Improved Fully Homomorphic Encryption

without Bootstrapping

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

SUMMARY: Gentry’s bootstrapping technique is the most famous method of obtaining fully homomorphic encryption. In previous work I proposed a fully homomorphic encryption without bootstrapping which has the weak point in the enciphering function. In this paper I propose the improved fully homomorphic public-key encryption scheme on non-associative octonion ring over finite field without bootstrapping technique. The plaintext $p$ consists of two sub-plaintext $u$ and $v$. The proposed fully homomorphic public-key encryption scheme is immune from the “$p$ and -$p$ attack”. The cipher text consists of three sub-cipher texts. As the scheme is based on computational difficulty to solve the multivariate algebraic equations of high degree while the almost all multivariate cryptosystems proposed until now are based on the quadratic equations avoiding the explosion of the coefficients. Because proposed fully homomorphic encryption scheme is based on multivariate algebraic equations with high degree or too many variables, it is against the Gröbner basis attack, the differential attack, rank attack and so on.

keywords: fully homomorphih 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.

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

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

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

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

In previous work[1],[2] I proposed a fully homomorphic encryption without bootstrapping which has the weak point in the enciphering function[17]. This paper is the revised chapter 4 of my work “Fully Homomorphic Encryption without bootstrapping” published in March, 2015 which was published by LAP LAMBERT Academic Publishing, Saarbrücken/Germany [1].

In this paper I propose a fully homomorphic encryption scheme on non-associative octonion ring over finite field which is based on computational difficulty to solve the multivariate algebraic equations of high degree while the almost all multivariate cryptosystems[3], [4],[5],[6],[7] proposed until now are based on the quadratic equations avoiding the explosion of the coefficients. Our scheme is against the Gröbner basis[8] attack, the differential attack, rank attack and so on.

§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 $O \left(2^{2000}\right)$. Let $O$ be the octonion [16] ring over a finite field $F_q$.

\[
O=\{(a_0,a_1,...,a_7) \mid a_j \in F_q (j=0,1,...,7)\}
\]

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

\[
A=(a_0,a_1,...,a_7), a_j \in F_q (j=0,1,...,7),
\]

\[
B=(b_0,b_1,...,b_7), b_j \in F_q (j=0,1,...,7).
\]

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

\[
A+B \mod q = (a_0 + b_0 \mod q, a_1 + b_1 \mod q, a_2 + b_2 \mod q, a_3 + b_3 \mod q, \\
a_4 + b_4 \mod q, a_5 + b_5 \mod q, a_6 + b_6 \mod q, a_7 + b_7 \mod q).
\]

Let 

\[
|A|^2 = a_0^2 + a_1^2 + \ldots + a_7^2 \mod q.
\]

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

\[
A^{-1} = (a_0/|A|^2 \mod q, -a_1/|A|^2 \mod q, ..., -a_7/|A|^2 \mod q) \iff \text{Octinv} \left( A \right).
\]

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

\section*{§2.2. Property of multiplication over octonion ring $O$}

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

\[
A,B,C \text{ etc. } \in O \text{ satisfy the following formulae in general where } A,B \text{ and } C \text{ have the inverse } A^{-1},B^{-1} \text{ and } C^{-1} \mod q.
\]
1) Non-commutative

\[ AB \neq BA \mod q. \quad (8) \]

2) Non-associative

\[ A(BC) \neq (AB)C \mod q. \quad (9) \]

3) Alternative

\[ (AA)B = A(AB) \mod q, \quad (10) \]
\[ A(BB) = (AB)B \mod q, \quad (11) \]
\[ (AB)A = A(BA) \mod q. \quad (12) \]

4) Moufang’s formulae [16],

\[ C(A(CB)) = ((CA)C)B \mod q, \quad (13) \]
\[ A(C(BC)) = ((AC)B)C \mod q, \quad (14) \]
\[ (CA)(BC) = (C(AB))C \mod q, \quad (15) \]
\[ (CA)(BC) = C((AB)C) \mod q. \quad (16) \]

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

**Lemma 1**

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

*(Proof)*

From (12)

\[ A^{-1}B = A^{-1}((BA)A^{-1}) = (A^{-1}(BA))A^{-1} \mod q, \]

By multiplying \( A \) from right side we have

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

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

**Lemma 2**

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

*(Proof:)*

Here proof is omitted and can be looked up in the **Appendix B.**
7) \( A \in O \) satisfies the following theorem.

**Theorem 1**

\[ A^2 = w \mathbf{1} + v A \mod q, \]  
(18)

where

\[ \exists w, v \in F_q, \]

\[ 1 = (1,0,0,0,0,0,0) \in O, \]

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

*Proof:*

\[ A^2 \mod q \]

\[ = (a_0 a_0 - a_1 a_1 + a_2 a_2 - a_3 a_3 - a_4 a_4 - a_5 a_5 - a_6 a_6 - a_7 a_7 \mod q, \]

\[ a_0 a_1 + a_1 a_0 + a_2 a_4 + a_3 a_7 - a_4 a_2 + a_5 a_6 - a_6 a_5 - a_7 a_3 \mod q, \]

\[ a_0 a_2 - a_1 a_4 + a_2 a_0 + a_3 a_5 + a_3 a_1 - a_4 a_3 + a_5 a_7 - a_7 a_6 \mod q, \]

\[ a_0 a_3 - a_1 a_7 - a_2 a_5 + a_3 a_0 + a_4 a_6 + a_5 a_2 - a_6 a_4 + a_7 a_1 \mod q, \]

\[ a_0 a_4 + a_1 a_2 - a_2 a_1 - a_3 a_6 + a_4 a_0 + a_5 a_7 + a_6 a_3 - a_7 a_5 \mod q, \]

\[ a_0 a_5 - a_1 a_6 + a_2 a_3 - a_3 a_2 - a_4 a_7 + a_5 a_0 + a_6 a_1 + a_7 a_4 \mod q, \]

\[ a_0 a_6 + a_1 a_5 - a_2 a_7 + a_3 a_4 - a_4 a_3 - a_5 a_1 + a_6 a_0 + a_7 a_2 \mod q, \]

\[ a_0 a_7 + a_1 a_3 + a_2 a_6 - a_3 a_1 + a_4 a_5 - a_5 a_4 - a_6 a_2 + a_7 a_0 \mod q) \]

\[ = (2a_0^2 - L \mod q, 2a_0 a_1 \mod q, 2a_0 a_2 \mod q, 2a_0 a_3 \mod q, 2a_0 a_4 \mod q, \]

\[ 2a_0 a_5 \mod q, 2a_0 a_6 \mod q, 2a_0 a_7 \mod q) \]

where

\[ L = a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2 \mod q. \]

Now we try to obtain \( u, v \in F_q \) that satisfy \( A^2 = w \mathbf{1} + v A \mod q \).

\[ w \mathbf{1} + v A = w(1,0,0,0,0,0,0) + v(a_0, a_1, \ldots, a_7) \mod q, \]

\[ A^2 = (2a_0^2 - L \mod q, 2a_0 a_1 \mod q, 2a_0 a_2 \mod q, 2a_0 a_3 \mod q, \]

\[ 2a_0 a_4 \mod q, 2a_0 a_5 \mod q, 2a_0 a_6 \mod q, 2a_0 a_7 \mod q). \]

As \( A^2 = w \mathbf{1} + v A = -L \mathbf{1} + 2a_0 A \mod q \), we have

\[ w = -L \mod q, \]
v=2a_0 \mod q. \quad \text{q.e.d.}

8) **Theorem 2**

$D \in O$ 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

$$BA = D \mod q.$$  \hspace{1cm} (19)

Then

$$B(AX) = (BA)X \mod q.$$ \hspace{1cm} (20)

We can select $C \in O$ that satisfies

$$B(AC) \neq (BA)C \mod q.$$ \hspace{1cm} (21)

(21) is contradictory to (20). \quad \text{q.e.d.}

9) **Theorem 3**

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

$$C(B(AX)) = DX \mod q$$ \hspace{1cm} (22)

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

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

$$B(AC) \neq (BA)C \mod q.$$ \hspace{1cm} (23)

*(Proof:)*

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

$$C(BA) = D \mod q.$$ \hspace{1cm} (24)

Then

$$C(B(AX)) = (C(BA))X \mod q.$$
We substitute $C$ to $X$ to obtain

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

From (12)

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

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

$$B(AC) = (BA)C \mod q \quad (24)$$

(24) is contradictory to (23). \hspace{1cm} \text{q.e.d.}

10) **Theorem 4**

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

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

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

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

$$C(BA) \neq (CB)A \mod q. \quad (25)$$

(Proof:)

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

$$C(BA) = ED \mod q \quad (26)$$

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

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

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

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

$$ED = (CB)A \mod q. \quad (27)$$

From (26) and (27) we have

$$C(BA) = (CB)A \mod q. \quad (28)$$

(28) is contradictory to (25). \hspace{1cm} \text{q.e.d.}

11) **Theorem 5**

$D \in O$ does not exist that satisfies the following equation.
\[ A(BA^{-1}X) = DX \mod q \]

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 \( X = 1 \)

\[ A(BA^{-1}) = D \mod q. \]

Then

\[ A(BA^{-1}X) = (A(BA^{-1}))X \mod q. \tag{29} \]

We can select \( C \in O \) such that

\[ (BA^{-1})(CA^2) \neq ((BA^{-1})C)A^2 \mod q. \tag{30} \]

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

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

\[ A(BA^{-1}(CA)) = (A(BA^{-1}))(CA) \mod q. \]

From Lemma 1

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

From (16)

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

By multiplying \( A^{-1} \) from left side we have

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

From Lemma 1

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

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

\[ B(A^{-1}((CA^2)A^{-1})) = ((BA^{-1})C)A \mod q. \]

From (14) we have

\[ ((BA^{-1})(CA^2))A^{-1} = ((BA^{-1})C)A \mod q. \]

Multiply \( A \) from right side we have

\[ ((BA^{-1})(CA^2)) = ((BA^{-1})C)A^2 \mod q. \tag{31} \]
§3. Proposed fully homomorphich 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 either of them being able to find the value of the individual numbers.

§3.1 Definition of homomorphic public-key encryption

A homomorphic public-key encryption scheme $\text{HPKE} := (\text{KeyGen}; \text{Enc}; \text{Dec}; \text{Eval})$ 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 $\text{KeyGen}$, on input the security parameter $1^\lambda$, outputs $(sk) \leftarrow \text{KeyGen}(1^\lambda)$, where $sk$ is a secret encryption/decryption key.

- Encryption. The algorithm $\text{Enc}$, on input system parameter $q$, secret keys $(sk)$ and a plaintext $p \in F_q$, outputs a ciphertext $C = (1C, 2C, 3C) \leftarrow \text{Enc}(sk; p)$.

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

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

§3.2 Definition of fully homomorphich public-key encryption

A scheme $\text{HPKE}$ 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 $\text{FHPKE} := (\text{KeyGen}; \text{Enc}; \text{Dec}; \text{Eval})$ 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 $sk \leftarrow \text{KeyGen}(1^\lambda)$, $\forall \text{ckt} \in CR_\lambda$, $\forall (p_1, \ldots, p_n) \in Fq^n$ where $n = n(\lambda)$, $\forall (C_1, \ldots, C_n)$ where $C_i \leftarrow (1C_i, 2C_i, 3C_i) \leftarrow \text{Enc}(sk; p_i)$, it holds that:

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

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

§3.3 Medium text

We define the medium text $M(p):=\{1M(p), 2M(p), 3M(p)\} \in O^3$ which is adopted in proposed fully homomorphic public-key encryption (FHPKE) scheme as follows.

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

$$[G]_0 = g_0 = 0 \mod q,$$
$$[H]_0 = h_0 = 0 \mod q,$$
$$[GH]_0 = [HG]_0 = g_0h_0 - (g_1h_1 + g_2h_2 + \ldots + g_7h_7) = 0 \mod q ,$$
$$[HG]_1 = [-GH]_1 = h_2g_4 + h_3g_7 - h_4g_2 + h_5g_6 - h_6g_5 - h_7g_3 \neq 0 \mod q,$$
$$L_G := |G|^2 = g_0^2 + g_1^2 + \ldots + g_7^2 \neq 0 \mod q ,$$
$$L_H := |H|^2 = h_0^2 + h_1^2 + \ldots + h_7^2 = 0 \mod q ,$$
$$G^2 = -L_G1 \mod q ,$$
$$H^2 = 0 \mod q ,$$

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

**Theorem 6**

$$GHG = L_GH \mod q ,$$
$$HGH = 0 \mod q ,$$
$$HG + GH = 0 \mod q .$$

*(Proof:)*

Here proof is omitted and can be looked up in the Appendix C.
Theorem 7

\[(GH)(HG) = 0 \mod q, \quad (32a)\]
\[(HG)(GH) = 0 \mod q. \quad (32b)\]

(Proof:)

From (15)

\[(GH)(HG) = (G(HH))G = (G(0))G = 0 \mod q,\]
\[(HG)(GH) = (H(GG))H = (H(-L_G1))H \]
\[= (-L_G1)H = 0 \mod q. \quad \text{q.e.d.}\]

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>G</th>
<th>H</th>
<th>GH</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>G</td>
<td>H</td>
<td>GH</td>
</tr>
<tr>
<td>G</td>
<td>G</td>
<td>-L_G1</td>
<td>GH</td>
<td>-L_GH</td>
</tr>
<tr>
<td>H</td>
<td>H</td>
<td>-GH</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GH</td>
<td>GH</td>
<td>L_GH</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Let \( p \in F_q \) be a plaintext and \( u,v \in F_q \) be the sub-plaintexts such that

\[ p = su + tv \mod q \in F_q, \]

where \( s,t \in F_q \) are the secret constant parameters such that

\[ GCD(s,q) = 1 \text{ and } GCD(t,q) = 1. \]

Let \( i_w, i_y, i_z \in F_q (i=1,2,3) \) be random numbers.

We define the medium text \( M(p) \) corresponding to the plaintext \( p \) by

\[ M(p) := \{^1M(p), ^2M(p), ^3M(p)\} \in O^3 \]
\[ ^1M(p) := ^1ku + ^1l vG + ^1wH + ^1yGH \in O, \]
\[ 2M(p) = 2^{(k_1)} + 2^{(l_1)} + w_1^{(l_1)} + 2^{(y_1)} G \mod q = O, \]
\[ 3M(p) = 3^{(k_1)} + 2^{(l_1)} + w_1^{(l_1)} + 2^{(y_1)} G \mod q = O, \]

where

\[ k_1, l_1 \in F_q \]

are the secret constant parameters such that

\[ GCD(k_1, q) = 1 \quad \text{and} \quad GCD(l_1, q) = 1 \quad (i=1,2,3). \]

\[ p = su + tv \mod q \in F_q \]

\[ = a[\beta M(p)]_0 + \beta[\gamma M(p)]_0 \]
\[ + a[\alpha M(p)]_0 + \beta[\gamma M(p)]_0 \]
\[ + a[\gamma M(p)]_0 + \beta[\gamma M(p)]_0 \]
\[ + a[\gamma M(p)]_0 + \beta[\gamma M(p)]_0 \mod q, \]
\[ = (a^{(k_1)} + \beta^{(l_1)} + \gamma^{(y_1)})u + (a^{(k_1)} + \beta^{(l_1)} + \gamma^{(y_1)})[GH]_1 v \mod q, \]

where \( \gamma \in F_q \) is a random number and \( \alpha, \beta \in F_q \) satisfy the following equations,

\[ (a^{(k_1)} + \beta^{(l_1)} + \gamma^{(y_1)}) = s \mod q, \]
\[ (a^{(k_1)} + \beta^{(l_1)} + \gamma^{(y_1)}) = t \mod q, \]

and \( k_1, 2k_1, l_1 \) and \( 2l_1 \) satisfy

\[ GCD(k_1, 2k_1, l_1, q) = 1 \mod q. \]

(Associativity of medium texts)

Let \( M(p_1) = \{1M(p_1), 2M(p_2), 3M(p_3)\} \in O^3 \), \( M(p_2) = \{1M(p_2), 2M(p_2), 3M(p_2)\} \in O^3 \) and \( M(p_3) = \{1M(p_3), 2M(p_3), 3M(p_3)\} \in O^3 \) be arbitrary three medium texts where

\[ 1M(p_1) = 1^{(k_1)}u_1 + 1^{(l_1)}v_1 + 1^{(y_1)}G \mod q \in O, \]
\[ 2M(p_1) = 2^{(k_1)}u_1 + 2^{(l_1)}v_1 + 2^{(y_1)}G \mod q \in O, \]
\[ 3M(p_1) = 3^{(k_1)}u_1 + 3^{(l_1)}v_1 + 3^{(y_1)}G \mod q \in O, \]
\[ 1M(p_2) = 1^{(k_2)}u_2 + 1^{(l_2)}v_2 + 1^{(y_2)}G \mod q \in O, \]
\[ 2M(p_2) = 2^{(k_2)}u_2 + 2^{(l_2)}v_2 + 2^{(y_2)}G \mod q \in O, \]
\[ 3M(p_2) = 3^{(k_2)}u_2 + 3^{(l_2)}v_2 + 3^{(y_2)}G \mod q \in O, \]
\[ 1M(p_3) = 1^{(k_3)}u_3 + 1^{(l_3)}v_3 + 1^{(y_3)}G \mod q \in O, \]
\[ 2M(p_3) = 2^{(k_3)}u_3 + 2^{(l_3)}v_3 + 2^{(y_3)}G \mod q \in O, \]
\[ 3M(p_3) = 3^{(k_3)}u_3 + 3^{(l_3)}v_3 + 3^{(y_3)}G \mod q \in O, \]
\[3^p(p_3):=3k^1+3^1v^3G+3w^3H+3^3y^3GH \mod q \in O.\]

As a set \(\{1,G,H,GH\}\) has an associative property on multiplication, for example,

\[
H(G(GH)) = H(-L_GH) = -L_GH^2 = 0 \mod q
\]

\[(HG)(GH) = -(GH)(GH) = 0 = H(G(GH)) \mod q,
\]

we have that

\[
(p^iM(p_1))^iM(p_2))^iM(p_3) = (p^iM(p_1))^iM(p_2))^iM(p_3) \mod q (i=1,2,3).
\]

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

\[
(p^iM(p_1))^iM(p_2))N \neq p^iM(p_1)^iM(p_2)N \mod q.
\]

That is, it is said that

though in general for arbitrary \(N \in O\)

\[
p^iM(p_1)^iM(p_2)^iM(p_3) \neq p^iM(p_1)^iM(p_2)^iM(p_3) \mod q (i=1,2,3),
\]

\[
p^iM(p_1)^iM(p_2)^iM(p_3) \neq p^iM(p_1)^iM(p_2)^iM(p_3) \mod q (i=1,2,3).
\]

§3.4 Proposed fully homomorphic public-key encryption

We propose a fully homomorphic public-key encryption (FHPKE) scheme on octonion ring over \(F_q\).

Here we define some parameters for describing FHPKE. Let \(q\) be as a large prime as \(O(2^{2000})\).

We select the element \(G=(g_0,g_1,\ldots,g_7) \in O\) and \(H=(h_0,h_1,\ldots,h_7) \in O\) such as defined in section §3.3 Medium text.

Let \(p \in F_q\) be a plaintext and \(u,v \in F_q\) be the sub-plaintexts such that \(p=uv+tv \mod q \in F_q\).

Let \(M(p) = \{p^iM(p),p^2M(p),p^3M(p)\} \subseteq O^3\) be the medium text where

\[
p^1M(p) := k^1+1v^1G+1w^1H+y^1GH \in O,
\]

\[
p^2M(p) := 2k^1+2v^1G+2w^1H+y^1GH \in O,
\]

\[
p^3M(p) := 3k^1+3v^1G+3w^1H+y^1GH \in O,
\]
\[ p = su + tv \mod q \in Fq \]
\[ = \alpha [^1M(p)]_0 + \beta [^2M(p)]_0 + \gamma [^3M(p)]_0 \]
\[ + \alpha [H[^1M(p) - [^1M(p)]_0 1)]_1 + \beta [H[^2M(p) - [^2M(p)]_0 1)]_1 \]
\[ + \gamma [H[^3M(p) - [^3M(p)]_0 1)]_1 \mod q, \]
\[ = (\alpha (k) + \beta (k) + \gamma (k))u + (\alpha (l) + \beta (l) + \gamma (l))[GH]_0 v \mod q. \]

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

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

\[ E(X,Y) := A_i \ldots (A_h (A_{h^{-1}} (\ldots (A_1^{-1} (X)) \ldots))) \ldots \mod q \in O[X,Y] \]  
(34)

\[ = (e_{000} x_0 y_0 + e_{010} x_0 y_1 + \ldots + e_{070} x_7 y_0, \]
\[ e_{100} x_0 y_0 + e_{110} x_0 y_1 + \ldots + e_{170} x_7 y_0, \]
\[ \ldots \ldots \]
\[ e_{700} x_0 y_0 + e_{710} x_0 y_1 + \ldots + e_{770} x_7 y_0) \]
\[ = \{e_{ijk}\} (i,j,k = 0,\ldots,7) \]  
(35)

with \( e_{ijk} \in Fq \) \((i,j,k = 0,\ldots,7)\) which is published in system centre.

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

As if \( Y = 1 \), then \( E(X,Y) = X \), some \( e_{ijk} \) are fixed such that
\[ e_{000} = 1, \ e_{010} = 0, \ldots, \ e_{070} = 0, \]
\[ e_{100} = 0, \ e_{110} = 1, \ldots, \ e_{170} = 0, \]
\[ \ldots \ldots \]
\[ e_{700} = 0, \ e_{710} = 0, \ldots, \ e_{770} = 1. \]

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

Let \( M(p_1) = \{^1M(p),^2M(p),^3M(p)\} \) and \( M(p_2) = \{^1M(p),^2M(p),^3M(p)\} \) be the medium texts corresponding to the plaintexts \( p_1 \) and \( p_2 \), respectively.

We define the addition and multiplication on \(^iE(X,Y)\) \((i = 1,2,3)\) as follows.

[Addition]

\[ E(X,^1M(p_1)) + E(X,^1M(p_2)) \mod q \]
\[ = A_i (\ldots (A_h (^1M(p_1) (A_{h^{-1}} (\ldots (A_1^{-1} (X) \ldots)))) \ldots) + A_i (\ldots (A_h (^1M(p_2) (A_{h^{-1}} (\ldots (A_1^{-1} (X) \ldots)))) \ldots) \ldots \]
\[ \begin{align*}
&= A_1(...(A_h([i^1M(p_1)+i^1M(p_2)](A_h^{-1}(...(...(A_1^{-1}X)...)...)))...)\mod q \\
&= E(X,i^1M(p_1)+i^1M(p_2)) \mod q \ (i=1,2,3).
\end{align*} \]

[Proof]

\[E(E(X,i^1M(p_2)),i^1M(p_1)) \mod q \]

\[= A_1(...(A_h([M(p_1)M(p_2)](A_h^{-1}(...(...(A_1^{-1}X)...)...)))...) \mod q \]

\[= A_1(...(A_h([M(p_1)M(p_2)](A_h^{-1}(...(...(A_1^{-1}X)...)...)))...) \mod q \]

We denote \(E(E(X,i^1M(p_2)),i^1M(p_1))\) by \(E(X,i^1M(p_1)<i^1M(p_2))\).

We notice that in general

\[E(X,M(p_1)M(p_2)=A_1(...(A_h([M(p_1)M(p_2)](A_h^{-1}(...(...(A_1^{-1}X)...)...)))...) \mod q \]

\[\neq A_1(...(A_h([M(p_1)M(p_2)](A_h^{-1}(...(...(A_1^{-1}X)...)...)))...) \mod q = E(X,i^1M(p_1)<i^1M(p_2)) \]

\[(i=1,2,3).\]

**Theorem 8**

For arbitrary \(p,p' \in O\),

if \(E(X,i^1M(p))= E(X,i^1M(p')) \mod q\) \((i=1,2,3)\), then \(p \equiv p' \mod q\),

where

\[p:=su+tv \mod q,\]

\[M(p):=\{1M(p),2M(p),3M(p)\} \in O^3,\]

\[1M(p):= ku_1+lv_1+wh+1yGH \in O,\]

\[2M(p):= ku_1+lv_1+wh+2yGH \in O,\]

\[3M(p):= ku_1+lv_1+wh+3yGH \in O,\]

\[p':=su'+tv' \mod q,\]

\[M(p'):=\{1M(p'),2M(p'),3M(p')\} \in O^3,\]

\[1M(p'):= ku_1+lv_1+wh+1y'GH \in O,\]

\[2M(p'):= ku_1+lv_1+wh+2y'GH \in O,\]

\[3M(p'):= ku_1+lv_1+wh+3y'GH \in O.\]

(Proof)
If \( E(X,^1M(p))= E(X,^1M(p')) \mod q \), then
\[
A_h^{-1}(\ldots (A_i^{-1}(E(A_i(\ldots (A_h 1) \ldots ))),^1M(p)) \mod q=^1M(p)
\]
\[
=A_h^{-1}(\ldots (A_i^{-1}(E(A_i(\ldots (A_h 1) \ldots )),^1M(p')) \mod q=^1M(p') \ (i=1,2,3) \mod q.
\]
Then we have
\[
^1M(p)=^1M(p') \ (i=1,2,3).
\]
\[
p=\alpha[^1M(p)]_0 +\beta[^2M(p)]_0 +\gamma[^3M(p)]_0
\]
\[
+\alpha[ (^1M(p)-[^1M(p)]_0 1) H]_1 +\beta[ (^2M(p)-[^2M(p)]_0 1) H]_1
\]
\[
+\gamma[ (^3M(p)-[^3M(p)]_0 1) H]_1 \mod q,
\]
\[
=p' \mod q,
\]
Then we have
\[
p= p' \mod q. \quad \text{q.e.d.}
\]

§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 \( h \) be a secret integer parameter. Let \( A:=\{A_1,\ldots A_h\} \in O^h \) be secret parameters. Let \( E(X,Y)=A_1(\ldots (A_h(Y(A_h^{-1}(\ldots (A_1^{-1}X) \ldots )))\ldots )) \mod q \in O[X,Y] \) 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 \( A:=\{A_1,\ldots A_h\} \in O^h \) with the order of the elements \( A_1,\ldots ,A_h \) . For parameters \( h=h(\lambda) \) defined in terms of the security parameter \( \lambda \) and for any PPT adversary \( A_d \) we have
\[
\Pr [A_1(\ldots (A_h(Y(A_h^{-1}(\ldots (A_1^{-1}X) \ldots )))\ldots )) \mod q =\{e_{ijk}\}(i,j,k=0,\ldots ,7) : \quad A=\{A_1,\ldots ,A_h\} \leftarrow A_d (1^i,q, E(X,Y))= \text{negl}(\lambda).
\]

To solve directly OEA(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 \( C(X,p)=\{E(X,^1M(p)), E(X,^2M(p)), E(X,^3M(p))\} \)
corresponding to the plaintexts \( p \) has the property of fully homomorphism.

### §3.7 Addition scheme on ciphertexts

Let

\[
M(p_1) := \{1M(p_1), 2M(p_1), 3M(p_1)\} \in O^3,
\]

\[
1M(p_1) := ku_1 + lv_1 G + w_1 H + y_1 GH \in O,
\]

\[
2M(p_1) := 2ku_1 + 2lv_1 G + 2w_1 H + 2y_1 GH \in O,
\]

\[
3M(p_1) := 3ku_1 + 3lv_1 G + 3w_1 H + 3y_1 GH \in O,
\]

\[
M(p_2) := \{1M(p_2), 2M(p_2), 3M(p_2)\} \in O^3,
\]

\[
1M(p_2) := ku_2 + lv_2 G + w_2 H + y_2 GH \in O,
\]

\[
2M(p_2) := 2ku_2 + 2lv_2 G + 2w_2 H + 2y_2 GH \in O,
\]

\[
3M(p_2) := 3ku_2 + 3lv_2 G + 3w_2 H + 3y_2 GH \in O,
\]

be medium texts to be encrypted where

\[
p_1 := (su_1 + tv_1) \mod q,
\]

\[
p_2 := (su_2 + tv_2) \mod q.
\]

Let \( C(X, p_1) := \{E(X, 1M(p_1)), E(X, 2M(p_1)), E(X, 3M(p_1))\} \in \{O[X]\}^3 \) and

\[
C(X, p_2) := \{E(X, 1M(p_2)), E(X, 2M(p_2)), E(X, 3M(p_2))\} \in \{O[X]\}^3
\]

be the ciphertexts corresponding to the plaintexts \( p_1 \) and \( p_2 \), respectively.

\[
C(X, p_1) + C(X, p_2) \mod q
\]

\[
:=(E(X, 1M(p_1)) + E(X, 1M(p_2)), E(X, 2M(p_1)) + E(X, 2M(p_2)), E(X, 3M(p_1)) + E(X, 3M(p_2))).
\]

\[
E(X, 1M(p_1)) + E(X, 1M(p_2))
\]

\[
=A_1(\ldots(A_h(M_1(A_h^{-1}(\ldots(A_1^{-1}X)\ldots))))\ldots) + A_1(\ldots(A_h(M_2(A_h^{-1}(\ldots(A_1^{-1}X)\ldots))))\ldots) \mod q
\]

\[
= A_1(\ldots(A_h([1M(p_1)] + 1M(p_2))(A_h^{-1}(\ldots(A_1^{-1}X)\ldots))))\ldots) \mod q
\]

\[
= A_1(\ldots(A_h([ku_1 + lv_1 G + w_1 H + y_1 GH + ku_2 + lv_2 G + w_2 H + y_2 GH](A_h^{-1}(\ldots(A_1^{-1}X)\ldots))))\ldots) \mod q
\]

\[
= A_1(\ldots(A_h([k(u_1 + u_2) + lv_1 G + w_1 H + y_1 GH + ku_2 + lv_2 G + w_2 H + y_2 GH](A_h^{-1}(\ldots(A_1^{-1}X)\ldots))))\ldots) \mod q
\]

\[
= A_1(\ldots(A_h([1M(p_1 + p_2)](A_h^{-1}(\ldots(A_1^{-1}X)\ldots))))\ldots) \mod q
\]
\[ = E(X, ^iM(p_1 + p_2)) \mod q \text{ (i=1,2,3).} \]

We have

\[ C(X,p_1)+C(X,p_2) = C(X,p_1+p_2) \mod q. \]

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

§3.8 Multiplication scheme on ciphertexts

§3.8.1 Expanded medium text and expanded plaintext

We define \(^1M(p_{12}), ^2M(p_{12})\) and \(^3M(p_{12})\) as expanded medium texts as follows.

\(^1M(p_{12}) := d_{11}^1M(p_1)^1M(p_2)+ d_{12}^2M(p_1)^2M(p_2)+ d_{13}^3M(p_1)^3M(p_2) \mod q \tag{37a} \]

\[=[d_{11}^1(k)^2 + d_{12}^2(k)^2 + d_{13}^3(k)^2]u_1u_2 + \]

\[ [d_{11}^1(k)^1 l + d_{12}^2(k)^1 l + d_{13}^3(k)^1 l](u_1v_2 + v_1u_2)G + \]

\[ [d_{11}^1(l)^2 + d_{12}^2(l)^2 + d_{13}^3(l)^2]v_1v_2G^2 + \] \(^1F(H, GH) \mod q \]

\[=\left\{[d_{11}^1(k)^2 + d_{12}^2(k)^2 + d_{13}^3(k)^2]u_1u_2 - L_G[d_{11}^1(l)^2 + d_{12}^2(l)^2 + d_{13}^3(l)^2]v_1v_2\right\}1 + \]

\[\left\{[d_{11}^1(k)^1 l + d_{12}^2(k)^1 l + d_{13}^3(k)^1 l](u_1v_2 + v_1u_2)\right\}G + \] \(^1F(H, GH) \mod q \]

\(^2M(p_{12}) := d_{21}^1M(p_1)^1M(p_2)+ d_{22}^2M(p_1)^2M(p_2)+ d_{23}^3M(p_1)^3M(p_2) \mod q \tag{37b} \]

\[=\left\{[d_{21}^1(k)^2 + d_{22}^2(k)^2 + d_{23}^3(k)^2]u_1u_2 - L_G[d_{21}^1(l)^2 + d_{22}^2(l)^2 + d_{23}^3(l)^2]v_1v_2\right\}1 + \]

\[\left\{[d_{21}^1(k)^1 l + d_{22}^2(k)^1 l + d_{23}^3(k)^1 l](u_1v_2 + v_1u_2)\right\}G + \] \(^2F(H, GH) \mod q. \]

\(^3M(p_{12}) := d_{31}^1M(p_1)^1M(p_2)+ d_{32}^2M(p_1)^2M(p_2)+ d_{33}^3M(p_1)^3M(p_2) \mod q \tag{37c} \]

\[=\left\{[d_{31}^1(k)^2 + d_{32}^2(k)^2 + d_{33}^3(k)^2]u_1u_2 - L_G[d_{31}^1(l)^2 + d_{32}^2(l)^2 + d_{33}^3(l)^2]v_1v_2\right\}1 + \]

\[\left\{[d_{31}^1(k)^1 l + d_{32}^2(k)^1 l + d_{33}^3(k)^1 l](u_1v_2 + v_1u_2)\right\}G + \] \(^3F(H, GH) \mod q \]

where

\(^iF(H, GH)\) is the linear combination of \(H\) and \(GH\) over \(Fq\) (i=1,2,3).

We define \(u_{12}, v_{12}\) as expanded sub-plaintexts and \(p_{12}\) as expanded plaintext as follows.

\[ u_{12} := su_1u_2 + (r^2/s)v_1v_2 \mod q \in Fq \tag{38a} \]

\[ v_{12} := s(u_1v_2 + u_2v_1) \mod q \in Fq \tag{38b} \]
\( p_{12} = su_{12} + tv_{12} \mod q \in F_q \).

We select \( (d_l) \) that satisfy the following equations.

\[
\begin{align*}
1^M(p_{12}) &= d_{11}^1 M(p_1)^1 M(p_2) + d_{12}^2 M(p_1)^2 M(p_2) + d_{13}^3 M(p_1)^3 M(p_2) \mod q \\
&= \mu_{12}^1 v_{12} G + F(H, GH) \mod q \\
&= k(su_{12} + (r^2/s)v_{12}) \mu_{12}^1 l(s(u_{12} + u_2 v_1) G + F(H, GH) \mod q \in O
\end{align*}
\]

\[
\begin{align*}
2^M(p_{12}) &= d_{21}^1 M(p_1)^1 M(p_2) + d_{22}^2 M(p_1)^2 M(p_2) + d_{23}^3 M(p_1)^3 M(p_2) \mod q \\
&= \nu_{12}^2 v_{12} G + F(H, GH) \mod q \\
&= k(su_{12} + (r^2/s)v_{12}) \nu_{12}^2 l(s(u_{12} + u_2 v_1) G + F(H, GH) \mod q \in O
\end{align*}
\]

\[
\begin{align*}
3^M(p_{12}) &= d_{31}^1 M(p_1)^1 M(p_2) + d_{32}^2 M(p_1)^2 M(p_2) + d_{33}^3 M(p_1)^3 M(p_2) \mod q \\
&= \lambda_{12}^3 v_{12} G + F(H, GH) \mod q
\end{align*}
\]

Then we have the following equations which a part of the public parameters, \( (d_l) \) has to satisfy.

\[
\begin{align*}
&d_{11} \mu_1 + d_{12} \nu_1 + d_{13} \lambda_1 \equiv 1 \mod q \\
&d_{21} \mu_2 + d_{22} \nu_2 + d_{23} \lambda_2 \equiv 1 \mod q \tag{39a}
\end{align*}
\]

\[
\begin{align*}
&d_{11} \mu_1 l + d_{12} \nu_1 l + d_{13} \lambda_1 l \equiv 1 \mod q \\
&d_{21} \mu_2 l + d_{22} \nu_2 l + d_{23} \lambda_2 l \equiv 1 \mod q \tag{39b}
\end{align*}
\]

\[
\begin{align*}
&d_{31} \mu_3 + d_{32} \nu_3 + d_{33} \lambda_3 \equiv 1 \mod q \\
&d_{31} \mu_3 l + d_{32} \nu_3 l + d_{33} \lambda_3 l \equiv 1 \mod q \tag{39c}
\end{align*}
\]

where \( ^i k, ^i l \ (i=1,2,3) \) satisfy

\[
\text{GCD}(\Delta, q) = 1
\]

where
\[\Delta = \begin{pmatrix}
(k^2) & (k^2) & (k^2) \\
(l^2) & (l^2) & (l^2) \\
1k & 1l & 2k & 2l & 3k & 3l
\end{pmatrix}.\]

Here we will show that

\[p_{12} = p_1 p_2 \mod q\]

\[= d[1M(p_{12})]_0 + \beta[2M(p_{12})]_0 + \gamma[3M(p_{12})]_0\]

\[+ d[(1M(p_{12}) - [1M(p_{12})]_0 1) H]_1 + \beta[(2M(p_{12}) - [2M(p_{12})]_0 1) H]_1\]

\[+ \gamma[(3M(p_{12}) - [3M(p_{12})]_0 1) H]_1 \mod q \in Fq.\]

From (38c), (38a) and (38b) we have

\[p_{12} = su_{12} + t\nu_{12} \mod q\]

\[= s(su_{12} + (\hat{r}^2/s)v_{12}) + ts(u_{v2} + u_{v1})\]

\[= (su_{1} + tv_{1}) (su_{2} + tv_{2})\]

\[= p_1 p_2 \mod q \in Fq.\]

On the other hand we have from (38c), (38a), (38b),(33a), (33b),(39a),(39b) and (39c)

\[p_{12} = su_{12} + t\nu_{12} \mod q\]

\[= (a(1k) + \beta(2k) + \gamma(3k)) (su_{12} + (\hat{r}^2/s)v_{12}) + (a(1l) + \beta(2l) + \gamma(3l))[GH]_1 (s(u_{v2} + u_{v1}))\]

\[= a[(1k) su_{12} + (1l)(\hat{r}^2/s)v_{12}] + \beta[(2k) su_{12} + (2l)(\hat{r}^2/s)v_{12}] + \gamma[(3k) su_{12} + (3l)(\hat{r}^2/s)v_{12}]\]

\[+ \alpha[(1l)s[GH]_1 (u_{v2} + u_{v1})] + \beta[(2l)s[GH]_1 (u_{v2} + u_{v1})] + \gamma[(3l)s[GH]_1 (u_{v2} + u_{v1})] + \alpha[(d_{11}(1k)^2 + d_{12}(2k)^2 + d_{13}(3k)^2) u_{u2} - L\alpha(d_{11}(1l)^2 + d_{12}(2l)^2 + d_{13}(3l)^2)v_{12})\]

\[+ \beta[(d_{21}(1k)^2 + d_{22}(2k)^2 + d_{23}(3k)^2) u_{u2} - L\alpha(d_{21}(1l)^2 + d_{22}(2l)^2 + d_{23}(3l)^2)v_{12})\]

\[+ \gamma[(d_{31}(1k)^2 + d_{32}(2k)^2 + d_{33}(3k)^2) u_{u2} - L\alpha(d_{31}(1l)^2 + d_{32}(2l)^2 + d_{33}(3l)^2)v_{12})\]

\[+ \alpha[(d_{11}(1k) + d_{12}(2k) + d_{13}(3k)) [GH]_1 (u_{v2} + u_{v1})]\]

\[+ \beta[(d_{21}(1k) + d_{22}(2k) + d_{23}(3k)) [GH]_1 (u_{v2} + u_{v1})]\]
\[ +\gamma \left[ (d_{31}(1) + d_{32}(k^2) + d_{33}(k^3)) [GH]_1 (u_1 v_2 + u_2 v_1) \right] \\
= a\left[ 1^1 M(p_{12}) + \beta[2^2 M(p_{12})] + \gamma[3^3 M(p_{12})] + \alpha \right] + \beta[2^2 M(p_{12})] + \gamma[3^3 M(p_{12})] \\
= \alpha[1^1 M(p_{12})] + \beta[2^2 M(p_{12})] + \gamma[3^3 M(p_{12})] + \gamma \left[ (\beta[2^2 M(p_{12})] + \gamma[3^3 M(p_{12})]) \right] H_1 \\
= \alpha + \beta + \gamma \mod q \in F_q. \]
+ d_{12} d_{22} M(p_1)^2 M(p_2)^2 M(p_3) + d_{12} d_{23} M(p_1)^3 M(p_2)^2 M(p_3)
+ d_{13} d_{31} M(p_1)^1 M(p_2)^3 M(p_3) + d_{13} d_{32} M(p_1)^2 M(p_2)^3 M(p_3)
+ d_{13} d_{33} M(p_1)^3 M(p_2)^3 M(p_3) \mod q \in O.

{^1}M(p_{1(23)}) \subseteq O

\begin{align*}
&= d_{11} M(p_1)^1 M(p_2)^2 M(p_3) + d_{12} M(p_1)^2 M(p_2)^3 M(p_3) \mod q
\end{align*}

Then we have in general

{^1}M(p_{1(23)}) \neq {^1}M(p_{1(23)}) \mod q \in O.

In the same manner we have in general

{^1}M(p_{1(23)}) \neq {^1}M(p_{1(23)}) \mod q \in O (i=2,3) \square.

We notice that

C(X, p_{1(23)}) \not\equiv C(X, p_{1(23)}) \mod q \in \{ O[X] \}^3

where

\begin{align*}
p_{123} = (p_1 p_2) p_3 = p_1 p_2 p_3 = p_1 (p_2 p_3) = p_1(23) \mod q \in Fq,
\end{align*}

\begin{align*}
C(X, p_{123}) &= \{ E(X, {^1}M(p_{123})) , E(X, {^2}M(p_{123})) , E(X, {^3}M(p_{123})) \} \subseteq \{ O[X] \}^3
C(X, p_{1(23)}) &= \{ E(X, {^1}M(p_{1(23)})) , E(X, {^2}M(p_{1(23)})) , E(X, {^3}M(p_{1(23)})) \} \subseteq \{ O[X] \}^3.
\end{align*}

§3.8.3 Multiplication scheme on ciphertexts

Here we consider the multiplicative operation on the ciphertexts.
Let
\[ C(X, p_1) := \{ E(X, 1^M(p_1)), E(X, 2^M(p_1)), E(X, 3^M(p_1)) \} \subseteq \{ O[X] \}^3 \]

and
\[ C(X, p_2) := \{ E(X, 1^M(p_2)), E(X, 2^M(p_2)), E(X, 3^M(p_2)) \} \subseteq \{ O[X] \}^3 \]
be the ciphertexts corresponding to the plaintexts \( p_1 \) and \( p_2 \), respectively.

Let
\[ C(X, p_{12}) := \{ E(X, 1^M(p_{12})), E(X, 2^M(p_{12})), E(X, 3^M(p_{12})) \} \subseteq \{ O[X] \}^3 \]
where three sub-ciphertexts \( E(X, 1^M(p_{12}))(i=1,2,3) \) are given such that
\[ E(X, 1^M(p_{12})) \subseteq O[X] \]
\[ = d_1 E(X, 1^M(p_1)) + d_2 E(X, 2^M(p_2)) + d_3 E(X, 3^M(p_2)) \]
\[ = d_1 E(X, 1^M(p_1)) + d_2 E(X, 2^M(p_2)) + d_3 E(X, 3^M(p_1)) \]
\[ (i=1,2,3). \]

We confirm that \( C(X, p_{12}) \) is the ciphertext corresponding to the plaintext \( p_1 p_2 \), that is, we decipher \( C(X, p_{12}) \) to obtain \( p_1 p_2 \) as follows.

\[ A_1^{-1}(...(A_1^{-1} (E(A_1(...(A_1 ... A_1 ... 1^M(p_{12})))...)) \]
\[ = A_1^{-1}(...(A_1^{-1} (d_1 E(A_1(...(A_1 ... 1^M(p_1)) < M(p_2)) \]
\[ + A_1^{-1}(...(A_1^{-1} (d_2 E(A_1(...(A_1 ... 2^M(p_1)) < M(p_2)) \]
\[ + A_1^{-1}(...(A_1^{-1} (d_3 E(A_1(...(A_1 ... 3^M(p_1)) < M(p_2)) \]
\[ = d_1 1^M(p_1) 1^M(p_2) + d_2 2^M(p_1) 2^M(p_2) + d_3 3^M(p_1) 3^M(p_2) \]
\[ = ^1M(p_{12}) \mod q \subseteq O (i=1,2,3). \]

From §3.8.1
\[ p_{12} = a [1^M(p_{12})]_0 + b [2^M(p_{12})]_0 + c [3^M(p_{12})]_0 \]
\[ + a [H(1^M(p_{12})-1^M(p_{12})]_0 [GH] \]
\[ + b [H(2^M(p_{12})-2^M(p_{12})]_0 [GH] \]
\[ + c [H(3^M(p_{12})-3^M(p_{12})]_0 [GH] \mod q, \]
\[ = p_1 p_2 \mod q \subseteq Fq. \]

§3.9 Property of proposed fully homomorphic encryption
The syntax of proposed scheme is given as follows.

-Key-Generation. The algorithm $\textbf{KeyGen}$, on input the security parameter $1^k$ and system parameter $q$, outputs
$$\textbf{sk}\leftarrow \textbf{KeyGen}(1^k) \text{ where } \textbf{sk}=(h^jA_{j=1,...,h},s,t^ik^j_{i=1,2,3}) \text{ is a secret encryption key and}$$
$$\textbf{pk}\leftarrow \textbf{KeyGen}(1^k) \text{ where } \textbf{pk}=\{(e_{ijk})_{0\leq i,j,k\leq 7}\cap \mathbb{F}_q, H, \alpha, \beta, \gamma \} \text{ is a public key.}$$

-Encryption. The algorithm $\textbf{Enc}$, on input system parameter $q$, and secret keys of user B, $\textbf{sk}_B=(h_B, B_{j=1,...,h_B}, s_B, t_B^ik_B^j_{i=1,2,3})$, public key of user A, $\textbf{pk}_A=\{(e_{ijk})_{0\leq i,j,k\leq 7}\cap \mathbb{F}_q, G_A, H_A, \alpha_A, \beta_A, \gamma_A\}$ and a plaintext $p \in \mathbb{F}_q$, outputs a ciphertext
$$\textbf{C}(X; \textbf{sk}_B, \textbf{pk}_A, p) \leftarrow \textbf{Enc}(\textbf{sk}_B, \textbf{pk}_A, p).$$

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

-Homomorphic-Evaluation. The algorithm $\textbf{Eval}$, on input system parameter $q$, an arithmetic circuit $\textbf{ckt}$, and a tuple of $n$ ciphertexts $(\textbf{C}_1, \ldots, \textbf{C}_n)$, outputs an evaluated ciphertext $\textbf{C}' \leftarrow \textbf{Eval}(\textbf{ckt}; \textbf{C}_1, \ldots, \textbf{C}_n)$ where $\textbf{C}_i=C(X; \textbf{sk}_B, \textbf{pk}_A, p_i)$ ($i=1, \ldots, n$).

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

1. Homomorphism: Let $\mathbb{CR}_q=\{CR_q^\lambda\}_{\lambda \subseteq \mathbb{N}}$ be the set of all polynomial sized arithmetic circuits. On input $\textbf{sk} \leftarrow \textbf{KeyGen}(1^k)$, $\textbf{pk} \leftarrow \textbf{KeyGen}(1^k)$, $\forall \text{ckt} \in \mathbb{CR}_q$, $\forall (p_1, \ldots, p_n) \in \mathbb{F}_q^n$ where $n=n(\lambda)$, $\forall (C_1, \ldots, C_n)$ where $C_i=C(X; \textbf{sk}_B, \textbf{pk}_A, p_i) \leftarrow \textbf{Enc}(\textbf{sk}_B, \textbf{pk}_A, p_i)$, ($i=1, \ldots, n$), we have $\textbf{Dec}(\textbf{sk}_A, \textbf{pk}_B; \textbf{Eval}(\textbf{ckt}; C_1, \ldots, C_n)) = \text{ckt}(p_1, \ldots, p_n)$. Then it holds that:
$$\Pr[\textbf{Dec}(\textbf{sk}_A, \textbf{pk}_B; \textbf{Eval}(\textbf{ckt}; C_1, \ldots, C_n)) \neq \text{ckt}(p_1, \ldots, p_n)] = \text{negl}(\lambda).$$

2. Compactness: As the output length of $\textbf{Eval}$ 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 $\textbf{Eval}$ is at most $\mu$ bits long regardless of the input circuit $\textbf{ckt}$ 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 $pk_A$ and the secret key of user B $sk_B$ through the insecure line.

1) System centre publishes the system parameter $[q]$.
2) User A selects $sk_A=(h_A, A_A, t_A, l_A, k_A(i=1,2,3))$ which is a secret key of user A and generates the public key of user A $pk_A=\{(e_{A_{ijk}})_{0\leq i,j,k<7} : G_{A_i}H_{A_i}, \alpha_A, \beta_A, \gamma_A\}$ such that
\[
E_A(X,Y)=A_1(\ldots(A_{hA}(Y(A_{hA}^{-1}(\ldots(A_1^{-1}X))))\ldots)) \mod q \in O[X,Y]
\]
\[
=\{e_{A_{ijk}}\}(i,j,k=0,\ldots,7).
\]
User A sends $\{e_{A_{ijk}}\}(i,j,k=0,\ldots,7)$ with $G_{A_i}H_{A_i}, \alpha_A, \beta_A, \gamma_A$ to system centre.
3) User B selects $sk_B=(h_B, A_B, t_B, l_B, k_B(i=1,2,3))$ which is a secret key of user B and generates the public key of user B $pk_B=\{(e_{B_{ijk}})_{0\leq i,j,k<7} : G_{B_i}H_{B_i}, \alpha_B, \beta_B, \gamma_B\}$ such that
\[
E_B(X,Y)=B_1(\ldots(B_{hB}(Y(B_{hB}^{-1}(\ldots(B_1^{-1}X))))\ldots)) \mod q \in O[X,Y]
\]
\[
=\{e_{B_{ijk}}\}(i,j,k=0,\ldots,7).
\]
User B sends $\{e_{B_{ijk}}\}(i,j,k=0,\ldots,7)$ with $G_{B_i}H_{B_i}, \alpha_B, \beta_B, \gamma_B$ to system centre.
4) User B downloads $E_A(X,Y)=\{e_{A_{ijk}}\}(i,j,k=0,\ldots,7)$ from system centre.
5) User B generates the common enciphering function $E_{BA}(X,Y)$ as follows.
\[
E_{B1}(X,Y):=E_A(E_A(X,Y),B_1)
\]
\[
=A_1(\ldots(A_{hA}(B_1(A_{hA}^{-1}(\ldots(A_1^{-1}[A_1(\ldots(A_{hA}(Y(A_{hA}^{-1}(\ldots(A_1^{-1}X))))\ldots)]))\ldots))))\ldots)
\]
\[
=A_1(\ldots(A_{hA}(B_1(Y(A_{hA}^{-1}(\ldots(A_1^{-1}X))))\ldots)) \mod q \in O[X,Y]
\]
\[
E_{B2}(X,Y):=E_{B1}(E_A(X,Y),B_2)
\]
\[
=A_1(\ldots(A_{hA}(B_1(B_2(A_{hA}^{-1}(\ldots(A_1^{-1}[A_1(\ldots(A_{hA}(Y(A_{hA}^{-1}(\ldots(A_1^{-1}X))))\ldots)]))\ldots))))\ldots)
\]
\[
=A_1(\ldots(A_{hA}(B_1(B_2(Y(A_{hA}^{-1}(\ldots(A_1^{-1}X))))\ldots)))) \mod q \in O[X,Y]
\]
\[
\ldots 
\]
\[
E_{Bhb}(X,Y):=E_{Bhb}(E_{A}(X,Y),B_{hb})
\]
\[
=\ldots(\ldots(A_{hA}(B_1(\ldots(B_{hb}(A_{hA}^{-1}(\ldots(A_1^{-1}[A_1(\ldots(A_{hA}(Y(A_{hA}^{-1}(\ldots(A_1^{-1}X))))\ldots)]))\ldots))))\ldots))\ldots)
\]
\[
=A_1(\ldots(A_{hA}(B_1(\ldots(B_{hb}(Y(A_{hA}^{-1}(\ldots(A_1^{-1}X))))\ldots)))) \mod q \in O[X,Y]
\]
\[
E_{Bhb}^{-1}(X,Y):=E_{Bhb}(E_{A}(X,B_{hb}^{-1}),Y)
\]
\[
=\ldots(\ldots(A_{hA}(B_1(\ldots(B_{hb}(Y(A_{hA}^{-1}(\ldots(A_1^{-1}[A_1(\ldots(A_{hA}(B_{hb}^{-1}(A_{hA}^{-1}(\ldots(A_1^{-1}X))))\ldots)]))\ldots))\ldots))\ldots))\ldots)
\]
\[ A_1(\ldots (A_{ha}(B_1(\ldots (B_{hb}(Y(B_{hb}^{-1}(A_{ha}^{-1}((A_1^{-1}X)\ldots )))\ldots )))\ldots )))\ldots ) = (e_{000}^{-1}m_0 + e_{001}^{-1}m_1 + \ldots + e_{078}^{-1}m_7, e_{090}^{-1}m_0 + e_{101}^{-1}m_1 + \ldots + e_{107}^{-1}m_7, \ldots) \mod q \in O[X,Y] \]
\[ e_{700}m_0 + e_{701}m_1 + \ldots + e_{707}m_7 \]

where \( iM(p) = (i_0, \ldots, i_7) \) (i=1,2,3).

\( (i_0, \ldots, i_7) \) is obtained by solving above simultaneous equation.

10) User A downloads the public key of user B \( \text{pk}_B = (\{e_{B_{ijk}}\}_{0 \leq i,j,k < 7} : G_B, H_B, \alpha_B, \beta_B, \gamma_B) \). Then the plaintext \( p \) is recovered such that

\[
p = \alpha_B [1M(p)]_0 + \beta_B [2M(p)]_0 + \gamma_B [3M(p)]_0
+ \alpha_B [H(1M(p)-1M(p))_01]_1 + \beta_B [H(2M(p)-2M(p))_01]_1
+ \gamma_B [H(3M(p)-3M(p))_01]_1 \mod q,
\]

\[
= \alpha_B (1m_0) + \beta_B (2m_0) + \gamma_B (3m_0) + \alpha_B [1M(p)-1m_0] H1 + \beta_B [2M(p)-2m_0] H1
+ \gamma_B [3M(p)-3m_0] H1 \mod q,
\]

\[
= \alpha_B (1m_0) + \beta_B (2m_0) + \gamma_B (3m_0) + \alpha_B ((0,1m_1,\ldots,1m_7)) H1 + \beta_B ((0,2m_1,\ldots,2m_7) H1
+ \gamma_B ((0,3m_1,\ldots,3m_7) H1 \mod q \in Fq.
\]

§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 \( X=(x_0, \ldots, x_7) \in O[X] \) and \( Y=(y_0, \ldots, y_7) \in O[X] \) be variables.

\[
E(X,Y)=A_1((\ldots (A_h(Y(A_h^{-1}(\ldots (A_1^{-1}X)\ldots ))\ldots ))\ldots ) \mod \in O[X,Y] \quad (40)
\]

\[
= (e_{000}x_0y_0 + e_{001}x_0y_1 + \ldots + e_{077}x_7y_7,
\]

\[
e_{100}x_0y_0 + e_{101}x_0y_1 + \ldots + e_{177}x_7y_7,
\]

\[
\ldots \quad \ldots
\]

\[
e_{700}x_0y_0 + e_{701}x_0y_1 + \ldots + e_{777}x_7y_7)^i, \quad (41)
\]

\[
= \{e_{ijk}\}_{i,j,k=0,\ldots,7}.
\]

\( A_{i} \in O \) to be selected randomly such that \( A_{i}^{-1} \) exist (j=1,\ldots,h) are parts of the secret keys of user A.
We try to find $A_i(i=1,\ldots,h)$ from coefficients of $E(X,Y)$, $e_{ijk} \in F_q$ ($i,j,k=0,1,\ldots,7$).

In case that $h=56$ the number of unknown variables $(A_i(i,j,k=1,\ldots,56))$ is $448(=64*8-64)$, the number of equations is $448(=64*8-64)$ such that

\[
\begin{align*}
F_{001}(A_1, \ldots, A_{56}) &= e_{001} \pmod{q}, \\
F_{002}(A_1, \ldots, A_{56}) &= e_{002} \pmod{q}, \\
& \quad \ldots \quad \ldots \\
F_{177}(A_1, \ldots, A_{56}) &= e_{077} \pmod{q}, \\
& \quad \ldots \quad \ldots \\
F_{777}(A_1, \ldots, A_{64}) &= e_{777} \pmod{q},
\end{align*}
\]

where $F_{001}, \ldots, F_{003}, F_{011}, \ldots, F_{017}, \ldots, F_{701}, \ldots, F_{776}, F_{777}$ are the 112($=56*2$)th algebraic multivariate equations.

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

\[
G > G' = (448 + d_{reg}C_{d_{reg}})^w = (25312C_{448})^w \gg O(2^{80}),
\]

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

\[
d_{reg} = 24864(=448*(112-1)/2 - \sqrt{448^2+112^2-1}/6).
\]

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

\section{4.2 Computing plaintext $p$ and $A_i$, $B_j$ from coefficients of ciphertext $E_{BA}(X,iM(p))$}

Ciphertext $E_{BA}(X,iM(p))(i=1,2,3)$ is generated by user B as follows.

\[
E_{BA}(X,iM(p)) \in O[X]
\]

\[
= A_1(\ldots(A_{hA}(B_1(\ldots(B_{hB}(1+iB^{j}+i^{j}yB^{3}+i^{j}yB^{3})B_{hB-1}^{-1}(B_{hB-1}^{-1}(\ldots(B_1^{-1}(A_{hA}^{-1}(\ldots(A_{hA}^{-1}(X)\ldots))))\ldots))))\ldots)))\ldots)
\]

\[
= A_1(\ldots(A_{hA}(B_1(\ldots(B_{hB}(1+iB^{j}+i^{j}yB^{3}+i^{j}yB^{3})B_{hB-1}^{-1}(B_{hB-1}^{-1}(\ldots(B_1^{-1}(A_{hA}^{-1}(\ldots(A_{hA}^{-1}(X)\ldots))))\ldots))))\ldots)))\ldots)
\]

\[
= (i^{e_{00}}x_0 + i^{e_{01}}x_1 + \ldots + i^{e_{07}}x_7,
\]

\[
i^{e_{10}}x_0 + i^{e_{11}}x_1 + \ldots + i^{e_{17}}x_7,
\]

\[
i^{e_{20}}x_0 + i^{e_{21}}x_1 + \ldots + i^{e_{27}}x_7,
\]

\[
i^{e_{30}}x_0 + i^{e_{31}}x_1 + \ldots + i^{e_{37}}x_7,
\]

\[
i^{e_{40}}x_0 + i^{e_{41}}x_1 + \ldots + i^{e_{47}}x_7,
\]

\[
i^{e_{50}}x_0 + i^{e_{51}}x_1 + \ldots + i^{e_{57}}x_7,
\]

\[
i^{e_{60}}x_0 + i^{e_{61}}x_1 + \ldots + i^{e_{67}}x_7,
\]

\[
i^{e_{70}}x_0 + i^{e_{71}}x_1 + \ldots + i^{e_{77}}x_7.
\]
\[ i e_7 x_0 + i e_7 x_1 + \ldots + i e_7 x_7 \mod \, q, \]

\[ = \{i e_j\} (j,k=0,\ldots,7; i=1,2,3) \]

with \( i e_j \in F_q (j,k=0,\ldots,7; i=1,2,3), \)

where \( p = su + tv \mod \, q. \)

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

We try to find plaintext \( p \) and \( A_i, B_j \) \((i=1,\ldots,h_A; j=1,\ldots,h_B)\) from coefficients of \( E_{BA}(X, M(p)) (i=1,2,3) \), \( i e_j \in F_q \) \((j,k=0,\ldots,7; i=1,2,3)\).

In case that \( h_A = 56 \) and \( h_B = 56 \) the number of unknown variables \((u,v,s,t, i_k, j, A_j, B_k, i=1,2,3; j,k=1,\ldots,56)\) is \( 906(=4+3*2+2*56*8) \), the number of equations is \( 192(=64*3) \) such that

\[
\begin{align*}
F_{100}(u,v,s,t,A_1,\ldots,A_{56}, B_1,\ldots,B_{56}) = & \ e_{00} \mod \ q, \\
F_{101}(u,v,s,t,A_1,\ldots,A_{56}, B_1,\ldots,B_{56}) = & \ e_{01} \mod \ q, \\
\vdots & \ \vdots \\
F_{107}(u,v,s,t,A_1,\ldots,A_{56}, B_1,\ldots,B_{56}) = & \ e_{07} \mod \ q, \\
\vdots & \ \vdots \\
F_{377}(u,v,s,t,A_1,\ldots,A_{56}, B_1,\ldots,B_{56}) = & \ e_{77} \mod \ q, 
\end{align*}
\]

(45)

where \( F_{100}, \ldots, F_{377} \) are the \( 227(=56*2*2+3) \)th algebraic multivariate equations.

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

\[ G > G' = (191 + d_{reg} C_{d_{reg}})^w = (21887 C_{191})^w \gg O(2^{80}), \]

(46)

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

\[ d_{reg} = 21696(=192*(227-1)/2 - 0\sqrt{(192*(227^2-1)/6))}. \]

(47)
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 $M(p)$ by

$$\begin{align*}
M(p):=\sum_{i=1}^{3} ku_1 iv G + iv w H + iv y H \in O, \quad (i=1,2,3)
\end{align*}$$

(48)

where $u \in \mathbb{F}_q$ is selected randomly, and $v=(p-su)r^{-1} \mod q$, plaintext $p=su+tv \mod q \in \mathbb{F}_q$.

We define the medium text $M(-p)$ by

$$\begin{align*}
M(-p):=\sum_{i=1}^{3} ku'1 iv G + iv w H + iv y H \in O, \quad (i=1,2,3),
\end{align*}$$

(49)

where $u' \in \mathbb{F}_q$ is selected randomly, and $v'=(p-su)r^{-1} \mod q, -p=su'+tv' \mod q$.

the ciphertext of $p$, $E_{BA}(X, M(p))(i=1,2,3),$

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

$$\begin{align*}
&= A_1(\ldots(A_{hA}(B_1(\ldots(B_{hb}^i M(p)(B_{hb}^{-1}(B_{hb}^{-1}(\ldots(B_1^{-1}(A_{hA}^{-1}(A_1^{-1}X)))))\ldots))))\ldots) \mod q
\end{align*}$$

$$\begin{align*}
&= A_1(\ldots(A_{hA}(B_1(\ldots(B_{hb}^i ku_1 iv G + iv w H + iv y H)(B_{hb}^{-1}(B_{hb}^{-1}(\ldots(B_1^{-1}(A_{hA}^{-1}(A_1^{-1}X)))))\ldots))))\ldots) \mod q,
\end{align*}$$

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

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

$$\begin{align*}
&= A_1(\ldots(A_{hA}(B_1(\ldots(B_{hb}^i ku_1 iv G + iv w H + iv y H)(B_{hb}^{-1}(B_{hb}^{-1}(\ldots(B_1^{-1}(A_{hA}^{-1}(A_1^{-1}X)))))\ldots))))\ldots) \mod q
\end{align*}$$

$$\begin{align*}
&= A_1(\ldots(A_{hA}(B_1(\ldots(B_{hb}^i ku_1 iv G + iv w H + iv y H)(B_{hb}^{-1}(B_{hb}^{-1}(\ldots(B_1^{-1}(A_{hA}^{-1}(A_1^{-1}X)))))\ldots))))\ldots) \mod q.
\end{align*}$$

As $p=su+tv \mod q$ and $-p=su'+tv' \mod q$, we have

$$\begin{align*}
p-p&=0=s(u+u')+(v+v') \mod q,
(v+v')&=-s t^{-1} (u+u') \mod q.
\end{align*}$$

We have

$$\begin{align*}
E_{BA}(X, M(p)) + E_{BA}(X, M(-p))
\end{align*}$$

$$\begin{align*}
&= E_{BA}(X, ku_1 iv G + iv w H + iv y H + ku_1 iv G + iv w H + iv y H) \mod q
\end{align*}$$
\[ E_{BA}(X, i(k+u')I^1+1(v+v')G+(i(w+w')H+(i(y+y')GH) \mod q \]
\[ = E_{BA}(X, (u+u')(i(k_{lst}^{-1}G)+(i(w+w')H+(i(y+y')GH) \mod q. \]

As \( i(k_{lst}^{-1}G) \neq 0 \mod q \) and in general \( u+u' \neq 0 \mod q \in F/q \), we have
\[ E_{BA}(X, iM(p))+ E_{BA}(X, iM(-p)) \neq 0 \mod q. (i=1,2,3) \] (50)

We can calculate \( |E_{BA}(1,iM(p))+ E_{BA}(1,iM(-p))|^2 \) as follows.
\[ E_{BA}(1,iM(p))+ E_{BA}(1,iM(-p))|^2 \]
\[ = |(u+u')(i(k_{lst}^{-1}G)+(i(w+w')H+(i(y+y')GH) |^2. \]

Even if \( (i(w+w')=(i(y+y')=(i(z+z')=0 \mod q \), we only have
\[ = (u+u')^2 ((i(k)^2+(i(lst)^{-1})^2 (g_1^2+g_2^2+...+g_7^2) \mod q \]
\[ = (u+u')^2 ((i(k)^2+(i(lst)^{-1})^2 L_G \mod q \]
\[ \neq 0 \mod q (i=1,2,3) \) (in general).

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 the system parameter \( q \). We select \( q=O(2^{2000}) \).

1) In case of \( h=56, q=O(2^{2000}) \), the size of \( e_{ik} \in F/q \) \((i,j,k=0,\ldots,7)\) which are the coefficients of elements in \( E(X,Y)= A_1(\ldots(A_h(Y(A_h^{-1}(\ldots(A_1^{-1}X)\ldots)))\ldots) \mod q \in O[X,Y] \) is \((448)(\log_2 q)\) bits =896kbis.

2) In case of \( h_A=56, q=O(2^{2000}) \), the complexity to obtain \( E_A(X,Y) \) from \( A_1,\ldots,A_{h_A}( \) and \( q \)
\[ (55*512+55*8*512)(\log_2 q)^2+56*(16*(\log_2 q)^2+2*(\log_2 q)^3)= O(2^{44}) \) bit-operations, where \( 56*(16*(\log_2 q)^2+2*(\log_2 q)^3) \) is the complexity for inverse of \( A_i^{-1}(i=1,\ldots,56). \)
3) In case of $h_B=56$, $q=O(2^{2000})$, the complexity to obtain $E_{BA}(X,Y)$ from $E_A(X,Y)$, $B_1,\ldots,B_{6B}, B_{6A}^{-1},\ldots,B_1^{-1}$ and $q$ is

$((512+64\times8\times8)\times56+(512+64\times8\times8)\times56) (\log_2 q)^2 = O(2^{43})$ bit-operations.

4) In case of $h_A=56$, $q=O(2^{2000})$, the complexity to obtain $E_{AB}(X,Y)$ from $E_B(X,Y)$, $A_1,\ldots,A_{6A}, A_{6A}^{-1},\ldots,A_1^{-1}$ and $q$ is

$(64\times8\times55+8\times64\times8\times56\times8\times64) (\log_2 q)^2 = O(2^{41})$ bit-operations.

5) In case of $q=O(2^{2000})$, the complexity to obtain $iC(X)=E_{BA}(X,\mathbf{i}M(p))(i=1,2,3)$ from $E_{BA}(X, Y), p, u, k, l, w, y, G, H, GH, s, t$ and $q$ is

$2* (\log_2 q)^2 +2*(\log_2 q)^3 +3*(1+9+8+64\times8) (\log_2 q)^2 = O(2^{35})$ bit-operations.

6) In case of $h_A=56$, $q=O(2^{2000})$, the complexity for deciphering $iC(X)=E_{BA}(X,\mathbf{i}M(p))(i=1,2,3)$ to obtain $p$ from $iC(X)=E_{BA}(X,\mathbf{i}M(p))(i=1,2,3)$, $H, A_1,\ldots,A_{6A}, A_{6A}^{-1},\ldots,A_1^{-1}$ and $q$ is

$[64\times56+3*(64\times56+64+64\times56+8\times8+7+7+7+\ldots+2+1+1+2+\ldots+7) +3+8\times8\times3+3]\times(\log_2 q)^2 +8\times2\times(\log_2 q)^3 = O((3584+3\times7464+198)2^{22}+2^{37}) = O(2^{38})$ bit-operations.

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

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

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

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.
§7. BIBLIOGRAPHY

[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.


Appendix A:

**Octinv(A)**

\[ S \leftarrow a_0^2 + a_1^2 + \ldots + a_7^2 \mod q. \]

\[ \% S^{-1} \mod q \]

\[ q[1] \leftarrow \text{q div } S ; \% \text{ integer part of } q/S \]

\[ r[1] \leftarrow \text{q mod } S ; \% \text{ residue} \]

\[ k \leftarrow 1 \]

\[ q[0] \leftarrow q \]

\[ r[0] \leftarrow S \]

while \( r[k] \neq 0 \)

begin

\[ k \leftarrow k + 1 \]

\[ q[k] \leftarrow r[k-2] \text{ div } r[k-1] \]

\[ r[k] \leftarrow r[k-2] \text{ mod } [r[k-1]} \]

end

\[ Q[k-1] \leftarrow (-1) \cdot q[k-1] \]

\[ L[k-1] \leftarrow 1 \]

\[ i \leftarrow k-1 \]

while \( i > 1 \)

begin

\[ Q[i-1] \leftarrow (-1) \cdot Q[i] \cdot q[i-1] + L[i] \]

\[ L[i-1] \leftarrow Q[i] \]

\[ i \leftarrow i-1 \]

end

\[ \text{invS} \leftarrow Q[1] \mod q \]

\[ \text{invA}[0] \leftarrow a_0 \cdot \text{invS} \mod q \]

For \( i=1, \ldots, 7, \)

\[ \text{invA}[i] \leftarrow (-1) \cdot a_i \cdot \text{invS} \mod q \]

Return \( A^{-1} = (\text{invA}[0], \text{invA}[1], \ldots, \text{invA}[7]) \)
Appendix B:
Lemma 2

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

(Proof):

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

\[ AB \mod q \]

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

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

\[
=\{ (a_0^2+a_1^2+\ldots+a_7^2) b_0 \}/|A|^2 = b_0 \mod q
\]

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

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

Similarly we have

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

Then we have

\[A^{-1}(AB) = B \mod q. \quad \text{q.e.d.}\]

**Appendix C:**

**Theorem 6**

Let \(O\) be the octonion ring over a finite field \(R\) such that

\[O = \{(a_0,a_1,\ldots,a_7) \mid a_j \in \mathbb{F}_q \ (j=0,1,\ldots,7)\}.\]

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

\[G=(g_0,g_1,\ldots,g_7), \ g_j \in \mathbb{F}_q \ (j=0,1,\ldots,7),\]
\[H=(h_0,h_1,\ldots,h_7), \ h_j \in \mathbb{F}_q \ (j=0,1,\ldots,7),\]

where

\[g_0=0 \mod q, \ h_0=0 \mod q,\]
\[L_G=g_0^2+g_1^2+\ldots+g_7^2 \neq 0 \mod q,\]
\[L_H=h_0^2+h_1^2+\ldots+h_7^2 = 0 \mod q\]

and

\[g_1h_1+g_2h_2+g_3h_3+g_4h_4+g_5h_5+g_6h_6+g_7h_7 = 0 \mod q.\]

\(G,H\) satisfy the following equations.

\[(GH)G = L_G H \mod q,\]
\[(HG)H = 0 \mod q,\]
\[HG+GH = 0 \mod q.\]
(Proof:)  

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

\[ [(GH)G]_0 \mod q \]
\[ = (g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7 ) g_0 \]
\[ \quad - (g_0h_1 + g_1h_0 + g_2h_4 + g_3h_7 + g_4h_2 + g_5h_6 + g_6h_5 - g_7h_3 ) g_1 \]
\[ \quad - (g_0h_2 - g_1h_4 + g_2h_0 + g_3h_5 + g_4h_1 + g_5h_3 + g_6h_7 - g_7h_6 ) g_2 \]
\[ \quad - (g_0h_3 - g_1h_7 - g_2h_5 + g_3h_0 + g_4h_6 + g_5h_2 - g_6h_4 + g_7h_1 ) g_3 \]
\[ \quad - (g_0h_4 + g_1h_2 - g_2h_1 - g_3h_6 + g_4h_0 + g_5h_7 + g_6h_3 - g_7h_5 ) g_4, \]
\[ \quad - (g_0h_5 - g_1h_6 + g_2h_3 - g_3h_2 - g_4h_7 + g_5h_0 + g_6h_1 + g_7h_4) g_5 \]
\[ \quad - (g_0h_6 + g_1h_5 - g_2h_7 + g_3h_4 - g_4h_3 - g_5h_1 + g_6h_0 + g_7h_2 ) g_6 \]
\[ \quad - (g_0h_7 + g_1h_3 + g_2h_6 - g_3h_1 + g_4h_5 - g_5h_4 - g_6h_2 + g_7h_0 ) g_7) \mod q \]

As
\[ h_0 = 0 \mod q, \]
\[ L_G := g_0^2 + g_1^2 + \ldots + g_7^2 \neq 0 \mod q, \]
\[ L_H := h_0^2 + h_1^2 + \ldots + h_7^2 = 0 \mod q \]

and
\[ g_1h_1 + g_2h_2 + g_3h_3 + g_4h_4 + g_5h_5 + g_6h_6 + g_7h_7 = 0 \mod q, \]

we have
\[(GH)G\]_0 \mod q
\]
\[
= (g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7) g_0
\]
\[- (g_0h_1 + g_1h_0 + g_2h_4 + g_3h_7 - g_4h_2 + g_5h_6 - g_6h_5 - g_7h_3) g_1
\]
\[- (g_0h_2 - g_1h_4 + g_2h_0 + g_3h_5 + g_4h_1 - g_5h_3 + g_6h_7 - g_7h_6) g_2
\]
\[- (g_0h_3 - g_1h_7 - g_2h_3 + g_3h_5 + g_4h_6 + g_5h_2 - g_6h_4 + g_7h_1) g_3
\]
\[- (g_0h_4 + g_1h_2 - g_2h_1 - g_3h_6 + g_4h_0 + g_5h_7 + g_6h_3 - g_7h_5) g_4,
\]
\[- (g_0h_5 - g_1h_6 + g_2h_3 - g_3h_2 - g_4h_7 + g_5h_0 + g_6h_1 + g_7h_4) g_5
\]
\[- (g_0h_6 + g_1h_5 - g_2h_7 + g_3h_4 - g_4h_3 - g_5h_1 + g_6h_0 + g_7h_2) g_6
\]
\[- (g_0h_7 + g_1h_3 + g_2h_6 - g_3h_1 + g_4h_5 - g_5h_4 - g_6h_2 + g_7h_0) g_7
\]

\[= h_1(-g_4g_2 - g_3g_3 + g_2g_4 + g_6g_5 + g_5g_6 + g_3g_7)
\]
\[+ h_2(g_4g_1 + g_5g_3 - g_4g_4 + g_4g_5 - g_4g_6 + g_4g_7)
\]
\[+ h_3(g_7g_1 + g_5g_2 - g_5g_3 - g_2g_4 + g_4g_6 - g_3g_7)
\]
\[+ h_4(-g_2g_1 + g_1g_2 + g_6g_3 - g_5g_5 - g_5g_6 + g_5g_7)
\]
\[+ h_5(g_6g_1 - g_3g_2 + g_2g_3 + g_4g_4 - g_3g_6 - g_3g_7)
\]
\[+ h_6(-g_5g_1 + g_7g_2 - g_4g_3 + g_3g_4 + g_5g_5 - g_3g_7)
\]
\[+ h_7(-g_3g_1 - g_6g_2 + g_1g_3 - g_5g_4 + g_4g_5 + g_2g_6)
\]

\[= 0 \mod q,
\]

\[(GH)G\]_1 \mod q
\]
\[
= (g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7) g_1
\]
\[+ (g_0h_1 + g_1h_0 + g_2h_4 + g_3h_7 - g_4h_2 + g_5h_6 - g_6h_5 - g_7h_3) g_0
\]
\[+ (g_0h_2 - g_1h_4 + g_2h_0 + g_3h_5 + g_4h_1 - g_5h_3 + g_6h_7 - g_7h_6) g_4
\]
\[+ (g_0h_3 - g_1h_7 - g_2h_3 + g_3h_5 + g_4h_6 + g_5h_2 - g_6h_4 + g_7h_1) g_7
\]
\[- (g_0h_4 + g_1h_2 - g_2h_1 - g_3h_6 + g_4h_0 + g_5h_7 + g_6h_3 - g_7h_5) g_2
\]
\[- (g_0h_5 - g_1h_6 + g_2h_3 - g_3h_2 - g_4h_7 + g_5h_0 + g_6h_1 + g_7h_4) g_6
\]
\[- (g_0h_6 + g_1h_5 - g_2h_7 + g_3h_4 - g_4h_3 - g_5h_1 + g_6h_0 + g_7h_2) g_5
\]
- (g_0 h_7 + g_1 h_3 + g_2 h_6 - g_0 h_1 + g_4 h_5 - g_0 h_4 - g_0 h_2 + g_7 h_0) g_3 \\
= 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_2 g_1 - g_4 g_0 + g_0 g_4 + g_5 g_7 g_1 g_2 - g_3 g_5 g_7 g_5 + g_6 g_3) \\
+ h_3 (-g_3 g_1 - g_2 g_0 - g_5 g_4 + g_0 g_7 - g_6 g_2 + g_2 g_6 + g_4 h_5 - g_1 g_3) \\
+ h_4 (-g_4 g_1 + g_2 g_0 - g_1 g_4 + g_6 g_7 g_0 g_2 + g_7 g_6 - g_3 g_5 + g_5 g_3) \\
+ h_5 (-g_5 g_1 - g_6 g_0 + g_3 g_4 + g_2 g_7 + g_7 g_2 + g_0 g_6 - g_1 g_5 - g_4 g_3) \\
+ h_6 (-g_6 g_1 + g_5 g_0 - g_7 g_4 + g_4 g_7 + g_3 g_2 - g_1 g_6 - g_0 g_5 - g_2 g_3) \\
+ h_7 (g_7 g_1 + g_3 g_0 + g_6 g_4 - g_1 g_7 g_5 g_2 - g_4 g_6 + g_2 g_5 - g_0 g_3) \\
= h_1 (-2 g_1^2 + L_G - 2 g_1 (h_2 g_2 + h_3 g_3 + h_4 g_4 + h_5 g_5 + h_6 g_6 + h_7 g_7)) \\
= h_1 (L_G - 2 g_1 (h_1 g_1 + h_2 g_2 + h_3 g_3 + h_4 g_4 + h_5 g_5 + h_6 g_6 + h_7 g_7)) \\
= h_1 L_G \mod q.

In the same manner we have

\[(GH)G = h_i L_G \mod q \quad (i=2, \ldots, 7)\].

Then we have

\[(GH)G = L_G H \mod q.\]

In the same manner we have

\[HG \mod q\]

\[= (h_0 g_0 - h_1 g_1 - h_2 g_2 - h_3 g_3 - h_4 g_4 - h_5 g_5 - h_6 g_6 - h_7 g_7 \mod q,\]

\[h_0 g_1 + h_1 g_0 + h_2 g_4 + h_3 g_7 - h_4 g_2 + h_5 g_6 - h_6 g_5 - h_7 g_3 \mod q,\]

\[h_0 g_2 - h_1 g_4 + h_2 g_0 + h_3 g_5 + h_4 g_1 - h_5 g_3 + h_6 g_7 - h_7 g_6 \mod q,\]

\[h_0 g_3 - h_1 g_7 - h_2 g_5 + h_3 g_0 + h_4 g_6 + h_5 g_2 - h_6 g_4 + h_7 g_1 \mod q,\]

\[h_0 g_4 + h_1 g_2 - h_2 g_1 - h_3 g_6 + h_4 g_0 + h_5 g_7 + h_6 g_5 - h_7 g_5 \mod q,\]

\[h_0 g_5 - h_1 g_6 + h_2 g_3 - h_3 g_2 - h_4 g_7 + h_5 g_0 + h_6 g_1 + h_7 g_4 \mod q,\]

\[h_0 g_6 + h_1 g_5 - h_2 g_7 + h_3 g_4 - h_4 g_3 - h_5 g_1 + h_6 g_0 + h_7 g_2 \mod q,\]

\[h_0 g_7 + h_1 g_3 + h_2 g_6 - h_3 g_1 + h_4 g_5 - h_5 g_4 - h_6 g_2 + h_7 g_0 \mod q).\]
\[(HG)H\]_0

\[
= (h_0 g_0 - h_1 g_1 - h_2 g_2 - h_3 g_3 - h_4 g_4 - h_5 g_5 - h_6 g_6 - h_7 g_7) h_0
- (h_0 g_1 + h_1 g_0 + h_2 g_4 + h_3 g_7 - h_4 g_2 + h_5 g_6 - h_6 g_5 - h_7 g_3) h_1
- (h_0 g_2 - h_1 g_4 + h_2 g_0 + h_3 g_5 + h_4 g_1 - h_5 g_3 + h_6 g_7 - h_7 g_6) h_2
- (h_0 g_3 - h_1 g_7 - h_2 g_5 + h_3 g_0 + h_4 g_6 + h_5 g_2 - h_6 g_4 + h_7 g_1) h_3
- (h_0 g_4 + h_1 g_2 - h_2 g_1 - h_3 g_6 + h_4 g_0 + h_5 g_7 + h_6 g_3 - h_7 g_5) h_4
- (h_0 g_5 - h_1 g_6 + h_2 g_3 - h_3 g_2 - h_4 g_7 + h_5 g_0 + h_6 g_1 + h_7 g_4) h_5
- (h_0 g_6 + h_1 g_5 - h_2 g_7 + h_3 g_4 - h_4 g_3 - h_5 g_1 + h_6 g_0 + h_7 g_2) h_6
- (h_0 g_7 + h_1 g_3 + h_2 g_6 - h_3 g_1 + h_4 g_5 - h_5 g_4 - h_6 g_2 + h_7 g_0) h_7 \mod q
\]

\[= 0 h_0 - g_0 (h_1^2 + h_2^2 + \ldots + h_7^2 +)
+ g_1 (-h_3 h_2 - h_7 h_3 + h_2 h_4 - h_6 h_5 + h_5 h_6 + h_3 h_7)
+ g_2 (h_4 h_1 - h_5 h_5 - h_1 h_4 + h_3 h_5 - h_7 h_6 + h_6 h_7)
+ g_3 (h_7 h_1 + h_5 h_2 - h_6 h_4 + h_2 h_5 + h_4 h_6 - h_1 h_7)
+ g_4 (-h_2 h_1 + h_1 h_2 + h_6 h_3 - h_7 h_5 - h_3 h_6 + h_5 h_7)
+ g_5 (h_8 h_1 - h_3 h_2 + h_2 h_3 + h_7 h_4 - h_1 h_6 - h_4 h_7)
+ g_6 (h_9 h_1 - h_3 h_2 + h_2 h_3 + h_7 h_4 - h_1 h_6 - h_4 h_7)
+ g_7 (-h_5 h_1 + h_7 h_2 - h_4 h_3 + h_3 h_4 + h_1 h_5 - h_2 h_7) \mod q
\]

\[= 0 \mod q.
\]

\[(HG)H\]_1

\[
= (h_0 g_0 - h_1 g_1 - h_2 g_2 - h_3 g_3 - h_4 g_4 - h_5 g_5 - h_6 g_6 - h_7 g_7) h_1
+(h_0 g_1 + h_1 g_0 + h_2 g_4 + h_3 g_7 - h_4 g_2 + h_5 g_6 - h_6 g_5 - h_7 g_3) h_0
+(h_0 g_2 - h_1 g_4 + h_2 g_0 + h_3 g_5 + h_4 g_1 - h_5 g_3 + h_6 g_7 - h_7 g_6) h_4
+(h_0 g_3 - h_1 g_7 - h_2 g_5 + h_3 g_0 + h_4 g_6 + h_5 g_2 - h_6 g_4 + h_7 g_1) h_7
-(h_0 g_4 + h_1 g_2 - h_2 g_1 - h_3 g_6 + h_4 g_0 + h_5 g_7 + h_6 g_3 - h_7 g_5) h_2
+(h_0 g_5 - h_1 g_6 + h_2 g_3 - h_3 g_2 - h_4 g_7 + h_5 g_0 + h_6 g_1 + h_7 g_4) h_6
\]
\(- (h_0g_6 + h_1g_5 - h_2g_7 + h_3g_4 - h_4g_3 - h_5g_1 + h_6g_0 + h_7g_2)h_5 \)
\(- (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 \mod q \]
\[= g_1 (-h_1^2 + h_4^2 + h_7^2 + h_2^2 + h_6^2 + h_5^2 + h_3^2) \]
\[+ g_2 (-h_2 h_1 + h_5 h_7 - h_1 h_2 - h_3 h_6 - h_7 h_5 + h_6 h_3) \]
\[+ g_3(-h_3 h_1 - h_5 h_4 - h_6 h_2 + h_2 h_6 + h_4 h_5 - h_1 h_3) \]
\[+ g_4(-h_4 h_1 - h_1 h_4 - h_6 h_7 + h_7 h_6 - h_3 h_5 + h_5 h_3) \]
\[+ g_5(-h_5 h_1 + h_3 h_4 - h_2 h_7 + h_7 h_2 - h_1 h_5 - h_4 h_3) \]
\[+ g_6(-h_6 h_1 - h_7 h_4 + h_4 h_7 + h_3 h_2 - h_1 h_6 - h_2 h_3) \]
\[+ g_7(-h_7 h_1 + h_4 h_4 - h_1 h_7 h_3 - h_2 - h_3 h_4 h_6 + h_2 h_5) \mod q \]
\[= -2(h_1^2 + g_2 h_1 + g_3 h_1 + g_4 h_1 + g_5 h_1 + g_6 h_1 + g_7 h_1) \mod q \]
\[= -2h_1( h_1 + g_2 h_2 + g_3 h_3 + g_4 h_4 + g_5 h_5 + g_6 h_6 + g_7 h_7) \mod q \]
\[= -2h_10 = 0 \mod q, \]

In the same manner we have

\[[(HG)H] = -2h_10 = 0 \mod q (i=2, \ldots, 7). \]

Then we have

\[(HG)H = 0 \mod q. \]

\[[GH]_0 + [HG]_0 = 0 + 0 = 0 \mod q, \]

\[[HG]_1 + [GH]_1 \]
\[= (h_2g_4 + h_3g_7 - h_4g_2 + h_5g_6 - h_6g_5 - h_7g_3) + (g_2h_4 + g_3h_7 - g_4h_2 + g_5h_6 - g_6h_5 - g_7h_3) \]
\[= 0 \mod q. \]

In the same manner we have

\[[HG]_1 + [GH]_1 = 0 \mod q (i=2, \ldots, 7). \]

Then we have

\[GH + GH = 0 \mod q. \quad \text{q.e.d.} \]