Fully Homomorphic Public-Key Encryption with Two Ciphertexts based on Discrete Logarithm Problem

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

Abstract. In previous paper I proposed the fully homomorphic public-key encryption based on discrete logarithm problem which may be vulnerable to "*m* and -*m* attack". In this paper I propose improved fully homomorphic public-key encryption (FHPKE) with composite number modulus based on the discrete logarithm assumption (DLA) and computational Diffie–Hellman assumption (CDH) of multivariate polynomials on octonion ring which is immune from "*m* and -*m* attack". The scheme has two ciphertexts corresponding to one plaintext.
keywords: fully homomorphic public-key encryption, discrete logarithm assumption, computational Diffie–Hellman assumption, octonion ring, factorization

§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, that is, we can construct the 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.

Gentry's bootstrapping technique is the most famous method of obtaining fully homomorphic encryption. In 2009 Gentry 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[5],[6]. Some fully homomorphic encryption schemes were proposed until now [7], [8], [9], [10], [11].

But Gentry's solution was to use a second layer of encryption, essentially to protect intermediate results when the system broke down and needed to be reset. In

Gentry's scheme and so on a task like finding a piece of text in an e-mail requires chaining together thousands of basic operations.

In previous works I proposed some fully homomorphic encryptions [1],[2],[3], [13], [14]. But these encryption schemes may be vulnerable to "*m* and -*m* attack".

In this paper I propose the fully homomorphic public-key encryption (FHPKE) with composite number modulus based on the discrete logarithm assumption (DLA) and computational Diffie–Hellman assumption (CDH) of multivariate polynomials on octonion ring which is immune from "*m* and -*m* attack". The scheme has two ciphertexts corresponding to one plaintext. Since the complexity for enciphering and deciphering become to be small enough to handle, the cryptosystem runs fast.

§2. Preliminaries for octonion operation

In this section we describe the operations on octonion ring and properties of octonion ring. The readers who understand the property of octonion may skip the section 2.

§2.1 Multiplication and addition on the octonion ring O

Let $r=pq$ be a composite number modulus to be as large as 2^{2000} where p and q are primes. Later (in section 6) we discuss the size of one of the system parameters, r.

Let O ,O_p and O_q be the octonion [4] rings over a residue class ring $R=\boldsymbol{Z}/r\boldsymbol{Z}$, $R_p=\boldsymbol{Z}/p\boldsymbol{Z}$, and $R_q=\boldsymbol{Z}/q\boldsymbol{Z}$ each such that

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

$$O_p=\{(a_0,a_1,\ldots,a_7) \mid a_j \in R_p\ (j=0,1,\ldots,7)\} \tag{1-1b}$$

$$O_q=\{(a_0,a_1,\ldots,a_7) \mid a_j \in R_q\ (j=0,1,\ldots,7)\} \tag{1-1c}$$

where

$$R=\boldsymbol{Z}/r\boldsymbol{Z},$$

$$R_p=\boldsymbol{Z}/p\boldsymbol{Z},$$

$$R_q=\boldsymbol{Z}/q\boldsymbol{Z}.$$

From Chinese remainder theorem $k \in R$ and $h \in R$ exist such that

$$pk+qh=1 \bmod r. \tag{2}$$

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

$$A=(a_0,a_1,\ldots,a_7),\ a_j \in R\ (j=0,1,\ldots,7), \tag{3a}$$

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

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

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

Let

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

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

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

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,

$$A^{J+1} = A \bmod r \in O.$$

Theorem 1

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

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

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

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

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

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

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

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

(*Proof*:)

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

Theorem 2

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

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

where

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

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

(*Proof*:)

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

In the same manner we have

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

$$A^{Jp+1}=A \bmod p,$$

where

$$Jp= \text{LCM}\ \{p^2-1,\ p-1\}=p^2-1,$$

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

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

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

where

$$J=\mathrm{LCM}\{Jp,Jq\}=\mathrm{LCM}\{p^2-1,q^2-1\}.$$

§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 r.

1) Non-commutative

$$AB\neq BA \bmod r.$$

2) Non-associative

$$A(BC)\neq(AB)C \bmod r.$$

3) Alternative

$$(AA)B=A(AB) \bmod r, \tag{11}$$

$$A(BB)=(AB)B \bmod r, \tag{12}$$

$$(AB)A=A(BA) \bmod r. \tag{13}$$

4) Moufang's formulae [4],

$$C(A(CB))=((CA)C)B \bmod r, \tag{14}$$

$$A(C(BC))=((AC)B)C \bmod r, \tag{15}$$

$$(CA)(BC)=(C(AB))C \bmod r, \tag{16}$$

$$(CA)(BC)=C((AB)C) \bmod r. \tag{17}$$

5) For positive integers n,m, we have

$$(AB)B^n=((AB)B^{n-1})B=A(B(B^{n-1}B))=AB^{n+1} \bmod r, \tag{18}$$

$$(AB^n)B=((AB)B^{n-1})B=A(B(B^{n-1}B))=AB^{n+1} \bmod r, \tag{19}$$

$$B^n(BA)=B(B^{n-1}(BA))=((BB^{n-1})B)A=B^{n+1}A \bmod r, \tag{20}$$

$$B(B^n A)=B(B^{n-1}(BA))= ((BB^{n-1})B)A=B^{n+1}A \bmod r. \quad (21)$$

From (15) and (19), we have

$$(AB^n)B^2=[((AB)B^{n-1})B]B=[(A(B\,(B^{n-1}B))]B =(AB^{n+1})B= AB^{n+2} \bmod r,$$

$$(AB^n)B^3=[((AB)B^{n-1})B]B^2=[(A(B(B^{n-1}B))]B^2= (AB^{n+1})B^2= AB^{n+3} \bmod r,$$

… …

$$(AB^n)B^m= AB^{n+m} \bmod r.$$

In the same manner we have

$$B^m(B^n A)= B^{n+m}A \bmod r.$$

6) **Lemma 1**

$$A(B((AB)^n))=(AB)^{n+1} \bmod r,$$

$$(((AB)^n)A)B =(AB)^{n+1} \bmod r.$$

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

(*Proof*:)

From (14) we have

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

Then

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

$$A(B(AB)^n)= (AB)^{n+1} \bmod r.$$

In the same manner we have

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

7) **Lemma 2**

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

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

(*Proof*:)

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

8) **Lemma 3**

$$A(BA^{-1}) = (AB)A^{-1} \bmod r.$$

(*Proof*:)

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

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

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

We multiply A from left side ,

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

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

$$ABA^{-1}.$$

9) From (13) and **Lemma 2** we have

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

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

10) **Lemma 4**

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

(*Proof*:)

From (17),

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

11) **Lemma 5**

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

(*Proof*:)

From (17),

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

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

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

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

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

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

$$= A^{-1}\ \{[(A((AB)(A^{-1}(AB)))]A^{-1}\} \mod r$$

$$= A^{-1}\ \{[(A((AB)B))]A^{-1}\} \mod r$$

$$= A^{-1}\ \{[A(A(BB))]A^{-1}\} \mod r$$

$$=\{\ A^{-1}\ [A(A(BB))]\}A^{-1} \mod r$$

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

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

12) **Lemma 6**

$$(AB^mA^{-1})(\ AB^nA^{-1}\ )= AB^{m+n}A^{-1} \mod r.$$

(*Proof*:)

From (16),

$$[A^{-1}\ (A^2(B^mA^{-1}))][(AB^n)A^{-1}]= \{A^{-1}\ [(A^2(B^mA^{-1}))(AB^n)]\}A^{-1} \mod r$$

$$= A^{-1}\{\ [(A(A(B^mA^{-1}))(AB^n)]A^{-1}\} \mod r$$

$$= A^{-1}\{\ [(A((AB^m)A^{-1}))(AB^n)]A^{-1}\} \mod r$$

$$= A^{-1}\ \{\ [((A(AB^m))A^{-1}))(AB^n)]\ A^{-1}\} \mod r$$

$$= A^{-1}\ \{\ [((A^2B^m)A^{-1}))(AB^n)]\ A^{-1}\} \mod r.$$

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

$$= A^{-1}\ \{\ (A^2B^m)[A^{-1}((AB^{\mathrm{n}})A^{-1})]\} \mod r$$

$$= A^{-1}\ \{\ (A^2B^m)[A^{-1}(A(B^nA^{-1}))]\} \mod r$$

$$= A^{-1}\ \{\ (A^2B^m)(B^nA^{-1})\} \mod r$$

$$= A^{-1}\ \{\ (A^{-1}(A^3B^m))(B^nA^{-1})\} \mod r.$$

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

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

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

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

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

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

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

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

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

Theorem 3

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

where

$$^{\exists}w,v \in \boldsymbol{R},$$

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

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

(*Proof*:)

$$A^2 \mod r$$

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

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

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

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

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

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

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

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

$$=(2a_0^2- L_A \mod r, 2a_0a_1 \mod r, 2a_0a_2 \mod r, 2a_0a_3 \mod r,$$

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

where

$$L_A= a_0^2+a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2 \mod r.$$

Now we try to obtain $u, v \in \boldsymbol{R}$ that satisfy $A^2=w\mathbf{1}+vA \mod r$.

$$w\mathbf{1}+vA= w(1,0,0,0,0,0,0,0)+v(a_0,a_1,\ldots,a_7) \mod r,$$

$$A^2 = (2a_0^2 - L_A \bmod r,\ 2a_0a_1 \bmod r,\ 2a_0a_2 \bmod r,\ 2a_0a_3 \bmod r,$$
$$2a_0a_4 \bmod r, 2\ a_0a_5 \bmod r, 2a_0a_6 \bmod r,\ 2a_0a_7 \bmod r).$$

Then we have

$$A^2 = w\mathbf{1} + vA = -L_A\ \mathbf{1} + 2\ a_0A \bmod r,$$

$$w = -L_A \bmod r,$$

$$v = 2a_0 \bmod r. \qquad \text{q.e.d.}$$

14) **Theorem 4**

$$A^t = w_t\mathbf{1} + v_tA \bmod r$$

where t is an integer and $w_t, v_t \in R$.

(*Proof*:)

From **Theorem 3**

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

If we can express A^t such that

$$A^t = w_t\mathbf{1} + v_tA \bmod r \in O\ ,\ w_t, v_t \in R,$$

Then

$$A^{t+1} = (w_t\mathbf{1} + v_tA)A \bmod r$$
$$= w_tA + v_t(-L_A\ \mathbf{1} + 2\ a_0A\ ) \bmod r$$
$$= -L_A\ v_t\mathbf{1} + (\ w_t + 2a_0v_t)A \bmod r.$$

We have

$$w_{t+1} = -L_A\ v_t \bmod r \in R,$$

$$v_{t+1} = w_t + 2a_0v_t \bmod r \in R. \quad \text{q.e.d.}$$

We can use **Power** (A,n,r) to obtain $A^n \bmod r$. (see the **Appendix E**)

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=**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.

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

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

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

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

(*Proof*:)

If D exists, we have at X=**1**

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

Then

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

We substitute C to X to obtain

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

From (13)

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

Multiplying C^{-1} from left side,

$$B(AC)=(BA)C \bmod r \tag{26}$$

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

17) **Theorem 7**

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

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

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

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

$$C(BA) \neq (CB)A \bmod r. \tag{27}$$

(*Proof*:)

If D and E exist, we have at X=**1**

$$C(BA)=ED \bmod r \tag{28}$$

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

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

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

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

$$ED =(CB)A \bmod r. \tag{29}$$

From (28) and (29) we have

$$C(BA) =(CB)A \bmod r. \tag{30}$$

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

18) **Theorem 8**

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

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

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

(*Proof*:)

If D exists, we have at X=**1**

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

Then

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

We can select $C \in O$ such that

$$(BA^{-1})(CA^2) \neq (BA^{-1})C)A^2 \bmod r. \tag{31}$$

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

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

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

From **Lemma 3**

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

From (17)

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

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

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

From **Lemma 3**

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

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

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

From (15) we have

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

Multiply A from right side we have

$$((BA^{-1})(CA^2)=((BA^{-1})C)A^2 \bmod r. \tag{32}$$

(32) is contradictory to (31). q.e.d.

§3. Preparation for fully homomorphic public-key encryption scheme

§3.1 Definition of homomorphic public-key encryption

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

In this work, the plaintext $m \in R(=Z/rZ)$ of the encryption schemes will be the element in finite 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}, system parameters $(r,A,B;F(X))$ where $r=pq$ and p and q are secret large primes, outputs (**pk**, **sk**) ← **KeyGen**$(1^{\lambda},r)$, where **pk** is a public encryption key and **sk** is a secret decryption key.

-Encryption. The algorithm **Enc**, on input system parameters $(r,A,B;F(X))$, public key **pk**, and a plaintext $m \in R$, components of plaintext $u,v \in R$, random noises $w,z \in R$, outputs a ciphertext $C=({}^1C,{}^2C) \in O[X]^2$ ←**Enc**(**pk**; m) where $F(X) \in O[X]$.

-Decryption. The algorithm **Dec**, on input system parameters $(r,A,B;F(X))$, secret key **sk** and a ciphertext $C=({}^1C,{}^2C) \in O[X]^2$, outputs a plaintext m^*←**Dec**(**sk**;C).

-Homomorphic-Evaluation. The algorithm **Eval**, on input system parameters $(r,A,B;F(X))$, an arithmetic circuit ckt, and a tuple of $2 \times n$ ciphertexts $(C_1,\ldots, C_n) \in \{O[X]\}^{2\times n}$, outputs a ciphertext $C' =({}^1C',{}^2C') \in O[X]^2$←**Eval**(ckt; $C_1,\ldots, C_n$).

§3.2 Definition of fully homomorphic public-key encryption

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

Definition (**Fully homomorphic public-key encryption**). A homomorphic public-key encryption scheme FHPKE :=(**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 (**pk**,**sk**) ←**KeyGen**$(1^{\lambda},r)$, $\forall$ ckt $\in$ CR_{λ}, $\forall (m_1,\ldots, m_n) \in R^n$ where $n = n(\lambda)$, $\forall (C_1,\ldots,C_n)$ where C_i← **Enc**(**pk**;m_i), it holds that:

$$\Pr[\textbf{Dec}(\textbf{sk};\textbf{Eval}(\text{ckt}; C_1,\ldots,C_n)) \neq \text{ckt}(m_1,\ldots, m_n)] = \text{negl}(\lambda).$$

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 Basic function

We consider the basic function before we propose a fully homomorphic public-key encryption (FHPKE) scheme based on the enciphering/deciphering functions on octonion ring over R

Let r be a composite number modulus selected by cloud data centre or system centre where $r=pq$, p and q are secret large primes.

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

Let $F(X)$ be a basic function.

S_i , $T_i\in O$ are selected randomly by cloud data centre or system centre. such that S_i^{-1} mod r and T_i^{-1} mod r exist (i=1,...,k).

Basic function $F(X)$ is defined as follows.

$$F(X):= ((S_k((\ldots((S_1X)T_1))\ldots))T_k \bmod r\in O[X] ,$$

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

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

$$\ldots. \quad \ldots.$$

$$f_{70}x_0+f_{71}x_0+ \ldots+f_{77}x_7) \bmod r,$$

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

with $f_{ij}\in R$ (i,j=0,…,7) which is published.

§3.4 Square root on composite number modulus

We discuss the calculation for the square root on composite modulus r.

Let $x\in R$ be the square root of $a\in R$. That is, $x^2=a$ mod r.

Here we consider to find the square root of a. We obtain next Theorem 9.

[Theorem 9]
If there exists the PPT algorithm **AL1** for obtaining the square root of a on composite modulus r, there exists the PPT algorithm that factorizes modulus r where a is a quadratic residue on modulus r.
(*Proof*:)
Let $e\in R$ be any element in R.

We can express e and e^2 mod r such that

$$e=e_q kp+e_p hq \bmod r,\ e_q \in R_q\ ,e_p \in R_p,$$

$$e^2=(e_q kp+e_p hq\ )^2 \bmod r,$$

$$=e_q{}^2 kp+e_p{}^2 hq \bmod r,$$

By using the PPT algorithm **AL1** we can obtain e' which is one of e_i (i=0,1,2,3), the square root of e^2 on composite modulus r such that

$$e_0=e_q kp+e_p hq \bmod r,$$

$$e_1=e_q kp-e_p hq \bmod r,$$

$$e_2=-e_q kp+e_p hq \bmod r,$$

$$e_3=-e_q kp-e_p hq \bmod r.$$

As

$$\mathrm{GCD}(e+e_1,r)=\mathrm{GCD}(2\ e_q kp, pq)=p,$$

$$\mathrm{GCD}(e+e_2,r)=\mathrm{GCD}(2\ e_p hq, pq)=q,$$

the composite number r is factorized with 1/2 of probability. q.e.d.

§4. Fully homomorphic public-key encryption scheme

§4.1 Public-key enciphering function

Here we construct the public-key encryption scheme by using the basic function $F(X)$

$$F(X)=(S_k((\ldots((S_1X)T_1))\ldots))T_k \bmod r\in O[X]\ ,$$

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

Anyone can calculate $F^{-1}(X)$, the inverse function of $F(X)$ such that

$$F^{-1}(X):=S_1{}^{-1}((\ldots((S_k{}^{-1}(XT_k{}^{-1}))\ldots))\ T_1{}^{-1}) \bmod r\in O[X]\ ,$$

$$=(g_{00}x_0+\ \ldots+g_{07}x_7,$$

$$g_{10}x_0+\ldots+g_{17}x_7,$$

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

$$g_{70}x_0+\ \ldots+g_{77}x_7) \bmod r,$$

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

with $g_{ij}\in \boldsymbol{R}$ (i,j =0,…,7).

ALINVF denote the algorithm for calculating the inverse function of $F(X)$.

We can calculate $F^{-1}(X) \in O[X]$ which is the inverse function of $F(X)$, given $F(X) \in O[X]$.

[**ALINVF**]

Given $F(X)$ and r,

$$
\begin{aligned}
F(F^{-1}(X)) &= F^{-1}(F(X)) = X \bmod r \in O[X] \\
&= (f_{00}(g_{00}x_0 + \ldots + g_{07}x_7) + \ldots + f_{07}(g_{70}x_0 + \ldots + g_{77}x_7), \\
&\quad f_{10}(g_{00}x_0 + \ldots + g_{07}x_7) + \ldots + f_{17}(g_{70}x_0 + \ldots + g_{77}x_7), \\
&\qquad \ldots \qquad \ldots \\
&\quad f_{70}(g_{00}x_0 + \ldots + g_{07}x_7) + \ldots + f_{77}(g_{70}x_0 + \ldots + g_{77}x_7)) \bmod r, \\
&= ((f_{00}g_{00} + \ldots + f_{07}g_{70})x_0 + \ldots + (f_{00}g_{07}x_0 + \ldots + f_{07}g_{77})x_7, \\
&\quad (f_{10}g_{00} + \ldots + f_{17}g_{70})x_0 + \ldots + (f_{10}g_{07}x_0 + \ldots + f_{17}g_{77})x_7, \\
&\qquad \ldots \qquad \ldots \\
&\quad (f_{70}g_{00} + \ldots + f_{77}g_{70})x_0 + \ldots + (f_{70}g_{07}x_0 + \ldots + f_{77}g_{77})x_7) \bmod r, \\
&= X = (x_0, \ldots, x_7).
\end{aligned}
$$

Then we obtain

$$
\left.
\begin{aligned}
f_{00}g_{00} + \ldots + f_{07}g_{70} &= 1 \bmod r \\
f_{10}g_{00} + \ldots + f_{17}g_{70} &= 0 \bmod r \\
\ldots \qquad & \ldots \\
f_{70}g_{00} + \ldots + f_{77}g_{70} &= 0 \bmod r
\end{aligned}
\right\}
$$

g_{i0}(i=0,…,7) is obtained by solving above simultaneous equation.

$$
\left.
\begin{aligned}
f_{00}g_{01} + \ldots + f_{07}g_{71} &= 0 \bmod r \\
f_{10}g_{01} + \ldots + f_{17}g_{71} &= 1 \bmod r \\
\ldots \qquad & \ldots \\
f_{70}g_{01} + \ldots + f_{77}g_{71} &= 0 \bmod r
\end{aligned}
\right\}
$$

g_{i1}(i=0,…,7) is obtained by solving above simultaneous equation.

....

$$\begin{cases} \cdots\cdots \\ f_{00}g_{07}+\ldots+f_{07}g_{77}=0 \bmod r \\ f_{10}g_{07}+\ldots+f_{17}g_{77}=0 \bmod r \\ \cdots\cdots \\ f_{70}g_{07}+\ldots+f_{77}g_{77}=1 \bmod r \end{cases}$$

$g_{i7}(i=0,\ldots,7)$ is obtained by solving above simultaneous equations.

Then we have $F^{-1}(X)$ from $F(X)$ and r. □

We define $F^{i}(X)$ and $F^{-i}(X)$ as follows where i is a positive integer.

$$F^2(X):=F(F(X)) \bmod r,$$

$$\cdots\cdots$$

$$F^{i}(X):=F(F^{i-1}(X)) \bmod r,$$

$$F^{-2}(X):=F^{-1}(F^{-1}(X)) \bmod r,$$

$$\cdots\cdots$$

$$F^{-i}(X):=F^{-1}(F^{-(i-1)}(X)) \bmod r.$$

The cloud data centre or system centre publishes the system parameters $(r,A,B;F(X))$.

We consider the communication between user U and user V. User U downloads the system parameters $(r,A,B;F(X))$ from cloud data centre or system centre. User U selects the random integer $a\in Z$ to be secret and generates the public function $F^a(X)$ by using algorithm **Power**$(F(X),a,r)$. (see the **Appendix F**)

User U sends the coefficient of $F^a(X)$, $f_{aij}\in R$ $(i,j=0,\ldots,7)$ to cloud data centre or system centre as the public-key of user U.

On the other hand user V downloads the system parameters $(r,A,B;F(X))$ and selects the random integer $b\in Z$ to be secret and generates the public function $F^b(X)$ by using algorithm **Power**$(F(X),b,r)$. User V sends the coefficient of $F^b(X)$, $f_{bij}\in R$ $(i,j=0,\ldots,7)$ to cloud data centre or system centre as the public-key of user V.

User V tries to send to user U the ciphertexts of the plaintexts which user V possesses. User V downloads the public-key of user U, $F^a(X)$, $f_{aij}\in R$ $(i,j=0,\ldots,7)$ from

cloud data centre or system centre.

User V calculates $F^{-a}(X)$ from $F^{a}(X)$ by using **ALINVF**.

User V generates the common enciphering function $F_{VU}(X,Y)$ between user U and user V as follows. By using algorithm **Power**($F^{a}(X),b,r$) user V obtain $F^{ab}(X)$.

User V obtain $F^{-ab}(X)$ from $F^{ab}(X)$ by using **ALINVF**.

Then user V generates $F_{VU}(X,Y)$, the common enciphering function of user U and user V such that

$$F_{VU}(X,Y):= F^{-ab}(YF^{ab}(X)) \bmod r \in O[X,Y]$$

In the same manner user U generates the common enciphering function

$$F_{UV}(X,Y):= F^{-ba}(YF^{ba}(X)) \bmod r \in O[X,Y]$$

where

$$F_{VU}(X,Y)= F_{UV}(X,Y) \bmod r.$$

We notice that

$$F_{VU}(X,\mathbf{1}) = F^{-ba}(\mathbf{1}F^{ba}(X))= F^{-ba}(F^{ba}(X))= X \bmod r.$$

User V confirms the system parameters ($r,A,B;F(X)$) from the cloud data centre or system centre where

$$A=(a_0,a_1,a_2,\ldots,a_7)\in O\ ,$$

$$B=(b_0,b_1,b_2,\ldots,b_7)\in O,$$

$$C=(1-a_0,-a_1,-a_2,\ldots,-a_7)\in O\ ,$$

$$L_A:=|A|^2= a_0^2+a_1^2+\ldots+a_7^2=0 \bmod r,$$

$$a_0=1/2 \bmod q,$$

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

$$b_0=0 \bmod r,$$

$$a_1b_1+\ldots+a_7b_7=0 \bmod r.$$

$$A+C=\mathbf{1} \bmod r,$$

$$L_C:=|C|^2=(1-a_0)^2+a_1{}^2+\ldots+a_7{}^2=0 \bmod r.$$

From Theorem 3 we have

$$A^2=-L_A\mathbf{1}+2\,a_0A=A \bmod r,$$

$$B^2=-L_B\mathbf{1}+2\,b_0B=\mathbf{0} \bmod r,$$

$$C^2=-L_C\mathbf{1}+2(1-a_0)C=C \bmod r,$$

$$[AB]_0=[BA]_0=a_0\,b_0-(a_1b_1+\ldots+a_7b_7)=0 \bmod r, \tag{33a}$$

$$[CB]_0=[BC]_0=(1-a_0)b_0+(a_1b_1+\ldots+a_7b_7)=0 \bmod r, \tag{33b}$$

$$L_{AB}=L_AL_B=L_{BA}=0 \bmod r,$$

$$L_{CB}=L_CL_B=L_{BC}=0 \bmod r,$$

$$(AB)^2=-L_{AB}\mathbf{1}+2\,[AB]_0AB=0\mathbf{1}+0AB=\mathbf{0} \bmod r,$$

$$(CB)^2=-L_{CB}\mathbf{1}+2\,[CB]_0CB=0\mathbf{1}+0CB=\mathbf{0} \bmod r,$$

$$(BA)^2=-L_{BA}\mathbf{1}+2\,[BA]_0BA=\mathbf{0} \bmod r,$$

$$(BC)^2=-L_{BC}\mathbf{1}+2\,[BC]_0BC=\mathbf{0} \bmod r.$$

Theorem 10

$$(AB)A=\mathbf{0} \bmod r, \tag{34a}$$

$$(BA)B=\mathbf{0} \bmod r. \tag{34b}$$

(*Proof*:)

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

Theorem 11

$$AB+BA=B \bmod r. \tag{35}$$

(*Proof*:)

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

Theorem 12

$$(AB)(BA) = \mathbf{0} \bmod r, \tag{36a}$$

$$(BA)(AB) = \mathbf{0} \bmod r. \tag{36b}$$

(*Proof*:)

From (17)

$$(AB)(BA) = (A(BB))A = (A(\mathbf{0}))A = \mathbf{0} \bmod r,$$

$$(BA)(AB) = (B(AA))B = (B(A))B = \mathbf{0} \bmod r. \quad \text{q.e.d.}$$

§4.2 Medium text

Here user V calculates the medium text ${}^1M$ and ${}^2M$ from the plaintext m which user V possesses as follows.

Let $m \in R$ be a plaintext.

Let $u, v \in R$ be the components of the plaintext m such that

$$m = u + v \bmod r.$$

Let $w, z \in R$ be random noises.

The medium text ${}^1M$ and ${}^2M$ are defined by

$${}^1M := uA + vC + {}^1wAB + {}^1zBA \bmod r \in O,$$

$${}^2M := vA - uC + {}^2wAB + {}^2zBA \bmod r \in O,$$

$$m := u + v \bmod r \in R$$

$$= 2[{}^1M]_0 \bmod r.$$

As

$A^2 = A \bmod r$, $AC = \mathbf{0} \bmod r$, $A(AB) = AB \bmod r$, $A(BA) = \mathbf{0} \bmod r$,

$CA = \mathbf{0} \bmod r$, $C^2 = C \bmod r$, $C(AB) = \mathbf{0} \bmod r$, $C(BA) = BA \bmod r$,

$(AB)A = \mathbf{0} \bmod r$, $(AB)C = AB \bmod r$, $(AB)^2 = \mathbf{0} \bmod r$, $(AB)(BA) = \mathbf{0} \bmod r$,

$(BA)A = BA \bmod r$, $(BA)C = \mathbf{0} \bmod r$, $(BA)(AB) = \mathbf{0} \bmod r$, $(BA)^2 = \mathbf{0} \bmod r$,

we have

$$({}^1M)^2=(uA+vC+{}^1wAB+{}^1zBA)\,(uA+vC+{}^1wAB+{}^1zBA) \bmod r$$

$$=u^2A+u{}^1wAB+v^2C+v{}^1zBA+v{}^1wAB+u{}^1zBA$$

$$=-uv\mathbf{1}+(u+v)\,(uA+vC+{}^1wAB+{}^1zBA)$$

$$=-uv\mathbf{1}+(u+v)\,{}^1M \bmod r.$$

On the other hand from Theorem 3

$$({}^1M)^2=-L_{1M}\mathbf{1}+2[{}^1M]_0\,{}^1M \bmod r.$$

From $[{}^1M]_0=ua_0+vc_0=(u+v)/2 \bmod r$

$$({}^1M)^2=-L_{1M}\mathbf{1}+(u+v)\,{}^1M \bmod r.$$

Then for any $m,u,v,{}^1w,{}^1z\in R$

$$L_{1M}=|{}^1M|^2=|uA+vC+{}^1wAB+{}^1zBA|^2=uv \bmod r. \tag{37a}$$

In the same manner we have

$$L_{2M}=|{}^2M|^2=|vA-uC+{}^2wAB+{}^2zBA|^2=-vu \bmod r. \tag{37b}$$

Theorem 13 (linear independence)

If

$${}^1M:=uA+vC+{}^1wAB+{}^1zBA=\mathbf{0} \bmod r,$$

then

$$u=v={}^1w={}^1z=0 \bmod r.$$

(*Proof*)

As $[A]_0=1/2 \bmod r$, $[AB]_0=0 \bmod r$ and $[BA]_0=0 \bmod r$,

$$2[{}^1M\,A]_0=u=0 \bmod r,$$

$$2[{}^1M\,C]_0=v=0 \bmod r.$$

We have

$${}^1wAB+{}^1zBA=\mathbf{0} \bmod r.$$

By multiply A from right side from Theorem 10

$${}^1w(AB)A+{}^1zBAA=\mathbf{0}A \bmod r,$$

$${}^1w\mathbf{0}+{}^1zBA=\mathbf{0} \bmod r.$$

We have

$${}^1z=0 \bmod r,$$

$${}^1w=0 \bmod r.$$ q.e.d.

In the same manner we have

If

$${}^2M:= vA-uC+{}^2wAB+{}^2zBA =\mathbf{0} \bmod r,$$

then

$$u=v={}^2w= {}^2z=0 \bmod r.$$

(Associative of medium texts)

Let

$${}^1M_1:= u_1A+v_1C+{}^1w_1AB+{}^1z_1BA \bmod r,$$

$${}^1M_2:= u_2A+v_2C+{}^1w_2AB+{}^1z_2BA \bmod r ,$$

$${}^1M_3:= u_3A+v_3C+{}^1w_3AB+{}^1z_3BA \bmod r.$$

Then we have

$${}^1M_1{}^1M_2 =(u_1A+v_1C+{}^1w_1AB+{}^1z_1BA)(u_2A+v_2C+{}^1w_2AB+{}^1z_2BA) \bmod r$$

$$= u_1u_2A+ v_1v_2C+(u_1 {}^1w_2+{}^1w_1v_2)AB +(v_1{}^1z_2+{}^1z_1u_2)BA \bmod r.$$

$$({}^1M_1{}^1M_2){}^1M_3$$

$$= [(u_1A+v_1C+{}^1w_1AB+{}^1z_1BA)(u_2A+v_2C+{}^1w_2AB+{}^1z_2BA)](u_3A+v_3C$$

$$+{}^1w_3AB+{}^1z_3BA) \bmod r$$

$$=(u_1u_2A+ v_1v_2C+(u_1{}^1 w_2+{}^1w_1v_2)AB$$

$$+(v_1{}^1z_2+{}^1z_1u_2)BA)(u_3A+v_3C+{}^1w_3AB+{}^1z_3BA)$$

$$=u_1u_2u_3A+v_1v_2v_3C+(u_1u_2{}^1w_3+u_1{}^1w_2v_3+{}^1w_1v_2v_3)AB$$

$$+(v_1{}^1z_2u_3+{}^1z_1u_2u_3+v_1v_2{}^1z_3)BA \bmod r.$$

$$^1M_1(^1M_2{}^1M_3)$$

$$= (u_1A+v_1C+{}^1w_1AB+{}^1z_1BA)\,[u_2u_3A+v_2v_3C+(u_2\,{}^1w_3+{}^1w_2v_3\,)AB$$

$$+(v_2{}^1z_3+{}^1z_2u_3)BA]\bmod r$$

$$=u_1u_2u_3A+v_1v_2v_3C+(u_1u_2{}^1w_3+u_1{}^1w_2v_3+{}^1w_1v_2v_3)AB$$

$$+(v_1{}^1z_2u_3+{}^1z_1u_2u_3+v_1v_2{}^1z_3)BA \bmod r.$$

Then we have

$$(^1M_1{}^1M_2)^1M_3= {}^1M_1(^1M_2{}^1M_3) \bmod r.$$

That is,it is said that $^1M_1$,$^1M_2$ and $^1M_3$ have the associative property.

Let

$$^1M_1:= u_1A+v_1C+{}^1w_1AB+{}^1z_1BA \bmod r,$$

$$^2M_2:= v_2A-u_2C+{}^2w_2AB+{}^2z_2BA \bmod r,$$

$$^1M_3:= u_3A+v_3C+{}^1w_3AB+{}^1z_3BA \bmod r.$$

$$^1M_1{}^2M_2 =(u_1A+v_1C+w_1AB+z_1BA)(v_2A-u_2C+w_2AB+z_2BA) \bmod r$$

$$= u_1v_2A- v_1u_2C+(\,u_1\,w_2-w_1u_2\,)AB +(\,v_1z_2+z_1v_2\,)BA \bmod r.$$

$$(^1M_1{}^2M_2)^1M_3$$

$$= [(u_1A+v_1C+w_1AB+z_1BA)(v_2A-u_2C+w_2AB+z_2BA)](\,u_3A+v_3C$$

$$+w_3AB+z_3BA)\bmod r$$

$$=(\,u_1v_2A- v_1u_2C+(\,u_1\,w_2-w_1u_2\,)AB +(\,v_1z_2+z_1v_2\,)BA)(\,u_3A+v_3C$$

$$+w_3AB+z_3BA)$$

$$=u_1v_2u_3A-v_1u_2v_3C+(u_1v_2w_3+u_1w_2v_3-w_1u_2\,v_3\,)AB$$

$$+(v_1z_2\,u_3+z_1v_2\,u_3- v_1u_2\,z_3)BA \bmod r.$$

$$^1M_1(^2M_2{}^1M_3)$$

$$= (u_1A+v_1C+w_1AB+z_1BA)\,(v_2A-u_2C+w_2AB+z_2BA)$$

$$(\,u_3A+v_3C+w_3AB+z_3BA)\bmod r$$

$$=(u_1A+v_1C+w_1AB+z_1BA)[\,v_2\,u_3A-u_2\,v_3C+(\,v_2\,w_3+w_2v_3\,)AB$$

$$+(\,z_2u_3-u_2z_3\,)BA]$$

$$=u_1\, v_2\, u_3A\text{-}v_1\, u_2\, v_3C+(u_1v_2w_3+u_1w_2v_3\text{-}w_1u_2v_3)AB$$

$$+(z_1v_2\, u_3+v_1z_2\, u_3\text{-}\, v_1u_2\, z_3)BA \bmod r.$$

Then we have

$$({}^1M_1{}^2M_2){}^1M_3={}^1M_1({}^2M_2{}^1M_3) \bmod r.$$

That is, it is said that ${}^1M_1$,${}^2M_2$ and ${}^1M_3$ have the associative property.

In the same manner we have

$$({}^iM_1{}^jM_2){}^kM_3={}^iM_1({}^jM_2{}^kM_3) \bmod r,\ \mathrm{i,j,k}\in\{1,2\}.\square$$

(Homomorphism on medium text)

We can obtain the plaintext m_1+m_2 from ${}^1M_1$,${}^1M_2$, the plaintext m_1m_2 from ${}^1M_1$,${}^1M_2$, ${}^2M_1$ and ${}^2M_2$ as follows.

$${}^1M_{1+2}:={}^1M_1+{}^1M_2 \bmod r$$

$${}^2M_{1+2}:={}^2M_1+{}^2M_2 \bmod r$$

$$m_{1+2}:=2[{}^1M_{1+2}]_0 \bmod r$$

$$=2(\, u_1\, a_0+\, v_1\, c_0) +2(u_2\, a_0+v_2\, c_0) \bmod r$$

$$= (u_1+v_1) +(\, u_2+v_2) \bmod r$$

$$=m_1+m_2 \bmod r. \qquad (38)$$

$${}^1M_1{}^1M_2 =(u_1A+v_1C+{}^1w_1AB+{}^1z_1BA)(u_2A+v_2C+{}^1w_2AB+{}^1z_2BA) \bmod r$$

$$= u_1u_2A+\, v_1v_2C+(\, u_1\, {}^1w_2+{}^1w_1v_2\,)AB +(\, v_1{}^1z_2+{}^1z_1u_2\,)BA \bmod r.$$

$${}^2M_1{}^2M_2 =(v_1A\text{-}u_1C+{}^2w_1AB+{}^2z_1BA)(v_2A\text{-}u_2C+{}^2w_2AB+{}^2z_2BA) \bmod r$$

$$= v_1v_2A+\, u_1u_2C+(\, v_1\, {}^2w_2\text{-}{}^2w_1u_2\,)AB +(\, \text{-}u_1{}^2z_2+{}^2z_1v_2\,)BA \bmod r.$$

$${}^1M_1{}^2M_2 =(u_1A+v_1C+{}^1w_1AB+{}^1z_1BA)(v_2A\text{-}u_2C+{}^2w_2AB+{}^2z_2BA) \bmod r$$

$$= u_1v_2A\text{-}\, v_1u_2C+(\, u_1\, {}^2w_2\text{-}{}^1w_1u_2\,)AB +(\, v_1{}^2z_2+{}^1z_1v_2\,)BA \bmod r.$$

$${}^2M_1{}^1M_2 =(v_1A\text{-}u_1C+{}^2w_1AB+{}^2z_1BA)(u_2A+v_2C+{}^1w_2AB+{}^1z_2BA) \bmod r$$

$$= v_1u_2A\text{-}\, u_1v_2C+(\, v_1{}^1w_2+{}^2w_1v_2\,)AB +(\text{-}\, u_1{}^1z_2+{}^2z_1u_2\,)BA \bmod r.$$

$${}^1M_{12}:=({}^1M_1{}^1M_2+{}^2M_1{}^2M_2)A\text{-}({}^1M_1{}^2M_2+{}^2M_1{}^1M_2)C$$

$$=(\, u_1u_2+\, v_1v_2)A+(v_1u_2+\, u_1v_2)C$$

$$+(v_1{}^1z_2+{}^1z_1u_2 - u_1{}^2z_2+{}^2z_1v_2)BA+(-u_1{}^2w_2+{}^1w_1u_2 - v_1{}^1w_2-{}^2w_1v_2)AB$$

$${}^2M_{12}:= ({}^1M_1{}^2M_2+{}^2M_1{}^1M_2)\,A-({}^1M_1{}^1M_2+{}^2M_1{}^2M_2)C$$

$$=(u_1v_2+ v_1u_2)A-(u_1u_2+ v_1v_2)C$$

$$+(v_1{}^2z_2+{}^1z_1v_2 - u_1{}^1z_2+{}^2z_1u_2)BA+(-u_1{}^1w_2-{}^1w_1v_2 - v_1{}^2w_2+{}^2w_1u_2)AB$$

$$m_{12}:=2[{}^1M_{12}]_0$$

$$=2(u_1u_2+ v_1v_2)a_0+2\,(u_1v_2+ v_1u_2)c_0$$

$$=u_1u_2+ v_1v_2+ u_1v_2+ v_1u_2$$

$$= (u_1+v_1)(u_2+v_2) \bmod r$$

$$= m_1m_2 \bmod r.$$

We have shown that we can obtain the plaintext m_1+m_2 from ${}^1M_{1+2}$, the plaintext m_1m_2 from ${}^1M_{12}$. □

We notice that in general, for any element $D\in O$,

$$A((BA)D)\neq(A(BA))D=(\mathbf{0})D=\mathbf{0}, \tag{39a}$$

$$A((AB)D) \neq(A(AB))D=(AB)D, \tag{39b}$$

$$(BA)(AD)\neq((BA)A)D=(BA)D, \tag{39c}$$

$$(AB)(AD)\neq((AB)A)D=(\mathbf{0})D=\mathbf{0}. \tag{39d}$$

§4.3 Enciphering

Let $(r,A,B;F(X))$ be the system parameters where $r=pq$, p and q are secret primes.

Let $F^u(X)$ be user U's public-key and $a\in Z$ be user U's secret key.

Let $F_{VU}(X,Y)$ or $F_{UV}(X,Y)$ be the common enciphering function between user U and user V.

User V generate medium text ${}^1M$, ${}^2M$ by using the plaintext $m\in R$, the compornents $u,v\in R$ of the plaintext m and random noises ${}^1w,{}^1z,{}^2w,{}^2z\in R$ such that

$${}^1M:=uA+vC+{}^1wAB+{}^1zBA \bmod r\in O,$$

$${}^2M:=vA-uC+{}^2wAB+{}^2zBA \bmod r\in O,$$

$m := u+v \bmod r \in R$.

User V calculates ciphertext $F_{VU}(X,{}^{k}M)$ by substituting medium texts ${}^{k}M \in O$ to Y of $F_{VU}(X,Y)$.

$$
\begin{aligned}
& F_{VU}(X,{}^{k}M) \\
&= ({}^{k}c_{00}x_0+\ldots+{}^{k}c_{07}x_7 , \\
&\quad \ldots \quad \ldots , \\
&\quad {}^{k}c_{70}x_0+\ldots+{}^{k}c_{77}x_7) \bmod r \\
&= \{{}^{k}c_{ij}\} \ (i,j=0,\ldots,7;k=1,2) .
\end{aligned}
$$

User V sends $\{{}^{k}c_{ij}\}$ $(i,j=0,\ldots,7;k=1,2)$ to user U through the unsecured line.

§4.4 Deciphering

User U deciphers $C(m,X):=(F_{VU}(X,{}^{1}M),\ F_{VU}(X,{}^{2}M))$ to obtain m from $\{{}^{k}c_{ij}\}$ $(i,j=0,\ldots,7;k=1,2)$ sent by user V as follows.

$$
\begin{aligned}
& F_{VU}(X,{}^{1}M) := \{{}^{1}c_{ij}\} \ (i,j=0,\ldots,7), \\
& F^{ba}(F_{VU}(F^{-ba}(\mathbf{1}),{}^{1}M)) \\
&\quad = F^{ba}(F^{-ab}({}^{1}MF^{ab}(F^{-ba}(\mathbf{1})))) \bmod r \\
&= {}^{1}M, \\
& F_{VU}(X,{}^{2}M) := \{{}^{2}c_{ij}\} \ (i,j=0,\ldots,7), \\
& F^{ba}(F_{VU}(F^{-ba}(\mathbf{1}),{}^{2}M)) \\
&\quad = F^{ba}(F^{-ab}({}^{2}MF^{ab}(F^{-ba}(\mathbf{1})))) \bmod r \\
&= {}^{2}M.
\end{aligned}
$$

$$
\begin{aligned}
m &= 2([{}^{1}M]_0 \bmod r \\
&= u+v \bmod r \in R.
\end{aligned}
$$

Theorem 14

For any $m,m' \in R$,

if $C(m,X) = C(m', X) \bmod r$, then $m = m' \bmod r$.

That is , if $m \neq m' \bmod r$, then $C(m, X) \neq C(m', X) \bmod r$

where

$$C(m, X)=(F_{AB}(X,{}^1M), F_{AB}(X,{}^2M))$$

$$C(m',X)=(F_{AB}(X,{}^1M'), F_{AB}(X,{}^2M'))$$

$${}^1M:=uA+vC+{}^1wAB+{}^1zBA \bmod r\in O,$$

$${}^1M':=u'A+v'C+{}^1w'AB+{}^1z'BA \bmod r\in O,$$

$${}^2M:=vA-uC+{}^2wAB+{}^2zBA \bmod r\in O,$$

$${}^2M:=v'A-u'C+{}^2w'AB+{}^2z'BA \bmod r\in O,$$

$$m:= u+v \bmod r,$$

$$m':= u'+v' \bmod r.$$

(*Proof*)

If $C(m, X)= C(m', X) \bmod r$, then

$$F_{UV}(X,{}^1M) = F_{UV}(X,{}^1M'),$$

$$F^{-ab}({}^1MF^{ab}(X))= F^{-ab}({}^1M'F^{ab}(X))$$

$$F^{-ab}({}^1MF^{ab}(F^{-ab}(\mathbf{1})))= F^{-ab}({}^1M'F^{ab}(F^{-ab}(\mathbf{1})))$$

$$F^{-ab}({}^1M)= F^{-ab}({}^1M')$$

$$F^{ab}(F^{-ab}({}^1M))= F^{ab}(F^{-ab}({}^1M')) \bmod r;$$

$${}^1M={}^1M' \bmod r$$

$$uA+vC+{}^1wAB+{}^1zBA = u'A+v'C+{}^1w'AB+{}^1z'BA \bmod r.$$

Then we have

$$(u - u')A+(v- v')C+({}^1w-{}^1w')AB+({}^1z-{}^1z')BA) =0 \bmod r.$$

From Theorem 13 we have

$$u- u'= v- v'={}^1w-{}^1w'={}^1z-{}^1z'=0 \bmod r,$$

$$u=u' \bmod r,$$

$$v=v' \bmod r,$$

$${}^1z = {}^1z' \bmod r,$$

$${}^1w= {}^1w' \bmod r.$$

We have

$$m=u+v=u'+v'=m' \bmod r. \qquad \text{q.e.d.}$$

§4.5 Addition scheme on ciphertexts

Let

$${}^1M_1:=u_1A+v_1C+{}^1w_1AB+{}^1z_1BA \bmod r\in O,$$

$${}^2M_1:=v_1A-u_1C+{}^2w_1AB+{}^2z_1BA \bmod r\in O,$$

$${}^1M_2:=u_2A+v_2C+{}^1w_2AB+{}^1z_2BA \bmod r\in O,$$

$${}^2M_2:=v_2A-u_2C+{}^2w_2AB+{}^2z_2BA \bmod r\in O,$$

be medium texts to be encrypted where

$$m_1:= u_1+v_1 \bmod r\in R$$

$$=2[{}^1M_1]_0 \bmod r,$$

$$m_2:= u_2+v_2 \bmod r\in R$$

$$=2[{}^1M_2]_0 \bmod r.$$

Let $C(m_1,X):=(F_{UV}(X,{}^1M_1),F_{UV}(X,{}^2M_1))$ and $C(m_2,X):= (F_{UV}(X,{}^1M_2),F_{UV}(X,{}^2M_2))$ be the ciphertexts.We difine the addiotion operation between $C(m_1,X) \bmod r$ and $C(m_2,X) \bmod r$ such that

$$C(m_1,X)+C(m_2,X) \bmod r$$

$$:=(F_{UV}(X,{}^1M_1)+ F_{UV}(X,{}^1M_2) \bmod r,F_{UV}(X,{}^2M_1)+F_{UV}(X,{}^2M_2) \bmod r)$$

$$=(F_{UV}(X,{}^1M_1+{}^1M_2) \bmod r, F_{UV}(X,{}^2M_1 +{}^2M_2) \bmod r)$$

$$=(F_{UV}(X,{}^1M_{1+2}) \bmod r, F_{UV}(X,{}^2M_{1+2}) \bmod r).$$

Then we have

$$C(m_1,X)+C(m_2,X) \bmod r$$

$$= C(m_{1+2},X) \bmod r,$$

$$= C(m_1+m_2, X) \bmod r.\text{(From (38))}$$

It has been shown that in this method we have the additional homomorphism of the plaintext m.

§4.6 Multiplication scheme on ciphertexts

Here we consider the multiplicative operation on the ciphertexts.

Let $C(m_1,X):=(F_{UV}(X,{}^1M_1) \bmod r, F_{UV}(X,{}^2M_1) \bmod r)$ and $C(m_2,X):= (F_{UV}(X,{}^1M_2) \bmod r, F_{UV}(X,{}^2M_2) \bmod r)$ be the ciphertexts where

$${}^1M_1:=u_1A+v_1C+{}^1w_1AB+{}^1z_1BA \bmod r \in O,$$

$${}^2M_1:=v_1A-u_1C+{}^2w_1AB+{}^2z_1BA \bmod r \in O,$$

$${}^1M_2:=u_2A+v_2C+{}^1w_2AB+{}^1z_2BA \bmod r \in O,$$

$${}^2M_2:=v_2A-u_2C+{}^2w_2AB+{}^2z_2BA \bmod r \in O,$$

$$m_1:= u_1+v_1 \bmod r \in R$$

$$=2[{}^1M_1]_0 \bmod r,$$

$$m_2:= u_2+v_2 \bmod r \in R$$

$$=2[{}^1M_2]_0 \bmod r.$$

We can calculate the ciphertext $C(m_1m_2,X)$ of the plaintext m_1m_2 by using

$$C(m_1,X) =(F_{UV}(X,{}^1M_1) \bmod r, F_{UV}(X,{}^2M_1) \bmod r)$$

and

$$C(m_2,X) = (F_{UV}(X,{}^1M_2) \bmod r, F_{UV}(X,{}^2M_2) \bmod r)$$

as follows.

$$K_{11}(X):= F_{UV}(F_{UV}(X,{}^1M_2),{}^1M_1)+ F_{UV}(F_{UV}(X,{}^2M_2),{}^2M_1) \bmod r$$

$$K_{12}(X):= F_{UV}(F_{UV}(X,{}^2M_2),{}^1M_1)+ F_{UV}(F_{UV}(X,{}^1M_2),{}^2M_1) \bmod r$$

$$K_1(X):= K_{11}((F_{UV}(X,A))- K_{12}((F_{UV}(X,C)) \bmod r$$

$$= F_{UV}(X, ({}^1M_1{}^1M_2+{}^2M_1{}^2M_2)A-({}^1M_1{}^2M_2+{}^2M_1{}^1M_2)C) \bmod r$$

$$= F_{UV}(X,{}^1M_{12}) \bmod r,$$

$$K_2(X):= K_{12}((F_{UV}(X,A))- K_{11}((F_{UV}(X,C)) \bmod r$$

$$= F_{UV}(X, ({}^1M_1{}^2M_2+{}^2M_1{}^1M_2)A-({}^1M_1{}^1M_2+{}^2M_1{}^2M_2)C) \bmod r$$

$$= F_{UV}(X,{}^2M_{12}) \bmod r,$$

where

$$^1M_{12} := (^1M_1{}^1M_2 + {}^2M_1{}^2M_2)A - (^1M_1{}^2M_2 + {}^2M_1{}^1M_2)C$$

$$= (u_1u_2 + v_1v_2)A + (u_1v_2 + v_1u_2)C$$

$$+ (v_1{}^1z_2 + {}^1z_1u_2 - u_1{}^2z_2 + {}^2z_1v_2)BA + (-u_1{}^2w_2 + {}^1w_1u_2 - v_1{}^1w_2 - {}^2w_1v_2)AB$$

$$^2M_{12} := (^1M_1{}^2M_2 + {}^2M_1{}^1M_2)A - (^1M_1{}^1M_2 + {}^2M_1{}^2M_2)C$$

$$= (u_1v_2 + v_1u_2)A - (u_1u_2 + v_1v_2)C$$

$$+ (v_1{}^2z_2 + {}^1z_1v_2 - u_1{}^1z_2 + {}^2z_1u_2)BA + (-u_1{}^1w_2 - {}^1w_1v_2 - v_1{}^2w_2 + {}^2w_1u_2)AB$$

$$m_{12} := 2[^1M_{12}]_0$$

$$= 2(u_1u_2 + v_1v_2)a_0 + 2(u_1v_2 + v_1u_2)c_0$$

$$= u_1u_2 + v_1v_2 + u_1v_2 + v_1u_2$$

$$= (u_1 + v_1)(u_2 + v_2) \bmod r$$

$$= m_1m_2 \bmod r.$$

We can express $^1M_{12}$ and $^2M_{12}$ such that

$$^1M_{12} = (u_1u_2 + v_1v_2)A + (u_1v_2 + v_1u_2)C + (-u_1{}^2w_2 + {}^1w_1u_2 - v_1{}^1w_2 - {}^2w_1v_2)AB$$

$$+ (v_1{}^1z_2 + {}^1z_1u_2 - u_1{}^2z_2 + {}^2z_1v_2)BA$$

$$= u_{12}A + v_{12}C + {}^1w_{12}AB + {}^1z_{12}BA \bmod r,$$

$$^2M_{12} = (u_1v_2 + v_1u_2)A - (u_1u_2 + v_1v_2)C + (-u_1{}^1w_2 - {}^1w_1v_2 - v_1{}^2w_2 + {}^2w_1u_2)AB$$

$$+ (v_1{}^2z_2 + {}^1z_1v_2 - u_1{}^1z_2 + {}^2z_1u_2)BA$$

$$= v_{12}A - u_{12}C + {}^2w_{12}AB + {}^2z_{12}BA \bmod r,$$

where

$$u_{12} := u_1u_2 + v_1v_2 \bmod r,$$

$$v_{12} := u_1v_2 + v_1u_2 \bmod r,$$

$$^1w_{12} := -u_1{}^2w_2 + {}^1w_1u_2 - v_1{}^1w_2 - {}^2w_1v_2 \bmod r,$$

$$^1z_{12} := v_1{}^1z_2 + {}^1z_1u_2 - u_1{}^2z_2 + {}^2z_1v_2 \bmod r,$$

$$^2w_{12} := -u_1{}^1w_2 - {}^1w_1v_2 - v_1{}^2w_2 + {}^2w_1u_2 \bmod r,$$

$$^2z_{12} := v_1{}^2z_2 + {}^1z_1v_2 - u_1{}^1z_2 + {}^2z_1u_2 \bmod r.$$

Then we have

$$C(m_{12},X) = (F_{UV}(X,{}^1M_{12}) \bmod r, F_{UV}(X,{}^2M_{12}) \bmod r)$$

$$= C(m_1m_2,X).$$

We can decipher the ciphertext $C(m_{12},X)$ to obtain the plaintext m_1m_2 such that

$$F^{ba}(F_{UV}(F^{-ba}(\mathbf{1}),{}^1M_{12}) \bmod r$$

$$= F^{ba}(F^{-ba}({}^1M_{12}F^{ba}(F^{-ba}(\mathbf{1}))) \bmod r$$

$$= {}^1M_{12} \bmod r,$$

$$m_{12} = 2[{}^1M_{12}]_0$$

$$= 2(u_1u_2 + v_1v_2 + (u_1v_2 + v_1u_2))c_0$$

$$= (u_1+v_1)(u_2+v_2) \bmod r$$

$$= m_1m_2 \bmod r.$$

It has been shown that in this method we have the multiplicative homomorphism of the plaintext m.

§4.7 Discrete logarithm assumption DLA(F,F^a;q)

Here we describe the assumption on which the proposed public-key scheme bases.

Let r be a composite number. Let a, b and k be integer parameters. Let $\boldsymbol{S}:=(S_1,\ldots,S_k)\in O^k$, $\boldsymbol{T}:=(T_1,\ldots,T_k)\in O^k$ such that S_1^{-1} ,…, S_k^{-1} and T_1^{-1} ,…, T_k^{-1} exist.

Let $F(X)=(S_k((\ldots((S_1X)T_1))\ldots))T_k \bmod r\in O[X]$ be a basic function.

Let $F^a(X) \bmod r\in O[X]$ be the public function.

X is a variable.

In the **DLA(F,F^a; r)** assumption, the adversary A_d is given $F^a(X)=\{ f_{aij} \}$ $(i,j=0,\ldots,7)$, system parameters $(r,A,B;F(X))$ where $F(X)= \{f_{ij}\}(i,j=0,\ldots,7)$ and his goal is to find the integer a. For parameters $k = k(\lambda)$, $a= a(\lambda)$ defined in terms of the security parameter λ and for any PPT adversary A_d we have

$$\Pr[F(X)= \{f_{ij}\}, F^a(X)=\{f_{aij}\}: a \leftarrow A_d(1^\lambda, \{f_{ij}\}, \{f_{aij}\})] = \mathrm{negl}(\lambda).$$

To solve directly **DLA(F,F^a;r)** assumption is known to be the discrete logarithm problem on the multivariate polynomial.

§4.8 Computational Diffie–Hellman assumption CDH($F,F^a,F^b;r$)

Let r be a composite number. Let a , b and k be integer parameters. Let $\boldsymbol{S}:=(S_1,\ldots,S_k)\in O^k$, $\boldsymbol{T}:=(T_1,\ldots,T_k)\in O^k$ such that S_1^{-1} ,…, S_k^{-1} and T_1^{-1} ,…, T_k^{-1} exist.

Let $F(X)=(S_k((\ldots((S_1X)T_1))\ldots))T_k \bmod r\in O[X]$ be a basic function.

Let $F^a(X) \bmod r\in O[X]$ be the public function of user U.

Let $F^b(X) \bmod r\in O[X]$ be the public function of user V.

X is a variable.

In the **CDH($F,F^a,F^b;r$)** assumption, the adversary A_d is given $F^a(X)=\{f_{aij}\}$, $F^b(X)=\{f_{bij}\}(i,j=0,\ldots,7)$, system parameters $(r,A,B;F(X))$ and his goal is to find $F_{UV}(X, Y)=F^{-ab}(YF^{ab}(X)) \bmod r$. For parameters $k = k(\lambda)$, $a= a(\lambda)$,and $b= b(\lambda)$ defined in terms of the security parameter λ and for any PPT adversary A_d we have

$\Pr[F(X)=\{f_{ij}\},F^a(X)=\{f_{aij}\},F^b(X)=\{f_{bij}\}:F_{UV}(X,Y)=F^{-ab}(YF^{ab}(X))\leftarrow A_d(1^\lambda,\{f_{ij}\},\{f_{aij}\},\{f_{bij}\})]= \mathrm{negl}(\lambda)$.

To solve directly **CDH($F,F^a,F^b;r$)** assumption is known to be the computational Diffie–Hellman assumption on the multivariate polynomial.

§4.9 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 parameters $(r,A,B;F(X))$, where $r=pq$ and p and q are secret large primes, outputs $(\mathbf{pk},\mathbf{sk})\leftarrow\mathbf{KeyGen}(1^\lambda)$, where $\mathbf{pk}=[\{f_{aij}\}(i,j=0,\ldots,7)]$ is a public key and $\mathbf{sk}=(a)$ is a secret key.

-Encryption. The algorithm **Enc**, on input system parameters $(r,A,B;F(X))$, public key $\mathbf{pk}=\{f_{aij}\}(i,j=0,\ldots,7)$ and a plaintext $m\in\boldsymbol{R}$, outputs a ciphertext $\boldsymbol{C}(m,X)\leftarrow\mathbf{Enc}(\mathbf{pk},;m)$ where ${}^1M=uA+vC+{}^1wAB+{}^1zBA \bmod r$, ${}^2M=vA-uC+{}^2wAB+{}^2zBA \bmod r$, $m=u+v \bmod r$.

-Decryption. The algorithm **Dec**, on input system parameters $(r,A,B;F(X))$, secret key $\mathbf{sk}=(a)$ and a ciphertext $\boldsymbol{C}(m,X)$, outputs plaintext $m=\mathbf{Dec}(\mathbf{sk};\boldsymbol{C}(m,X))$ where $\boldsymbol{C}(m,X)\leftarrow\mathbf{Enc}(\mathbf{pk};m)$.

-Homomorphic-Evaluation. The algorithm **Eval**, on input system parameters $(r,A,B;F(X))$, an arithmetic circuit ckt, and a tuple of $2\times n$ ciphertexts $(C_1,\ldots,C_n)$,

outputs an evaluated ciphertext $C' \in O[X]^2 \leftarrow$ **Eval**(ckt;$C_1,\ldots,C_n$) where C_i=**C**(m_i,X) (i=1,…,n).

§4.10 Property of proposed fully homomorphic public-key encryption

(**Fully homomorphic encryption**) Proposed fully homomorphic public-key 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 (**pk**,**sk**) $\leftarrow$**KeyGen**(1^λ), $\forall$ckt $\in CR_\lambda$, $\forall(m_1,\ldots,m_n) \in R^n$ where $n = n(\lambda)$, $\forall(C_1,\ldots,C_n)$ where $C_i \leftarrow E$(**pk**;p_i), ${}^1M_i = u_iA+v_iC+{}^1w_iAB+{}^1z_iBA$ mod r, ${}^2M_i=v_iA-u_iC+{}^2w_iAB+{}^2z_iBA$ mod r, $m_i=u_i+v_i$ mod r. (i =1,…,n),
   we have
   Dec(**sk**;**Eval**(ckt; $C_1,\ldots,C_n$)) = ckt($m_1,\ldots,m_n$).

Then it holds that:

$$\Pr[\textbf{Dec}(\textbf{sk}; \textbf{Eval}(\text{ckt}; C_1,\ldots,C_n)) \neq \text{ckt}(m_1,\ldots,m_n)] = \text{negl}(\lambda).$$

2. Compactness: As the output length of **Eval** is at most $t\log_2 q = t\lambda$ where t 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.

§5. Analysis of proposed scheme

Here we analyze the proposed fully homomorphic pulic-key encryption scheme described in section 4.

§5.1 Computing plaintext *m* from coefficients of ciphertext $F_{UV}(X,M)$

Ciphertext $C(m_n,X)$:=($F_{UV}(X,{}^1M_n)$,$F_{UV}(X,{}^2M_n)$) is given such that

$$F_{UV}(X,{}^kM_n) = F^{-ba}({}^kM_nF^{ba}(X)) \bmod r \in O[X]$$

$$= ({}^kc_{n00}x_0+{}^kc_{n01}x_1+\ldots+{}^kc_{n07}x_7,$$

$${}^kc_{n10}x_0+{}^kc_{n11}x_1+\ldots+{}^kc_{n17}x_7,$$

$$\ldots \qquad \ldots$$

$${}^kc_{n70}x_0+{}^kc_{n71}x_1+\ldots+{}^kc_{n77}x_7) \bmod r,$$

$$= \{{}^kc_{nij}\}(i,j=0,\ldots,7;n=1,2,\ldots;\ k=1,2)$$

with ${}^{k}c_{nij} \in \boldsymbol{R}$ $(i,j,n=1,2,\ldots;k=1,2)$,

where

$$ {}^{1}M_n = u_n A + v_n C + {}^{1}v_n AB + {}^{1}w_n BA \bmod r \in O, $$

$$ {}^{2}M_n = v_n A - u_n C + {}^{2}v_n AB + {}^{2}w_n BA \bmod r \in O, $$

$$ u_n, v_n, {}^{1}w_n, {}^{1}z_n, {}^{2}w_n, {}^{2}z_n, \in R \ (n=0,\ldots,7). $$

Let $F_{UV}(X, Y) := \{d_{ijh}\}(i,j,h=0,\ldots,7)$ such that

$$ \begin{aligned} F_{UV}(X, Y) &= F^{-ba}(YF^{ba}(X)) \bmod q \in O[X,Y] \\ &= (d_{000}x_0y_0 + d_{001}x_0y_1 + \ldots + d_{077}x_7y_7, \\ &\quad d_{100}x_0y_0 + d_{101}x_0y_1 + \ldots + d_{177}x_7y_7, \\ &\quad \ldots\ldots \quad \ldots\ldots \\ &\quad d_{700}x_0y_0 + d_{701}x_0y_1 + \ldots + d_{777}x_7y_7) \bmod r, \\ &= \{d_{ijh}\}(i,j,h=0,\ldots,7) \end{aligned} $$

with $d_{ijh} \in R(i,j,h=0,\ldots,7)$ which is secret.

Anyone except user U and user V does not know $\{d_{ijh}\}$ $(i,j,h=0,\ldots,7)$ which is a common enciphering function between user U and user V. Here we try to find ${}^{k}M_n = ({}^{k}m_{n0},\ldots,{}^{k}m_{n7})$ from $\{{}^{k}c_{nij}\}(i,j=0,\ldots,7;n=1,\ldots,4;k=1,2)$ in condition that $d_{ijh}(i,j,h=0,\ldots,7)$ are unkown parameters. We have the following simultaneous equations from $F_{UV}(X, Y)$ and $F_{UV}(X, {}^{k}M_n)$ where $d_{ijh}(i,j,h=0,\ldots,7)$ and $({}^{k}m_{n0},\ldots,{}^{k}m_{n7})$ are unknown variables.

$$ \left.\begin{aligned} d_{i00}{}^{k}m_{n0} + d_{i01}{}^{k}m_{n1} + \ldots + d_{i07}{}^{k}m_{n7} &= {}^{k}c_{ni0} \bmod r \\ d_{i10}{}^{k}m_{n0} + d_{i11}{}^{k}m_{n1} + \ldots + d_{i17}{}^{k}m_{n7} &= {}^{k}c_{ni1} \bmod r \\ \cdots & \\ \cdots & \\ d_{i70}{}^{k}m_{n0} + d_{i71}{}^{k}m_{n1} + \ldots + d_{i77}{}^{k}m_{n7} &= {}^{k}c_{ni7} \bmod r \end{aligned}\right\} $$

$$ (i=0,\ldots,7) $$

For ${}^{k}M_n$ $(n=1,\ldots,4;k=1,2)$ we obtain the same equations, the number of which is 512(=64*4*2).We also obtain 8 equations such as

$$ |F_{UV}(\mathbf{1}, {}^{k}M_n)|^2 = ({}^{k}c_{n00})^2 + ({}^{k}c_{n10})^2 + \ldots + ({}^{k}c_{n70})^2 \bmod r $$

$$=|{}^{k}M_n|^2=({}^{k}m_{n0})^2+({}^{k}m_{n1})^2+\ldots+({}^{k}m_{n7})^2 \bmod r,(n=1,\ldots,4;k=1,2). \qquad (40)$$

The number of unknown variables ${}^{k}M_n(n=1,\ldots,4;k=1,2)$ and d_{ijh} $(i,j,h=0,...,7)$ is 576(=512+8*4*2). The number of equations is 520(=512+8). Then the complexity G_{reb} required for solving above simultaneous quadratic algebraic equations by using Gröbner basis is given such as

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

where G_{reb}' 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.

§5.2 Attack by using the ciphertexts of *m* and *-m*

I show that we cannot easily distinguish the ciphertexts of $-m$ by using the ciphertext $C(m,X) =(F_{UV}(X, {}^{1}M), F_{UV}(X, {}^{2}M))$. We try to attack by using "*m* and *-m* attack".

Given the ciphertext $C(m,X)=(F_{UV}(X,{}^{1}M), F_{UV}(X,{}^{2}M))$, we try to find the ciphertext $C(m_-, X)$ corresponding to the plaintext $m_-=-m \bmod r$

where

$${}^{1}M=uA+vC+{}^{1}wAB+{}^{1}zBA \bmod r\in O,$$

$${}^{2}M=vA-uC+{}^{2}wAB+{}^{2}zBA \bmod r\in O,$$

$$m=u+v \bmod r\in R$$

$$=2\,[{}^{1}M]_0 \bmod r,$$

$$u,v\ ,{}^{1}w,\ {}^{1}z,\ {}^{2}w,\ {}^{2}z\in R.$$

Let

$${}^{1}N:=sA+tC+{}^{1}w_-AB+{}^{1}z_-BA \bmod r\in O,$$

$${}^{2}N:=tA-sC+{}^{2}w_-AB+{}^{2}z_-BA \bmod r\in O,$$

$$m_-:=-m= s+t \bmod r\in R,$$

$s,t,{}^1w_-,\ {}^1z_-,\ {}^2w_-,{}^2z_-\in R.$

We calculate ${}^1M+{}^1N$ such that

$${}^1M+{}^1N=uA+vC+{}^1wAB+{}^1zBA+sA+tC+{}^1w_-AB+{}^1z_-BA \bmod r$$

$$=(u+s)A+(v+t)C+({}^1w+{}^1w_-)AB+({}^1z+{}^1z_-)BA \bmod r.$$

As $m+m_-=u+v+s+t=0 \bmod r$, we have

$$u+s=-(v+t) \bmod r.$$

$${}^1M+{}^1N$$

$$=(u+s)(A-C)+({}^1w+{}^1w_-)AB+({}^1z+{}^1z_-)BA \bmod r$$

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

Then we have

$$F_{UV}(\mathbf{1},{}^1M)+F_{UV}(\mathbf{1},{}^1N)$$

$$=F^{-ba}(({}^1M+{}^1N)\,(F^{-ba}(\mathbf{1})))$$

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

Next we calculate $|F_{UV}(\mathbf{1},{}^jM)\pm F_{UV}(\mathbf{1},{}^kN)|^2$ where $j,k\in\{1,2\}$.

1) $|F_{UV}(\mathbf{1},{}^1M)+F_{UV}(\mathbf{1},{}^1N)|^2$

$$=|{}^1M+{}^1N|^2$$

$$=|(u+s)(A-C)+({}^1w+{}^1w_-)AB+({}^1z+{}^1z_-)BA\,|^2 \bmod r$$

From (37a)

$$=-(u+s)^2 \bmod r\neq 0\in R \text{ (in general).}$$

2) $|F_{UV}(\mathbf{1},{}^1M)-F_{UV}(\mathbf{1},{}^1N)|^2$

$$=|{}^1M-{}^1N|^2$$

$$=|(u-s)A+(v-t)C+({}^1w-{}^1w_-)AB+({}^1z-{}^1z_-)BA\,|^2 \bmod r$$

$$=(u-s)(v-t) \bmod r\neq 0\in R \text{ (in general).}$$

3) $|F_{UV}(\mathbf{1},{}^1M)+F_{UV}(\mathbf{1},{}^2N)|^2$

$$=|{}^1M+{}^2N|^2 \bmod r$$

$$=|(u+t)A+(v-s)C+({}^1w+{}^2w_-)AB+({}^1z+{}^2z_-)BA\,|^2 \bmod r$$

$=(u+t)(v-s) \bmod r$

$=-(v+s)(v-s) \bmod r$

$=s^2-v^2 \bmod r$

$\neq 0 \in R$ (in general).

4) $|F_{UV}(\mathbf{1}, {}^1M)-F_{UV}(\mathbf{1}, {}^2N)|^2$

$=|{}^1M-{}^2N|^2 \bmod r$

$=|(u-t)A+(v+s)C+({}^1w-{}^2w_-)AB+({}^1z-{}^2z_-)BA\,|^2 \bmod r$

$=(u-t)(v+s) \bmod r$

$=-(u-t)(u+t) \bmod r$

$=t^2-u^2 \bmod r \neq 0 \in R$ (in general).

5) $|F_{UV}(\mathbf{1},{}^2M)+F_{UV}(\mathbf{1}, {}^1N)|^2=|{}^2M+{}^1N|^2 \bmod r$

$=|(v+s)A+(-u+t)C+({}^2w+{}^1w_-)AB+({}^2z+{}^1z_-)BA\,|^2 \bmod r$

$=(v+s)(-u+t) \bmod r$

$=-(u+t)(-u+t) \bmod r,$

$=u^2-t^2 \bmod r,$

$\neq 0 \in R$ (in general).

6) $|F_{UV}(\mathbf{1},{}^2M)-F_{UV}(\mathbf{1}, {}^1N)|^2=|{}^2M-{}^1N|^2 \bmod r$

$=|(v-s)A+(-u-t)C+({}^2w-{}^1w_-)AB+({}^2z-{}^1z_-)BA\,|^2 \bmod r$

$=-(v-s)(u+t) \bmod r$

$=(v-s)(v+s) \bmod r,$

$=v^2-s^2 \bmod r \neq 0 \in R$ (in general).

7) $|F_{UV}(\mathbf{1},{}^2M)+F_{UV}(\mathbf{1},{}^2N)|^2=|{}^2M+{}^2N|^2 \bmod r$

$=|(v+t)A+(-u-s)C+({}^2w+{}^2w_-)AB+({}^2z+{}^2z_-)BA\,|^2 \bmod r$

$=-(v+t)(u+s) \bmod r$

$=(v+t)(v+t) \bmod r,$

$=(v+t)^2 \bmod r,$

$\neq 0 \in R$ (in general).

8) $F_{UV}(\mathbf{1},{}^2M) - F_{UV}(\mathbf{1},{}^2N)|^2 = |{}^2M - {}^2N|^2 \bmod r$

$= |(v-t)A + (-u+s)C + ({}^2w - {}^2\bar{w})AB + ({}^2z - {}^2\bar{z})BA\,|^2 \bmod r$

$= (v-t)(-u+s) \bmod r$

$\neq 0 \in R$ (in general).

It is said that the attack by using " m and $-m$ attack" is not efficient. Then we cannot easily distinguish the ciphertexts of $-m$ by using the ciphertext $C(m,X) = (F_{UV}(X, {}^1M), F_{UV}(X, {}^2M))$.

§5.3 Attack by using the ciphertexts $C(m,X)$ of m

We try to obtain the plaintext m directly from the ciphertext $C(m,X) = (F_{UV}(X, {}^1M), F_{UV}(X, {}^2M))$ where

$F_{UV}(X,Y) = F^{-ba}(YF^{ba}(X))$,

$m = u+v \bmod r \in R$,

${}^1M = uA + vC + {}^1wAB + {}^1zBA \bmod r \in O$,

${}^2M = vA - uC + {}^2wAB + {}^2zBA \bmod r \in O$.

From Theorem 3 and (37a),(37b) we have

$L_1 := |F_{UV}(\mathbf{1}, {}^1M)|^2 = |{}^1M|^2 = uv \bmod r$,

$|F_{UV}(\mathbf{1}, {}^2M)|^2 = |{}^2M|^2 = -vu \bmod r$,

$L_2 := |F_{UV}(\mathbf{1}, {}^1M - {}^2M)|^2 = |{}^1M - {}^2M|^2 = (u-v)(v+u) = u^2 - v^2 \bmod r$,

$|F_{UV}(\mathbf{1}, {}^1M + {}^2M)|^2 = |{}^1M + {}^2M|^2 = (u+v)(v-u) = v^2 - u^2 \bmod r$.

If we can solve the following equation, we obtain $u^2 \bmod r$ and $v^2 \bmod r$.

$X^2 - L_2X - (L_1)^2 = 0 \bmod r$,

$X = \{L_2 + [(L_2)^2 + 4(L_1)^2]^{1/2}\}/2,\ \{L_2 - [(L_2)^2 + 4(L_1)^2]^{1/2}\}/2$.

We need to calculate $[(L_2)^2 + 4(L_1)^2]^{1/2}$ to solve the above equation.From Theorem 9, calculating $[(L_2)^2 + 4(L_1)^2]^{1/2}$ is as difficult as factorizing modulus r.

It is said that the attack by using the ciphertext $C(m,X)$ is not efficient.

§6. The size of the modulus *r* and the complexity for enciphering/deciphering

We consider the size of one of the system parameters, r.

Theorem 2 shows that the order l of an element $K \in O$ is LCM $\{ p^2-1, q^2-1\}$ in general. The complexity required for obtaining the discrete logarithm of $K^x \in O$ is O($sqrt(l)$) where l is the order of an element $K \in O$[12]. We select the size of r such that O($sqrt(l)$) is larger than 2^{2000}. Then we need to select modulus r such as $O(r) = 2^{2000}$.

We calculate the size of the parameter and the complexity required for the opration in k=8 of $F(X)=(S_k((...((S_1X)T_1))\ldots))T_k \bmod r = \{f_{ij}\}$ $(i,j=0,\ldots,7) \in O[X]$.

1) The size of $f_{ij} \in R(i,j=0,\ldots,7)$ which are the coefficients of elements in $F(X) \bmod r \in O[X]$ is $(64)(\log_2 r)$ bits =128kbits,
2) The size of $f_{aij} \in R(i,j=0,\ldots,7)$ which are the coefficients of elements in $F^a(X) \bmod q \in O[X]$ is $(64)(\log_2 r)$ bits =128kbits, and the size of system parameters $(r,A,B;F(X))$ is as large as 162kbits.
3) The complexity G_1 to obtain $F(X)$ is $(64*8*15)(\log_2 r)^2 = 2^{35}$ bit-operations.
4) The size of $F_{UV}(X,M) = F^{-ba}(YF^{ba}(X)) \in O[X,Y]$ is $(512)(\log_2 r)$ bits =1024 kbits.
5) The complexity G_2 to obtain $F^a(X), f_{aij} \in R$ $(i,j=0,\ldots,7)$ from $F(X)$ and a, is

   $(8*8*8)*2*(\log_2 r)*(\log_2 r)^2 = 2^{43}$ bit-operations.

6) The complexity G_3 to obtain $F^{-1}(X)$ from $F(X)$ by using Gaussian elimination is

   $\{8*(8^2+\ldots+2^2+1^2+1+2+\ldots+7)+7*(8+7+6+\ldots+2)\}(\log_2 r)^2+8*(\log_2 r)^3$

   $=2101*(\log_2 r)^2+ 8*(\log_2 r)^3 = 2^{37}$ bit-operations,

   because 8 simultaneus equations have the same coefficients and 8 inverse operations are required.

7) The complexity G_4 to obtain $F^{ab}(X)$ from $F^a(X)$ and b, is

   $(8*8*8)*2*(\log_2 q)*(\log_2 q)^2 = 2^{43}$ bit-operations.

8) The complexity G_5 to obtain $F_{UV}(X,Y) := F^{-ba}(YF^{ba}(X))$ from $F^{ba}(X)$ is

   $G_3+(512*8)*(\log_2 r)^2 = 2^{37}$ bit-operations.

9) The complexity $G_{encipher}$ for enciphering to calculate $C(m, X)=(F_{AB}(X,{}^1M), F_{AB}(X,{}^2M))$ from $F_{UV}(X,Y)$ and ${}^1M, {}^2M$ is $2*(64*8)*(\log_2 r)^2 = 2^{32}$ bit-operations.

The size of $C(m, X)=(F_{AB}(X,{}^1M), F_{AB}(X,{}^2M))$ is (64*2)* ($\log_2 r$) bits =256kbits.

We notice that the complexity $G_{encipher}$ required for enciphering every plaintext m is only 2^{32} bit-operations.

10) The complexity $G_{decipher}$ required for deciphering from $F_{VU}(X,{}^1M)$,$F_{UV}(X,{}^2M)$, $F^{ba}(X)$ and $F^{-ba}(X)$ is given as follows.

As

$$F_{VU}(X,{}^1M): =\{{}^1c_{ij}\}\ (i,j=0,\ldots,7),$$

$$F^{ba}(F_{VU}(F^{-ba}(\mathbf{1}),{}^1M))$$

$$= F^{ba}(\ F^{-ab}({}^1MF^{ab}(F^{-ba}(\mathbf{1})))) \bmod r$$

$$={}^1M,$$

$$m=2[{}^1M]_0 \bmod r \in R,$$

the complexity $G_{decipher}$ is $(64*2+1)(\log_2 r)^2= 2^{29}$ bit-operations.

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

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

where the size of modulus n is 2048bits.

Then our scheme requires smaller complexity to encipher a plaintext and decipher ciphertexts than RSA scheme.

§7. Conclusion

We proposed the fully homomorphic public-key encryption scheme with two ciphertexts based on the discrete logarithm assumption and computational Diffie–Hellman assumption. Our scheme requires not too large complexity to encipher and decipher. It was shown that our scheme is immune from "m and $-m$ attack"**.**

§8. BIBLIOGRAPHY

[1] Masahiro, Y. (2015). Fully Homomorphic Encryption without bootstrapping. Saarbrücken/Germany: LAP LAMBERT Academic Publishing.

[2] Mashiro Yagisawa," Fully Homomorphic Encryption without bootstrapping", Cryptology ePrint Archive, Report 2015/474, 2015. http://eprint.iacr.org/.

[3] Mashiro Yagisawa," Fully Homomorphic Encryption on Octonion Ring", Cryptology ePrint Archive, Report 2015/733, 2015. http://eprint.iacr.org/.

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

[5] Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices.In the 41st ACM Symposium on Theory of Computing (STOC), 2009.

[6] Craig Gentry, A Fully Homomorphic Encryption Scheme, 2009. Available at http://crypto.stanford.edu/craig/craig-thesis.pdf .

[7] 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.

[8] Damien Stehle; Ron Steinfeld (2010-05-19). "Faster Fully Homomorphic Encryption" (PDF). International Association for Cryptologic Research. Retrieved 2010-09-15.

[9] 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.

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

[11] 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/.

[12] Pollard, J.M.(1978),"Monte Carlo methods for index computation mod p", Mathematics of Computation 32(143);918-924. doi:10.2307/2006496

[13] Mashiro Yagisawa," Fully Homomorphic Encryption with Composite Number Modulus", Cryptology ePrint Archive, Report 2015/1040, 2015. http://eprint.iacr.org/.

[14] Mashiro Yagisawa," Improved Fully Homomorphic Encryption with Composite Number Modulus", Cryptology ePrint Archive, Report 2016/050, 2016. http://eprint.iacr.org/.

Appendix A:

Octinv(*A*) ----------

$S \leftarrow a_0^2+a_1^2+\ldots+a_7^2 \bmod r$.
% $S^{-1} \bmod r$
r[1] ← r div S ;% integer part of r/S
Res[1] ← r mod S ;% Residue
k ←1
r[0] ← r
Res[0] ← S
while Res[k] ≠ 0
begin
k← k + 1
r[k] ← Res[k−2] div Res[k−1]
Res[k] ← res[k−2] mod Res[k−1]
end
Q [k−1] ← (-1)∗r[k−1]
L[k−1] ← 1
i ← k−1
while i > 1
begin
Q[i−1] ← (-1)∗Q[i] ∗r[i−1] + L[i]
L[i−1] ← Q[i]
i← i−1
end

invS ← Q[1] mod *r*
invA[0] ← a_0∗invS mod *r*
For *i*=1,…,7,
invA[*i*] ← (-1)∗a_i∗invS mod *r*
Return A^{-1}= (invA[0], invA[1],…, invA[7])

Appendix B:

Theorem 1

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

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

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

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

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

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

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

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

(*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

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

[step 2]

When $n=k$,

If it holds that

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

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

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

from (9)

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

then

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

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

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

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

as was required. q.e.d.

Appendix C:

Theorem 2

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

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

where

$$J:= LCM\ \{q^2\text{-}1,q\text{-}1\}=q^2\text{-}1,$$
$$N:=a_{11}^2+ a_{12}^2+\ldots+a_{17}^2\neq 0 \bmod q.$$

(*Proof*:)

From (8) and (9) it comes that

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

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,

$$(-N)^{(q-1)/2}=-1 \bmod q.$$
$$a_{n0}\text{-}\ 2\ a_{10}\ a_{n\text{-}1,0} +(\ a_{10}^2 +N)\ a_{n\text{-}2,0}=0 \bmod q\ ,$$
$$a_{n0}=(\beta^n(a_{10}\text{-}\alpha) + (\beta\text{-}\ a_{10})\alpha^n)/(\ \beta\text{-}\ \alpha)\ over\ Fq[\alpha]$$
$$b_n=(\beta^n\text{-}\alpha^n)/(\ \beta\text{-}\ \alpha)\ over\ Fq[\alpha]$$

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

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

$$\alpha = a_{10} + \sqrt{-N}\ over\ Fq[\alpha],$$

$$\beta = a_{10} - \sqrt{-N}\ \ over\ Fq[\alpha].$$

We can calculate β^{q^2} as follows.

$$\beta^{q^2} = (a_{10} - \sqrt{-N})^{q^2} \quad over\ Fq[\alpha]$$

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

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

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

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

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

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

In the same manner we obtain

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

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

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

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

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 $\alpha,\beta \in Fq,$ 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

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

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)

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

$$= a_{10}{}^{n-1} + b_{n-1} a_{10} \bmod q$$

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

$$\ldots \quad \ldots$$

$$= (n-1) a_{10}{}^{n-1} + b_1 a_{10}{}^{n-1} \bmod q$$

$$= n a_{10}{}^{n-1} \bmod q.$$

Then we have

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

$$a_{qj} = q a_{10}{}^{q-1} a_{1j} \bmod q = 0, (j = 1,2,\ldots,7)\ .$$

Appendix D:
Lemma 2

$$A^{-1}(AB) = B \bmod r$$

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

(*Proof*:)

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

$$AB \bmod r$$

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

$$\begin{aligned}
&[A^{-1}(AB)]_0\\
&=\{ a_0(a_0b_0-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7)\\
&\quad +a_1(a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3)\\
&\quad + a_2(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6)\\
&\quad +a_3(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)\\
&\quad +a_4(a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5)\\
&\quad + a_5(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4)\\
&\quad +a_6(a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2)\\
&\quad +a_7(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0)\} /|A|^2 \bmod r\\
&=\{(a_0^2+a_1^2+\ldots+a_7^2) b_0\} /|A|^2 = b_0 \bmod r
\end{aligned}$$

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

$$
\begin{aligned}
&[A^{-1}(AB)]_1 \\
=&\{\, a_0(a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3) \\
&-a_1(a_0b_0-a_1b_1-\, a_2b_2-\, a_3b_3-a_4b_4-\, a_5b_5-a_6b_6-a_7b_7) \\
&-a_2(a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5) \\
&-a_3(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0) \\
&+a_4(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6) \\
&-\, a_5(a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2) \\
&+a_6(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4\,) \\
&+a_7(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)\}\ /|A|^2 \bmod r \\
=&\{(\, a_0^2+a_1^2+\ldots+a_7^2)\, b_1\}\ /|A|^2=b_1 \bmod r.
\end{aligned}
$$

Similarly we have

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

Then

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

Appendix E:

$$P=A^n \bmod r \in O$$

Power(A,n,r) ----------
$P \leftarrow 1$
while $n \neq 0$
begin
if n is even then $A \leftarrow A*A \bmod r$, $n \leftarrow n/2$
otherwise $P \leftarrow A*P \bmod r$, $n \leftarrow n$-1
end
Return P

Appendix F:

$$P(X)=A^n(X) \bmod r \in O[X]$$

Power($A(X)$,n,r) ----------
$P(X) \leftarrow \mathbf{1} \in O$
while $n \neq 0$
begin
if n is even then $A(X) \leftarrow A(A(X)) \bmod r$, $n \leftarrow n/2$
otherwise $P(X) \leftarrow A(P(X)) \bmod r$, $n \leftarrow n$-1
end
Return $P(X)$

Appendix G:
Theorem 9

Let O be the octonion ring over a finite ring R such that

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

Let $A,B \in O$ be the octonions such that

$$A=(a_0,a_1,\ldots,a_7),\ a_j \in R\ (j=0,1,\ldots,7),$$

$$B=(b_0,b_1,\ldots,b_7),\ b_j \in R\ (j=0,1,\ldots,7),$$

where

$$b_0=0 \bmod r\,,\ a_0=1/2 \bmod r\,,$$

$$a_0^2+a_1^2+\ldots+a_7^2=0 \bmod r,$$

$$b_0^2+b_1^2+\ldots+b_7^2=0 \bmod r$$

and

$$a_1b_1+ a_2b_2+a_3b_3+_4b_4+ a_5b_5+a_6b_6+a_7b_7=0 \bmod r.$$

A,B satisfy the following equations.

$$(AB)A= \mathbf{0} \bmod r,$$

$$(BA)B= \mathbf{0} \bmod r\,.$$

(*Proof*:)

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

$[(AB)A]_0 \bmod r$

$= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7)\, a_0$

$-(a_0b_1 + a_1b_0 + a_2b_4 + a_3b_7 - a_4b_2 + a_5b_6 - a_6b_5 - a_7b_3)\, a_1$

$-(a_0b_2 - a_1b_4 + a_2b_0 + a_3b_5 + a_4b_1 - a_5b_3 + a_6b_7 - a_7b_6)\, a_2$

$-(a_0b_3 - a_1b_7 - a_2b_5 + a_3b_0 + a_4b_6 + a_5b_2 - a_6b_4 + a_7b_1)\, a_3$

$-(a_0b_4 + a_1b_2 - a_2b_1 - a_3b_6 + a_4b_0 + a_5b_7 + a_6b_3 - a_7b_5)\, a_4,$

$-(a_0b_5 - a_1b_6 + a_2b_3 - a_3b_2 - a_4b_7 + a_5b_0 + a_6b_1 + a_7b_4)\, a_5$

$-(a_0b_6 + a_1b_5 - a_2b_7 + a_3b_4 - a_4b_3 - a_5b_1 + a_6b_0 + a_7b_2)\, a_6,$

$-(a_0b_7 + a_1b_3 + a_2b_6 - a_3b_1 + a_4b_5 - a_5b_4 - a_6b_2 + a_7b_0)\, a_7) \bmod r$

As

$b_0 = 0 \bmod r$,

$a_0^2 + a_1^2 + \ldots + a_7^2 = 0 \bmod r$,

$b_0^2 + b_1^2 + \ldots + b_7^2 = 0 \bmod r$

and

$a_1b_1 + a_2b_2 + a_3b_3 + {}_4b_4 + a_5b_5 + a_6b_6 + a_7b_7 = 0 \bmod r$,

we have

$[(AB)A]_0 \bmod r$

$= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7)\, a_0$

$-(a_0b_1 + a_1b_0 + a_2b_4 + a_3b_7 - a_4b_2 + a_5b_6 - a_6b_5 - a_7b_3)\, a_1$

$-(a_0b_2 - a_1b_4 + a_2b_0 + a_3b_5 + a_4b_1 - a_5b_3 + a_6b_7 - a_7b_6)\, a_2$

$-(a_0b_3 - a_1b_7 - a_2b_5 + a_3b_0 + a_4b_6 + a_5b_2 - a_6b_4 + a_7b_1)\, a_3$

$-(a_0b_4 + a_1b_2 - a_2b_1 - a_3b_6 + a_4b_0 + a_5b_7 + a_6b_3 - a_7b_5)\, a_4,$

$-(a_0b_5 - a_1b_6 + a_2b_3 - a_3b_2 - a_4b_7 + a_5b_0 + a_6b_1 + a_7b_4)\, a_5$

$-(a_0b_6 + a_1b_5 - a_2b_7 + a_3b_4 - a_4b_3 - a_5b_1 + a_6b_0 + a_7b_2)\, a_6$

$-(a_0b_7 + a_1b_3 + a_2b_6 - a_3b_1 + a_4b_5 - a_5b_4 - a_6b_2 + a_7b_0)\, a_7$

$= (a_0 0 - 0)\, a_0$

$$
\begin{aligned}
&- a_0 (a_1 b_1+a_2b_2+a_3b_3+a_4b_4+a_5b_5+a_6b_6+a_7b_7)\\
&- a_1(a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3-a_2b_4-a_3b_7+a_4b_2 -a_5b_6+a_6b_5+a_7b_3)\\
&- a_2 (a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6-a_3b_5-a_4b_1+a_5b_3-a_6b_7+a_7b_6)\\
&- a_3 (a_4b_6+a_5b_2-a_6b_4+a_7b_1-a_4b_6 -a_5b_2+ a_6b_4-a_7b_1)\\
&- a_4 (a_5b_7+ a_6b_3 -a_7b_5-a_5b_7- a_6b_3+a_7b_5)\\
&- a_5 (a_6b_1+a_7b_4-a_6b_1-a_7b_4)\\
&-(a_7b_2) a_6-(-a_6b_2) a_7\\
&=0 \bmod r,
\end{aligned}
$$

$$
\begin{aligned}
&[(AB)A]_1 \bmod r\\
&= \quad (a_0b_0 - a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7)a_1\\
&\quad +(a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3)a_0\\
&\quad +(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6)a_4\\
&\quad +(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)a_7\\
&\quad -(a_0b_4+a_1b_2 -a_2b_1 -a_3b_6+a_4b_0+a_5b_7+ a_6b_3 -a_7b_5)a_2\\
&\quad +(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4)a_6\\
&\quad -(a_0b_6+a_1b_5 -a_2b_7+a_3b_4 -a_4b_3 -a_5b_1+a_6b_0 +a_7b_2)a_5\\
&\quad -(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0)a_3\\
&= (a_00-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7)a_1\\
&\quad +2(a_1b_1+a_2b_2+a_3b_3+a_4b_4+a_5b_5+a_6b_6+a_7b_7)a_1\\
&\quad +(a_0b_1+0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3)a_0\\
&\quad +(a_0b_2-a_1b_4+0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6)a_4\\
&\quad +(a_0b_3-a_1b_7-a_2b_5+0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)a_7\\
&\quad -(a_0b_4+a_1b_2 -a_2b_1 -a_3b_6+0+a_5b_7+ a_6b_3 -a_7b_5)a_2\\
&\quad +(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+0+a_6b_1+a_7b_4)a_6\\
&\quad -(a_0b_6+a_1b_5 -a_2b_7+a_3b_4 -a_4b_3 -a_5b_1+0 +a_7b_2)a_5
\end{aligned}
$$

$$
\begin{aligned}
&-(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+0)a_3\\
&=b_1(a_1^2+a_0^2+a_4^2+a_7^2+a_2^2+a_6^2+a_5^2+a_3^2)\\
&+b_2(a_2a_1-a_4a_0+a_0a_4+a_5a_7-a_1a_2-a_3a_6-a_7a_5+a_6a_3)\\
&+b_3(a_3a_1-a_7a_0-a_5a_4+a_0a_7-a_6a_2+a_2a_6+a_4b_5-a_1a_3)\\
&+b_4(a_4a_1+a_2a_0-a_1a_4-a_6a_7-a_0a_2+a_7a_6-a_3a_5+a_5a_3)\\
&+b_5(a_5a_1-a_6a_0+a_3a_4-a_2a_7+a_7a_2+a_0a_6-a_1a_5-a_4a_3)\\
&+b_6(a_6a_1+a_5a_0-a_7a_4+a_4a_7+a_3a_2-a_1a_6-a_0a_5-a_2a_3)\\
&+b_7(a_7a_1+a_3a_0+a_6a_4-a_1a_7-a_5a_2-a_4a_6+a_2a_5-a_0a_3)\\
&=0 \bmod r.
\end{aligned}
$$

In the same manner we have

$$[(AB)A]_i=0 \bmod r \ (i=2,\ldots,7).$$

Then we have

$$(AB)A=\mathbf{0} \bmod r.$$

In the same manner we have

$$(BA)B=\mathbf{0} \bmod r.$$ q.e.d.

Appendix H:
Theorem 10

Let O be the octonion ring over a finite ring R such that

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

Let $A,B \in O$ be the octonions such that

$$A=(a_0,a_1,\ldots,a_7),\ a_j \in R\ (j=0,1,\ldots,7),$$

$$B=(b_0,b_1,\ldots,b_7),\ b_j \in R\ (j=0,1,\ldots,7),$$

where

$$b_0=0 \bmod r\ ,\ a_0=1/2 \bmod r\ ,$$

$$a_0^2+a_1^2+\ldots+a_7^2=0 \bmod r,$$

$$b_0^2+b_1^2+\ldots+b_7^2=0 \bmod r$$

and

$$a_1b_1+ a_2b_2+a_3b_3+_4b_4+ a_5b_5+a_6b_6+a_7b_7=0 \bmod r.$$

A,B satisfy the following equations.

$$AB+BA= B \bmod r.$$

(*Proof*:)

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

$$BA \bmod r$$

$$= (b_0a_0 - b_1a_1 - b_2a_2 - b_3a_3 - b_4a_4 - b_5a_5 - b_6a_6 - b_7a_7 \bmod r,$$

$$b_0a_1 + b_1a_0 + b_2a_4 + b_3a_7 - b_4a_2 + b_5a_6 - b_6a_5 - b_7a_3 \bmod r,$$

$$b_0a_2 - b_1a_4 + b_2a_0 + b_3a_5 + b_4a_1 - b_5a_3 + b_6a_7 - b_7a_6 \bmod r,$$

$$b_0a_3 - b_1a_7 - b_2a_5 + b_3a_0 + b_4a_6 + b_5a_2 - b_6a_4 + b_7a_1 \bmod r,$$

$$b_0a_4 + b_1a_2 - b_2a_1 - b_3a_6 + b_4a_0 + b_5a_7 + b_6a_3 - b_7a_5 \bmod r,$$

$$b_0a_5 - b_1a_6 + b_2a_3 - b_3a_2 - b_4a_7 + b_5a_0 + b_6a_1 + b_7a_4 \bmod r,$$

$$b_0a_6 + b_1a_5 - b_2a_7 + b_3a_4 - b_4a_3 - b_5a_1 + b_6a_0 + b_7a_2 \bmod r,$$

$$b_0a_7 + b_1a_3 + b_2a_6 - b_3a_1 + b_4a_5 - b_5a_4 - b_6a_2 + b_7a_0 \bmod r).$$

$$[AB + BA]_0 = a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7$$

$$+ b_0a_0 - b_1a_1 - b_2a_2 - b_3a_3 - b_4a_4 - b_5a_5 - b_6a_6 - b_7a_7$$

$$= 0 - 0 + 0 - 0 = 0 = b_0 \bmod r.$$

$$[AB + BA]_1 = a_0b_1 + a_1b_0 + a_2b_4 + a_3b_7 - a_4b_2 + a_5b_6 - a_6b_5 - a_7b_3$$

$$+ b_0a_1 + b_1a_0 + b_2a_4 + b_3a_7 - b_4a_2 + b_5a_6 - b_6a_5 - b_7a_3$$

$$= 2a_0b_1 = b_1 \bmod r.$$

In the same manner

$$[AB + BA]_i = b_i \quad (i = 2, \ldots, 7).$$

We have

$$AB + BA = B \bmod r. \qquad \text{q.e.d.}$$