_{12}^2+\ldots+a_{17}^2\neq 0 \bmod q.$$

(*Proof*:)

Here proof is omitted and can be looked up in the **Appendix C.**

§2.3. Property of multiplication over octonion ring *O*

A,B,C etc.$\in O$ satisfy the following formulae in general where A,B and C have the inverse A^{-1} ,B^{-1} and C^{-1} mod q.

1) Non-commutative

$$AB \neq BA \quad \text{mod } q.$$

2) Non-associative

$$A(BC) \neq (AB)C \quad \text{mod } q.$$

3) Alternative

$$(AA)B=A(AB) \quad \text{mod } q, \tag{11}$$

$$A(BB)=(AB)B \quad \text{mod } q, \tag{12}$$

$$(AB)A=A(BA) \quad \text{mod } q. \tag{13}$$

4) Moufang's formulae [16],

$$C(A(CB))=((CA)C)B \quad \text{mod } q, \tag{14}$$

$$A(C(BC))=((AC)B)C \quad \text{mod } q, \tag{15}$$

$$(CA)(BC)=(C(AB))C \quad \text{mod } q, \tag{16}$$

$$(CA)(BC)=C((AB)C) \quad \text{mod } q. \tag{17}$$

5) For positive integers n,m, we have

$$(AB)B^n =((AB)B^{n-1})B=A(B(B^{n-1}B))=AB^{n+1} \quad \text{mod } q, \tag{18}$$

$$(AB^{n})B =((AB)B^{n-1})B=A(B(B^{n-1}B))=AB^{n+1} \quad \text{mod } q , \tag{19}$$

$$B^n (BA) =B(B^{n-1}(BA))= ((BB^{n-1})B)A=B^{n+1}A \quad \text{mod } q , \tag{20}$$

$$B(B^n A)=B(B^{n-1}(BA))= ((BB^{n-1})B)A=B^{n+1}A \quad \text{mod } q. \tag{21}$$

From (12) and (19), we have

$$[(AB^n)B]B =[AB^{n+1}]B \quad \text{mod } q,$$

$$(AB^n)(BB) =[(AB^n)B]B =[AB^{n+1}]B= AB^{n+2} \quad \text{mod } q,$$

$$(AB^n)B^2= AB^{n+2} \quad \text{mod } q,$$

$$\cdots \qquad \cdots$$

$$(AB^n)B^m= AB^{n+m} \quad \text{mod } q.$$

In the same way we have

$$B^m(B^n A)= B^{n+m}A \quad \text{mod } q.$$

6) **Lemma 1**

$$A(B((AB)^n))=(AB)^{n+1} \quad \text{mod } q,$$

$$(((AB)^n)A)B =(AB)^{n+1} \quad \text{mod } q\,.$$

where n is a positive integer and B has the inverse B^{-1}.

(*Proof*:)

From (14) we have

$$B(A(B((AB)^n)=\mathbf{(}(BA)B\mathbf{)}(AB)^n=\mathbf{(}B(AB)\mathbf{)}(AB)^n=B(AB)^{n+1} \quad \text{mod } q.$$

Then

$$B^{-1}(B(A(B(AB)^n))= B^{-1}(B\,(AB)^{n+1}) \quad \text{mod } q,$$

$$A(B(AB)^n)= (AB)^{n+1} \quad \text{mod } q.$$

In the same way we have

$$(((AB)^n)A)B=(AB)^{n+1} \quad \text{mod } q. \qquad\qquad \text{q.e.d.}$$

7) **Lemma 2**

$$A^{-1}(AB)= B \text{ mod } q,$$

$$(BA)A^{-1}= B \text{ mod } q\,.$$

(*Proof*:)

Here proof is omitted and can be looked up in the **Appendix D**.

8) **Lemma 3**

$$A(BA^{-1})= (AB)A^{-1} \text{ mod } q.$$

(*Proof*:)

From (17) we substitute A^{-1} to C, we have

$$(A^{-1}A)(B\,A^{-1})= A^{-1}\,((AB)\,A^{-1}) \text{ mod } q,$$

$$(B\,A^{-1})= A^{-1}\,((AB)\,A^{-1}) \text{ mod } q.$$

We multiply A from left side ,

$$A(B\,A^{-1})= A(A^{-1}\,((AB)\,A^{-1}))= (AB)\,A^{-1} \bmod q. \qquad \text{q.e.d.}$$

We can express $A(BA^{-1})$, $(AB)A^{-1}$ such that

$$ABA^{-1}.$$

9) From (13) and Lemma 2 we have

$$A^{-1}((A(BA^{-1}))A)= A^{-1}(A((BA^{-1})A))= (BA^{-1})A=B \bmod q,$$

$$(A^{-1}((AB)A^{-1}))A=((A^{-1}(AB))A^{-1})A= A^{-1}(AB)=B \bmod q\,.$$

10) **Lemma 4**

$$(BA^{-1})(AB)=B^2 \bmod q\,.$$

(*Proof*:)

From (17),

$$(BA^{-1})(AB)=B((A^{-1}A)B)=B^2 \bmod q. \qquad \text{q.e.d.}$$

11a) **Lemma 5a**

$$(ABA^{-1})(\,ABA^{-1}\,)= AB^2A^{-1} \bmod q.$$

(*Proof*:)

From (17),

$$(ABA^{-1})(\,ABA^{-1}\,) \quad \bmod q$$

$$=[A^{-1}\,(A^2(BA^{-1}))][(AB)A^{-1}]= A^{-1}\,\{[(A^2(BA^{-1}))(AB)]A^{-1}\} \quad \bmod q$$

$$= A^{-1}\,\{[(A(A(BA^{-1})))(AB)]A^{-1}\} \quad \bmod q$$

$$= A^{-1}\,\{[(A((AB)A^{-1}))(AB)]A^{-1}\} \quad \bmod q$$

$$= A^{-1}\,\{[(A(AB))A^{-1}))(AB)]A^{-1}\} \quad \bmod q.$$

We apply (15) to inside of [.],

$$= A^{-1}\,\{[(A((AB)(A^{-1}(AB)))]A^{-1}\} \quad \bmod q$$

$$= A^{-1}\,\{[(A((AB)B))]A^{-1}\} \quad \bmod q$$

$$= A^{-1}\,\{[A(A(BB))]A^{-1}\} \quad \bmod q$$

$$=\{\,A^{-1}\,[A(A(BB))]\}A^{-1} \quad \bmod q$$

$$=(A(BB))A^{-1} \mod q$$

$$=AB^2A^{-1} \mod q. \qquad \text{q.e.d.}$$

11b) **Lemma 5b**

$$[A_1(\ldots(A_rBA_r^{-1})\ldots)A_1^{-1}]\,[A_1(\ldots(A_rBA_r^{-1})\ldots)A_1^{-1}]$$

$$= A_1(\ldots(A_rB^2A_r^{-1})\ldots)A_1^{-1} \mod q.$$

where

$$A_i \in O \text{ has the inverse } A_i^{-1} \mod q \ (i=1,\ldots,r).$$

(*Proof*:)

As we use Lemma 5a repeatedly we have

$$\{A_1(\,[A_2(\ldots(A_rBA_r^{-1})\ldots)A_2^{-1}]\,)A_1^{-1}\,\}\{A_1(\,[A_2(\ldots(A_rBA_r^{-1})\ldots)A_2^{-1}]\,)A_1^{-1}\,\} \mod q$$

$$=A_1(\,[A_2(\ldots(A_rBA_r^{-1})\ldots)A_2^{-1}]\,[A_2(\ldots(A_rBA_r^{-1})\ldots)A_2^{-1}]\,)A_1^{-1} \mod q$$

$$=A_1(A_2([A_3(\ldots(A_rBA_r^{-1})\ldots)A_3^{-1}][A_3(\ldots(A_rBA_r^{-1})\ldots)A_3^{-1})A_2^{-1}]\,)A_1^{-1} \mod q$$

$$\ldots \qquad \ldots$$

$$= A_1(A_2(\ldots([A_rBA_r^{-1}]\,[A_rBA_r^{-1}])\ldots)A_2^{-1})A_1^{-1} \mod q$$

$$= A_1(A_2(\ldots(A_rB^2A_r^{-1})\ldots)A_2^{-1})A_1^{-1} \mod q$$

q.e.d.

11c) **Lemma 5c**

$$A_1^{-1}\,(A_1BA_1^{-1})\,A_1$$

$$= B \mod q.$$

where

$$A_1 \in O \text{ has the inverse } A_1^{-1} \mod q.$$

(*Proof*:)

$$A_1^{-1}\,(A_1BA_1^{-1})\,A_1 = A_1^{-1}\,[((A_1B)A_1^{-1})\,A_1] \mod q,$$

From Lemma 2 we have

$$= A_1^{-1}\,(A_1B) = B \mod q. \qquad \text{q.e.d.}$$

11d) **Lemma 5d**

$$A_r^{-1}(\ldots(A_1^{-1}[A_1(\ldots(A_rBA_r^{-1})\ldots)A_1^{-1}]A_1)\ldots)A_r$$
$$= B \bmod q.$$

where

$$A_i \in O \text{ has the inverse } A_i^{-1} \bmod q \ (i=1,\ldots,r).$$

(*Proof*:)

As we use Lemma 5c repeatedly we have

$$A_r^{-1}(\ldots(A_1^{-1}[A_1(\ldots(A_rBA_r^{-1})\ldots)A_1^{-1}]A_1)\ldots)A_r$$
$$= A_r^{-1}(\ldots(A_2^{-1}[A_2(\ldots(A_rBA_r^{-1})\ldots)A_2^{-1}]A_2)\ldots)A_r \bmod q$$
$$\ldots \qquad \ldots$$
$$= A_r^{-1}[A_rBA_r^{-1}]A_r \bmod q$$
$$=B \bmod q \qquad \text{q.e.d.}$$

12) **Lemma 6**

$$(AB^mA^{-1})(AB^nA^{-1}) = AB^{m+n}A^{-1} \quad \bmod q.$$

(*Proof*:)

From (16),

$$[A^{-1}(A^2(B^mA^{-1}))][(AB^n)A^{-1}] = \{A^{-1}[(A^2(B^mA^{-1}))(AB^n)]\}A^{-1} \quad \bmod q$$
$$= A^{-1}\{[(A(A(B^mA^{-1}))(AB^n)]A^{-1}\} \quad \bmod q$$
$$= A^{-1}\{[(A((AB^m)A^{-1}))(AB^n)]A^{-1}\} \quad \bmod q$$
$$= A^{-1}\{[((A(AB^m))A^{-1}))(AB^n)]A^{-1}\} \quad \bmod q$$
$$= A^{-1}\{[((A^2B^m)A^{-1}))(AB^n)]A^{-1}\} \quad \bmod q.$$

We apply (15) to inside of { . },

$$= A^{-1}\{(A^2B^m)[A^{-1}((AB^n)A^{-1})]\} \quad \bmod q$$
$$= A^{-1}\{(A^2B^m)[A^{-1}(A(B^nA^{-1}))]\} \quad \bmod q$$
$$= A^{-1}\{(A^2B^m)(B^nA^{-1})\} \quad \bmod q$$
$$= A^{-1}\{(A^{-1}(A^3B^m))(B^nA^{-1})\} \quad \bmod q.$$

We apply (17) to inside of { . },

$$= A^{-1}\{A^{-1}([(A^3B^m)B^n]A^{-1})]\} \mod q$$

$$= A^{-1}\{A^{-1}((A^3B^{m+n})A^{-1})\} \mod q$$

$$= A^{-1}\{(A^{-1}(A^3B^{m+n}))A^{-1}\} \mod q$$

$$= A^{-1}\{(A^2B^{m+n})A^{-1}\} \mod q$$

$$=\{A^{-1}(A^2B^{m+n}))\}A^{-1} \mod q$$

$$=(AB^{m+n})A^{-1} \mod q$$

$$=AB^{m+n}A^{-1} \mod q.$$ q.e.d

13) $A \in O$ satisfies the following theorem.

Theorem 3

$$A^2=w\mathbf{1}+vA \mod q,$$

where

$$^{\exists}w,v \in Fq,$$

$$\mathbf{1}=(1,0,0,0,0,0,0,0) \in O,$$

$$A=(a_0,a_1,\ldots,a_7) \in O.$$

(*Proof*:)

$$A^2 \mod q$$

$$\begin{aligned}
=(\quad & a_0a_0-a_1a_1-a_2a_2-a_3a_3-a_4a_4-a_5a_5-a_6a_6-a_7a_7 \mod q,\\
& a_0a_1+a_1a_0+a_2a_4+a_3a_7-a_4a_2+a_5a_6-a_6a_5-a_7a_3 \mod q,\\
& a_0a_2-a_1a_4+a_2a_0+a_3a_5+a_4a_1-a_5a_3+a_6a_7-a_7a_6 \mod q,\\
& a_0a_3-a_1a_7-a_2a_5+a_3a_0+a_4a_6+a_5a_2-a_6a_4+a_7a_1 \mod q,\\
& a_0a_4+a_1a_2-a_2a_1-a_3a_6+a_4a_0+a_5a_7+a_6a_3-a_7a_5 \mod q,\\
& a_0a_5-a_1a_6+a_2a_3-a_3a_2-a_4a_7+a_5a_0+a_6a_1+a_7a_4 \mod q,\\
& a_0a_6+a_1a_5-a_2a_7+a_3a_4-a_4a_3-a_5a_1+a_6a_0+a_7a_2 \mod q,\\
& a_0a_7+a_1a_3+a_2a_6-a_3a_1+a_4a_5-a_5a_4-a_6a_2+a_7a_0 \mod q)
\end{aligned}$$

$$=(2a_0^2 - L \bmod q,\ 2a_0a_1 \bmod q,\ 2a_0a_2 \bmod q,\ 2a_0a_3 \bmod q,\ 2a_0a_4 \bmod q,\ 2a_0a_5 \bmod q,$$
$$2a_0a_6 \bmod q,\ 2a_0a_7 \bmod q)$$

where

$$\mathrm{L}= a_0^2+a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2 \bmod q.$$

Now we try to obtain $u, v \in Fq$ that satisfy $A^2=w\mathbf{1}+vA \bmod q$.

$$w\mathbf{1}+vA= w(1,0,0,0,0,0,0,0)+v(a_0,a_1,\ldots,a_7) \bmod q,$$
$$A^2= (2a_0^2 - L \bmod q,\ 2a_0a_1 \bmod q,\ 2a_0a_2 \bmod q,\ 2a_0a_3 \bmod q,\ 2a_0a_4 \bmod q,$$
$$2\ a_0a_5 \bmod q, 2a_0a_6 \bmod q,\ 2a_0a_7 \bmod q).$$

Then we have

$$A^2=w\mathbf{1}+vA=-L\mathbf{1}+2\ a_0A \bmod q,$$
$$w= -L \bmod q,$$
$$\mathrm{v}=2a_0 \bmod q. \qquad\qquad \text{q.e.d.}$$

14) **Theorem 4**

$$A^h=w_h\mathbf{1}+v_hA \bmod q$$

where h is an integer and $w_h,v_h \in Fq$.

(*Proof*:)

From Theorem 3

$$A^2=w_2\mathbf{1}+v_2A=-L\mathbf{1}+2a_0A \bmod q.$$

If we can express A^h such that

$$A^h=w_h\mathbf{1}+v_hA \bmod q \in O\ ,\ w_h,v_h \in Fq,$$

Then

$$A^{h+1}=(w_h\mathbf{1}+v_hA)A \bmod q$$
$$=w_hA+v_h(-L\mathbf{1}+2\ a_0A\ ) \bmod q$$
$$=-Lv_h\mathbf{1}+(\ w_h+2a_0\mathrm{v}_\mathrm{h})A \bmod q.$$

We have

$$w_{\mathrm{h}+1}= -L\ v_h \bmod q \in Fq,$$

$$v_{h+1}= w_h+2a_0v_h \mod q\in Fq. \qquad \text{q.e.d.}$$

15) **Theorem 5**

$D\in O$ does not exist that satisfies the following equation.

$$B(AX)=DX \bmod q\ ,$$

where $B,A,D\in O$, and X is a variable.

(*Proof*:)

When $X=\mathbf{1}$, we have

$$BA=D \bmod q.$$

Then

$$B(AX)=(BA)X \bmod q.$$

We can select $C\in O$ that satisfies

$$B(AC)\neq(BA)C \bmod q. \tag{22}$$

We substitute $C\in O$ to X to obtain

$$B(AC)=(BA)C \bmod q. \tag{23}$$

(23) is contradictory to (22). q.e.d.

16) **Theorem 6**

$D\in O$ does not exist that satisfies the following equation.

$$C(B(AX))=DX \bmod q \tag{24}$$

where $C,B,A,D\in O$, C has inverse C^{-1} mod q and X is a variable.

B,A,C are non-associative, that is,

$$B(AC)\neq(BA)C \bmod q. \tag{25}$$

(*Proof*:)

If D exists, we have at $X=\mathbf{1}$

$$C(BA)=D \bmod q.$$

Then

$$C(B(AX))=(C(BA))X \bmod q.$$

We substitute C to X to obtain

$$C(B(AC))=(C(BA))C \bmod q.$$

From (13)

$$C(B(AC))=(C(BA))C=C((BA)C) \bmod q$$

Multiplying C^{-1} from left side ,

$$B(AC)=(BA)C \bmod q \qquad (26)$$

(26) is contradictory to (25). q.e.d.

17) **Theorem 7**

D and $E \in O$ do not exist that satisfy the following equation.

$$C(B(AX))= E\,(DX) \bmod q$$

where C,B,A,D and $E \in O$ have inverse and X is a variable.

A,B,C are non-associative, that is,

$$C(BA) \neq (CB)A \bmod q. \qquad (27)$$

(*Proof*:)

If D and E exist, we have at $X=\mathbf{1}$

$$C(BA)=ED \bmod q \qquad (28)$$

We have at $X=(ED)^{-1}=D^{-1}E^{-1} \bmod q$.

$$C(B(\mathrm{A}(D^{-1}E^{-1})))= E\,(D(D^{-1}E^{-1})) \bmod q=\mathbf{1},$$

$$(C(B(A(D^{-1}E^{-1})))^{-1} \bmod q=\mathbf{1},$$

$$((ED)A^{-1})B^{-1})C^{-1} \bmod q=\mathbf{1},$$

$$ED =(CB)A \bmod q. \qquad (29)$$

From (28) and (29) we have

$$C(BA) =(CB)A \bmod q. \qquad (30)$$

(30) is contradictory to (27). q.e.d.

18) **Theorem 8**

$D \in O$ does not exist that satisfies the following equation.

$$A(B(A^{-1}X))=DX \bmod q$$

where $B,A,D \in O$, A has inverse A^{-1} mod q and X is a variable.

(*Proof*:)

If D exists, we have at $X=\mathbf{1}$

$$A(BA^{-1})=D \bmod q.$$

Then

$$A\,(B(A^{-1}X))=(A(BA^{-1}))X \bmod q. \qquad (31)$$

We can select $C \in O$ such that

$$(BA^{-1})(CA^2) \neq (BA^{-1})C)A^2 \bmod q. \qquad (32)$$

That is, (BA^{-1}), C and A^2 are non-associative.

Substituing $X=CA$ in (31), we have

$$A\,(B(A^{-1}(CA)))=(A(BA^{-1}))(CA) \bmod q.$$

From Lemma 3

$$A\,(B((A^{-1}C)A)))=(A(BA^{-1}))(CA) \bmod q.$$

From (17)

$$A\,(B((A^{-1}C)A)))=A([(BA^{-1})C]A) \bmod q.$$

Multiply A^{-1} from left side we have

$$B((A^{-1}C)A))= ((BA^{-1})C)A \bmod q.$$

From Lemma 3

$$B(A^{-1}(CA))=((BA^{-1})C)A \bmod q.$$

Transforming CA to $((CA^2)A^{-1})$, we have

$$B(A^{-1}((CA^2)A^{-1}))=((BA^{-1})C)A \bmod q.$$

From (15) we have

$$((BA^{-1})(CA^{2}))A^{-1}=((BA^{-1})C)A \bmod q.$$

Multiply A from right side we have

$$((BA^{-1})(CA^{2})=((BA^{-1})C)A^{2} \bmod q. \tag{33}$$

(33) is contradictory to (32). q.e.d.

§3. Concept of proposed fully homomorphic encryption scheme

Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on ciphertext and obtain an encrypted result which decrypted matches the result of operations performed on the plaintext. For instance, one person could add two encrypted numbers and then another person could decrypt the result, without either of them being able to find the value of the individual numbers.

§3.1 Definition of homomorphic encryption

A homomorphic encryption scheme **HE** := (**KeyGen; Enc; Dec; Eval**) is a quadruple of PPT (Probabilistic polynomial time) algorithms.

In this work, the medium text space M_e of the encryption schemes will be octonion ring, and the functions to be evaluated will be represented as arithmetic circuits over this ring, composed of addition and multiplication gates. The syntax of these algorithms is given as follows.

-Key-Generation. The algorithm **KeyGen**, on input the security parameter 1^{λ}, outputs (**sk**) ← **KeyGen**(1^{λ}) , where **sk** is a secret encryption/decryption key.

-Encryption. The algorithm **Enc**, on input system parameter q, secret keys(**sk**) and a plaintext $u \in Fq$, outputs a ciphertext C ←**Enc**(**sk**; u).

-Decryption. The algorithm **Dec**, on input system parameter q, secret key(**sk**) and a ciphertext C, outputs a plaintext u^*←**Dec**(**sk**;C).

-Homomorphic-Evaluation. The algorithm **Eval**, on input system parameter q, an arithmetic circuit ckt, and a tuple of n ciphertexts ($C_1,\ldots, C_n$),
outputs a ciphertext C' ←**Eval**(ckt; $C_1,\ldots, C_n$).

The security notion needed in this scheme is security against chosen plaintext attacks (**IND-CPA** security), defined as follows.

Definition 1 (**IND-CPA security**). A scheme HE is **IND-CPA** secure if for any PPT adversary A_d it holds that:

$$\mathrm{Adv}^{\mathrm{CPA}}_{\mathrm{HE}}[\lambda] := |\Pr[A_d(\mathbf{Enc}(\mathbf{sk};0)) = 1] - \Pr[A_d(\mathbf{Enc}(\mathbf{sk};1)) = 1]| = \mathrm{negl}(\lambda)$$

where $(\mathbf{sk}) \leftarrow \mathbf{KeyGen}(1^\lambda)$.

§3.2 Definition of fully homomorphic encryption

A scheme HE is fully homomorphic if it is both compact and homomorphic with respect to a class of circuits. More formally:

Definition 2 (**Fully homomorphic encryption**). A homomorphic encryption scheme FHE :=(**KeyGen; Enc; Dec; Eval**) is fully homomorphic if it satisfies the following properties:

1. Homomorphism: Let $CR = \{CR_\lambda\}_{\lambda\in N}$ be the set of all polynomial sized arithmetic circuits. On input $\mathbf{sk} \leftarrow \mathbf{KeyGen}(1^\lambda)$, $\forall$ ckt $\in CR_\lambda$, $\forall (u_1,\dots, u_n) \in Fq^n$ where $n = n(\lambda)$, $\forall (C_1,\dots,C_n)$

   where $C_i \leftarrow \mathbf{Enc}(\mathbf{sk};u_i$, it holds that:

$$\Pr[\mathbf{Dec}(\mathbf{sk};\mathbf{Eval}(\mathrm{ckt}; C_1,\dots,C_n)) \neq \mathrm{ckt}(u_1,\dots, u_n)] = \mathrm{negl}(\lambda).$$

2. Compactness: There exists a polynomial $\mu = \mu(\lambda)$ such that the output length of **Eval** is at most μ bits long regardless of the input circuit ckt and the number of its inputs.

§3.3 Proposed fully homomorphic enciphering/deciphering functions

We propose a fully homomorphic encryption (FHE) scheme based on the enciphering/deciphering functions on octonion ring over ***Fq***.

First we define the medium text M as follows.

We select the element $B=(b_0,b_1,\dots,b_7)$ and $H=(b_0,-b_1,\dots,-b_7)\in O$ such that,

$$L_B:=|B|^2= b_0^2+b_1^2+\dots+b_7^2 \bmod q=0,$$

$$b_0\neq 1 \bmod q,$$

$$b_1\neq 0 \bmod q.$$

Then we have

$$L_H:=|H|^2= b_0^2+b_1^2+\dots+b_7^2 \bmod q=0,$$

$$B+H=2b_0\mathbf{1} \bmod q,$$

$$B^2=2\,b_0B \bmod q,$$

$$H^2=2\,b_0H \bmod q,$$

$$BH=HB=\mathbf{0} \bmod q.$$

Let $u\in \boldsymbol{Fq}$ be a plaintext to belong to the set of the plaintext $P=\{u \mid u\in \boldsymbol{Fq}\}$.

Let v and $w\in \boldsymbol{Fq}$ be the random numbers.

We define the medium text M by

$$M:= R_1(\ldots(R_r(u\mathbf{1}+vB+w\,H)R_r^{-1})\ldots)R_1^{-1}\in O,$$

and

$$|M\,|^2=(u+v\,b_0+w\,b_0)^2+(v\text{-}w)/^2(b_1^{\,2}+\ldots+b_7^{\,2})\neq 0 \bmod q$$

where

$$u+v+w=T\in Fq\text{:secret constant parameter},$$

$$R_i\in O \quad \text{such that } R_i^{-1} \text{ exists } (i=1,\ldots,r) \text{ and}$$

$$R_iB\neq BR_i \bmod q(i=1,\ldots,r),$$

$$R_iH\neq H_i \bmod q(i=1,\ldots,r).$$

Then

$$u^2+2b_0(v+w)u+4b_0^{\,2}vw+(v\text{-}w)^2(b_0^{\,2}+b_1^{\,2}+\ldots+b_7^{\,2})\neq 0 \bmod q,$$

$$(u+2\,b_0v)(u+2\,b_0w)\neq 0 \bmod q,$$

We have

$$u+2\,b_0v\neq 0 \bmod q$$

and

$$u+2\,b_0w\neq 0 \bmod q.$$

Here we simplify the expression of medium text M such that

$$M:= R(u\mathbf{1}+vB+w\,H)R^{-1}\in O,$$

Let

$$M_1:=R(u_1\mathbf{1}+v_1B+w_1H)R^{-1}\in O,$$

$$M_2 := R(u_2\mathbf{1}+v_2B+w_2H)R^{-1} \in O,$$

We have

$$M_1M_2 = [R\,(u_1\mathbf{1}+v_1B+w_1H)R^{-1}][R(u_2\mathbf{1}+v_2B+w_2H)R^{-1}]$$

$= R\,[(u_1 u_2)\mathbf{1}+(u_1 v_2+ v_1 u_2+2\,b_0\,v_1\,v_2)B+(u_1w_2+ w_1 u_2+ 2\,b_0w_1w_2)H]\,R^{-1}$

$=M_2M_1 \bmod q$.

We show the reason as follows by using Lemma 5b.

$[R\,BR^{-1}][RBR^{-1}]= RB^2R^{-1}= 2\,b_0RBR^{-1} \bmod q,$

$[R\,HR^{-1}][RHR^{-1}]= RH^2R^{-1}=2\,b_0\,RHR^{-1} \bmod q,$

and

$[R\,(B+H)R^{-1}] =[R\,B\,R^{-1}+ R\,HR^{-1}] =2\,b_0\mathbf{1} \bmod q$**.**

We multiply $[R\,BR^{-1}]$ from right side, we have

$[R\,B\,R^{-1}+ R\,HR^{-1}]\,[R\,BR^{-1}]= 2\,b_0\mathbf{1}[R\,BR^{-1}]= 2\,b_0\,[R\,BR^{-1}] \bmod q,$

$2\,b_0\,[R\,B\,R^{-1}]+ [R\,HR^{-1}]\,[R\,BR^{-1}] = 2\,b_0\,[R\,BR^{-1}] \bmod q.$

Then

$[R\,HR^{-1}][RBR^{-1}]= \mathbf{0} \bmod q.$

In the same manner we have

$[R\,BR^{-1}][RHR^{-1}]= \mathbf{0} \bmod q.$

We have shown that we can obtain the multiple of u_1 and u_2 from M_1M_2.

Here I define the some parameters for describing FHE.

Let q be a prime more than 2.

Let $M=(m_0,m_1,\ldots,m_7)=R(u\mathbf{1}+vB+w\,H)R^{-1}\in O$ be the medium plaintext.

Let $X=(x_0,\ldots,x_7)\ \in O[X]$ be a variable.

Let $E(u,X)$ and $D(X)$ be a enciphering and a deciphering function of user A.

Let $C(X)=E(u,X)\in O[X]$ be the ciphertext.

A_i , $Z_i\in O$ is selected randomly such that A_i^{-1} and Z_i^{-1} exist (i=1,...,k) which are the secret keys of user A.

Enciphering function $C(X)=E(u,X)$ is defined as follows.

$C(X)=E(u,X):=$

$$(A_1((\ldots((A_k(M[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\,Z_1^{-1} \bmod q\in O[X] \qquad (34)$$

$$\begin{aligned}
=(\,& e_{00}x_0+e_{01}x_1+\ldots+e_{07}x_7,\\
& e_{10}x_0+e_{11}x_1+\ldots+e_{17}\,x_7,\\
& \quad\ldots.\qquad \ldots.\\
& e_{70}x_0+e_{71}x_1+\ldots+e_{77}\,x_7),
\end{aligned} \qquad (35)$$

$$= \{e_{ij}\}(i,j=0,\ldots,7) \qquad (36)$$

with $e_{ij} \in \boldsymbol{Fq}$ $(i,j=0,\ldots,7)$ which is published in cloud centre.
Here we notice how to construct enciphering function.
We show a part of process for constructing enciphering function $E(u,X)$ as follows.

$$A_1^{-1}X$$
$$(A_1^{-1}X)Z_1$$
$$A_2^{-1}((A_1^{-1}X)Z_1)$$
$$(A_2^{-1}((A_1^{-1}X)Z_1))Z_2$$
$$\ldots$$
$$(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k$$
$$M[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]$$
$$A_k(M[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k])$$
$$(A_k(M[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}$$
$$\ldots$$
$$(A_1((\ldots((A_k(M[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))Z_1^{-1}$$

Let D be the deciphering function defined as follows .

$$G_1(X):=A_k^{-1}((\ldots((A_1^{-1}(X Z_1))\ldots))Z_k), \qquad (37)$$

$$G_2(X):=A_1((\ldots((A_k(X Z_k^{-1}))\ldots)) Z_1^{-1}), \qquad (38)$$

$$D(X):= G_1(C(G_2(X)) \bmod q=MX. \qquad (39)$$

$D(\mathbf{1})=M=(m_0,m_1,\ldots,m_7)=R_1(\ldots(R_r(u\mathbf{1}+vB+w H)R_r^{-1})\ldots)R_1^{-1}$

$=R[u\mathbf{1}+vB+wH]R^{-1}= R[u\mathbf{1}+v(b_0,b_1,\ldots,b_7)+w(b_0,-b_1,\ldots,-b_7)]R^{-1}$.

Then we obtain the plaintext u as follows.

Let $(m_0',m_1',\ldots,m_7'):= R^{-1}(m_0,m_1,\ldots,m_7)R \bmod q$

$= R_r^{-1}(\ldots(R_1^{-1}(m_0,m_1,\ldots,m_7)R_1)\ldots)R_r \bmod q$.

By solving the following equations, we have the plaintext u.

$$u + (b_0v+b_0w) = m_0' \bmod q,\ldots\ldots..(a)$$

$$v\text{-}w = m_1' / b_1 \bmod q\ldots\ldots\ldots\ldots\ldots(b)$$

$$u + v+w =T \bmod q\ldots\ldots\ldots\ldots\ldots(c)$$

From (a),(b),(c) we obtain u such that

$$u = (m_0'-Tb_0)/(1- b_0) \bmod q.$$

§3.4 Elements on octonion ring assumption EOR($k,r,n;q$)

Here we describe the assumption on which the proposed scheme bases.

Elements on octonion ring assumption EOR($k,n;q$).

Let q be a prime more than 2. Let k ,r and n be integer parameters. Let $\boldsymbol{A}:=(A_1,\ldots,A_k)\in O^k$, $\boldsymbol{Z}:=(Z_1,\ldots,Z_k)\in O^k$,$\boldsymbol{R}:=(R_1,\ldots,R_r)\in O^r$.Let $C_i(X):=E(u_i\ ,X)=(A_1((\ldots((A_k(M_i\ [(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\ Z_1^{-1} \bmod q\in O[X]$ where medium text $M_i=(m_{i0},\ldots,m_{i7}):=R_1(\ldots(R_r(u_i\mathbf{1}+v_iB+w_iH)R_r^{-1})\ldots)R_1^{-1}\in O$, plaintext u_i (i=1,…,n), X is a variable.

In the **EOR**($k,r,n;q$) assumption, the adversary $\mathrm{A_d}$ is given $C_i(X)$ (i=1,…,n) randomly and his goal is to find a set of elements $\boldsymbol{A}=(A_1,\ldots,A_k)\in O^k$, $\boldsymbol{Z}=(Z_1,\ldots,Z_k)\in O^k$,$\boldsymbol{R}=(R_1,\ldots,R_r)\in O^r$, with the order of the elements $A_1,\ldots, A_k$, $Z_1,\ldots,Z_k, R_1,\ldots,R_r$ and plaintexts u_i(i=1,…,n). For parameters $k = k(\lambda)$, $r = r(\lambda)$ and n=$n(\lambda)$ defined in terms of the security parameter λ and for any PPT adversary $\mathrm{A_d}$ we have

$$\Pr\left[(A_1((\ldots((A_k(M_i[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\ Z_1^{-1} \bmod q = C_i(X)\ (i=1,\ldots,n) : \boldsymbol{A}=(A_1,\ldots, A_k),\ M_i(i=1,\ldots,n)\leftarrow \mathrm{A_d}\ (1^\lambda, C_i(X)\ (i=1,\ldots,n))\right]= \mathrm{negl}(\lambda).$$

To solve directly **EOR**($k,r,n;q$) assumption is known to be the problem for solving the multivariate algebraic equations of high degree which is known to be NP-hard.

§3.5 Syntax of proposed algorithms

The syntax of proposed scheme is given as follows.

-Key-Generation. The algorithm **KeyGen**, on input the security parameter 1^λ and system parameter q, outputs **sk**=($\boldsymbol{A},\boldsymbol{Z},\boldsymbol{R},B,H$)←**KeyGen**($1^\lambda$), where **sk** is a secret encryption /dencryption key.

-Encryption. The algorithm **Enc**, on input system parameter q, and secret keys **sk**=($\boldsymbol{A},\boldsymbol{Z},\boldsymbol{R},B,H$) and a plaintext $u\in \boldsymbol{Fq}$, outputs a ciphertext $\boldsymbol{C}(X$;**sk**,u)←**Enc**(**sk**;u).

-Decryption. The algorithm **Dec**, on input system parameter q, secret keys **sk** and a ciphertext $\boldsymbol{C}(X$;**sk**,u), outputs plaintext **Dec**(**sk**; $\boldsymbol{C}(X$;**sk**,u)) where $\boldsymbol{C}(X$;**sk**,u) ←**Enc**(**sk**; u).

-Homomorphic-Evaluation. The algorithm **Eval**, on input system parameter q, an arithmetic circuit ckt, and a tuple of n ciphertexts ($C_1,\ldots, C_n$), outputs an evaluated ciphertext C'←**Eval**(ckt; $C_1,\ldots, C_n$) where C_i= $\boldsymbol{C}(X$;**sk**,u_i) (i=1,…,n).

Theorem 9

For any $u,u' \in O$,

if $E(u, X)= E(u', X) \bmod q$, then $u= u' \bmod q$.

That is , if $u \neq u' \bmod q$, then $E(u, X) \neq E(u', X) \bmod q$.

(*Proof*)

If E $E(u, X)= E(u', X) \bmod q$, then

$$G_1(E(u, (G_2(X))= G_1(E(u', (G_2(X)) \bmod q$$

$$MX=M'X \bmod q$$

where

$$M=R_1(\ldots(R_r(u\mathbf{1}+vB+w H)R_r^{-1})\ldots)R_1^{-1} \bmod q,$$

$$M'=R_1(\ldots(R_r(u'\mathbf{1}+v'B+w'H)R_r^{-1})\ldots)R_1^{-1} \bmod q.$$

We substitute **1** to X in above expression, we obtain

$$M =M' \bmod q.$$

$$R_1(\ldots(R_r(u\mathbf{1}+vB+w H)R_r^{-1})\ldots)R_1^{-1}= R_1(\ldots(R_r(u'\mathbf{1}+v'B+w'H)R_r^{-1})\ldots)R_1^{-1} \bmod q$$

$$u\mathbf{1}+vB+w H= u'\mathbf{1}+v'B+w'H \bmod q.$$

Then we have

$$u+(v+w)b_0= u'+(v'+w')b_0 \bmod q,$$

From the definition of T

$$u+v+w= u'+v'+w'=T.$$

$$u+(v+w)b_0-Tb_0= u'+(v'+w')b_0 -Tb_0 \bmod q,$$

$$u(1-b_0)= u' (1-b_0) \bmod q,$$

As $b_0 \neq 1 \bmod q$,

$$u=u' \bmod q . \qquad \text{q.e.d}$$

Next it is shown that the encrypting function $E(u,X)$ has the property of fully homomorphism.

We simply express above equation such that

$(A_1((\ldots((A_k(M[((A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k])Z_k^{-1}))\ldots))\ Z_1^{-1} \bmod q$

$=(\mathbf{A}(M[(\mathbf{A}^{-1}X)\mathbf{Z}]))\mathbf{Z}^{-1} \bmod q.$

§3.6 Addition/subtraction scheme on ciphertexts

Let $M_1:=R[u_1\mathbf{1}+v_1B+w_1H]R^{-1}$, $M_2:= R[u_2\mathbf{1}+v_2B+w_2H]R^{-1}\in O$ be medium texts to be encrypted
where

Let $C_1(X)= E(u_1, X)$ and $C_2(X)= E(u_2, X)$ be the ciphertexts.

$C_1(X)\pm C_2(X) \bmod q =E(u_1,X) \pm E(u_2,X) \bmod q$

$=(A_1((\ldots((A_k(M_1[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\, Z_1^{-1}$

$+(A_1((\ldots((A_k(M_2[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\, Z_1^{-1} \bmod q$

$=(A_1((\ldots((A_k([M_1 \pm M_2]\, [(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\, Z_1^{-1} \bmod q$

$=(A_1((\ldots((A_k([R(u_1\mathbf{1}+v_1B+w_1H\pm(u_2\mathbf{1}+v_2B+w_2H))R^{-1}]\quad [(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\, Z_1^{-1} \bmod q$

$=(A_1((\ldots((A_k([R((u_1\pm u_2)\mathbf{1}+(v_1\pm v_2)B+(w_1\pm w_2)H))R^{-1}]\quad [(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\, Z_1^{-1} \bmod q$

$= E(u_1\pm u_2,X) \bmod q.$

§3.7 Multiplication scheme on ciphertexts

§3.7.1 Multiplicative property of *B* and *H*

We consider multiplication of B and H where

$$B+H=2b_0\mathbf{1} \bmod q,$$

$$B^2=2\, b_0B \bmod q,$$

$$H^2=2\, b_0H \bmod q,$$

$$BH=HB=\mathbf{0} \bmod q.$$

For any $A\in O$, form (11) we have

$$(RBR^{-1})(\, (RBR^{-1})\, A) \bmod q$$

$$=(\, (RBR^{-1})\, (RBR^{-1}))\, A \bmod q$$

$$=(RB^2R^{-1})A \bmod q \quad \text{(From Lemma5a)}$$

$$= (2b_0)\, (RBR^{-1})A \bmod q \qquad (40a)$$

$$(RBR^{-1})(\ (RHR^{-1})\ A) \bmod q$$

$$=(\ (RBR^{-1})\ (R(2b_0\mathbf{1}\text{-}B)R^{-1}))\ A \bmod q$$

$$=(2b_0)\ (\ (RBR^{-1})\ (R\mathbf{1}R^{-1}))\ A\text{-}\ (\ (RBR^{-1})\ (RBR^{-1}))\ A \bmod q$$

$$=(2b_0)(RBR^{-1})\ A\text{-}\ (2b_0)(RBR^{-1})\ A \bmod q$$

$$=\mathbf{0} \bmod q \qquad (40b)$$

In the same manner we have

$$(RHR^{-1})(\ (RHR^{-1})\ A) \bmod q$$

$$=(2b_0)\ (RHR^{-1})A \bmod q \qquad (40c)$$

$$(RHR^{-1})(\ (RBR^{-1})\ A) = 0 \bmod q \qquad (40d)$$

§3.7.2 Multiplication of ciphertexts

Here we consider the multiplicative operation on the ciphertexts.

Let $C_1(X)= E(u_1, X)$ and $C_2(X)= E\ (u_2, X)$ be the ciphertexts.

$C_1(C_2(X)) \bmod q = E(u_1, E\ (u_2,X)) \bmod q$

$=(A_1((\ldots((A_k(M_1[(A_k^{-1}((\ldots((A_1^{-1}\{(A_1((\ldots((A_k(M_2[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))$
$Z_1^{-1}\ \})Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\ Z_1^{-1} \bmod q$

$=(A_1((\ldots((A_k(M_1[M_2[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]]))Z_k^{-1}))\ldots))\ Z_1^{-1} \bmod q$

$=(A_1((\ldots((A_k(M_1(M_2[((A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\ Z_1^{-1} \bmod q.$ (41)

$=(\boldsymbol{A}(M_1(M_2[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q.$

Substituting $R\ (u_1\mathbf{1}+v_1B+w_1H)\ R^{-1}$, $R\ (u_2\mathbf{1}+v_2B+w_2H)\ R^{-1}$ to M_1,M_2

we have from (40a)~(40d)

$=(\boldsymbol{A}(\ [R(u_1\mathbf{1}+v_1B+w_1H)R^{-1}]([R\ (u_2\mathbf{1}+v_2B+w_2H)\ R^{-1}]\ [(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q,$

$= (\boldsymbol{A}(\ [R\ (u_1\mathbf{1})\ R^{-1}]([R(u_2\mathbf{1}+v_2B+w_2H)\ R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q.$

$+ (\boldsymbol{A}(\ [R\ (v_1B)\ R^{-1}]\ ([R(u_2\mathbf{1}+v_2B+w_2H)\ R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$+ (\boldsymbol{A}(\ [R\ (w_1H)\ R^{-1}]\ ([R(u_2\mathbf{1}+v_2B+w_2H)\ R^{-1}]\ [(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}$ mod.

$= (\boldsymbol{A}(\ [R\ (u_1\mathbf{1})\ R^{-1}\ ]([R(u_2\mathbf{1})\ R^{-1}\ ][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q.$

$+ (\boldsymbol{A}([R\,(u_1\mathbf{1})\,R^{-1}]\,([R\,(v_2B)\,R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$+ (\boldsymbol{A}([R\,(u_1\mathbf{1})\,R^{-1}]\,([R\,(w_2H)\,R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$+ (\boldsymbol{A}([R\,(v_1B)\,R^{-1}]([\,R\,(u_2\mathbf{1})\,R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$+ (\boldsymbol{A}([R\,(v_1B)\,R^{-1}]([\,R\,(v_2B)\,R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$+ (\boldsymbol{A}([R\,(v_1B)\,R^{-1}]([\,R\,(w_2H)\,R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$+(\boldsymbol{A}([R\,(w_1H)\,R^{-1}]([\,R\,(u_2\mathbf{1})\,R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$+ (\boldsymbol{A}([R\,(w_1H)\,R^{-1}]([\,R\,(v_2B)\,R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$+ (\boldsymbol{A}([R\,(w_1H)\,R^{-1}]([\,R\,(w_2H)\,R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$= (\boldsymbol{A}([R\,(u_1u_2\mathbf{1}+ u_1v_2B + u_1w_2H+ v_1u_2B + v_1v_2BB + v_1w_2BH+$

$w_1u_2H + w_1v_2HB +w_1w_2HH)\,R^{-1}]\,[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-11} \bmod q$

$= (\boldsymbol{A}([R(u_1u_2\mathbf{1}+(u_1v_2+v_1u_2+2b_0v_1v_2)B+(u_1w_2+w_1u_22b_0w_1w_2)H)R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-11} \bmod q$

$= (\boldsymbol{A}([R(u_1\mathbf{1}+v_1B+w_1H)R^{-1})(R(u_2\mathbf{1}+v_2B+w_2H)R^{-1})][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$

$= (\boldsymbol{A}((M_1M_2\,)\,[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q.$

Then we have

$$C_1(C_2(X)) \bmod q = E(u_1\,,E\,(u_2,X)) \bmod q$$

$$= E(u_1u_2,X)) \bmod q.$$

It has been shown that in this method we have the multiplicative homomorphism on the plaintext u.

§3.10 Property of proposed fully homomorphic encryption

(**IND-CPA security**). Proposed fully homomorphic encryption is **IND-CPA** secure.

As adversary A_d does not know **sk**, A_d is not able to calculate M from the value of $E(u,X)$.

For any PPT adversary A_d it holds that:

$$\mathrm{Adv}^{\mathrm{CPA}}_{\mathrm{HE}}\,[\lambda] := |\Pr[A_d(E(u_0,X)) = 1] - \Pr[A_d((E(u_1,X))= 1]| = \mathrm{negl}(\lambda)$$

where **sk** ←**KeyGen**(1^λ).

(**Fully homomorphic encryption**). Proposed fully homomorphic encryption =(**KeyGen; Enc; Dec; Eval**) is fully homomorphic because it satisfies the following properties:

1. Homomorphism: Let $CR = \{CR_\lambda\}_{\lambda\in N}$ be the set of all polynomial sized arithmetic circuits. On input **sk** $\leftarrow$**KeyGen**(1^λ), $\forall$ckt $\in$ CR_λ, $\forall(u_1,\ldots,u_n) \in P^n$ where $n = n(\lambda)$, $\forall(C_1,\ldots,C_n)$ where $C_i \leftarrow(E(u_i,X))$, $(i=1,\ldots,n)$,
we have D(**sk**;**Eval**(ckt; $C_1,\ldots,C_n$)) = ckt($u_1,\ldots,u_n$).

Then it holds that:

$$\Pr[D(\mathbf{sk};\ \mathbf{Eval}(\text{ckt};\ C_1,\ldots,C_n)) \neq \text{ckt}(u_1,\ldots,u_n)] = \text{negl}(\lambda).$$

2. Compactness: As the output length of **Eval** is at most $k\log_2 q=k\lambda$ where k is a positive integer, there exists a polynomial $\mu = \mu(\lambda)$ such that the output length of **Eval** is at most μ bits long regardless of the input circuit ckt and the number of its inputs.

§6. Analysis of proposed scheme

Here we analyze the proposed fully homomorphism encryption scheme.

§6.1 Computing plaintext *u* and A_i , Z_i (i=1,…,k) from coefficients of ciphertext $E(u,X)$ to be published

Ciphertext $E(u_s,X)$ *is* published by cloud data centre as follows.

$$E(u_s,X)=$$

$$(A_1((\ldots((A_k(M_s[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\ Z_1^{-1} \bmod q\in O[X]$$

$$=(\boldsymbol{A}((R[u_s\mathbf{1}+v_sB+w_sH]R^{-1})[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q\in O[X]\ ,$$

$$=(\ e_{s00}x_0+e_{s01}x_1+\ \ldots+e_{s07}x_7,$$

$$e_{s10}x_0+e_{s11}x_1+\ \ldots+e_{s17}\ x_7,$$

$$\ldots\qquad\ldots$$

$$e_{s70}x_0+e_{s71}x_1+\ \ldots+e_{s77}\ x_7)\quad \bmod q,$$

$$=\{e_{sjk}\}(j,r=0,\ldots,7;s=1,2,3)$$

with $e_{sjt}\in \boldsymbol{Fq}$ $(j,t=0,\ldots,7;s=1,2,3)$ which is published,
where A_i , Z_i, $R_j \in O$ to be selected randomly such that A_i^{-1}, Z_i^{-1} and R_j^{-1} exist (i=1,...,k;j=1,…,r) are the secret keys of user A.

We try to find plaintext u from coefficients of $E(u,X)$, $e_{jt}\in\boldsymbol{Fq}$ $(j,t=0,\ldots,7)$.

In case that k=8, r=8 and s =3 the number of unknown variables (u_s,v_s,w_s, A_i , Z_i, R_j

(k,r=1,…,8;s=1,2,3)) is 201(=3*3+3*8*8), the number of equations is 192(=64*3) such that

$$\left.\begin{array}{l} F_{100}(M,A_1,A_2,\ldots,A_7)=e_{100} \bmod q, \\ F_{101}(M,A_1,A_2,\ldots,A_7)=e_{101} \bmod q, \\ \quad\cdots \qquad \cdots \\ F_{107}(M,A_1,A_2,\ldots,A_7)=e_{107} \bmod q, \\ \quad\cdots \qquad \cdots \\ \quad\cdots \qquad \cdots \\ F_{377}(M,A_1,A_2,\ldots,A_7)=e_{377} \bmod q, \end{array}\right\} \tag{42}$$

where $F_{100},\ldots,F_{377}$ are the 49(=8*2*3+1)th algebraic multivariate equations.

Then the complexity G required for solving above simultaneous equations by using Gröbner basis is given [8]such as

$$G>G'=({}_{191+dreg}C_{dreg})^w=({}_{4799}C_{191})^w >> O(2^{80}), \tag{43}$$

where G' is the complexity required for solving 192 simultaneous algebraic equations with 191 variables by using Gröbner basis,
where w=2.39, and

$$d_{reg} = 4608\ (=192*(49-1)/2 - 0\sqrt{\ }(192*(49\string^2-1)/6)). \tag{44}$$

The complexity G required for solving above simultaneous equations by using Gröbner basis is enough large for secure.

§6.2 Computing plaintext u_i and d_{ijk} (i,j,k=0,…,7)

We try to computing plaintext u_i and d_{ijk} (i,j,k=0,…,7) from coefficients of ciphertext $E(u_i,X)$ to be published.

At first let $E(Y,X) \in O[X,Y]$ be the enciphering function such as

$$E(Y,X):= (A_1((\ldots((A_k(Y[((A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k])Z_k^{-1}))\ldots))\ Z_1^{-1} \bmod q \in O[X,Y]\ ,$$

$$\begin{aligned} =(&d_{000}x_0y_0+d_{001}x_0y_1+ \ldots+d_{077}x_7y_7, \\ &d_{100}x_0y_0+d_{101}x_0y_1+ \ldots+d_{177}x_7y_7, \\ &\qquad\qquad \ldots. \qquad \ldots. \\ &d_{700}x_0y_0+d_{701}x_0y_1+ \ldots+d_{777}x_7y_7) \bmod q, \end{aligned} \tag{45a}$$

$$=\{d_{ijk}\}(i,j,k=0,\ldots,7) \tag{45b}$$

with $d_{ijk}\in \boldsymbol{Fq}$ $(i,j,k=0,\ldots,7)$.

Next we substitute M_i to Y, where

$$M_i=(m_{i0},m_{i1},\ldots,m_{i7}) \in O. \tag{46}$$

We have

$$E(u_i,X)=(A_1((\ldots((A_k(M_i[((A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k])Z_k^{-1}))\ldots))\ Z_1^{-1}\bmod q\in \quad O[X]\ ,$$

$$\begin{aligned}&=(d_{000}x_0m_{i0}+d_{001}x_0m_{i1}+\ \ldots+d_{077}x_7m_{i7},\\ &\quad d_{100}x_0m_{i0}+d_{101}x_0m_{i1}+\ \ldots+d_{177}x_7m_{i7},\\ &\qquad\qquad \ldots. \qquad\qquad \ldots.\\ &\quad d_{700}x_0m_{i0}+d_{701}x_0m_{i1}+\ \ldots+d_{777}x_7m_{i7})\bmod q,\end{aligned} \tag{47a}$$

$$=\{d_{ijk}\}(i,j,k=0,\ldots,7) \tag{47b}$$

with $d_{ijk}\in \boldsymbol{Fq}$ $(i,j,k=0,\ldots,7)$.

Then we obtain 64 equations from (35) and (47a) as follows.

$$\left.\begin{aligned}&d_{000}m_{i0}+d_{001}m_{i1}+\ \ldots+d_{007}m_{i7}=e_{00}\\ &d_{010}m_{i0}+d_{011}m_{i1}+\ \ldots+d_{017}m_{i7}=e_{01}\\ &\qquad\quad \ldots. \qquad\qquad \ldots.\\ &d_{070}m_{i0}+d_{071}m_{i1}+\ \ldots+d_{077}m_{i7}=e_{07}\end{aligned}\right\} \tag{48a}$$

$$\left.\begin{aligned}&d_{100}m_{i0}+d_{101}m_{i1}+\ \ldots+d_{107}m_{i7}=e_{10}\\ &d_{110}m_{i0}+d_{111}m_{i1}+\ \ldots+d_{117}m_{i7}=e_{11}\\ &\quad \ldots. \qquad\qquad\qquad \ldots.\\ &d_{170}m_{i0}+d_{171}m_{i1}+\ \ldots+d_{177}m_{i7}=e_{17}\end{aligned}\right\} \tag{48b}$$

$$\ldots. \qquad\qquad\qquad \ldots.$$

$$\ldots. \qquad\qquad\qquad \ldots.$$

$$\left.\begin{aligned}&d_{700}m_{i0}+d_{701}m_{i1}+\ \ldots+d_{707}m_{i7}=e_{70}\\ &d_{710}m_{i0}+d_{711}m_{i1}+\ \ldots+d_{717}m_{i7}=e_{71}\\ &\qquad \ldots. \qquad\qquad \ldots.\\ &\end{aligned}\right\} \tag{48c}$$

$d_{770}m_{i0}+d_{771}m_{i1}+ \ldots +d_{777}m_{i7}=e_{77}$

For $M_1,\ldots, M_8$ we obtain the same equations, the number of which is 512.
We also obtain the 8 equations such as

$$| E(M_i,\mathbf{1})|^2= |M_i|^2= m_{i0}{}^2+m_{i1}{}^2+\ldots+m_{i7}{}^2 \bmod q,(i=1,\ldots,8). \quad (49)$$

The number of unknown variables M_i and d_{ijk} $(i,j,k=0,\ldots,7)$ is 576(=512+64).
The number of equations is 520(=512+8).
Then the complexity G required for solving above simultaneous quadratic algebraic equations by using Gröbner basis is given such as

$$G\approx G'=({}_{520+dreg}C_{dreg})^w =({}_{763}C_{243})^{w}=O(2^{1634})>> 2^{80}, \quad (50)$$

where G' is the complexity required for solving 520 simultaneous quadratic algebraic equations with 520 variables by using Gröbner basis,

where w=2.39,

and

$$d_{reg} = 243(=520*(2-1)/2 - 1\sqrt{}(520*(4-1)/6) \quad (51)$$

It is thought to be difficult computationally to solve the above simultaneous algebraic equations by using Gröbner basis.

§6.3 Attack by using the ciphertexts of *u* and -*u*

I show that we can not easily distinguish the ciphertexts of u and $-u$.

We try to attack by using “u and $-u$ attack”.
We define
the medium text M by

$$M:=R(u\mathbf{1}+vB+wH)R^{-1}\in O, \quad (52)$$

where

a plaintext $u\in \boldsymbol{Fq}$, and random numbers $v,w\in \boldsymbol{Fq}$,.

u,v and w satisfy that

$u+v +w= T \bmod q$,

the medium text M_- by

M_{-}:= $R(-u\mathbf{1}+v'B+w'H)R^{-1}\in O$, (53)

where

random numbers $v', w' \in \boldsymbol{Fq}$ such that

$-u+v' +w'= T \bmod q$,

the ciphertext of u by $=(\boldsymbol{A}(M[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$.

By using simple style expression of $E(u, X)$

$$C(X):=E(u, X)= (\boldsymbol{A}(M[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q\in O[X] , \quad (54)$$

the ciphertext of u_{-} by

$$C_{-}(X):=E(u_{-}, X)= (\boldsymbol{A}(M_{-}[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \quad \bmod q\in O[X] . \quad (55)$$

We have

$$C(X)+ C_{-}(X) = (\boldsymbol{A}([M + M_{-}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \quad \bmod q$$

$$= (\boldsymbol{A}([R(u\mathbf{1}+vB+wH -u\mathbf{1}+v'B+w'H)R^{-1}] [(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q$$

(in eneral)

$$= \quad (\boldsymbol{A}([R((v+ v')B+(w+ w') H)R^{-1}] [(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}\neq\mathbf{0} \quad \bmod q \quad (56)$$

We can calculate $| C(\mathbf{1})+ C_{-}(\mathbf{1}) |^2$ as follows.

Then, from $|H|^2=0 \bmod q$, we have

$$| C(\mathbf{1})+ C_{-}(\mathbf{1}) |^2$$

$$=| (\boldsymbol{A}([R(u\mathbf{1}+vB+wH -u\mathbf{1}+v'B+w'H)R^{-1}] [(\boldsymbol{A}^{-1}\mathbf{1})\boldsymbol{Z}]))\boldsymbol{Z}^{-1} |^2 \bmod q$$

$$=| (\boldsymbol{A}([(v+ v')B+(w+ w')H] [(\boldsymbol{A}^{-1}\mathbf{1})\boldsymbol{Z}]))\boldsymbol{Z}^{-1}|^2 \bmod q$$

$$=|2b_0(v+ v')\mathbf{1}+(w +w'-v- v')H|^2=0 \bmod q$$

$$=(2b_0(v+ v')+(w +w'-v- v')b_0)^2+(w +w'-v- v')^2(b_1^2+\ldots+b_7^2) \bmod q$$

$$=(2b_0(v+ v')+(w +w'-v- v') b_0)^2+(w +w'-v- v')^2(-b_0^2) \bmod q$$

$$=(2b_0)^2(v+ v')^2+4 b_0^2(v+ v') (w +w'-v- v') \bmod q$$

$=(2b_0)^2\,(v+v')(w+w') \bmod q \neq 0 \bmod q$ (in general).

It is said that the attack by using "*u* and -*u* attack" is not efficient.

That is, in general

$C(\mathbf{1})+C_{-}(\mathbf{1}) \neq \mathbf{0} \bmod q$,

and

$|C(\mathbf{1})+C_{-}(\mathbf{1})|^2 \neq 0 \bmod q$.

Then we can not easily distinguish the ciphertexts of u and $-u$.

§7. The size of the modulus *q* and the complexity for enciphering/ deciphering

We consider the size of the system parameter q. We select the size of q such that $O(q)$,the order of the plaintext is larger than $O(2^{80})$. Then we need to select modulus $q = O(2^{80})$.

In case of k=8, $q=O(2^{80})$, the size of $e_{ij} \in \boldsymbol{Fq}$ (i,j=0,…,7) which are the coefficients of elements in $E(u,X)=(\boldsymbol{A}(M[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1} \bmod q \in O[X]$ is $(64)(\log_2 q)$bits =5120bits, and the size of system parameters q is less than 80bits.

In case of k=8 , $q=O(2^{80})$, the complexity to obtain $E(u,X)$ is

$(32*512+16*16)(\log_2 q)^2+16*(\log_2 q)^3= O(2^{27})$ bit-operations,

where $16*16*(\log_2 q)^2+16*(\log_2 q)^3$ is the complexiy for inverse of $\boldsymbol{A}^{-1}$ and $\boldsymbol{Z}^{-1}$.

And the complexity required for deciphering is given as follows.
Let $C:=(A_1((\ldots((A_k(M[(A_k^{-1}((\ldots((A_1^{-1}\mathbf{1})Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\,Z_1^{-1} \bmod q$.
We have
$A_k\,((\ldots((A_1^{-1}\,(C\,Z_1))\,Z_2))\ldots.)\,Z_k) = M[(A_k^{-1}((\ldots((A_1^{-1}\mathbf{1})Z_1))\ldots))Z_k] \bmod q$,
$M=[A_k\,((\ldots((A_1^{-1}\,(C\,Z_1))\,Z_2))\ldots.)\,Z_k)][(A_k^{-1}((\ldots((A_1^{-1}\mathbf{1})Z_1))\ldots))Z_k]^{-1} \bmod q$.

$=R_1(\ldots(R_r(u\mathbf{1}+vB+w\,H)R_r^{-1})\ldots)R_1^{-1}$

$(u\mathbf{1}+vB+w\,H)= R_r^{-1}\,(\ldots(R_1^{-1}M\,R_1)\ldots)\,R_r =(m_0',m_1',\ldots,m_7')$:

$u = (m_0'-Tb_0)/(1-b_0) \bmod q$.

Then the complexity G is

$$(16*64+15*64+16*64+2)(\log_2 q)^2+(1+8)*[16*(\log_2 q)^2+(\log_2 q)^3]+(\log_2 q)^3$$

$$=(3154)(\log_2 q)^2+(10)(\log_2 q)^3= O(2^{25}) \text{ bit-operations.}$$

On the other hand the complexity of the enciphering and deciphering in RSA scheme is

$$O(2(\log n)^3)=O(2^{34}) \text{ bit-operations}$$

where the size of modulus n is 2048bits.

Then our scheme requires small memory space and complexity to encipher and decipher so that we are able to implement our scheme to the mobile device.

§8. Conclusion

We proposed the new fully homomorphism encryption scheme based on the octonion ring over finite field that requires small memory space and complexity to encipher and decipher. It was shown that our scheme is immune from the Gröbner basis attacks by calculating the complexity to obtain the Gröbner basis for the multivariate algebraic equations**.**

The proposed scheme does not require a "bootstrapping" process so that the complexity to encipher and decipher is not large.

§10.Acknowledgments

This paper is the revised chapter 4 of my work "Fully Homomorphic Encryption without bootstrapping" published in March, 2015 which was published by LAP LAMBERT Academic Publishing, Saarbrücken/Germany [1].

I would like to thankYongge Wang for some discussion on the scheme [17].

§11.BIBLIOGRAPHY

[1] Masahiro, Y. (2015). Fully Homomorphic Encryption without bootstrapping. Saarbrüken/Germany: LAP LAMBERT Academic Publishing.
[2] 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.
[3] T. Matsumoto, H. Imai, H. Harashima, and H. Miyakawa, "A class of asymmetric cryptosystems using obscure representations of enciphering functions, " in 1983 National Convention Record on Information Systems, IECE Japan, 1983.
[4] T. Matsumoto, and H. Imai, "Public quadratic polynomial-tuples for efficient signature verification and message-encryption," Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88, pp.419–453, New York, NY, USA, 1988, Springer-Verlag New York, Inc.
[5] S. Tsujii, K. Tadaki, and R. Fujita, "Piece in hand concept for enhancing the security of multivariate type public key cryptosystems: Public key without containing all the information of secret key," Cryptology ePrint Archive, Report 2004/366, 2004.
[6] C.Wolf, and B. Preneel, "Taxonomy of public key schemes based on the problem of multivariate quadratic equations," Cryptology ePrint Archive, Report 2005/077, 2005, http://eprint.iacr.org/.
[67] 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] 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.
[9] Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices.In the 41st ACM Symposium on Theory of Computing (STOC), 2009.
[10] Craig Gentry, A Fully Homomorphic Encryption Scheme, 2009. Available at http://crypto.stanford.edu/craig/craig-thesis.pdf .
[11] Marten van Dijk; Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan (2009-12-11). "Fully Homomorphic Encryption over the Integers" (PDF). International Association for Cryptologic Research. Retrieved 2010-03-18.
[12] Damien Stehle; Ron Steinfeld (2010-05-19). "Faster Fully Homomorphic Encryption" (PDF). International Association for Cryptologic Research. Retrieved 2010-09-15.

[13] JS Coron, A Mandal, D Naccache, M Tibouchi ,” Fully homomorphic encryption over the integers with shorter public keys”, Advances in Cryptology–CRYPTO 2011, 487-504.

[14] Halevi, Shai. "An Implementation of homomorphic encryption". Retrieved 30 April 2013. Available at https://github.com/shaih/HElib .

[15] Nuida and Kurosawa,”(Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces”, Cryptology ePrint Archive, Report 2014/777, 2014. http://eprint.iacr.org/.

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

[17] Yongge Wang,” Notes on Two Fully Homomorphic Encryption Schemes Without Bootstrapping”, Cryptology ePrint Archive, Report 2015/519, 2015. http://eprint.iacr.org/.

[18] Masahiro Yagisawa,” Fully Homomorphic Encryption Without bootstrapping”, Cryptology ePrint Archive, Report 2015/474, 2015. http://eprint.iacr.org/.

Appendix A:

Octinv(*A*) --

```
S ← a0^2+a1^2+…+a7^2 mod q.
% S^-1 mod q
    q[1] ← q div S ;% integer part of q/S
    r[1] ← q mod S ;% residue
    k ←1
    q[0] ← q
    r[0] ← S
    while r[k] ≠ 0
        begin
            k← k + 1
            q[k] ← r[k−2] div r[k−1]
            r[k] ← r[k−2] mod [rk−1]
        end
Q [k−1] ← (-1)*q[k−1]
L[ k−1] ← 1
i ← k−1
while   i > 1
    begin
        Q[ i−1] ← (-1)*Q[ i] *q[i−1] + L[ i]
        L[ i−1 ] ← Q[ i ]
        i← i−1
    end

invS ← Q[1] mod q
invA[0] ← a0*invS mod q
For i=1,…,7,
    invA[i] ← (-1)*ai*invS mod q
Return A^-1= (invA[0], invA[1],…, invA[7])
```

Appendix B:

Theorem 1

Let $A=(a_{10},a_{11},\ldots,a_{17})\in O$, $a_{1j}\in$ $\boldsymbol{Fq}$ $(j=0,1,\ldots,7)$.

Let $A^n=(a_{n0},a_{n1},\ldots,a_{n7})\in O$, $a_{nj}\in$ $\boldsymbol{Fq}$ $(n=1,\ldots,7;j=0,1,\ldots,7)$.

a_{00} ,a_{nj} 's(n=1,2,…;j=0,1,…)and b_n's (n=0,1,…) satisfy the equations such that

$N= a_{11}^2+\ldots+a_{17}^2 \bmod q$

$a_{00}=1, b_0=0, b_1=1,$

$a_{n0}= a_{n-1,0}\, a_{10} - b_{n-1}N \bmod q$,(n=1,2,…) (8)

$b_n= a_{n-1,0}+ b_{n-1}a_{10} \bmod q$,(n=1,2,…) (9)

$a_{nj}= b_na_{1j} \bmod q$,(n=1,2,…;j=1,2,…,7) . (10)

(*Proof*:)

We use mathematical induction method.

[step 1]

When n=1, (8) holds because

$a_{10}= a_{00}\, a_{10} - b_0N=a_{10} \bmod q.$

(9) holds because

$b_1= a_{00}+ b_0a_{10} =a_{00} =1 \bmod q.$

(10) holds because

$a_{1j}= b_1a_{1j} = a_{1j} \bmod q$,(j=1,2,…,7)

[step 2]

When $n=k$,

If it holds that

$a_{k0}= a_{k-1,0}\, a_{10} - b_{k-1}N \bmod q$,(k=2,3,4,…) ,

$b_k= a_{k-1,0}+ b_{k-1}a_{10} \bmod q,$

$a_{kj}= b_ka_{1j} \bmod q$,(j=1,2,…,7),

from (9)

$b_{k-1}= a_{k-2,0}+ b_{k-2}a_{10} \bmod q$,(k=2,3,4,…),

then

$A^{k+1}=A^kA=(a_{k0} , b_ka_{11},\ldots, b_ka_{17})(a_{10},a_{11},\ldots,a_{17})$

$=(a_{k0}\, a_{10} - b_kN, a_{k0}\, a_{11}+ b_ka_{11}\, a_{10},\ldots, a_{k0}\, a_{17}+ b_ka_{17}\, a_{10})$

$=(a_{k0}\, a_{10} - b_kN, (a_{k0} + b_ka_{10})a_{11},\ldots, (a_{k0} + b_ka_{10})a_{17})$

$=(a_{k+1,0}, \mathrm{b}_{k+1,0}\, a_{11},\ldots, \mathrm{b}_{k+1,0}\, a_{17}),$

as was required. q.e.d.

Appendix C:

Theorem 2

For an element $A=(a_{10},a_{11},\ldots,a_{17})\in O$,

$A^{J+1}=A \bmod q$,

where

$J:= LCM\{q^2-1,q-1\}=q^2-1$,

$N:=a_{11}^2+a_{12}^2+\ldots+a_{17}^2\neq 0 \bmod q$.

(*Proof*:)

From (8) and (9) it comes that

$a_{n0}= a_{n-1,0}\,a_{10} - b_{n-1}N \bmod q$,

$b_n= a_{n-1,0}+ b_{n-1}a_{10} \bmod q$,

$a_{n0}\, a_{10} + b_n N= (a_{n-1,0}\,a_{10} - b_{n-1}N)\, a_{10} +(a_{n-1,0}+ b_{n-1}a_{10})N= a_{n-1,0}\,a_{10}^2 + a_{n-1,0}\, N \bmod q$,

$b_n N= a_{n-1,0}\,a_{10}^2 + a_{n-1,0}\, N- a_{n0}\, a_{10} \bmod q$,

$b_{n-1} N= a_{n-2,0}\,a_{10}^2 + a_{n-2,0}\, N- a_{n-1,0}\, a_{10} \bmod q$,

$a_{n0}= 2\, a_{10}a_{n-1,0} - (a_{10}^2 +N)\, a_{n-2,0} \bmod q$, $(n=1,2,\ldots)$.

1) In case that $-N\neq 0 \bmod q$ is quadratic non-residue of prime q,

Because $-N\neq 0 \bmod q$ is quadratic non-residue of prime q,

$(-N)^{(q-1)/2}=-1 \bmod q$.

$a_{n0} - 2\, a_{10}\, a_{n-1,0} +(a_{10}^2 +N)\, a_{n-2,0}=0 \bmod q$,

$a_{n0}=(\beta^n(a_{10}-\alpha) + (\beta- a_{10})\alpha^n)/(\beta- \alpha)$ *over* $Fq[\alpha]$

$b_n=(\beta^n-\alpha^n)/(\beta- \alpha)$ *over* $Fq[\alpha]$

where α,β are roots of algebraic quadratic equation such that

$t^2-2a_{10}t+a_{10}^2+N=0$.

$\alpha = \mathrm{a}_{10} + \sqrt{-N}$ *over* $Fq[\alpha]$,

$\beta = \mathrm{a}_{10} - \sqrt{-N}$ *over* $Fq[\alpha]$.

We can calculate β^{q^2} as follows.

$\beta^{q^2} = (\mathrm{a}_{10} - \sqrt{-N})^{q^2}$ *over* $Fq[\alpha]$

$= (\mathrm{a}_{10}{}^{q} - \sqrt{-N}(-N)^{(q-1)/2})^{q}$ *over* $Fq[\alpha]$

$= (\mathrm{a}_{10} \quad - \sqrt{-N}(-N)^{(q-1)/2})^{q}$ *over* $Fq[\alpha]$

$= (\mathrm{a}_{10}{}^{q} - \sqrt{-N}(-N)^{(q-1)/2}(-N)^{(q-1)/2})\ over\ Fq[\alpha]$

$= \mathrm{a}_{10} \quad - \sqrt{-N}(-1)(-1)$ *over* $\boldsymbol{Fq}[\alpha]$

$= \mathrm{a}_{10} - \sqrt{-N}$ *over* $\boldsymbol{Fq}[\alpha]$

$= \beta\ over\ Fq[\alpha].$

In the same manner we obtain

$\alpha^{q^2} = \alpha\ over\ \boldsymbol{Fq}[\alpha].$

$a_{q^2,0} = (\beta^{q^2}(\mathrm{a}_{10} - \alpha) + (\beta - \mathrm{a}_{10})\alpha^{q^2})/(\beta - \alpha)$

$=(\beta(a_{10}-\alpha) + (\beta- a_{10})\alpha)/(\beta- \alpha)=a_{10}$ mod q.

$b_{q^2} = (\beta^{q^2} - \alpha^{q^2})/(\beta - \alpha) = 1$ mod q.

Then we obtain

$A^{q2}=(a_{q2,0}, b_{q2}a_{11},\ldots,b_{q2}a_{17})$

$=(a_{10}, a_{11},\ldots,a_{17})=A$ mod q

2) In case that $-N\neq 0$ mod q is quadratic residue of prime q

$a_{n0}=(\beta^{n}(a_{10}-\alpha) + (\beta- a_{10})\alpha^{n})/(\beta- \alpha)$ mod q,

$b_{n0}=(\beta^{n}-\alpha^{n})/(\beta- \alpha)$ mod q ,

As $\alpha,\beta\in\boldsymbol{Fq}$, from Fermat's little Theorem

$\beta^{q}=\beta$ mod q,

$\alpha^{q}=\alpha$ mod q.

Then we have

$a_{q0}=(\beta^{q}(a_{10}-\alpha) + (\beta- a_{10})\alpha^{q})/(\beta- \alpha)$ mod q

$=(\beta(a_{10}-\alpha) + (\beta- a_{10})\alpha)/(\beta- \alpha)$ mod q

$=a_{10}$ mod q

$b_{q}=(\beta^{q}-\alpha^{q})/(\beta- \alpha)=1$ mod q.

Then we have

$a^q=(a_{q0}, b_q a_{11},\ldots,b_q a_{17})$
$=(a_{10}, a_{11},\ldots,a_{17})=a \bmod q$.

We therefore arrive at the equation such as
$A^{J+1}=A \bmod q$ for arbitrary element $A\in O$,
where

$J=$ LCM $\{q^2-1,q-1\}=q^2-1$,

as was required. q.e.d.

We notice that
in case that $-N=0 \bmod q$
$a_{00}=1$, $b_0=0$, $b_1=1$,
From (8)
$a_{n0}=a_{n-1,0}\,a_{10} \bmod q$,($n=1,2,\ldots$),
then we have
$a_{n0}=a_{10}{}^{n} \bmod q$,($n=1,2,\ldots$).
$a_{q0}=a_{10}{}^{q}=a_{10} \bmod q$.

From (9),

$b_n=a_{n-1,0}+b_{n-1}a_{10} \bmod q$,($n=1,2,\ldots$)
$=a_{10}{}^{n-1}+b_{n-1}a_{10} \bmod q$
$=2a_{10}{}^{n-1}+b_{n-2}a_{10}{}^2 \bmod q$
$\ldots \quad \ldots$
$=(n-1)a_{10}{}^{n-1}+b_1a_{10}{}^{n-1} \bmod q$
$=na_{10}{}^{n-1} \bmod q$.
Then we have
$a_{nj}=na_{10}{}^{n-1}a_{1j} \bmod q$,($n=1,2,\ldots;j=1,2,\ldots,7$) .
$a_{qj}=qa_{10}{}^{q-1}a_{1j} \bmod q =0$,($j=1,2,\ldots,7$) .

Appendix D:

Lemma 2

$$A^{-1}(AB)= B$$
$$(BA)A^{-1}= B$$

(*Proof*:)

$A^{-1}= (a_0/|A|^2 \bmod q, -a_1/|A|^2 \bmod q,\ldots, -a_7/|A|^2 \bmod q)$.

$AB \bmod q$

$= (a_0b_0-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7 \bmod q,$
$a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3 \bmod q,$
$a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6 \bmod q,$
$a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1 \bmod q,$
$a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5 \bmod q,$
$a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4 \bmod q,$
$a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2 \bmod q,$
$a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0 \bmod q)$.

$[A^{-1}(AB)]_0$

$=\{ a_0(a_0b_0-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7)$
$+a_1(a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3)$
$+ a_2(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6)$
$+a_3(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)$
$+a_4(a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5)$
$+ a_5(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4)$
$+a_6(a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2)$
$+a_7(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0)\} /|A|^2 \bmod q$

$=\{(a_0^2+a_1^2+\ldots+a_7^2) b_0\} /|A|^2 =b_0 \bmod q$

where $[M]_n$ denotes the n-th element of $M\in O$.

$[A^{-1}(AB)]_1$

$=\{ a_0(a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3)$
$-a_1(a_0b_0-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7)$
$-a_2(a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5)$

$$-a_3(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0)$$
$$+a_4(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6)$$
$$-a_5(a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2)$$
$$+a_6(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4)$$
$$+a_7(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)\} /|A|^2 \bmod q$$

$$=\{(a_0^2+a_1^2+\ldots+a_7^2)\, b_1\} /|A|^2=\mathrm{b}_1 \bmod q.$$

Similarly we have

$[A^{-1}(AB)]_i=b_i \bmod q$ (i=2,3,…,7).

Then

$$A^{-1}(AB)= B \bmod q. \qquad \text{q.e.d.}$$