FHPKE based on multivariate discrete logarithm problem

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

Abstract. Previously I proposed fully homomorphic public-key encryption (FHPKE) based on discrete logarithm problem which is vulnerable to quantum computer attacks. In this paper I propose FHPKE based on *multivariate* discrete logarithm assumption. This encryption scheme is thought to withstand to quantum computer attacks. Though I can construct this scheme over many non-commutative rings, I will adopt the FHPKE scheme based on the octonion ring as the typical example for showing how this scheme is constructed. The *multivariate* discrete logarithm problem (MDLP) is defined such that given $f(x)$, $g(x)$, $h(x)$ and a prime q, final goal is to find m_0, m_1, n_0, $n_1 \in \boldsymbol{Fq}^*$ where $h(x)=f$^$m_0(g$^$n_0(x))+f$^$m_1(g$^$n_1(x))$ mod q over octonion ring.

keywords: fully homomorphic public-key encryption, multivariate discrete logarithm problem, octonion ring, post quantum cryptography

§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 public-key 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 public-key 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.

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.

In previous works I proposed fully homomorphic encryptions. But the encryption schemes in some previous works [14, 15, 16, 17, 18, 19, 20] may be vulnerable to “p and - p attack”. And the encryption schemes in other previous works [11, 12, 22, 23] may be vulnerable to quantum computer attacks.

In this paper I propose FHPKE based on *multivariate* discrete logarithm assumption which is thought to withstand to quantum computer attacks and “p and - p attack”. Though I can construct this scheme over many non- commutative rings, I will adopt the FHPKE scheme based on the octonion ring as the typical example for showing how this scheme is constructed. The *multivariate* discrete logarithm problem (MDLP) is defined such that given $f(x)$, $g(x)$, $h(x)$ and a prime q, final goal is to find m_0, m_1, n_0, $n_1 \in \boldsymbol{Fq^*}$ where $h(x)=f^{m0}(g^{n0}(x))+f^{m1}(g^{n1}(x))$ mod q over octonion ring.

In this scheme I describe fully homomorphic public-key encryption (FHPKE) with the recursive ciphertex. A ciphertext consists of three sub-ciphertexts corresponding to one plaintext. When we execute the additional operation or multiplicative operation, a new three sub-ciphertexts are generated from the three sub-ciphertexts recursively without revealing the plaintexts.

§2. Related works

The utility of fully homomorphic encryption has been long recognized. The problem of constructing such a scheme was first proposed within a year of the development of RSA [4]. For more than 30 years, it was unclear whether fully homomorphic encryption was even possible. During this period, the best result was the Boneh-Goh-Nissim cryptosystem which supports evaluation of an unlimited number of addition operations but at most one multiplication.

Craig Gentry [1] using lattice-based cryptography showed the first fully homomorphic encryption scheme as announced by IBM on June 25, 2009 [5, 6].

Gentry's Ph.D. thesis [7] provides additional details. Gentry also published a high-level overview of the van Dijk et al. construction [8].

In 2009, Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan presented a second fully homomorphic encryption scheme [9] , which uses many of the tools of Gentry's construction, but which does not require ideal lattices. Instead, they show that the somewhat homomorphic component of Gentry's ideal lattice-based scheme can be replaced with a very simple somewhat homomorphic scheme that uses integers. The scheme is therefore conceptually simpler than Gentry's ideal lattice scheme, but has similar properties with regards to homomorphic operations and efficiency. The somewhat homomorphic component in the work of van Dijk et al. is similar to an encryption scheme proposed by Levieil and Naccache in 2008, and also to one that was proposed by Bram Cohen in 1998 [10]. Cohen's method is not even additively homomorphic, however. The

Levieil-Naccache scheme is additively homomorphic, and can be modified to support also a small number of multiplications.

In 2010, Nigel P. Smart and Frederik Vercauteren presented a refinement of Gentry's scheme giving smaller key and ciphertext sizes, but which is still not fully practical. At the rump session of Eurocrypt 2010, Craig Gentry and Shai Halevi presented a working implementation of fully homomorphic encryption (i.e. the entire bootstrapping procedure) together with performance numbers. In 2014, Nuida and Kurosawa proposed (batch) fully homomorphic encryption over integers [13].

§3. Basic concept on FHPKE in this scheme

Here I describe the basic concept on the method for constructing this fully homomorphic public-key encryption over the non-commutative ring.

Let $\mathcal{R}$ be non-associative and non-commutative ring.

Let q be an odd prime.

1)We adopt $\mathrm{F}(X), \mathrm{G}(X) \in \mathcal{R}[X]$ and q as system parameters.

2)Let $h_{\mathrm{A}}(X) \in \mathcal{R}[X]$ be the public-key and m_{A0}, m_{A1},n_{A0} $n_{\mathrm{A1}} \in \boldsymbol{Fq^*}$ be the secret keys of user A.

where $h_{\mathrm{A}}(X) := f^{mA0}(g^{nA0}(x)) + f^{mA1}(g^{nA1}(x)) \bmod q \in \mathcal{R}[X]$.

3)Let $h_{\mathrm{B}}(X) \in \mathcal{R}[X]$ be the public-key and m_{B0}, m_{B1}, n_{B0}, $n_{\mathrm{B1}} \in \boldsymbol{Fq^*}$ be the secret keys of user B.

where $h_{\mathrm{B}}(X) := f^{mB0}(g^{nB0}(x)) + f^{mB1}(g^{nB1}(x)) \bmod q \in \mathcal{R}[X]$.

4)User A generates the common encryption key $\mathrm{F}_{\mathrm{AB}}(X,Y)$ between user A and user B as follows.

$\mathrm{E}_{\mathrm{AB}}(X) := f^{mA0}(h_{\mathrm{B}}(g^{nA0}(x))) + f^{mA1}(h_{\mathrm{B}}(g^{nA1}(x)))$

$= f^{mA0}(f^{mB0}(g^{nB0}(g^{nA0}(x)))) + f^{mA0}(f^{mB1}(g^{nB1}(g^{nA0}(x))))$

$+ f^{mA1}(f^{mB0}(g^{nB0}(g^{nA1}(x)))) + f^{mA1}(f^{mB1}(g^{nB1}(g^{nA1}(x))) \bmod q \in \mathcal{R}[X]$.

$= f^{mA0+mB0}(g^{nB0+nA0}(x)) + f^{mA0+ mB1}(g^{nB1+nA0}(x))$

$+ f^{mA1+mB0}(g^{nB0+nA1}(x)) + f^{mA1+ mB1}(g^{nB1+nA1}(x))) \bmod q \in \mathcal{R}[X]$

$\mathrm{F}_{\mathrm{AB}}(X,Y) := \mathrm{E}_{\mathrm{AB}}{}^{-1}(Y(\mathrm{E}_{\mathrm{AB}}(X))) \in \mathcal{R}[X,Y]$.

In the same manner user B generates the common encryption key $\mathrm{F}_{\mathrm{BA}}(X)$ between user B and user A such that

5)$\mathrm{E}_{\mathrm{BA}}(X) := f^{mB0+mA0}(g^{nA+nB0}(x)) + f^{mB0+ mA1}(g^{nA1+nB0}(x))$

$+ f^{mB1+mA0}(g^{nA0+nB1}(x)) + f^{mB1+ mA1}(g^{nA1+nB1}(x))) \bmod q \in \mathcal{R}[X]$,

$\mathrm{F}_{\mathrm{BA}}(X,Y) := \mathrm{E}_{\mathrm{BA}}{}^{-1}(Y(\mathrm{E}_{\mathrm{BA}}(X))) = \mathrm{F}_{\mathrm{AB}}(X,Y) \in \mathcal{R}[X,Y]$.

6)Let $M \in \mathcal{R}$ be the plaintext.

7)User A generates the ciphertext $\mathrm{C}(X)$ such that

$C(X):= F_{AB}(M,X):= E_{AB}^{-1}(M(E_{AB}(X)))\in\mathcal{R}[X]$.

8)User B deciphers the ciphertext to obtain the plaintext *M*.

$E_{BA}(C(E_{BA}^{-1}(\mathbf{1})))= E_{BA}(E_{AB}^{-1}(M(E_{AB}(E_{BA}^{-1}(\mathbf{1}))))) =M\mathbf{1}=M\in\mathcal{R}$**.**

We notice that we need to structure the plaintext *M* so that the ciphertext C has the fully homomorphic property.

Though I can construct this scheme over many non-commutative rings, I adopt the FHPKE scheme based on the octonion ring as an example. In this paper I will show by using this example how this scheme is constructed.

§4. Preliminaries for octonion operations

In this section we describe the operations on octonion ring and properties of octonion ring. The readers who understand the property of octonion may skip the section 4.

§4.1 Multiplication and addition on the octonion ring *O*

Let q be a prime modulus to be as large as 2^{256} where q is a prime. Later (in section 8) we discuss the size of q, one of the system parameters.

Let O be the octonion [2] ring over a finite field $R=\mathbf{Z}/q\mathbf{Z}$ such that

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

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

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

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

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

$$A+B \bmod q$$

$$=(a_0+b_0 \bmod q,\ a_1+b_1 \bmod q,\ a_2+b_2 \bmod q,\ a_3+b_3 \bmod q\ ,$$

$$a_4+b_4 \bmod q,\ a_5+b_5 \bmod q,\ a_6+b_6 \bmod q,\ a_7+b_7 \bmod q\ ). \qquad (5)$$

Let

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

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

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

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

§4.2 Order of the element in *O*

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

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

Theorem 1

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

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

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

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

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

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

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

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

(*Proof*:)

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

Theorem 2

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

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

where

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

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

(*Proof*:)

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

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

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

where

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

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

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

1) Non-commutative

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

2) Non-associative

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

3) Alternative

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

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

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

4) Moufang's formulae [2],

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

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

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

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

5) **Lemma 1**

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

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

(*Proof*:)

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

Theorem 3

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

where

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

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

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

(*Proof*:)

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

where

$$L_{\mathrm{A}}= a_0^2+a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2 \bmod q.$$

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

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

$$A^2= (2a_0^2\text{-}\ L_A \bmod q,\ 2a_0a_1 \bmod q,\ 2a_0a_2 \bmod q,\ 2a_0a_3 \bmod q,$$

$$2a_0a_4 \bmod q,\ 2\ a_0a_5 \bmod q,\ 2a_0a_6 \bmod q,\ 2a_0a_7 \bmod q).$$

Then we have

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

$$w=\text{-}\ L_A \bmod q,$$

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

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

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

§5.1 Definition of homomorphic public-key encryption

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

In this work, the plaintext $p \in R(=\boldsymbol{Z}/q\boldsymbol{Z})$ of the encryption schemes will be the element in finite field, and the functions to be evaluated will be represented as arithmetic circuits over this field, composed of addition and multiplication gates. The syntax of these algorithms is given as follows.

-Key-Generation. The algorithm **KeyGen**, on input the security parameter 1^λ, system parameters $(q,G,H;f(X), g(X))$ where q is a large prime, outputs (**pk**, **sk**) ← **KeyGen**$(1^\lambda,q)$, where **pk** is a public key and **sk** is a secret key.

-Encryption. The algorithm **Enc**, on input system parameters $(q,G,H;f(X), g(X))$, public-key **pk**, and a plaintext $p \in R$, components of plaintext $u,v \in R$, random noises $w,z \in R$, outputs a ciphertext $C=({}^1C, {}^2C, {}^3C) \in \{O[X]\}^3$ ←**Enc**(**pk**; p) where $f(X), g(X) \in O[X]$.

-Decryption. The algorithm **Dec**, on input system parameters $(q,G,H;f(X), g(X))$, secret key **sk** and a ciphertext $C=({}^1C, {}^2C, {}^3C) \in \{O[X]\}^3$, outputs a plaintext p^*←**Dec**(**sk**;C).

-Homomorphic-Evaluation. The algorithm **Eval**, on input system parameters $(q,G,H;f(X), g(X))$, an arithmetic circuit ckt, and a tuple of $3 \times n$ ciphertexts $(C_1,\ldots, C_n) \in \{O[X]\}^{3\times n}$, outputs a ciphertext $C'=({}^1C',{}^2C'\ ,{}^3C') \in \{O[X]\}^3$←**Eval**(ckt; $C_1,\ldots, C_n$).

§5.2 Definition of fully homomorphic public-key encryption

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

Definition (**Fully homomorphic public-key encryption**). A homomorphic public-key encryption scheme FHPKE :=(**KeyGen; Enc; Dec; Eval**) is fully homomorphic if it satisfies the following properties:

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

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

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

§5.3 Basic function

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

Let q be a prime modulus selected by system centre.

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

Let $g(X)$ and $f(X)$ be the basic functions.

Basic functions $g(X)$ and $f(X)$ are defined as follows.

$$\begin{aligned}
&g(X)\in O[X],\\
&:=(g_{00}x_0+g_{01}x_1+\ldots+g_{07}x_7,\\
&\quad g_{10}x_0+g_{11}x_1+\ldots+g_{17}x_7,\\
&\quad \ldots. \qquad \ldots.\\
&\quad g_{70}x_0+g_{71}x_1+\ldots+g_{77}x_7) \bmod q,\\
&=\{g_{ij}\}\ (i,j=0,\ldots,7)
\end{aligned}$$

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

Let $\mathbf{G}\in R^{8\times 8}$ be the matrix (g_{ij}).

We select **G** such that the characteristic equation CH$_g$(t)=0 mod q of **G** is irreducible, and the solutions of $\mathrm{CH}_g(t)=0 \bmod q$, $\eta_0, \eta_1, \ldots, \eta_6$ and η_7 are different each other.

$\mathrm{CH}_g(t)$ is equal to the minimal polynomial of η_i ($i=0,\ldots,7$) because the minimal polynomial of η_i ($i=0,\ldots,7$) divides $\mathrm{CH}_g(t)$ from Cayley-Hamilton theorem .

$$
\begin{aligned}
& f(X) \in O[X] , \\
& :=(f_{00}x_0+f_{01}x_1+ \ldots +f_{07}x_7, \\
& \quad f_{10}x_0+f_{11}x_1+ \ldots +f_{17}x_7, \\
& \quad \ldots. \qquad \ldots. \\
& \quad f_{70}x_0+f_{71}x_1+ \ldots +f_{77}x_7) \bmod q, \\
& =\{f_{ij}\} \ (i,j=0,\ldots,7)
\end{aligned}
$$

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

Let $\mathbf{F} \in R^{8\times 8}$ be the matrix (f_{ij}).

We select $\mathbf{F}$ such that the characteristic equation $\mathrm{CH}_f(t)=0 \bmod q$ of $\mathbf{F}$ is irreducible,

$\mathrm{CH}_f(t) \neq \mathrm{CH}_g(t) \bmod q$, and the solutions of $\mathrm{CH}_f(t)=0 \bmod q$, $\zeta_0, \zeta_1, \ldots, \zeta_7$ are different each other.

$\mathrm{CH}_f(t)$ is equal to the minimal polynomial of ζ_i ($i=0,\ldots,7$) because the minimal polynomial of ζ_i ($i=0,\ldots,7$) divides $\mathrm{CH}_f(t)$ from Cayley-Hamilton theorem.

Theorem 4

Let $\mathrm{CH}_g(t)$ be the characteristic equation of $\mathbf{G}$ to be irreducible over R.

Let $\eta_0, \eta_1, \ldots, \eta_6$ and η_7 be different solutions of $\mathrm{CH}_g(t)=0 \bmod q$.

Let $\mathrm{CH}_f(t)$ be the characteristic equation of $\mathbf{F}$ to be irreducible over R.

Let $\zeta_0, \zeta_1, \ldots, \zeta_6$ and ζ_7 be different solutions of $\mathrm{CH}_f(t)=0 \bmod q$.

There does not exist the integer k such that $\zeta_i=\eta_j{}^k \bmod q$ ($i,j \in \{0,1,\ldots,7\}$) .

(*Proof:*)

If

$\zeta_i=\eta_j{}^k \bmod q$ ($i,j \in \{0,1,\ldots,7\}$) ,

then

η_i satisfies the equation of degree 7, $\mathrm{CH}_f(\eta_i{}^k)=0 \bmod q$ because $\eta_j{}^8$ is given as the polynomial of degree

7 of η_j from $\mathrm{CH}_g(\eta_j)=0 \bmod q$.

It is contradictory to that the minimal polynomial of η_i is $\mathrm{CH}_g(t)=0$ of degree 8.   q.e.d.

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

$$\begin{aligned}
&g^{-1}(X)\in O[X]\ ,\\
&:=(g'_{00}x_0+ \ldots +g'_{07}x_7,\\
&\quad g'_{10}x_0+\ldots+g'_{17}x_7,\\
&\quad \ldots. \quad \ldots.\\
&\quad g'_{70}x_0+ \ldots +g'_{77}x_7) \bmod q,\\
&=\{g'_{ij}\}(i,j=0,\ldots,7)
\end{aligned}$$

with $g'_{ij}\in \boldsymbol{R}$ $(i,j=0,\ldots,7)$.

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

[**ALINVF**]

Given $g(X)$ and q,

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

Then we obtain

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

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

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

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

....

....

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

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

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

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

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

....

$g^{i}(X):=g(g^{i-1}(X)) \bmod q$;

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

....

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

$$g^{-2}(X):=g^{-1}(g^{-1}(X)) \bmod q,$$

....

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

$$f^{-2}(X):=f^{-1}(f^{-1}(X)) \bmod q,$$

....

$$f^{-i}(X):=f^{-1}(f^{-(i-1)}(X)) \bmod q.$$

We can define $g^{0}(X)=X$ and $f^{0}(X)=X$.

§6. Fully homomorphic public-key encryption scheme

§6.1 Public-key enciphering function

The system centre publishes the system parameters $(q, G, H; f(X), g(X))$.(G and H are defined later in this section.)

We consider the communication between user A and user B. User A downloads the system parameters $(q, G, H; f(X),g(X))$ from system centre. User A selects the random integers m_{a0}, m_{a1},n_{a0}, $n_{a1}\in \boldsymbol{Fq}^*$ to be secret and generates the functions $f^{m_{ai}}(X)$ and $g^{n_{ai}}(X)$ by using algorithm **Power**($f(X)$, m_{ai}, q) and **Power**($g(X)$, n_{ai}, q) (i=0,1). (see the **Appendix F**). User A generates the public function $h_a(X)$

$$h_a(X)=f^{m_{a0}}(g^{n_{a0}}(X)) + f^{m_{a1}}(g^{n_{a1}}(X)) \bmod q=\{\, h_{aij} \,\}_{(i,j=0,\ldots,7)}$$

by using $f^{m_{a0}}(X)$, $g^{n_{a0}}(X)$, $f^{m_{a1}}(X)$ and $g^{n_{a1}}(X)$. User A sends the coefficient of $h_a(X)$, $h_{aij}\in R$ (i,j =0,…,7) to system centre that is a part of the public-key of user A.

On the other hand user B downloads the system parameters $(q, G, H; f(X),g(X))$ and selects the random integers m_{b0}, m_{b1},n_{b0}, $n_{b1}\in \boldsymbol{Fq}^*$ to be secret and generates the function $f^{m_{bi}}(X)$ and $g^{n_{bi}}(X)$ by using algorithm **Power**($f(X)$, m_{bi}, q) and **Power**($g(X)$, n_{bi}, q) (i=0,1). User B generates the public function

$$h_b(X) = f^{m_{b0}}(g^{n_{b0}}(X))) + f^{m_{b1}}(g^{n_{b1}}(X))) \bmod q=\{\, h_{bij} \,\}(i,j=0,\ldots,7)$$

by using $f^{m_{b0}}(X)$, $g^{n_{b0}}(X)$, $f^{m_{b1}}(X)$ and $g^{n_{b1}}(X)$. User B sends the coefficient of $h_b(X)$, $h_{bij}\in R$ (i,j =0,…,7) to system centre that is a part of the public-key of user B.

User B tries to send to user A the ciphertexts of the plaintexts which user B possesses. User B downloads the public-key of user A, $h_a(X)$,that is, $h_{aij} \in R$ $(i,j=0,\ldots,7)$ from system centre.

User B calculates $E_{ba}(X)$ by using $h_a(X)$,$f^{mb0}(X)$, $g^{nb0}(X)$,$f^{mb1}(X)$ and $g^{nb1}(X)$ such that

$$E_{ba}(X):=f^{nb0}(h_a(g^{nb0}(X))+f^{nb1}(h_a(g^{nb1}(X))$$

$$=f^{mb0}(f^{ma0}(g^{na0}(g^{nb0}(X)))) + f^{mb0}(f^{ma1}(g^{na1}(g^{nb0}(X))))$$

$$+ f^{mb1}(f^{ma0}(g^{na0}(g^{nb1}(X)))) + f^{mb1}(f^{ma1}(g^{na1}(g^{nb1}(X))))$$

$$= f^{mb0+ma0}(g^{na0+nb0}(X)) + f^{mb0+ma1}(g^{na1+nb0}(X)) + f^{mb1+ma0}(g^{na0+nb1}(X)) + f^{mb1+ma1}(g^{na1+nb1}(X)) \bmod q.$$

User B calculates $E_{ba}{}^{-1}(X)$ from $E_{ba}(X)$ by using **ALINVF**.

User B generates the common enciphering function $F_{\mathrm{BA}}(X,Y)$ between user B and user A such that

$$F_{\mathrm{BA}}(X,Y):= E_{ba}{}^{-1}(YE_{ba}(X)) \bmod q \in O[X,Y].$$

In the same manner user A generates the common enciphering function

$$F_{\mathrm{AB}}(X,Y):= E_{ab}{}^{-1}(YE_{ab}(X)) \bmod q \in O[X,Y]$$

where

$$F_{\mathrm{BA}}(X,Y)= F_{\mathrm{AB}}(X,Y) \bmod q.$$

We notice that

$$F_{\mathrm{BA}}(X,\mathbf{1}) = E_{ba}{}^{-1}(\mathbf{1}E_{ba}(X)) = E_{ba}{}^{-1}(E_{ba}(X)) = X \bmod q.$$

User B confirms the system parameters $(q, G, H; f(X), g(X))$ downloaded from the system centre where

$$G=(g_0,g_1,g_2,\ldots,g_7) \in O\,,$$

$$GCD\,(g_0(g_0\text{-}2), q)=1,$$

$$H=(h_0,h_1,h_2,\ldots,h_7) \in O,$$

$$L_G:=|G|^2= g_0{}^2+g_1{}^2+\ldots+g_7{}^2=0 \bmod q,$$

$$L_H:=|H|^2= h_0{}^2+h_1{}^2+\ldots+h_7{}^2=0 \bmod q,$$

$$h_0=0 \bmod q,$$

$$g_1h_1+\ldots+g_7h_7=0 \bmod q.$$

From Theorem 3 we have

$$G^2 = -L_G\mathbf{1} + 2\, g_0 G = 2 g_0 G \bmod q,$$

$$H^2 = -L_H\mathbf{1} + 2\, h_0 H = \mathbf{0} \bmod q,$$

$$[GH]_0 = [HG]_0 = g_0 h_0 - (\, g_1 h_1 + \ldots + g_7 h_7) = 0 \bmod q, \tag{18}$$

$$L_{GH} = L_G L_H = L_{HG} = 0 \bmod q,$$

$$(GH)^2 = -L_{GH}\mathbf{1} + 2\,[GH]_0 GH = 0\mathbf{1} + 0GH = \mathbf{0} \bmod q,$$

$$(HG)^2 = -L_{HG}\mathbf{1} + 2\,[HG]_0 HG = \mathbf{0} \bmod q.$$

Theorem 5

$$(GH)G = \mathbf{0} \bmod q, \tag{19a}$$

$$(HG)H = \mathbf{0} \bmod q. \tag{19b}$$

(*Proof*:)

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

Theorem 6

$$GH + HG = 2 g_0 H \bmod q. \tag{20}$$

(*Proof*:)

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

Theorem 7

$$(GH)(HG) = \mathbf{0} \bmod q, \tag{21a}$$

$$(HG)(GH) = \mathbf{0} \bmod q. \tag{21b}$$

(*Proof*:)

From (17)

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

$$(HG)(GH) = (H(GG))H = 2g_0\, (H(G))H = \mathbf{0} \bmod q. \qquad \text{q.e.d.}$$

§6.2 Medium text

Here user B calculates the medium text ${}^1M$, ${}^2M$ and ${}^3M$ from the plaintext p which user B possesses as follows.

Let $p \in R$ be a plaintext.

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

$p := su + tv \bmod q$ where $s, t \in R$ are secret parameters such that

$GCD(s,q)=1$ and $GCD(t,q)=1$.

Let ${}^iw, {}^iz \in R$ (i=1,2,3) be random noises.

Three medium texts ${}^1M$, ${}^2M$ and ${}^3M$ corresponding to one plaintext p are defined by

$${}^1M := {}^1ku\,\mathbf{1} + {}^1lvG + {}^1wGH + {}^1zHG \bmod q \in O,$$

$${}^2M := {}^2ku\,\mathbf{1} + {}^2lvG + {}^2wGH + {}^2zHG \bmod q \in O,$$

$${}^3M := {}^3ku\,\mathbf{1} + {}^3lvG + {}^3wGH + {}^3zHG \bmod q \in O,$$

$GCD({}^ik, q)=1$ and $GCD({}^il, q)=1$ (i=1,2,3),

$p := su + tv \bmod q \in R$

$= \alpha[{}^1M]_0 + \beta[{}^2M]_0 \bmod q,$

where α and $\beta \in R$ satisfy the following equation,

$\alpha({}^1ku + {}^1lvg_0) + \beta({}^2ku + {}^2lvg_0)$

$= (\alpha\,{}^1k + \beta\,{}^2k)u + (\alpha\,{}^1lg_0 + \beta\,{}^2lg_0)v$

$= su + tv = p \bmod q,$

where ${}^1k, {}^2k$, ${}^1l$ and ${}^2l$ satisfy

$$GCD({}^1k\,{}^2l - {}^2k\,{}^1l, q) = 1 \bmod q. \tag{22a}$$

Then relation between s, t and α, β is as follows.

$$(\alpha\,{}^1k + \beta\,{}^2k) = s \bmod q, \tag{22b}$$

$$(\alpha\,{}^1lg_0 + \beta\,{}^2lg_0) = t \bmod q. \tag{22c}$$

α, β are published as a part of the user's public-key while $s, t, {}^1k, {}^2k, {}^3k, {}^1l, {}^2l, {}^3l$ are secret.

As

$$G^2=2g_0G \bmod q \quad, \quad G(GH)= 2g_0\, GH \bmod q \quad, \quad G(HG)=\mathbf{0} \bmod q,$$

$$(GH)\, G=\mathbf{0} \bmod q \quad, \quad (GH)^2=\mathbf{0} \bmod q \quad, \quad (GH)(\,HG)=\mathbf{0} \bmod q,$$

$$(HG)G=2g_0HG \bmod q, \quad (HG)(GH)=\mathbf{0} \bmod q \quad, \quad (HG)^2=\mathbf{0} \bmod q,$$

we have

$$({}^1M\,)^2=({}^1ku\;\mathbf{1}+{}^1lvG+{}^1wGH+{}^1zHG)\;({}^1ku\;\mathbf{1}+{}^1lvG+{}^1wGH+{}^1zHG) \bmod r$$

$$=({}^1k)^2u^2\mathbf{1}+(2\,{}^1ku\,{}^1lv+2g_0\,({}^1lv)^2)G+(2\,{}^1ku\,{}^1w+2g_0\,{}^1lv\;{}^1lw\,)GH+(2\,{}^1ku\,{}^1z+2g_0\,{}^1z\,{}^1lv)HG \bmod q$$

$$=-(({}^1k)^2u^2+2\,g_0\,({}^1lv)\,({}^1ku\,))\mathbf{1}+2\,({}^1ku+g_0\,({}^1lv))\,({}^1ku\;\mathbf{1}+{}^1lvG+{}^1wGH+{}^1zHG) \bmod q$$

$$=-({}^1ku+2\,g_0\,({}^1lv)\,)({}^1ku\,))\mathbf{1}+2\,({}^1ku+g_0\,({}^1lv))\,{}^1M \bmod q$$

$$=-({}^1ku+2\,g_0\,({}^1lv)\,)({}^1ku\,))\mathbf{1}+2[{}^1M]_0\,{}^1M \bmod q.$$

On the other hand from Theorem 3

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

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

$$L_{1M}=|{}^1M|^2=|\,{}^1ku\;\mathbf{1}+{}^1lvG+{}^1wGH+{}^1zHG|^2=({}^1ku+2\,g_0\,({}^1lv)\,)({}^1ku\,) \bmod q. \tag{23a}$$

In the same manner we have

$$L_{2M}=|{}^2M|^2=|{}^2ku\;\mathbf{1}+{}^2lvG+{}^2wGH+{}^2zHG\,|^2=({}^2ku+2\,g_0\,({}^2lv)\,)({}^2ku\,) \bmod q. \tag{23b}$$

$$L_{3M}=|{}^3M|^2=|{}^3ku\;\mathbf{1}+{}^3lvG+{}^3wGH+{}^3zHG\,|^2=({}^3ku+2\,g_0\,({}^3lv)\,)({}^3ku\,) \bmod q. \tag{23c}$$

Theorem 8 (linear independence between 1, *G*, *GH* and *HG*)

If

$${}^1M:=\,{}^1ku\;\mathbf{1}+{}^1lvG+{}^1wGH+{}^1zHG=\mathbf{0} \bmod q,$$

then

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

(*Proof*)

As $[G]_0=g_0 \bmod q$,$[GH]_0=0 \bmod q$ and $[HG]_0=0 \bmod q$,

$$[{}^1M\,G]_0={}^1kg_0u+2\,{}^1l\,g_0v=0 \bmod q,$$

$$[{}^1M\,]_0={}^1ku+{}^1l\,g_0v=0 \bmod q.$$

As $GCD({}^1kg_0\,{}^1lg_0-{}^1k2\,{}^1lg_0,q)=GCD(\,{}^1k\,{}^1l\,g_0(g_0-2),q)=1$,

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

We have

$${}^1wGH+{}^1zHG=\mathbf{0} \bmod q.$$

By multiply G from right side from Theorem 5

$${}^1w(GH)G+{}^1zHGG=\mathbf{0}G \bmod q,$$

$${}^1w\mathbf{0}+{}^1z2g_0HG=\mathbf{0} \bmod q.$$

We have

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

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

In the same manner

if

$${}^2M={}^2ku\ \mathbf{1}+{}^2lvG+{}^2wGH+{}^2zHG \bmod q=\mathbf{0}\in O,$$

$${}^3M={}^3ku\ \mathbf{1}+{}^3lvG+{}^3wGH+{}^3zHG \bmod q=\mathbf{0}\in O,$$

then

$$u=v={}^iw={}^iz=0 \bmod q \text{ (i=2,3)}.$$

(Associativity of medium texts)

Let

$${}^1M_1:={}^1ku_1\ \mathbf{1}+{}^1lv_1G+{}^1w_1GH+{}^1z_1HG \bmod q\in O,$$

$${}^1M_2:={}^1ku_2\ \mathbf{1}+{}^1lv_2G+{}^1w_2GH+{}^1z_2HG \bmod q\in O,$$

$${}^1M_3:={}^1ku_3\ \mathbf{1}+{}^1lv_3G+{}^1w_3GH+{}^1z_3HG \bmod q\in O.$$

Then we have

$${}^1M_1{}^1M_2=({}^1ku_1\ \mathbf{1}+{}^1lv_1G+{}^1w_1GH+{}^1z_1HG)({}^1ku_2\ \mathbf{1}+{}^1lv_2G+{}^1w_2GH+{}^1z_2HG) \bmod q$$

$$=({}^1k)^2\ u_1u_2\mathbf{1}+({}^1ku_1{}^1lv_2+{}^1lv_1{}^1ku_2+2g_0{}^1lv_1{}^1lv_2)G+$$

$$({}^1ku_1\ {}^1w_2+{}^1w_1{}^1ku_2+2g_0{}^1lv_1{}^1w_2\ )GH+(\ {}^1ku_1{}^1z_2+{}^1z_1{}^1ku_2+2g_0{}^1z_1{}^1lv_2)HG \bmod q.$$

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

$= [({}^1k)^2\, u_1u_2\mathbf{1}+({}^1ku_1{}^1lv_2 +{}^1lv_1{}^1ku_2 +2g_0{}^1lv_1{}^1lv_2)G+$

$({}^1ku_1\,{}^1w_2+{}^1w_1{}^1ku_2+2g_0{}^1lv_1{}^1w_2\,)GH +(\,{}^1ku_1{}^1z_2+{}^1z_1{}^1ku_2+2g_0{}^1z_1{}^1lv_2)HG]$

$(\,{}^1ku_3\,\mathbf{1}+{}^1lv_3G+{}^1w_3GH+{}^1z_3HG) \bmod q$

$=(({}^1k)^3u_1u_2u_3)\mathbf{1}$

$+[({}^1k)^2u_1u_2{}^1lv_3+({}^1ku_1{}^1lv_2+{}^1lv_1{}^1ku_2+2g_0{}^1lv_1{}^1lv_2){}^1ku_3+2g_0({}^1ku_1{}^1lv_2 +{}^1lv_1{}^1ku_2 +2g_0{}^1lv_1{}^1lv_2)\,{}^1lv_3]G$

$+[({}^1k)^2u_1u_2{}^1w_3+({}^1ku_1{}^1w_2+{}^1w_1{}^1ku_2+2g_0{}^1lv_1{}^1w_2){}^1ku_3+2g_0({}^1ku_1{}^1lv_2+{}^1lv_1{}^1ku_2+2g_0{}^1lv_1{}^1lv_2)\,{}^1w_3]GH$

$+[({}^1k)^2\, u_1u_2{}^1z_3+(\,{}^1ku_1{}^1z_2+{}^1z_1{}^1ku_2+2g_0{}^1z_1{}^1lv_2)\,{}^1ku_3 +2g_0({}^1ku_1{}^1z_2+{}^1z_1{}^1ku_2+2g_0{}^1z_1{}^1lv_2)\,{}^1lv_3]HG$

$=(({}^1k)^3u_1u_2u_3)\mathbf{1}$

$+[({}^1k)^2\,({}^1l)\,(u_1u_2v_3+u_1v_2u_3+v_1u_2\,u_3)+2g_0({}^1k\,)({}^1l)^2(v_1v_2u_3+u_1v_2\,v_3 +v_1u_2\,v_3) +(2g_0)^2\,({}^1l)^3v_1v_2v_3]G$

$+[({}^1k)^2\,u_1u_2{}^1w_3+({}^1ku_1{}^1w_2+{}^1w_1{}^1ku_2+2g_0{}^1lv_1{}^1w_2){}^1ku_3+2g_0({}^1ku_1{}^1lv_2+{}^1lv_1{}^1ku_2+2g_0{}^1lv_1{}^1lv_2)\,{}^1w_3]GH$

$+[({}^1k)^2\, u_1u_2{}^1z_3+({}^1ku_1{}^1z_2+{}^1z_1{}^1ku_2+2g_0{}^1z_1{}^1lv_2){}^1ku_3+2g_0({}^1ku_1{}^1z_2+{}^1z_1{}^1ku_2+2g_0{}^1z_1{}^1lv_2){}^1lv_3]HG \bmod q.$

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

$= ({}^1ku_1\,\mathbf{1}+{}^1lv_1A+{}^1w_1GH+{}^1z_1HG)\,[({}^1k)^2\, u_2u_3\mathbf{1}+({}^1ku_2{}^1lv_3 +{}^1lv_2{}^1ku_3 +2g_0{}^1lv_2{}^1lv_3)G+$

$({}^1ku_2{}^1w_3+{}^1w_2{}^1ku_3+2g_0{}^1lv_2{}^1w_3)GH +(\,{}^1ku_2{}^1z_3+{}^1z_2{}^1ku_3+2g_0{}^1z_2{}^1lv_3)HG]\bmod q$

$=(({}^1k)^3u_1u_2u_3)\mathbf{1}$

$+[{}^1ku_1({}^1ku_2{}^1lv_3 +{}^1lv_2{}^1ku_3 +2g_0{}^1lv_2{}^1lv_3)+{}^1lv_1({}^1k)^2\, u_2u_3$

$+(2g_0)\,{}^1lv_1\,({}^1ku_2{}^1lv_3 +{}^1lv_2{}^1ku_3 +2g_0{}^1lv_2{}^1lv_3)]G$

$+[{}^1ku_1({}^1ku_2{}^1w_3+{}^1w_2{}^1ku_3+2g_0{}^1lv_2{}^1w_3)+ 2g_0\,{}^1lv_1({}^1ku_2{}^1w_3+{}^1w_2{}^1ku_3+2g_0{}^1lv_2{}^1w_3)+\,{}^1w_1({}^1k)^2\, u_2u_3]GH$

$+[{}^1ku_1(\,{}^1ku_2{}^1z_3+{}^1z_2{}^1ku_3+2g_0{}^1z_2{}^1lv_3)+\,{}^1z_1({}^1k)^2\, u_2u_3+2g_0{}^1z_1({}^1ku_2{}^1lv_3 +{}^1lv_2{}^1ku_3 +2g_0{}^1lv_2{}^1lv_3)]HG$

$=(({}^1k)^3u_1u_2u_3)\mathbf{1}$

$+[({}^1k)^2({}^1l)\,(u_1u_2v_3+u_1v_2u_3+v_1u_2\,u_3)+2g_0({}^1k)(\,{}^1l)^2(v_1v_2u_3+u_1v_2\,v_3 +v_1u_2\,v_3) +(2g_0)^2({}^1l)^3v_1v_2v_3]G$

$+[({}^1k)^2u_1u_2{}^1w_3+({}^1ku_1{}^1w_2+{}^1w_1{}^1ku_2+2g_0{}^1lv_1{}^1w_2){}^1ku_3+2g_0({}^1ku_1{}^1lv_2+{}^1lv_1{}^1ku_2+2g_0{}^1lv_1{}^1lv_2)\,{}^1w_3]GH$

$+[({}^1k)^2\, u_1u_2{}^1z_3+({}^1ku_1{}^1z_2+{}^1z_1{}^1ku_2+2g_0{}^1z_1{}^1lv_2){}^1ku_3+2g_0({}^1ku_1{}^1z_2+{}^1z_1{}^1ku_2+2g_0{}^1z_1{}^1lv_2){}^1lv_3]HG \bmod q.$

Then we have

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

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

In the same manner we have

$$({}^iM_1{}^iM_2){}^iM_3={}^iM_1({}^iM_2{}^iM_3) \bmod q, \mathrm{i}=2,3.\square$$

(Homomorphism on medium text)

We can obtain the plaintext p_1+p_2 and p_1p_2 from ${}^1M_1$, ${}^1M_2$, ${}^2M_1$,${}^2M_2$, ${}^3M_1$, ${}^3M_2$ as follows.

$${}^1M_1:={}^1ku_1\,\mathbf{1}+{}^1lv_1G+{}^1w_1GH+{}^1z_1HG \bmod q\in O,$$

$${}^2M_1:={}^2ku_1\,\mathbf{1}+{}^2lv_1G+{}^2w_1GH+{}^2z_1HG \bmod q\in O,$$

$${}^3M_1:={}^3ku_1\,\mathbf{1}+{}^3lv_1G+{}^3w_1GH+{}^3z_1HG \bmod q\in O,$$

$${}^1M_2:={}^1ku_2\,\mathbf{1}+{}^1lv_2G+{}^1w_2GH+{}^1z_2HG \bmod q\in O,$$

$${}^2M_2:={}^2ku_2\,\mathbf{1}+{}^2lv_2G+{}^2w_2GH+{}^2z_2HG \bmod q\in O,$$

$${}^3M_2:={}^3ku_2\,\mathbf{1}+{}^3lv_2G+{}^3w_2GH+{}^3z_2HG \bmod q\in O.$$

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

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

$${}^3M_{1+2}:={}^3M_1+{}^3M_2 \bmod q$$

$$p_1:= su_1+tv_1 \bmod q$$

$$p_2:= su_2+tv_2 \bmod q$$

$$p_{1+2}: =\alpha[{}^1M_{1+2}]_0 +\beta[{}^2M_{1+2}]_0 \bmod q,$$

$$=\alpha({}^1ku_1+{}^1lv_12g_0+{}^1ku_2+{}^1lv_22g_0) +\beta({}^2ku_1 +{}^2lv_12g_0+{}^2ku_2+{}^2lv_22g_0)$$

$$= (\alpha\,{}^1ku +\beta\,{}^2k)(u_1+u_2)+ (\alpha\,{}^1l2g_0+\beta\,{}^2l2g_0) (v_1+v_2).$$

From (22b) , (22c) we have

$$=s(u_1+u_2)+t (v_1+v_2)$$

$$= su_1+tv_1+ su_2+tv_2$$

$$=p_1+ p_2 \bmod q. \tag{24}$$

We can consider that $({}^1M_{1+2},{}^2M_{1+2},{}^3M_{1+2})$ is the medium text of the plaintext p_{1+2}.

Next we try to calculate the multiplication of medium texts.

${}^1M_1{}^1M_2 =({}^1ku_1\,\mathbf{1}+{}^1lv_1G+{}^1w_1GH+{}^1z_1HG)(\,{}^1ku_2\,\mathbf{1}+{}^1lv_2G+{}^1w_2GH+{}^1z_2HG) \bmod q$

$=({}^1k)^2\, u_1u_2\mathbf{1}+({}^1k{}^1l)\,(u_1v_2+v_1u_2)G+2g_0{}^1lv_1{}^1lv_2G+{}^1w_{12}'GH+{}^1z_{12}'HG \bmod q$

where ${}^1w_{12}',{}^1z_{12}' \in R$.

${}^2M_1{}^2M_2 =({}^2ku_1\,\mathbf{1}+{}^2lv_1G+{}^2w_1GH+{}^2z_1HG)(\,{}^2ku_2\,\mathbf{1}+{}^2lv_2G+{}^2w_2GH+{}^2z_2HG) \bmod q$

$=({}^2k)^2\, u_1u_2\mathbf{1}+({}^2k{}^2l\,)\,(u_1v_2+v_1u_2)G+2g_0{}^2lv_1{}^2lv_2G+{}^2w_{12}'GH+{}^2z_{12}'HG \bmod q$

where ${}^2w_{12}',{}^2z_{12}' \in R$.

${}^3M_1{}^3M_2=({}^3ku_1\,\mathbf{1}+{}^3lv_1G+{}^3w_1GH+{}^3z_1HG)({}^3ku_2\,\mathbf{1}+{}^3lv_2G+{}^3w_2GH+{}^3z_2HG) \bmod q$

$=({}^3k)^2\, u_1u_2\mathbf{1}+({}^3k{}^3l)\,(u_1v_2+v_1u_2)G+2g_0{}^3lv_1{}^3lv_2G+{}^3w_{12}'GH+{}^3z_{12}'HG \bmod q$

where ${}^3w_{12}',{}^3z_{12}' \in R$.

We define ${}^1M_{12}$, ${}^2M_{12}$ and ${}^3M_{12}$ as follows.

${}^1M_{12}:=d_{11}{}^1M_1{}^1M_2+ d_{12}{}^2M_1{}^2M_2+ d_{13}{}^3M_1{}^3M_2$

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

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

$[d_{11}({}^1l)^2+ d_{12}\,({}^2l)^2+ d_{13}({}^3l)^2]2g_0v_1v_2G+{}^1w_{12}GH+{}^1z_{12}HG \bmod q$

where ${}^1w_{12},{}^1z_{12} \in R$.

${}^2M_{12}: =d_{21}{}^1M_1{}^1M_2+ d_{22}{}^2M_1{}^2M_2+ d_{23}{}^3M_1{}^3M_2$

$=[d_{21}({}^1k)^2 + d_{22}({}^2k)^2+ d_{23}({}^3k)^2]u_1u_2\mathbf{1}+$

$[d_{21}{}^1k{}^1l + d_{22}{}^2k{}^2l + d_{23}{}^3k{}^3l](u_1v_2+v_1u_2)G+$

$[d_{21}({}^1l)^2+ d_{22}\,({}^2l)^2+ d_{23}({}^3l)^2]2g_0v_1v_2G+{}^2w_{12}GH+{}^2z_{12}HG \bmod q$

where ${}^2w_{12},{}^2z_{12} \in R$.

${}^3M_{12}: =d_{31}{}^1M_1{}^1M_2+ d_{32}{}^2M_1{}^2M_2+ d_{33}{}^3M_1{}^3M_2$

$=[d_{31}({}^1k)^2 + d_{32}({}^2k)^2+ d_{33}({}^3k)^2]u_1u_2\mathbf{1}+$

$[d_{31}({}^1k{}^1l\,)+ d_{32}({}^2k{}^2l\,)+ d_{33}({}^3k{}^3l)](u_1v_2+v_1u_2)G+$

$[d_{31}({}^1l)^2+ d_{32}\,({}^2l)^2+ d_{33}({}^3l)^2]2g_0v_1v_2G+{}^3w_{12}GH+{}^3z_{12}HG \bmod q$

where ${}^3w_{12}, {}^3z_{12} \in R$.

We define u_{12}, v_{12} and p_{12} as follows.

$$u_{12} := su_1u_2 \bmod q \in R \tag{25a}$$

$$v_{12} := s(u_1v_2 + u_2v_1) + tv_1v_2 \bmod q \in R \tag{25b}$$

$$p_{12} := su_{12} + tv_{12} \bmod q \in R. \tag{25c}$$

We select (d_{ij}) that satisfy the following equations.

$$\begin{aligned}{}^1M_{12} &= d_{11}{}^1M_1{}^1M_2 + d_{12}{}^2M_1{}^2M_2 + d_{13}{}^3M_1{}^3M_2 \\ &= {}^1ku_{12}\,\mathbf{1} + {}^1lv_{12}G + {}^1w_{12}GH + {}^1z_{12}HG \bmod q \\ &= {}^1k\,su_1u_2\mathbf{1} + {}^1l\,s(u_1v_2 + u_2v_1)G + {}^1l\,tv_1v_2G + {}^1w_{12}GH + {}^1z_{12}HG \bmod q \end{aligned} \tag{26a}$$

$$\begin{aligned}{}^2M_{12} &= d_{21}{}^1M_1{}^1M_2 + d_{22}{}^2M_1{}^2M_2 + d_{23}{}^3M_1{}^3M_2 \\ &= {}^2ku_{12}\,\mathbf{1} + {}^2lv_{12}G + {}^2w_{12}GH + {}^2z_{12}HG \bmod q \\ &= {}^2k\,su_1u_2\mathbf{1} + {}^2l\,s(u_1v_2 + u_2v_1)G + {}^2l\,tv_1v_2G + {}^2w_{12}GH + {}^2z_{12}HG \bmod q \end{aligned} \tag{26b}$$

$$\begin{aligned}{}^3M_{12} &:= d_{31}{}^1M_1{}^1M_2 + d_{32}{}^2M_1{}^2M_2 + d_{33}{}^3M_1{}^3M_2 \\ &= {}^3ku_{12}\,\mathbf{1} + {}^3lv_{12}G + {}^3w_{12}GH + {}^3z_{12}HG \bmod q. \\ &= {}^3k\,su_1u_2\mathbf{1} + {}^3l\,s(u_1v_2 + u_2v_1)G + {}^3l\,tv_1v_2G + {}^3w_{12}GH + {}^3z_{12}HG \bmod q. \end{aligned} \tag{26c}$$

Then we have the equations that the public parameters (d_{ij}) have to satisfy as follows.

$$\begin{cases} d_{11}({}^1k)^2 + d_{12}({}^2k)^2 + d_{13}({}^3k)^2 = {}^1k\,s \bmod q \\ d_{11}({}^1k{}^1l) + d_{12}({}^2k{}^2l) + d_{13}({}^3k{}^3l) = {}^1l\,s \bmod q \\ d_{11}({}^1l)^2 + d_{12}\,({}^2l)^2 + d_{13}({}^3l)^2 = {}^1l\,t/(2g_0) \bmod q \end{cases}$$

$$\begin{cases} d_{21}({}^1k)^2 + d_{22}({}^2k)^2 + d_{23}({}^3k)^2 = {}^2k\,s \bmod q \\ d_{21}({}^1k{}^1l) + d_{22}({}^2k{}^2l) + d_{23}({}^3k{}^3l) = {}^2l\,s \bmod q \\ d_{21}({}^1l)^2 + d_{22}\,({}^2l)^2 + d_{23}({}^3l)^2 = {}^2l\,t/(2g_0) \bmod q \end{cases}$$

$$\begin{cases} d_{31}({}^1k)^2 + d_{32}({}^2k)^2 + d_{33}({}^3k)^2 = {}^3k\,s \bmod q \\ d_{31}({}^1k{}^1l) + d_{32}({}^2k{}^2l) + d_{33}({}^3k{}^3l) = {}^3l\,s \bmod q \\ d_{31}({}^1l)^2 + d_{32}\,({}^2l)^2 + d_{33}({}^3l)^2 = {}^3l\,t/(2g_0) \bmod q \end{cases}$$

where ${}^ik, {}^il$ (i=1,2,3) satisfy

$$\Delta = \begin{vmatrix} ({}^1k)^2 & ({}^2k)^2 & ({}^3k)^2 \\ {}^1k\,{}^1l & {}^2k\,{}^2l & {}^3k\,{}^3l \\ ({}^1l)^2 & ({}^2l)^2 & ({}^3l)^2 \end{vmatrix},$$

GCD(Δ , q) = 1.

Here we show that $p_{12}=\alpha[{}^1M_{12}]_0 + \beta[{}^2M_{12}]_0 \bmod q = p_1p_2 \bmod q$.

From (25c), (25a) and (25b) we have

$p_{12}= su_{12}+tv_{12} \bmod q$

$= s(su_1u_2)+t(s(u_1v_2 + u_2v_1)+ tv_1v_2)$

$= (su_1+ tv_1)\,(su_2 + tv_2)$

$= p_1p_2 \bmod q$.

On the other hand we have from (25c), (25a), (25b) ,(22b) and (22c)

$p_{12}= su_{12}+tv_{12} \bmod q$

$=(\alpha\, {}^1k+\beta\, {}^2k)\, su_1u_2+(\alpha\, {}^1lg_0+\beta\, {}^2lg_0)\, (s(u_1v_2 + u_2v_1)+ tv_1v_2)$

$=\alpha[\, {}^1k\, su_1u_2+ {}^1lg_0(s(u_1v_2 + u_2v_1)+ tv_1v_2)]+\beta[\, {}^2k\, su_1u_2+ {}^2lg_0\, (s(u_1v_2 + u_2v_1)+ tv_1v_2)]$

$=\alpha[{}^1M_{12}]_0 +\beta[{}^2M_{12}]_0 \bmod q$.

We can consider that $({}^1M_{12}, {}^2M_{12}, {}^3M_{12})$ is the medium text of the plaintext p_{12}.

We have shown that we can obtain the plaintext p_1+p_2 from ${}^1M_{1+2}$, ${}^2M_{1+2}$, the plaintext p_1p_2 from ${}^1M_{12}$,${}^2M_{12}$. □

§6.3 Enciphering

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

$f(X)\in O[X]=\{f_{ij}\}$, $(i,j=0,\dots,7)$,

$g(X)\in O[X]=\{g_{ij}\}$, $(i,j=0,\dots,7)$.

Let $(q,G,H;f(X),g(X))$ be the system parameters where q is a prime.

Let $[h_b(X),(d_{bij}),\alpha_b,\beta_b]$(i,j=1,2,3) be user B's public keys and $[m_b, n_b,({}^ik_b),({}^il_b),({}^iw_b, {}^iz_b),s_b,t_b]$ (i=1,2,3) be user B's secret keys.

Let $F_{\mathrm{BA}}(X,Y)$ or $F_{\mathrm{AB}}(X,Y)$ be the common enciphering function between user A and user B.

User B generate medium text ${}^1M$, ${}^2M$, ${}^3M$ by using the plaintext $p\in R$, the components $u,v\in R$ of the plaintext p, secret parameters ${}^1k_b,{}^1l_b$, ${}^2k_b,{}^2l_b$, ${}^3k_b,{}^3l_b,\in R$ and random noises ${}^1w_b,{}^1z_b$, ${}^2w_b,{}^2z_b$, ${}^3w_b,{}^3z_b\in R$ such that

$${}^1M:={}^1k_bu\,\mathbf{1}+{}^1l_bvG+{}^1w_bGH+{}^1z_bHG \bmod q\in O,$$

$${}^2M:={}^2k_bu\,\mathbf{1}+{}^2l_bvG+{}^2w_bGH+{}^2z_bHG \bmod q\in O,$$

$${}^3M:={}^3k_bu\,\mathbf{1}+{}^3l_bvG+{}^3w_bGH+{}^3z_bHG \bmod q\in O,$$

$$p:= s_bu+t_bv \bmod q\in R$$

$$=\alpha_b[{}^1M]_0 +\beta_b[{}^2M]_0 \bmod q,$$

where

$$(\alpha_b\, {}^1k_b+\beta_b\, {}^2k_b)=s_b \bmod q,$$

$$(\alpha_b{}^1l_bg_0+\beta_b\, {}^2l_bg_0)=t_b \bmod q.$$

User B calculates three sub-ciphertexts $F_{\mathrm{BA}}(X, {}^kM)$ by substituting medium texts ${}^kM\in O$ to Y of $F_{\mathrm{BA}}(X,Y)$ (k=1,2,3).

$$F_{\mathrm{BA}}(X, {}^kM)\in O\,[X]$$

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

$$\ldots \qquad \ldots \quad ,$$

$${}^kc_{70}x_0+\ldots+{}^kc_{77}x_7\,) \bmod q$$

$$=\{{}^kc_{ij}\}\ (i,j=0,\ldots,7;k=1,2,3)\,.$$

Ciphertext $C(p, X)$ consists of three sub-ciphertexts $F_{\mathrm{BA}}(X, {}^kM)$ (k=1,2,3) such that

$$C(p, X):=(F_{\mathrm{BA}}(X,{}^1M), F_{\mathrm{BA}}(X,{}^2M), F_{\mathrm{BA}}(X,{}^3M))\in \{O\,[X]\}^3.$$

User B sends $\{{}^kc_{ij}\}$ $(i,j=0,\ldots,7;k=1,2,3)$ to user A through the insecure line.

§6.4 Deciphering

User A downloads user B's public-keys $[h_b(X),(d_{bij}),\alpha_b,\beta_b](i,j=1,2,3)$ from the system centre and receives the ciphertext $C(p, X)$ from user B. User A deciphers $C(p, X)=(F_{\mathrm{BA}}(X,{}^1M), F_{\mathrm{BA}}(X,{}^2M), F_{\mathrm{BA}}(X,{}^3M)) =\{{}^kc_{ij}\}$ $(i,j=0,\ldots,7;k=1,2,3)$ sent by user B to obtain p as follows.

User A calculates $E_{ab}(X)$ by using $h_b(X), f^{ma0}(X), g^{na0}(X), f^{ma1}(X)$, and $g^{na1}(X)$ such that

$E_{ab}(X) := f^{ma0}(h_b(g^{na0}(X))) + f^{ma1}(h_b(g^{na1}(X)))$

$= f^{ma0}(f^{mb0}(g^{nb0}(g^{na0}(X)))) + f^{ma0}(f^{mb1}(g^{nb1}(g^{na0}(X))))$

$+ f^{ma1}(f^{mb0}(g^{nb0}(g^{na1}(X)))) + f^{ma1}(f^{mb1}(g^{nb1}(g^{na1}(X))))$

$= f^{ma0+mb0}(g^{nb0+na0}(X)) + f^{ma0+mb1}(g^{nb1+na0}(X)) + f^{ma1+mb0}(g^{nb0+na1}(X)) + f^{ma1+mb1}(g^{nb1+na1}(X)) \bmod q.$

User A calculates $E_{ab}^{-1}(X)$ from $E_{ab}(X)$ by using **ALINVF**.

$F_{\mathrm{BA}}(X, {}^{\mathrm{e}}M) := \{{}^{\mathrm{e}}c_{ij}\}$ $(i, j = 0, \ldots, 7; \mathrm{e} = 1,2,3)$,

$E_{ab}(F_{\mathrm{BA}}(E_{ab}^{-1}(\mathbf{1}), {}^{\mathrm{e}}M))$

$= E_{ab}(E_{ba}^{-1}({}^{\mathrm{e}}ME_{ba}(E_{ab}^{-1}(\mathbf{1})))) \bmod q$

$= {}^{\mathrm{e}}M$ (e=1,2,3) ,(because $E_{ab}(X) = E_{ba}(X)$).

$\alpha_b[{}^1M]_0 + \beta_b[{}^2M]_0 \bmod q = p$ $(= s_b u + t_b v \bmod q) \in R$,

where

$(\alpha_b\, {}^1k_b + \beta_b\, {}^2k_b) = s_b \bmod q$,

$(\alpha_b\, {}^1l_b g_0 + \beta_b\, {}^2l_b g_0) = t_b \bmod q$.

After this the lower subscript "*b*" is omitted.

Theorem 9

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

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

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

where

$C(p, X) = (F_{\mathrm{AB}}(X, {}^1M), F_{\mathrm{AB}}(X, {}^2M), F_{\mathrm{AB}}(X, {}^3M))$

$C(p', X) = (F_{\mathrm{AB}}(X, {}^1M'), F_{\mathrm{AB}}(X, {}^2M'), F_{\mathrm{AB}}(X, {}^3M'))$

${}^1M := {}^1ku\,\mathbf{1} + {}^1lvG + {}^1wGH + {}^1zHG \bmod q \in O$,

${}^1M' := {}^1ku'\,\mathbf{1} + {}^1lv'G + {}^1w'GH + {}^1z'HG \bmod q \in O$,

${}^2M := {}^2ku\,\mathbf{1} + {}^2lvG + {}^2wGH + {}^2zHG \bmod q \in O$,

$^2M' := {}^2ku'\,\mathbf{1} + {}^2lv'G + {}^2w'GH + {}^2z'HG \bmod q \in O$,

$^3M := {}^3ku\,\mathbf{1} + {}^3lvG + {}^3wGH + {}^3zHG \bmod q \in O$,

$^3M' := {}^3ku'\,\mathbf{1} + {}^3lv'G + {}^3w'GH + {}^3z'HG \bmod q \in O$,

$p := su + tv \bmod q$,

$p' := su' + tv' \bmod q$.

(*Proof*)

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

$F_{\mathrm{AB}}(X, {}^1M) = F_{\mathrm{AB}}(X, {}^1M')$,

$E_{ab}{}^{-1}\,({}^1ME_{ab}\,(X)) = E_{ab}{}^{-1}\,({}^1M'\,E_{ab}\,(X))$,

$E_{ab}{}^{-1}\,({}^1ME_{ab}\,(E_{ab}{}^{-1}\,(\mathbf{1}))) = E_{ab}{}^{-1}\,({}^1M'\,E_{ab}\,(E_{ab}{}^{-1}\,(\mathbf{1})))$,

$E_{ab}{}^{-1}\,({}^1M) = E_{ab}{}^{-1}\,({}^1M')$,

$E_{ab}\,(E_{ab}{}^{-1}\,({}^1M)) = E_{ab}\,(E_{ab}{}^{-1}\,({}^1M')) \bmod q$,

$^1M = {}^1M' \bmod q$,

$^1ku\,\mathbf{1} + {}^1lvG + {}^1wGH + {}^1zHG = {}^1ku'\,\mathbf{1} + {}^1lv'G + {}^1w'GH + {}^1z'HG \bmod q$.

Then we have

$^1k\,(u - u')\mathbf{1} + {}^1l\,(v - v')G + ({}^1w - {}^1w')GH + ({}^1z - {}^1z')HG = 0 \bmod q$.

From Theorem 8 we have

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

$u = u' \bmod q$,

$v = v' \bmod q$,

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

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

We have

$p = su + tv = su' + tv' = p' \bmod q$. q.e.d.

§6.5 Addition scheme on ciphertexts

Let

$${}^{1}M_{1}:={}^{1}ku_{1}\,\mathbf{1}+{}^{1}lv_{1}G+{}^{1}w_{1}GH+{}^{1}z_{1}HG \bmod q\in O,$$

$${}^{2}M_{1}:={}^{2}ku_{1}\,\mathbf{1}+{}^{2}lv_{1}G+{}^{2}w_{1}GH+{}^{2}z_{1}HG \bmod q\in O,$$

$${}^{3}M_{1}:={}^{3}ku_{1}\,\mathbf{1}+{}^{3}lv_{1}G+{}^{3}w_{1}GH+{}^{3}z_{1}HG \bmod q\in O,$$

$${}^{1}M_{2}:={}^{1}ku_{2}\,\mathbf{1}+{}^{1}lv_{2}G+{}^{1}w_{2}GH+{}^{1}z_{2}HG \bmod q\in O,$$

$${}^{2}M_{2}:={}^{2}ku_{2}\,\mathbf{1}+{}^{2}lv_{2}G+{}^{2}w_{2}GH+{}^{2}z_{2}HG \bmod q\in O,$$

$${}^{3}M_{2}:={}^{3}ku_{2}\,\mathbf{1}+{}^{3}lv_{2}G+{}^{3}w_{2}GH+{}^{3}z_{2}HG \bmod q\in O,$$

be medium texts to be encrypted where

$$p_{1}:= su_{1}+tv_{1} \bmod q =\alpha[{}^{1}M_{1}]_{0} +\beta[{}^{2}M_{1}]_{0} \bmod q,$$

$$p_{2}:= su_{2}+tv_{2} \bmod q =\alpha[{}^{1}M_{2}]_{0} +\beta[{}^{2}M_{2}]_{0} \bmod q.$$

$$(\alpha\, {}^{1}k+\beta\, {}^{2}k)=s \bmod q,$$

$$(\alpha\, {}^{1}lg_{0}+\beta\, {}^{2}lg_{0})=t \bmod q.$$

Let

$$C(p_{1},X):=(F_{\mathrm{AB}}(X,{}^{1}M_{1}),F_{\mathrm{AB}}(X,{}^{2}M_{1}) ,F_{\mathrm{AB}}(X,{}^{3}M_{1}))$$

$$C(p_{2},X):= (F_{\mathrm{AB}}(X,{}^{1}M_{2}),F_{\mathrm{AB}}(X,{}^{2}M_{2}) ,F_{\mathrm{AB}}(X,{}^{3}M_{2}))$$

be the ciphertexts. We define the additional operation between $C(p_{1},X) \bmod q$ and $C(p_{2},X) \bmod q$ such that

$$C(p_{1},X)+C(p_{2},X) \bmod q$$

$$:= (F_{\mathrm{AB}}(X,{}^{1}M_{1})+ F_{\mathrm{AB}}(X,{}^{1}M_{2}) \bmod q, F_{\mathrm{AB}}(X,{}^{2}M_{1})+F_{\mathrm{AB}}(X,{}^{2}M_{2}) \bmod q, F_{\mathrm{AB}}(X,{}^{3}M_{1})+F_{\mathrm{AB}}(X,{}^{3}M_{2}) \bmod q)$$

$$=(F_{\mathrm{AB}}(X,{}^{1}M_{1}+{}^{1}M_{2}) \bmod q, F_{\mathrm{AB}}(X, {}^{2}M_{1} +{}^{2}M_{2}) \bmod q, F_{\mathrm{AB}}(X, {}^{3}M_{1} +{}^{3}M_{2}) \bmod q)$$

$$=(F_{\mathrm{AB}}(X,{}^{1}M_{1+2}) \bmod q, F_{\mathrm{AB}}(X, {}^{2}M_{1+2}) \bmod q, F_{\mathrm{AB}}(X, {}^{3}M_{1+2}) \bmod q).$$

Then we have

$$C(p_{1},X)+C(p_{2},X) \bmod q$$

$$= C(p_{1+2},X) \bmod q,$$

$$= C(p_{1}+p_{2}, X) \bmod q.\text{(From (24))}$$

We can consider that $C(p_{1+2},X) =(F_{\mathrm{AB}}(X,{}^{1}M_{1+2}) \bmod q, F_{\mathrm{AB}}(X, {}^{2}M_{1+2}) \bmod q, F_{\mathrm{AB}}(X, {}^{3}M_{1+2}) \bmod q)$ is the ciphertext of the plaintext p_{1+2}.

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

§6.6 Multiplication scheme on ciphertexts

Here we consider the multiplicative operation on the ciphertexts.

Let

$$C(p_1,X):=(F_{AB}(X,{}^1M_1),F_{AB}(X,{}^2M_1),F_{AB}(X,{}^3M_1))$$

$$C(p_2,X):=(F_{AB}(X,{}^1M_2),F_{AB}(X,{}^2M_2),F_{AB}(X,{}^3M_2))$$

be the ciphertexts where

$${}^1M_1:={}^1ku_1\,\mathbf{1}+{}^1lv_1G+{}^1w_1GH+{}^1z_1HG \bmod q\in O,$$

$${}^2M_1:={}^2ku_1\,\mathbf{1}+{}^2lv_1G+{}^2w_1GH+{}^2z_1HG \bmod q\in O,$$

$${}^3M_1:={}^3ku_1\,\mathbf{1}+{}^3lv_1G+{}^3w_1GH+{}^3z_1HG \bmod q\in O,$$

$${}^1M_2:={}^1ku_2\,\mathbf{1}+{}^1lv_2G+{}^1w_2GH+{}^1z_2HG \bmod q\in O,$$

$${}^2M_2:={}^2ku_2\,\mathbf{1}+{}^2lv_2G+{}^2w_2GH+{}^2z_2HG \bmod q\in O,$$

$${}^3M_2:={}^3ku_2\,\mathbf{1}+{}^3lv_2G+{}^3w_2GH+{}^3z_2HG \bmod q\in O,$$

$$p_1:=su_1+tv_1 \bmod q=\alpha[{}^1M_1]_0+\beta[{}^2M_1]_0 \bmod q,$$

$$p_2:=su_2+tv_2 \bmod q=\alpha[{}^1M_2]_0+\beta[{}^2M_2]_0 \bmod q$$

where

$$(\alpha\,{}^1k+\beta\,{}^2k)=s \bmod q,$$

$$(\alpha\,{}^1lg_0+\beta\,{}^2lg_0)=t \bmod q.$$

We can calculate the ciphertext $C(p_1p_2, X)$ of the plaintext p_1p_2 by using

$$C(p_1,X)=(F_{AB}(X,{}^1M_1),F_{AB}(X,{}^2M_1),F_{AB}(X,{}^3M_1))$$

and

$$C(p_2,X)=(F_{AB}(X,{}^1M_2),F_{AB}(X,{}^2M_2),F_{AB}(X,{}^3M_2))$$

with a part of user A's public-key (d_{ij}) as follows.

$$K_1(X):=F_{AB}(F_{AB}(X,{}^1M_2),{}^1M_1)=F_{AB}(X,{}^1M_1{}^1M_2) \bmod q$$

$$K_2(X):=F_{\rm AB}(F_{\rm AB}(X,{}^2M_2),{}^2M_1)=F_{\rm AB}(X,{}^2M_1{}^2M_2)\bmod q$$

$$K_3(X):=K_{11}((F_{\rm AB}((X,{}^3M_2),{}^3M_1)=F_{\rm AB}(X,{}^3M_1{}^3M_2)\bmod q$$

$${}^1C_{12}(X):=d_{11}K_1(X)+d_{12}K_2(X)+d_{13}K_3(X)=F_{\rm AB}(X,{}^1M_{12})\bmod q$$

$${}^2C_{12}(X):=d_{21}K_1(X)+d_{22}K_2(X)+d_{23}K_3(X)=F_{\rm AB}(X,{}^2M_{12})\bmod q$$

$${}^3C_{12}(X):=d_{31}K_1(X)+d_{32}K_2(X)+d_{33}K_3(X)=F_{\rm AB}(X,{}^3M_{12})\bmod q$$

where

$${}^1M_{12}:=d_{11}{}^1M_1{}^1M_2+d_{12}{}^2M_1{}^2M_2+d_{13}{}^3M_1{}^3M_2\bmod q$$

$${}^2M_{12}:=d_{21}{}^1M_1{}^1M_2+d_{22}{}^2M_1{}^2M_2+d_{23}{}^3M_1{}^3M_2\bmod q$$

$${}^3M_{12}:=d_{31}{}^1M_1{}^1M_2+d_{32}{}^2M_1{}^2M_2+d_{33}{}^3M_1{}^3M_2\bmod q.$$

Here we show that

$$C(p_1p_2,X):=(F_{\rm AB}(X,{}^1M_{12}),F_{\rm AB}(X,{}^2M_{12}),F_{\rm AB}(X,{}^3M_{12}))$$

is the ciphertext of the plaintext p_1p_2.

First we decipher $(F_{\rm AB}(X,{}^1M_{12}), F_{\rm AB}(X,{}^2M_{12}), F_{\rm AB}(X,{}^3M_{12}))$ to obtain the medium texts ${}^1M_{12},{}^2M_{12},{}^3M_{12}$ by using the $E_{ab}(X)$ and $E_{ab}{}^{-1}(X)$ with a part of user A's public-key,$[\alpha,\beta]$.

$$E_{ab}(F_{\rm AB}(E_{ab}{}^{-1}(\mathbf{1}),{}^eM_{12}))$$

$$=E_{ab}(E_{ab}{}^{-1}({}^eM_{12}E_{ab}(E_{ab}{}^{-1}(\mathbf{1}))))\bmod q$$

$$={}^eM_{12},\ (e=1,2,3).$$

From (26a) and (26b)

$$p_{12}=\alpha[{}^1M_{12}]_0+\beta[{}^2M_{12}]_0\bmod q,$$

$$=\alpha[{}^1k\,su_1u_2+{}^1l\,s(u_1v_2+u_2v_1)g_0+{}^1l\,tv_1v_2\,g_0]$$

$$+\beta[{}^2k\,su_1u_2+{}^2l\,s(u_1v_2+u_2v_1)g_0+{}^2l\,tv_1v_2g_0]\quad\bmod q$$

$$=(\alpha{}^1k+\beta{}^2k)su_1u_2+(\alpha{}^1l+\beta{}^2l)s(u_1v_2+u_2v_1)g_0+(\alpha{}^1l+\beta{}^2l)t\,v_1v_2\,g_0\bmod q$$

$$=s^2u_1u_2+st(u_1v_2+u_2v_1)+t^2\,v_1v_2\bmod q$$

$$=(su_1+tv_1)(su_2+tv_2)$$

$$=p_1p_2\bmod q.$$

We have shown that we can obtain the plaintext p_1p_2 from $C(p_1,X)$, $C(p_2,X)$.□

We can define that

$$C(p_{12},X) := (F_{\mathrm{AB}}(X,{}^1M_{12}),F_{\mathrm{AB}}(X,{}^2M_{12}) ,F_{\mathrm{AB}}(X,{}^3M_{12}))$$

We can consider $C(p_{12},X)$ as the ciphertext of the plaintext p_{12}.

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

§6.7 Multivariate discrete logarithm assumption (MDLA)

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

Let q be a prime. Let m_0 ,n_0, m_1 and $n_1 \in \boldsymbol{Fq}^*$ be the integer parameters.

Let $f(X)= \{f_{ij}\}_{(i,j=0,\dots,7)} \in O[X]$ and $g(X)= \{g_{ij}\}_{(i,j=0,\dots,7)} \in O[X]$ be basic functions

where there exists no integer k such that satisfies the following equation

$$f(X)= g^{k}(X) \bmod q, k \in Z.$$

Let $h(X)=f^{m0}(g^{n0}(X))+f^{m1}(g^{n1}(X)) \bmod q =\{ h_{ij} \}_{(i,j=0,\dots,7)} \in O[X]$ be a part of the public function.

X is a variable.

In the **MDLA($f(X)$,$g(X)$, $f^{m0}(g^{n0}(X))+f^{m1}(g^{n1}(X))$;$q$)**, the adversary $\mathrm{A_d}$ is given $f(X)= \{f_{ij}\}_{(i,j=0,\dots,7)}$, $g(X)= \{g_{ij}\}_{(i,j=0,\dots,7)}$, $h(X)=f^{m0}(g^{n0}(X))+f^{m1}(g^{n1}(X)) \bmod q=\{ h_{ij} \}_{(i,j=0,\dots,7)}$ and system parameters (q, G, H; $f(X)$,$g(X)$) and his goal is to find m_0 ,n_0, m_1 and $n_1 \in \boldsymbol{Fq}^*$. For parameters $m_i = m_i(\lambda)$, $n_i= n_i(\lambda)$ (i=0,1) defined in terms of the security parameter λ and for any PPT adversary $\mathrm{A_d}$, we have

$$\Pr [\, f(X)=\{f_{ij}\}, g(X)=\{g_{ij}\}, f^{m0}(g^{n0}(X)) + f^{m1}(g^{n1}(X)) \bmod q = \{h_{ij}\}:$$

$$m_0, n_0, m_1, n_1 \leftarrow \mathrm{A_d}\, (1^{\lambda},\{f_{ij}\},\{g_{ij}\},\{h_{ij}\})] = \mathrm{negl}(\lambda).$$

MDLA($f(X)$, $g(X)$, $f^{m0}(g^{n0}(X))+f^{m1}(g^{n1}(X))$;$q$) on the multivariate polynomials is different from the discrete logarithm assumption that is defined on the finite field because there exists no integer k such that $g(X)=f^{k}(X) \bmod q$.

§6.8 Numerical example

In this section we simply show numerical example relating proposed fully homomorphic encryption scheme and I specify the lower subscript such as “a”, ”b”.

[Data communication]

1) System centre publishes system parameters [q, G, H; $f(X)$, $g(X)$]

where

q=1931.

G=(966,132,57,9,2,0,0,0)$\in O$, H=(0,63,43,9,369,28,7,1)$\in O$.

We notice that $|G|^2$=0 mod q, $|H|^2$=0 mod q,

GH=(0,712,932,1187,1241,1145,187,111)$\in O$,

HG=(0,1282,1042,753,1059,814,1751,1821)$\in O$,

Numerical examples of $f(X)=\{f_{ij}\}$ and $g(X)=\{g_{ij}\}$ are omitted here.

2) User A selects secret key $m_{a0},n_{a0},m_{a1},n_{a1}\in \boldsymbol{Fq}^*$ and calculates $f^{\,ma0}(X)$, $f^{\,ma1}(X)$, $g^{na0}(X)$, $g^{na1}(X)$.

3) User A calculates $h_a(X)= f^{ma0}(g^{na0}(X))) + f^{ma1}(g^{na1}(X)))$ mod q to be user A's public-key. User A sends public-key $h_a(X)$ =\{ h_{aij} \} with (d_{aij}), α_a and β_a to system centre.

4) User B selects secret key m_{b0},n_{b0}, $m_{b1},n_{b1}\in \boldsymbol{Fq}^*$ and calculates $f^{\,mb0}(X)$, $f^{\,mb1}(X)$, $g^{nb0}(X)$, $g^{nb1}(X)$.

5) User B calculates $h_b(X)= f^{mb0}(g^{nb0}(X))) + f^{mb1}(g^{nb1}(X)))$ mod q to be user B's public-key.

User B sends $h_b(X)$ =\{ h_{bij} \} with (d_{bij}), α_b and β_b to system centre.

His public-key is $[h_b(X), (d_{bij}), \alpha_b, \beta_b]$

where

$(\alpha_b\,{}^1k_b+\beta_b\,{}^2k_b)=s_b$ mod q,

$(\alpha_b\,{}^1l_bg_{b0}+\beta_b\,{}^2l_bg_{b0})=t_b$ mod q.

(d_{bij})=(1834,1633,33 ; 909,782,131 ; 1234,795,17).

We notice that

Det(d_{bij})=0 mod q.

6) User B downloads user A's public-key $h_a(X)$ from system centre and generates common enciphering function $E_{ba}(X)$ as follows.

$$E_{ba}(X) := f^{nb0}(h_a(g^{nb0}(X))) + f^{nb1}(h_a(g^{nb1}(X)))$$

$$= f^{nb0}(f^{ma0}(g^{na0}(g^{nb0}(X)))) + f^{nb0}(f^{ma1}(g^{na1}(g^{nb0}(X))))$$

$$+ f^{nb1}(f^{ma0}(g^{na0}(g^{nb1}(X)))) + f^{nb1}(f^{ma1}(g^{na1}(g^{nb1}(X))))$$

$$= f^{mb0+ma0}(g^{na0+nb0}(X)) + f^{mb0+ma1}(g^{na1+nb0}(X))$$

$$+ f^{mb1+ma0}(g^{na0+nb1}(X)) + f^{mb1+ma1}(g^{na1+nb1}(X)) \bmod q.$$

User B calculates $E_{ba}{}^{-1}(X)$ from $E_{ba}(X)$ by using **ALINVF**.

7) User B calculates $F_{\mathrm{BA}}(X,Y)$ such that

$F_{\mathrm{BA}}(X,Y)= E_{ba}{}^{-1}\,(Y\,E_{ba}\,(X))$ mod q.

8) User B selects $[({}^{\mathrm{i}}k_b),({}^{\mathrm{i}}l_b),({}^{\mathrm{i}}w_b, {}^{\mathrm{i}}z_b), s_b,t_b]$ to be secret

where

$({}^{\mathrm{i}}k_b)=(7,9,13)$, $({}^{\mathrm{i}}l_b)=(11,17,19)$,

$({}^{1}w_{b1},{}^{1}z_{b1})=(2,3)$, $({}^{2}w_{b1},{}^{2}z_{b1})=(3,11)$, $({}^{3}w_{b1},{}^{3}z_{b1})=(7,13)$,

$({}^{1}w_{b2},{}^{1}z_{b2})=(2,1)$, $({}^{2}w_{b2},{}^{2}z_{b2})=(1,2)$, $({}^{3}w_{b2},{}^{3}z_{b2})=(3,1)$,

$s_b=1359$, $t_b=964$,

9) User B selects the plaintexts $(p_1, p_2) =(740,149)$ which he possesses.

10) User B calculates $(u_1,v_1)=(123,234)$, $(u_2,v_2)=(67,98)$ which satisfy the following equations,

$p_1= s_bu_1+t_bv_1$ mod q=1359*123+964*234 =740mod q,

$p_2= s_bu_2+t_bv_2$ mod q=1359*67+964*98 =149mod q.

11) By using the plaintexts $(p_1, p_2) =(740,149)$ user B calculates the medium texts

$({}^{1}M_1, {}^{2}M_1, {}^{3}M_1)$, $({}^{1}M_2, {}^{2}M_2, {}^{3}M_2)$ such that

${}^{1}M_1={}^{1}k_bu_1\mathbf{1}+{}^{1}l_bv_1G+{}^{1}w_{b1}GH+{}^{1}z_{b1}HG$ mod q=(217,1320,1090,765,1152,870,1765,1823),

${}^{2}M_1={}^{2}k_bu_1\mathbf{1}+{}^{2}l_bv_1G+{}^{2}w_{b1}GH+{}^{2}z_{b1}HG$ mod q=(1165,654,1560,1302,156,803,512,1054),

${}^{3}M_1={}^{3}k_bu_1\mathbf{1}+{}^{3}l_bv_1G+{}^{3}w_{b1}GH+{}^{3}z_{b1}HG$ mod q=(1891,257,1221,182,450,1218,900,1278),

${}^{1}M_2={}^{1}k_bu_2\mathbf{1}+{}^{1}l_bv_2G+{}^{1}w_{b2}GH+{}^{1}z_{b2}HG$ mod q=(1008,177,629,1243,1835,1173,194,112),

${}^{2}M_2={}^{2}k_bu_2\mathbf{1}+{}^{2}l_bv_2G+{}^{2}w_{b2}GH+{}^{2}z_{b2}HG$ mod q=(1436,1123,1428,308,898,842,1758,1822),

${}^{3}M_2={}^{3}k_bu_2\mathbf{1}+{}^{3}l_bv_2G+{}^{3}w_{b2}GH+{}^{3}z_{b2}HG$ mod q=(1802,103,1836,1762,782,387,381,223).

12) User B enciphers the medium texts $({}^{1}M_1,{}^{2}M_1,{}^{3}M_1)$, $({}^{1}M_2,{}^{2}M_2,{}^{3}M_2)$ to generate ciphertexts

$C(p_1,X) =(F_{\mathrm{BA}}(X,{}^{1}M_1), F_{\mathrm{BA}}(X,{}^{2}M_1) , F_{\mathrm{BA}}(X,{}^{3}M_1))$,

$C(p_2,X) =(F_{\mathrm{BA}}(X,{}^{1}M_2), F_{\mathrm{BA}}(X,{}^{2}M_2) , F_{\mathrm{BA}}(X,{}^{3}M_2))$.

13) User B sends $C(p_1, X)$, $C(p_2, X)$ to user A.

14) User A receives $C(p_1, X)$, $C(p_2, X)$ from user B.

User A downloads user B's public-key $[h_b(X), (d_{bij}), \alpha_b, \beta_b]$ from system centre and calculates

$$E_{ab}\,(X):=f^{ma0}(h_b(g^{na0}(X)))+f^{ma1}(h_b(g^{na1}(X)))$$

$$=f^{ma0}(f^{mb0}(g^{nb0}(g^{na0}(X)))) +f^{ma0}(f^{mb1}(g^{nb1}(g^{na0}(X))))$$

$$+f^{ma1}(f^{mb0}(g^{nb0}(g^{na1}(X)))) +f^{ma1}(f^{mb1}(g^{nb1}(g^{na1}(X))))$$

$$=f^{ma0+mb0}(g^{nb0+na0}(X)) +f^{ma0+mb1}(g^{nb1+na0}(X))$$

$$+f^{ma1+mb0}(g^{nb0+na1}(X)))+f^{ma1+mb1}(g^{nb1+na1}(X)))\ \mathrm{mod}\ q.$$

User A calculates $E_{ab}{}^{-1}(X)$ from $E_{ab}(X)$ by using **ALINVF**.

15) User A deciphers $C(p_{\mathrm{i}}, X)=(F_{\mathrm{BA}}(X,{}^1M_{\mathrm{i}}), F_{\mathrm{BA}}(X,{}^2M_{\mathrm{i}}) , F_{\mathrm{BA}}(X,{}^3M_{\mathrm{i}}))$ (i=1,2) to obtain p_1,p_2 as follows.

$$E_{ab}(F_{\mathrm{BA}}(E_{ab}{}^{-1}(\mathbf{1}),{}^{\mathrm{e}}M_{\mathrm{i}}))$$
$$= E_{ab}\,(E_{ba}{}^{-1}\,({}^{\mathrm{e}}M_{\mathrm{i}}\,E_{ba}\,(E_{ab}{}^{-1}(\mathbf{1})))) \bmod q$$
$$={}^{\mathrm{e}}M_{\mathrm{i}},(\mathrm{e}=1,2,3).$$
$$p_{\mathrm{i}}=\alpha_b[{}^1M_{\mathrm{i}}]_0 +\beta_b[{}^2M_{\mathrm{i}}]_0 \bmod q \ (\mathrm{i}=1,2).$$

[Data processing]

16) User B wants to process his data. He selects random number $y\in R$.

He generates another encryption function $F_{*\mathrm{B}}(X,Y)=E_{yb}{}^{-1}(YE_{yb}(X)) \bmod q$.

He calculates $C^*(p_1,X)$, $C^*(p_2,X)$ such that

$$C^*(p_1,X):=(F_{*\mathrm{B}}(X,{}^1M_1), F_{*\mathrm{B}}\,(X,{}^2M_1) , F_{*\mathrm{B}}\,(X,{}^3M_1)),$$
$$C^*(p_2,X):=(F_{*\mathrm{B}}\,(X,{}^1M_2), F_{*\mathrm{B}}\,(X,{}^2M_2) , F_{*\mathrm{B}}\,(X,{}^3M_2)).$$

17) User B sends his ciphered data $C^*(p_1, X)$, $C^*(p_2,X)$ with the method for processing to data processing centre D. He requires to have $C^*(p_1+p_2, X)$, $C^*(p_1p_2,X)$.

18) Data processing centre D receives user B's ciphered data $C^*(p_1, X)$, $C^*(p_2, X)$ with the method for processing.

19) Data processing centre D downloads user B's public-key $[h_b(X), (d_{bij}), \alpha_b, \beta_b]$. He uses only (d_{bij}). Data processing centre D calculates $C^*(p_1+p_2, X)$, $C^*(p_1p_2,X)$ without knowing ${}^1M_1,{}^1M_2,{}^2M_1,{}^2M_2,{}^3M_1,{}^3M_2$ and so on as follows.

$$C^*(p_1+p_2,X):=(F_{*\mathrm{B}}(X,{}^1M_1)+F_{*\mathrm{B}}(X,{}^1M_2),F_{*\mathrm{B}}(X,{}^2M_1)+F_{*\mathrm{B}}(X,{}^2M_2),F_{*\mathrm{B}}(X,{}^3M_1)+ FB_{*\mathrm{B}}(X,{}^3M_2)),$$
$$=(F_{*\mathrm{B}}(X,{}^1M_1+{}^1M_2),F_{*\mathrm{B}}(X,{}^2M_1+{}^2M_2),F_{*\mathrm{B}}(X,{}^3M_1+M_2)),$$
$$= (F_{*\mathrm{B}}(X,(1225,1497,1719,77,1056,112,28,4)),$$
$$F_{*\mathrm{B}}(X,(670,1777,1057,1610,1054,1645,339,945)),$$
$$F_{*\mathrm{B}}(X,(1762,360,1126,13,1232,1605,1281,1501))).$$

$$K_1(X):= F_{*\mathrm{B}}((F_{\mathrm{B}*}(X, Y)=(X, {}^1M_2)), {}^1M_1)= F_{*\mathrm{B}}(X,{}^1M_1{}^1M_2) \bmod q$$
$$= F_{*\mathrm{B}}(X,(997,1232,1536,596,1898,269,503,783))$$
$$K_2(X):= F_{*\mathrm{B}}((F_{\mathrm{B}*}(X,Y)=(X,{}^2M_2)),{}^2M_1)= F_{\mathrm{B}*}(X,{}^2M_1{}^2M_2) \bmod q$$
$$= F_{*\mathrm{B}}(X,(733,331,767,905,1128,850,1284,716))$$
$$K_3(X):= F_{*\mathrm{B}}((F_{\mathrm{UB}}(X,Y)=(X,{}^3M_2)),{}^3M_1)= F_{*\mathrm{B}}(X,{}^3M_1{}^3M_2) \bmod q$$
$$= F_{*\mathrm{B}}(X,(879,235,340,999,1583,1143,1409,1785))$$
$${}^1K_{12}(X):= d_{11}K_1(X)+d_{12}\,K_2(X)+d_{13}\,K_3(X)$$
$$= F_{*\mathrm{B}}(X, d_{11}{}^1M_1{}^1M_2+ d_{12}{}^2M_1{}^2M_2+ d_{13}{}^3M_1{}^3M_2) \bmod q$$

$= F_{*\mathrm{B}}(X,(1583,92,552,908,1222,1632,1274,1306))$

${}^2K_{12}(X) := d_{21}K_1(X)+d_{22}\, K_2(X)+d_{23}\, K_3(X) \bmod q$

$= F_{*\mathrm{B}}(X,\, d_{21}{}^1M_1{}^1M_2+ d_{22}{}^2M_1{}^2M_2+ d_{23}{}^3M_1{}^3M_2) \bmod q$

$= F_{*\mathrm{B}}(X,(1553,1816,1422,1609,1284,766,682,1245))$

${}^3K_{12}(X) := d_{31}K_1(X)+d_{32}\, K_2(X)+d_{33}\, K_3(X) \bmod q$

$= F_{*\mathrm{B}}(X,\, d_{31}{}^1M_1{}^1M_2+ d_{32}{}^2M_1{}^2M_2+ d_{33}{}^3M_1{}^3M_2) \bmod q$

$= F_{*\mathrm{B}}(X,(1250,1253,669,500,482,1766,913,1677))$

$C^*(p_1p_2,\, X) := ({}^1K_{12}(X),\, {}^2K_{12}(X),\, {}^3K_{12}(X))$.

20) Data processing centre D sends $C^*(p_1+p,\, X)$, $C^*(p_1p_2,\, X)$ to user B.

21) User B receives $C^*(p_1+p_2,\, X)$, $C^*(p_1p_2,\, X)$ from Data processing centre D.

22) User B deciphers $C^*(p_1+p_2,\, X)$ to obtain p_1+p_2 as follows.

$F_{*\mathrm{B}}\,(X,{}^{\mathrm{e}}M) := \{{}^{\mathrm{e}}c_{ij}\}$ $(i,j=0,\ldots,7;\mathrm{e}=1,2,3)$,

$E_{yb}\,[F_{*\mathrm{B}}(E_{yb}{}^{-1}(\mathbf{1}),{}^{\mathrm{e}}M_1)+ F_{*\mathrm{B}}\,(E_{yb}{}^{-1}(\mathbf{1}),{}^{\mathrm{e}}M_2)] \bmod q$

$= E_{yb}\,(E_{yb}{}^{-1}\,({}^{\mathrm{e}}M_1\, E_{yb}\,(E_{yb}{}^{-1}\,(\mathbf{1}))))+ E_{yb}\,(E_{yb}{}^{-1}\,({}^{\mathrm{e}}M_2\, E_{yb}\,(E_{yb}{}^{-1}\,(\mathbf{1})))) \bmod q$

$= {}^{\mathrm{e}}M_1+{}^{\mathrm{e}}M_2 \bmod q$,

$p_{1+2}=\alpha_b[{}^1M_1+{}^1M_2]_0 +\beta_b[{}^2M_1+{}^2M_2]_0 \bmod q$,

$=191[1225]+217[670] \bmod q$,

$=889$

[verification]

$p_1+p_2 =740+149=889= p_{1+2} \bmod q$,

23) User B deciphers $C^*(p_1p_2,\, X)$ to obtain p_1p_2 as follows.

$E_{yb}\,({}^{\mathrm{e}}K_{12}\,(E_{yb}{}^{-1}\,(\mathbf{1})))$

$= E_{yb}\,(E_{yb}{}^{-1}\,((d_{\mathrm{e}1}{}^1M_1{}^1M_2+ d_{\mathrm{e}2}{}^2M_1{}^2M_2+ d_{\mathrm{e}3}{}^3M_1{}^3M_2)\, E_{yb}\,(E_{yb}{}^{-1}\,(\mathbf{1})))) \bmod q$

$= d_{\mathrm{e}1}{}^1M_1{}^1M_2+ d_{\mathrm{e}2}{}^2M_1{}^2M_2+ d_{\mathrm{e}3}{}^3M_1{}^3M_2$, $(\mathrm{e}=1,2,3)$

$p_{12}=\alpha[d_{11}{}^1M_1{}^1M_2+d_{12}{}^2M_1{}^2M_2+d_{13}{}^3M_1{}^3M_2]_0+\beta[d_{21}{}^1M_1{}^1M_2+d_{22}{}^2M_1{}^2M_2+d_{23}{}^3M_1{}^3M_2]_0 \bmod q$,

$=191[1583]+217[1553] \bmod q$,

$=193$

[verification]

$p_1p_2 =740*149=193 \bmod q = p_{12}$,

§7. Analysis of proposed scheme

Here we analyse the proposed fully homomorphic public-key encryption scheme described in section 6.

§7.1 Computing m_0, m_1, n_0 and n_1 from public key $h(X)$

We try to compute m_0, m_1, n_0 and n_1 from the coefficients of $h(X) = f^{m0}(g^{n0}(X))) + f^{m1}(g^{n1}(X)))$ mod $q = \{ h_{ij} \}$.

Let

$\{f^k{}_{ij}\}:=f^k(X)$ mod $q\in O[X]$, $\{f^1{}_{ij}\}:=f(X)$ mod $q\in O[X]$, $\{f^0{}_{ij}\}:= X$ mod $q\in O[X]$,

$\{g^k{}_{ij}\}:= g^k(X)$ mod $q\in O[X]$, $\{g^1{}_{ij}\}:= g(X)$ mod $q\in O[X]$, $\{g^0{}_{ij}\}:= X$ mod $q\in O[X]$,

$(k=2,3,\ldots)$.

$h(X) = f^{m0}(g^{n0}(X))) + f^{m1}(g^{n1}(X)))$ mod $q = \{ h_{ij} \}$.

Then we have

$g^k{}_{0j}= g_{00}g^{k-1}{}_{0j}+ g_{01}g^{k-1}{}_{1j}+\ldots+ g_{07}\, g^{k-1}{}_{7j}$ mod q,

$g^k{}_{1j}= g_{10}g^{k-1}{}_{0j}+ g_{11}g^{k-1}{}_{1j}+\ldots+ g_{17}\, g^{k-1}{}_{7j}$ mod q,

…. ….

$g^k{}_{7j}= g_{70}g^{k-1}{}_{0j}+ g_{71}g^{k-1}{}_{1j}+\ldots+ g_{77}\, g^{k-1}{}_{7j}$ mod q,

$(j=0,\ldots,7)$.

Let $\boldsymbol{g}^k{}_d:=(g^k{}_{0d}, g^k{}_{1d},\ldots, g^k{}_{7d})^{\mathrm{d}}\in R^{8\times1}$, $\boldsymbol{g}^0{}_d:=\mathbf{1}_d\in R^{8\times1}$, $\mathbf{G}:= (g_{ij})\in R^{8\times8}$, $(k=0,1,\ldots ;d=0,1,\ldots,7)$,

where

$\mathbf{1}_0=(1,0,..,0)^{\mathrm{t}}\in R^{8\times1}$, $\mathbf{1}_1=(0,1,0,..,0)^{\mathrm{t}}\in R^{8\times1},\ldots$, $\mathbf{1}_7=(0,..,0,1)^{\mathrm{t}}\in R^{8\times1}$,

We remember that the characteristic equation $\mathrm{CH}_g(t) =|\mathbf{G}\text{-}\mathbf{E}t|=0$ of $\mathbf{G}$ is irreducible equation of degree 8 and has different 8 eigenvalues $(\eta_0, \eta_1, \ldots,\eta_7)$.(See **§5.3**)

We have

$\boldsymbol{g}^k{}_d=\mathbf{G}\,\boldsymbol{g}^{k-1}{}_d= \mathbf{G}^{k-1}\,\boldsymbol{g}^1{}_d=\mathbf{G}^k\,\boldsymbol{g}^0{}_d=(\mathbf{P}_g{}^{-1}(\mathbf{D}_g)^k\,\mathbf{P}_g)\;\mathbf{1}_d$ mod q $\in R^{8\times1}$ $(k=0,1,\ldots ;d=0,1,\ldots,7)$

where $\mathbf{D}_g$ is a diagonal matrix($(\mathbf{D}_g)_{ii}=\eta_i$, $(i=0,\ldots,7)$ and $\mathbf{P}_g$ is a regular matrix.

We have

$g^k{}_{id}=u_{id0}(\eta_0)^k+ u_{id1}(\eta_1)^k +, \ldots,+ u_{id7}(\eta_7)^k$ mod q, $(i,d=0,\ldots,7{:}k=1,2,\ldots)$, $u_{idj}\in R$ $(j=0,\ldots,7)$.

As

$(\mathrm{CH}_g(\eta_i))^{q\wedge s}=(\mathrm{CH}_g(\eta_i{}^{q\wedge s}))=0$ mod q $(i=0,\ldots,7{:}s=1,2,\ldots)$,

$\eta_i{}^{q\wedge s}$ are also the solutions of $\mathrm{CH}_g(t)=0$ mod q ,that is, $\eta_i{}^{q\wedge s}\in\{\eta_0, \eta_1, \ldots,\eta_7\}(i=0,\ldots,7{:}s=1,2,\ldots)$.

Then we have k=q^8 at most such that $\eta_i^k = \eta_i$ mod q and $\eta_i^d \neq \eta_i$ mod q for integer 1<d<k (i=0,…,7).

That is,

$$\mathbf{G}^{q\wedge 8}= (\mathbf{P}_g^{-1}\mathbf{D}_g\mathbf{P}_g)^{q\wedge 8}=\mathbf{P}_g^{-1}(\mathbf{D}_g)^{q\wedge 8}\,\mathbf{P}_g= \mathbf{P}_g^{-1}\mathbf{D}_g\mathbf{P}_g =\mathbf{G} \text{ mod } q.$$

As the order of **G** is q^8 at most, we can select $f(X)$ such that no integer k exists that satisfies $f(X)=g^k(X)$ mod $q \in O[X]$ because the number of possible cases of $f(X)$ is q^64.

In the same manner we have

$$\boldsymbol{f}^k{}_d{:=}(f^k{}_{0d},f^k{}_{1d},\ldots,f^k{}_{7d})^{\mathrm{t}},\boldsymbol{f}^0{}_d{:=}\,\boldsymbol{g}^{\,n}{}_d,\ \mathbf{F}{:=}\,(f_{ij}),\ (k=0,1,\ldots\ ;d=0,1,\ldots,7),$$

$$\boldsymbol{f}^k{}_d=\mathbf{F}\,\boldsymbol{f}^{k\text{-}1}{}_d=\mathbf{F}^k\,\boldsymbol{f}^0{}_d= \mathbf{F}^k\,\boldsymbol{g}^{\,n}{}_d \text{ mod } q,\ (k=0,1,\ldots\ ;d=0,1,\ldots,7).$$

We remember that the characteristic equation CH$_f(t)$ =|**F**-**E**t|=0 of **F** is irreducible equation of degree 8 and has different 8 eigenvalues (ζ_0, ζ_1, …,ζ_7).(See **§5.3**).

We have

F= $\mathbf{P}_f^{-1}\mathbf{D}_f\mathbf{P}_f$ mod q where $\mathbf{D}_f$ is a diagonal matrix($(\mathbf{D}_f)_{ii}=\zeta_i$, i=0,…,7) and $\mathbf{P}_f$ is a regular matrix.

Then we have k=q^8 at most such that $\zeta_i^k=\zeta_i$ mod q and $\zeta_i^d \neq \zeta_i$ mod q for integer 1<d<k (i=0,…,7).

That is,

$$\mathbf{F}^{q\wedge 8}= (\mathbf{P}_f^{-1}\mathbf{D}_f\mathbf{P}_f)^{q\wedge 8}=\mathbf{P}_f^{-1}(\mathbf{D}_f)^{q\wedge 8}\,\mathbf{P}_f= \mathbf{P}_f^{-1}\mathbf{D}_f\mathbf{P}_f=\mathbf{F} \text{ mod } q.$$

$$\boldsymbol{f}^{n,k}{}_d=\mathbf{F}\,\boldsymbol{f}^{n,k\text{-}1}{}_d=\mathbf{F}^k\,\boldsymbol{f}^{n,0}{}_d= \mathbf{F}^k\,\boldsymbol{g}^n{}_d=(\,\mathbf{P}_f^{-1}(\mathbf{D}_f)^k\,\mathbf{P}_f)\,\boldsymbol{g}^n{}_d \text{ mod } q\ (k=0,1,\ldots\ ;d=0,1,\ldots,7).$$

Let **H**:= (h_{ij})$\in R^{8\times 8}$.

$$\mathbf{H}=(\boldsymbol{f}^{no,m0}{}_0,\boldsymbol{f}^{n0,m0}{}_1,\ldots,\boldsymbol{f}^{n0,m0}{}_7)+ (\boldsymbol{f}^{n1,m1}{}_0,\boldsymbol{f}^{n1,m1}{}_1,\ldots,\boldsymbol{f}^{n1,m1}{}_7)$$

Then h_{ij} is given as follows.

$$h_{ij}= \Sigma_{0=<u,v=<7}\, r_{0uvij}(\zeta_u)^{m0}(\eta_v)^{n0} +\Sigma_{0=<u,v=<7}\, r_{1uvij}(\zeta_u)^{m1}(\eta_v)^{n1} \text{ mod } q;\ m_0,m_1,n_0,n_1 \in \boldsymbol{Fq*};$$

$$r_{0uvij},\ r_{1uvij} \in R\ (u,v,i,j=0,\ldots,7) \quad \text{(A)}.$$

We notice that there does not exist the integer k such that $(\eta_v)^k=\zeta_u$ mod q (u,v∈{0,1,….,7},k∈Z).

h_{ij} (i,j=0,…,7) consists of the linear combination of 128(=64*2) terms such as $(\zeta_u)^{m0}(\eta_v)^{n0}$ and $(\zeta_u)^{m1}(\eta_v)^{n1}$.

As the above simultaneous equation (A) has only 64 equations, it is thought that it is difficult to obtain each value of the term such as $(\zeta_u)^{m0}(\eta_v)^{n0}$ or $(\zeta_u)^{m1}(\eta_v)^{n1}$ (u,v=0,1,….,7).

It is thought that it is difficult to obtain m_0, m_1, n_0 and $n_1 \in \boldsymbol{Fq^*}$ from $\{h_{ij}\}(i,j=0,\ldots,7)$.

§7.2 Computing medium text ^1M,^2M,^3M from coefficients of ciphertext $F_{\mathrm{AB}}(X,M)$

Ciphertext $C(p_n,X)$:=$(F_{\mathrm{AB}}(X,{}^1M_n), F_{\mathrm{AB}}(X,{}^2M_n), F_{\mathrm{AB}}(X,{}^3M_n))$ is given such that

$$
\begin{aligned}
F_{\mathrm{AB}}(X,{}^{\mathrm{k}}M_n) &= E_{ab}^{-1}({}^{\mathrm{k}}M_nE_{ab}(X)) \bmod q \in O[X] \\
&= ({}^{\mathrm{k}}c_{n00}x_0+{}^{\mathrm{k}}c_{n01}x_1+\ldots+{}^{\mathrm{k}}c_{n07}x_7, \\
&\quad\ {}^{\mathrm{k}}c_{n10}x_0+{}^{\mathrm{k}}c_{n11}x_1+\ldots+{}^{\mathrm{k}}c_{n17}x_7, \\
&\quad\ \ldots\ldots \qquad \ldots\ldots \\
&\quad\ {}^{\mathrm{k}}c_{n70}x_0+{}^{\mathrm{k}}c_{n71}x_1+\ldots+{}^{\mathrm{k}}c_{n77}x_7) \bmod q, \\
&= \{{}^{\mathrm{k}}c_{nij}\}(i,j=0,\ldots,7;n=1,2,\ldots;\mathrm{k}=1,2,3)
\end{aligned}
$$

with ${}^{\mathrm{k}}c_{nij} \in R$ $(i,j,n=1,2,\ldots;\mathrm{k}=1,2,3)$,

where

$$
\begin{aligned}
{}^1M_n &= {}^1k\,u_n\mathbf{1}+{}^1lv_nG+{}^1w_nGH+{}^1z_nHG \bmod q \in O, \\
{}^2M_n &= {}^2k\,u_n\mathbf{1}+{}^2lv_nG+{}^2w_nGH+{}^2z_nHG \bmod q \in O, \\
{}^3M_n &= {}^3k\,u_n\mathbf{1}+{}^3lv_nG+{}^3w_nGH+{}^3z_nHG \bmod q \in O, \\
& u_n,v_n,{}^1w_n,{}^1z_n,{}^2w_n,{}^2z_n,{}^3w_n,{}^3z_n \in R\ (n=0,\ldots,7).
\end{aligned}
$$

$F_{\mathrm{AB}}(X,Y)$:= $\{\gamma_{ijh}\}(i,j,h=0,\ldots,7)$ is given such that

$$
\begin{aligned}
F_{\mathrm{AB}}(X,Y) &= E_{ab}^{-1}(Y\,E_{ab}(X)) \bmod q \in O[X,Y] \\
&= (\gamma_{000}x_0y_0+\gamma_{001}x_0y_1+\ldots+\gamma_{077}x_7y_7, \\
&\quad\ \gamma_{100}x_0y_0+\gamma_{101}x_0y_1+\ldots+\gamma_{177}x_7y_7, \\
&\quad\ \ldots\ldots \qquad \ldots\ldots \\
&\quad\ \gamma_{700}x_0y_0+\gamma_{701}x_0y_1+\ldots+\gamma_{777}x_7y_7) \bmod q, \\
&= \{\gamma_{ijh}\}(i,j,h=0,\ldots,7)
\end{aligned}
$$

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

Anyone except user A and user B does not know $\{\gamma_{ijh}\}$ $(i,j,h=0,\ldots,7)$ which is a common enciphering function between user A and user B. Here we try to find ${}^{\mathrm{k}}M_n=({}^{\mathrm{k}}m_{n0},\ldots,{}^{\mathrm{k}}m_{n7})$ from $\{{}^{\mathrm{k}}c_{nij}\}(i,j=0,\ldots,7;n=1,2,3;\mathrm{k}=1,2,3)$ in condition that $\gamma_{ijh}(i,j,h=0,\ldots,7)$ are unknown parameters. We have the following simultaneous equations from $F_{\mathrm{AB}}(X, Y)$ and $F_{\mathrm{AB}}(X, {}^{\mathrm{k}}M_n)$ where $\gamma_{ijh}(i,j,h=0,\ldots,7)$ and $({}^{\mathrm{k}}m_{n0},\ldots,{}^{\mathrm{k}}m_{n7})$ are unknown variables.

$$\left\{\begin{array}{l} \gamma_{i00}{}^{\mathrm{k}}m_{n0}+\gamma_{i01}{}^{\mathrm{k}}m_{n1}+\ldots+\gamma_{i07}{}^{\mathrm{k}}m_{n7}={}^{\mathrm{k}}c_{ni0} \bmod q \\ \gamma_{i10}{}^{\mathrm{k}}m_{n0}+\gamma_{i11}{}^{\mathrm{k}}m_{n1}+\ldots+\gamma_{i17}{}^{\mathrm{k}}m_{n7}={}^{\mathrm{k}}c_{ni1} \bmod q \\ \qquad\qquad\ldots \\ \qquad\qquad\ldots \\ \gamma_{i70}{}^{\mathrm{k}}m_{n0}+\gamma_{i71}{}^{\mathrm{k}}m_{n1}+\ldots+\gamma_{i77}{}^{\mathrm{k}}m_{n7}={}^{\mathrm{k}}c_{ni7} \bmod q \end{array}\right.$$

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

For ${}^{\mathrm{k}}M_n$ $(n=1,2,3;\mathrm{k}=1,2,3)$ we obtain the same equations, the number of which is 576(=64*3*3). We also obtain 8 equations such as

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

$$=|{}^{\mathrm{k}}M_n|^2=({}^{\mathrm{k}}m_{n0})^2+({}^{\mathrm{k}}m_{n1})^2+\ldots+({}^{\mathrm{k}}m_{n7})^2 \bmod q,(n=1,\ldots,4;\mathrm{k}=1,2,3).$$

The number of unknown variables ${}^{\mathrm{k}}M_n(n=1,2,3;\mathrm{k}=1,2,3)$ and γ_{ijh} $(i,j,h=0,\ldots,7)$ is 584(=8*3*3+512). The number of equations is 585(=576+9). Then the complexity G_{reb} required for solving above simultaneous quadratic algebraic equations by using Gröbner basis [3] is given such as

$$G_{reb}=({}_{584+dreg}C_{dreg})^{w}=({}_{876}\mathrm{C}_{292})^{\mathrm{w}}=2^{1910}>>2^{80},$$

where w=2.39, and

$$d_{reg}=292(=585*(2-1)/2-0\sqrt{}(585*(4-1)/6)).$$

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

§7.3Attack by using the ciphertexts of *p* and *-p*

I show that we cannot easily distinguish the ciphertexts of $-p$ by using the ciphertext $C(p,X)$

$=(F_{\mathrm{AB}}(X, {}^{1}M), F_{\mathrm{AB}}(X, {}^{2}M), F_{\mathrm{AB}}(X, {}^{3}M))$. We try to attack by using “*p* and *-p* attack”.

Given the ciphertext $C(p, X)=(F_{\mathrm{AB}}(X,{}^{1}M), F_{\mathrm{AB}}(X, {}^{2}M), F_{\mathrm{AB}}(X,{}^{3}M))$, we try to find the ciphertext $C(p_{-}, X)$ corresponding to the plaintext $p_{-}=-p \bmod q$

where

$${}^{1}M:={}^{1}ku\,\mathbf{1}+{}^{1}lvG+{}^{1}wGH+{}^{1}zHG \bmod q\in O,$$

$^2M{:=}{}^2ku\,\mathbf{1}+{}^2lvG+{}^2wGH+{}^2zHG \bmod q\in O,$

$^3M{:=}{}^3ku\,\mathbf{1}+{}^3lvG+{}^3wGH+{}^3zHG \bmod q\in O,$

$p{:=}\,su+tv \bmod q\in R$

$=\alpha[{}^1M]_0+\beta[{}^2M]_0 \bmod q,$

where

$(\alpha\,{}^1k+\beta\,{}^2k)=s \bmod q,$

$(\alpha\,{}^1lg_0+\beta\,{}^2lg_0)=t \bmod q.$

Let

$^1N{:=}{}^1ku_-\,\mathbf{1}+{}^1lv_-G+{}^1w_-GH+{}^1z_-HG \bmod q\in O,$

$^2N{:=}{}^2ku_-\,\mathbf{1}+{}^2lv_-G+{}^2w_-GH+{}^2z_-HG \bmod q\in O,$

$^3N{:=}{}^3ku_-\,\mathbf{1}+{}^3lv_-G+{}^3w_-GH+{}^3z_-HG \bmod q\in O,$

$p_-{:=}-p=su_-+tv_- \bmod q\in R,$

u-$,v_-,{}^1w_-,\ {}^1z_-\,,{}^2w_-\,,{}^2z_-\in R.$

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

$^1M+{}^1N={}^1ku\,\mathbf{1}+{}^1lvG+{}^1wGH+{}^1zHG+{}^1ku_-\,\mathbf{1}+{}^1lv_-G+{}^1w_-GH+{}^1z_-HG \bmod q$

$={}^1k(u+u_-)\mathbf{1}+{}^1l\,(v+v_-)G+({}^1w+{}^1w_-)GH+({}^1z+{}^1z_-)HG \bmod q.$

As $p+p_-=s(u+u_-)+t(v+v_-)=0 \bmod q$, we have

$u+u_-=-(v+v_-)\,t/s \bmod q.$

$^1M+{}^1N$

$=-(v+v_-)\,{}^1k\,t/s\,\mathbf{1}+{}^1l\,(v+v_-)G+({}^1w+{}^1w_-)GH+({}^1z+{}^1z_-)HG \bmod q$

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

Then we have

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

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

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

Next we calculate $|F_{\mathrm{AB}}(\mathbf{1}, {}^{j}M)+ F_{\mathrm{AB}}(\mathbf{1}, {}^{k}N)|^2$ where $\mathrm{j,k} \in \{1,2,3\}$.

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

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

$=|-(v+v_{-})\,{}^{1}k\,t/s\,\mathbf{1} +{}^{1}l\,(v+ v_{-})G +({}^{1}w+{}^{1}w_{-})GH+({}^{1}z+{}^{1}z_{-})HG\,|^2 \bmod q$

From (23a)

$=-(v+v_{-})\,{}^{1}k\,t/s[-(v+v_{-})\,{}^{1}k\,t/s +2\,g_0\,({}^{1}l\,(v+ v_{-}))] \bmod q$

$=-(v+v_{-})^2\,{}^{1}k\,t/s[-{}^{1}k\,t/s +2\,g_0\,] \bmod q$

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

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

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

$=|-(v-v_{-})\,{}^{1}k\,t/s\,\mathbf{1} +{}^{1}l\,(v- v_{-})G +({}^{1}w-{}^{1}w_{-})GH+({}^{1}z-{}^{1}z_{-})HG|^2 \bmod q$

$=-(v-v_{-})\,{}^{1}k\,t/s[-(v-v_{-})\,{}^{1}k\,t/s +2\,g_0\,({}^{1}l\,(v- v_{-}))] \bmod q$

$=-(v-v_{-})^2\,{}^{1}k\,t/s[-{}^{1}k\,t/s +2\,g_0\,] \bmod q$

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

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

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

${}^{1}M+{}^{2}N={}^{1}ku\,\mathbf{1}+{}^{1}lvG+{}^{1}wGH+{}^{1}zHG +{}^{2}ku_{-}\,\mathbf{1}+{}^{2}lv_{-}G+{}^{2}w_{-}GH+{}^{2}z_{-}HG \bmod q$

$=|({}^{1}ku +{}^{2}ku_{-}\,)\mathbf{1} + ({}^{1}l\,v+ {}^{2}l\,v_{-})G +({}^{1}w+{}^{2}w_{-})GH+({}^{1}z+{}^{2}z_{-})HG\,|^2 \bmod q$

$=|(-{}^{1}k(u_{-} +(v+v_{-}\,)\,t/s) +{}^{2}ku_{-}\,)\mathbf{1} + ({}^{1}l\,v+ {}^{2}l\,v_{-})G +({}^{1}w+{}^{2}w_{-})GH+({}^{1}z+{}^{2}z_{-})HG\,|^2 \bmod q$

$=(-{}^{1}k(u_{-} +(v+v_{-}\,)\,t/s) +{}^{2}ku_{-}\,)\,[(-{}^{1}k(u_{-} +(v+v_{-}\,)\,t/s) +{}^{2}ku_{-}\,)+ 2\,g_0\,({}^{1}l\,v+ {}^{2}l\,v_{-})] \bmod q$

$= (u_{-}\,(-{}^{1}k + {}^{2}k\,) -{}^{1}k\,(v+v_{-}\,)\,t/s)\,[(u_{-}\,(-{}^{1}k + {}^{2}k\,) -{}^{1}k\,(v+v_{-}\,)\,t/s)+ 2\,g_0\,({}^{1}l\,v+ {}^{2}l\,v_{-})] \bmod q$

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

…. ….

…. ….

It is said that the attack by using "*p* and -*p* attack" is not efficient. Then we cannot easily distinguish the ciphertexts of -*p* by using the ciphertext $C(p,X)=(F_{\mathrm{AB}}(X,{}^{1}M),F_{\mathrm{AB}}(X,{}^{2}M),F_{\mathrm{AB}}(X, {}^{3}M))$.

§7.4 Attack by using α and β

We try to obtain the plaintext p directly from the ciphertext $C(p,X)$ =($F_{\mathrm{AB}}(X, {}^1M)$, $F_{\mathrm{AB}}(X, {}^2M)$, $F_{\mathrm{AB}}(X, {}^3M)$) by using α and β where α and β satisfy the following equation,

$$(\alpha\, {}^1k+\beta\, {}^2k)=s \bmod q,$$

$$(\alpha\, {}^1lg_0+\beta\, {}^2lg_0)=t \bmod q.$$

If $E_{ba}(X)$ is known, we can obtain the plaintext p directly from the ciphertext $C(p,X)$ as follows.

$$E_{ba}\,(F_{\mathrm{AB}}(E_{ba}{}^{-1}\,(\mathbf{1}),{}^{\mathrm{e}}M))$$

$$= E_{ba}\,(E_{ab}{}^{-1}\,({}^{\mathrm{e}}M\, E_{ab}\,(E_{ba}{}^{-1}\,(\mathbf{1})))) \bmod q$$

$$={}^{\mathrm{e}}M, (\mathrm{e}=1,2,3),$$

$${}^1M_1:={}^1ku_1\,\mathbf{1}+{}^1lv_1G+{}^1w_1GH+{}^1z_1HG \bmod q\in O,$$

$${}^2M_1:={}^2ku_1\,\mathbf{1}+{}^2lv_1G+{}^2w_1GH+{}^2z_1HG \bmod q\in O,$$

$${}^3M_1:={}^3ku_1\,\mathbf{1}+{}^3lv_1G+{}^3w_1GH+{}^3z_1HG \bmod q\in O,$$

$$p=\alpha[{}^1M]_0+\beta[{}^2M]_0 \bmod q\ (= su+tv \bmod q).$$

But the adversary $\mathrm{A_d}$ does not know $E_{ba}(X)$. Though he knows α and β, he cannot obtain the plaintext p directly from the ciphertext $C(p,X)$.

Even if he obtains u and v, he cannot obtain the plaintext p without knowing s and t where

$$(\alpha\, {}^1k+\beta\, {}^2k)=s \bmod q,(\ {}^1k,\ {}^2k \text{ are secret})$$

$$(\alpha\, {}^1lg_0+\beta\, {}^2lg_0)=t \bmod q\ (\ {}^1l,\ {}^2l,g_0 \text{ are secret}).$$

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

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

In section **7.1** it is shown that the size of order l of matrices **F**,**G** is $O(q^8)$. The complexity required for obtaining the discrete logarithm of matrices $\mathbf{F}^m$, $\mathbf{G}^{\mathrm{n}}\in R^{8\times 8}$ is $O(sqrt(l))= O(q^4)$ [21]. We select the size of q such that $\mathrm{O}(sqrt(l))$ is larger than 2^{2000}. Then we need to select modulus q such as $O\,(q)= 2^{256}$.

We calculate the size of the parameter and the complexity required for $F_{\mathrm{AB}}(X,M)$.

1) The size of $f_{ij}\in R(i,j=0,\ldots,7)$ which are the coefficients of elements in $f(X) \bmod q\in O[X]$ is $(64)(\log_2 q)$ bits =17kbits,

2) The size of $h_{ij}\in R(i,j=0,\ldots,7)$ which are the coefficients of elements in $h(X)$ mod $q\in O[X]$ is $(64)(\log_2 q)$ bits =17kbits, and the size of system parameters $(q,G,H;f(X),g(X))$ is as large as 38kbits.

3) The complexity G_1 to obtain $f^{-1}(X)$ from $f(X)$ by using Gaussian elimination is

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

$=2101*(\log_2 q)^2+8*(\log_2 q)^3=2^{18}$bit-operations,

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

4) The complexity G_2 to obtain $h(X)=f^{m0}(g^{n0}(X))+f^{m1}(g^{n1}(X))$ mod q from $f(X),g(X)$, m_0, n_0, m_1 and n_1 is $(2*512+3*2*(\log_2 q^8)*512)(\log_2 q)^2=2^{39}$ bit-operations.

5) The size of $F_{\mathrm{AB}}(X,M)=E_{ab}{}^{-1}(YE_{ab}(X))\in O[X,Y]$ is $(512)(\log_2 q)$ bits =128 kbits.

6) The complexity G_3 to obtain $E_{ab}(X)=f^{na0}(h_b(g^{na0}(X)))+f^{na1}(h_b(g^{na1}(X)))$ mod q from $h_b(X)$, $f^{na0}(X)$, $f^{na1}(X)$,$g^{na0}(X)$ and $g^{na1}(X)$ is

$(2*2*512)*(\log_2 q)^2=2^{27}$bit-operations.

7) The complexity G_4 to obtain $F_{\mathrm{AB}}(X)=E_{ab}{}^{-1}(YE_{ab}(X))\in O[X,Y]$ from $E_{ab}(X)$ is

$512*8*(\log_2 q)^2+G_1=2^{28}+2^{18}=2^{29}$ bit-operations.

8) The complexity G_5 for calculating ${}^1M,{}^2M$ and ${}^3M$ from plaintext p is $3*(26)*(\log_2 q)^2=2^{23}$ bit-operations.

9) The complexity G_{encipher} for enciphering to calculate $C(p,X)=(F_{\mathrm{AB}}(X,{}^1M), F_{\mathrm{AB}}(X,{}^2M)$, $F_{\mathrm{AB}}(X,{}^3M))$ from $F_{\mathrm{AB}}(X,Y)$, ${}^1M$,${}^2M$ and ${}^3M$ is $3*(64*8)*(\log_2 q)^2=2^{27}$ bit-operations.

The size of $C(p,X)=(F_{\mathrm{AB}}(X,{}^1M), F_{\mathrm{AB}}(X,{}^2M), F_{\mathrm{AB}}(X,{}^3M))$ is $(64*3)*(\log_2 q)$ bits =48kbits.

We notice that the complexity $(G_{\mathrm{encipher}}+G_5)$ required for enciphering every plaintext p is only 2^{27} bit-operations.

10) The complexity G_{decipher} required for deciphering from $F_{\mathrm{AB}}(X,{}^1M)$,$F_{\mathrm{AB}}(X,{}^2M)$,$F_{\mathrm{AB}}(X,{}^3M)$, $E_{ba}(X)$and $E_{ba}{}^{-1}(X)$ is given as follows.

As

$F_{\mathrm{AB}}(X,{}^{\mathrm{e}}M):=\{{}^{\mathrm{e}}c_{ij}\}$ $(i,j=0,\ldots,7;\mathrm{e}=1,2,3)$,

$E_{ba}(F_{\mathrm{AB}}(E_{ba}{}^{-1}(\mathbf{1}),{}^{\mathrm{e}}M))$

$=E_{ba}(E_{ab}{}^{-1}({}^{\mathrm{e}}M\,E_{ab}(E_{ba}{}^{-1}(\mathbf{1}))))$ mod q

$={}^{e}M,$

$p=\alpha[{}^{1}M]_0 +\beta[{}^{2}M]_0 \bmod q \in R,$

the complexity G_{decipher} is $(64*2+2)(\log_2 q)^2= 2^{23}$ bit-operations.

11) The complexity G_{multiply} required for generating $C(p_1p_2,X)$ from $C(p_1,X)$ and $C(p_2,X)$ is given as follows.

As

$C(p_1p_2,X) = (F_{AB}(X,{}^{1}M_{12}),F_{AB}(X,{}^{2}M_{12}) ,F_{AB}(X,{}^{3}M_{12})),$

$K_1(X)= F_{AB}(X, {}^{1}M_1{}^{1}M_2) = F_{AB}(F_{AB}(X,{}^{1}M_2),{}^{1}M_1) \bmod q,$

$K_2(X)= F_{AB}(X, {}^{2}M_1{}^{2}M_2) = F_{AB}(F_{AB}(X,{}^{2}M_2),{}^{2}M_1)\bmod q,$

$K_3(X)= F_{AB}(X, {}^{3}M_1{}^{3}M_2) = K_{11}((F_{AB}((X,{}^{3}M_2),{}^{3}M_1) \bmod q,$

$F_{AB}(X, {}^{1}M_{12}) = d_{11}\, K_1(X)+ d_{12}\, K_2(X)+ d_{13}\, K_3(X) \bmod q,$

$F_{AB}(X, {}^{2}M_{12}) = d_{21}\, K_1(X)+ d_{22}\, K_2(X)+ d_{23}\, K_3(X) \bmod q,$

$F_{AB}(X, {}^{3}M_{12}) = d_{31}\, K_1(X)+ d_{32}\, K_2(X)+ d_{33}\, K_3(X)\bmod q,$

the complexity G_{multiply} is $(512*3+64*3*3)(\log_2 q)^2= 2^{27}$ bit-operations.

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

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

where the size of modulus n is 2048bits.

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

§9. Conclusion

We proposed the fully homomorphic public-key encryption scheme with the recursive ciphertext based on multivariate discrete logarithm assumption. Our scheme requires not too large complexity to encipher and decipher. It was shown that our scheme is immune from "*p* and -*p* attack"**.**

As theoretically a part of the system parameter G and H needs not to be published, it is possible that G and H belong to user's secret keys. In this case the system parameter is $[q, f(x), g(x)]$.

User A is also able to adopt the public function $h_a(X)$ such that

$$h_a(X)=f^{na0}(g^{na0}(X))+f^{na1}(g^{na1}(X))+\ldots+f^{nak}(g^{nak}(X)) \bmod q=\{h_{aij}\}$$

for an integer k. In this case user B generates the common enciphering function $F_{\mathrm{BA}}(X,Y)$ between user B and user A such that

$$E_{ba}(X):=f^{nb0}(h_a(g^{nb0}(X)))+f^{nb1}(h_a(g^{nb1}(X)))+\ldots+f^{nbk}(h_a(g^{nbk}(X))) \bmod q$$

$$F_{\mathrm{BA}}(X,Y):=E_{ba}{}^{-1}(YE_{ba}(X)) \bmod q \in O[X,Y].$$

§10.Acknowledgments

This paper is the revised chapter 4 of my work ” Fully Homomorphic Public-Key Encryption with Three Ciphertexts”, published in February, 2017 which was published by LAP LAMBERT Academic Publishing, Saarbrücken/Germany [22]. I thank for the publisher (Lambert Academic, Germany) for kindly providing an opportunity to accomplish the task.

Bibliography

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

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

[3] 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.

[4] R. L. Rivest, L. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, 1978.

[5] http://www-03.ibm.com/press/us/en/pressrelease/27840.wss

[6] Michael Cooney (2009-06-25). ""IBM touts encryption innovation". Computer World. Retrieved 2009-07-14.

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

[8] Craig Gentry. "Computing Arbitrary Functions of Encrypted Data". Association for Computing Machinery.

[9] 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.

[10] Bram Cohen. "Simple Public Key Encryption".
Available at http://en.wikipedia.org/wiki/Cohen's_cryptosystem .

[11] Mashiro Yagisawa,” FHPKE with Zero Norm Noises based on DLA&CDH”, Cryptology ePrint Archive, Report 2016/738, 2016. http://eprint.iacr.org/.

[12] Mashiro Yagisawa," Fully Homomorphic Public-Key Encryption with Two Ciphertexts based on Discrete Logarithm Problem", Cryptology ePrint Archive, Report 2016/054, 2016. http://eprint.iacr.org/.

[13] 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/.

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

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

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

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

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

[19] Mashiro Yagisawa," Fully Homomorphic Encryption with Isotropic Elements", Cryptology ePrint Archive, Report 2016/462, 2016. http://eprint.iacr.org/.

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

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

[22] Masahiro, Y. (2017). Fully Homomorphic Public-Key Encryption with Three Ciphertexts, Saarbrücken / Germany : LAP LAMBERT Academic Publishing.

[23] Mashiro Yagisawa," FHE with Recursive Ciphertext", Cryptology ePrint Archive, Report 2017/198, 2017. http://eprint.iacr.org/.

Appendix A:

```
**Octinv**($A$) ---------------------------------------------------------------------------------------
S ← $a_0^2+a_1^2+\ldots+a_7^2$ mod $q$.
% $S^{-1}$ mod $q$
q[1] ← q div S ;% integer part of q/S
Res[1] ← q mod S ;% Residue
k ←1
q[0] ← q
Res[0] ← S
while Res[k]  $\neq$  0
begin
    k← k + 1
    q[k] ← Res[k−2] div Res[k−1]
    Res[k] ← Res[k−2] mod Res[k−1]
end
Q [k−1] ← (-1)*q[k−1]
L[ k−1] ← 1
i ← k−1
while    i > 1
begin
    Q[ i−1] ← (-1)*Q[ i] *q[i−1] + L[ i]
    L[ i−1 ] ← Q[ i ]
    i← i−1
end

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

Appendix B:

Theorem 1

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

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

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

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

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

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

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

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

(*Proof*:)

We use mathematical induction method.

[step 1]

When n=1, (8) holds because

$$a_{10}=a_{00}\,a_{10}-b_0N=a_{10} \bmod q.$$

(9) holds because

$$b_1=a_{00}+b_0a_{10}=a_{00}=1 \bmod q.$$

(10) holds because

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

[step 2]

When $n=k$,

If it holds that

$$a_{k0}=a_{k-1,0}\,a_{10}-b_{k-1}N \bmod q\ ,(k=2,3,4,\ldots)\ ,$$
$$b_k=a_{k-1,0}+b_{k-1}a_{10} \bmod q,$$
$$a_{kj}=b_ka_{1j} \bmod q\ ,(j=1,2,\ldots,7),$$

from (9)

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

then

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

as was required. q.e.d.

Appendix C:

Theorem 2

For an element A=(a_{10},a_{11},…,a_{17})∈R,

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

where

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

(*Proof*:)

From (8) and (9) it comes that

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

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

Because - N≠0 mod q is quadratic non-residue of prime q,

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

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

$$t^2\text{-}2a_{10}t+a_{10}^2+N=0.$$
$$\alpha = \mathrm{a}_{10} + \sqrt{-N}\ \ over\ \ Fq[\alpha],$$
$$\beta = \mathrm{a}_{10} - \sqrt{-N}\ \ over\ Fq[\alpha].$$

We can calculate β^{q^2} as follows.

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

In the same manner we obtain

$$\alpha^{q^2} = \alpha \ \ over \ \ Fq[\alpha].$$
$$a_{q^2,0} = (\beta^{q^2}(\mathrm{a}_{10} - \alpha) + (\beta - \mathrm{a}_{10})\alpha^{q^2})/(\beta - \alpha)$$
$$=(\beta(a_{10}-\alpha) + (\beta- a_{10})\alpha)/(\beta- \alpha)=a_{10} \ \ \mathrm{mod}\, q.$$
$$b_{q^2} = (\beta^{q^2} - \alpha^{q^2})/(\beta - \alpha) = 1 \ \ \mathrm{mod}\, q.$$

Then we obtain

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

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

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

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

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

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

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

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

Then we have

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

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

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

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

Then we have

$$a^{q} =(a_{q0}, b_{q}a_{11},\ldots,b_{\mathrm{q}}a_{17})$$

$$=(a_{10}, a_{11},\ldots,a_{17})=a \ \mathrm{mod}\, q.$$

We therefore arrive at the equation such as

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

where

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

as was required. q.e.d.

We notice that
in case that N=0 mod q

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

From (8)

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

then we have

$$a_{n0}= a_{10}{}^{n} \bmod q ,(n=1,2,...).$$

$$a_{q0}= a_{10}{}^{q}= a_{10} \bmod q.$$

From (9)

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

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

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

… …

$$= (n\text{-}1)a_{10}{}^{n\text{-}1}+ b_1a_{10}{}^{\mathrm{n\text{-}1}} \bmod q$$

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

Then we have

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

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

Appendix D:

Lemma 1

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

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

(*Proof*:)

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

$AB \bmod q$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Similarly we have

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

Then

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

Appendix E:

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

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

Appendix F:

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

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

Appendix G:

Theorem 5

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

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

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

$$G=(g_0,g_1,\ldots,g_7),\ g_j \in R\ (j=0,1,\ldots,7),$$

$$H=(h_0,h_1,\ldots,h_7),\ h_j \in R\ (j=0,1,\ldots,7),$$

where

$$h_0=0 \bmod q,$$

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

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

and

$$g_1h_1+ g_2h_2+g_3h_3+_4h_4+ g_5h_5+g_6h_6+g_7h_7=0 \bmod q.$$

A,B satisfy the following equations.

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

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

(*Proof:*)

$$GH \bmod q$$

$$= (\ g_0h_0 - g_1h_1- g_2h_2- g_3h_3-g_4h_4- g_5h_5-g_6h_6-g_7h_7 \bmod q,$$

$$g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3 \bmod q,$$

$$g_0h_2-g_1h_4+g_2h_0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6 \bmod q,$$

$$g_0h_3-g_1h_7-g_2h_5+g_3h_0+g_4h_6+g_5h_2-g_6h_4+g_7h_1 \bmod q,$$

$$g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+g_4h_0+g_5h_7+ g_6h_3 -g_7h_5 \bmod q,$$

$$g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+g_5h_0+g_6h_1+g_7h_4 \bmod q,$$

$$g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+g_6h_0 +g_7h_2 \bmod q,$$

$$g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+g_7h_0 \bmod q)$$

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

$$= (g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7)\, g_0$$

$$-(g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3)\, g_1$$

$$-(g_0h_2-g_1h_4+g_2h_0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6)\, g_2$$

$$-(g_0h_3-g_1h_7-g_2h_5+g_3h_0+g_4h_6+g_5h_2-g_6h_4+g_7h_1)\, g_3$$

$$-(g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+g_4h_0+g_5h_7+ g_6h_3 -g_7h_5)\, g_{4,}$$

$$-(g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+g_5h_0+g_6h_1+g_7h_4)\, g_5$$

$$-(g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+g_6h_0 +g_7h_2)\, g_{6,}$$

$$-(g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+g_7h_0)\, g_7) \bmod q$$

As

$$h_0=0 \bmod q\,,$$

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

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

and

$$g_1h_1+ g_2h_2+g_3h_3+{}_4h_4+ g_5h_5+g_6h_6+g_7h_7=0 \bmod q,$$

we have

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

$$=(g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7)\, g_0$$

$$-(g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3)\, g_1$$

$$-(g_0h_2-g_1h_4+g_2h_0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6)\, g_2$$

$$-(g_0h_3-g_1h_7-g_2h_5+g_3h_0+g_4h_6+g_5h_2-g_6h_4+g_7h_1)\, g_3$$

$$-(g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+g_4h_0+g_5h_7+ g_6h_3 -g_7h_5)\, g_{4,}$$

$$-(g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+g_5h_0+g_6h_1+g_7h_4)\, g_5$$

$$-(g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+g_6h_0 +g_7h_2)\, g_6$$

$$-(g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+g_7h_0)\, g_7$$

$$=(g_00- 0)\, g_0$$

$- g_0 (g_1 h_1+g_2h_2+g_3h_3+g_4h_4+g_5h_5+g_6h_6+g_7h_7)$

$- g_1(g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3-g_2h_4-g_3h_7+g_4h_2 -g_5h_6+g_6h_5+g_7h_3)$

$- g_2 (g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6-g_3h_5-g_4h_1+g_5h_3-g_6h_7+g_7h_6)$

$- g_3 (g_4h_6+g_5h_2-g_6h_4+g_7h_1-g_4h_6 -g_5h_2+ g_6h_4-g_7h_1)$

$- g_4 (g_5h_7+ g_6h_3 -g_7h_5-g_5h_7- g_6h_3+g_7h_5)$

$- g_5 (g_6h_1+g_7h_4-g_6h_1-g_7h_4)$

$-(g_7h_2) g_6-(-g_6h_2) g_7$

$=0 \bmod q,$

$[(GH)G]_1 \bmod q$

$= \quad (g_0h_0 - g_1h_1- g_2h_2- g_3h_3-g_4h_4- g_5h_5-g_6h_6-g_7h_7)g_1$

$+(g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3)g_0$

$+(g_0h_2-g_1h_4+g_2h_0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6)g_4$

$+(g_0h_3-g_1h_7-g_2h_5+g_3h_0+g_4h_6+g_5h_2-g_6h_4+g_7h_1)g_7$

$-(g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+g_4h_0+g_5h_7+ g_6h_3 -g_7h_5)g_2$

$+(g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+g_5h_0+g_6h_1+g_7h_4)g_6$

$-(g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+g_6h_0 +g_7h_2)g_5$

$-(g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+g_7h_0)g_3$

$= (g_0 0-g_1h_1- g_2h_2- g_3h_3-g_4h_4- g_5h_5-g_6h_6-g_7h_7)g_1$

$+2(g_1h_1+g_2h_2+g_3h_3+g_4h_4+g_5h_5+g_6h_6+g_7h_7)g_1$

$+(g_0h_1+0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3)g_0$

$+(g_0h_2-g_1h_4+0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6)g_4$

$+(g_0h_3-g_1h_7-g_2h_5+0+g_4h_6+g_5h_2-g_6h_4+g_7h_1)g_7$

$-(g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+0+g_5h_7+ g_6h_3 -g_7h_5)g_2$

$+(g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+0+g_6h_1+g_7h_4)g_6$

$-(g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+0 +g_7h_2)g_5$

$-(g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+0)g_3$

$= \quad h_1 (g_1^2+g_0^2+g_4^2+g_7^2+g_2^2+g_6^2+g_5^2+g_3^2)$

$+ h_2 (g_2g_1-g_4g_0+g_0g_4+g_5g_7-g_1g_2-g_3g_6-g_7g_5+g_6g_3)$

$+ h_3 (g_3g_1 -g_7g_0 -g_5g_4+g_0g_7 -g_6g_2+g_2g_6+g_4h_5- g_1g_3)$

$+ h_4 (g_4g_1+g_2g_0-g_1g_4-g_6g_7-g_0g_2+g_7g_6-g_3g_5+g_5g_3)$

$+h_5 (g_5g_1-g_6g_0+g_3g_4-g_2g_7+g_7g_2+g_0g_6-g_1g_5-g_4g_3)$

$+ h_6 (g_6g_1+g_5g_0-g_7g_4+g_4g_7+g_3g_2-g_1g_6-g_0g_5-g_2g_3)$

$+ h_7(g_7g_1+g_3g_0+g_6g_4-g_1g_7-g_5g_2-g_4g_6+g_2g_5-g_0g_3)$

$=0 \bmod q.$

In the same manner we have

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

Then we have

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

In the same manner we have

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

Appendix H:

Theorem 6

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

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

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

$$G=(g_0,g_1,\ldots,g_7),\ g_j \in R\ (j=0,1,\ldots,7),$$

$$H=(h_0,h_1,\ldots,h_7),\ h_j \in R\ (j=0,1,\ldots,7),$$

where

$$h_0=0 \bmod q\,,$$

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

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

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,H satisfy the following equations.

$$GH+HG= 2g_0H \bmod q.$$

(*Proof*:)

$GH \bmod q$

$= (g_0h_0 - g_1h_1- g_2h_2- g_3h_3-g_4h_4- g_5h_5-g_6h_6-g_7h_7 \bmod q,$

$g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3 \bmod q,$

$g_0h_2-g_1h_4+g_2h_0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6 \bmod q,$

$g_0h_3-g_1h_7-g_2h_5+g_3h_0+g_4h_6+g_5h_2-g_6h_4+g_7h_1 \bmod q,$

$g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+g_4h_0+g_5h_7+ g_6h_3 -g_7h_5 \bmod q,$

$g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+g_5h_0+g_6h_1+g_7h_4 \bmod q,$

$g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+g_6h_0 +g_7h_2 \bmod q,$

$g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+g_7h_0 \quad \bmod q),$

$HG \bmod q$

$= (h_0g_0 - h_1g_1- h_2g_2- h_3g_3-h_4g_4- h_5g_5-h_6g_6-h_7g_7 \bmod q,$

$h_0g_1+h_1g_0+h_2g_4+h_3g_7-h_4g_2+h_5g_6-h_6g_5-h_7g_3 \bmod q,$

$h_0g_2-h_1g_4+h_2g_0+h_3g_5+h_4g_1-h_5g_3+h_6g_7-h_7g_6 \bmod q,$

$h_0g_3-h_1g_7-h_2g_5+h_3g_0+h_4g_6+h_5g_2-h_6g_4+h_7g_1 \bmod q,$

$h_0g_4+h_1g_2 -h_2g_1 -h_3g_6+h_4g_0+h_5g_7+ h_6g_3 -h_7g_5 \bmod q,$

$h_0g_5-h_1g_6+h_2g_3-h_3g_2-h_4g_7+h_5g_0+h_6g_1+h_7g_4 \bmod q,$

$h_0g_6+h_1g_5 -h_2g_7+h_3g_4 -h_4g_3 -h_5g_1+h_6g_0 +h_7g_2 \bmod q,$

$h_0g_7+h_1g_3+h_2g_6-h_3g_1+h_4g_5-h_5g_4-h_6g_2+h_7g_0 \bmod q).$

$[GH +HG]_0= g_0h_0 - g_1h_1- g_2h_2- g_3h_3-g_4h_4- g_5h_5-g_6h_6-g_7h_7$

$+ h_0g_0 - h_1g_1- h_2g_2- h_3g_3-h_4g_4- h_5g_5-h_6g_6-h_7g_7$

$=0-0+0-0=0 =2g_0h_0 \bmod q.$

$[GH +HG]_1= g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3$

$+ h_0g_1+h_1g_0+h_2g_4+h_3g_7-h_4g_2+h_5g_6-h_6g_5-h_7g_3$

$= 2g_0h_1 \bmod q.$

In the same manner

$[GH +HG]_i= 2g_0h_i \quad (i=2,\ldots,7).$

We have

$GH +HG =2g_0H \bmod q.$ q.e.d.