Fully Homomorphic Encryption with Composite Number Modulus

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 ring with composite number modulus where the plaintext *p* consists of three numbers *u*,*v*,*w*. The proposed fully homomorphic encryption scheme is immune from the "*p* and -*p* 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.

It is proved that if there exists the PPT algorithm that decrypts the plaintext from the ciphertexts of the proposed scheme, there exists the PPT algorithm that factors the given composite number modulus.
keywords: fully homomorphic encryption, multivariate algebraic equation, Gröbner basis, octonion, factoring

§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 ring with composite number modulus 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.

It is proved that if there exists the PPT algorithm that decrypts the plaintext from the ciphertexts of the proposed scheme, there exists the PPT algorithm that factors the given composite number modulus.

§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 s and t be 1000-digit primes where s and t are secret.

Let $q=st$ be a fixed modulus to be 2000-digit composite number.

Let O be the octonion [16] ring over a ring $\mathbf{Z}/q\mathbf{Z}$.

$$O=\{(a_0,a_1,\ldots,a_7) \mid a_j\in \mathbf{Z}/q\mathbf{Z}\ (j=0,1,\ldots,7)\} \quad (1)$$

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

$$A=(a_0,a_1,\ldots,a_7),\ a_j\in \mathbf{Z}/q\mathbf{Z}\ (j=0,1,\ldots,7), \quad (2)$$

$$B=(b_0,b_1,\ldots,b_7),\ b_j\in \mathbf{Z}/q\mathbf{Z}\ (j=0,1,\ldots,7). \quad (3)$$

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

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

Let

$$|A|^2= a_0^2+a_1^2+\ldots+a_7^2 \bmod q. \quad (6)$$

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

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

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

§2.2. 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

$$AB \neq BA \mod q.$$

2) Non-associative

$$A(BC) \neq (AB)C \mod q.$$

3) Alternative

$$(AA)B=A(AB) \mod q, \tag{8}$$

$$A(BB)=(AB)B \mod q, \tag{9}$$

$$(AB)A=A(BA) \mod q. \tag{10}$$

4) Moufang's formulae [16],

$$C(A(CB))=((CA)C)B \mod q, \tag{11}$$

$$A(C(BC))=((AC)B)C \mod q, \tag{12}$$

$$(CA)(BC)=(C(AB))C \mod q, \tag{13}$$

$$(CA)(BC)=C((AB)C) \mod q. \tag{14}$$

5) For positive integers *n*,*m*, we have

$$(AB)B^n =((AB)B^{n-1})B=A(B(B^{n-1}B))=AB^{n+1} \mod q, \tag{15}$$

$$(AB^n)B =((AB)B^{n-1})B=A(B(B^{n-1}B))=AB^{n+1} \mod q , \tag{16}$$

$$B^n (BA) =B(B^{n-1}(BA))= ((BB^{n-1})B)A=B^{n+1}A \mod q , \tag{17}$$

$$B(B^n A)=B(B^{n-1}(BA))= ((BB^{n-1})B)A=B^{n+1}A \mod q. \tag{18}$$

From (9) and (16), we have

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

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

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

$$\cdots \qquad \cdots$$

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

In the same way we have

$$B^m(B^n A)= B^{n+m}A \mod q. \tag{19}$$

6) **Lemma 1**

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

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

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

(*Proof*:)

From (12) we have

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

Then

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

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

In the same way we have

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

7) **Lemma 2**

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

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

(*Proof*:)

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

8) **Lemma 3**

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

(*Proof*:)

From (14) we substitute A^{-1} to C, we have

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

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

We multiply A from left side,

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

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

$$ABA^{-1}.$$

9) From (10) 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 (14),

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

11a) **Lemma 5a**

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

(*Proof*:)

From (14),

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

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

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

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

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

We apply (12) to inside of [.],

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

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

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

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

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

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

11b) **Lemma 5b**

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

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

where

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

(*Proof*:)

As we use Lemma 5a repeatedly we have

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

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

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

$$\ldots \qquad \ldots$$

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

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

q.e.d.

11c) **Lemma 5c**

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

$$= B \bmod q.$$

where

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

(*Proof*:)

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

From Lemma 2 we have

$$= A_1^{-1}\,(A_1B) = B \bmod q.$$ 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 (13),

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

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

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

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

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

We apply (12) 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 (12) to inside of { . },

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

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

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

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

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

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

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

[Theorem 1]

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

where

$$^{\exists}w,v\in \mathbf{Z}/q\mathbf{Z},$$

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

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

(*Proof*:)

$$A^2 \mod q$$

$$=(a_0a_0-a_1a_1-a_2a_2-a_3a_3-a_4a_4-a_5a_5-a_6a_6-a_7a_7 \mod q,$$

$$a_0a_1+a_1a_0+a_2a_4+a_3a_7-a_4a_2+a_5a_6-a_6a_5-a_7a_3 \mod q,$$

$$a_0a_2-a_1a_4+a_2a_0+a_3a_5+a_4a_1-a_5a_3+a_6a_7-a_7a_6 \mod q,$$

$$a_0a_3-a_1a_7-a_2a_5+a_3a_0+a_4a_6+a_5a_2-a_6a_4+a_7a_1 \mod q,$$

$$a_0a_4+a_1a_2-a_2a_1-a_3a_6+a_4a_0+a_5a_7+a_6a_3-a_7a_5 \mod q,$$

$$a_0a_5-a_1a_6+a_2a_3-a_3a_2-a_4a_7+a_5a_0+a_6a_1+a_7a_4 \mod q,$$

$$a_0a_6+a_1a_5-a_2a_7+a_3a_4-a_4a_3-a_5a_1+a_6a_0+a_7a_2 \mod q,$$

$$a_0a_7+a_1a_3+a_2a_6-a_3a_1+a_4a_5-a_5a_4-a_6a_2+a_7a_0 \mod q)$$

$$=(2a_0^2-L \mod q,\ 2a_0a_1 \mod q,\ 2a_0a_2 \mod q,\ 2a_0a_3 \mod q,$$

$$2a_0a_4 \mod q,\ 2a_0a_5 \mod q, 2a_0a_6 \mod q,\ 2a_0a_7 \mod q)$$

where

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

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

$$A^2=w\mathbf{1}+vA=-L\mathbf{1}+2\,a_0A \bmod q, \qquad (20)$$

$$w= -L \bmod q,$$

$$\mathrm{v}=2a_0 \bmod q.$$ q.e.d.

14) **[Theorem 2]**

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

where h is an integer and $w_h,v_h \in \mathbf{Z}/q\mathbf{Z}$.

(*Proof*:)

From Theorem 1

$$A^2=w_2\mathbf{1}+v_2A=-L\mathbf{1}+2a_0A \bmod q. \qquad (21)$$

If we can express A^h such that

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

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

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

$$v_{\mathrm{h+1}}= w_h+2a_0\mathrm{v}_\mathrm{h} \bmod q \in \mathbf{Z}/q\mathbf{Z}.$$ q.e.d.

15) **[Theorem 3]**

$D \in O$ 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=**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 4]**

$D \in O$ 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=**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 (10)

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

Multiplying C^{-1} from left side ,

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

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

17) **[Theorem 5]**

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 6]**

$D\in O$ 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

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

We can select $C\in O$ such that

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

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 (14)

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

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 (12) we have

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

Multiply A from right side we have

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

(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 $p \in ZqZ$, outputs a ciphertext C ←**Enc**(**sk**; p).

-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 (**sk**) ←**KeyGen**(1^λ).

§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 **sk** ←**KeyGen**(1^λ), $\forall$ ckt $\in CR_\lambda$, $\forall (p_1,\ldots, p_n) \in (\mathbf{Z}/q\mathbf{Z})^n$ where n = n(λ), $\forall (C_1,\ldots,C_n)$

   where C_i← **Enc**(**sk**;u_i), it holds that:

$$\Pr[\mathbf{Dec}(\mathbf{sk};\mathbf{Eval}(\text{ckt}; C_1,\ldots,C_n)) \neq \text{ckt}(p_1,\ldots, p_n)] = \text{negl}(\lambda).$$

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 $\mathbf{Z}/q\mathbf{Z}$.

First we define the secret parameters B and H as follows.

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

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

$$b_0 \neq 0 \bmod s \text{ and } b_0 \neq 0 \bmod t,$$

$$b_1 \neq 0 \bmod s \text{ and } b_1 \neq 0 \bmod t,$$

where

s and t are secret primes,

$q=st$ is published as a system parameter.

Then we have

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

$$B^2=2\, b_0 B \bmod q, \text{ (from theorem1)}$$

$$H^2=2\,h_0H \bmod q, \text{ (from theorem1)}$$

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

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

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

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

Let $p\in \boldsymbol{Z}/q\boldsymbol{Z}$ be a plaintext to belong to the set of the plaintext $P=\{p \mid p\in \boldsymbol{Z}/q\boldsymbol{Z}\}$.

Let u,v and $w\in \boldsymbol{Z}/q\boldsymbol{Z}$ be the numbers such that

$$p:= (u+2b_0v)ks+(u+2b_0w)ht \bmod q,$$

$$= u+ (2b_0ks)v+ (2b_0ht)w \bmod q,$$

where k and h exist that satisfy the following equation from chinese remainder theorem,

$$ks+ht =1 \bmod q,$$

$$k,h\in \boldsymbol{Z}/q\boldsymbol{Z}.$$

How to calculate u, v and w from p.

Given $p\in \boldsymbol{Z}/q\boldsymbol{Z}$.

After $u\in \boldsymbol{Z}/q\boldsymbol{Z}$ is selected randomly such that

$$\mathrm{GCD}(p-u,q)=1,$$

v and w are given such that

$$v_0:=(p-u)(2b_0ks)^{-1}=(p-u)(2b_0)^{-1} \bmod t,$$

$$w_0:=(p-u)(2b_0ht)^{-1}=(p-u)(2b_0)^{-1} \bmod s.$$

Next $\alpha\in \boldsymbol{F}s$ and $\beta\in \boldsymbol{F}t$ are selected arbitrarily. We have

$$v=v_0+\alpha t \bmod q,\ \alpha\in \boldsymbol{F}s,$$

$$w=w_0+\beta s \bmod q,\ \beta\in \boldsymbol{F}t.$$

(Numerical example)

Given $s=7, t=11, q=77, b_0=17, k=8, h=2$,   (8*7+2*11=1 mod 77)

when $p=43, u=59$, $\alpha=5, \beta=8$, we have,

$$v_0:= (p-u)(2b_0)^{-1} =(43-59)(2*17)^{-1}=6 \bmod 11,$$

$$w_0 := (p-u)(2b_0)^{-1} = (43-59)(2*17)^{-1} = 2 \bmod 7,$$

$$v = v_0 + \alpha t = 6+5*11 = 61 \bmod 77,$$

$$w = w_0 + \beta s = 2+8*7 = 58 \bmod 77.$$

We are able to recover p by using the value of u,v,w.

$$(u+2b_0v)ks+(u+2b_0w)ht \bmod q$$

$$=(59+2*17*61)*8*7+(59+2*17*58)*2*11$$

$$=2133*56+2031*22=43=p. \quad \square$$

We define the medium text M by

$$M=(m_0,\ldots,m_7):= R_1(\ldots(R_r([u\mathbf{1}+ vB + wH])R_r^{-1})\ldots)R_1^{-1} \in O,$$

where

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

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

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

Then we have

$$|M|^2=(u+ b_0v+ b_0w)^2+ (v- w)^2 (b_1^2+\ldots+b_7^2)$$

$$=(u+ b_0v+ b_0w)^2+ (v- w)^2 (-b_0^2) \bmod q,$$

$$= u^2+ 2u(b_0v+ b_0w) +b_0^2(v+w)^2 - b_0^2 (v- w)^2 \bmod q,$$

$$= u^2+ 2u(b_0v+ b_0w) +4b_0^2vw \bmod q,$$

$$=(u+ 2b_0v) (u+ 2b_0w)\neq 0 \bmod q \text{ (in general)}.$$

Here we simplify the expression of medium text M such that

$$M:= \boldsymbol{R}([u\mathbf{1}+ vB + wH])\boldsymbol{R}^{-1} \in O.$$

We show relation between M and p.

$$(m'_0,m'_1,\ldots,m'_7):= R_r^{-1}(\ldots(R_1^{-1}(M R_1)\ldots)R_r = (u\mathbf{1}+ vB + wH) \in O,$$
$$(m'_0+ m'_1b_0/ b_1)ks+(m'_0- m'_1 b_0/ b_1)ht \bmod q$$
$$=[(u+vb_0+wb_0+(vb_1-wb_1)b_0/b_1)ks+(u+vb_0+wb_0-(vb_1-wb_1)b_0/b_1)ht]$$

$$= [(u+2b_0v)ks+(u+2b_0w)ht] \bmod q$$
$$=u +(2b_0ks)v+ (2b_0ht)w \bmod q$$
$$=p.$$

Let

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

$$p_1:=u_1+(2b_0ks)v_1+(2b_0ht)w_1 \bmod q,$$

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

$$p_2:=u_2+(2b_0ks)v_2+(2b_0ht)w_2 \bmod q.$$

We have

$$M_1M_2 = [\boldsymbol{R}\,(u_1\mathbf{1}+v_1B+w_1H)\boldsymbol{R}^{-1}][\boldsymbol{R}(u_2\mathbf{1}+v_2B+w_2H)\boldsymbol{R}^{-1}]$$
$$= \boldsymbol{R}[(u_1u_2)\mathbf{1}+(u_1v_2+v_1u_2+2b_0v_1v_2)B+(u_1w_2+w_1u_2+2b_0w_1w_2)H]\boldsymbol{R}^{-1} \qquad (34)$$
$$=M_2M_1 \bmod q.$$

We show the reason by using Lemma 5 as follows.

$$[\boldsymbol{R}\,B\boldsymbol{R}^{-1}][\boldsymbol{R}B\boldsymbol{R}^{-1}]= \boldsymbol{R}B^2\boldsymbol{R}^{-1}= 2\,b_0\boldsymbol{R}B\boldsymbol{R}^{-1} \bmod q,$$
$$[\boldsymbol{R}\,H\boldsymbol{R}^{-1}][\boldsymbol{R}H\boldsymbol{R}^{-1}]= \boldsymbol{R}H^2\boldsymbol{R}^{-1}=2\,h_0\boldsymbol{R}H\boldsymbol{R}^{-1} \bmod q,$$

and

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

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

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

Then

$$[\boldsymbol{R}\,H\boldsymbol{R}^{-1}]\,[\boldsymbol{R}\,B\boldsymbol{R}^{-1}] =\mathbf{0} \bmod q.$$

In the same manner we have

$$[\boldsymbol{R}\,B\boldsymbol{R}^{-1}]\,[\boldsymbol{R}\,H\boldsymbol{R}^{-1}] =\mathbf{0} \bmod q.$$

Then we have (34).

$$\text{Let } (m^*_0,m^*_1,\ldots,m^*_7) := R_r^{-1}(\ldots(R_1^{-1}(\,[M_1M_2\,]\,R_1)\ldots)R_r \bmod q$$
$$=(\,u_1u_2)\mathbf{1}+(\,u_1v_2+v_1u_2+2b_0v_1v_2)B+(\,u_1w_2+ w_1u_2+ 2b_0w_1w_2)H \bmod q.$$

We can show that we obtain p_1p_2 the multiple of p_1 and p_2 from $(m^*_0, m^*_1,\ldots, m^*_7)$ as follows.

$$p_1\,p_2=(\,u_1+(2b_0ks)v_1+(2b_0ht)w_1\,)(u_2+(2b_0ks)v_2+(2b_0ht)w_2)$$
$$=u_1\,u_2+u_2(2b_0ks)v_1+u_2(2b_0ht)w_1 +u_1(2b_0ks)v_2 +(2b_0ks)v_1\,(2b_0ks)v_2$$
$$+ u_1\,(2b_0ht)w_2 + (2b_0ht)w_1\,(2b_0ht)w_2 \bmod q,$$
$$=u_1\,u_2+ u_2\,v_1\,(2b_0k)s + u_2\,w_1\,(2b_0h)t + u_1\,v_2\,(2b_0k)s + v_1\,v_2\,(2b_0)^2ks\,ks$$
$$+ u_1\,w_2\,(2b_0h)t + (2b_0)^2htht w_1\,w_2 \bmod q,$$
$$= u_1\,u_2+u_2\,v_1\,(2b_0k)s + u_1\,v_2\,(2b_0k)s + v_1\,v_2\,(2b_0)^2ks$$
$$+ u_2\,w_1\,(2b_0h)t +u_1\,w_2\,(2b_0h)t + w_1\,w_2\,(2b_0)^2ht \quad \bmod q,$$

$$=u_1u_2+2\, b_0\, (u_1v_2+u_2v_1+2b_0v_1v_2)ks$$
$$+2\, b_0\, (u_1w_2 + w_1u_2 + 2b_0w_1w_2)ht \bmod q. \qquad (35)$$

$$m^*_0+ m^*_1b_0/b_1$$
$$= u_1\, u_2+(\, u_1\, v_2+v_1\, u_2+2\, b_0v_1\, v_2)b_0+(\, u_1w_2+ w_1\, u_2+ 2b_0w_1w_2)b_0$$
$$+(\, u_1\, v_2+v_1\, u_2+2\, b_0v_1\, v_2)b_0-(\, u_1w_2+ w_1\, u_2+ 2b_0w_1w_2)b_0 \bmod q$$
$$= u_1u_2+2(\, u_1v_2+v_1u_2+2b_0v_1v_2)b_0 \bmod q, \qquad (36)$$
$$m^*_0- m^*_1b_0/b_1$$
$$= u_1\, u_2+(\, u_1\, v_2+v_1\, u_2+2\, b_0v_1\, v_2)b_0+(\, u_1w_2+ w_1\, u_2+ 2b_0w_1w_2)b_0$$
$$-(\, u_1\, v_2+v_1\, u_2+2\, b_0v_1\, v_2)b_0+(\, u_1w_2+ w_1\, u_2+ 2b_0w_1w_2)b_0 \bmod q$$
$$= u_1\, u_2+2(\, u_1w_2+ w_1\, u_2+ 2b_0w_1w_2)b_0 \bmod q. \qquad (37)$$

Then we have the plaintext p_{12} corresponding to $[M_1M_2\,]$ as follows.

$$p_{12} :=(m^*_0+ m^*_1b_0/b_1)\, ks+(\, m^*_0- m^*_1b_0/b_1)\, ht \bmod q$$
$$=(\, u_1\, u_2+2(\, u_1\, v_2+v_1\, u_2+2\, b_0\, v_1\, v_2)b_0)\, ks$$
$$+(\, u_1\, u_2+2(\, u_1w_2+ w_1\, u_2+ 2b_0w_1w_2)b_0)\, ht \bmod q$$
$$=u_1\, u_2+2(\, u_1\, v_2+v_1\, u_2+2\, b_0v_1\, v_2)ksb_0$$
$$+2(\, u_1w_2+ w_1\, u_2+ 2b_0w_1w_2)htb_0 \bmod q$$
$$= u_1u_2+2\, b_0\, (\, u_1\, v_2+v_1\, u_2+2\, b_0v_1v_2)ks+2\, b_0\, (u_1w_2+ w_1\, u_2+2b_0w_1w_2)ht \bmod q$$
$$= p_1p_2 \bmod q\, . \qquad (38)$$

Here I define the some parameters for describing FHE.

Let s and t be secret 1000-digit primes.

Let $q=st$ be a 2000-digit composite number to be published as a system parameter.

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

Let p be a plaintext such that

$$p:= (m_0+ m_1b_0/\, b_1)\, k\, s+ (m_0- m_1\, b_0/\, b_1)\, h\, t = (u+2v\, b_0)\, k\, s+ (u+2b_0w)\, h\, t \bmod q.$$

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

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

Let $C(X)=E(p,X)\in O[X]$ 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 $E(p,X) = C(X)$ is defined as follows.

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

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

$$=(\, e_{00}x_0+e_{01}x_1+\, \ldots+e_{07}x_7,$$

$$e_{10}x_0+e_{11}x_1+\, \ldots+e_{17}\, x_7,$$

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

$$e_{70}x_0+e_{71}x_1+ \ldots+e_{77}\, x_7), \qquad (39)$$

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

with $e_{ij}\in \boldsymbol{Z}/q\boldsymbol{Z}$ $(i,j=0,\ldots,7)$ which is published in cloud centre,
where

$$(m'_0,m'_1,\ldots,m'_7):= R_r^{-1}(\ldots(R_1^{-1}(M\, R_1)\ldots)R_r = (u\mathbf{1}+ vB + wH)\in O,$$

$$p= (m'_0+ m'_1b_0/ b_1)ks+ (m'_0- m'_1\, b_0/ b_1)\, h\, t = (u+2v\, b_0)\, k\, s+ (u+2b_0w)\, h\, t \bmod q.$$

Here we notice how to construct enciphering function.
We show a part of process for constructing enciphering function $E(p,X)$ as follows.

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

Let D be the deciphering function defined as follows .

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

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

$$D(X):= G_1(C(G_2(X)) \bmod q=MX. \qquad (40)$$

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

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

Then we can obtain the plaintext p as follows.

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

From $(m_0', m_1',\ldots,m_7')$, we obtain the plaintext p.

$$m_0' =u + vb_0+wb_0 \bmod q,$$

$$m_1' = v\, b_1 - w b_1 \bmod q,$$

$$m_0' + m_1'\, b_0/\, b_1 = u + 2v b_0 \bmod q,$$

$$m_0' - m_1'\, b_0/\, b_1 = u + 2w b_0 \bmod q,$$

$$\begin{aligned}(m_0' + m_1'\, b_0/\, b_1)\, k\, s + (m_0' - m_1'\, b_0/\, b_1)\, h\, t \bmod q \\ = (u + 2k\, vsb_0)\, k\, s + (u + 2h\, wtb_0)\, h\, t \bmod q \\ = u + 2b_0 ksv + 2b_0 htw \bmod q = p. \qquad (41)\end{aligned}$$

§3.4 Assumption

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

§3.4.1 Factoring assumption Fact(q)

Let q be as a large composite number where $q = st$ with $q = q(\lambda)$, where λ is a security parameter, and s and t are prime numbers.

In the Fact(q) assumption, the PPT(Probabilistic polynomial time) algorithm AL is given n and the goal is to find primes s,t.

For a parameter $q = q(\lambda)$ defined in terms of the security parameter λ and for any PPT algorithm AL , we have

Pr[q=st with $q = q(\lambda)$: $(s, t) \leftarrow \mathrm{AL}(1^{\lambda},q)$]= negl($\lambda$).

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

Let q be a 2000-digit composite number. 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 $C_i(X) := E(p_i ,X)=(A_1((\ldots((A_k(M_i\,[(A_k^{-1}((\ldots((A_1^{-1}X)Z_1))\ldots))Z_k]))Z_k^{-1}))\ldots))\, Z_1^{-1} \bmod q\in O[X]$ where medium text $M_i=(m_{i0},\ldots, m_{i7}):= R_1(\ldots(R_r(u_i\mathbf{1}+ksv_iB+htw_iH)R_r^{-1})\ldots)R_1^{-1}\in O$, plaintext p_i (i=1,…,n), X is a variable.

In the **EOR**($k,r,n;q$) assumption, the PPT 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 p_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

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

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 $\mathbf{sk}=(\boldsymbol{A},\boldsymbol{Z},\boldsymbol{R},B,H,s,t)\leftarrow\mathbf{KeyGen}(1^\lambda)$, where **sk** is a secret encryption /dencryption key.

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

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

-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 $C'\leftarrow\mathbf{Eval}(\text{ckt}; C_1,\ldots,C_n)$ where $C_i=\boldsymbol{C}(X;\mathbf{sk},p_i)$ $(i=1,\ldots,n)$.

[Theorem 7]

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

$$\text{if } E(p, X)= E(p', X) \bmod q \text{ , then } p=p' \bmod q.$$

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

(*Proof*)

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

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

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

where

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

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

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

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

$$R_1(\ldots(R_r(u\mathbf{1}+ vB + wH)R_r^{-1})\ldots)R_1^{-1}$$

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

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

Then we have

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

$$(v- w)b_1=(v'-w')b_1 \bmod q,$$

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

$$u+2vb_0= u'+2v'b_0 \bmod q,$$

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

$$u+2 wb_0= u'+2 w'b_0 \bmod q,$$

$$p=k(u+2v\, b_0)s+h(u+2b_0w)t \bmod q,$$

$$=k(u'+2v'\, b_0)s+h(u'+2b_0w')t =p' \bmod q.$$

q.e.d

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

We simply express the encrypting function such that

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

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

§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 $C_1(X)= E(p_1, X)$ and $C_2(X)= E(p_2, X)$ be the ciphertexts,

$$p_1= (u_1+2v_1\, b_0)\, k\, s+ (u_1+2b_0w_1)\, h\, t \bmod q,$$
$$p_2= (u_2+2v_2\, b_0)\, k\, s+ (u_2+2b_0w_2)\, h\, t \bmod q.$$

$$C_1(X)\pm C_2(X) \bmod q =E(p_1,X) \pm E(p_2,X) \bmod q$$

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

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

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

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

$$= \boldsymbol{A}(([\boldsymbol{R}((u_1\pm u_2)\mathbf{1}+(v_1\pm v_2)B+(w_1\pm w_2)H))\boldsymbol{R}^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}])\boldsymbol{Z}^{-1}) \bmod q .$$

We have the plaintext p_{12}corresponding to $E(p_1,X) \pm E (p_2,X)$ as follows.

$$p_{12}:= ((u_1\pm u_2)+2(v_1\pm v_2)\, b_0)\, k\, s+ ((u_1\pm u_2)+2b_0(w_1\pm w_2))\, h\, t \bmod q$$

$$= p_1\pm p_2 \bmod q.$$

Then we have

$$E(p_1,X) \pm E (p_2,X) \bmod q= E(p_1\pm p_2,X) \bmod q.$$

§3.7 Multiplication scheme on ciphertexts

Here we consider the multiplicative operation on the ciphertexts.
Let $C_1(X)= E(p_1, X)$ and $C_2(X)= E(p_2, X)$ be the ciphertexts corresponding to the plaintexts p_1 and p_2.

$$C_1(C_2(X)) \bmod q =E(p_1,E(p_2,X)) \bmod q$$

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

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

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

$$=\boldsymbol{A}((M_1(M_2[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q. \qquad (42)$$

We show the operation on B and H beforehand.

$$\boldsymbol{A}(([RBR^{-1}]([R\, HR^{-1}]\, [(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q$$

$$= \boldsymbol{A}(([RBR^{-1}]([R\, (2b_0\mathbf{1}\text{-B})R^{-1}]\, [(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q$$

$$=\boldsymbol{A}(([RBR^{-1}]([R(2b_0\mathbf{1})R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1})\text{-}\boldsymbol{A}(([RBR^{-1}][RBR^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q$$

$$=2b_0\, \boldsymbol{A}(([RBR^{-1}]([(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1})\text{-}\boldsymbol{A}(([RB^2R^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q$$

$$=2b_0\, \boldsymbol{A}(([RBR^{-1}]([(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1})\text{- } 2b_0\, \boldsymbol{A}(([RBR^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q$$

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

In the same manner we have

$$\boldsymbol{A}(([RHR^{-1}]([R\,BR^{-1}]\,[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q=\mathbf{0} \bmod q.$$

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

$$C_1(C_2(X)) \bmod q = E(p_1,E(p_2,X)) \bmod q=\boldsymbol{A}((M_1(M_2[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q.$$

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

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

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

$$+ \boldsymbol{A}(([\boldsymbol{R}\,(w_1H)\,\boldsymbol{R}^{-1}]\,([\boldsymbol{R}(u_2\mathbf{1}+v_2B+w_2HH)\,\boldsymbol{R}^{-1}]\,[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod.$$

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

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

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

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

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

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

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

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

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

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

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

$$=\boldsymbol{A}(([\boldsymbol{R}(u_1u_2\mathbf{1}+(u_1v_2+v_1u_2+2b_0v_1v_2)B+(u_1w_2+w_1u_2+2b_0w_1w_2)H)\boldsymbol{R}^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q$$

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

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

Then we have

$$C_1(C_2(X)) \bmod q = E(p_1,E\,(p_2,X)) \bmod q$$

$$=\boldsymbol{A}(([\boldsymbol{R}(u_1u_2\mathbf{1}+(u_1v_2+v_1u_2+2b_0v_1v_2)B+(u_1w_2+w_1u_2+2b_0w_1w_2)H)\boldsymbol{R}^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}]))\boldsymbol{Z}^{-1}) \bmod q.$$

Let $(m_0^*,m_1^*,\ldots,m_7^*):= R_r^{-1}(\ldots(R_1^{-1}(\,[M_1M_2]\,R_1)\ldots)R_r \bmod q$.

$$=(u_1u_2\mathbf{1}+(u_1v_2+v_1u_2+2b_0v_1v_2)B+(u_1w_2+w_1u_2+2b_0w_1w_2)H) \bmod q.$$

We have the plaintext p_{12} of M_1M_2 as follows.

$$p_{12}:=k(m_0^*+ m_1^* b_0/ b_1)s+h(m_0^*- m_1^*b_0/ b_1)t \bmod q$$
$$= (u_1u_2+2 b_0 (u_1 v_2+v_1 u_2+2 b_0v_1v_2))ks+(u_1u_2+2b_0 (u_1w_2+ w_1u_2+2b_0w_1w_2))ht \bmod q$$
$$= u_1u_2+2 b_0 (u_1 v_2+v_1 u_2+2 b_0v_1v_2)ks+2b_0 (u_1w_2+ w_1u_2+2b_0w_1w_2)ht \bmod q$$
$$= (u_1+2b_0ksv_1+2b_0htw_1)(u_2+2b_0ksv_2+2b_0htw_2) \bmod q$$
$$= p_1p_2 \bmod q .$$

Then we have

$$C_1(C_2(X)) \bmod q =E(p_1,E (p_2,X)) \bmod q=E(p_1p_2,X)) \bmod q.$$

It has been shown that this scheme has the multiplicative homomorphism.

§3.8 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 $E(p,X)$.

For any PPT adversary A_d it holds that:

$$\mathrm{Adv}^{CPA}_{HE} [\lambda] :=|\Pr[A_d(E(p_0,X)) = 1] - \Pr[A_d((E(p_1,X))= 1]|= \mathrm{negl}(\lambda)$$

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** ←**KeyGen**(1^λ), $\forall$ckt $\in$ CR_λ, $\forall(p_1,\ldots,p_n) \in (\mathbf{Z}/q\mathbf{Z})^n$ where $n = n(\lambda)$, $\forall(C_1,\ldots,C_n)$ where C_i ←$(E(p_i,X))$, (i =1,…,n),
we have D(**sk**;**Eval**(ckt; $C_1,\ldots,C_n$)) = ckt($p_1,\ldots,p_n$).

Then it holds that:

$$\Pr[D(\mathbf{sk}; \mathbf{Eval}(\mathrm{ckt}; C_1,\ldots,C_n)) \neq \mathrm{ckt}(p_1,\ldots,p_n)] = \mathrm{negl}(\lambda).$$

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.

§4. Analysis of proposed scheme

Here we analyze the proposed fully homomorphism encryption scheme.

§4.1 Computing (p,u,v,w) from coefficients of ciphertext $E(p,X)$ to be published

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

$$E(p, X)= \boldsymbol{A}((M[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}])\boldsymbol{Z}^{-1})\bmod q\in O[X]$$
$$=(e_{00}x_0+e_{01}x_1+ \ldots+e_{07}x_7,$$
$$e_{10}x_0+e_{11}x_1+ \ldots+e_{17} x_7,$$
$$\ldots. \qquad \ldots.$$
$$e_{70}x_0+e_{71}x_1+ \ldots+e_{77} x_7) \quad \bmod q,$$
$$=\{e_{jt}\}(j,t=0,\ldots,7)$$

with $e_{jt}\in \boldsymbol{Z}/q\boldsymbol{Z}$ (j,t=0,…,7) which is stored in cloud data centre,
where

$$M= [\boldsymbol{R}\ (u\mathbf{1}+ vB + wH)\boldsymbol{R}^{-1} \bmod q,$$
$$M'=(m'_0,m'_1,\ldots,m'_7) = R_r^{-1}(\ldots(R_1^{-1}(M\, R_1)\ldots)R_r = (u\mathbf{1}+ vB + wH)\bmod q$$
$$= u\mathbf{1}+v(b_0,b_1,\ldots,b_7)+w(b_0,-b_1,\ldots,-b_7) \bmod q.$$
$$(m'_0+ m'_1b_0/ b_1)ks+(m'_0- m'_1 b_0/ b_1)ht \bmod q$$
$$=(u+vb_0+wb_0+(vb_1-wb_1)b_0/b_1)ks+(u+vb_0+wb_0-(vb_1-wb_1)b_0/b_1)ht \bmod q$$
$$=(u+2b_0v)ks+(u+2b_0w)ht \bmod q$$
$$=u+2b_0vks+2b_0wht \bmod q$$
$$=p\in Z/qZ.$$

and

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.

[Theorem 8]

When $\det\{e_{jt}\}\neq 0 \bmod q$,

if there exists the PPT algorithm AL for obtaining any plaintext and parameters (p,u,v,w) from coefficients of $E(p, X)$, $e_{jt}\in \boldsymbol{Z}/q\boldsymbol{Z}$ (j,t =0,…,7), there exists the PPT algorithm that factors modulus q.

(*Proof*:)

At first we calculate the $E(p^{-1} \bmod q, X)= \{e'_{jt}\}(j,t=0,\ldots,7)$ from the $\{e_{jt}\}(j,t=0,\ldots,7)$.

$$E(p,E(p^{-1} , X \bmod q))= E(pp^{-1} \bmod q, X)= E(1 \bmod q, X))=X \bmod q$$
$$=(e_{00}(e'_{00}x_0+\ldots+e'_{07}x_7)+e_{01}(e'_{10}x_0+ \ldots+e_{1'7}\, x_7)+ \ldots+e_{07}(e'_{70}x_0+ \ldots+e'_{77}\, x_7),$$
$$e_{10}(e'_{00}x_0+\ldots+e'_{07}x_7)+e_{11}(e'_{10}x_0+\ldots+e_{1'7}\, x_7)+ \ldots+e_{17}\, (e'_{70}x_0+\ldots+e'_{77}\, x_7),$$

$$\cdots \qquad \cdots$$
$$e_{70}(e'_{00}x_0+\ldots+e'_{07}x_7)+e_{71}(e'_{10}x_0+\ldots+e_{1'7}\,x_7)+\ldots+e_{77}\,(e'_{70}x_0+\ldots+e'_{77}\,x_7))\bmod q,$$
$$= X \bmod q = (x_0,x_1,\ldots,x_7) \bmod q.$$

We have the following simultaneous equations.

$$\left.\begin{array}{l} e_{00}e'_{00}+e_{01}e'_{10}+\ldots+e_{07}e'_{70}=1 \bmod q \\ e_{10}e'_{00}+e_{11}e'_{10}+\ldots+e_{17}e'_{70}=0 \bmod q \\ \quad\ldots \qquad\qquad \ldots \\ e_{70}e'_{00}+e_{71}e'_{10}+\ldots+e_{77}e'_{70}=0 \bmod q \end{array}\right\}$$

$$\left.\begin{array}{l} e_{00}e'_{01}+e_{01}e'_{11}+\ldots+e_{07}e'_{71}=0 \bmod q \\ e_{10}e'_{01}+e_{11}e'_{11}+\ldots+e_{17}e'_{71}=1 \bmod q \\ \quad\ldots \qquad\qquad \ldots \\ e_{70}e'_{01}+e_{71}e'_{11}+\ldots+e_{77}e'_{71}=0 \bmod q \end{array}\right\}$$

$$\cdots \qquad \cdots$$
$$\cdots \qquad \cdots$$

$$\left.\begin{array}{l} e_{00}e'_{07}+e_{01}e'_{17}+\ldots+e_{07}e'_{77}=0 \bmod q \\ e_{10}e'_{07}+e_{11}e'_{17}+\ldots+e_{17}e'_{77}=0 \bmod q \\ \quad\ldots \qquad\qquad \ldots \\ e_{70}e'_{07}+e_{71}e'_{17}+\ldots+e_{77}e'_{77}=1 \bmod q \end{array}\right\}$$

We obtain $\{e'_{jt}\}(j,t=0,\ldots,7)$ by solving above simultaneous equations as $\det\{e_{jt}\}\neq 0 \bmod q$.
We can obtain (p,u,v,w) from $\{e_{jt}\}(j,t=0,\ldots,7)$ and (p^{-1},u',v',w') from $\{e'_{jt}\}(j,t=0,\ldots,7)$ by using the PPT algorithm AL
where

$$\left.\begin{array}{l} p= (u+2b_0v)ks+ (u+2b_0w)ht \bmod q \\ p^{-1}= (u'+2b_0v')ks+ (u'+2b_0w')ht \bmod q \end{array}\right\}$$

We transform above equations.

$$\left.\begin{array}{l} 2b_0vks +2b_0wht = p - u \bmod q \\ 2b_0v'ks+2b_0w'ht = p^{-1} -u' \bmod q \end{array}\right\}$$

As we select v,w,v' and w' randomly when we generate the medium text M,M' from plaintext p and p^{-1}, we have in general

$$vw'- v'w\neq 0 \bmod q.$$

Then we obtain $ks \bmod q$ and $ht \bmod q$ by solving the above simultaneous equation.
We obtain the value of s and t with overwhelming probability by calculating

$$\mathrm{GCD}(v(p^{-1}- u')-v'(p - u)\ , q)=t$$

or

$$\mathrm{GCD}(-w(p^{-1}- u')+w'(p - u)\ , q))=s,$$

as was required. q.e.d.

We have shown that proposed scheme is a fully homomorphic encryption with provable security.

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

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

$$E(p_d,X)= \boldsymbol{A}((M_d[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}])\boldsymbol{Z}^{-1}) \bmod q$$

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

$$=(e_{d00}x_0+e_{d01}x_1+ \ldots+e_{d07}x_7,$$

$$e_{d10}x_0+e_{d11}x_1+ \ldots+e_{d17} x_7,$$

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

$$e_{d70}x_0+e_{d71}x_1+ \ldots+e_{d77} x_7) \quad \bmod q,$$

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

with $e_{djt}\in\boldsymbol{Z}/q\boldsymbol{Z}$ (j,t=0,…,7;d=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 p from coefficients of $E(p,X)$, $e_{djt}\in\boldsymbol{Z}/q\boldsymbol{Z}$ (j,t =0,…,7;d=1,2,3).

In case that k=8, r=8 and d =3 the number of unknown variables (u_d,v_d,w_d, A_i , Z_i, R_j (i,j=1,…,8;d=1,2,3)) is 201(=3*3+3*8*8), the number of equations is 192(=64*3) such that

$$\left.\begin{aligned}
&F_{100}(M,A_1,A_2,\ldots,A_7)=e_{100} \bmod q,\\
&F_{101}(M,A_1,A_2,\ldots,A_7)=e_{101} \bmod q,\\
&\cdots \qquad \cdots\\
&F_{107}(M,A_1,A_2,\ldots,A_7)=e_{107} \bmod q,\\
&\cdots \qquad \cdots\\
&\cdots \qquad \cdots\\
&F_{377}(M,A_1,A_2,\ldots,A_7)=e_{377} \bmod q,
\end{aligned}\right\} \quad (43)$$

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

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

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

$$d_{reg}=4608\ (=192*(49-1)/2 - 0\surd(192*(49\hat{}2-1)/6)).$$

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

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

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

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

$$\begin{aligned}Enc(Y,X) &:= \boldsymbol{A}((Y[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}])\boldsymbol{Z}^{-1}) \bmod q\in O[X,Y],\\ &=(d_{000}x_0y_0+d_{001}x_0y_1+\ldots+d_{077}x_7y_7,\\ &\quad d_{100}x_0y_0+d_{101}x_0y_1+\ldots+d_{177}x_7y_7,\\ &\quad \ldots.\quad \ldots.\\ &\quad d_{700}x_0y_0+d_{701}x_0y_1+\ldots+d_{777}x_7y_7) \bmod q, \qquad (44)\\ &=\{d_{ijk}\}(i,j,k=0,\ldots,7)\end{aligned}$$

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

Next we substitute M_i to Y, where

$$M_i=(m_{i0},m_{i1},\ldots,m_{i7}) = u_i\mathbf{1}+ v_iB + w_iH \bmod q\in O. \qquad (45)$$

We have

$$\begin{aligned}E(p_i,X) &= \boldsymbol{A}((M_i[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}])\boldsymbol{Z}^{-1}) \bmod q\in O[X]\ ,\\ &=(d_{000}x_0m_{i0}+d_{001}x_0m_{i1}+\ldots+d_{077}x_7m_{i7},\\ &\quad d_{100}x_0m_{i0}+d_{101}x_0m_{i1}+\ldots+d_{177}x_7m_{i7},\end{aligned}$$

$$\text{....} \qquad \text{....}$$

$$d_{700}x_0m_{i0}+d_{701}x_0m_{i1}+\ \dots+d_{777}x_7m_{i7})\ \mathrm{mod}\ q, \qquad (46)$$

$$=\{d_{ijk}\}(i,j,k=0,\dots,7)$$

with $d_{ijk}\in \mathbf{Z}/q\mathbf{Z}$ $(i,j,k=0,\dots,7)$.

Then we obtain 64 equations from (39) and (46) as follows.

$$\left.\begin{array}{l} d_{000}m_{i0}+d_{001}m_{i1}+\ \dots+d_{007}m_{i7}=e_{00} \\ d_{010}m_{i0}+d_{011}m_{i1}+\ \dots+d_{017}m_{i7}=e_{01} \\ \qquad \text{....} \qquad \text{....} \\ d_{070}m_{i0}+d_{071}m_{i1}+\ \dots+d_{077}m_{i7}=e_{07} \end{array}\right\} \qquad (47a)$$

$$\left.\begin{array}{l} d_{100}m_{i0}+d_{101}m_{i1}+\ \dots+d_{107}m_{i7}=e_{10} \\ d_{110}m_{i0}+d_{111}m_{i1}+\ \dots+d_{117}m_{i7}=e_{11} \\ \qquad \text{....} \qquad \text{....} \\ d_{170}m_{i0}+d_{171}m_{i1}+\ \dots+d_{177}m_{i7}=e_{17} \end{array}\right\} \qquad (47b)$$

$$\text{....} \qquad \text{....}$$
$$\text{....} \qquad \text{....}$$

$$\left.\begin{array}{l} d_{700}m_{i0}+d_{701}m_{i1}+\ \dots+d_{707}m_{i7}=e_{70} \\ d_{710}m_{i0}+d_{711}m_{i1}+\ \dots+d_{717}m_{i7}=e_{71} \\ \qquad \text{....} \qquad \text{....} \\ d_{770}m_{i0}+d_{771}m_{i1}+\ \dots+d_{777}m_{i7}=e_{77} \end{array}\right\} \qquad (47c)$$

For $M_0,\dots, M_7$ we obtain the same equations, the number of which is 512.
We also obtain the 8 equations such as

$$|\,E(p_i,\mathbf{1})|^2=|M_i|^2=m_{i0}{}^2+m_{i1}{}^2+\dots+m_{i7}{}^2\ \mathrm{mod}\ q,(i=0,\dots,7). \qquad (48)$$

The number of unknown variables M_i and d_{ijk} $(i,j,k=0,\dots,7)$ 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

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

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

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

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

§4.4 Attack by using the ciphertexts of *p* and *-p*

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

We try to attack by using "p and $-p$ attack".

Let $M := \boldsymbol{R}(u\mathbf{1}+vB+wH)\boldsymbol{R}^{-1} \in O$.

Let a plaintext $p \in \boldsymbol{Z}/q\boldsymbol{Z}$ and numbers $u,v,w \in \boldsymbol{Z}/q\boldsymbol{Z}$, such that

$$p=k(u+2v\, b_0)s+h(u+2b_0w)t = u+2v\, b_0\, ks+2b_0w\, ht \bmod q.$$

Let $E(p, X)$ be the ciphertext of p.

By using simple style expression of $E(p, X)$ we have

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

Let $E(-p, X)$ be the ciphertext of $-p$.

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

where

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

$$-p=k(u'+2v'\, b_0)s+h(u'+2b_0w')t,$$

$$u',v',w' \in \boldsymbol{Z}/q\boldsymbol{Z}.$$

Then we have

$$p - p=k(u+2v\, b_0)s+h(u+2b_0w)t+ k(u'+2v'\, b_0)s+h(u'+2b_0w')t$$

$$=(u+u')+2\,b_0ks\,(v+v')+2b_0h\,t(w+w')=0 \bmod q\in \boldsymbol{Z}/q\boldsymbol{Z}.$$

$$(u+u')=-2\,b_0ks\,(v+v')-2b_0h\,t(w+w') \bmod q. \qquad (49)$$

We have

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

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

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

$$=\boldsymbol{A}([\boldsymbol{R}(-2b_0ks(v+v')\mathbf{1}-2b_0ht(w+w')\mathbf{1}+(v+v')B+(w+w')H)\boldsymbol{R}^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}])\boldsymbol{Z}^{-1})$$

$$=\boldsymbol{A}([\boldsymbol{R}((B-2b_0\,ks\,\mathbf{1})(v+v')+(H-2b_0\,ht\,\mathbf{1})(w+w'))\boldsymbol{R}^{-1}][(\boldsymbol{A}^{-1}X)\boldsymbol{Z}])\boldsymbol{Z}^{-1})$$

$$\neq \mathbf{0} \bmod q \text{ (in general).}$$

[Theorem 9]

Even if $|M|^2=|\boldsymbol{R}(u\mathbf{1}+vB+wH)\boldsymbol{R}^{-1}|^2=0 \bmod q$, p exists such that $p\neq 0 \bmod q$,

where

$$p=k(u+2v\,b_0)s+h(u+2b_0w)t=u+2\,b_0vks+2b_0w\,ht \bmod q,$$

$$u,v,w\in \boldsymbol{Z}/q\boldsymbol{Z}.$$

(*Proof*:)

$$|M|^2=|\boldsymbol{R}(u\mathbf{1}+vB+wH)\boldsymbol{R}^{-1}|^2 \quad \bmod q$$

$$=|u\mathbf{1}+vB+wH|^2 \bmod q$$

$$=(u+b_0v+b_0w)^2+(v-w)^2(b_1^2+\ldots+b_7^2)$$

$$=(u+b_0v+b_0w)^2+(v-w)^2(-b_0^2)$$

$$=((u+b_0v+b_0w)+(v-w)b_0)\,((u+b_0v+b_0w)-(v-w)b_0) \bmod q$$

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

We solve the above equation to obtain 4 solutions.

1) $u+2b_0v=0 \bmod s$, and $u+2b_0v=0 \bmod t$,
2) $u+2b_0w=0 \bmod s$, and $u+2b_0w=0 \bmod t$,
3) $u+2b_0v=0 \bmod s$ and $u+2b_0w=0 \bmod t$,
4) $u+2b_0v=0 \bmod t$ and $u+2b_0w=0 \bmod s$.

In case that $u+2b_0v=0 \bmod s$, and $u+2b_0v=0 \bmod t$,

$$p=k(u+2v\, b_0)s+h(u+2b_0w)t = h(u+2b_0w)t \neq 0 \bmod q \text{ (in general).}$$

In case that $u+2b_0w=0 \bmod s$, and $u+2b_0w=0 \bmod t$,

$$p=k(u+2v\, b_0)s+h(u+2b_0w)t = k(u+2b_0v)s \neq 0 \bmod q \text{ (in general).}$$

In case that $u+2b_0v=0 \bmod s$ and $u+2b_0w=0 \bmod t$,

$$p=k(u+2v\, b_0)s+h(u+2b_0w)t = \alpha' sks+\beta' tht \neq 0 \bmod q$$

$$= \alpha ks+\beta ht \neq 0 \bmod q \text{ (in general),}$$

where $\alpha,\ \alpha',\ \beta,\ \beta' \in \boldsymbol{Z}/q\boldsymbol{Z}$.

In case that $u+2b_0v=0 \bmod t$ and $u+2b_0w=0 \bmod s$,

$$p=k(u+2v\, b_0)s+h(u+2b_0w)t = k\alpha' ts+h\beta' st = 0 \bmod q.$$

q.e.d.

(Numerical example in case that $u+2b_0v=0 \bmod s$ and $u+2b_0w=0 \bmod t$)

Given s=7, t=11,q=77,b_0=17,k=8,h=2, (8*7+2*11=1 mod 77).

When u=38, then

$v=(-u)(2b_0)^{-1} \bmod 7=4*6=3 \bmod 7$,

$w=(-u)(2b_0)^{-1} \bmod 11=6*1=6 \bmod 11$,

$p=k(u+2\, b_0v)s+h(u+2b_0w)t=8(38+2*17*3)*7+2*(38+2*17*6)*11 \bmod 77=74$,

$|M|^2=|\boldsymbol{R}(u\mathbf{1}+vB+wH)\boldsymbol{R}^{-1}|^2 \quad \bmod q$,

$=|u\mathbf{1}+vB+wH|^2 \bmod q$,

$=(u+2b_0v)\ (u+ 2b_0w) =(38+2*17*3)(38+2*17*6)=63*11=0 \bmod 77.$

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

Let

$$p=k(u+2v\ b_0)s+h(u+2b_0w)t = u+2v\ b_0\ ks+2b_0w\ ht \bmod q,$$

$$p'=-p=k(u'+2v'\ b_0)s+h(u'+2b_0w')t = u'+2\ b_0v'\ ks+2b_0w'ht \bmod q,$$

we have

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

$$=|\ E(p, \mathbf{1})+ E(p', \mathbf{1})\ |^2=|\ E(p, \mathbf{1})+ E(-p, \mathbf{1})\ |^2=|\ E(p - p\ ,\mathbf{1})\ |^2=|\ E(0, \mathbf{1})\ |^2$$

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

$$=|\ (B-2b_0\ ks\ \mathbf{1})(v+v') + (H-2b_0\ ht\ \mathbf{1})(w+w')\ |\ ^2 \bmod q \quad \text{(from (49))}$$

$$=[(b_0-2\ b_0\ ks)\ (v+v') + (b_0-2b_0\ ht\ )(w+w')]^2+(b_1(v+v')\ -b_1(w+w'))^2+\ldots$$

$$+(b_7(v+v')\ -b_7(w+w'))^2 \bmod q$$

$$=[(b_0(ht-ks)\ (v+v') + b_0(sk-ht)(w+w')]^2+(b_1(v+v')\ -b_1(w+w'))^2+\ldots$$

$$+(b_7(v+v')\ -b_7(w+w'))^2 \bmod q$$

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

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

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

$$= 0 \bmod q.$$

But from Theorem 9 there exist many tuples of plaintexts (p, p') such that

$p+ p'\neq 0 \bmod q$ and $|\ E(p, \mathbf{1})+ E(p', \mathbf{1})\ |^2= |\ E(p +p', \mathbf{1})\ |^2=0 \bmod q$.

Then it is said that the attack by using “p and $-p$ attack” is not efficient in general.

We can not easily distinguish the ciphertexts of p and $-p$.

§5. 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 side of the composite number is as large as 2^{2000}. Then we need to select modulus $O(q)=2^{2000}$.

1) In case of $k=8$, $O(q)=2^{2000}$, the size of $e_{ij}\in \boldsymbol{Z}/q\boldsymbol{Z}(i,j=0,\ldots,7)$ which are the coefficients of elements in $E(p,X)=\boldsymbol{A}((M[(\boldsymbol{A}^{-1}X)\boldsymbol{Z}])\boldsymbol{Z}^{-1}) \bmod q\in O[X]$ is $(64)(\log_2 q)$bits =128kbits, and the size of system parameters q is 2000bits.
2) In case of $k=8$, $r=8$, $O(q)=2^{2000}$, the complexity to obtain $E(p,X)$ is $(32*512+8)(\log_2 q)^2+ K_{AZ} = 2^{38}$ bit-operations,

where

$K_{AZ}=16*16*(\log_2 q)^2+16*(\log_2 q)^3=2^{37}$ bit-operations is the complexiy required for inverse of $\boldsymbol{A}^{-1}$ and $\boldsymbol{Z}^{-1}$.

3) 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

$$(A_k\,((\ldots((A_1^{-1}\,C\,)Z_1))\,Z_2))\ldots.))Z_k = M[(A_k^{-1}((\ldots((A_1^{-1}\mathbf{1})Z_1))\ldots))Z_k] \bmod q,$$

$$M=[(A_k\,((\ldots((A_1^{-1}\,C\,)Z_1))\,Z_2))\ldots))\,Z_k][(A_k^{-1}((\ldots((A_1^{-1}\mathbf{1})Z_1))\ldots))Z_k]^{-1} \bmod q.$$

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

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

$$k(m_0'+ m_1'\,b_0/\,b_1)s+h(m_0'- m_1'\,b_0/\,b_1)t \bmod q=p\,.$$

Then the complexity G required for deciphering is

$(16*64+15*64+1+16*64)(\log_2 q)^2+K_{AZ}+(1+8)*(\log_2 q)^3+ 8*(\log_2 q)^2$
$= 2^{38}$ bit-operations.

4) The complexity required for addition/subtraction operation on ciphertexts , $E(p_1, X)\pm E(p_2, X)$ has no multiplication.

5) The complexity G_M required for multiplication operation on ciphertexts, $E(p_1, E\,(p_2,X))$ is $(8*8*8)(\log_2 n)^2= 2^{31}$.

On the other hand the complexity required for enciphering and deciphering in RSA scheme is $O(2(\log n)^3) = 2^{34}$ bit-operations and the complexity required for multiplication operation $a^{m_1 m_2} \bmod n$ in RSA scheme is $O(2(\log n)^3)=2^{34}$ bit-operations where the modulus n is 2048-digit composite number.

Though our scheme requires memory space larger than RAS scheme and the complexity required to encipher and decipher is as large as RSA scheme, the complexity G_M required for multiplication operation on ciphertexts is less than RSA.

§6. Conclusion

We proposed the new fully homomorphism encryption scheme based on the octonion ring over finite ring. 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. We proved that if there exists the PPT algorithm that decrypts the plaintext from the ciphertexts of the proposed scheme, there exists the PPT algorithm that factors the given composite number modulus.

§7. Acknowledgments

In this paper we have proposed the scheme which we improve the encryption scheme described in 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. Saarbrücken/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/.
[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] 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:

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 $[M]_i$ denotes the i-th element of $M\in O$.

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

$=\{ a_0(a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3)$

$-a_1(a_0b_0-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7)$

$-a_2(a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5)$

$-a_3(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0)$

$+a_4(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6)$

$- a_5(a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2)$

$+a_6(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4\ )$

$+a_7(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)\}\ /|A|^2 \bmod q$

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

Similarly we have

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

Then

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