International Journal of Information and Communication Sciences
2018; 3(2): 50-65
http://www.sciencepublishinggroup.com/j/ijics
doi: 10.11648/j.ijics.20180302.15
ISSN: 2575-1700 (Print); ISSN: 2575-1719 (Online)

Fully Homomorphic Public-Key Encryption Against Ciphertext Square Attack with Two Ciphertexts

Masahiro Yagisawa

Yokohama-shi, Kanagawa-ken, Japan

Email address:
tfkt8398yagi@outlook.jp

To cite this article:
Masahiro Yagisawa. Fully Homomorphic Public-Key Encryption Against Ciphertext Square Attack with Two Ciphertexts. *International Journal of Information and Communication Sciences*. Vol. 3, No. 2, 2018, pp. 50-65. doi: 10.11648/j.ijics.20180302.15

Received: July 12, 2018; **Accepted**: September 4, 2018; **Published**: October 8, 2018

Abstract: A fully homomorphic public-key encryption (FHPKE) is the important cryptosystem as the basic scheme for the cloud computing. Since Gentry discovered in 2009 the first fully homomorphic encryption scheme, some fully homomorphic encryption schemes were proposed. In the systems proposed until now the bootstrapping process is the main bottleneck and the large complexity for computing the ciphertext is required. The existence of an efficient fully homomorphic cryptosystem would have great practical implications in the outsourcing of private computations, for instance, in the context of cloud computing. In recent year Yagisawa proposed fully homomorphic encryptions without bootstrapping which have the weak point in the enciphering function or not immune from "ciphertext square attack" which is the attack proposed in this article. In this article, a new FHPKE against "ciphertext square attack" is proposed which does not need the bootstrapping and does not require the large complexity for enciphering. The scheme has the following features; (a) its security bases on computational difficulty to solve the multivariate algebraic equations of high degrees; (b) it requires two ciphertexts corresponding to a plaintext. We describe concretely how to construct the proposed system over octonion ring. It is shown that proposed system is immune from "ciphertext square attack", "m and -m attack" and the Gröbner basis attacks and the complexity to encipher and decipher is not large.

Keywords: Two Ciphertexts, Ciphertext Square Attack, Fully Homomorphic Public-Key Encryption, Multivariate Algebraic Equation, Gröbner Basis, Non-associative Ring

1. Introduction

A cryptosystem which supports both addition and multiplication (thereby preserving the ring structure of the plaintexts) is known as fully homomorphic encryption (FHE) and is very powerful. Using such a scheme, any circuit can be homomorphically evaluated, effectively allowing the construction of programs which may be run on encryptions of their inputs to produce an encryption of their output. Since such a program never decrypts its input, it can be run by an untrusted party without revealing its inputs and internal state. The existence of an efficient and fully homomorphic cryptosystem would have great practical implications in the outsourcing of private computations, for instance, in the context of cloud computing.

In 2009 Gentry, an IBM researcher, has created a homomorphic encryption scheme that makes it possible to encrypt the data in such a way that performing a mathematical operation on the encrypted information and then decrypting the result produces the same answer as performing an analogous operation on the unencrypted data [1, 2].

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

Some fully homomorphic encryption schemes were proposed until now [3-7].

In recent year Yagisawa proposed fully homomorphic encryptions without bootstrapping [8, 9] which have the weak point in the enciphering function [10]. After that Yagisawa proposed the some fully homomorphic encryption schemes [11-13].

In this paper we show that these Yagisawa's schemes are not immune from "ciphertext square attack". We construct

another fully homomorphic public-key system against "ciphertext square attack" with two ciphertexts which is based on computational difficulty to solve the multivariate algebraic equations of high degree while the almost all multivariate cryptosystems [14-17] proposed until now are based on the quadratic equations avoiding the explosion of the coefficients. Proposed scheme is immune from the Gröbner basis [18] attack, the differential attack, rank attack and so on.

2. Preliminaries for Octonion Operation

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

2.1. Multiplication and Addition on Octonion Ring O

Let q be a fixed modulus to be as large prime as 2^{2000}.
Let O be the octonion [19] ring over a finite field Fq.

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

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

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

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

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

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

Let

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

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

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

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

2.2. Property of Multiplication over Octonion Ring O

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

(1) Non-commutative

$$AB\neq BA \bmod q. \quad (8)$$

(2) Non-associative

$$A(BC)\neq(AB)C \bmod q. \quad (9)$$

(3) Alternative

$$(AA)B=A(AB) \bmod q, \quad (10)$$

$$A(BB)=(AB)B \bmod q, \quad (11)$$

$$(AB)A=A(BA) \bmod q. \quad (12)$$

(4) Moufang's formulae [19],

$$C(A(CB))=((CA)C)B \bmod q, \quad (13)$$

$$A(C(BC))=((AC)B)C \bmod q, \quad (14)$$

$$(CA)(BC)=(C(AB))C \bmod q, \quad (15)$$

$$(CA)(BC)=C((AB)C) \bmod q. \quad (16)$$

(5) Lemma 1

$$A^{-1}(AB)=B \bmod q, \quad (17)$$

$$(BA)A^{-1}=B \bmod q. \quad (18)$$

(Proof:)
Here proof is omitted and can be looked up in the Appendix B.

(6) Lemma 2

$$(A^{-1}B)A=A^{-1}(BA) \bmod q. \quad (19)$$

(Proof)
From (12)

$$A^{-1}B=A^{-1}((BA)A^{-1})=(A^{-1}(BA))A^{-1} \bmod q. \quad (20)$$

By multiplying A from right side we have

$$(A^{-1}B)A=A^{-1}(BA) \bmod q.\ \text{q.e.d.} \quad (21)$$

(7) Lemma 3

$$(ABA^{-1})(ABA^{-1})=AB^2A^{-1} \bmod q. \quad (22)$$

(Proof:)

$$\begin{aligned}&(ABA^{-1})(ABA^{-1}) \bmod q\\ &=[A^{-1}(A^2(BA^{-1}))][(AB)A^{-1}] \bmod q\end{aligned}$$

from (16),

$$\begin{aligned}&=A^{-1}\{[(A^2(BA^{-1}))(AB)]A^{-1}\} \bmod q\\ &=A^{-1}\{[(A(A(BA^{-1})))(AB)]A^{-1}\} \bmod q\\ &=A^{-1}\{[(A((AB)A^{-1}))(AB)]A^{-1}\} \bmod q\\ &=A^{-1}\{[(A(AB))A^{-1}))(AB)]A^{-1}\} \bmod q.\end{aligned}$$

We apply (13) to inside of [.],

$$\begin{aligned}&=A^{-1}\{[(A((AB)(A^{-1}(AB)))]A^{-1}\} \bmod q\\ &=A^{-1}\{[(A((AB)B))]A^{-1}\} \bmod q\\ &=A^{-1}\{[A(A(BB))]A^{-1}\} \bmod q\\ &=\{A^{-1}[A(A(BB))]\}A^{-1} \bmod q\\ &=(A(BB))A^{-1} \bmod r\\ &=AB^2A^{-1} \bmod q.\ \text{q.e.d.}\end{aligned} \quad (23)$$

(8) Theorem 1

$$A^2=-L_A1+ 2a_0A \bmod q, \quad (24)$$

where

$$L_A= a_0^2+a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2 \bmod q\in Fq, \quad (25)$$

$$1=(1,0,0,0,0,0,0,0)\in O, \quad (26)$$

$$A=(a_0,a_1,\ldots,a_7)\in O. \quad (27)$$

(Proof:)

$A^2 \bmod q$

$=(a_0a_0 - a_1a_1 - a_2a_2 - a_3a_3 - a_4a_4 - a_5a_5 - a_6a_6 - a_7a_7 \bmod q,$
$a_0a_1+a_1a_0+a_2a_4+a_3a_7-a_4a_2+a_5a_6-a_6a_5-a_7a_3 \bmod q,$
$a_0a_2-a_1a_4+a_2a_0+a_3a_5+a_4a_1-a_5a_3+a_6a_7-a_7a_6 \bmod q,$
$a_0a_3-a_1a_7-a_2a_5+a_3a_0+a_4a_6+a_5a_2-a_6a_4+a_7a_1 \bmod q,$
$a_0a_4+a_1a_2-a_2a_1-a_3a_6+a_4a_0+a_5a_7+a_6a_3-a_7a_5 \bmod q,$
$a_0a_5-a_1a_6+a_2a_3-a_3a_2-a_4a_7+a_5a_0+a_6a_1+a_7a_4 \bmod q,$
$a_0a_6+a_1a_5-a_2a_7+a_3a_4-a_4a_3-a_5a_1+a_6a_0+a_7a_2 \bmod q,$
$a_0a_7+a_1a_3+a_2a_6-a_3a_1+a_4a_5-a_5a_4-a_6a_2+a_7a_0 \bmod q)$
$=(2a_0^2- L_A \bmod q, 2a_0a_1 \bmod q, 2a_0a_2 \bmod q, 2a_0a_3 \bmod q,$
$2a_0a_4 \bmod q, 2a_0a_5 \bmod q, 2a_0a_6 \bmod q, 2a_0a_7 \bmod q)$
$=-L_A1+2a_0(a_0,a_1,\ldots,a_7) \bmod q,$
$=-L_A1+2a_0A \bmod q, \quad (28)$

where

$$L_A= a_0^2+a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2 \bmod q\in Fq. \quad (29)$$

q.e.d.

(9) Theorem 2

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

$$AA^*= A^*A= L_A1\in O \quad (30)$$

where

$$L_A= a_0^2+a_1^2+\ldots+a_7^2 \bmod q\in Fq. \quad (31)$$

(Proof:)

As

$$A+A^*=(2a_0,0,\ldots,0)=2a_01\in O, \quad (32)$$

$$A^2=- L_A 1+2a_0A = -L_A1+(A+A^*)A$$

$$= -L_A1+ A (A+A^*) \bmod q, \quad (33)$$

we have

$$L_A1=A^*A = AA^* \bmod q\in O. \text{ q.e.d.} \quad (34)$$

(10) Theorem 3

$$L_AL_B= L_{AB} \bmod q\in Fq \quad (35)$$

where

$$A=(a_0,a_1,\ldots,a_7), B=(b_0,b_1,\ldots,b_7) , C=(c_0,c_1,\ldots,c_7)\in O, \quad (36)$$

$$C=AB \bmod q\in O, \quad (37)$$

$$L_A=a_0^2+a_1^2+\ldots+a_7^2 \bmod q, \quad (38)$$

$$L_B=b_0^2+b_1^2+\ldots+b_7^2 \bmod q, \quad (39)$$

$$L_{AB}=c_0^2+c_1^2+\ldots+c_7^2 \bmod q \quad (40)$$

(Proof:)

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

(11) Theorem 4

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

$$B(AX)=DX \bmod q\in O[X], \quad (41)$$

where $B,A,D\in O$ and X are variables.

(Proof:)

When X=1, we have

$$BA=D \bmod q. \quad (42)$$

Then

$$B(AX)=(BA)X \bmod q. \quad (43)$$

We can select $C\in O$ that satisfies

$$B(AC)\neq(BA)C \bmod q. \quad (44)$$

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

$$B(AC)=(BA)C \bmod q. \quad (45)$$

(45) is contradictory to (44). q.e.d.

(12) Theorem 5

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

$$C(B(AX))=DX \bmod q\in O[X], \quad (46)$$

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

$$B(AC)\neq(BA)C \bmod q. \quad (47)$$

(Proof:)

If D exists, we have at X=1

$$C(BA)=D \bmod q. \quad (48)$$

Then

$$C(B(AX))=(C(BA))X \bmod q. \quad (49)$$

We substitute C to X to obtain

$$C(B(AC))=(C(BA))C \bmod q. \quad (50)$$

From (12)

$$C(B(AC))=(C(BA))C=C((BA)C) \bmod q. \quad (51)$$

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

$$B(AC)=(BA)C \bmod q \quad (52)$$

(52) is contradictory to (47). q.e.d.

(13) Theorem 6

D and E∈O do not exist that satisfy the following equation.

$$C(B(AX))= E (DX) \bmod q \in O[X], \quad (53)$$

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

$$C(BA) \neq (CB)A \bmod q. \quad (54)$$

(Proof:)

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

$$C(BA)=ED \bmod q. \quad (55)$$

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

$$C(B(A(D^{-1}E^{-1})))= E (D(D^{-1}E^{-1})) \bmod q=1, \quad (56)$$

$$(C(B(A(D^{-1}E^{-1}))))^{-1} \bmod q=1, \quad (57)$$

$$(((ED)A^{-1})B^{-1})C^{-1} \bmod q=1, \quad (58)$$

$$ED =(CB)A \bmod q. \quad (59)$$

From (55) and (59) we have

$$C(BA) =(CB)A \bmod q. \quad (60)$$

(60) is contradictory to (54). q.e.d.

(14) Theorem 7

D∈O does not exist that satisfies the following equation.

$$A(B(A^{-1}X))=DX \bmod q \in O[X], \quad (61)$$

where B,A,D∈O, A has the inverse A^{-1} mod q and X is a variable.

(Proof:)

If D exists, we have at X=1

$$A(BA^{-1})=D \bmod q. \quad (62)$$

Then

$$A (B(A^{-1}X))=(A(BA^{-1}))X \bmod q. \quad (63)$$

We can select C∈O such that

$$(BA^{-1})(CA^2) \neq ((BA^{-1})C)A^2 \bmod q. \quad (64)$$

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

Substituting CA to X in (63), we have

$$A (B(A^{-1}(CA)))=(A(BA^{-1}))(CA) \bmod q. \quad (65)$$

From Lemma 2

$$A (B((A^{-1}C)A))=(A(BA^{-1}))(CA) \bmod q. \quad (66)$$

From (16)

$$A (B((A^{-1}C)A)))=A([(BA^{-1})C]A) \bmod q. \quad (67)$$

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

$$B((A^{-1}C)A))= ((BA^{-1})C)A \bmod q. \quad (68)$$

From Lemma 2

$$B(A^{-1}(CA))=((BA^{-1})C)A \bmod q. \quad (69)$$

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

$$B(A^{-1}((CA^2)A^{-1}))=((BA^{-1})C)A \bmod q. \quad (70)$$

From (14) we have

$$((BA^{-1})(CA^2))A^{-1}=((BA^{-1})C)A \bmod q. \quad (71)$$

Multiply A from right side we have

$$(BA^{-1})(CA^2)=((BA^{-1})C)A^2 \bmod q. \quad (72)$$

(72) is contradictory to (64). q.e.d.

3. Yagisawa's Scheme

In recent year Yagisawa proposed fully homomorphic public-key encryptions with medium texts which consist of some octonion elements [11-13]. We describe " Fully homomorphic public-key encryption with small ciphertext size" [13] as an example of Yagisawa's encryption scheme.

3.1. Yagisawa's Encryption Scheme

Let q be a prime.

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

$$[G]_0=g_0=1/2 \bmod q, \quad (73)$$

$$[H]_0=h_0=0 \bmod q, \quad (74)$$

$$L_G:=|G|^2= g_0^2+g_1^2+\ldots+g_7^2=0 \bmod q , \quad (75)$$

$$L_H:=|H|^2= h_0^2+h_1^2+\ldots+h_7^2=0 \bmod q , \quad (76)$$

$$g_1h_1+g_2h_2+\ldots+ g_7h_7=0 \bmod q, \quad (77)$$

where we denote i-th element of octonion K∈O such as $[K]_i$.

Then we have

$[GH]_0= [HG]_0=g_0h_0-(g_1h_1+g_2h_2+\ldots+ g_7h_7)=0 \bmod q$,

$$G^2 \bmod q =2g_0G=G, \quad (78)$$

$$H^2 \bmod q =2h_0H =0=(0,0\ldots,0). \quad (79)$$

Let p∈Fq be a plaintext and u,v,w∈Fq be the random numbers.

The medium text M ∈O is defined as

$$M:=pG+uH+vGH+wHG \bmod q \in O. \quad (80)$$

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

$$p= 2[M]_0 \bmod q \in Fq. \quad (81)$$

Let $sk_A=(r_A ,A_j(j=1,\ldots,r_A))$ be a secret key of user A and $pk_A=(\{e_{Aijk}\}_{0\leq i,j,k\leq 7})$ be the public key of user A such that

$E_A(X,Y):=A_1(\ldots(A_{rA}(Y(A_{rA}^{-1}(\ldots(A_1^{-1}X)\ldots))))\ldots) \bmod q \in O[X,Y]$

$$=\{e_{Aijk}\}(i,j,k=0,\ldots,7). \quad (82)$$

Let $sk_B=(r_B, A_{B\,j}(j=1,\ldots,r_B))$ be a secret key of user B and $pk_B=(\{e_{Bijk}\}_{0\leq i,j,k\leq 7})$ be the public key of user B such that

$E_B(X,Y):= B_1(\ldots(B_{rB}(Y(B_{rB}^{-1}(\ldots(B_1^{-1}X)\ldots))))\ldots) \bmod q \in O[X,Y]$

$$=\{e_{Bijk}\}(i,j,k=0,\ldots,7). \quad (83)$$

Let $E_{BA}(X,Y)$ be the common enciphering function between user A and user B such that

$$E_{BA}(X,Y) : =A_1(\ldots(A_{rA}(B_1(\ldots(B_{rB}(Y(B_{rB}^{-1}(\,B_{rB\text{-}1}^{-1}\,(\ldots(B_1^{-1}$$

$$(A_{rA}^{-1}(\ldots(A_1^{-1}X)\ldots)))\ldots)))))\ldots)))\ldots) \bmod q \in O[X,Y] \quad (84)$$

Let C(X,p) be the ciphertext of the plaintext p such that

$C(X,p):= E_{BA}(X,M) \in O[X,Y]$

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

$$=\{c_{jkl}\}\ (j,k,l=0,\ldots,7), \quad (85)$$

where

$$M= pG+uH+vGH+wHG \in O\ ,u,v,w \in Fq. \quad (86)$$

3.2. Analysis of Yagisawa's Encryption Scheme

We adopt"ciphertext square attack". We calculate M^2 mod q here.

$$\text{As } |M|^2=0 \bmod q \text{ from [13],}$$

$$M^2=-|M|^2 1+2[M]_0 M \bmod q$$

$$=2[pG]_0 M \bmod q$$

$$=pM \bmod q. \quad (87)$$

Then we have

$C(C(X,p),p)= A_1(\ldots(A_{rA}(B_1(\ldots(B_{rB}(M(B_{rB}^{-1}(\ldots(B_1^{-1}(A_{rA}^{-1}$
$(\ldots (A_1^{-1}[A_1(\ldots(A_{rA}(B_1(\ldots(B_{rB}(M(B_{rB}^{-1}(\ldots(B_1^{-1}(A_{rA}^{-1}(\ldots(A_1^{-1}$
$X) \ldots)])\ldots)\bmod q$

$= A_1(\ldots(A_{rA}(B_1(\ldots(B_{rB}(M^2(B_{rB}^{-1}(\ldots(B_1^{-1}(A_{rA}^{-1}(\ldots(A_1^{-1}X)$
$\ldots)\bmod q$

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

$$= pC(X,p) \bmod q. \quad (88)$$

That is, we get the plaintext p.

We call the above scheme "ciphertext square attack (CSA)".

As the norm of medium text $|M|^2$ is zero and the 0-th element of medium text $[M]_0$ consists of the plaintext p, ciphertext square attack is efficient. In next section we describe the enciphering system where the norm of medium text $|M|^2$ is not zero and the 0-th element of medium text $[M]_0$ consists of the plaintext and a random parameter.

4. Proposed Fully Homomorphic Public-Key Encryption Scheme

We propose the encryption scheme with two ciphertexts to be immune from "ciphertext square attack".

4.1. Definition of Homomorphic Public-Key Encryption

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

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

-Key-Generation. The algorithm KeyGen, on input the security parameter 1λ, outputs (sk) ← KeyGen(1λ) , where sk is a secret key and (pk) ← KeyGen(1λ) , where pk is a public key.

-Encryption. The algorithm Enc, on input system parameter (q,S), secret key(sk), public key(pk) and a plaintext $m \in Fq$, outputs a ciphertext $C \in O \leftarrow Enc(sk,pk;m)$

where $S \in O$ is a part of system parameter such that $S^{-1} \bmod q \in O$ exists.

-Decryption. The algorithm Dec, on input system parameter (q,S), secret key(sk) and a ciphertext C, outputs a plaintext m*←Dec(sk;C).

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

4.2. Definition of Fully Homomorphic Public-Key Encryption

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

Definition (Fully homomorphic public-key encryption). A homomorphic encryption scheme HPKE :=(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 $sk \leftarrow KeyGen(1\lambda), \forall ckt \in CR\lambda, \forall(m_1,\ldots, m_n) \in Fq^n$ where $n = n(\lambda)$, $\forall(C_1,\ldots,C_n)$ where $Ci \leftarrow Enc(sk,pk;m_i)$ $(i=1,..,n)$, it holds that:
$Pr[Dec(sk;Eval(ckt; C_1,\ldots,C_n)) \neq ckt(m_1,\ldots, m_n)] = negl(\lambda)$.

(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.

4.3. Medium Text

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

We select the modulus q to be the prime.

We select the secret elements $G=(g_0,g_1,\ldots, g_7)\in O$ and $H=(h_0,-g_1,\ldots, -g_7)\in O$ such that

$$[G]_0=g_0=1/2 \bmod q, \tag{89}$$

$$[H]_0=h_0=1/2 \bmod q, \tag{90}$$

$$[G]_1=g_1\neq 0 \bmod q, \tag{91}$$

$$G+H=1 \bmod q, \tag{92}$$

$$L_G:=|G|^2= g_0{}^2+g_1{}^2+\ldots+g_7{}^2=0 \bmod q\ , \tag{93}$$

$$L_H:=|H|^2= h_0{}^2+g_1{}^2+\ldots+g_7{}^2=0 \bmod q\ , \tag{94}$$

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

Then we have

$$G^2 \bmod q =2g_0G=G, \tag{95}$$

$$H^2 \bmod q =2h_0H =H. \tag{96}$$

Let $m\in Fq$ be a plaintext , $h,k\in Fq,(h\neq k)$ be fixed secret parameters and $u,v\in Fq$ be the random numbers where h and k are given in (99),(100).

The medium text ${}^1M$,${}^2M\in O$ are defined as

$${}^1M:=(m+u)G+(m+v)H \bmod q\in O, \tag{97}$$

$${}^2M:=(m+hu)G+(m+kv)H \bmod q\in O, \tag{98}$$

$$h^2+2h-1 =\alpha h \bmod q, \tag{99}$$

$$k^2+2k-1 =\alpha k \bmod q, \tag{100}$$

where $\alpha\in Fq$ is an arbitrary parameter.

The plaintext m is given from the medium text ${}^1M$ or ${}^2M$ such that

$$m=[{}^1M]_0+[{}^1M]_1(h+k)/(2g_1(h-k))-[{}^2M]_1/(g_1(h-k)) \bmod q\in Fq. \tag{101}$$

Let $sk_A=(r_A\ ,A_j(j=1,\ldots,r_A),G_A)$ be a secret key of user A and $pk_A=(\{e_{Aijk}\}_{0\leqq i,j,k\leqq 7})$ be the public key of user A such that

$E_A(X,Y):=A_1(\ldots(A_{rA}(Y(A_{rA}{}^{-1}(\ldots(A_1{}^{-1}X)\ldots))))\ldots) \bmod q\in O[X,Y]$

$$=\{e_{Aijk}\}(i,j,k=0,\ldots,7). \tag{102}$$

Let $sk_B=(r_B\ ,A_{B\,j}(j=1,\ldots,r_B)\ ,G_B)$ be a secret key of user B and $pk_B=(\{e_{Bijk}\}_{0\leqq i,j,k\leqq 7}\ )$ be the public key of user B such that

$E_B(X,Y):= B_1(\ldots(B_{rB}(Y(B_{rB}{}^{-1}(\ldots(B_1{}^{-1}X)\ldots))))\ldots) \bmod q\in O[X,Y]$

$$=\{e_{Bijk}\}(i,j,k=0,\ldots,7). \tag{103}$$

Let $E_{BA}(X,Y)$ be the common enciphering function between user A and user B such that

$$E_{BA}(X,Y) : =A_1(\ldots(A_{rA}(B_1(\ldots(B_{rB}(Y(B_{rB}{}^{-1}(\ B_{rB\text{-}1}{}^{-1}\ (\ldots(B_1{}^{-1}$$

$$(A_{rA}{}^{-1}(\ldots(A_1{}^{-1}X)\ldots)))\ldots)))))\ldots)))\ldots) \bmod q\in O[X,Y] \tag{104}$$

Let C(m) be the ciphertext corresponding to the plaintext m such that

${}^iC(m):= E_{BA}({}^iM,S)\in O$

$=A_1(\ldots(A_{rA}(B_1(\ldots(B_{rB}(S(B_{rB}{}^{-1}(\ldots(B_1{}^{-1}(A_{rA}{}^{-1}(\ldots(A_1{}^{-1}$

$({}^iM)\ldots) \bmod q$

$$=\{{}^ic_j\}\ (i=1,2;\ j=0,\ldots,7), \tag{105}$$

where

$${}^1M:=(m+u)G+(m+v)H \bmod q\in O, \tag{106}$$

$${}^2M:=(m+hu)G+(m+kv)H \bmod q\in O, \tag{107}$$

$$m,u,v\in Fq, \tag{108}$$

$S\in O$ is one of the system parameters.

(Addition and multiplication of medium texts)

[Addition]

Let

$${}^1M_1:=(m_1+u_1)G+(m_1+v_1)H \bmod q\in O, \tag{109}$$

$${}^2M_1:=(m_1+hu_1)G+(m_1+kv_1)H \bmod q\in O, \tag{110}$$

be medium texts corresponding to the plaintext m_1 and

$${}^1M_2:=(m_2+u_2)G+(m_2+v_2)H \bmod q\in O, \tag{111}$$

$${}^2M_2:=(m_2+hu_2)G+(m_2+kv_2)H \bmod q\in O, \tag{112}$$

be medium texts corresponding to the plaintext m_2 where

$$m_1=[{}^1M_1]_0+[{}^1M_1]_1(h+k)/(2g_1(h-k))-[{}^2M_1]_1/(g_1(h-k)) \bmod q\in Fq, \tag{113}$$

$$m_2=[{}^1M_2]_0+[{}^1M_2]_1(h+k)/(2g_1(h-k))-[{}^2M_2]_1/(g_1(h-k)) \bmod q\in Fq. \tag{114}$$

Let ${}^1M_{1+2}$, ${}^2M_{1+2}$ be the medium texts corresponding to the sum of the plaintexts m_1 and m_2 such that

$${}^1M_{1+2}:={}^1M_1+{}^1M_2\in O$$
$$=(m_1+u_1)G+(m_1+v_1)H+(m_2+u_2)G+(m_2+v_2)H \bmod q,$$
$$=(m_1+m_2+v_1+v_2)G+(m_1+m_2+v_1+v_2)H \bmod q, \tag{115}$$
$${}^2M_{1+2}:={}^2M_1+{}^2M_2\in O$$
$$=(m_1+hu_1)G+(m_1+kv_1)H+(m_2+hu_2)G+(m_2+kv_2)H$$
$$=(m_1+m_2+h(u_1+u_2))G+(m_1+m_2+k(v_1+ v_2))H \bmod q. \tag{116}$$

We obtain m_{1+2} , the sum of m_1 and m_2 as follows.

$$m_{1+2}:= [{}^1M_{1+2}]_0+[{}^1M_{1+2}]_1(h+k)/(2g_1(h-k))-[{}^2M_{1+2}]_1/(g_1(h-k))$$
$$=m_1+m_2 \bmod q\in Fq. \tag{117}$$

[Multiplication]

First we calculate ${}^1M_1{}^1M_2 \bmod q$, ${}^2M_1{}^2M_2 \bmod q$, ${}^1M_1{}^2M_2$

mod q and ${}^2M_1{}^1M_2$ mod q as follows.

$${}^1M_1\ {}^1M_2 \in O$$

$$=((m_1+u_1)G+(m_1+v_1)H)((m_2+u_2)G+(m_2+v_2)H)$$

$$=(m_1+u_1)(m_2+u_2)\ G+(m_1+v_1)(m_2+v_2)H,$$

$$=(m_1m_2+m_1u_2+u_1m_2+u_1u_2)G+(m_1m_2+m_1v_2+v_1m_2+v_1v_2)H],$$

$$\text{mod q} \tag{118}$$

$${}^2M_1\ {}^2M_2 \in O$$

$$=((m_1+hu_1)G+(m_1+kv_1)H)((m_2+hu_2)G+(m_2+kv_2)H)$$

$$=(m_1+hu_1)(m_2+hu_2)\ G+(m_1+kv_1)(m_2+kv_2)H \text{ mod q},$$

$$=(m_1m_2+hm_1u_2+hu_1m_2+h^2u_1u_2)G+(m_1m_2+km_1v_2+kv_1m_2$$

$$+k^2v_1v_2)H], \text{ mod q} \tag{119}$$

$${}^1M_1\ {}^2M_2 \in O$$

$$=((m_1+u_1)G+(m_1+v_1)H)((m_2+hu_2)G+(m_2+kv_2)H)$$

$$=(m_1+u_1)(m_2+hu_2)\ G+(m_1+v_1)(m_2+kv_2)H,$$

$$=(m_1m_2+hm_1u_2+u_1m_2+hu_1u_2)G$$

$$+(m_1m_2+km_1v_2+v_1m_2+kv_1v_2)H \text{ mod q}, \tag{120}$$

$${}^2M_1{}^1M_2 \in O$$

$$=((m_1+hu_1)G+(m_1+ku_1)H)((m_2+u_2)G+(m_2+v_2)H)$$

$$=(m_1+hu_1)(m_2+u_2)G+(m_1+kv_1)(m_2+v_2)H \text{ mod q}, \tag{121}$$

$$=(m_1m_2+m_1u_2+hu_1m_2+hu_1u_2)G+(m_1m_2+m_1v_2+kv_1m_2$$

$$+kv_1v_2)H] \text{ mod q}, \tag{122}$$

We define ${}^1M_{12}$ and ${}^2M_{12}$, the medium texts corresponding to the product of m_1 and m_2 as follows.

Here we select α such that

$$\alpha=0 \tag{123}$$

as an example.

As

$$h^2+2h-1=\alpha h=0 \text{ mod q}, \tag{124}$$

$$k^2+2k-1=\alpha k=0 \text{ mod q} \tag{125}$$

and

$$h \neq k, \tag{126}$$

we have

$${}^1M_{12}:=({}^1M_1{}^1M_2-{}^2M_1{}^2M_2,+{}^1M_1{}^2M_2+{}^2M_1{}^1M_2)/2 \text{ mod q}$$

$$=(m_1m_2+m_1u_2+u_1m_2+2hu_1u_2)G$$

$$+(m_1m_2+m_1v_2+v_1m_2+2kv_1v_2)H] \text{ mod q} \in O \tag{127}$$

$${}^2M_{12}:=({}^1M_1{}^1M_2+3({}^2M_1{}^2M_2)-{}^1M_1{}^2M_2-{}^2M_1{}^1M_2)/2 \text{ mod q}$$

$$=(m_1m_2+hm_1u_2+hu_1m_2+2h^2u_1u_2)G$$

$$+(m_1m_2+km_1v_2+kv_1m_2+2k^2v_1v_2)H] \text{ mod q} \in O \tag{128}$$

Naturally we can define the plaintexts m_{12} and the random number u_{12} and v_{12} to satisfy the following equations.

As h+k=-2,

$$m_{12}:=[{}^1M_{12}]_0-([{}^1M_{12}]_1+[{}^2M_{12}]_1)/(g_1(h-k)) \text{ mod q}$$

$$=(m_1m_2+(u_2+v_2)m_1/2+(u_1+v_1)m_2/2+hu_1u_2+kv_1v_2)$$

$$-[(u_2-v_2)m_1+(u_1-v_1)m_2+2hu_1u_2-2kv_1v_2$$

$$+(hu_2-kv_2)m_1+(hu_1-kv_1)m_2+2h^2u_1u_2-2k^2v_1v_2]g_1/(g_1(h-k))$$

$$=(m_1m_2+(1/2-(1+h)/(h-k))u_2m_1$$

$$+(1/2+(1+k)/(h-k))v_2m_1$$

$$+(1/2-(1+h)/(h-k))u_1m_2$$

$$+(1/2+(1+k)/(h-k))v_1m_2$$

$$+(h-(2h+2h^2)/(h-k)u_1u_2$$

$$+(k+(2k+2k^2)/(h-k)v_1v_2$$

$$=m_1m_2 \text{ mod q} \in Fq. \tag{129}$$

Here we notice that

since that

$$h=-1+\sqrt{2}=\text{mod q},$$

$$k=-1-\sqrt{2}\text{mod q}.$$

$$1/2-(1+h)/(h-k)=1/2-\sqrt{2}/(2\sqrt{2})=0\text{mod q} \tag{130}$$

$$1/2+(1+k)/(h-k)=1/2-\sqrt{2}/(2\sqrt{2})=0\text{mod q}. \tag{131}$$

$$u_{12}:=m_1u_2+u_1m_2+2hu_1u_2 \text{ mod q} \in Fq. \tag{132}$$

$$v_{12}:=m_1v_2+v_1m_2+2kv_1v_2 \text{ mod q} \in Fq. \tag{133}$$

We can express ${}^1M_{12}$, ${}^2M_{12}$ as follows.

$${}^1M_{12}=(m_{12}+u_{12})G+(m_{12}+v_{12})H \text{ mod q} \in O \tag{134}$$

$${}^2M_{12}=(m_{12}+hu_{12})G+(m_{12}+kv_{12})H \text{ mod q} \in O. \tag{135}$$

4.4. Proposed Fully Homomorphic Public-Key Encyption

We propose a fully homomorphic public-key encryption (FHPKE) scheme on octonion ring over Fq. Here we define some parameters for describing FHPKE.

We select the elements

$$G=(g_0,g_1,\ldots,g_7) \in O, \tag{136}$$

$$H=(h_0,-g_1,\ldots,-g_7) \in O, \tag{137}$$

where

$$g_0=1/2 \text{ mod q}, \tag{138}$$

$$h_0=1/2 \text{ mod q}, \tag{139}$$

$$g_1 \neq 0 \bmod q, \quad (140)$$

$$g_0^2+g_1^2+\ldots+g_7^2=0 \bmod q \in Fq. \quad (141)$$

as defined in section 4.3 Medium text.

Let $m \in Fq$ be a plaintext and $u \in Fq$ be the random parameter.

The medium texts ${}^1M$ and ${}^2M$ are defined as

$${}^1M:=(m+u)G+(m+v)H \bmod q \in O, \quad (142)$$

$${}^2M:=(m+hu)G+(m+kv)H \bmod q \in O, \quad (143)$$

$$h^2+2h-1=\alpha h \bmod q, \quad (144)$$

$$k^2+2k-1=\alpha k \bmod q. \quad (145)$$

We select as an example,

$$\alpha=0. \quad (146)$$

The plaintext m is given from the medium texts ${}^1M$ and ${}^2M$ as follows.

$$m=[{}^1M]_0-([{}^1M]_1+[{}^2M]_1)/(g_1(h-k)) \bmod q \in Fq. \quad (147)$$

where

$$g_1 \neq 0 \bmod q. \quad (148)$$

[Basic enciphering function f(X,Y)]

Basic enciphering function $f(X,Y) \in O[X,Y]$ is defined as follows.

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

We select $A_1,\ldots, A_r \in O$ such that A_j (j=1,..,r) has the inverse A_i^{-1} mod q. We define the basic enciphering function f(X,Y) such that

$$\begin{aligned}
&f(X,Y):=A_1^{-1}(\ldots(A_r^{-1}(Y(A_r(\ldots(A_1X)...) \bmod q \in O[X,Y]\\
&=(f_{000}x_0y_0+f_{001}x_0y_1+ \ldots+f_{077}x_7y_7,\\
&f_{100}x_0y_0+f_{101}x_0y_1+ \ldots+f_{177}x_7y_7,\\
&\ldots. \ldots.\\
&f_{700}x_0y_0+f_{701}x_0y_1+ \ldots+f_{777}x_7y_7)^t,\\
&= \{f_{ijk}\}(i,j,k=0,\ldots,7). \quad (149)
\end{aligned}$$

Since $f(X,1)=X$ at Y=1, some f_{ijk} are determined such that

$f_{000}=1$, $f_{010}=0$, …, $f_{070}=0$,

$f_{100}=0$, $f_{110}=1$, …, $f_{170}=0$,

… …

$f_{700}=0$, $f_{710}=0$, …, $f_{770}=1$.

Let $g(X,Y) \in O[X,Y]$ be a sub-enciphering function such that

$$\begin{aligned}
&g(X,Y):=\\
&(\ldots((XA_1)A_2)\ldots)A_r)Y)A_r^{-1})\ldots)A_1^{-1} \bmod q \in O[X,Y]\\
&=(g_{000}x_0y_0+g_{001}x_0y_1+ \ldots+g_{077}x_7y_7,\\
&g_{100}x_0y_0+g_{101}x_0y_1+ \ldots+g_{177}x_7y_7,\\
&\ldots. \ldots.\\
&g_{700}x_0y_0+g_{701}x_0y_1+ \ldots+g_{777}x_7y_7)^t,\\
&= \{g_{ijk}\}(i,j,k=0,\ldots,7). \quad (150)
\end{aligned}$$

Since $g(X,1)=X$ at Y=1, some g_{ijk} are determined such that

$g_{000}=1$, $g_{010}=0$, …, $g_{070}=0$,

$g_{100}=0$, $g_{110}=1$, …, $g_{170}=0$,

… …

$g_{700}=0$, $g_{710}=0$, …, $g_{770}=1$.

Theorem 8

Let

$$R_n=U_n((\ldots((U_2((U_1((PQ)U_1))U_2))\ldots))U_n) \bmod q \in O \quad (151)$$

$$L_n=(U_n((\ldots((U_2((U_1(PQ))U_1))U_2))\ldots))U_n \bmod q \in O \quad (152)$$

$$M_n=[U_n(\ldots(U_2(U_1P)\ldots)][(\ldots(QU_1)U_2)\ldots)U_n] \bmod q \in O \quad (153)$$

where

$P, Q, U_j \in O$ (j=1,2,…,n).

For any positive integer n, it holds that

$$R_n \bmod q = L_n \bmod q = M_n \bmod q. \quad (154)$$

(Proof)

We use the mathematical induction.

In case that n=1, from (15),(16)

$R_1=U_1((PQ)U_1)=(U_1(PQ))U_1=(U_1P)(QU_1) \bmod q$ is obtained. That is,

$$R_1=L_1=M_1 \bmod q. \quad (155)$$

In case that n=t-1,if $R_{t-1}=L_{t-1}=M_{t-1} \bmod q$, then

$$\begin{aligned}
&U_t(R_{t-1}U_t)=U_t((U_{t-1}((\ldots((U_1((PQ)U_1))\ldots))U_{t-1}\,))U_t)\\
&=R_t \bmod q \quad (156)
\end{aligned}$$

$$\begin{aligned}
&U_t(R_{t-1}U_t)=U_t(L_{t-1}U_t)\\
&=U_t(((U_{t-1}((\ldots((U_2((U_1(PQ))U_1))U_2))\ldots))U_{t-1})U_t)\\
&=(U_t((U_{t-1}((\ldots((U_2((U_1(PQ))U_1))U_2))\ldots))U_{t-1}))U_t\\
&=L_t \bmod q. \quad (157)
\end{aligned}$$

$$\begin{aligned}
&U_t(R_{t-1}U_t)= U_t(M_{t-1}U_t)\\
&=U_t(([U_{t-1}(U_{t-2}(\ldots(U_1P))\ldots)][(\ldots((QU_1)\ldots)U_{t-2})U_{t-1}])U_t)
\end{aligned}$$

from (16)

$$\begin{aligned}
&=(U_t[(U_{t-1}(\ldots(U_2(U_1P))\ldots)]) ([(\ldots((QU_1)U_2)\ldots)U_{t-1})]U_t)\\
&=[U_t(U_{t-1}(\ldots(U_2(U_1P))\ldots)][(\ldots((QU_1)U_2)\ldots)U_{t-1})U_t]\\
&=M_t \bmod q \quad (158)
\end{aligned}$$

That is, we obtain

$$R_t=L_t=M_t \bmod q. \quad (159)$$

So for n=1,2,…, we obtain

$$R_n \bmod q = L_n \bmod q = M_n \bmod q. \text{ q.e.d.} \quad (160)$$

4.5. Addition and Multiplication of f(X,S)

Let ${}^1M_1$, ${}^2M_1$ and ${}^1M_2$, ${}^2M_2$ be the medium texts corresponding to the plaintexts m_1 and m_2 such that

$${}^1M_1:=(m_1+u_1)G+(m_1+v_1)H \bmod q \in O, \quad (161)$$

$${}^2M_1:=(m_1+hu_1)G+(m_1+kv_1)H \bmod q \in O, \quad (162)$$

$${}^1M_2:=(m_2+u_2)G+(m_2+v_2)H \bmod q \in O, \quad (163)$$

$${}^2M_2:=(m_2+hu_2)G+(m_2+kv_2H \bmod q \in O. \quad (164)$$

We define the addition and multiplication of f(X,S) as

follows.

[Addition]

$f({}^iM_1,S)+ f({}^iM_2,S) \bmod q \in O$

$= A_1^{-1}(\ldots(A_r^{-1}(S\ (A_r(..\ (A_1\ {}^iM_1)...) + A_1^{-1}(\ldots(A_r^{-1}(S\ (A_r(..\ (A_1\ {}^iM_2)...)) \bmod q$

$= A_1^{-1}(\ldots(A_r^{-1}(S\ (A_r(..\ (A_1\ ({}^iM_1+{}^iM_2))..) \bmod q$

$=f({}^iM_1+{}^iM_2,S) \bmod q \in O.(i=1,2)$ (165)

[Multiplication]

$f({}^iM_1,S)\{\ [f(1,S)\ ]^{-1}[f({}^iM_2,S)g(1,S)]\} \bmod q \in O$

$=f({}^iM_1,S)\{[f(1,S)]^{-1}[(A_1^{-1}(\ldots(A_r^{-1}(S(A_r(..(A_1{}^iM_2)...)$

$(\ldots(1A_1)\ldots)A_r)S)A_r^{-1})\ldots)A_1^{-1})]\}$

from Theorem 8

$=f({}^iM_1,S)\{[f(1,S)]^{-1}[(A_1^{-1}(\ldots(A_r^{-1}(S(A_r(..(A_11)...)$

$(\ldots({}^iM_2A_1)\ldots)A_r)S)A_r^{-1})\ldots)A_1^{-1})]\}$

$=f({}^iM_1,S)\ \{[\ f(1,S)\ ]^{-1}\ [\ f(1,S)g({}^iM_2,S)]\} \bmod q$

from Lemma 1,

$=f({}^iM_1,S)g({}^iM_2,S) \bmod q$

$=[A_1^{-1}(\ldots(A_r^{-1}(S(A_r(..(A_1{}^iM_1)...)][(\ldots({}^iM_2A_1)\ldots$

$)A_r)S)A_r^{-1})\ldots)A_1^{-1}]$

from Theorem 8

$=[A_1^{-1}(\ldots(A_r^{-1}(S\ (A_r(..\ (A_1({}^iM_1{}^iM_2)...)][(\ldots(1A_1)\ldots$

$)A_r)S)A_r^{-1})\ldots)A_1^{-1}]$

$=f({}^iM_1{}^iM_2,S)g(1,S) \bmod q(i=1,2).$ (166)

Then we have

$$f({}^iM_1{}^iM_2,S)=[f({}^iM_1,S)\{[f(1,S)]^{-1}[f({}^iM_2,S)g(1,S)]\}][g(1,S)]^{-1} \bmod q \in O.\ (i=1,2) \quad (167)$$

That is, we can obtain $f({}^iM_1{}^iM_2,S)$ from $f({}^iM_1,S)$, $f({}^iM_2,S)$, $f(1,S)$ and $g(1,S)$ without $g({}^iM_2,S)$ $(i=1,2)$.

4.6. Octonion Elements Assumption OEA (q)

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

Octonion elements assumption OEA(q)

Let q be a prime. Let r be a secret integer parameter. Let $A:=\{A_1,\ldots,A_r\} \in O^r$ be secret parameters. Let $f(X,Y)= A_1^{-1}(\ldots(A_r^{-1}\ (Y\ (A_r(\ldots(A_1X)\ldots) \bmod q \in O[X,Y]$ and $g(X,Y)= (\ldots(XA_1)\ldots)A_r)Y)A_r^{-1})\ldots)A_1^{-1} \bmod q \in O[X,Y]$ be the basic enciphering function and sub-basic enciphering function where X and Y are variables.

In the OEA(q) assumption, the adversary A_d is given $f(X,Y)$, $g(X,Y)$ and his goal is to find a set of parameters $A=\{A_1,\ldots,A_r\} \in O^r$ with the order of the elements $A_1,\ldots, A_r$. For parameters $r= r(\lambda)$ defined in terms of the security parameter λ and for any PPT adversary A_d we have

$$\Pr[A_1^{-1}(\ldots(A_r^{-1}(Y(A_r(\ldots(A_1X)\ldots))\ldots) \bmod q=\{f_{ijk}\}(i,j,k= 0,\ldots,7),\ (\ldots(XA_1)\ldots)A_r)Y)A_r^{-1})\ldots)A_1^{-1} \bmod q=\{g_{ijk}\}(i,j,k =0,\ldots,7):\ A=\{A_1,\ldots,A_r\}\leftarrow A_d(1^\lambda,q,f(X,Y),g(X,Y))]= \mathrm{negl}(\lambda). \quad (168)$$

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

4.7. Property of Proposed fully Homomorphic Encryption

The syntax of proposed scheme is given as follows.

-Key-Generation. The algorithm KeyGen, on input the security parameter 1^λ and system parameter (q,S) outputs

$sk\leftarrow KeyGen(1^\lambda)$ where $sk=(r_A, A_j(j=1,\ldots,r_A), G_A)$ is a secret encryption key and

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

-Encryption. The algorithm Enc, on input system parameter (q,S) and secret keys of user B, $sk_B=(r_B, B_j(j=1,\ldots,r_B), G_B)$, public key of user A, $pk_A=(\{f_{Aijk}\}_{0\leqq i,j,k\leqq 7}, \{g_{Aijk}\}_{0\leqq i,j,k\leqq 7})$ and a plaintext $m\in Fq$, outputs a ciphertext $C(m;sk_B, pk_A)\in O^2 \leftarrow Enc(sk_B, pk_A;m)$.

-Decryption. The algorithm Dec, on input system parameter (q,S), secret keys of user A, sk_A, public key of user B, pk_B and a ciphertext $C(m;sk_B, pk_A)$, outputs plaintext $m^* \in Fq = Dec(sk_A,pk_B;C(m;sk_B,pk_A))$ where $C(m;sk_B,pk_A) \leftarrow Enc(sk_B, pk_A;m)$.

-Homomorphic-Evaluation. The algorithm Eval, on input system parameter (q,S), an arithmetic circuit ckt, and a tuple of n ciphertexts $(C_1,\ldots, C_n)\in O^{2n}$, outputs an evaluated cipher text $C'\leftarrow Eval(ckt; C_1,\ldots, C_n)$ where $C_j= C(m_j;sk_B, pk_A)$.

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

1. Homomorphism: Let $CR = \{CR_\lambda\}_{\lambda\in N}$ be the set of all polynomial sized arithmetic circuits. On input $sk \leftarrow KeyGen(1^\lambda)$, $pk\leftarrow KeyGen(1^\lambda), \forall ckt \in CR_\lambda, \forall(m_1,\ldots,m_n) \in Fq^n$ where $n= n(\lambda)$, $\forall(C_1,\ldots,C_n)\in O^{2n}$ where $C_j=C(m_j;sk_B,pk_A)\leftarrow Enc(sk_B,pk_A;m_j),(j =1,\ldots,n)$, we have $Dec(sk_A, pk_B ;Eval(ckt; C_1,\ldots,C_n)) = ckt(m_1,\ldots,m_n)$.

Then it holds that:

$$\Pr[Dec(sk_A,pk_B;Eval(ckt; C_1,\ldots,C_n))\neq ckt(m_1,\ldots,m_n)] =\mathrm{negl}(\lambda). \quad (169)$$

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

4.8. Procedure for Constructing Proposed Public-Key Encryption

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

User B tries to send his information to user A by using the public-key of user A pk_A and the secret key of user B sk_B through the insecure line.

(1) System centre publishes the system parameter(q,S).

(2) User A downloads system parameter (q,S) and selects $sk_A=(r_A, A_j(j=1,\ldots,r_A), G_A)$ which is a secret key of user A and generates the public key of user A $pk_A=(\{f_{Aijk}\}_{0\leqq i,j,k\leqq 7}, \{g_{Aijk}\}_{0\leqq i,j,k\leqq 7})$ such that

$f_A(X,Y):=A_1^{-1}(\ldots(A_{rA}^{-1}(Y(A_{rA}(\ldots(A_1X)\ldots) \bmod q \in O[X,Y]$

$=\{f_{Aijk}\}(i,j,k=0,\ldots,7),$ (170)

$g_A(X,Y):=(\ldots(XA_1)\ldots)A_{rA})Y)A_{rA}^{-1})\ldots)A_1^{-1} \bmod q\in O[X, Y]$

$=\{g_{ijk}\}(i,j,k=0,\ldots,7),$ (171)

User A sends $[\{f_{Aijk}\}, \{g_{Aijk}\}\ (i,j,k=0,\ldots,7)]$ to system centre.

(3) User B downloads system parameter (q,S) and selects $sk_B=(r_B, B_j(j=1,\ldots,r_B),G_B)$ which is a secret key of user B and generates the public key of user B $pk_B=(\{f_{Bijk}\}_{0\leq i,j,k\leq 7}, \{g_{Bijk}\}_{0\leq i,j,k\leq 7})$ such that

$f_B(X,Y):= B_1^{-1}(\ldots(B_{rB}^{-1}(Y(B_{rB}\ (\ldots(B_1X)\ldots) \bmod q\in O[X, Y]$

$=\{f_{Bijk}\}(i,j,k=0,\ldots,7),$ (172)

$g_B(X,Y):= (\ldots(XB_1)\ldots)B_{rB})Y)B_{rB}^{-1})\ldots)B_1^{-1} \bmod q\in O[X, Y]$

$=\{g_{ijk}\}(i,j,k=0,\ldots,7).$ (173)

User B sends $[\{f_{Bijk}\},\{g_{Bijk}\}\ (i,j,k=0,\ldots,7)]$ to system centre.

(4) User B downloads $f_A(X,Y)=\{f_{Aijk}\}$, $g_A(X,Y)=\{g_{Aijk}\}$ $(i,j,k=0,\ldots,7)$ from system centre.

(5) User B generates the common enciphering function $f_{BA}(X,Y)$ as follows.

$f_{B1\text{-}1}(X,Y):=f_A(f_A(X,Y),B_1^{-1})$

$=A_1^{-1}\ (\ldots(A_{rA}^{-1}\ (B_1^{-1}(A_{rA}\ (\ldots(A_1\ [A_1^{-1}\ (\ldots(A_{rA}^{-1}\ (Y(A_{rA}\ (\ldots(A_1X)\ldots))))\ldots)])\ldots)))\ldots)$

$=A_1^{-1}\ (\ldots(A_{rA}^{-1}\ (B_1^{-1}(Y(A_{rA}\ (\ldots(A_1X)\ldots)))))\ldots) \bmod q\in O[X,Y]$ (174)

$f_{B2\text{-}1}(X,Y):= f_{B1\text{-}1}\ (f_A(X,Y),B_2^{-1})$

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(B_2^{-1}(A_{rA}(\ldots(A_1^{-1}[A_1(\ldots(A_{rA}^{-1}\ (Y(A_{rA}(\ldots(A_1X)\ldots)\ldots)])\ldots)$

$=A_1^{-1}\ (\ldots(A_{rA}^{-1}\ (B_1^{-1}(B_2^{-1}(Y(A_{rA}\ (\ldots(A_1X)\ldots)\ldots) \bmod q\in O[X,Y]$ (175)

… …

$f_{BrB\text{-}1}(X,Y):= f_{BrB\text{-}1\text{-}1}(f_A(X,Y),B_{rB}^{-1})$

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(A_{rA}(\ldots(A_1[A_1^{-1}(\ldots(A_{rA}^{-1}\ (Y(A_{rA}(\ldots(A_1X)\ldots)\ldots)])\ldots)$

$=A_1^{-1}(\ldots(A_{rA}^{-1}\ (B_1^{-1}(\ldots(B_{rB}^{-1}(Y(A_{rA}\ (\ldots(A_1X)\ldots)\ldots) \bmod q\in O[X,Y]$ (176)

$f_{BrB}(X,Y):= f_{BrB\text{-}1}(f_A(X,B_{rB}),Y)$

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(Y(A_{rA}\ (\ldots(A_1[A_1^{-1}(\ldots(A_{rA}^{-1}\ (B_{rB}(A_{rA}(\ldots(A_1X)\ldots)\ldots)])\ldots)$

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(Y(B_{rB}\ (A_{rA}(\ldots(A_1X)\ldots) \bmod q\in O[X,Y]$ (177)

$f_{BrB\text{-}1}(X,Y)= f_{BrB}\ (f_A(X,B_{rB\text{-}1}),Y)$

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(Y(B_{rB}(A_{rA}(\ldots(A_1[A_1^{-1}(\ldots(A_{rA}^{-1}\ (B_{rB\text{-}1}(A_{rA}(\ldots(A_1X)\ldots)])\ldots) \bmod q\in O[X,Y]$ (178)

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(Y(B_{rB}(B_{rB\text{-}1}(A_{rA}(\ldots(A_1X)\ldots) \bmod q\in O[X,Y]$ (179)

… …

$f_{BA}(X,Y)=f_{B1}(X,Y) := f_{B2}(f_A(X,B_1),Y)$

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(Y(B_{rB}(\ldots(B_2(A_{rA}(\ldots(A_1[A_1^{-1}\ (\ldots(A_{rA}^{-1}(B_1(A_{rA}(\ldots(A_1X)\ldots)])\ldots) \bmod q\in O[X,Y]$

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(Y(B_{rB}(\ldots(B_1(A_{rA}(\ldots(A_1X)\ldots) \bmod q\in O[X,Y]$

$=\{f_{BAijk}\}(i,j,k=0,\ldots,7).$ (180)

(6) User B generates the fixed secret parameters T_{BA} and $\beta(=(g_1(h\text{-}k))^{-1} \bmod q)$ as follows.

$T_{BA}= f_{BA}(1,S)$

$=A_1^{-1}(\ldots(A_{rA}^{-1}\ (B_1^{-1}(\ldots(B_{rB}^{-1}(S(B_{rB}(\ldots(B_1(A_{rA}(\ldots(A_11)\ldots)$ (181)

$\beta=(g_1(h\text{-}k))^{-1} \bmod q$ (182)

(7) User B generates the sub-common enciphering function $g_{BA}(X,Y)$ in the same manner as follows.

$g_{BA}(X,Y):=$

$(\ldots((XA_1)A_2)\ldots)A_{rA})B_1)..)B_{rB})Y)B_{nB}^{-1})..)B_1^{-1})A_{nA}^{-1})\ \ldots)A_1^{-1} \bmod q\in O[X,Y].$ (183)

(8) User A generate $f_{AB}(X,Y)$ and $g_{AB}(X,Y)$ such that

$f_{AB}(X,Y):=A_1^{-1}(\ldots(A_{rA}^{-1}(f_B((A_{rA}(\ldots(A_1X)\ldots),Y)))\ldots) \in O\ [X,Y]$

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(Y(B_{rB}(\ldots(B_1(A_{rA}(\ldots(A_1X)\ldots) \in O[X,Y]$

$=\{f_{ABijk}\}(i,j,k=0,\ldots,7) = f_{BA}(X,Y)\in O[X,Y],$ (184)

$g_{AB}(X,Y):=(\ldots((XA_1)A_2)\ldots)A_{rA})B_1)..)B_{rB})Y)B_{rB}^{-1})..)B_1^{-1})$

$A_{rA}^{-1})\ldots)A_1^{-1} \bmod q\in O[X,$ (185)

(9) User B enciphers the plaintext m by using $f_{BA}(X,Y)$ such that

$C(m):= [f_{BA}({}^1M, T_{BA}); f_{BA}({}^2M, T_{BA}),]\in O^2$

$=({}^1c_0,\ldots,{}^1c_7;{}^2c_0,\ldots,{}^2c_7)$ (186)

where

${}^1M:= (m+u)G_B+(m+v)H_B \bmod q\in O,$ (187)

${}^2M:=((m+hu)G_B+ (m+kv)H_B \bmod q\in O,$ (188)

$T_{BA} =f_{BA}(1,S)\in O,$ (189)

(10) User B sends $[C(m)= ({}^1c_0,\ldots,{}^1c_7;{}^2c_0,\ldots,{}^2c_7)\in O^2, \beta_B]$ to user A

through the insecure line.

(11) User A receives $[C(m)= ({}^1c_0,\ldots,{}^1c_7;{}^2c_0,\ldots,{}^2c_7)\in O^2, \beta_B]$ and deciphers as follows.

User A calculates T_{AB} .

$T_{AB}= f_{AB}(1,S)$

$=A_1^{-1}(\ldots(A_{rA}^{-1}\ (B_1^{-1}(\ldots(B_{rB}^{-1}(S(B_{rB}(\ldots(B_1(A_{rA}(\ldots(A_11)\ldots)$

$= T_{BA} \bmod q.$ (190)

Let $({}^{i}z_0,\ldots,{}^{i}z_7) := {}^{i}M$ (i=1,2).
$f_{AB}({}^{i}M, T_{AB})$ (i=1,2)
$=A_1^{-1}(\ldots(A_{nA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(T_{AB}(B_{rB}(\ldots(B_1(A_{rA}(\ldots(A_1{}^{i}M)$
$\ldots)\bmod q\in O$
$=(f_{00}{}^{i}z_0+f_{01}{}^{i}z_1+\ldots+f_{07}{}^{i}z_7,$
$f_{10}{}^{i}z_0+f_{11}{}^{i}z_1+\ldots+f_{17}{}^{i}z_7,$
$\ldots.\ \ldots.$

$$f_{70}{}^{i}z_0+f_{71}{}^{i}z_1+\ldots+f_{77}{}^{i}z_7)^t \bmod q, = ({}^{i}c_0,\ldots,{}^{i}c_7)\ (i=1,2)\ . \quad (191)$$

where
$f_{jk}\in Fq$ (j,k=0,…,7).
User A solves above simultaneous equation to obtain $({}^{i}z_0,\ldots,{}^{i}z_7) = {}^{i}M$(i=1,2).
(12) User A recovers the plaintext m as follows.

$$[{}^{1}M]_0-([{}^{1}M]_1+[{}^{1}M]_1)\ \beta_B \bmod q = m\in Fq, \quad (192)$$

where

$$g_1\neq 0 \bmod q. \quad (193)$$

Theorem 9
For arbitrary $P,Q\in O$
$f_{BA}(P, T_{BA})\ g_{BA}(Q, T_{BA})$
$= f_{BA}(PQ, T_{BA})\ g_{BA}(1, T_{BA})$

$$= f_{BA}(1,T_{BA})\ g_{BA}(PQ, T_{BA}) \bmod q\in O. \quad (194)$$

[Proof]
From Theorem 8
$f_{BA}(P, T_{BA})g_{BA}(Q, T_{BA})$
$= f_{BA}(PQ, T_{BA})\ g_{BA}(1, T_{BA}) \bmod q\in O$

$$=f_{BA}(1, T_{BA})g_{BA}(PQ, T_{BA}) \bmod q\in O.\ \text{q.e.d.} \quad (195)$$

We notice that
$f_{BA}(P, T_{BA})g_{BA}(1, T_{BA})= f_{BA}(1P, T_{BA})g_{BA}(1, T_{BA})$

$$=f_{BA}(1, T_{BA})g_{BA}(P, T_{BA}) \bmod q\in O. \quad (196)$$

Then we have
$g_{BA}(P,T_{BA})=(f_{BA}(1,T_{BA}))^{-1}[f_{BA}(P,T_{BA})g_{BA}(1,T_{BA})]$
$\bmod q\ \in O,$ (197)
$f_{BA}(P,T_{BA}) =[f_{BA}(1,T_{BA})g_{BA}(P,T_{BA})]\ (\ g_{BA}(1,T_{BA}))^{-1}$
$\bmod q\in O.$ (198)

In case that the third party that does not know the value of T_{BA} tries to calculate the ciphertext corresponding to product of two plaintexts, he uses $[f_{BA}(1, T_{BA}), g_{BA}(1, T_{BA})]$ such that
$\{f_{BA}({}^{i}M_1,T_{BA})[(f_{BA}(1,T_{BA}))^{-1}(f_{BA}({}^{i}M_2,T_{BA})g_{BA}(1,T_{BA}))]\}$
$(g_{BA}(1,T_{BA}))^{-1}$

$$=f_{BA}({}^{i}M_1{}^{i}M_2,T_{BA}) \bmod q\in O.\ (i=1,2) \quad (199)$$

We describe in detail in next section.

4.9. Procedure for Addition and Multiplication on CipherTexts by Third Party

Here we show the procedure that the third party calculates the ciphertexts corresponding to the sum and the product of n plaintexts by using n ciphertexts.

(1) Through the insecure line, user B uploads his data $\{C(m_j)= [f_{BA}({}^{1}M_j,T_{BA});f_{BA}({}^{2}M_j,T_{BA})](j=1,\ldots,n)\}$ and $[f_{BA}(1, T_{BA}), g_{BA}(1, T_{BA})]$ to the cloud centre by using the common enciphering function $f_{BA}(X,Y)$ and sub-common enciphering function $g_{BA}(X,Y)$ of user A and user B where user A is also allowed to be user B.
(2) User B requests the ciphertext corresponding to the sum of m_i (i=1,…,n) and the ciphertext corresponding to the product of m_i (i=1,…,n) to user U.(user U is the data processing centre or the cloud centre).
(3) User U downloads the system parameter (q,S) from the system centre .
(4) User U downloads $\{C(m_j) =[f_{BA}({}^{1}M_j,T_{BA}); f_{BA}({}^{2}M_j,T_{BA})]\ (j=1,\ldots,n)\ \}$ and $[f_{BA}(1, T_{BA}), g_{BA}(1, T_{BA})]$ from cloud centre where

$${}^{1}M_j := (m_j+u_j)G_B+(m_j+v_j)H_B \bmod q\in O, \quad (200)$$

$${}^{2}M_j := (m_j+hu_j)G_B+(m_j+kv_j)H_B \bmod q\in O, \quad (201)$$

(j=1,…,n)

(5) User U calculates $[f_{BA}(1,T_{BA})]^{-1} \bmod q, [g_{BA}(1,T_{BA})]^{-1} \bmod q$.
(6) User U calculates the ciphertext corresponding to the sum of m_i (i=1,…,n) and the ciphertext corresponding to the product of mi (i=1,…,n) as follows.

[Ciphertext corresponding to sum of m_j (j=1,…,n)]
$C(m_{1+\ldots+n}):=C(m_1+\ldots+ m_n)$
$=[f_{BA}({}^{1}M_1 +\ldots+{}^{1}M_n,T_{BA}); f_{BA}({}^{2}M_1 +\ldots+{}^{2}M_n,T_{BA})]\in O^2$
$=[f_{BA}({}^{1}M_1,T_{BA}) +\ldots+f_{BA}({}^{1}M_h,T_{BA}) \bmod q;$
$f_{BA}({}^{2}M_1,T_{BA})+\ldots+f_{BA}({}^{2}M_h,T_{BA}) \bmod q]\in O^2$

$$= ({}^{1}c_{+0},\ldots,{}^{1}c_{+7};{}^{2}c_{+0},\ldots,{}^{2}c_{+7}). \quad (202)$$

[Ciphertext corresponding to product of m_j (j=1,…,n)]
(a) $f_{BA}({}^{i}M_1{}^{i}M_2,T_{BA})=$
$\{f_{BA}({}^{i}M_1,T_{BA})[(f_{BA}(1,T_{BA}))^{-1}(f_{BA}({}^{i}M_2,T_{BA})g_{BA}(1,T_{BA}))]\}$

$$(g_{BA}(1,T_{BA}))^{-1} \bmod q(i=1,2) \quad (203)$$

(b) $f_{BA}({}^{1}M_1{}^{2}M_2,T_{BA})=$
$\{f_{BA}({}^{1}M_1,T_{BA})[(f_{BA}(1,T_{BA}))^{-1}(f_{BA}({}^{2}M_2,T_{BA})g_{BA}(1,T_{BA}))]\}$

$$(g_{BA}(1,T_{BA}))^{-1} \bmod q \quad (204)$$

(c) $f_{BA}({}^{2}M_1{}^{1}M_2,T_{BA})=$
$\{f_{BA}({}^{2}M_1,T_{BA})[(f_{BA}(1,T_{BA}))^{-1}(f_{BA}({}^{1}M_2,T_{BA})g_{BA}(1,T_{BA}))]\}$

$$(g_{BA}(1,T_{BA}))^{-1} \bmod q \quad (205)$$

(d) $f_{BA}({}^{1}M_{12},T_{BA})=$
$[f_{BA}({}^{1}M_1{}^{1}M_2,T_{BA})-f_{BA}({}^{1}M_1{}^{2}M_2,T_{BA})]$

$$=f_{BA}(({}^{1}M_1{}^{1}M_2-{}^{1}M_1{}^{2}M_2),T_{BA}) \quad (206)$$

(e) $f_{BA}({}^{2}M_{12},T_{BA})=$
$[f_{BA}({}^{2}M_1{}^{1}M_2,T_{BA})-f_{BA}({}^{2}M_1{}^{2}M_2,T_{BA})]$

$$=f_{BA}(({}^{2}M_1{}^{1}M_2-{}^{2}M_1{}^{2}M_2) ,T_{BA}) \quad (207)$$

(f) $C(m_1m_2)= C(m_{12})= [f_{BA}({}^1M_{12},T_{BA}); f_{BA}({}^2M_{12},T_{BA})]$
$=[f_{BA}(({}^1M_1{}^1M_2-{}^1M_1{}^2M_2)) ,T_{BA});$
$f_{BA}(({}^2M_1{}^1M_2-{}^2M_1{}^2M_2) ,T_{BA})]\in O^2$ (208)

… …

(g) In the same manner
$f_{BA}({}^1M_{12\ldots n},T_{BA})=$

$[f_{BA}({}^1M_{12\ldots n-1}{}^1M_n,T_{BA})-f_{BA}({}^1M_{12\ldots n-1}{}^2M_n,T_{BA})]$ (209)

$=f_{BA}(({}^1M_{12\ldots n-1}{}^1M_n-{}^1M_{12\ldots n-1}{}^2M_n),T_{BA}))$,
$f_{BA}({}^2M_{12\ldots n},T_{BA})=$
$[f_{BA}({}^2M_{12\ldots n-1}{}^1M_n,T_{BA})-f_{BA}({}^2M_{12\ldots n-1}{}^2M_n,T_{BA})]$

$=f_{BA}(({}^2M_{12\ldots n-1}{}^1M_n- {}^2M_{12\ldots n-1}{}^2M_n),T_{BA}))$ (210)

(h) $C(m_1m_2...m_n)= C(m_{12\ldots n}) \in O^2$
$= [f_{BA}({}^1M_{12\ldots n},T_{BA}); f_{BA}({}^2M_{12\ldots n},T_{BA})]$

$= ({}^1c_{*0},\ldots,{}^1c_{*7}; {}^2c_{*0},\ldots,{}^2c_{*7})$. (211)

(7) User U sends $\{({}^1c_{+0},\ldots,{}^1c_{+7}; {}^2c_{+0},\ldots,{}^2c_{+7})$ and $({}^1c_{*0},\ldots,{}^1c_{*7}; {}^2c_{*0},\ldots,{}^2c_{*7})\}$ to user B.

(8) ser B deciphers to obtain $(m_1+\ldots+ m_n) \bmod q$ and $m_1m_2 \ldots m_n \bmod q$ as follows.

Let

$${}^1M_+=({}^1s_{+0},\ldots,{}^1s_{+7}):={}^1M_1 +\ldots+{}^1M_n \bmod q, \quad (212)$$

$${}^2M_+=({}^2s_{+0},\ldots,{}^2s_{+7}):={}^2M_1 +\ldots+{}^2M_n \bmod q, \quad (213)$$

$${}^1M_*=({}^1s_{*0},\ldots,{}^1s_{*7}):= {}^1M_{12\ldots n} \bmod q, \quad (214)$$

$${}^2M_*=({}^2s_{*0},\ldots,{}^2s_{*7}):= {}^2M_{12\ldots n} \bmod q. \quad (215)$$

$f_{AB}({}^iM_+, T_{AB})$
$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(T_{AB}(B_{rB}(\ldots(B_1(A_{rA}(\ldots(A_1$
${}^iM_+)\ldots) \bmod q\in O$
$=(f_{00}{}^is_{+0}+f_{01}{}^i s_{+1}+ \ldots+f_{07}{}^is_{+7},$
$f_{10}{}^is_{+0}+ f_{11}{}^is_{+1}+ \ldots+ f_{17}{}^is_{+7},$
…. ….
$f_{70}{}^is_{+0}+ f_{71}{}^is_{+1}+ \ldots+ f_{77}{}^is_{+7})^t \bmod q,$

$= ({}^ic_{+0},\ldots,{}^ic_{+7})$ (i=1,2). (216)

$({}^is_{+0},\ldots,{}^is_{+7})$ is obtained by solving above simultaneous equation (i=1,2).

User B has

$$m_1+\ldots+ m_n ={}^1s_{+0}-({}^1s_{+1}+{}^2s_{+1})\,\beta_B \bmod q\in Fq. \quad (217)$$

$f_{AB}({}^iM_*, T_{AB})$
$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(T_{AB}(B_{rB}(\ldots(B_1(A_{rA}(\ldots(A_1$
${}^iM_*)\ldots) \bmod q\in O$
$=(f_{00}{}^is_{*0}+f_{01}{}^is_{*1}+ \ldots+f_{07}{}^i s_{*7},$
$f_{10}{}^is_{*0}+f_{11}{}^is_{*1}+ \ldots+ f_{17}{}^is_{*7},$
…. ….
$f_{70}{}^is_{*0}+ f_{71}{}^is_{*1}+ \ldots+ f_{77}{}^is_{*7})^t \bmod q,$

$= ({}^ic_{*0},\ldots,{}^ic_{*7})$ (i=1,2). (218)

$({}^is_{*0},\ldots,{}^is_{*7})$ is obtained by solving above simultaneous equation(i=1,2).

User B has

$$m_1m_2 \ldots m_n ={}^1s_{*0} -({}^1s_{*1}+{}^2s_{*1})\,\beta_B \bmod q\in Fq. \quad (219)$$

5. Analysis of Proposed Scheme

Here we analyse the proposed fully homomorphic encryption scheme.

5.1. Ciphertext Square Attack

Ciphertext is given as follows.

$$C(m):= [f_{BA}({}^1M, T_{BA}); f_{BA}({}^2M, T_{BA}),], \quad (220)$$

$${}^1M:= (m+u)G+(m+v)H \bmod q\in O, \quad (221)$$

$${}^2M:= (m+hu)G+(m+kv)H) \bmod q\in O. \quad (222)$$

As

$$({}^1M)^2 =(m+u)^2G+(m+v)^2H \bmod q\neq m({}^1M), \quad (223)$$

$$({}^2M)^2 = (m+hu)^2G+(m+kv)^2H \bmod q\neq m({}^2M), \quad (224)$$

we have

$$f_{BA}(({}^jM)^2,T_{BA})\neq mf_{BA}({}^jM,T_{BA}) \ (j=1,2). \quad (225)$$

"Ciphertext square attack" is not efficient for the proposed encryption scheme.

5.2. Computing A_i from $\{f_{ijk}\}$, Coefficients of f(X,Y) and g(X,Y)

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

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

$f(X,Y)= A_1^{-1}(\ldots(A_r^{-1}(Y(A_r(.. (A_1X)...) \bmod q\in O[X,Y]$
$=(f_{000}x_0y_0+f_{001}x_0y_1+ \ldots+f_{077}x_7y_7,$
$f_{100}x_0y_0+f_{101}x_0y_1+ \ldots+f_{177}x_7y_7,$
…. ….
$f_{700}x_0y_0+f_{701}x_0y_1+ \ldots+f_{777}x_7y_7)^t,$

$= \{f_{ijk}\}$ (i,j,k=0,…,7), (226)

$g(X,Y):=(\ldots((XA_1)A_2)\ldots)A_r)Y)A_r^{-1})\ldots)A_1^{-1} \bmod q\in O[X,Y]$
$=(g_{000}x_0y_0+g_{001}x_0y_1+ \ldots+g_{077}x_7y_7,$
$g_{100}x_0y_0+g_{101}x_0y_1+ \ldots+g_{177}x_7y_7,$
…. ….
$g_{700}x_0y_0+g_{701}x_0y_1+ \ldots+g_{777}x_7y_7)^t,$

$= \{g_{ijk}\}$(i,j,k=0,…,7). (227)

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

We try to find A_i(i=1,…,r) from f_{ijk}, $g_{ijk}\in Fq$ (i,j,k=0,…,7).

In case that r=56 the number of unknown variables (A_j (j=1,…,56)) is 448(=56*8), the number of equations is 896(=(64*8-64)*2) such that

$$\left.\begin{array}{c} F_{001}(A_1,\dots,A_{56}) = f_{001}\ mod\ q, \\ \dots\ \dots \\ F_{ijk}(A_1,\dots,A_{56}) = f_{ijk} mod\ q (k\neq 0), \\ \dots\ \dots \\ F_{777}(A_1,\dots,A_{56}) = f_{777}\ mod\ q, \\ G_{001}(A_1,\dots,A_{56}) = g_{001}\ mod\ q, \\ \dots\ \dots \\ G_{ijk}(A_1,\dots,A_{56}) = g_{ijk} mod\ q (k\neq 0), \\ \dots\ \dots \\ G_{777}(A_1,\dots,A_{56}) = g_{777}\ mod\ q, \end{array}\right\} \quad (228)$$

where $F_{001},\dots, F_{777}, G_{001},\dots, G_{777}$ are the 112^{th} $(=56*2)^{th}$ algebraic multivariate equations.

Then the complexity G required for solving above simultaneous equations by using Gröbner basis[18] is given such as

$$G>G'=({}_{448+dreg}C_{dreg})^w=({}_{493}C_{45})^w\approx 2^{509}>> 2^{80}, \quad (229)$$

where G' is the complexity required for solving 896(=448*2) simultaneous quadratic equations with 448 variables by using Gröbner basis, where w=2.39, and

$$d_{reg}\approx 0.0858*448+1.04*(448)\text{^}(1/3)-1.47+1.71*448\text{^}(-1/3)+448\text{^}(-2/3)>45. \quad (230)$$

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

5.3. Computing Medium Text ${}^jM$ and A_j, B_j from Ciphertext C(m)

Ciphertext C(m)

$$=({}^1c_0,\dots,{}^1c;{}^2c_0,\dots,{}^2c)=[f_{BA}({}^1M,T_{BA});\ f_{BA}({}^2M,T_{BA})] \quad (231)$$

is generated by user B as follows.

Let $({}^jz_0,\dots,{}^jz_7) : ={}^jM$ (j=1,2).

$C(m) =f_{BA}({}^jM,T_{BA})\in O$

$= A_1^{-1}(\dots(A_{rA}^{-1}(B_1^{-1}(\dots(B_{rB}^{-1}(T_{BA} \ (B_{rB}(\dots(B_1(A_{rA}(\dots(A_1\ {}^jM)\dots)\in O$

$=(f_{00}{}^jz+f_{01}{}^jz_1+ \dots+f_{07}{}^jz_7,$

$f_{10}{}^jz_0+f_{11}{}^jz_1+ \dots+f_{17}{}^jz_7,$

$\dots. \dots.$

$f_{70}{}^jz_0+f_{71}{}^jz_1+ \dots+f_{77}{}^jz_7)^t,$

$= ({}^jc_0,\dots,{}^jc_7)$ (j=1,2). (232)

$({}^jz_0,\dots,{}^jz_7) ={}^jM$(j=1,2) is obtained by solving above simultaneous equation.

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

We try to find medium text ${}^jM$ and A_h, B_k (j=1,2 ;h=1,…,r_A ;k=1,…,r_B) from ${}^jc_h\in Fq$ (j=1,2;h=0,…,7).

In case that r_A =56 and r_B=56 the number of unknown variables (($^jz_0,\dots,{}^jz_7$)(j=1,2), T_{BA}, A_h , B_k, (h,k=1,…,56)) is 920(=8*2+8+2*56*8), the number of equations is 16 such that

$$\left.\begin{array}{c} F_0(({}^jz_0,\dots,{}^jz_7),A_1,..,A_{56},B_1,..,B_{56}) = {}^jc_0\ mod\ q, \\ F_1(({}^jz_0,\dots,{}^jz_7),A_1,..,A_{56},B_1,..,B_{56}) = {}^jc_1\ mod\ q, \\ \dots\ \dots \\ F_7(({}^jz_0,\dots,{}^jz_7),A_1,..,A_{56},B_1,..,B_{56}) = {}^jc_7\ \mathrm{mod}\ q, \\ (j=1,2) \end{array}\right\} \quad (233)$$

where $F_0,\dots,F_7$ are the 226^{th}(=56*2*2+2)th algebraic multivariate equations.

Then the complexity G required for solving above simultaneous equations by using Gröbner basis [18] is given such as

$$G>G'=({}_{920+dreg}C_{dreg})^w=({}_{104532}C_{920})^w >> 2^{80}, \quad (234)$$

where G' is the complexity required for solving 921 simultaneous algebraic equations with 920 variables by using Gröbner basis,

where w=2.39, and

$$d_{reg}\approx 103612(=921*(226-1)/2-0\sqrt{(921*(226\text{^}2-1)/6)}). \quad (235)$$

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

5.4. Attack by Using the Ciphertexts of m and -m

We show that we cannot easily distinguish the ciphertexts corresponding to m and -m. We try to attack by using "m and -m attack". We define the medium texts ${}^1M_+$, ${}^2M_+$ by

$${}^1M_+:=(m+u)G_B+(m+v)H_B \ \mathrm{mod}\ q\in O, \quad (236)$$

$${}^2M_+:=(m+hu)G_B+(m+kv)H_B \ \mathrm{mod}\ q\in O. \quad (237)$$

where $u,v\in Fq$ are selected randomly, and plaintext $m\in Fq$.

We define the medium texts ${}^1M_-$, ${}^2M_-$ corresponding to the plaintext -m by

$${}^1M_-:=(-m+u')G_B+(-m+v')H_B \ \mathrm{mod}\ q\in O, \quad (238)$$

$${}^2M_-:=(-m+hu')G_B+(-m+kv')H_B \ \mathrm{mod}\ q\in O, \quad (239)$$

where $u',v'\in Fq$ are selected randomly.

The ciphertext corresponding to m , $C(m) =[f_{BA}({}^1M_+, T_{BA}); f_{BA}({}^2M_+, T_{BA})]\in O^2$ is given as follows.

$f_{BA}({}^1M_+, T_{BA})\in O$

$$=A_1^{-1}(\dots(A_{rA}^{-1}(B_1^{-1}(\dots(B_{rB}^{-1}(T_{BA}(B_{rB}(\dots(B_1(A_{rA}(\dots(A_1\ {}^1M_+)\dots)\in O, \quad (240)$$

$f_{BA}({}^2M_+, T_{BA})\in O$

$$=A_1^{-1}(\dots(A_{rA}^{-1}(B_1^{-1}(\dots(B_{rB}^{-1}(T_{BA}(B_{rB}(\dots(B_1(A_{rA}(\dots(A_1\ {}^2M_+)\dots)\in O. \quad (241)$$

The ciphertext corresponding to -m , $C(-m) =[f_{BA}({}^1M_-, T_{BA}); f_{BA}({}^2M_-, T_{BA})]\in O^2$ is given as follows.

$f_{BA}({}^1M_-, T_{BA})$

$$=A_1^{-1}(\dots(A_{rA}^{-1}(B_1^{-1}(\dots(B_{rB}^{-1}(T_{BA}\ (B_{rB}(\dots(B_1(A_{rA}(\dots(A_1\ {}^1M_-)\dots)\in O, \quad (242)$$

$f_{BA}({}^2M_-, T_{BA}) \in O$

$=A_1^{-1}(\ldots(A_{rA}^{-1}(B_1^{-1}(\ldots(B_{rB}^{-1}(T_{BA}\ (B_{rB}(\ldots(B_1(A_{rA}(\ldots(A_1\ {}^2M_-)\ldots) \in O.$ (243)

As m-m= 0 mod q, we have

$f_{BA}({}^1M_+, T_{BA})+ f_{BA}({}^1M_-, T_{BA}) \bmod q$

$= f_{BA}({}^1M_+ + {}^1M_-, T_{BA}) \bmod q$

$=f_{BA}((m+u)G_B+(m+v)H_B+(-m+u')G_B+(-m+v')H_B), T_{BA})$

$= f_{BA}((u+u')\ G_B +(v+v')H_B), T_{BA}) \bmod q$ (244)

As in general $u+u' \neq 0 \bmod q \in Fq$, $v+v' \neq 0 \bmod q \in Fq$,we have

$f_{BA}({}^1M_+, T_{BA})+ f_{BA}({}^1M_-, T_{BA}) \bmod q \neq 0.$ (245)

In the same manner it is said that

$f_{BA}({}^2M_+, T_{BA})+ f_{BA}({}^2M_-, T_{BA}) \bmod q \neq 0.$ (246)

When m-m= 0 mod q, we can calculate

$| f_{BA}({}^1M, T_{BA})+ f_{BA}({}^1M_-, T_{BA}) |^2$ as follows.

$| f_{BA}({}^1M, T_{BA})+ f_{BA}({}^1M_-, T_{BA}) |^2 \bmod q$

$=| f_{BA}((u+u')\ G_B +(v+v')H_B, T_{BA})|^2 \bmod q$

$= |T_{BA}|^2|(u+u')\ G_B +(v+v')H_B|^2 \bmod q,$

$=|T_{BA}|^2[(u+u'+v+v')^2/4-((u+u'-(v+v'))^2/4] \bmod q$

$=|T_{BA}|^2[(u+u')(v+v')] \bmod q$

$\neq 0 \bmod q$ (in general). (247)

In the same manner

$| f_{BA}({}^2M, T_{BA})+ f_{BA}({}^2M_-, T_{BA}) |^2 \bmod q$

$=|T_{BA}|^2[hk(u+u')(v+v')] \bmod q$, (h,k are secret parameters)

$\neq 0 \bmod q$ (in general). (248)

It is said that the attack by using "m and -m attack" is not efficient. Then we cannot easily distinguish the cipher texts of m and -m.

6. The Size of the Modulus q and the Complexity for Enciphering /Deciphering

We consider the size of the modulus q. We select $q \approx 2^{2000}$.

(1) In case of $q \approx 2^{2000}$, the size of $f_{ijk} \in Fq$ (i,j,k=0,…,7) which are the coefficients of elements in $f(X,Y)=A_1^{-1}(\ldots(A_r^{-1}\ (Y(A_r(..\ (A_1X)...) \bmod q \in O[X,Y]$ is $(448)(\log_2 q)$bits ≈896kbits and the size of $g_{ijk} \in Fq$ (i,j,k=0,…,7) which are the coefficients of elements in $g(X,Y):=(\ldots((XA_1)A_2)\ldots)A_r)Y)A_r^{-1})\ldots)A_1^{-1} \bmod q \in O[X,Y]$ is $(448)(\log_2 q)$bits ≈896kbits. Then the size of f_{ijk} and g_{ijk} (i,j,k=0,…,7) is $2*(448)(\log_2 q)$bits ≈1792kbits. The size of plaintext m is 2kbits and the size of ciphertext $C(m) \in O$ is 32kbits.

(2) In case of r=56, $q \approx 2^{2000}$, the complexity to obtain f(X,Y) from $A_1,\ldots,A_r$ and q is

$(55*8*64+55*8*512)(\log_2 q)^2+56*(16*(\log_2 q)^2+2*(\log_2 q)^3) \approx 2^{41}$ bit-operations,

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

And the complexity to obtain g(X,Y) from $A_1,\ldots,A_r$ and q is $\approx 2^{41}$ bit-operations.

(3) In case of $r_B=56$, $q \approx 2^{2000}$, the complexity to obtain $f_{BA}(X,Y)$ from $f_A(X,Y)$, $B_1,\ldots,B_{rB}$, $B_{rB}^{-1},\ldots,B_1^{-1}$ and q is

$((512+64*8*8)*56+(512+64*8*8)*56)\ (\log_2 q)^2 \approx 2^{41}$ bit-operations.

In the same manner, the complexity to obtain $g_{BA}(X,Y)$ from $f_A(X,Y)$, $B_1,\ldots,B_{rB}$, $B_{rB}^{-1},\ldots,B_1^{-1}$ and q is

$((512+64*8*8)*56+(512+64*8*8)*56)(\log_2 q)^2 \approx 2^{41}$bit-operations.

(4) In case of $r_A=56$, $q \approx 2^{2000}$, the complexity to obtain $f_{AB}(X,Y)$ from $f_B(X,Y)$, $A_1,\ldots,A_{rA}$, $A_{rA}^{-1},\ldots,A_1^{-1}$ and q is

$((512+64*8*8)*56+(512+64*8*8)*56)(\log_2 q)^2 \approx 2^{41}$ bit-operations.

(5) In case of $q \approx 2^{2000}$, the complexity for enciphering m to obtain $C(m)=[\ f_{BA}({}^1M,T_{BA}), f_{BA}({}^2M,T_{BA})]$ from $f_{BA}(X,Y)$, ${}^1M$, ${}^2M$, T_{BA} and q is $2*(2*64*8)\ (\log_2 q)^2 \approx 2^{33}$ bit-operations.

(6) In case of $q \approx 2^{2000}$, the complexity for calculating $T_{BA} = f_{BA}(1,S)$ from $f_{BA}(X,Y)$, S and q is $64(\log_2 q)^2 \approx 2^{28}$ bit-operations.

(7) In case of $q \approx 2^{2000}$, the complexity for calculating $h = [f_{BA}(S,S)]_0$, $k = [f_{BA}(S,S)]_1$ from $f_{BA}(X,Y)$, S and q is at most $7*2*512*2(\log_2 q)^2 \approx 2^{36}$ bit-operations.

(8) In case of $q \approx 2^{2000}$, the complexity for deciphering $C(m) =[f_{BA}({}^1M, T_{BA}), f_{BA}({}^2M, T_{BA})]$ to obtain m from C(m), $f_{AB}(X,Y)$, T_{AB} , β and q is

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

$\approx(2*(512+232)+1)*2^{22}+16*2^{33}=1489*2^{22}+16*2^{33}$

$\approx 2^{38}$ bit-operations.

(9) In case of $r_A=56$, $q \approx 2^{2000}$, the complexity for calculating $f_{BA}({}^1M_{12},T_{BA})$, $f_{BA}({}^2M_{12},T_{BA})$ from $f_{BA}({}^1M_1,T_{BA})$, $f_{BA}({}^1M_2,S)$, $f_{BA}({}^2M_1,T_{BA})$, $f_{BA}({}^2M_2,S)$, $f_{BA}(1,T_{BA})$, $g_{BA}(1,T_{BA})$ and q is

$4*[4*64*(\log_2 q)^2]+2*2*(\log_2 q)^3+4*8*(\log_2 q)^2 \approx 2^{36}$ bit-operations.

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

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

where the size of modulus n is 2048bits.

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

7. Conclusion

We presented a fully homomorphic public-key encryption scheme with two ciphertexts based on the octonion ring over finite field. It was shown that proposed scheme is immune from "ciphertext square attack" ,"m and -m attack" and the Gröbner basis attacks and it does not require a "bootstrapping" process so that the complexity to encipher and decipher is not large. We described concretely how to construct the system over octonion ring. On the theoretical side, there are still some open problems, including the problem of whether octonion elements assumption OEA(q) holds or not, and there is a need for more careful studying of

attacks based on the algorithm for solving the multivariate algebraic equations of high degrees.

Appendix

Appendix A:
Octinv(A) ----------
$S \leftarrow a_0^2+a_1^2+\ldots+a_7^2 \bmod q$.
% $S^{-1} \bmod q$
q[1] ← q div S ;% integer part of q/S
r[1] ← q mod S ;% residue
k ←1
q[0] ← q
r[0] ← S
while r[k] ≠ 0
begin
k← k + 1
q[k] ← r[k−2] div r[k−1]
r[k] ← r[k−2] mod [rk−1]
end
Q [k−1] ← (-1)∗q[k−1]
L[k−1] ← 1
i ← k−1
while i > 1
begin
Q[i−1] ← (-1)∗Q[i] ∗q[i−1] + L[i]
L[i−1] ← Q[i]
i← i−1
end
invS ← Q[1] mod q
invA[0] ← 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:
Lemma 2
$A^{-1}(AB)= B \bmod q$
$(BA)A^{-1}= B \bmod q$
(Proof:)
$A^{-1}= (a_0 / |A|^2 \bmod q, -a_1 / |A|^2 \bmod q,\ldots, -a_7 / |A|^2 \bmod q)$.
AB mod q
= ($a_0b_0-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7 \bmod q$,
$a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3 \bmod q$,
$a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6 \bmod q$,
$a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1 \bmod q$,
$a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5 \bmod q$,
$a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4 \bmod q$,
$a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2 \bmod q$,
$a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0 \bmod q$).
$[A^{-1}(AB)]_0$
=$\{ a_0(a_0b_0-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7)$
$+a_1(a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3)$
$+ a_2(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6)$
$+a_3(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)$
$+a_4(a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5)$
$+ a_5(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4)$
$+a_6(a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2)$
$+a_7(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0)\}/|A|^2 \bmod q$
$=\{(a_0^2+a_1^2+\ldots+a_7^2)\ b_0\}\ /|A|^2 = b_0 \bmod q$
where $[M\ ]_n$ denotes the n-th element of $M \in O$.
$[A^{-1}(AB)]_1$
=$\{ a_0(a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3)$
$-a_1(a_0b_0-a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7)$
$-a_2(a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5)$
$-a_3(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0)$
$+a_4(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6)$
$- a_5(a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2)$
$+a_6(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4\ )$
$+a_7(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)\}\ /|A|^2 \bmod q$
$=\{(a_0^2+a_1^2+\ldots+a_7^2)\ b_1\}\ /|A|^2 = b_1 \bmod q$.
Similarly we have
$[A^{-1}(AB)]_i = b_i \bmod q\ (i=2,3,\ldots,7)$.
Then we have
$A^{-1}(AB)= B \bmod q$. q.e.d.
Appendix C:
Theorem 3
$L_AL_B= L_{AB} \bmod q \in Fq$
where
$A=(a_0,a_1,\ldots,a_7)$, $B=(b_0,b_1,\ldots,b_7)$, $C=(c_0,c_1,\ldots,c_7) \in O$,
$C=AB \bmod q \in O$.
$L_A=a_0^2+a_1^2+\ldots+a_7^2=0 \bmod q$,
$L_B=b_0^2+b_1^2+\ldots+b_7^2=0 \bmod q$
$L_{AB}=c_0^2+c_1^2+\ldots+c_7^2=0 \bmod q$
(Proof:)
AB mod q
= ($a_0b_0 - a_1b_1- a_2b_2- a_3b_3-a_4b_4- a_5b_5-a_6b_6-a_7b_7 \bmod q$,
$a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3 \bmod q$,
$a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6 \bmod q$,
$a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1 \bmod q$,
$a_0b_4+a_1b_2 -a_2b_1 -a_3b_6+a_4b_0+a_5b_7+ a_6b_3 -a_7b_5 \bmod q$,
$a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4 \bmod q$,
$a_0b_6+a_1b_5 -a_2b_7+a_3b_4 -a_4b_3 -a_5b_1+a_6b_0 +a_7b_2 \bmod q$,
$a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0 \bmod q$)
$L_{AB}= a_0^2(b_0^2+\ldots+ b_7^2)$
$+ a_1^2(b_1^2+ b_0^2+ b_4^2+ b_7^2+ b_2^2+ b_6^2+ b_5^2+b_3^2)$
$+ a_2^2(b_1^2+ b_0^2+ b_4^2+ b_7^2+ b_2^2+ b_6^2+ b_5^2+b_3^2)$
$+ a_3^2(b_3^2+ b_7^2+ b_5^2+ b_0^2+ b_6^2+ b_2^2+ b_4^2+b_1^2)$
$+ a_4^2(b_4^2+ b_2^2+ b_1^2+ b_6^2+ b_0^2+ b_7^2+ b_3^2+b_5^2)$
$+ a_5^2(b_5^2+ b_6^2+ b_3^2+ b_2^2+ b_7^2+ b_0^2+ b_1^2+b_4^2)$
$+ a_6^2(b_6^2+ b_5^2+ b_7^2+ b_4^2+ b_3^2+ b_1^2+ b_0^2+b_2^2)$
$+ a_7^2(b_7^2+ b_3^2+ b_1^2+ b_6^2+ b_5^2+ b_4^2+ b_2^2+b_0^2)$
$- 2a_0b_0\, a_1b_1+2\, a_0b_1a_1b_0 -\ldots.-a_6b_2a_7b_0+ a_6b_0\, a_7b_2 \bmod q$
$=(a_0^2+a_1^2+\ldots+a_7^2)(b_0^2+b_1^2+\ldots+b_7^2) \bmod q$
$= L_AL_B \bmod q$. q.e.d.

References

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

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

[3] 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.

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

[5] JS Coron, A Mandal, D Naccache, M Tibouchi ," Fully homomorphic encryption over the integers with shorter public keys", Advances in Cryptology–CRYPTO 2011, 487-504.

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

[7] 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/.

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

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

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

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

[12] Masahiro Yagisawa," Improved Fully Homomorphic Encryption without Bootstrapping", Cryptology ePrint Archive, Report 2017/763, 2017. http://eprint.iacr.org/.

[13] Masahiro Yagisawa," Fully homomorphic public-key encryption with small ciphertext size", Cryptology ePrint Archive, Report 2018/088, 2018. http://eprint.iacr.org/.

[14] Shigeo Tsujii , Kohtaro Tadaki , Masahito Gotaishi ,Ryo Fujita ,and Masao Kasahara ,"Proposal Integrated MPKC:PPS—STS Enhanced Perturbed Piece in Hand Method—," IEICE Tech. Rep.ISEC2009-27,SITE2009-19,ICSS2009-41(2009-07),July 2009.

[15] T. Matsumoto, and H. Imai, "Public quadratic polynomial-tuples for efficient signature verification and message-encryption," Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88, pp.419–453, New York, NY, USA, 1988, Springer-Verlag New York, Inc.

[16] S. Tsujii, K. Tadaki, and R. Fujita, "Piece in hand concept for enhancing the security of multivariate type public key cryptosystems: Public key without containing all the information of secret key," Cryptology ePrint Archive, Report 2004/366, 2004.

[17] C.Wolf, and B. Preneel, "Taxonomy of public key schemes based on the problem of multivariate quadratic equations," Cryptology ePrint Archive, Report 2005/077, 2005, http://eprint.iacr.org/.

[18] 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.

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