

# Fully homomorphic public-key encryption

## with small ciphertext size

Masahiro Yagisawa†

†Resident in Yokohama-shi

Sakae-ku, Yokohama-shi, Japan

[tfkt8398yagi@outlook.jp](mailto:tfkt8398yagi@outlook.jp)

**SUMMARY:** In previous work I proposed a fully homomorphic encryption without bootstrapping which has the *large* size of ciphertext. This time I propose the fully homomorphic public-key encryption scheme on non-associative octonion ring over finite field with the *small* size of ciphertext. In this scheme the size of ciphertext is one-third of the size in the scheme proposed before. Because proposed scheme adopts the medium text with zero norm, it is immune from the “ $p$  and  $-p$  attack”. As the proposed scheme is based on computational difficulty to solve the multivariate algebraic equations of high degree, it is immune from the Gröbner basis attack, the differential attack, rank attack and so on.

**keywords:** fully homomorphic public-key encryption, multivariate algebraic equation, Gröbner basis, non-associative 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, for instance, in the context of cloud computing.

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

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

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

In previous work [1], [2] I proposed a fully homomorphic encryption without bootstrapping which has the weak point in the enciphering function [17]. Next I proposed another FHPKE with the large size of ciphertext [18].

In this paper I propose a fully homomorphic encryption scheme with the small size of ciphertext which is based on computational difficulty to solve the multivariate algebraic equations of high degree while the almost all multivariate cryptosystems [3], [4], [5], [6], [7] proposed until now are based on the quadratic equations avoiding the explosion of the coefficients. Proposed scheme is immune from the Gröbner basis [8] attack, the differential attack, rank attack and so on.

In this scheme the size of ciphertext is 64 times as large as that of the modulus  $q$  while in the scheme proposed before the size of ciphertext is 192 times as large as that of the modulus  $q$  [18].

## §2. Preliminaries for octonion operation

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

### §2.1 Multiplication and addition on octonion ring $O$

Let  $q$  be a fixed modulus to be as large prime as  $O(2^{2000})$ . Let  $O$  be the octonion [16] ring over a finite field  $Fq$ .

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

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

$$A = (a_0, a_1, \dots, a_7), \ a_j \in Fq \ (j=0, 1, \dots, 7), \quad (2)$$

$$B = (b_0, b_1, \dots, b_7), \ b_j \in Fq \ (j=0, 1, \dots, 7). \quad (3)$$

$$AB \text{ mod } q$$

$$= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7 \text{ mod } q,$$

$$a_0b_1 + a_1b_0 + a_2b_4 + a_3b_7 - a_4b_2 + a_5b_6 - a_6b_5 - a_7b_3 \text{ mod } q,$$

$$\begin{aligned}
& a_0b_2 - a_1b_4 + a_2b_0 + a_3b_5 + a_4b_1 - a_5b_3 + a_6b_7 - a_7b_6 \pmod q, \\
& a_0b_3 - a_1b_7 - a_2b_5 + a_3b_0 + a_4b_6 + a_5b_2 - a_6b_4 + a_7b_1 \pmod q, \\
& a_0b_4 + a_1b_2 - a_2b_1 - a_3b_6 + a_4b_0 + a_5b_7 + a_6b_3 - a_7b_5 \pmod q, \\
& a_0b_5 - a_1b_6 + a_2b_3 - a_3b_2 - a_4b_7 + a_5b_0 + a_6b_1 + a_7b_4 \pmod q, \\
& a_0b_6 + a_1b_5 - a_2b_7 + a_3b_4 - a_4b_3 - a_5b_1 + a_6b_0 + a_7b_2 \pmod q, \\
& a_0b_7 + a_1b_3 + a_2b_6 - a_3b_1 + a_4b_5 - a_5b_4 - a_6b_2 + a_7b_0 \pmod q) \tag{4}
\end{aligned}$$

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

Let

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

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

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

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

## §2.2. Property of multiplication over octonion ring $O$

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

1) Non-commutative

$$AB \neq BA \pmod q. \tag{8}$$

2) Non-associative

$$A(BC) \neq (AB)C \pmod q. \tag{9}$$

3) Alternative

$$(AA)B = A(AB) \pmod q, \tag{10}$$

$$A(BB) = (AB)B \pmod q, \tag{11}$$

$$(AB)A = A(BA) \pmod q. \tag{12}$$

4) Moufang's formulae [16],

$$C(A(CB))=((CA)C)B \text{ mod } q, \quad (13)$$

$$A(C(BC))=((AC)B)C \text{ mod } q, \quad (14)$$

$$(CA)(BC)=(C(AB))C \text{ mod } q, \quad (15)$$

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

5)  $A$  and  $B \in O$  satisfy the following lemma.

**Lemma 1**

$$(A^{-1}B)A=A^{-1}(BA) \text{ mod } q. \quad (17)$$

*(Proof)*

From (12)

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

By multiplying  $A$  from right side we have

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

6)  $A \in O$  satisfies the following lemma.

**Lemma 2**

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

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

*(Proof:)*

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

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

**Theorem 1**

$$A^2=w\mathbf{1}+vA \text{ mod } q, \quad (18)$$

where

$$\exists w, v \in Fq,$$

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

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

*(Proof:)*

$$\begin{aligned}
& A^2 \bmod q \\
& = (a_0a_0 - a_1a_1 - a_2a_2 - a_3a_3 - a_4a_4 - a_5a_5 - a_6a_6 - a_7a_7 \bmod q, \\
& \quad a_0a_1 + a_1a_0 + a_2a_4 + a_3a_7 - a_4a_2 + a_5a_6 - a_6a_5 - a_7a_3 \bmod q, \\
& \quad a_0a_2 - a_1a_4 + a_2a_0 + a_3a_5 + a_4a_1 - a_5a_3 + a_6a_7 - a_7a_6 \bmod q, \\
& \quad a_0a_3 - a_1a_7 - a_2a_5 + a_3a_0 + a_4a_6 + a_5a_2 - a_6a_4 + a_7a_1 \bmod q, \\
& \quad a_0a_4 + a_1a_2 - a_2a_1 - a_3a_6 + a_4a_0 + a_5a_7 + a_6a_3 - a_7a_5 \bmod q, \\
& \quad a_0a_5 - a_1a_6 + a_2a_3 - a_3a_2 - a_4a_7 + a_5a_0 + a_6a_1 + a_7a_4 \bmod q, \\
& \quad a_0a_6 + a_1a_5 - a_2a_7 + a_3a_4 - a_4a_3 - a_5a_1 + a_6a_0 + a_7a_2 \bmod q, \\
& \quad a_0a_7 + a_1a_3 + a_2a_6 - a_3a_1 + a_4a_5 - a_5a_4 - a_6a_2 + a_7a_0 \bmod q) \\
& = (2a_0^2 - L \bmod q, 2a_0a_1 \bmod q, 2a_0a_2 \bmod q, 2a_0a_3 \bmod q, 2a_0a_4 \bmod q, \\
& \quad 2a_0a_5 \bmod q, 2a_0a_6 \bmod q, 2a_0a_7 \bmod q)
\end{aligned}$$

where

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

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

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

As  $A^2 = w\mathbf{1} + vA = -L\mathbf{1} + 2a_0A \bmod q$ , we have

$$\begin{aligned}
w & = -L \bmod q, \\
v & = 2a_0 \bmod q. \qquad \qquad \qquad \text{q.e.d.}
\end{aligned}$$

## Theorem 2

Let  $A^* = (a_0, -a_1, \dots, -a_7) \in O$  be the conjugate of  $A = (a_0, a_1, \dots, a_7) \in O$ . We have

$$AA^* = A^*A = L_A \mathbf{1}$$

where

$$L_A = a_0^2 + a_1^2 + \dots + a_7^2 \bmod q.$$

[Proof]

As

$$A+A^*=(2a_0,0,\dots,0)=2a_0\mathbf{1}\in O,$$

$$A^2=-L_A\mathbf{1}+2a_0A=-L_A\mathbf{1}+(A+A^*)A=-L_A\mathbf{1}+A(A+A^*)\text{ mod } q,$$

we have

$$L_A\mathbf{1}=A^*A=AA^*\text{ mod } q. \quad \text{q.e.d.}$$

### 8) Theorem 3

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

$$B(AX)=DX \text{ mod } q, \quad (19)$$

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

(Proof:)

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

$$BA=D \text{ mod } q.$$

Then

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

We can select  $C\in O$  that satisfies

$$B(AC)\neq(BA)C \text{ mod } q. \quad (20)$$

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

$$B(AC)=(BA)C \text{ mod } q. \quad (21)$$

(21) is contradictory to (20). q.e.d.

### 9) Theorem 4

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

$$C(B(AX))=DX \text{ mod } q \quad (22)$$

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

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

$$B(AC)\neq(BA)C \text{ mod } q. \quad (23)$$

(Proof:)

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

$$C(BA)=D \text{ mod } q.$$

Then

$$C(B(AX))=(C(BA))X \text{ mod } q.$$

We substitute  $C$  to  $X$  to obtain

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

From (12)

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

By multiplying  $C^{-1}$  from left side, we have

$$B(AC)=(BA)C \text{ mod } q \tag{24}$$

(24) is contradictory to (23).

q.e.d.

## 10) Theorem 5

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

$$C(B(AX))= E (DX) \text{ mod } q$$

where  $C, B, A, D$  and  $E \in O$  have inverse and  $X$  is a variable and  $A, B, C$  are non-associative, that is,

$$C(BA) \neq (CB)A \text{ mod } q. \tag{25}$$

(Proof:)

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

$$C(BA)=ED \text{ mod } q. \tag{26}$$

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

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

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

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

$$ED=(CB)A \text{ mod } q. \tag{27}$$

From (26) and (27) we have

$$C(BA) = (CB)A \pmod{q}. \quad (28)$$

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

### 11) **Theorem 6**

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

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

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

(Proof:)

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

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

Then

$$A(B(A^{-1}X)) = (A(BA^{-1}))X \pmod{q}. \quad (29)$$

We can select  $C \in O$  such that

$$(BA^{-1})(CA^2) \neq ((BA^{-1})C)A^2 \pmod{q}. \quad (30)$$

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

Substituting  $X = CA$  in (29), we have

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

From **Lemma 1**

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

From (16)

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

By multiplying  $A^{-1}$  from left side we have

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

From **Lemma 1**

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

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

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



From (14) we have

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

Multiply  $A$  from right side we have

$$((BA^{-1})(CA^2)) = ((BA^{-1})C)A^2 \pmod q. \quad (31)$$

(31) is contradictory to (30).

q.e.d.

### §3. Proposed fully homomorphic public-key encryption scheme

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

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

-Key-Generation. The algorithm **KeyGen**, on input the security parameter  $1^\lambda$ , outputs  $(\mathbf{sk}) \leftarrow \mathbf{KeyGen}(1^\lambda)$ , where  $\mathbf{sk}$  is a secret encryption/decryption key and  $(\mathbf{pk}) \leftarrow \mathbf{KeyGen}(1^\lambda)$ , where  $\mathbf{pk}$  is a public encryption/decryption key.

-Encryption. The algorithm **Enc**, on input system parameter  $(q, G, H)$ , secret key  $(\mathbf{sk})$ , public key  $(\mathbf{pk})$  and a plaintext  $p \in Fq$ , outputs a ciphertext  $C \in O \leftarrow \mathbf{Enc}(\mathbf{sk}, \mathbf{pk}; p)$  where  $G = (g_0, g_1, \dots, g_7) \in O$  and  $H = (h_0, h_1, \dots, h_7) \in O$ .

-Decryption. The algorithm **Dec**, on input system parameter  $(q, G, H)$ , secret key  $(\mathbf{sk})$ , public keys  $(\mathbf{pk})$  and a ciphertext  $C$ , outputs a plaintext  $p^* \leftarrow \mathbf{Dec}(\mathbf{sk}, \mathbf{pk}; C)$ .

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

### §3.2 Definition of fully homomorphic public-key encryption

A scheme HPKE 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 encryption scheme FHPKE :=(**KeyGen**; **Enc**; **Dec**; **Eval**) is fully homomorphic if it satisfies the following properties:

1. Homomorphism: Let  $CR = \{CR_\lambda\}_{\lambda \in \mathbb{N}}$  be the set of all polynomial sized arithmetic circuits. On input  $\mathbf{sk} \leftarrow \mathbf{KeyGen}(1^\lambda)$ ,  $\mathbf{pk} \leftarrow \mathbf{KeyGen}(1^\lambda)$ ,  $\forall \text{ckt} \in CR_\lambda$ ,  $\forall (p_1, \dots, p_n) \in Fq^n$  where  $n = n(\lambda)$ ,  $\forall (C_1, \dots, C_n)$  where  $C_i \leftarrow \mathbf{Enc}(\mathbf{sk}, \mathbf{pk}; p_i)$  ( $i=1, \dots, n$ ), it holds that:

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

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

### §3.3 Medium text

We define the medium text  $M \in O$  which is adopted in proposed fully homomorphic public-key encryption (FHPKE) scheme as follows.

We select the element  $G=(g_0, g_1, \dots, g_7) \in O$  and  $H=(h_0, h_1, \dots, h_7) \in O$  such that

$$[G]_0 = g_0 = 1/2 \pmod q, \quad (32a)$$

$$[H]_0 = h_0 = 0 \pmod q, \quad (32b)$$

$$L_G := |G|^2 = g_0^2 + g_1^2 + \dots + g_7^2 = 0 \pmod q, \quad (32c)$$

$$L_H := |H|^2 = h_0^2 + h_1^2 + \dots + h_7^2 = 0 \pmod q, \quad (32d)$$

$$g_1 h_1 + g_2 h_2 + \dots + g_7 h_7 = 0 \pmod q. \quad (32e)$$

where we denote the  $i$ -th element of octonion  $M \in O$  such as  $[M]_i$ .

Then we have

$$[GH]_0 = [HG]_0 = g_0 h_0 - (g_1 h_1 + g_2 h_2 + \dots + g_7 h_7) = 0 \pmod q, \quad (33a)$$

$$G^2 \pmod q = 2g_0 G = G, \quad (33b)$$

$$H^2 \pmod q = 2h_0 H = \mathbf{0} = (0, 0, \dots, 0). \quad (33c)$$

**Theorem 7**

$$GHG = \mathbf{0} \pmod{q}, \quad (34a)$$

$$HGH = \mathbf{0} \pmod{q}. \quad (34b)$$

(Proof:)

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

**Theorem 8**

$$(GH)(HG) = \mathbf{0} \pmod{q}, \quad (35a)$$

$$(HG)(GH) = \mathbf{0} \pmod{q}. \quad (35b)$$

(Proof:)

From (15)

$$(GH)(HG) = (G(HH))G = (G(\mathbf{0}))G = \mathbf{0} \pmod{q},$$

$$(HG)(GH) = (H(GG))H = (H(G))H = \mathbf{0} \pmod{q}. \quad \text{q.e.d.}$$

Table 1 gives the multiplication table of  $\{G, H, GH, HG\}$ .

Table1. multiplication table of  $\{G, H, GH, HG\}$ ..

	$G$	$H$	$GH$	$HG$
$G$	$G$	$GH$	$GH$	$\mathbf{0}$
$H$	$HG$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$GH$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$HG$	$HG$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$

Let  $p \in \mathbf{F}q$  be a plaintext and  $u, v, w \in \mathbf{F}q$  be the random numbers.

The medium text  $M$  is defined as

$$M := pG + uH + vGH + wHG \pmod{q} \in \mathbf{F}q. \quad (36)$$

The plaintext  $p$  is given from the medium text  $M$  such that

$$p= 2[M]_0 \text{ mod } q \in Fq. \quad (37)$$

### Lemma 3

For any  $A=(a_0,a_1,\dots,a_7) \in O, B=(b_0,b_1,\dots,b_7) \in O$

$$(A+B)^*=A^*+B^* \text{ mod } q, \quad (38a)$$

$$(AB)^*=B^*A^* \text{ mod } q \quad (38b)$$

where

$$A^*=(a_0,-a_1,\dots,-a_7) \in O, B^*=(b_0,-b_1,\dots,-b_7) \in O.$$

(Proof)

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

### Theorem 9

$$|M|^2=|pG+uH+vGH+wHG|^2=0 \text{ mod } q \in Fq. \quad (39)$$

(Proof:)

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

### Theorem 10

$$GH^*+HG^* = \mathbf{0} \text{ mod } q, \quad (40a)$$

$$G^*H+H^*G = \mathbf{0} \text{ mod } q. \quad (40b)$$

(Proof:)

As

$$HG^* =(GH^*)^*, H^*G =(G^*H)^*,$$

then

$$GH^*+ HG^*=2[GH^*]_0\mathbf{1}=2(g_0h_0+g_1h_1+g_2h_2+\dots + g_7h_7) \mathbf{1}=0\mathbf{1}=\mathbf{0} \text{ mod } q.$$

$$G^*H+H^*G =2[G^*H]_0\mathbf{1}=2(g_0h_0+g_1h_1+g_2h_2+\dots + g_7h_7) \mathbf{1}=0\mathbf{1}=\mathbf{0} \text{ mod } q.$$

q.e.d.

**Theorem 11**

$$G(H^*G^*)+(GH)G^* = \mathbf{0} \text{ mod } q, \quad (41a)$$

$$G^*(HG)+(G^*H^*)G = \mathbf{0} \text{ mod } q. \quad (41b)$$

(Proof:)

$$(GH)G^* = (G(GH)^*)^* = (G(H^*G^*))^*$$

Then

$$G(H^*G^*)+(GH)G^* = 2[(GH)G^*]_0 \mathbf{1}$$

$$= 2[(GH)(2g_0 \mathbf{1} - G)]_0 \mathbf{1}$$

$$= 2[(GH)2g_0 \mathbf{1} - (GH)G]_0 \mathbf{1}$$

$$= 2 [(GH) - \mathbf{0}]_0 \mathbf{1}$$

$$= 2 [GH]_0 \mathbf{1} = \mathbf{0} \text{ mod } q.$$

In the same manner

$$G^*(HG)+(G^*H^*)G = \mathbf{0} \text{ mod } q. \text{ q.e.d.}$$

**Theorem 12**

$$G(G^*H^*)+(HG)G^* = \mathbf{0} \text{ mod } q, \quad (42a)$$

$$G^*(GH)+(H^*G^*)G = \mathbf{0} \text{ mod } q. \quad (42b)$$

(Proof:)

As

$$((HG)G^*)^* = G(HG)^* = G(G^*H^*),$$

then

$$G(G^*H^*)+(HG)G^* = 2[(HG)G^*]_0 \mathbf{1}$$

$$= 2[(HG)(2g_0 \mathbf{1} - G)]_0 \mathbf{1}$$

$$= 2[(HG)2g_0 \mathbf{1} - (HG)G]_0 \mathbf{1}$$

$$= 2 [(HG) - HG]_0 \mathbf{1} = \mathbf{0} \text{ mod } q.$$

In the same manner

$$G^*(GH)+(H^*G^*)G = \mathbf{0} \text{ mod } q. \text{ q.e.d.}$$

**(Associativity of medium texts)**

Let  $M_1, M_2, M_3 \in O$  be arbitrary three medium texts where

$$M_1 := p_1G + u_1H + v_1GH + w_1HG \text{ mod } q \in O,$$

$$M_2 := p_2G + u_2H + v_2GH + w_2HG \text{ mod } q \in O,$$

$$M_3 := p_3G + u_3H + v_3GH + w_3HG \text{ mod } q \in O.$$

$$\begin{aligned} M_1 M_2 &= (p_1G + u_1H + v_1GH + w_1HG)(p_2G + u_2H + v_2GH + w_2HG) \text{ mod } q \\ &= p_1 p_2 G + \mathbf{0}H + (p_1 u_2 + p_1 v_2)GH + (u_1 p_2 + w_1 p_2)HG, \end{aligned}$$

$$\begin{aligned} (M_1 M_2) M_3 &= [p_1 p_2 G + (p_1 u_2 + p_1 v_2)GH + (u_1 p_2 + w_1 p_2)HG](p_3G + u_3H + v_3GH + w_3HG) \\ &= p_1 p_2 p_3 G + (p_1 p_2 u_3 + p_1 p_2 v_3)GH + (u_1 p_2 p_3 + w_1 p_2 p_3)HG, \end{aligned}$$

$$M_2 M_3 = p_2 p_3 G + (p_2 u_3 + p_2 v_3)GH + (u_2 p_3 + w_2 p_3)HG,$$

$$\begin{aligned} M_1 (M_2 M_3) &= (p_1G + u_1H + v_1GH + w_1HG)[p_2 p_3 G + (p_2 u_3 + p_2 v_3)GH + (u_2 p_3 + w_2 p_3)HG] \\ &= p_1 p_2 p_3 G + (p_1 p_2 u_3 + p_1 p_2 v_3)GH + (u_1 p_2 p_3 + w_1 p_2 p_3)HG. \end{aligned}$$

We have that

$$\begin{aligned} (M_1 M_2) M_3 &= p_1 p_2 p_3 G + (p_1 p_2 u_3 + p_1 p_2 v_3)GH + (u_1 p_2 p_3 + w_1 p_2 p_3)HG \\ &= M_1 (M_2 M_3) \text{ mod } q. \end{aligned} \tag{43a}$$

We have that

$$M_1 M_2 \dots M_h = p_1 p_2 \dots p_h G + \mathbf{0}H + (v_{12\dots h})GH + (w_{12\dots h})HG \text{ mod } q \in O, \tag{43b}$$

where

$$v_{12\dots h}, w_{12\dots h} \in \mathbf{F}q, M_i = p_i G + u_i H + v_i GH + w_i HG \text{ mod } q \in O, p_i, u_i, v_i, w_i \in \mathbf{F}q.$$

But we notice that in general for arbitrary  $N \in O$ ,

$$(M_1 M_2)N \neq M_1(M_2 N) \text{ mod } q.$$

Basic enciphering function  $E(X, Y)$  is defined as follows.

Let  $X=(x_0, \dots, x_7) \in O[X]$  and  $Y=(y_0, \dots, y_7) \in O[X]$  be variables.

$$E(X,Y):=A_1(\dots(A_r(Y(A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) \bmod q \in O[X,Y] \quad (44)$$

$$=(e_{000}x_0y_0 + e_{001}x_0y_1 + \dots + e_{077}x_7y_7,$$

$$e_{100}x_0y_0 + e_{101}x_0y_1 + \dots + e_{177}x_7y_7,$$

.....

$$e_{700}x_0y_0 + e_{701}x_0y_1 + \dots + e_{777}x_7y_7)^t, \quad (45)$$

$$= \{e_{ijk}\}(i,j,k=0, \dots, 7) \quad (46)$$

with  $e_{ijk} \in \mathbf{F}q$  ( $i,j,k=0, \dots, 7$ ) which is published by user A.

$A_i \in O$  is selected randomly such that  $A_i^{-1}$  exists ( $i=1, \dots, r$ ) which is the secret key of user A.

As if  $Y=\mathbf{1}$ , then  $E(X,Y)=X$ , some  $e_{ijk}$  are fixed such that

$$e_{000}=1, e_{010}=0, \dots, e_{070}=0,$$

$$e_{100}=0, e_{110}=1, \dots, e_{170}=0,$$

...

$$e_{700}=0, e_{710}=0, \dots, e_{770}=1.$$

### §3.5 Addition and multiplication of $E(X,Y)$

Let  $M_1$  and  $M_2$  be the medium texts corresponding to the plaintexts  $p_1$  and  $p_2$ , respectively.

We define the addition and multiplication on  $E(X,Y)$  as follows.

[Addition]

$$E(X, M_1) + E(X, M_2) \bmod q$$

$$= A_1(\dots(A_r(M_1(A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) + A_1(\dots(A_r(M_2(A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) =$$

$$A_1(\dots(A_r([M_1 + M_2](A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) \bmod q$$

$$= E(X, M_1 + M_2) \bmod q.$$

[Multiplication]

$$E(E(X, M_2), M_1) \bmod q$$

$$= A_1(\dots(A_r(M_1(A_r^{-1}(\dots(A_1^{-1}[A_1(\dots(A_r(M_2(A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots)]\dots))))\dots))$$

$$= A_1(\dots(A_r(M_1(M_2(A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) \bmod q.$$

We denote  $E(E(X, M_2), M_1)$  by  $E(X, M_1 \otimes M_2)$ .

We notice that in general

$$E(X, M_1 M_2) = A_1(\dots(A_r([M_1 M_2](A_r^{-1}(\dots(A_1^{-1} X)\dots))))\dots) \bmod q$$

$$\neq A_1(\dots(A_r(M_1(M_2(A_r^{-1}(\dots(A_1^{-1} X)\dots))))\dots) \bmod q = E(X, M_1 \otimes M_2).$$

### Theorem 13

For arbitrary plaintexts  $p, p' \in O$ ,

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

where

$$M := pG + uH + vGH + wHG \in O,$$

$$M' := p'G + u'H + v'GH + w'HG \in O.$$

(Proof)

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

$$A_r^{-1}(\dots(A_1^{-1}(E(A_1(\dots(A_r \mathbf{1})\dots))), M) \bmod q = M$$

$$= A_r^{-1}(\dots(A_1^{-1}(E(A_1(\dots(A_r \mathbf{1})\dots))), M') \bmod q = M' \bmod q.$$

Then we have

$$M = M'.$$

$$p = 2[M]_0 \bmod q \in \mathbf{F}q,$$

$$= 2[M']_0 \bmod q \in \mathbf{F}q,$$

$$= p' \bmod q.$$

Then we have

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

### §3.6 Octonion elements assumption OEA( $q$ )

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

#### Octonion Elements assumption OEA( $q$ )

Let  $q$  be a prime more than 2. Let  $r$  be a secret integer parameter. Let  $A := \{A_1, \dots, A_r\} \in \mathcal{O}^r$  be secret parameters. Let  $E(X, Y) = A_1(\dots(A_r(Y(A_r^{-1}(\dots(A_1^{-1} X)\dots))))\dots) \bmod q \in \mathcal{O}[X, Y]$  be the basic enciphering function where  $X$  and  $Y$  are variables.

In the OEA( $q$ ) assumption, the adversary  $A_d$  is given  $E(X, Y)$  and his goal is to find a set of parameters  $A = \{A_1, \dots, A_r\} \in \mathcal{O}^r$  with the order of the elements  $A_1, \dots, A_r$ .



For parameters  $r = r(\lambda)$  defined in terms of the security parameter  $\lambda$  and for any PPT adversary  $A_d$  we have

$$\Pr [E(X, Y) = A_1(\dots(A_r(Y(A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) \bmod q = \{e_{ijk}\}(i, j, k = 0, \dots, 7) : \\ A = \{A_1, \dots, A_r\} \leftarrow A_d(1^\lambda, q, E(X, Y))] = \text{negl}(\lambda).$$

To solve directly **OE**A( $q$ ) assumption is known to be the problem for solving the multivariate algebraic equations of high degree which is known to be NP-hard.

Next it is shown that the ciphertext  $C(X, p) := E(X, M)$  corresponding to the plaintexts  $p$  has the property of fully homomorphism where  $M = pG + uH + vGH + wHG \bmod q \in Fq$ .

### §3.7 Addition scheme on ciphertexts

Let

$$M_1 := p_1 \mathbf{1} + u_1 G + v_1 H + w_1 GH \in O,$$

$$M_2 := p_2 \mathbf{1} + u_2 G + v_2 H + w_2 GH \in O,$$

be medium texts to be encrypted.

Let  $C(X, p_1) := E(X, M_1) \in O[X]$  and  $C(X, p_2) := E(X, M_2) \in O[X]$  be the ciphertexts corresponding to the plaintexts  $p_1$  and  $p_2$ , respectively.

$$\begin{aligned} C(X, p_1) + C(X, p_2) \bmod q &:= E(X, M_1) + E(X, M_2) \bmod q \\ &= A_1(\dots(A_r(M_1(A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) + A_1(\dots(A_r(M_2(A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) \bmod q \\ &= A_1(\dots(A_r([M_1 + M_2](A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) \bmod q \\ &= E(X, M_1 + M_2) \bmod q. \end{aligned}$$

We have

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

It has been shown that in this method we have the additive homomorphism.

### §3.8 Multiplication scheme on ciphertexts

Here we consider the multiplicative operation on the ciphertexts.

Let

$$C(X, p_1) := E(X, M_1) \in O[X]$$

and

$$C(X,p_2):=E(X,M_2)\in O[X]$$

be the ciphertexts corresponding to the plaintexts  $p_1$  and  $p_2$ , respectively.

Let

$$C(X,p_{12})=E(X,M_{12})\in O[X]$$

$$:=E(E(X,M_2),M_1) \bmod q$$

$$=A_1(\dots(A_r(M_1(A_r^{-1}(\dots(A_1^{-1}[A_1(\dots(A_r(M_2(A_r^{-1}(\dots(A_1^{-1}X)\dots))))))\dots))))))\dots)$$

$$=A_1(\dots(A_r(M_1(M_2(A_r^{-1}(\dots(A_1^{-1}X)\dots))))))\dots) \bmod q.$$

We confirm that  $C(X,p_{12})$  is the ciphertext corresponding to the plaintext  $p_1p_2$ , that is, we decipher  $C(X,p_{12})$  to obtain  $p_1p_2$  as follows.

$$M_{12}:=A_r^{-1}(\dots(A_1^{-1}(C(A_1(\dots(A_r\mathbf{1})\dots),p_{12}))))\dots)$$

$$=A_r^{-1}(\dots(A_1^{-1}(A_1(\dots(A_r(M_1(M_2(A_r^{-1}(\dots(A_1^{-1}(A_1(\dots(A_r\mathbf{1})\dots))))))\dots))))\dots))$$

$$=M_1(M_2\mathbf{1})\bmod q,$$

$$=M_1M_2 \bmod q,$$

$$=p_1p_2G+\mathbf{0}H+(p_1u_2+p_1v_2)GH+(u_1p_2+w_1p_2)HG \bmod q \in O.$$

From (37) we have

$$p_{12}=2[M_1M_2]_0 \bmod q,$$

$$=p_1p_2 \bmod q \in Fq.$$

### §3.9 Property of proposed fully homomorphic encryption

The syntax of proposed scheme is given as follows.

-Key-Generation. The algorithm **KeyGen**, on input the security parameter  $1^\lambda$  and system parameter  $(q,G,H)$  outputs

$\mathbf{sk} \leftarrow \mathbf{KeyGen}(1^\lambda)$  where  $\mathbf{sk}=(r, A_j(j=1, \dots, r))$  is a secret encryption key and

$\mathbf{pk} \leftarrow \mathbf{KeyGen}(1^\lambda)$  where  $\mathbf{pk}=(\{e_{ijk}\}_{0 \leq i,j,k \leq 7})$  is a public key.

-Encryption. The algorithm **Enc**, on input system parameter  $q$ , and secret keys of user B,  $\mathbf{sk}_B=(r_B, B_j(j=1, \dots, r_B))$ , public key of user A,  $\mathbf{pk}_A=(\{e_{Aijk}\}_{0 \leq i,j,k \leq 7})$  and a plaintext  $p \in Fq$ , outputs a ciphertext  $C(X;\mathbf{sk}_B, \mathbf{pk}_A, p) \leftarrow \mathbf{Enc}(\mathbf{sk}_B, \mathbf{pk}_A; p)$ .

-Decryption. The algorithm **Dec**, on input system parameter  $q$ , secret keys of user A,  $\mathbf{sk}_A$ , public key of user B,  $\mathbf{pk}_B$  and a ciphertext  $C(X; \mathbf{sk}_B, \mathbf{pk}_A, p)$ , outputs plaintext  $\mathbf{Dec}(\mathbf{sk}_A, \mathbf{pk}_B; C(X; \mathbf{sk}_B, \mathbf{pk}_A, p))$  where  $C(X; \mathbf{sk}_B, \mathbf{pk}_A, p) \leftarrow \mathbf{Enc}(\mathbf{sk}_B, \mathbf{pk}_A; p)$ .

-Homomorphic-Evaluation. The algorithm **Eval**, on input system parameter  $q$ , an arithmetic circuit  $\text{ckt}$ , and a tuple of  $n$  ciphertexts  $(C_1, \dots, C_n)$ , outputs an evaluated ciphertext  $C' \leftarrow \mathbf{Eval}(\text{ckt}; C_1, \dots, C_n)$  where  $C_i = C(X; \mathbf{sk}_B, \mathbf{pk}_A, p_i)$  ( $i=1, \dots, n$ ).

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

1. Homomorphism: Let  $CR = \{CR_\lambda\}_{\lambda \in \mathbb{N}}$  be the set of all polynomial sized arithmetic circuits. On input  $\mathbf{sk} \leftarrow \mathbf{KeyGen}(1^\lambda)$ ,  $\mathbf{pk} \leftarrow \mathbf{KeyGen}(1^\lambda)$ ,  $\forall \text{ckt} \in CR_\lambda$ ,  $\forall (p_1, \dots, p_n) \in Fq^n$  where  $n = n(\lambda)$ ,  $\forall (C_1, \dots, C_n)$  where  $C_i = C(X; \mathbf{sk}_B, \mathbf{pk}_A, p_i) \leftarrow \mathbf{Enc}(\mathbf{sk}_B, \mathbf{pk}_A; p_i)$ , ( $i=1, \dots, n$ ), we have  $\mathbf{Dec}(\mathbf{sk}_A, \mathbf{pk}_B; \mathbf{Eval}(\text{ckt}; C_1, \dots, C_n)) = \text{ckt}(p_1, \dots, p_n)$ .

Then it holds that:

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

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

### §3.10 Procedure for constructing public-key encryption

For the understanding we show the procedure for constructing the public-key encryption scheme by using the cryptosystem described in above sections.

User B try to send his information to user A by using the public-key of user A  $\mathbf{pk}_A$  and the secret key of user B  $\mathbf{sk}_B$  through the insecure line.

- 1) System centre publishes the system parameter  $[q, G, H]$ .
- 2) User A downloads the system parameter  $[q, G, H]$  and calculates  $GH, HG$ .
- 3) User A selects  $\mathbf{sk}_A = (r_A, A_j (j=1, \dots, r_A))$  which is a secret key of user A and generates the public key of user A  $\mathbf{pk}_A = (\{e_{A_{ijk}}\}_{0 \leq i, j, k \leq 7})$  such that
 
$$E_A(X, Y) := A_1(\dots(A_{r_A}(Y(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots)))) \dots) \bmod q \in O[X, Y]$$

$$= \{e_{A_{ijk}}\} (i, j, k=0, \dots, 7).$$

User A sends  $\{e_{Aijk}\}(i,j,k=0,\dots,7)$  to system centre.

- 4) User B downloads the system parameter  $[q,G,H]$  and calculates  $GH, HG$ .  
 5) User B selects  $\mathbf{sk}_B=(r_B, A_{Bj}(j=1,\dots,r_B))$  which is a secret key of user B and

generates the public key of user B  $\mathbf{pk}_B=(\{e_{Bijk}\}_{0\leq i,j,k\leq 7})$  such that  
 $E_B(X,Y):=B_1(\dots(B_{r_B}(Y(B_{r_B}^{-1}(\dots(B_1^{-1}X)\dots))))\dots)\bmod q\in O[X,Y]$   
 $=\{e_{Bijk}\}(i,j,k=0,\dots,7).$

User B sends  $\{e_{Bijk}\}(i,j,k=0,\dots,7)$  to system centre.

- 6) User B downloads  $E_A(X,Y)=\{e_{Aijk}\}(i,j,k=0,\dots,7)$  from system centre.  
 7) User B generates the common enciphering function  $E_{BA}(X,Y)$  as follows.

$$\begin{aligned} E_{B1}(X,Y) &:= E_A(E_A(X,Y), B_1) \\ &= A_1(\dots(A_{r_A}(B_1(A_{r_A}^{-1}(\dots(A_1^{-1}[A_1(\dots(A_{r_A}(Y(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots)]\dots))))\dots))\dots) \\ &= A_1(\dots(A_{r_A}(B_1(Y(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots))\dots)\bmod q\in O[X,Y] \end{aligned}$$

$$\begin{aligned} E_{B2}(X,Y) &:= E_{B1}(E_A(X,Y), B_2) \\ &= A_1(\dots(A_{r_A}(B_1(B_2(A_{r_A}^{-1}(\dots(A_1^{-1}[A_1(\dots(A_{r_A}(Y(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots)]\dots))))\dots))\dots) \\ &= A_1(\dots(A_{r_A}(B_1(B_2(Y(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots))\dots))\bmod q\in O[X,Y] \end{aligned}$$

... ..

$$\begin{aligned} E_{B_{rB}}(X,Y) &:= E_{B_{rB-1}}(E_A(X,Y), B_{rB}) \\ &= A_1(\dots(A_{r_A}(B_1(\dots(B_{rB}(A_{r_A}^{-1}(\dots(A_1^{-1}[A_1(\dots(A_{r_A}(Y(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots)]\dots))))\dots))\dots))\dots) \\ &= A_1(\dots(A_{r_A}(B_1(\dots(B_{rB}(Y(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots))\dots))\dots)\bmod q\in O[X,Y] \end{aligned}$$

$$\begin{aligned} E_{B_{rB}^{-1}}(X,Y) &:= E_{B_{rB}}(E_A(X, B_{rB}^{-1}), Y) \\ &= A_1(\dots(A_{r_A}(B_1(\dots(B_{rB}(Y(A_{r_A}^{-1}(\dots(A_1^{-1}[A_1(\dots(A_{r_A}(B_{rB}^{-1}(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots)]\dots))))\dots))\dots))\dots) \\ &= A_1(\dots(A_{r_A}(B_1(\dots(B_{rB}(Y(B_{rB}^{-1}(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots))\dots))\dots))\bmod q\in O[X,Y] \end{aligned}$$

$$\begin{aligned} E_{B_{rB-1}^{-1}}(X,Y) &= E_{B_{rB}^{-1}}(E_A(X, B_{rB-1}^{-1}), Y) \\ &= A_1(\dots(A_{r_A}(B_1(\dots(B_{rB}(Y(B_{rB}^{-1}(A_{r_A}^{-1}(\dots(A_1^{-1}[A_1(\dots(A_{r_A}(B_{rB-1}^{-1}(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots)]\dots))))\dots))\dots))\dots) \\ &= A_1(\dots(A_{r_A}(B_1(\dots(B_{rB}(Y(B_{rB}^{-1}(B_{rB-1}^{-1}(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))\dots))\dots))\dots))\dots)\bmod q\in O[X,Y] \end{aligned}$$

... ..



$$2[M]_0 \bmod q = p \in \mathbf{F}q.$$

#### §4. Analysis of proposed scheme

Here we analyze the proposed fully homomorphism encryption scheme.

##### §4.1 Computing $A_i$ from coefficients of $E(X,Y)$

Basic enciphering function  $E(X,Y)$  is given as follows.

Let  $X=(x_0, \dots, x_7) \in O[X]$  and  $Y=(y_0, \dots, y_7) \in O[X]$  be variables.

$$E(X,Y) = A_1(\dots(A_r(Y(A_r^{-1}(\dots(A_1^{-1}X)\dots)))) \dots) \bmod q \in O[X,Y] \quad (47)$$

$$= (e_{000}x_0y_0 + e_{001}x_0y_1 + \dots + e_{077}x_7y_7,$$

$$e_{100}x_0y_0 + e_{101}x_0y_1 + \dots + e_{177}x_7y_7,$$

.... ..

$$e_{700}x_0y_0 + e_{701}x_0y_1 + \dots + e_{777}x_7y_7)^t, \quad (48)$$

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

$A_j \in O$  to be selected randomly such that  $A_j^{-1}$  exist ( $j=1, \dots, r$ ) are parts of the secret keys of user A.

We try to find  $A_i (i=1, \dots, r)$  from coefficients of  $E(X,Y)$ ,  $e_{ijk} \in \mathbf{F}q (i,j,k=0, \dots, 7)$ .

In case that  $r=56$  the number of unknown variables ( $A_j (j=1, \dots, 56)$ ) is 448 ( $=56*8$ ), the number of equations is 448 ( $=56*8$ ) such that

$$\left. \begin{aligned} F_{001}(A_1, \dots, A_{56}) &= e_{001} \bmod q, \\ F_{002}(A_1, \dots, A_{56}) &= e_{002} \bmod q, \\ &\dots \dots \\ F_{177}(A_1, \dots, A_{56}) &= e_{177} \bmod q, \\ &\dots \dots \\ F_{777}(A_1, \dots, A_{64}) &= e_{777} \bmod q, \end{aligned} \right\} \quad (49)$$

where  $F_{001}, \dots, F_{007}, F_{011}, \dots, F_{017}, \dots, F_{701}, \dots, F_{776}, F_{777}$  are the 112 ( $=56*2$ )<sup>th</sup> algebraic multivariate equations.

Then the complexity  $G$  required for solving above simultaneous equations by

using Gröbner basis is given [8] such as

$$G > G^? = (448 + d_{reg} C_{d_{reg}})^w = (25367 C_{448})^w \gg O(2^{80}), \quad (50)$$

where  $G^?$  is the complexity required for solving 449 simultaneous algebraic equations with 448 variables by using Gröbner basis, where  $w=2.39$ , and

$$d_{reg} = 24919 (= 449 * (112 - 1) / 2 - 0 \sqrt{(449 * (112^2 - 1) / 6)}). \quad (51)$$

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

#### §4.2 Computing plaintext $p$ and $A_i, B_j$ from coefficients of ciphertext $E_{BA}(X, M)$

Ciphertext  $E_{BA}(X, M)$  is generated by user B as follows.

$$E_{BA}(X, M) \in O[X]$$

$$= A_1(\dots(A_{r_A}(B_1(\dots(B_{r_B}(M(B_{r_B}^{-1}(B_{r_B-1}^{-1}(\dots(B_1^{-1}(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))))))))))))\dots)$$

$$= A_1(\dots(A_{r_A}(B_1(\dots(B_{r_B}([p\mathbf{1} + uG + vH + wGH](B_{r_B}^{-1}(B_{r_B-1}^{-1}(\dots(B_1^{-1}(A_{r_A}^{-1}(\dots(A_1^{-1}X)\dots))))))))))\dots))\dots) \bmod q$$

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

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

.....

$$e_{70}x_0 + e_{71}x_1 + \dots + e_{77}x_7)^t \bmod q,$$

$$= \{e_{jk}\} (j, k=0, \dots, 7)$$

$$\text{with } e_{jk} \in \mathbf{Fq} (j, k=0, \dots, 7),$$

where  $p$  is the plaintext.

$A_j, B_k \in O$  to be selected randomly such that  $A_j^{-1}$  and  $B_k^{-1}$  exist ( $j=1, \dots, r_A; k=1, \dots, r_B$ ) are parts of the secret keys of user A and user B respectively.

We try to find plaintext  $p$  and  $A_i, B_j$  ( $i=1, \dots, r_A; j=1, \dots, r_B$ ) from coefficients of  $E_{BA}(X, M)$ ,  $e_{jk} \in \mathbf{Fq}$  ( $j, k=0, \dots, 7$ ).

In case that  $r_A = 56$  and  $r_B = 56$  the number of unknown variables ( $p, u, v, w, A_j, B_k$ , ( $j, k=1, \dots, 56$ )) is  $900 (= 4 + 2 * 56 * 8)$ , the number of equations is 64 such that

$$\begin{aligned}
F_{00}(p,u,v,w,A_1,\dots,A_{56}, B_1,\dots,B_{56}) &= e_{00} \bmod q, \\
F_{01}(p,u,v,w,A_1,\dots,A_{56}, B_1,\dots,B_{56}) &= e_{01} \bmod q, \\
&\dots \quad \dots \\
F_{77}(p,u,v,w,A_1,\dots,A_{56}, B_1,\dots,B_{56}) &= e_{77} \bmod q,
\end{aligned} \tag{52}$$

where  $F_{00}, \dots, F_{77}$  are the  $225(=56*2*2+1)^{\text{th}}$  algebraic multivariate equations.

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

$$G > G' = (63 + d_{reg} C_{d_{reg}})^w = (7231 C_{63})^w = 2^{518} \gg O(2^{80}), \tag{53}$$

where  $G'$  is the complexity required for solving 64 simultaneous algebraic equations with 63 variables by using Gröbner basis,

where  $w=2.39$ , and

$$d_{reg} = 7168(=64*(225-1)/2 - 0\sqrt{(64*(225^2-1)/6)}). \tag{54}$$

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

### §4.3 Attack by using the ciphertexts of $p$ and $-p$

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

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

$$M := p\mathbf{1} + uG + vH + wGH \in O, \tag{55}$$

where  $p$  is a plaintext  $p \in \mathbf{F}q$  and  $u, v, w \in \mathbf{F}q$  is selected randomly.

We define the medium text  $M-$  by

$$M- := -p\mathbf{1} + u'G + v'H + w'GH \in O, \tag{56}$$

where  $u', v', w' \in \mathbf{F}q$  are selected randomly.

The ciphertext of  $p$ ,  $E_{BA}(X, M)$  is given as follows.

$$E_{BA}(X, M)$$

$$= A_1(\dots(A_{rA}(B_1(\dots(B_{rB}(M(B_{rB}^{-1}(B_{rB-1}^{-1}(\dots(B_1^{-1}(A_{rA}^{-1}(\dots(A_1^{-1}X)\dots))))))\dots)))\dots))\dots) \bmod q$$

$$= A_1(\dots(A_{rA}(B_1(\dots(B_{rB}([p\mathbf{1} + uG + vH + wGH])(B_{rB}^{-1}(B_{rB-1}^{-1}(\dots(B_1^{-1}(A_{rA}^{-1}(\dots(A_1^{-1}X)\dots))))\dots)))\dots))\dots) \bmod q,$$

the ciphertext of  $-p$ ,  $E_{BA}(X, M-)$ ,



$$E_{BA}(X, M^-)$$

$$= A_1(\dots(A_{rA}(B_1(\dots(B_{rB}(M - (B_{rB}^{-1}(B_{rB-1}^{-1}(\dots(B_1^{-1}(A_{rA}^{-1}(\dots(A_1^{-1}X)\dots))))))\dots)))\dots))\dots) \bmod q$$

$$= A_1(\dots(A_{rA}(B_1(\dots(B_{rB}([-p\mathbf{1} + u'G + v'H + w'GH])(B_{rB}^{-1}(B_{rB-1}^{-1}(\dots(B_1^{-1}(A_{rA}^{-1}(\dots(A_1^{-1}X)\dots))))\dots)))\dots))\dots) \bmod q.$$

As  $p-p=0 \bmod q$ ,

we have

$$E_{BA}(X, M) + E_{BA}(X, M^-)$$

$$= E_{BA}(X, p\mathbf{1} + uG + vH + wGH - p\mathbf{1} + u'G + v'H + w'GH) \bmod q$$

$$= E_{BA}(X, (p-p)\mathbf{1} + (u+u')G + (v+v')H + (w+w')GH) \bmod q$$

$$= E_{BA}(X, (u+u')G + (v+v')H + (w+w')GH) \bmod q.$$

As  $(u+u')G + (v+v')H + (w+w')GH \neq \mathbf{0} \bmod q \in O$ ,

we have

$$E_{BA}(X, M) + E_{BA}(X, M^-) \neq \mathbf{0} \bmod q. \tag{57}$$

We can calculate  $|E_{BA}(\mathbf{1}, M) + E_{BA}(\mathbf{1}, M^-)|^2$  as follows.

$$|E_{BA}(\mathbf{1}, M) + E_{BA}(\mathbf{1}, M^-)|^2 = |(u+u')G + (v+v')H + (w+w')GH|^2 \bmod q.$$

From Theorem 9 we have

$$|(u+u')G + (v+v')H + (w+w')GH|^2 = 0 \bmod q,$$

and

$$|E_{BA}(\mathbf{1}, M)|^2 = |M|^2 = 0 \bmod q.$$

It is said that the attack by using “ $p$  and  $-p$  attack” is not efficient. Then we can not easily distinguish the ciphertexts of  $p$  and  $-p$ .

## §5. The size of the modulus $q$ and the complexity for enciphering /deciphering

We consider the size of one of the system parameter,  $q$ . We select  $q=O(2^{2000})$ .

1) In case of  $r=56$ ,  $q=O(2^{2000})$ , the size of  $e_{ijk} \in Fq$  ( $i,j,k=0,\dots,7$ ) which are the coefficients of elements in  $E(X,Y)= A_1(\dots(A_r(Y(A_r^{-1}(\dots(A_1^{-1}X)\dots))))\dots) \bmod q \in O[X,Y]$  is  $(448)(\log_2 q)\text{bits} = 896\text{kbits}$ .

2) In case of  $r_A=56$ ,  $q=O(2^{2000})$ , the complexity to obtain  $E_A(X,Y)$  from  $A_1,\dots,A_{r_A}$ ( and  $q$  is

$$(55*512+55*8*512)(\log_2 q)^2+56*(16*(\log_2 q)^2+2*(\log_2 q)^3) = O(2^{41}) \text{ bit-operations,}$$

where  $56*(16*(\log_2 q)^2+2*(\log_2 q)^3)$  is the complexiy for inverse of  $A_i^{-1}(i=1,\dots,56)$ .

3) In case of  $r_B=56$ ,  $q=O(2^{2000})$ , the complexity to obtain  $E_{BA}(X,Y)$  from  $E_A(X,Y)$ ,  $B_1,\dots,B_{r_B}$ ,  $B_{r_B}^{-1},\dots,B_1^{-1}$  and  $q$  is

$$((512+64*8*8)*56+(512+64*8*8)*56) (\log_2 q)^2 = O(2^{43}) \text{ bit-operations.}$$

4) In case of  $r_A=56$ ,  $q=O(2^{2000})$ , the complexity to obtain  $E_{AB}(X,Y)$  from  $E_B(X,Y)$ ,  $A_1,\dots,A_{r_A}$ ,  $A_{r_A}^{-1},\dots,A_1^{-1}$  and  $q$  is

$$(64*8*55+8*64*8+56*8*8*64) (\log_2 q)^2 = O(2^{41}) \text{ bit-operations.}$$

5) In case of  $q=O(2^{2000})$ , the complexity to obtain  $C(X,p)= E_{BA}(X,M)$  from  $E_{BA}(X, Y)$ ,  $p,u,v,w,G,H,GH$  and  $q$  is

$$(1+8+8+8+64*8) (\log_2 q)^2 = O(2^{32}) \text{ bit-operations.}$$

6) In case of  $r_A=56$ ,  $q=O(2^{2000})$ , the complexity for deciphering  $C(X,p)=E_{BA}(X,M)$  to obtain  $p$  from  $C(X,p)= E_{BA}(X,M)$ ,  $A_1,\dots,A_{r_A}$ ,  $A_{r_A}^{-1},\dots,A_1^{-1}$  and  $q$  is

$$[64*55+1*(64+64*56+8*8+7*7+\dots+2*2+1+1+2+\dots+7)+1](\log_2 q)^2+8*2*(\log_2 q)^3$$

$$= O((3520+1*3880+1)2^{22}+2^{37}) = O(7401*2^{22}+2^{37}) = O(2^{38}) \text{ bit-operations.}$$

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

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

where the size of modulus  $n$  is 2048bits.

Then our scheme does not require large complexity to encipher and decipher so that we are able to implement our scheme to the mobile device.

## **§6. Conclusion**

We proposed the fully homomorphic public-key encryption scheme based on the octonion ring over finite field. It was shown that our scheme is immune from the Gröbner basis attacks by calculating the complexity to obtain the Gröbner basis for the multivariate algebraic equations. The proposed scheme does not require a “bootstrapping” process so that the complexity to encipher and decipher is not large.

It was shown that in this scheme the size of ciphertext is one-third of the size in the scheme proposed before.

## §7. BIBLIOGRAPHY

- [1] Masahiro Yagisawa, "Fully Homomorphic Encryption Without bootstrapping", Cryptology ePrint Archive, Report 2015/474, 2015. <http://eprint.iacr.org/>.
- [2] Masahiro, Y. (2015). Fully Homomorphic Encryption without bootstrapping. Saarbrücken/Germany: LAP LAMBERT Academic Publishing.
- [3] Shigeo Tsujii, Kohtaro Tadaki, Masahito Gotaishi, Ryo Fujita, and Masao Kasahara, "Proposal Integrated MPKC:PPS—STS Enhanced Perturbed Piece in Hand Method---," IEICE Tech. Rep. ISEC2009-27, SITE2009-19, ICSS2009-41(2009-07), July 2009.
- [4] T. Matsumoto, and H. Imai, "Public quadratic polynomial-tuples for efficient signature verification and message-encryption," Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88, pp.419–453, New York, NY, USA, 1988, Springer-Verlag New York, Inc.
- [5] S. Tsujii, K. Tadaki, and R. Fujita, "Piece in hand concept for enhancing the security of multivariate type public key cryptosystems: Public key without containing all the information of secret key," Cryptology ePrint Archive, Report 2004/366, 2004.
- [6] C. Wolf, and B. Preneel, "Taxonomy of public key schemes based on the problem of multivariate quadratic equations," Cryptology ePrint Archive, Report 2005/077, 2005, <http://eprint.iacr.org/>.
- [7] Shigeo Tsujii, Kohtaro Tadaki, Masahito Gotaishi, Ryo Fujita, and Masao Kasahara, "Proposal Integrated MPKC:PPS—STS Enhanced Perturbed Piece in Hand Method---," IEICE Tech. Rep. ISEC2009-27, SITE2009-19, ICSS2009-41(2009-07), July 2009.
- [8] M. Bardet, J. C. Faugere, and B. Salvy, "On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations," Proceeding of the International Conference on Polynomial System Solving(ICPSS2004), pp.71-75, November 2004.
- [9] Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In the 41st ACM Symposium on Theory of Computing (STOC), 2009.
- [10] Craig Gentry, A Fully Homomorphic Encryption Scheme, 2009. Available at <http://crypto.stanford.edu/craig/craig-thesis.pdf>.
- [11] Marten van Dijk; Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan (2009-12-11). "[Fully Homomorphic Encryption over the Integers](#)" (PDF). International Association for Cryptologic Research. Retrieved 2010-03-18.
- [12] Damien Stehle; Ron Steinfeld (2010-05-19). "Faster Fully Homomorphic Encryption" (PDF). International Association for Cryptologic Research. Retrieved 2010-09-15.
- [13] JS Coron, A Mandal, D Naccache, M Tibouchi, "Fully homomorphic

encryption over the integers with shorter public keys”, Advances in Cryptology–CRYPTO 2011, 487-504.

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

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

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

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

[18] Mashiro Yagisawa, "Improved Fully Homomorphic Encryption without bootstrapping", Cryptology ePrint Archive, Report 2017/763, 2017. <http://eprint.iacr.org/>.

**Appendix A:**

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

```

S ← a02+a12+...+a72 mod q.
% S-1 mod q
q[1] ← q div S ;% integer part of q/S
r[1] ← q mod S ;% residue
k ← 1
q[0] ← q
r[0] ← S
while r[k] ≠ 0
  begin
    k ← k + 1
    q[k] ← r[k-2] div r[k-1]
    r[k] ← r[k-2] mod [rk-1]
  end
Q[k-1] ← (-1)*q[k-1]
L[k-1] ← 1
i ← k-1
while i > 1
  begin
    Q[i-1] ← (-1)*Q[i]*q[i-1] + L[i]
    L[i-1] ← Q[i]
    i ← i-1
  end

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

```

---

**Appendix B:****Lemma 2**

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

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

(Proof:)

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

$$AB \pmod{q}$$

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

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

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

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

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

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

$$\begin{aligned} &= \{ a_0(a_0b_1 + a_1b_0 + a_2b_4 + a_3b_7 - a_4b_2 + a_5b_6 - a_6b_5 - a_7b_3) \\ &\quad - a_1(a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7) \\ &\quad - a_2(a_0b_4 + a_1b_2 - a_2b_1 - a_3b_6 + a_4b_0 + a_5b_7 + a_6b_3 - a_7b_5) \\ &\quad - a_3(a_0b_7 + a_1b_3 + a_2b_6 - a_3b_1 + a_4b_5 - a_5b_4 - a_6b_2 + a_7b_0) \end{aligned}$$

$$\begin{aligned}
& +a_4(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6) \\
& - a_5(a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2) \\
& +a_6(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4) \\
& +a_7(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1) \} /|A|^2 \bmod q \\
& =\{(a_0^2+a_1^2+\dots+a_7^2) b_1\} /|A|^2=b_1 \bmod q.
\end{aligned}$$

Similarly we have

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

Then we have

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

## Appendix C:

### Theorem 7

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

$$O=\{(a_0,a_1,\dots,a_7) \mid a_j \in \mathbf{F}q \quad (j=0,1,\dots,7)\}.$$

Let  $G,H \in O$  be the octonions such that

$$G=(g_0,g_1,\dots,g_7), \quad g_j \in \mathbf{F}q \quad (j=0,1,\dots,7),$$

$$H=(h_0,h_1,\dots,h_7), \quad h_j \in \mathbf{F}q \quad (j=0,1,\dots,7),$$

where

$$g_0=1/2 \bmod q, \quad h_0=0 \bmod q,$$

$$L_G=g_0^2+g_1^2+\dots+g_7^2=0 \bmod q,$$

$$L_H=h_0^2+h_1^2+\dots+h_7^2=0 \bmod q$$

and

$$g_1h_1+g_2h_2+g_3h_3+g_4h_4+g_5h_5+g_6h_6+g_7h_7=0 \bmod q.$$

$G$  and  $H$  satisfy the following equations.

$$(GH)G= \mathbf{0} \bmod q,$$

$$(HG)H= \mathbf{0} \bmod q.$$

(Proof.)

$$GH \bmod q$$



$$\begin{aligned}
&= ( g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7 \bmod q, \\
&\quad g_0h_1 + g_1h_0 + g_2h_4 + g_3h_7 - g_4h_2 + g_5h_6 - g_6h_5 - g_7h_3 \bmod q, \\
&\quad g_0h_2 - g_1h_4 + g_2h_0 + g_3h_5 + g_4h_1 - g_5h_3 + g_6h_7 - g_7h_6 \bmod q, \\
&\quad g_0h_3 - g_1h_7 - g_2h_5 + g_3h_0 + g_4h_6 + g_5h_2 - g_6h_4 + g_7h_1 \bmod q, \\
&\quad g_0h_4 + g_1h_2 - g_2h_1 - g_3h_6 + g_4h_0 + g_5h_7 + g_6h_3 - g_7h_5 \bmod q, \\
&\quad g_0h_5 - g_1h_6 + g_2h_3 - g_3h_2 - g_4h_7 + g_5h_0 + g_6h_1 + g_7h_4 \bmod q, \\
&\quad g_0h_6 + g_1h_5 - g_2h_7 + g_3h_4 - g_4h_3 - g_5h_1 + g_6h_0 + g_7h_2 \bmod q, \\
&\quad g_0h_7 + g_1h_3 + g_2h_6 - g_3h_1 + g_4h_5 - g_5h_4 - g_6h_2 + g_7h_0 \bmod q)
\end{aligned}$$

$$[(GH)G]_0 \bmod q$$

$$\begin{aligned}
&= ( g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7 ) g_0 \\
&\quad - (g_0h_1 + g_1h_0 + g_2h_4 + g_3h_7 - g_4h_2 + g_5h_6 - g_6h_5 - g_7h_3) g_1 \\
&\quad - (g_0h_2 - g_1h_4 + g_2h_0 + g_3h_5 + g_4h_1 - g_5h_3 + g_6h_7 - g_7h_6) g_2 \\
&\quad - (g_0h_3 - g_1h_7 - g_2h_5 + g_3h_0 + g_4h_6 + g_5h_2 - g_6h_4 + g_7h_1) g_3 \\
&\quad - (g_0h_4 + g_1h_2 - g_2h_1 - g_3h_6 + g_4h_0 + g_5h_7 + g_6h_3 - g_7h_5) g_4 \\
&\quad - (g_0h_5 - g_1h_6 + g_2h_3 - g_3h_2 - g_4h_7 + g_5h_0 + g_6h_1 + g_7h_4) g_5 \\
&\quad - (g_0h_6 + g_1h_5 - g_2h_7 + g_3h_4 - g_4h_3 - g_5h_1 + g_6h_0 + g_7h_2) g_6 \\
&\quad - (g_0h_7 + g_1h_3 + g_2h_6 - g_3h_1 + g_4h_5 - g_5h_4 - g_6h_2 + g_7h_0) g_7) \bmod q
\end{aligned}$$

As

$$h_0 = 0 \bmod q,$$

$$L_G := g_0^2 + g_1^2 + \dots + g_7^2 = 0 \bmod q,$$

$$L_H := h_0^2 + h_1^2 + \dots + h_7^2 = 0 \bmod q$$

and

$$g_1h_1 + g_2h_2 + g_3h_3 + g_4h_4 + g_5h_5 + g_6h_6 + g_7h_7 = 0 \bmod q,$$

we have

$$[(GH)G]_0 \bmod q$$

$$\begin{aligned}
&= (g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7) g_0 \\
&\quad - (g_0h_1 + g_1h_0 + g_2h_4 + g_3h_7 - g_4h_2 + g_5h_6 - g_6h_5 - g_7h_3) g_1 \\
&\quad - (g_0h_2 - g_1h_4 + g_2h_0 + g_3h_5 + g_4h_1 - g_5h_3 + g_6h_7 - g_7h_6) g_2 \\
&\quad - (g_0h_3 - g_1h_7 - g_2h_5 + g_3h_0 + g_4h_6 + g_5h_2 - g_6h_4 + g_7h_1) g_3 \\
&\quad - (g_0h_4 + g_1h_2 - g_2h_1 - g_3h_6 + g_4h_0 + g_5h_7 + g_6h_3 - g_7h_5) g_4 \\
&\quad - (g_0h_5 - g_1h_6 + g_2h_3 - g_3h_2 - g_4h_7 + g_5h_0 + g_6h_1 + g_7h_4) g_5 \\
&\quad - (g_0h_6 + g_1h_5 - g_2h_7 + g_3h_4 - g_4h_3 - g_5h_1 + g_6h_0 + g_7h_2) g_6 \\
&\quad - (g_0h_7 + g_1h_3 + g_2h_6 - g_3h_1 + g_4h_5 - g_5h_4 - g_6h_2 + g_7h_0) g_7 \\
&= h_1(-g_4g_2 - g_7g_3 + g_2g_4 - g_6g_5 + g_5g_6 + g_3g_7) \\
&\quad + h_2(g_4g_1 - g_5g_3 - g_1g_4 + g_3g_5 - g_7g_6 + g_6g_7) \\
&\quad + h_3(g_7g_1 + g_5g_2 - g_6g_4 - g_2g_5 + g_4g_6 - g_1g_7) \\
&\quad + h_4(-g_2g_1 + g_1g_2 + g_6g_3 - g_7g_5 - g_3g_6 + g_5g_7) \\
&\quad + h_5(g_6g_1 - g_3g_2 + g_2g_3 + g_7g_4 - g_1g_6 - g_4g_7) \\
&\quad + h_6(-g_5g_1 + g_7g_2 - g_4g_3 + g_3g_4 + g_1g_5 - g_2g_7) \\
&\quad + h_7(-g_3g_1 - g_6g_2 + g_1g_3 - g_5g_4 + g_4g_5 + g_2g_6) \\
&= 0 \pmod{q},
\end{aligned}$$

$$[(GH)G]_1 \pmod{q}$$

$$\begin{aligned}
&= (g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7) g_1 \\
&\quad + (g_0h_1 + g_1h_0 + g_2h_4 + g_3h_7 - g_4h_2 + g_5h_6 - g_6h_5 - g_7h_3) g_0 \\
&\quad + (g_0h_2 - g_1h_4 + g_2h_0 + g_3h_5 + g_4h_1 - g_5h_3 + g_6h_7 - g_7h_6) g_4 \\
&\quad + (g_0h_3 - g_1h_7 - g_2h_5 + g_3h_0 + g_4h_6 + g_5h_2 - g_6h_4 + g_7h_1) g_7 \\
&\quad - (g_0h_4 + g_1h_2 - g_2h_1 - g_3h_6 + g_4h_0 + g_5h_7 + g_6h_3 - g_7h_5) g_2 \\
&\quad + (g_0h_5 - g_1h_6 + g_2h_3 - g_3h_2 - g_4h_7 + g_5h_0 + g_6h_1 + g_7h_4) g_6 \\
&\quad - (g_0h_6 + g_1h_5 - g_2h_7 + g_3h_4 - g_4h_3 - g_5h_1 + g_6h_0 + g_7h_2) g_5 \\
&\quad - (g_0h_7 + g_1h_3 + g_2h_6 - g_3h_1 + g_4h_5 - g_5h_4 - g_6h_2 + g_7h_0) g_3
\end{aligned}$$

$$\begin{aligned}
&= h_1 (-g_1^2 + g_0^2 + g_4^2 + g_7^2 + g_2^2 + g_6^2 + g_5^2 + g_3^2) \\
&+ h_2 (-g_2g_1 - g_4g_0 + g_0g_4 + g_5g_7 - g_1g_2 - g_3g_6 - g_7g_5 + g_6g_3) \\
&+ h_3 (-g_3g_1 - g_7g_0 - g_5g_4 + g_0g_7 - g_6g_2 + g_2g_6 + g_4g_5 - g_1g_3) \\
&+ h_4 (-g_4g_1 + g_2g_0 - g_1g_4 - g_6g_7 - g_0g_2 + g_7g_6 - g_3g_5 + g_5g_3) \\
&+ h_5 (-g_5g_1 - g_6g_0 + g_3g_4 - g_2g_7 + g_7g_2 + g_0g_6 - g_1g_5 - g_4g_3) \\
&+ h_6 (-g_6g_1 + g_5g_0 - g_7g_4 + g_4g_7 + g_3g_2 - g_1g_6 - g_0g_5 - g_2g_3) \\
&+ h_7 (-g_7g_1 + g_3g_0 + g_6g_4 - g_1g_7 - g_5g_2 - g_4g_6 + g_2g_5 - g_0g_3) \\
&= h_1 (-2g_1^2 + L_G) - 2g_1(h_2g_2 + h_3g_3 + h_4g_4 + h_5g_5 + h_6g_6 + h_7g_7) \\
&= h_1 (L_G) - 2g_1(h_1g_1 + h_2g_2 + h_3g_3 + h_4g_4 + h_5g_5 + h_6g_6 + h_7g_7) \\
&= 0 \pmod{q}.
\end{aligned}$$

In the same manner we have

$$[(GH)G]_i = 0 \pmod{q} \quad (i=2, \dots, 7).$$

Then we have

$$(GH)G = \mathbf{0} \pmod{q}.$$

In the same manner we have

$$HG \pmod{q}$$

$$\begin{aligned}
&= (h_0g_0 - h_1g_1 - h_2g_2 - h_3g_3 - h_4g_4 - h_5g_5 - h_6g_6 - h_7g_7 \pmod{q}, \\
&\quad h_0g_1 + h_1g_0 + h_2g_4 + h_3g_7 - h_4g_2 + h_5g_6 - h_6g_5 - h_7g_3 \pmod{q}, \\
&\quad h_0g_2 - h_1g_4 + h_2g_0 + h_3g_5 + h_4g_1 - h_5g_3 + h_6g_7 - h_7g_6 \pmod{q}, \\
&\quad h_0g_3 - h_1g_7 - h_2g_5 + h_3g_0 + h_4g_6 + h_5g_2 - h_6g_4 + h_7g_1 \pmod{q}, \\
&\quad h_0g_4 + h_1g_2 - h_2g_1 - h_3g_6 + h_4g_0 + h_5g_7 + h_6g_3 - h_7g_5 \pmod{q}, \\
&\quad h_0g_5 - h_1g_6 + h_2g_3 - h_3g_2 - h_4g_7 + h_5g_0 + h_6g_1 + h_7g_4 \pmod{q}, \\
&\quad h_0g_6 + h_1g_5 - h_2g_7 + h_3g_4 - h_4g_3 - h_5g_1 + h_6g_0 + h_7g_2 \pmod{q}, \\
&\quad h_0g_7 + h_1g_3 + h_2g_6 - h_3g_1 + h_4g_5 - h_5g_4 - h_6g_2 + h_7g_0 \pmod{q}).
\end{aligned}$$

$$\begin{aligned}
& [(HG)H]_0 \\
&= (h_0g_0 - h_1g_1 - h_2g_2 - h_3g_3 - h_4g_4 - h_5g_5 - h_6g_6 - h_7g_7)h_0 \\
&\quad - (h_0g_1 + h_1g_0 + h_2g_4 + h_3g_7 - h_4g_2 + h_5g_6 - h_6g_5 - h_7g_3)h_1 \\
&\quad - (h_0g_2 - h_1g_4 + h_2g_0 + h_3g_5 + h_4g_1 - h_5g_3 + h_6g_7 - h_7g_6)h_2 \\
&\quad - (h_0g_3 - h_1g_7 - h_2g_5 + h_3g_0 + h_4g_6 + h_5g_2 - h_6g_4 + h_7g_1)h_3 \\
&\quad - (h_0g_4 + h_1g_2 - h_2g_1 - h_3g_6 + h_4g_0 + h_5g_7 + h_6g_3 - h_7g_5)h_4 \\
&\quad - (h_0g_5 - h_1g_6 + h_2g_3 - h_3g_2 - h_4g_7 + h_5g_0 + h_6g_1 + h_7g_4)h_5 \\
&\quad - (h_0g_6 + h_1g_5 - h_2g_7 + h_3g_4 - h_4g_3 - h_5g_1 + h_6g_0 + h_7g_2)h_6 \\
&\quad - (h_0g_7 + h_1g_3 + h_2g_6 - h_3g_1 + h_4g_5 - h_5g_4 - h_6g_2 + h_7g_0)h_7 \pmod{q} \\
&= 0 \cdot h_0 - g_0(h_1^2 + h_2^2 + \dots + h_7^2) \\
&\quad + g_1(-h_4h_2 - h_7h_3 + h_2h_4 - h_6h_5 + h_5h_6 + h_3h_7) \\
&\quad + g_2(h_4h_1 - h_5h_3 - h_1h_4 + h_3h_5 - h_7h_6 + h_6h_7) \\
&\quad + g_3(h_7h_1 + h_5h_2 - h_6h_4 - h_2h_5 + h_4h_6 - h_1h_7) \\
&\quad + g_4(-h_2h_1 + h_1h_2 + h_6h_3 - h_7h_5 - h_3h_6 + h_5h_7) \\
&\quad + g_5(h_6h_1 - h_3h_2 + h_2h_3 + h_7h_4 - h_1h_6 - h_4h_7) \\
&\quad + g_6(h_6h_1 - h_3h_2 + h_2h_3 + h_7h_4 - h_1h_6 - h_4h_7) \\
&\quad + g_7(-h_5h_1 + h_7h_2 - h_4h_3 + h_3h_4 + h_1h_5 - h_2h_7) \pmod{q} \\
&= 0 \pmod{q}.
\end{aligned}$$

$$\begin{aligned}
& [(HG)H]_1 \\
&= (h_0g_0 - h_1g_1 - h_2g_2 - h_3g_3 - h_4g_4 - h_5g_5 - h_6g_6 - h_7g_7)h_1 \\
&\quad + (h_0g_1 + h_1g_0 + h_2g_4 + h_3g_7 - h_4g_2 + h_5g_6 - h_6g_5 - h_7g_3)h_0 \\
&\quad + (h_0g_2 - h_1g_4 + h_2g_0 + h_3g_5 + h_4g_1 - h_5g_3 + h_6g_7 - h_7g_6)h_4 \\
&\quad + (h_0g_3 - h_1g_7 - h_2g_5 + h_3g_0 + h_4g_6 + h_5g_2 - h_6g_4 + h_7g_1)h_7 \\
&\quad - (h_0g_4 + h_1g_2 - h_2g_1 - h_3g_6 + h_4g_0 + h_5g_7 + h_6g_3 - h_7g_5)h_2 \\
&\quad + (h_0g_5 - h_1g_6 + h_2g_3 - h_3g_2 - h_4g_7 + h_5g_0 + h_6g_1 + h_7g_4)h_6 \\
&\quad - (h_0g_6 + h_1g_5 - h_2g_7 + h_3g_4 - h_4g_3 - h_5g_1 + h_6g_0 + h_7g_2)h_5
\end{aligned}$$

$$\begin{aligned}
& -(h_0g_7+h_1g_3+h_2g_6-h_3g_1+h_4g_5-h_5g_4-h_6g_2+h_7g_0)h_3 \pmod q \\
&= g_1(-h_1^2+h_4^2+h_7^2+h_2^2+h_6^2+h_5^2+h_3^2) \\
&+ g_2(-h_2h_1+h_5h_7-h_1h_2-h_3h_6-h_7h_5+h_6h_3) \\
&+ g_3(-h_3h_1-h_5h_4-h_6h_2+h_2h_6+h_4h_5-h_1h_3) \\
&+ g_4(-h_4h_1-h_1h_4-h_6h_7+h_7h_6-h_3h_5+h_5h_3) \\
&+ g_5(-h_5h_1+h_3h_4-h_2h_7+h_7h_2-h_1h_5-h_4h_3) \\
&+ g_6(-h_6h_1-h_7h_4+h_4h_7+h_3h_2-h_1h_6-h_2h_3) \\
&+ g_7(-h_7h_1+h_6h_4-h_1h_7-h_5h_2-h_4h_6+h_2h_5) \pmod q \\
&= -2(g_1h_1^2+g_2h_2h_1+g_3h_3h_1+g_4h_4h_1+g_5h_5h_1+g_6h_6h_1+g_7h_7h_1) \pmod q \\
&= -2h_1(g_1h_1+g_2h_2+g_3h_3+g_4h_4+g_5h_5+g_6h_6+g_7h_7) \pmod q \\
&= -2h_1 \cdot 0 = 0 \pmod q,
\end{aligned}$$

In the same manner we have

$$[(HG)H]_i = -2h_i \cdot 0 = 0 \pmod q \quad (i=2, \dots, 7).$$

Then we have

$$(HG)H = \mathbf{0} \pmod q. \quad \text{q.e.d.}$$

## Appendix D:

### Lemma 3

For any  $A=(a_0, a_1, \dots, a_7), B=(b_0, b_1, \dots, b_7) \in O$

$$(A+B)^* = A^* + B^* \pmod q,$$

$$(AB)^* = B^*A^* \pmod q$$

where

$$A^* = (a_0, -a_1, \dots, -a_7) \in O, B^* = (b_0, -b_1, \dots, -b_7) \in O.$$

(Proof)

$$(A+B)^* = (a_0 + b_0, a_1 + b_1, \dots, a_7 + b_7)^* \pmod q,$$

$$= (a_0 + b_0, -a_1 - b_1, \dots, -a_7 - b_7) \pmod q,$$

$$\begin{aligned}
A^*+B^* &= (a_0, -a_1, \dots, -a_7) + (b_0, -b_1, \dots, -b_7) \pmod q, \\
&= (a_0 + b_0, -a_1 - b_1, \dots, -a_7 - b_7) \pmod q = (A+B)^*.
\end{aligned}$$

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

$$\begin{aligned}
B^*A^* &= (b_0, -b_1, \dots, -b_7) (a_0, -a_1, \dots, -a_7) \\
&= (b_0a_0 - b_1a_1 - b_2a_2 - b_3a_3 - b_4a_4 - b_5a_5 - b_6a_6 - b_7a_7 \pmod q, \\
&\quad -b_0a_1 - b_1a_0 + b_2a_4 + b_3a_7 - b_4a_2 + b_5a_6 - b_6a_5 - b_7a_3 \pmod q, \\
&\quad -b_0a_2 - b_1a_4 - b_2a_0 + b_3a_5 + b_4a_1 - b_5a_3 + b_6a_7 - b_7a_6 \pmod q, \\
&\quad -b_0a_3 - b_1a_7 - b_2a_5 - b_3a_0 + b_4a_6 + b_5a_2 - b_6a_4 + b_7a_1 \pmod q, \\
&\quad -b_0a_4 + b_1a_2 - b_2a_1 - b_3a_6 - b_4a_0 + b_5a_7 + b_6a_3 - b_7a_5 \pmod q,
\end{aligned}$$

$$\begin{aligned}
& -b_0a_5 - b_1a_6 + b_2a_3 - b_3a_2 - b_4a_7 - b_5a_0 + b_6a_1 + b_7a_4 \pmod q, \\
& -b_0a_6 + b_1a_5 - b_2a_7 + b_3a_4 - b_4a_3 - b_5a_1 - b_6a_0 + b_7a_2 \pmod q, \\
& -b_0a_7 + b_1a_3 + b_2a_6 - b_3a_1 + b_4a_5 - b_5a_4 - b_6a_2 - b_7a_0 \pmod q). \\
& =(AB)^* \pmod q. \qquad \text{q.e.d}
\end{aligned}$$

## Appendix E:

### Theorem 9

$$|M|^2 = |pG + uH + vGH + wHG|^2 = 0 \pmod q.$$

(Proof:)

In general for any  $N \in O$ ,

as

$$N + N^* = 2[N]_0 \mathbf{1} \in O, \quad N^2 = -L_N \mathbf{1} + 2[N]_0 N,$$

$$N^2 + NN^* = N^2 + N^*N = 2[N]_0 N = N^2 + L_N \mathbf{1},$$

we have

$$L_N \mathbf{1} = NN^* = N^*N.$$

$$\begin{aligned}
MM^* &= (pG + uH + vGH + wHG)(pG + uH + vGH + wHG)^* \pmod q \\
&= (pG + uH + vGH + wHG)(pG^* + uH^* + v(GH)^* + w(HG)^*) \pmod q \\
&= p^2 GG^* + pu(GH^* + HG^*) + pv(G(GH)^* + (GH)G^*) \\
&\quad + pw(G(GH)^* + (HG)G^*) + \\
&\quad + u^2 HH^* + uv(H(GH)^* + (GH)H^*) + uw(H(HG)^* + (HG)H^*) \\
&\quad + v^2(GH)(GH)^* + vw((GH)(HG)^* + (HG)(GH)^*) \\
&\quad + w^2(HG)(HG)^* \\
&= p^2 L_G \mathbf{1} + pu2[GH^*]_0 \mathbf{1} + pv2[(GH)G^*]_0 \mathbf{1} + pw2[(HG)G^*]_0 \mathbf{1} \\
&\quad + u^2 L_H \mathbf{1} + uv2[(GH)H^*]_0 \mathbf{1} + uw2[(HG)H^*]_0 \mathbf{1} \\
&\quad + v^2 L_{GH} \mathbf{1} + vw2[((GH)(HG))^*]_0 \mathbf{1} + w^2 L_{HG} \mathbf{1} \pmod q \\
&= p^2 \mathbf{0} + pu2[G(2h_0 \mathbf{1} - H)]_0 \mathbf{1} + pv2[(GH)(2g_0 \mathbf{1} - G)]_0 \mathbf{1}
\end{aligned}$$

$$\begin{aligned}
& +pw^2[(HG) (2g_0\mathbf{1}-G)]_0\mathbf{1} \\
& + u^2 \mathbf{0} + uv^2[(GH) (2h_0\mathbf{1}-H)]_0\mathbf{1} + uw^2[(HG) (2h_0\mathbf{1}-H)]_0\mathbf{1} \\
& + v^2 \mathbf{0} + vw^2[((GH) (2[HG]_0\mathbf{1}-HG))]_0\mathbf{1} + w^2 \mathbf{0} \pmod q \\
& = pu^2[-GH]_0\mathbf{1} + pv^2[GH-GHG]_0\mathbf{1} + pw^2[(HG-HG)]_0\mathbf{1} \\
& + uv^2[-GHH]_0\mathbf{1} + uw^2[-HGH]_0\mathbf{1} + vw^2[-(GH) (HG)]_0\mathbf{1} \pmod q \\
& = pu^2[-GH]_0\mathbf{1} + pv^2[GH-\mathbf{0}]_0\mathbf{1} + pw^2[\mathbf{0}]_0\mathbf{1} \\
& + uv^2[\mathbf{0}]_0\mathbf{1} + uw^2[\mathbf{0}]_0\mathbf{1} + vw^2[\mathbf{0}]_0\mathbf{1} \pmod q \\
& = \mathbf{0}\mathbf{1} + \mathbf{0}\mathbf{1} + \mathbf{0}\mathbf{1} + \mathbf{0}\mathbf{1} + \mathbf{0}\mathbf{1} + \mathbf{0}\mathbf{1} = \mathbf{0} \pmod q.
\end{aligned}$$

Then we have

$$MM^* = L_M\mathbf{1} = \mathbf{0} \pmod q.$$

$$L_M = |M|^2 = |pG + uH + vGH + wHG|^2 = 0 \pmod q.$$

q.e.d.