FHPKE with Zero Norm Noises based on DLA&CDH

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

Abstract. In this paper I propose the fully homomorphic public-key encryption(FHPKE) scheme with zero norm noises that is based on the discrete logarithm assumption(DLA) and computational Diffie–Hellman assumption(CDH) of multivariate polynomials on octonion ring. Since the complexity for enciphering and deciphering become to be small enough to handle, the cryptosystem runs fast.
keywords: fully homomorphic public-key encryption, discrete logarithm assimption, computational Diffie–Hellman assumption, octonion ring

§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.

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 work I proposed some fully homomorphic encryptions [2],[3],[13], [14],[15],[16],[17]. And I also proposed "Fully Homomorphic Public-key Encryption Based on Discrete Logarithm Problem" [1].

In cloud computing system the fully homomorphic public-key system which runs fast is strongly required now.

In this paper I propose improved fully homomorphic public-key encryption with zero norm cipher text where zero norm medium text is generated and enciphered. 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 q be a fixed modulus to be as large prime as 2^{2000}. Later (in section 6) we discuss the size of one of the system parameters, q.

Let O be the octonion [4] ring over a finite field Fq.

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

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

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

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

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

$$A+B \bmod q$$
$$=(a_0+b_0 \bmod q,\ a_1+b_1 \bmod q,\ a_2+b_2 \bmod q,\ a_3+b_3 \bmod q,$$
$$a_4+b_4 \bmod q,\ a_5+b_5 \bmod q,\ a_6+b_6 \bmod q,\ a_7+b_7 \bmod q). \qquad (5)$$

Let

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

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

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

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

§2.2 Order of the element in *O*

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

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

Theorem 1

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

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

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

$$N:= a_{11}{}^2+\ldots+a_{17}{}^2 \quad \bmod q$$
$$a_{00}:=1,\ b_0:=0,\ b_1:=1,$$
$$a_{n0}= a_{n-1,0}\,a_{10} - b_{n-1}N \bmod q ,(n=1,2,\ldots), \qquad (8)$$
$$b_n = a_{n-1,0}+ b_{n-1}a_{10} \bmod q ,(n=1,2,\ldots), \qquad (9)$$
$$a_{nj}= b_na_{1j} \bmod q ,(n=1,2,\ldots;j=1,2,\ldots,7) . \qquad (10)$$

(*Proof*:)

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

Theorem 2

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

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

where

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

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

(*Proof*:)

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

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

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

1) Non-commutative

$$AB\neq BA \quad \bmod q.$$

2) Non-associative

$$A(BC)\neq(AB)C \quad \bmod q.$$

3) Alternative

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

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

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

4) Moufang's formulae [4],

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

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

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

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

5) For positive integers n,m, we have

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

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

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

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

From (15) and (19), we have

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

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

$$\dots \qquad \dots$$

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

In the same manner we have

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

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 (14) 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 manner 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 D**.

8) **Lemma 3**

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

(*Proof*:)

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

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

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

We multiply A from left side ,

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

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

$$ABA^{-1}.$$

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

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

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

10) **Lemma 4**

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

(*Proof*:)

From (17),

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

11) **Lemma 5**

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

(*Proof*:)

From (17),

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

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

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

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

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

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

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

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

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

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

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

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

12) **Lemma 6**

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

(*Proof*:)

From (16),

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Theorem 3

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

where

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

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

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

(*Proof*:)

$$A^2 \bmod q$$

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

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

where

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

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

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

Then we have

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

14) **Theorem 4**

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

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

(*Proof*:)

From **Theorem 3**

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

If we can express A^t such that

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

Then

$$A^{t+1} = (w_t\mathbf{1}+v_tA)A \bmod q$$
$$= w_tA+v_t(-L_A\ \mathbf{1}+2\ a_0A\ ) \bmod q$$
$$= -\ L_A\ v_t\mathbf{1}+(\ w_t+2a_0\mathrm{v}_\mathrm{t})A \bmod q.$$

We have

$$w_{t+1} = -\ L_A\ v_t \bmod q \in Fq,$$

$$v_{t+1}=w_t+2a_0v_t \mod q\in Fq. \quad \text{q.e.d.}$$

We can use **Power**(A,n,q) to obtain A^n mod q. (see the **Appendix E**)

15) **Theorem 5**

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

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

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

(*Proof*:)

When X=**1**, we have

$$BA=D \mod q.$$

Then

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

We can select $C\in O$ that satisfies

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

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

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

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

16) **Theorem 6**

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

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

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,

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

(*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 (13)

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

Multiplying C^{-1} from left side,

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

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

17) **Theorem 7**

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

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

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

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

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

(*Proof*:)

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

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

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

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

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

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

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

From (28) and (29) we have

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

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

18) **Theorem 8**

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

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

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

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

We can select $C \in O$ such that

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

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

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

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

From **Lemma 3**

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

From (17)

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

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

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

From **Lemma 3**

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

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

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

From (15) we have

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

Multiply A from right side we have

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

(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 $p\in Fq$ of the encryption schemes will be the element in finite field, 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 (**pk**, **sk**) ← **KeyGen**(1^λ) , where **pk** is a public encryption key and **sk** is a secret decryption key.

-Encryption. The algorithm **Enc**, on input system parameters $(q,A,B;F(X))$, public key **pk**, and a plaintext $p\in Fq$, random noises $u,v\in Fq$, outputs a ciphertext $C\in O[X]$ ←**Enc**(**pk**; p) where q is a large prime, $F(X)\in O[X]$.

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

-Homomorphic-Evaluation. The algorithm **Eval**, on input system parameters $(q,A,B;F(X))$, an arithmetic circuit ckt, and a tuple of n ciphertexts $(C_1,\ldots, C_n)\in \{O[X]\}^n$,

outputs a ciphertext $C'\in O[X]$←**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^λ), $\forall$ckt $\in CR_\lambda$, $\forall(p_1,\ldots,p_n)\in Fq^n$ where $n = n(\lambda)$, $\forall(C_1,\ldots,C_n)$ where C_i← **Enc**(**pk**;p_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 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 ***Fq***.

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 such that S_i^{-1} mod q and T_i^{-1} mod q exist (i=1,...,k).

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

$$\begin{aligned} F(X) &:= ((S_k((\ldots((S_1X)T_1))\ldots))T_k \bmod q\in O[X]\ ,\\ &=(f_{00}x_0+f_{01}x_0+\ \ldots+f_{07}x_7,\\ &\quad f_{10}x_0+f_{11}x_0+\ \ldots+f_{17}x_7,\\ &\quad \ldots\quad \ldots\\ &\quad f_{70}x_0+f_{71}x_0+\ \ldots+f_{77}x_7) \bmod q,\\ &=\{f_{ij}\}\ (i,j=0,\ldots,7) \end{aligned}$$

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

§4. Fully homomorphic public-key encryption scheme

§4.1 Public-key encryption function

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

$$F(X)=(S_k((\ldots((S_1X)T_1))\ldots))T_k \bmod q \in O[X],$$
$$=\{f_{ij}\}(i,j=0,\ldots,7).$$

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

$$F^{-1}(X):=S_1^{-1}((\ldots((S_k^{-1}(XT_k^{-1}))\ldots))\ T_1^{-1}) \bmod q \in O[X],$$
$$=(g_{00}x_0+\ldots+g_{07}x_7,$$
$$g_{10}x_0+\ldots+g_{17}x_7,$$
$$\ldots.\qquad\ldots.$$
$$g_{70}x_0+\ldots+g_{77}x_7) \bmod q,$$
$$=\{g_{ij}\}(i,j=0,\ldots,7)$$

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

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 q,

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

Then we obtain

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

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

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

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

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

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

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

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

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

We define $F^{i}(X)$ as follows where i is an integer.

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

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

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

....

We consider the communication between user U and user V. User U downloads the basic function $F(X)$ from cloud data centre or system centre. User U selects the random integer a to be secret and generates the public function $F^{a}(X)$ by using algorithm **Power**($F(X)$,a,q). (see the **Appendix F**)

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

On the other hand user V selects the random integer b to be secret and generates the public function $F^{b}(X)$ by using algorithm **Power**($F(X)$,b,q). User V sends the coefficient of $F^{b}(X)$, $f_{bij} \in \boldsymbol{Fq}$ $(i,j = 0,\ldots,7)$ 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, $F^{a}(X)$, $f_{aij} \in \boldsymbol{Fq}$ $(i,j = 0,\ldots,7)$ 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 encryption function $F_{\mathrm{VU}}(X,Y)$ between user U and user V as follows. By using algorithm **Power**($F^{a}(X)$,b,q) user V obtain $F^{ab}(X)$.

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

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

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

In the same manner user U generates the common encryption function

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

where

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

We notice that

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

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

$$A=(a_0,a_1,a_2,\ldots,a_7)\in O \text{ and } B=(b_0,b_1,b_2,\ldots,b_7)\in O,$$

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

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

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

$$b_0=0 \bmod q,$$

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

From Theorem 3 we have

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

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

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

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

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

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

where we denote the i-th element of octonion $M=(m_0,m_1,\ldots,m_7)$ such as

$$[M]_i=m_i\ (i=0,\ldots,7).$$

Theorem 9

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

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

(*Proof*:)

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

Theorem 10

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

(*Proof*:)

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

Theorem 11

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

$$(BA)(AB) =\mathbf{0} \bmod q, \tag{36b}$$

(*Proof*:)

From (17)

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

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

§4.2 Medium text

Here user V calculates the medium text M from the plaintext p which user V possesses as follows.

Let $p\in \boldsymbol{Fq}$ be a plaintext and $u,v\in \boldsymbol{Fq}$ be random noises.

The medium text M is defined by

$$M:= pA+uAB+vBA\in O.$$

As

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

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

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

We have

$$\begin{aligned}
&M^2=(pA+uAB+vBA)^2 \bmod q\\
&=(pA+uAB+vBA)\,(pA+uAB+vBA)\\
&= p^2A+puAB+vpBA\\
&=p(pA+uAB+vBA)\\
&=pM \bmod q.
\end{aligned}$$

On the other hand from Theorem 3

$$M^2=-L_M\mathbf{1}+2[M]_0M \bmod q.$$

From $[M]_0=pa_0=p/2 \bmod q$

$$M^2=-L_M\mathbf{1}+pM \bmod q.$$

Then for any $p,u,v\in \boldsymbol{Fq}$

$$L_M=|M|^2=|\, pA+uAB+vBA\,|^2=0 \bmod q. \tag{37}$$

Theorem 12 (linear independence)

If

$$M=pA+uAB+vBA=\mathbf{0}\in O,$$

then

$$p=u=v=0 \bmod q.$$

(*Proof*)

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

$$p=0 \bmod q.$$

We have

$$uAB+vBA=\mathbf{0} \bmod q.$$

By multiply A from right side from Theorem 9

$$u(AB)A+vBAA=\mathbf{0}A \bmod q,$$

$$u\mathbf{0}+vBA=\mathbf{0} \bmod q.$$

We have

$$v=0 \bmod q,$$

$$u=0 \bmod q. \qquad \text{q.e.d.}$$

Let

$$M_1:=p_1A+u_1AB+v_1BA \bmod q\in O,$$

$$M_2 := p_2A + u_2AB + v_2BA \bmod q \in O,$$

$$M_3 := p_3A + u_3AB + v_3BA \bmod q \in O.$$

Then we have

$$M_1 + M_2 = (p_1A + u_1AB + v_1BA) + (p_2A + u_2AB + v_2BA) \bmod q$$

$$= (p_1 + p_2)A + (u_1 + u_2)AB + (v_1 + v_2)BA \bmod q$$

and

$$M_1M_2 = (p_1A + u_1AB + v_1BA)(p_2A + u_2AB + v_2BA) \bmod q$$

$$= p_1p_2A + p_1u_2\, AB + v_1p_2BA \bmod q.$$

$$(M_1M_2)M_3$$

$$= [(p_1A + u_1AB + v_1BA)(p_2A + u_2AB + v_2BA)](p_3A + u_3AB + v_3BA) \bmod q$$

$$= (p_1p_2A + p_1u_2\, AB + v_1p_2BA)(p_3A + u_3AB + v_3BA)$$

$$= p_1p_2\, p_3A + p_1p_2\, u_3\, AB + v_1p_2\, p_3BA \bmod q.$$

$$M_1(M_2M_3)$$

$$= (p_1A + u_1AB + v_1BA)\, [\, (p_2A + u_2AB + v_2BA)\, (p_3A + u_3AB + v_3BA)\,] \bmod q$$

$$= (p_1A + u_1AB + v_1BA)\, (p_2p_3A + p_2u_3\, AB + v_2p_3BA)$$

$$= p_1p_2p_3A + p_1p_2\, u_3\, AB + v_1p_2\, p_3BA \bmod q.$$

Then we have

$$(M_1M_2)M_3 = M_1(M_2M_3) \bmod q.$$

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

We can obtain the plaintext p_1+p_2 from M_1+M_2 , the plaintext p_1p_2 from M_1M_2 and the plaintext $p_1p_2\, p_3$ from $M_1M_2\, M_3$ as follows.

$$2[M_1+M_2]_0 = 2(p_1+p_2)a_0 = p_1+p_2 \bmod q,$$

$$2[M_1M_2]_0 = 2\, p_1p_2a_0 = p_1p_2 \bmod q,$$

$$2[M_1M_2M_3]_0 = 2\, p_1p_2\, p_3a_0 = p_1p_2\, p_3 \bmod q,$$

where we denote the i-th element of octonion $M=(m_0,m_1,\ldots,m_7)$ such as

$$[M]_i = m_i.(i=0,\ldots,7)$$

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

$$A((BA)D) \neq (A(BA))D = (\mathbf{0})D = \mathbf{0}, \tag{38a}$$

$$A((AB)D) \neq (A(AB))D = (AB)D, \tag{38b}$$

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

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

§4.3 Enciphering

Let $(q,A,B;F(X))$ be system parameters.

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

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

User V generate medium text M by using the plaintyext p and random noises u,v such that

$$M := pA + uAB + vBA \in O.$$

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

$$\begin{aligned} &F_{\mathrm{VU}}(X,M) \\ &= (\, c_{00}x_0 + \ldots + c_{07}x_7\,, \\ &\quad\ \ \ldots \qquad \ldots \quad , \\ &\quad\ c_{70}x_0 + \ldots + c_{77}x_7\,) \bmod q \\ &= \{c_{ij}\}\ (i,j=0,\ldots,7)\,. \end{aligned}$$

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

§4.4 Deciphering

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

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

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

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

$=M=(m_0,\ldots,m_7)$,

$2m_0 \bmod q = p$.

Theorem 13

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

if $C(p,X)= C(p', X) \bmod q$, then $p= p' \bmod q$.

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

where

$$C(p, X)= F_{\mathrm{AB}}(X,M),$$

$$C(p',X)= F_{\mathrm{AB}}(X,M'),$$

$$M= pA+uAB+vBA \bmod q,$$

$$M'= p'A+u'AB+v'BA \bmod q.$$

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

$$F_{\mathrm{AB}}(X,M) = F_{\mathrm{AB}}(X,M'),$$

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

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

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

$$F^{ab}(F^{-ab}(M))= F^{ab}(F^{-ab}(M')) \bmod q,$$

$$M=M' \bmod q$$

where

$$pA+uAB+vBA = p'A+u'AB+v'BA \bmod q.$$

$$[pA+uAB+vBA]_0=[p'A+u'AB+v'BA]_0 \bmod q,$$

$$pa_0=p'a_0 \bmod q.$$

As $a_0\neq 0 \bmod q$, we have

$$p=p' \bmod q. \quad \text{q.e.d.}$$

§4.5 Addition scheme on ciphertexts

Let

$$M_1 := p_1A + u_1AB + v_1BA \in O,$$

$$M_2 := p_2A + u_2AB + v_2BA \in O$$

be medium texts to be encrypted.

Let $C_1(p_1,X) := F_{UV}(X,M_1)$ and $C_2(p_2,X) := F_{UV}(X,M_2)$ be the ciphertexts.

$$C_1(p_1,X) + C_2(p_2,X) \bmod q = F_{UV}(X,M_1) + F_{UV}(X,M_2) \bmod q$$

$$= F_{UV}(X,M_1+M_2) \bmod q$$

$$= F_{UV}(X, (p_1+p_2)A + (u_1+u_2)AB + (v_1+v_2)BA) \bmod q$$

$$= C(p_1+p_2,X) \bmod q.$$

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

§4.6 Multiplication scheme on ciphertexts

Here we consider the multiplicative operation on the ciphertexts.

Let $C_1(p_1,X) := F_{UV}(X,M_1)$ and $C_2(p_2,X) := F_{UV}(X,M_2)$ be the ciphertexts.

We calculate the ciphertext of the plaintext p_1p_2 such that

$$C(p_1,C(p_2,X)) \bmod q$$

$$= F_{UV}(F_{UV}(X,M_2),M_1) \bmod q$$

$$= F^{-ba}(M_1F^{ba}(F^{-ba}(M_2F^{ba}(X)))) \bmod q$$

$$= F^{-ba}(M_1(M_2F^{ba}(X))) \bmod q.$$

We can obtain the plaintext of the ciphertext $C(p_1,C(p_2,X))$ as follows.

$$F^{ba}\, C(p_1,C(p_2, F^{-ba}(\mathbf{1})))$$

$$= F^{ba}\,(F^{-ba}(M_1(M_2F^{ba}(F^{-ba}))))$$

$$= M_1M_2 \bmod q$$

$$2[M_1M_2 \bmod q]_0$$

$$=2[(p_1A+u_1AB+v_1BA)(p_2A+u_2AB+v_2BA) \bmod q]_0$$

$$= 2[p_1p_2A+p_1u_2\, AB + v_1p_2BA \bmod q\,]_0.$$

$$=2\, p_1p_2a_0 \bmod q$$

$$= p_1p_2 \bmod q.$$

Then we have

$$C(p_1,C(p_2,X)) = C(p_1p_2,X)) \bmod q.$$

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

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

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

Let q be a prime more than 2. Let a, b and k be integer parameters. Let $\boldsymbol{S}$:=(S_1,…,S_k)∈ O^k, $\boldsymbol{T}$:=(T_1,…,T_k)∈O^k such that S_1^{-1} ,…, S_k^{-1} and T_1^{-1} ,…, T_k^{-1} exist.

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

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

In the **DLA(F,F^a; q)** assumption, the adversary A_d is given $F^a(X)=\{f_{aij}\}$ (i,j=0,…,7), system parameters (q,A,B;$F(X)$) where $F(X)=\{f_{ij}\}$(i,j=0,…,7)and his goal is to find the integer $0<a<q^2$. 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;q)** 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;q)

Let q be a prime more than 2. Let a , b and k be integer parameters. Let $\boldsymbol{S}$:=(S_1,…,S_k)∈ O^k, $\boldsymbol{T}$:=(T_1,…,T_k)∈O^k such that S_1^{-1} ,…, S_k^{-1} and T_1^{-1} ,…, T_k^{-1} exist.

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

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

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

Let $C(p,X)=F_{\mathrm{UV}}(X,M)$ be the cipher text where $M= pA+uAB+vBA \bmod q \in O$, $p \in Fq$ is a plaintext, $u,v \in Fq$ are random noises , X is a variable.

In the **CDH(*F*,*F* *a*,*F* *b*;*q*)** assumption, the adversary A_d is given $F^{a}(X)=\{f_{aij}\}$, $F^{b}(X)=\{f_{bij}\}$ $(i,j=0,\ldots,7)$, system parameters $(q,A,B;F(X))$ and his goal is to find $F_{\mathrm{UV}}(X, Y)=F^{-ab}(YF^{ab}(X)) \bmod q$. 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 $[F(X)= \{f_{ij}\},F^{a}(X)=\{f_{aij}\}, F^{b}(X)=\{f_{bij}\}: F_{\mathrm{UV}}(X,Y)=F^{-ab}(YF^{ab}(X)) \leftarrow A_d (1^{\lambda}, \{f_{ij}\}, \{f_{aij}\} , \{f_{bij}\})]=$ negl(λ).

To solve directly **CDH(*F*,*F* *a*,*F* *b*;*q*)** 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 $(q,A,B;F(X))$, outputs (**pk**,**sk**)$\leftarrow$**KeyGen**(1^{λ}), where **pk**=[$\{f_{aij}\}$ $(i,j=0,\ldots,7)$] is a public key and **sk=**(a) is a secret key.

-Encryption. The algorithm **Enc**, on input system parameters $(q,A,B;F(X))$, public key **pk**=$\{f_{aij}\}$ $(i,j=0,\ldots,7)$ and a plaintext $p \in$ ***Fq***, outputs a ciphertext ***C***$(p,X)\leftarrow$**Enc(pk,**;p) where $M= pA+uAB+vBA \bmod q$.

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

-Homomorphic-Evaluation. The algorithm **Eval**, on input system parameters $(q,A,B;F(X))$, an arithmetic circuit ckt, and a tuple of n ciphertexts $(C_1,\ldots, C_n)$, outputs an evaluated ciphertext $C'\leftarrow$**Eval**(ckt; $C_1,\ldots, C_n$) where C_i=***C***(p_i,X) $(i=1,\ldots,n)$.

§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_λ, $\forall(p_1,\ldots,p_n) \in \boldsymbol{Fq}^n$ where $n = n(\lambda)$, $\forall(C_1,\ldots,C_n)$ where $C_i \leftarrow E(\mathbf{pk}; p_i)$, $M_i= p_iA+u_iAB+v_iBA$ mod q, $(i =1,\ldots,n)$, we have **Dec**(**sk**;**Eval**(ckt; $C_1,\ldots,C_n$)) = ckt($p_1,\ldots,p_n$).

Then it holds that:

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

2. Compactness: As the output length of **Eval** is at most $r\log_2 q=r\lambda$ where r 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 *p* from coefficients of ciphertext $F_{UV}(X,M)$ to be published

Ciphertext $F_{UV}(X, M_r)$ is published by cloud data centre or system centre as follows.

$$\begin{aligned}F_{UV}(X, M_r) &= F^{-ba}(M_rF^{ba}(X)) \bmod q \in O[X]\\ &=(c_{r00}x_0+c_{r01}x_1+ \ldots +c_{r07}x_7,\\ &\quad c_{r10}x_0+c_{r11}x_1+ \ldots +c_{r17}x_7,\\ &\quad \ldots\qquad \ldots\\ &\quad c_{r70}x_0+c_{r71}x_1+ \ldots +c_{r77}x_7) \bmod q,\\ &=\{c_{rij}\}(i,j=0,\ldots,7;r=0,\ldots,7)\end{aligned}$$

with $c_{rij}\in \boldsymbol{Fq}$ $(i,j,r=0,\ldots,7)$ which is published,

where

$$M_r= p_rA+u_rAB+v_rBA \bmod q\in O,$$

$$p_r,u_r,v_r\in \boldsymbol{Fq}\ (r=0,\ldots,7).$$

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

$$\begin{aligned}F_{UV}(X, Y) &= F^{-ba}(YF^{ba}(X)) \bmod q\in O[X,Y]\\ &=(d_{000}x_0y_0+d_{001}x_0y_1+ \ldots +d_{077}x_7y_7,\end{aligned}$$

$$d_{100}x_0y_0+d_{101}x_0y_1+\ldots+d_{177}x_7y_7,$$

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

$$d_{00}x_0y_0+d_{701}x_0y_1+\ldots+d_{777}x_7y_7) \bmod q,$$

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

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

Anyone except user U and user V does not know $\{d_{ijk}\}$ $(i,j,k=0,\ldots,7)$ which is a common enciphering function. Here we try to find $M_r=(m_{r0},\ldots,m_{r7})$ from $\{c_{rij}\}(i,j,r=0,\ldots,7)$ in condition that $d_{ijk}(i,j=0,\ldots,7)$ are unkown parameters. We have the following simultaneous equations from $F_{\mathrm{UV}}(X, Y)$ and $F_{\mathrm{UV}}(X, M)$ where $d_{ijk}(i,j=0,\ldots,7)$ and $(m_{r0},\ldots,m_{r7})$ are unknown variables.

$$\left.\begin{array}{c} d_{i00}m_{r0}+d_{i01}m_{r1}+\ldots+d_{i07}m_{r7}=c_{ri0} \bmod q \\ d_{i10}m_{r0}+d_{i11}m_{r1}+\ldots+d_{i17}m_{r7}=c_{ri1} \bmod q \\ \ldots \\ \ldots \\ d_{i70}m_{r0}+d_{i71}m_{r1}+\ldots+d_{i77}m_{r7}=c_{ri7} \bmod q \end{array}\right\}$$

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

For $M_r(r=0,\ldots,7)$ we obtain the same equations, the number of which is 512.
We also obtain 8 equations such as

$$|\,F_{\mathrm{UV}}(\mathbf{1}, M_r)|^2= c_{r00}{}^2+ c_{r10}{}^2+\ldots+c_{r70}{}^2 \bmod q$$

$$=|M_r|^2= m_{r0}{}^2+m_{r1}{}^2+\ldots+m_{r7}{}^2 \bmod q,(r=0,\ldots,7). \tag{40}$$

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

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

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

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

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 *p* and *-p*

I show that we cannot easily distinguish the ciphertexts of $-p$ by using the cipher text $C(p,X) = F_{\mathrm{UV}}(X, M)$.

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

$$M{:=}\, pA{+}uAB{+}vBA \bmod q \in O,$$

$$p,u,v \ \in \boldsymbol{Fq}$$

$$M_{-}{:=}\ {-}pA{+}u'AB{+}v'BA \bmod q \in O,$$

$$u',v' \ \in \boldsymbol{Fq}.$$

As

$$F_{\mathrm{UV}}(X, M){=}\, F^{\,-ba}(M\,F^{\,ba}(X)) \bmod q \in O[X]$$

$$F_{\mathrm{UV}}(X, M_{-}){=}\, F^{\,-ba}(M_{-}F^{\,ba}(X)) \bmod q \in O[X],$$

We have

$$F_{\mathrm{UV}}(X, M){+}\, F_{\mathrm{UV}}(X, M_{-}){=}\, F_{\mathrm{UV}}(X, M{+}M_{-}).$$

From p +($-p$)=0 mod q, we have

$$M + M_{-}$$

$$= pA{+}uAB{+}vBA\ {-}pA{+}u'AB{+}v'BA \bmod q$$

$$= (u{+}u')\,AB{+}(v{+}v')\,BA \bmod q$$

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

Then we have

$$F_{\mathrm{UV}}(X, M{+}M_{-}){\neq}\mathbf{0} \bmod q \text{ (in general).}$$

Next we show " p and $-p$ attack" is not efficient even if we can calculate

$|\,F_{\mathrm{UV}}(X, M)+ F_{\mathrm{UV}}(X, M_{-})\,|^2$ as follows.

$$L_{M+M-} := |\,F_{\mathrm{UV}}(X, M)+ F_{\mathrm{UV}}(X, M_{-})|^2 = |\,M+M_{-}\,|^2 \bmod q$$

$$\begin{aligned}
&(\,M+M_{-}\,)^2 \bmod q\\
&=((u+u')\,AB+(v+v')\,BA)^2 \bmod q\\
&=((u+u')^2\,(AB)^2+(u+u')\,(v+v')(\,AB)(\,BA)+\\
&\qquad (v+v')\,(u+u')(\,BA\,)(AB)+ (v+v')^2\,(BA)^{\,2} \bmod q.
\end{aligned}$$

As $(AB)^2=\mathbf{0}$, $(AB)\,(BA)=\mathbf{0}$, $(BA)\,(AB)=\mathbf{0}$, $(BA)^2=\mathbf{0}$, we have

$$(\,M+M_{-}\,)^2=\mathbf{0} \bmod q.$$

As from (33) $[M+M_{-}]_0= (u+u')\,[\,AB]_0+ (v+v')\,[\,BA]_0=0 \bmod q$, we have

$$\begin{aligned}
&(\,M+M_{-}\,)^2=-L_{M+M-}\mathbf{1}+2[M+M_{-}]_0(\,M+M_{-}\,)=\mathbf{0} \bmod q,\\
&L_{M+M-}=|\,F_{\mathrm{UV}}(X, M)+ F_{\mathrm{UV}}(X, M_{-})|^2= 0 \bmod q.
\end{aligned}$$

But we have always such equation as

$$|\,F_{\mathrm{UV}}(X, M)+ F_{\mathrm{UV}}(X, M')|^2=|M+M'|^2 \bmod q=0,$$

where

$$M'= p'A+u'AB+v'BA \bmod q\in O,$$

$$p'\in \boldsymbol{Fq}$$

because

$$\begin{aligned}
&|M+M'|^2 =|\,pA+uAB+vBA + p'A+u'AB+v'BA\,|^2\\
&=|(\,p+p')A +(\,u+u')AB+(v+v')BA|^2 \bmod q\\
&=0 \bmod q \text{ (from (37))}.
\end{aligned}$$

.

That is, even if

$$|\,F_{\mathrm{UV}}(X, M)+ F_{\mathrm{UV}}(X, M_{-})|^2=0 \bmod q,$$

it does not always hold that

$$p+p' =0 \bmod q.$$

It is said that the attack by using "p and $-p$ attack" is not efficient.

Then we cannot easily distinguish the ciphertexts of $-p$ by using the cipher text $C(p,X) = F_{\mathrm{UV}}(X, M)$.

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

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

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

1) In case of k=8, the size of $f_{ij} \in \boldsymbol{Fq}$ $(i,j=0,\ldots,7)$ which are the coefficients of elements in $F(X)$ mod $q \in O[X]$ is $(64)(\log_2 q)$bits =128kbits,
2) In case of k=8, the size of $f_{aij} \in \boldsymbol{Fq}$ $(i,j=0,\ldots,7)$ which are the coefficients of elements in $F^{a}(X)$ mod $q \in O[X]$ is $(64)(\log_2 q)$bits =128kbits,

   and the size of system parameters $(q,A,B;F(X))$ is as large as 162kbits.

3) In case of k=8 , the complexity G1 to obtain $F(X)$ is

   $(64*8*15)(\log_2 q)^2 = 2^{35}$ bit-operations.

4) In case of k=8, the size of $F_{\mathrm{UV}}(X,M) = F^{-ba}(YF^{ba}(X)) \in O[X,Y]$ is $(512)(\log_2 q)$bits =1024kbits.
5) In case of k=8 , the complexity G3 to obtain $F^{a}(X), f_{aij} \in \boldsymbol{Fq}$ $(i,j=0,\ldots,7)$ from $F(X)$ and a, is

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

6) In case of k=8 , the complexity G4 to obtain $F^{-1}(X)$ from $F(X)$ by using Gaussian elimination is

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

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

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

7) In case of k=8 , the complexity G5 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) In case of k=8 , the complexity G6 to obtain $F_{UV}(X,Y) := F^{-ba}(YF^{ba}(X))$ from $F^{ba}(X)$ is

$G4+(512*8)*(\log_2 q)^2 = 2^{37}$ bit-operations.

9) In case of k=8 , the complexity $G_{encipher}$ for enciphering to calculate $F_{UV}(X,M)$ from $F_{UV}(X,Y)$and M is

$(64*8)*(\log_2 q)^2 = 2^{31}$ bit-operations.

We notice that the complexity $G_{encipher}$ required for enciphering every plaintext M is only 2^{31} bit-operations.

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

As

$$F^{ba}(F_{UV}((F^{-ba}(\mathbf{1}),M))=M \bmod q$$

$$M=(m_0,m_1,\ldots,m_7)= (pA+uAB+vBA) \bmod q$$

$$2[M]_0=2pa_0=p \bmod q,$$

then the complexity $G_{decipher}$ is

$$(2*64+1)(\log_2 q)^2= 2^{29} \text{ bit-operations.}$$

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 a cipher text than RSA scheme.

§7. Conclusion

We proposed the fully homomorphism public-key encryption scheme with zero norm noises based on the discrete logarithm assumption and computational Diffie–Hellman assumption that requires not too large complexity to encipher and decipher. It was shown that our scheme is immune from "*p* and -*p* attack"**.**

§8. BIBLIOGRAPHY

[1] Mashiro Yagisawa," Fully Homomorphic Public-key Encryption Based on Discrete Logarithm Problem", Cryptology ePrint Archive, Report 2016/054, 2016. http://eprint.iacr.org/.
[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] Masahiro, Y. (2015). Fully Homomorphic Encryption without bootstrapping. Saarbrücken/Germany: LAP LAMBERT Academic Publishing.
[14] Mashiro Yagisawa," Fully Homomorphic Encryption with Composite Number Modulus", Cryptology ePrint Archive, Report 2015/1040, 2015. http://eprint.iacr.org/.
[15] Mashiro Yagisawa," Improved Fully Homomorphic Encryption with Composite Number Modulus", Cryptology ePrint Archive, Report 2016/050, 2016. http://eprint.iacr.org/.
[16] Mashiro Yagisawa," Fully Homomorphic Encryption with Isotropic Elements",

Cryptology ePrint Archive, Report 2016/462, 2016. http://eprint.iacr.org/.
[17] Mashiro Yagisawa," Fully Homomorphic Encryption with Zero Norm Cipher Text", Cryptology ePrint Archive, Report 2016/653, 2016. http://eprint.iacr.org/.

Appendix A:

Octinv(A) --

S ← $a_0^2+a_1^2+\ldots+a_7^2$ 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] $\neq$ 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] ← a_0*invS mod q

For i=1,…,7,

invA[i] ← (-1)*a_i*invS mod q

Return A^{-1}= (invA[0], invA[1],…, invA[7])

Appendix B:

Theorem 1

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

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

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

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

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

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

from (9)

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

then

$$\begin{aligned}A^{k+1}=A^kA&=(a_{k0},\ b_ka_{11},\ldots,\ b_ka_{17})(a_{10},a_{11},\ldots,a_{17})\\&=(a_{k0}\,a_{10}-b_kN,\ a_{k0}\,a_{11}+b_ka_{11}\,a_{10},\ldots,\ a_{k0}\,a_{17}+b_ka_{17}\,a_{10})\\&=(a_{k0}\,a_{10}-b_kN,\ (a_{k0}+b_ka_{10})a_{11},\ldots,\ (a_{k0}+b_ka_{10})a_{17})\\&=(a_{k+1,0},\ b_{k+1,0}\,a_{11},\ldots,\ b_{k+1,0}\,a_{17}),\end{aligned}$$

as was required. q.e.d.

Appendix C:

Theorem 2

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

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

where

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

(*Proof*:)

From (8) and (9) it comes that

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

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

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

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

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

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

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

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

We can calculate β^{q^2} as follows.

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

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

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

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

$$= a_{10} \quad - \sqrt{-N}(-1)(-1) \quad over\ \boldsymbol{Fq}[\alpha]$$

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

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

In the same manner we obtain

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

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

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

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

Then we obtain

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

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

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

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

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

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

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

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

Then we have

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

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

$$=a_{10} \mod q$$

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

Then we have

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

We therefore arrive at the equation such as

$A^{J+1}=A \bmod q$ for arbitrary element $A \in O$,

where

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

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)

$$a_{n0}= a_{n\text{-}1,0}\, a_{10} \bmod q\ ,(n=1,2,\ldots),$$

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),

$$b_n= a_{n\text{-}1,0}+ b_{n\text{-}1}a_{10} \bmod q\ ,(n=1,2,\ldots)$$
$$= a_{10}{}^{n\text{-}1}+ b_{n\text{-}1}a_{10} \bmod q$$
$$= 2a_{10}{}^{n\text{-}1}+ b_{n\text{-}2}a_{10}{}^2 \bmod q$$
$$\ldots \qquad \ldots$$
$$= (n\text{-}1)a_{10}{}^{n\text{-}1}+ b_1 a_{10}{}^{n\text{-}1} \bmod q$$
$$= na_{10}{}^{n\text{-}1} \bmod q.$$

Then we have

$$a_{nj}= na_{10}{}^{n\text{-}1}a_{1j} \bmod q\ ,(n=1,2,\ldots;j=1,2,\ldots,7)\ .$$
$$a_{qj}= qa_{10}{}^{q\text{-}1}a_{1j} \bmod q =0,(\,j=1,2,\ldots,7)\ .$$

Appendix D:
Lemma 2

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

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

(*Proof*:)

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

$AB \bmod q$

$= (a_0b_0-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7 \bmod q,$

$a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3 \bmod q,$

$a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6 \bmod q,$

$a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1 \bmod q,$

$a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5 \bmod q,$

$a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4 \bmod q,$

$a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2 \bmod q,$

$a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0 \bmod q)$.

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

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

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

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

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

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

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

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

$+a_7(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0)\} /|A|^2 \bmod q$

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

where $[M]_i$ 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

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

Then

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

Appendix E:

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

Power(A,n,q) --

$P \leftarrow 1$

while $n \neq 0$

begin

if n is even then $A \leftarrow A*A \bmod q$, $n \leftarrow n/2$

otherwise $P \leftarrow A*P \bmod q$, $n \leftarrow n-1$

end

Return P

Appendix F:

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

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

Appendix G:
Theorem 9

Let O be the octonion ring over a finite field Fq.

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

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

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

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

where

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

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

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

and

$$a_1b_1+a_2b_2+a_3b_3+{}_4b_4+a_5b_5+a_6b_6+a_7b_7=0 \bmod q.$$

A,B satisfy the following equations.

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

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

(*Proof*:)

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

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

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

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

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

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

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

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

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

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

As

$b_0=0 \bmod q$,

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

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

and

$a_1b_1+ a_2b_2+a_3b_3+_4b_4+ a_5b_5+a_6b_6+a_7b_7=0 \bmod q$,

we have

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

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

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

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

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

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

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

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

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

$=(a_00- 0)\, a_0$

$- a_0 (a_1 b_1+a_2b_2+a_3b_3+a_4b_4+a_5b_5+a_6b_6+a_7b_7)$

$- a_1(a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3-a_2b_4-a_3b_7+a_4b_2 -a_5b_6+a_6b_5+a_7b_3)$

$- a_2 (a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6-a_3b_5-a_4b_1+a_5b_3-a_6b_7+a_7b_6)$

$- a_3 (a_4b_6+a_5b_2-a_6b_4+a_7b_1-a_4b_6 -a_5b_2+ a_6b_4-a_7b_1)$

$- a_4 (a_5b_7+ a_6b_3 -a_7b_5-a_5b_7- a_6b_3+a_7b_5)$

$- a_5 (a_6b_1+a_7b_4-a_6b_1-a_7b_4)$

$-(a_7b_2) a_6-(-a_6b_2) a_7$

$=0 \bmod q,$

$[(AB)A]_1 \bmod q$

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

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

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

$+(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)a_7$

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

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

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

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

$= (a_00-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7)a_1$

$+2(a_1b_1+a_2b_2+a_3b_3+a_4b_4+a_5b_5+a_6b_6+a_7b_7)a_1$

$+(a_0b_1+0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3)a_0$

$+(a_0b_2-a_1b_4+0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6)a_4$

$+(a_0b_3-a_1b_7-a_2b_5+0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)a_7$

$-(a_0b_4+a_1b_2 -a_2b_1 -a_3b_6+0+a_5b_7+ a_6b_3 -a_7b_5)a_2$

$+(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+0+a_6b_1+a_7b_4)a_6$

$-(a_0b_6+a_1b_5 -a_2b_7+a_3b_4 -a_4b_3 -a_5b_1+0 +a_7b_2)a_5$

$-(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+0)a_3$

$= b_1 (a_1^2+a_0^2+a_4^2+a_7^2+a_2^2+a_6^2+a_5^2+a_3^2)$

$+ b_2 (a_2a_1-a_4a_0+a_0a_4+a_5a_7-a_1a_2-a_3a_6-a_7a_5+a_6a_3)$

$+ b_3 (a_3a_1 -a_7a_0 -a_5a_4+a_0a_7 -a_6a_2+a_2a_6+a_4b_5- a_1a_3)$

$+ b_4 (a_4a_1+a_2a_0-a_1a_4-a_6a_7-a_0a_2+a_7a_6-a_3a_5+a_5a_3)$

$+b_5 (a_5a_1-a_6a_0+a_3a_4-a_2a_7+a_7a_2+a_0a_6-a_1a_5-a_4a_3)$

$+ b_6 (a_6a_1+a_5a_0-a_7a_4+a_4a_7+a_3a_2-a_1a_6-a_0a_5-a_2a_3)$

$+b_7(a_7a_1+a_3a_0+a_6a_4-a_1a_7-a_5a_2-a_4a_6+a_2a_5-a_0a_3)$

$=0 \bmod q.$

In the same manner we have

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

Then we have

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

In the same manner we have

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

Appendix H:
Theorem 10

Let O be the octonion ring over a finite field Fq.

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

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

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

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

where

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

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

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

and

$$a_1b_1+ a_2b_2+a_3b_3+{}_4b_4+ a_5b_5+a_6b_6+a_7b_7=0 \bmod q.$$

A,B satisfy the following equations.

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

(*Proof*:)

$$AB \bmod q$$

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

$BA \bmod q$

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

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

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

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

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

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

$b_0a_6+b_1a_5 -b_2a_7+b_3a_4 -b_4a_3 -b_5a_1+b_6a_0 +b_7a_2 \bmod q,$

$b_0a_7+b_1a_3+b_2a_6-b_3a_1+b_4a_5-b_5a_4-b_6a_2+b_7a_0 \bmod q).$

$[AB +BA]_0= a_0b_0 - a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7$

$+ b_0a_0 - b_1a_1- b_2a_2- b_3a_3-b_4a_4- b_5a_5-b_6a_6-b_7a_7$

$=0-0+0-0=0 =b_0 \bmod q.$

$[AB +BA]_1= a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3$

$+ b_0a_1+b_1a_0+b_2a_4+b_3a_7-b_4a_2+b_5a_6-b_6a_5-b_7a_3$

$= 2a_0b_1= b_1 \bmod q$

In the same manner

$$[AB +BA]_{\mathrm{i}}= b_i \quad (i=2,\ldots,7).$$

We have

$$AB +BA =B \bmod q. \qquad \text{q.e.d.}$$