FHE with Recursive Ciphertext

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

Abstract. In this paper I propose 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. The scheme is based on the discrete logarithm assumption (DLA) and computational Diffie–Hellman assumption (CDH) of multivariate polynomials on octonion ring with composite number modulus. The scheme is immune from "*m* and - *m* attack".
keywords: fully homomorphic public-key encryption, discrete logarithm assumption, computational Diffie–Hellman assumption, octonion ring, factorization

§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 some fully homomorphic encryptions [11],[12],[18],[19],[20],[21],[22],[23],[24]. But the encryption schemes in previous works may be vulnerable to "m and -m attack".

In this paper I propose 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. The scheme is based on the discrete logarithm assumption (DLA) and computational Diffie–Hellman assumption (CDH) of multivariate polynomials on octonion ring with composite number modulus. The scheme is immune from "m and - m attack". The scheme is also based on computational difficulty to solve the multivariate algebraic equations of high degree while the almost all multivariate public-key cryptosystems [13],[14],[15],[16] proposed until now are based on the quadratic equations avoiding the explosion of the coefficients. Our scheme is against the Gröbner basis [3] attack, the differential attack, rank attack and so on.

§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. Recently, Nuida and Kurosawa proposed (batch) fully homomorphic encryption over integers [17].

§3. 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 3.

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

Let $r=pq$ be a composite number modulus to be as large as 2^{2000} where p and q are primes. Later (in section 6) we discuss the size of r, one of the system parameters.

Let O ,O_p and O_q be the octonion [2] rings over a residue class ring $R=\mathbf{Z}/r\mathbf{Z}$, $R_p=\mathbf{Z}/p\mathbf{Z}$, and $R_q=\mathbf{Z}/q\mathbf{Z}$ each such that

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

$$O_p=\{(a_0,a_1,\ldots,a_7) \mid a_j \in R_p\ (j=0,1,\ldots,7)\} \quad (1b)$$

$$O_q=\{(a_0,a_1,\ldots,a_7) \mid a_j \in R_q\ (j=0,1,\ldots,7)\} \quad (1c)$$

where

$$R=\mathbf{Z}/r\mathbf{Z},$$

$$R_p=\mathbf{Z}/p\mathbf{Z},$$

$$R_q=\mathbf{Z}/q\mathbf{Z}.$$

From Chinese remainder theorem $k \in R$ and $h \in R$ exist such that

$$pk+qh=1 \bmod r. \quad (2)$$

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

$$A=(a_0,a_1,\ldots,a_7),\ a_j \in R\ (j=0,1,\ldots,7), \quad (3a)$$

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

$AB \bmod r$

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

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

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

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

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

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

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

$$a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0 \bmod r) \quad (4)$$

$$A+B \bmod r$$

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

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

Let

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

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

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

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

§3.2 Order of the element in *O*

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

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

Theorem 1

Let $A:=(a_{10},a_{11},\dots,a_{17})\in O_q$, $a_{1j}\in R_q$ $(j=0,1,\dots,7)$.

Let $(a_{n0},a_{n1},\dots,a_{n7}) :=A^n\in O_q$, $a_{nj}\in R_q$ $(n=1,2,\dots;j=0,1,\dots,7)$.

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

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

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

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

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

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

(*Proof*:)

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

Theorem 2

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

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

where

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

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

(*Proof*:)

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

In the same manner we have

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

$$A^{Jp+1}=A \bmod p,$$

where

$$Jp= \mathrm{LCM}\,\{p^2\text{-}1, p\text{-}1\}=p^2\text{-}1,$$

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

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

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

where

$$J= \mathrm{LCM}\,\{Jp, Jq\}= \mathrm{LCM}\,\{ p^2\text{-}1,q^2\text{-}1\}.$$

§3.3. 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 r.

1) Non-commutative

$$AB \neq BA \bmod r.$$

2) Non-associative

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

3) Alternative

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

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

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

4) Moufang's formulae [2],

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

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

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

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

5) For positive integers n,m, we have

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

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

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

$$B(B^nA) = B(B^{n-1}(BA)) = ((BB^{n-1})B)A = B^{n+1}A \bmod r. \tag{21}$$

From (15) and (19), we have

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

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

… …

$$(AB^n)B^m = AB^{n+m} \bmod r.$$

In the same manner we have

$$B^m(B^n A) = B^{n+m} A \bmod r.$$

6) **Lemma 1**

$$A(B((AB)^n)) = (AB)^{n+1} \quad \bmod r,$$

$$(((AB)^n)A)B = (AB)^{n+1} \quad \bmod r\,.$$

where n is a positive integer and B has the inverse B^{-1}.

(*Proof*:)

From (14) we have

$$B(A(B((AB)^n) = ((BA)B)(AB)^n = (B(AB))(AB)^n = B(AB)^{n+1} \quad \bmod r.$$

Then

$$B^{-1}(B(A(B(AB)^n))) = B^{-1}(B\,(AB)^{n+1}) \bmod r,$$

$$A(B(AB)^n) = (AB)^{n+1} \quad \bmod r.$$

In the same manner we have

$$(((AB)^n)A)B = (AB)^{n+1} \quad \bmod r. \qquad \text{q.e.d.}$$

7) **Lemma 2**

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

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

(*Proof*:)

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

Theorem 3

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

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*:)

$$A^2 \bmod r$$

$$=(a_0a_0-a_1a_1-a_2a_2-a_3a_3-a_4a_4-a_5a_5-a_6a_6-a_7a_7 \bmod r,$$

$$a_0a_1+a_1a_0+a_2a_4+a_3a_7-a_4a_2+a_5a_6-a_6a_5-a_7a_3 \bmod r,$$

$$a_0a_2-a_1a_4+a_2a_0+a_3a_5+a_4a_1-a_5a_3+a_6a_7-a_7a_6 \bmod r,$$

$$a_0a_3-a_1a_7-a_2a_5+a_3a_0+a_4a_6+a_5a_2-a_6a_4+a_7a_1 \bmod r,$$

$$a_0a_4+a_1a_2-a_2a_1-a_3a_6+a_4a_0+a_5a_7+a_6a_3-a_7a_5 \bmod r,$$

$$a_0a_5-a_1a_6+a_2a_3-a_3a_2-a_4a_7+a_5a_0+a_6a_1+a_7a_4 \bmod r,$$

$$a_0a_6+a_1a_5-a_2a_7+a_3a_4-a_4a_3-a_5a_1+a_6a_0+a_7a_2 \bmod r,$$

$$a_0a_7+a_1a_3+a_2a_6-a_3a_1+a_4a_5-a_5a_4-a_6a_2+a_7a_0 \bmod r)$$

$$=(2a_0^2-L_A \bmod r,\ 2a_0a_1 \bmod r,\ 2a_0a_2 \bmod r,\ 2a_0a_3 \bmod r,$$

$$2a_0a_4 \bmod r,\ 2a_0a_5 \bmod r,\ 2a_0a_6 \bmod r,\ 2a_0a_7 \bmod r)$$

where

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

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

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

$$A^2= (2a_0^2-L_A \bmod r,\ 2a_0a_1 \bmod r,\ 2a_0a_2 \bmod r,\ 2a_0a_3 \bmod r,$$

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

Then we have

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

$$w=-L_A \bmod r,$$

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

14) **Theorem 4**

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

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

(*Proof*:)

From **Theorem 3**

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

If we can express A^t such that

$$A^t = w_t\mathbf{1} + v_t A \bmod r \in O\ ,\ w_t,\ v_t \in R,$$

Then

$$A^{t+1} = (w_t\mathbf{1} + v_t A)A \bmod r$$

$$= w_t A + v_t(-L_A\ \mathbf{1} + 2\,a_0 A\ ) \bmod r$$

$$= -\ L_A\ v_t\mathbf{1} + (\ w_t + 2a_0 v_t)A \bmod r.$$

We have

$$w_{t+1} = -\ L_A\ v_t \bmod r \in R,$$

$$v_{t+1} = w_t + 2a_0 v_t\ \ \bmod r \in R. \quad \text{q.e.d.}$$

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

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

§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 plaintext $m \in R(=Z/rZ)$ of the encryption schemes will be the element in finite ring, and the functions to be evaluated will be represented as arithmetic circuits over this ring, composed of addition and multiplication gates. The syntax of these algorithms is given as follows.

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

-Encryption. The algorithm **Enc**, on input system parameters $(r,G,H;F(X))$, public-key **pk**, and a plaintext $m \in R$, 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**; m) where $F(X) \in O[X]$.

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

-Homomorphic-Evaluation. The algorithm **Eval**, on input system parameters $(r,G,H;F(X))$, 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; $C_1,\ldots, C_n$).

§4.2 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,r), $\forall$ckt $\in CR_\lambda$, $\forall (m_1,\ldots, m_n) \in R^n$ where $n = n(\lambda)$, $\forall (C_1,\ldots,C_n)$ where C_i← **Enc**(**pk**;m_i), it holds that:

$$\Pr[\mathbf{Dec}(\mathbf{sk};\mathbf{Eval}(\text{ckt}; C_1,\ldots,C_n)) \neq \text{ckt}(m_1,\ldots, m_n)] = \text{negl}(\lambda).$$

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

§4.3 Basic function

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

Let r be a composite number modulus selected by system centre where $r=pq$, p and q are secret large primes.

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

Let $F(X)$ be a basic function.

S_i , $T_i \in O$ are selected randomly by system centre. such that S_i^{-1} mod r and T_i^{-1} mod r exist (i=1,...,k).

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

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

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

§4.4 Square root on composite number modulus

We discuss the calculation for the square root on composite modulus r.

Let $x\in R$ be the square root of $a\in R$. That is, $x^2=a \bmod r$.

Here we consider to find the square root of a. We obtain next Theorem 5.

Theorem 5

If there exists the PPT algorithm **AL1** for obtaining the square root of a on composite modulus r, there exists the PPT algorithm that factorizes modulus r where a is a quadratic residue on modulus r.

(*Proof*:)

Let $e\in R$ be any element in R.

We can express e and $e^2 \bmod r$ such that

$$e=e_qkp+e_phq \bmod r,\ e_q\in R_q,\ e_p\in R_p,$$

$$e^2=(e_qkp+e_phq)^2 \bmod r,$$

$$=e_q^2kp+e_p^2hq \bmod r,$$

By using the PPT algorithm **AL1** we can obtain e' which is one of e_i (i=0,1,2,3), the square root of e^2 on composite modulus r such that

$$e_0=e_qkp+e_phq \bmod r,$$

$$e_1=e_qkp-e_phq \bmod r,$$

$$e_2=-e_qkp+e_phq \bmod r,$$

$$e_3=-e_qkp-e_phq \bmod r.$$

As

$$\mathrm{GCD}(e+e_1,r)=\mathrm{GCD}(2\, e_qkp,\, pq)=p,$$

$$\mathrm{GCD}(e+e_2,r)=\mathrm{GCD}(2\, e_phq,\, pq)=q,$$

the composite number r is factorized with 1/2 of probability. q.e.d.

§5. Fully homomorphic public-key encryption scheme
§5.1 Public-key enciphering function

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

$$F(X)=(S_k((\ldots((S_1 X)T_1))\ldots))T_k \bmod r \in O[X],$$

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

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

$$F^{-1}(X):=S_1^{-1}((\ldots((S_k^{-1}(XT_k^{-1}))\ldots))\,T_1^{-1}) \bmod r \in O[X],$$

$$=(g'_{00}x_0+\ldots+g'_{07}x_7,$$

$$g'_{10}x_0+\ldots+g'_{17}x_7,$$

$$\ldots \quad \ldots$$

$$g'_{70}x_0+\ldots+g'_{77}x_7) \bmod r,$$

$$=\{g'_{ij}\}(i,j=0,\ldots,7)$$

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

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

We can calculate $F^{-1}(X) \in O[X]$ which is the inverse function of $F(X)$, given $F(X) \in O[X]$.

[**ALINVF**]

Given $F(X)$ and r,

$$F(F^{-1}(X))=F^{-1}(F(X))=X \bmod r \in O[X]$$

$$=(f_{00}(g'_{00}x_0+\ldots+g'_{07}x_7)+\ldots+f_{07}(g'_{70}x_0+\ldots+g'_{77}x_7),$$

$$f_{10}(g'_{00}x_0+\ldots+g'_{07}x_7)+\ldots+f_{17}(g'_{70}x_0+\ldots+g'_{77}x_7),$$

$$\ldots \quad \ldots$$

$$f_{70}(g'_{00}x_0+\ldots+g'_{07}x_7)+\ldots+f_{77}(g'_{70}x_0+\ldots+g'_{77}x_7)) \bmod r,$$

$$=((f_{00}g'_{00}+\ldots+f_{07}g'_{70})x_0+\ldots+(f_{00}g'_{07}x_0+\ldots+f_{07}g'_{77})x_7,$$

$$(f_{10}g'_{00}+\ldots+f_{17}g'_{70})x_0+\ldots+(f_{10}g'_{07}x_0+\ldots+f_{17}g'_{77})x_7,$$

$$\ldots \quad \ldots$$

$$(f_{70}g'_{00}+\ldots+f_{77}g'_{70})x_0+\ldots+(f_{70}g'_{07}x_0+\ldots+f_{77}g'_{77})x_7) \bmod r,$$

$$=X=(x_0,\ldots,x_7).$$

Then we obtain

$$\begin{cases} f_{00}g'_{00}+\ldots+f_{07}g'_{70}=1 \bmod r \\ f_{10}g'_{00}+\ldots+f_{17}g'_{70}=0 \bmod r \\ \ldots\ldots \quad \ldots\ldots \\ f_{70}g'_{00}+\ldots+f_{77}g'_{70}=0 \bmod r \end{cases}$$

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

$$\begin{cases} f_{00}g'_{01}+\ldots+f_{07}g'_{71}=0 \bmod r \\ f_{10}g'_{01}+\ldots+f_{17}g'_{71}=1 \bmod r \\ \ldots\ldots \quad \ldots\ldots \\ f_{70}g'_{01}+\ldots+f_{77}g'_{71}=0 \bmod r \end{cases}$$

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

....

....

$$\begin{cases} f_{00}g'_{07}+\ldots+f_{07}g'_{77}=0 \bmod r \\ f_{10}g'_{07}+\ldots+f_{17}g'_{77}=0 \bmod r \\ \ldots\ldots \quad \ldots\ldots \\ f_{70}g'_{07}+\ldots+f_{77}g'_{77}=1 \bmod r \end{cases}$$

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

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

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

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

....

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

$$F^{-2}(X):=F^{-1}(F^{-1}(X)) \bmod r,$$

....

$$F^{-i}(X):=F^{-1}(F^{-(i-1)}(X)) \bmod r.$$

The system centre publishes the system parameters $(r,G,H;F(X))$.(G and H are defined later)

We consider the communication between user A and user B. User A downloads the system parameters $(r,G,H;F(X))$ from system centre. User A selects the random integer $a \in Z$ to be secret and generates the public function $F^a(X)$ by using algorithm **Power**$(F(X),a,r)$. (see the **Appendix F**)

User A sends the coefficient of $F^a(X)$, $f_{aij} \in R$ $(i,j=0,\ldots,7)$ to system centre that is a part of the public-key of user A.

On the other hand user B downloads the system parameters $(r,G,H;F(X))$ and selects the random integer $b \in Z$ to be secret and generates the public function $F^b(X)$ by using algorithm **Power**$(F(X),b,r)$. User B sends the coefficient of $F^b(X)$, $f_{bij} \in R$ $(i,j=0,\ldots,7)$ 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, $F^a(X)$,that is, $f_{aij} \in R$ $(i,j=0,\ldots,7)$ from system centre.

User B calculates $F^{-a}(X)$ from $F^{a}(X)$ by using **ALINVF**.

User B generates the common enciphering function $F_{\mathrm{BA}}(X,Y)$ between user A and user B as follows. By using algorithm **Power**$(F^{a}(X),b,r)$ user B obtain $F^{ab}(X)$.

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

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

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

In the same manner user A generates the common enciphering function

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

where

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

We notice that

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

User B confirms the system parameters $(r,G,H;F(X))$ downloaded from the system centre where

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

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

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

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

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

$$h_0=0 \bmod r,$$

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

From Theorem 3 we have

$$G^2=-L_G\mathbf{1}+2\,g_0G=2g_0G \bmod r,$$

$$H^2=-L_H\mathbf{1}+2\,h_0H=\mathbf{0} \bmod r,$$

$$[GH]_0=[HG]_0= g_0h_0\text{-}(\,g_1h_1+\ldots+g_7h_7)=0 \bmod r, \qquad (22)$$

$$L_{GH}= L_GL_H= L_{HG}=0 \bmod r,$$

$$(GH)^2=-L_{GH}\mathbf{1}+2\,[GH]_0GH=0\mathbf{1}+0GH=\mathbf{0} \bmod r,$$

$$(HG)^2=-L_{HG}\mathbf{1}+2\,[HG]_0HG=\mathbf{0} \bmod r.$$

Theorem 6

$$(GH)G= \mathbf{0} \bmod r, \qquad (23a)$$

$$(HG)H= \mathbf{0} \bmod r. \qquad (23b)$$

(*Proof*:)

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

Theorem 7

$$GH+HG= 2g_0H \bmod r. \qquad (24)$$

(*Proof*:)

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

Theorem 8

$$(GH)(HG) = \mathbf{0} \bmod r, \tag{25a}$$

$$(HG)(GH) = \mathbf{0} \bmod r. \tag{25b}$$

(*Proof*:)

From (17)

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

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

§5.2 Medium text

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

Let $m \in R$ be a plaintext.

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

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

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

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

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

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

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

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

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

$m := su + tv \bmod r \in R$

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

where α and β satisfy the following equation,

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

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

$=su+tv=m \bmod r,$

where

$$GCD\,({}^1k{}^2l - {}^2k{}^1l\,, r)=1 \bmod r. \quad (26a)$$

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

$$(\alpha\, {}^1k+\beta\, {}^2k)=s \bmod r, \quad (26b)$$

$$(\alpha\, {}^1lg_0+\beta\, {}^2lg_0)=t \bmod r. \quad (26c)$$

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

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

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

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

we have

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

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

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

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

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

On the other hand from Theorem 3

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

From $[{}^1M]_0=({}^1ku+g_0\,({}^1lv)) \bmod r$

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

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

$$L_{1M}=|{}^1M|^2=|\,{}^1ku\ \mathbf{1}+{}^1lvG+{}^1wGH+{}^1zHG|^2=({}^1ku+2\,g_0\,({}^1lv)\,)({}^1ku\,) \bmod r. \quad (27a)$$

In the same manner we have

$$L_{2M}=|{}^2M|^2=|{}^2ku\ \mathbf{1}+{}^2lvG+{}^2wGH+{}^2zHG\,|^2=({}^2ku+2\,g_0\,({}^2lv)\,)({}^2ku\,) \bmod r. \quad (27b)$$

$$L_{3M}=|{}^3M|^2=|{}^3ku\ \mathbf{1}+{}^3lvG+{}^3wGH+{}^3zHG\,|^2=({}^3ku+2\,g_0\,({}^3lv)\,)({}^3ku\,) \bmod r. \quad (27c)$$

Theorem 9 (linear independence)

If

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

then

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

(*Proof*)

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

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

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

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

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

We have

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

By multiply G from right side from Theorem 6

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

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

We have

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

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

In the same manner

If

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

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

then

$$u = v = {}^{i}w = {}^{i}z = 0 \bmod r \ (i=2,3).$$

(Associativity of medium texts)

Let

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

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

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

Then we have

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$+[({}^1k)^2({}^1l)(u_1u_2v_3+u_1v_2u_3+v_1u_2u_3)+2g_0({}^1k)({}^1l)^2(v_1v_2u_3+u_1v_2v_3+v_1u_2v_3)+(2g_0)^2({}^1l)^3v_1v_2v_3]G$

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

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

Then we have

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

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

In the same manner we have

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

(Homomorphism on medium text)

We can obtain the plaintext m_1+m_2 and m_1m_2 from ${}^1M_1$, ${}^1M_2$, ${}^2M_1$, ${}^2M_2$, ${}^3M_1$, ${}^3M_2$ as follows.

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

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

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

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

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

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

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

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

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

$m_1 := su_1 + tv_1 \bmod r$

$m_2 := su_2 + tv_2 \bmod r$

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

$= \alpha({}^1ku_1 + {}^1lv_1 2g_0 + {}^1ku_2 + {}^1lv_2 2g_0) + \beta({}^2ku_1 + {}^2lv_1 2g_0 + {}^2ku_2 + {}^2lv_2 2g_0)$

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

From (26b) , (26c) we have

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

$= su_1 + tv_1 + su_2 + tv_2$

$= m_1 + m_2 \bmod r.$ (28)

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

Next we try to calculate the multiplication of medium texts.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$u_{12}:= su_1u_2 \bmod r\in R$ (29a)

$v_{12}:= s(u_1v_2 + u_2v_1)+ tv_1v_2 \bmod r\in R$ (29b)

$m_{12}:= su_{12}+tv_{12} \bmod r\in R$. (29c)

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

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

$={}^1ku_{12}\,\mathbf{1}+{}^1lv_{12}G+{}^1w_{12}GH+{}^1z_{12}HG \bmod r$

$= {}^1k\,su_1u_2\mathbf{1}+{}^1l\,s(u_1v_2 + u_2v_1)G+{}^1l\,tv_1v_2G+{}^1w_{12}GH+{}^1z_{12}HG \bmod r$ (30a)

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

$={}^2ku_{12}\,\mathbf{1}+{}^2lv_{12}G+{}^2w_{12}GH+{}^2z_{12}HG \bmod r$

$={}^2k\,su_1u_2\mathbf{1}+{}^2l\,s(u_1v_2 + u_2v_1)G+{}^2l\,tv_1v_2G+{}^2w_{12}GH+{}^2z_{12}HG \bmod r$ (30b)

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

$={}^3ku_{12}\,\mathbf{1}+{}^3lv_{12}G+{}^3w_{12}GH+{}^3z_{12}HG \bmod r$.

$= {}^3k\,su_1u_2\mathbf{1}+{}^3l\,s(u_1v_2 + u_2v_1)G+{}^3l\,tv_1v_2G+{}^3w_{12}GH+{}^3z_{12}HG \bmod r$. (30c)

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

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

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

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

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

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

$\mathrm{GCD}(\Delta, r) = 1.$

Here we show that $m_{12}=\alpha[{}^1M_{12}]_0 + \beta[{}^2M_{12}]_0 \bmod r = m_1m_2 \bmod r$.

From (29c), (29a) and (29b) we have

$m_{12} = su_{12}+tv_{12} \bmod r$

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

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

$= m_1m_2 \bmod r.$

On the other hand we have from (29c), (29a) , (29b) ,(26b) and (26c)

$m_{12} = su_{12}+tv_{12} \bmod r$

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

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

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

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

We have shown that we can obtain the plaintext m_1+m_2 from ${}^1M_{1+2}$, ${}^2M_{1+2}$, the plaintext m_1m_2 from ${}^1M_{12}$,${}^2M_{12}$. □

§5.3 Enciphering

Let $(r,G,H;F(X))$ be the system parameters where $r=pq$, p and q are secret primes.

Let $[F^b(X),(d_{bij}),\alpha_b,\beta_b]$(i,j=1,2,3) be user B's public keys and $[b,({}^ik_b),({}^il_b),({}^iw_b, {}^iz_b),s_b,t_b]$ (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 $m\in R$, the components $u,v\in R$ of the plaintext m , 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

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

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

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

$$m:= s_bu+t_bv \bmod r\in R$$

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

where

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

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

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).

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

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

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

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

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

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

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

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

§5.4 Deciphering

User A deciphers $C(m, X)=(F_{BA}(X,{}^{1}M), F_{BA}(X,{}^{2}M), F_{BA}(X,{}^{3}M))$ to obtain m from $\{{}^{k}c_{ij}\}$ (i, j=0,…,7;k=1,2,3) sent by user B as follows.

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

$F^{ba}(F_{BA}(F^{-ba}(\mathbf{1}),{}^{e}M))$

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

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

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

$= s_bu+t_bv \bmod r\in R$,

where

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

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

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

Theorem 10

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

if $C(m, X)= C(m', X) \bmod r$, then $m= m' \bmod r$.

That is , if $m \neq m' \bmod r$, then $C(m, X)\neq C(m', X) \bmod r$

where

$C(m, X)=(F_{AB}(X,{}^{1}M), F_{AB}(X,{}^{2}M))$

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

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

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

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

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

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

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

$m := su + tv \bmod r$,

$m' := su' + tv' \bmod r$.

(*Proof*)

If $C(m, X) = C(m', X) \bmod r$, then

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

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

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

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

$F^{ab}(F^{-ab}({}^1M)) = F^{ab}(F^{-ab}({}^1M')) \bmod r$,

$^1M = {}^1M' \bmod r$

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

Then we have

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

From Theorem 9 we have

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

$u = u' \bmod r$,

$v = v' \bmod r$,

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

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

We have

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

§5.5 Addition scheme on ciphertexts

Let

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

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

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

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

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

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

be medium texts to be encrypted where

$$m_1 := su_1 + tv_1 \bmod r = \alpha[{}^{1}M_1]_0 + \beta[{}^{2}M_1]_0 \bmod r,$$

$$m_2 := su_2 + tv_2 \bmod r = \alpha[{}^{1}M_2]_0 + \beta[{}^{2}M_2]_0 \bmod r.$$

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

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

Let

$$C(m_1,X) := (F_{AB}(X,{}^{1}M_1), F_{AB}(X,{}^{2}M_1), F_{AB}(X,{}^{3}M_1))$$

$$C(m_2,X) := (F_{AB}(X,{}^{1}M_2), F_{AB}(X,{}^{2}M_2), F_{AB}(X,{}^{3}M_2))$$

be the ciphertexts. We define the additional operation between $C(m_1,X) \bmod r$ and $C(m_2,X) \bmod r$ such that

$$C(m_1,X) + C(m_2,X) \bmod r :=$$

$$(F_{AB}(X,{}^{1}M_1) + F_{AB}(X,{}^{1}M_2) \bmod r,\ F_{AB}(X,{}^{2}M_1) + F_{AB}(X,{}^{2}M_2) \bmod r,\ F_{AB}(X,{}^{3}M_1) + F_{AB}(X,{}^{3}M_2) \bmod r)$$

$$= (F_{AB}(X,{}^{1}M_1 + {}^{1}M_2) \bmod r,\ F_{AB}(X,{}^{2}M_1 + {}^{2}M_2) \bmod r,\ F_{AB}(X,{}^{3}M_1 + {}^{3}M_2) \bmod r)$$

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

Then we have

$$C(m_1,X) + C(m_2,X) \bmod r$$

$$= C(m_{1+2},X) \bmod r,$$

$= C(m_1+m_2, X) \bmod r$.(From (28))

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

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

§5.6 Multiplication scheme on ciphertexts

Here we consider the multiplicative operation on the ciphertexts.

Let

$C(m_1,X) := (F_{AB}(X,{}^1M_1), F_{AB}(X,{}^2M_1), F_{AB}(X,{}^3M_1))$

$C(m_2,X) := (F_{AB}(X,{}^1M_2), F_{AB}(X,{}^2M_2), F_{AB}(X,{}^3M_2))$

be the ciphertexts where

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

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

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

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

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

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

$m_1 := su_1 + tv_1 \bmod r = \alpha[{}^1M_1]_0 + \beta[{}^2M_1]_0 \bmod r$,

$m_2 := su_2 + tv_2 \bmod r = \alpha[{}^1M_2]_0 + \beta[{}^2M_2]_0 \bmod r$

where

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

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

We can calculate the ciphertext $C(m_1m_2, X)$ of the plaintext m_1m_2 by using

$$C(m_1,X) = (F_{AB}(X,{}^1M_1), F_{AB}(X,{}^2M_1), F_{AB}(X,{}^3M_1))$$

and

$$C(m_2,X) = (F_{AB}(X,{}^1M_2), F_{AB}(X,{}^2M_2), F_{AB}(X,{}^3M_2))$$

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

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

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

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

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

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

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

where

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

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

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

Here we show that $(F_{AB}(X, {}^1M_{12}), F_{AB}(X, {}^2M_{12}), F_{AB}(X, {}^3M_{12}))$ is the ciphertext of the plaintext m_1m_2.

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

$F^{ba}(F_{AB}(F^{-ba}(\mathbf{1}), {}^eM_{12}))$

$= F^{ba}(F^{-ab}({}^eM_{12}F^{ab}(F^{-ba}(\mathbf{1})))) \bmod r$

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

From (30a) and (30b)

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

$= \alpha[{}^1k\, su_1u_2 + {}^1l\, s(u_1v_2 + u_2v_1)g_0 + {}^1l\, tv_1v_2\, g_0] + \beta[{}^2k\, su_1u_2 + {}^2l\, s(u_1v_2 + u_2v_1)g_0 + {}^2l\, tv_1v_2g_0] \bmod r$

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

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

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

$= m_1m_2 \bmod r$.

We have shown that we can obtain the plaintext m_1m_2 from $C(m_1,X), C(m_2,X)$.□

We can define that

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

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

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

§5.7 Discrete logarithm assumption DLA(F,F^a; r)

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

Let r be a composite number. Let a, b and k be integer parameters. Let $\boldsymbol{S}:=(S_1,\ldots,S_k)\in O^k$, $\boldsymbol{T}:=(T_1,\ldots,T_k)\in O^k$ such that $S_1^{-1},\ldots, S_k^{-1}$ and $T_1^{-1},\ldots, T_k^{-1}$ exist.

Let $F(X)=(S_k((\ldots((S_1XT_1))\ldots))T_k \bmod r\in O[X]$ be a basic function.

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

X is a variable.

In the **DLA(F,F^a; r)** assumption, the adversary A_d is given $F^a(X)=\{ f_{aij} \}$ $(i,j=0,\ldots,7)$, system parameters $(r,G,H;F(X))$ where $F(X)= \{f_{ij}\}(i,j=0,\ldots,7)$ and his goal is to find the integer a. For parameters $k = k(\lambda)$, $a= a(\lambda)$ defined in terms of the security parameter λ and for any PPT adversary A_d we have

$$\Pr\,[F(X)= \{ f_{ij} \}, F^a(X)=\{ f_{aij} \}: a \leftarrow A_d\,(1^\lambda, \{ f_{ij} \}, \{ f_{aij} \})]= \mathrm{negl}(\lambda).$$

To solve directly **DLA(F,F^a;r)** assumption is known to be the discrete logarithm problem on the multivariate polynomials.

§5.8 Computational Diffie–Hellman assumption CDH(F,F^a, F^b; r)

Let r be a composite number. Let a , b and k be integer parameters. Let $\boldsymbol{S}:=(S_1,\ldots,S_k)\in O^k$, $\boldsymbol{T}:=(T_1,\ldots,T_k)\in O^k$ such that $S_1^{-1},\ldots, S_k^{-1}$ and $T_1^{-1},\ldots, T_k^{-1}$ exist.

Let $F(X)=(S_k((\ldots((S_1XT_1))\ldots))T_k \bmod r\in O[X]$ be a basic function.

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

Let $F^b(X) \bmod r\in O[X]$ be the public function of user B.

X is a variable.

In the **CDH(F,F^a,F^b;r)** assumption, the adversary A_d is given $F^a(X)=\{f_{aij}\}$, $F^b(X) =\{ f_{bij} \}(i,j=0,\ldots,7)$, system parameters $(r,G,H;F(X))$ and his goal is to find $F_{UV}(X, Y)= F^{-ab}(YF^{ab}(X)) \bmod r$. For parameters $k = k(\lambda)$, $a= a(\lambda)$,and $b= b(\lambda)$ defined in terms of the security parameter λ and for any PPT adversary A_d we have

$\Pr[F(X)=\{f_{ij}\},F^a(X)=\{f_{aij}\},F^b(X)=\{f_{bij}\}:F_{UV}(X,Y)=F^{-ab}(YF^{ab}(X))\leftarrow A_d(1^\lambda,\{f_{ij}\},\{f_{aij}\},\{f_{bij}\})]=\mathrm{negl}(\lambda)$.

To solve directly **CDH(*F*,*F***$\mathbf{F^a}$**,**$\mathbf{F^b}$**;*r*)** assumption is known to be the computational Diffie–Hellman assumption on the multivariate polynomials.

§5.9 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 $[r,G,H;F(X)]$

where

$r=pq=1927$, $p=41$, $q=47$, p and q are secret parameters.

$G=(35,33,39,3,3,1,0,0)$, $H=(0,62,43,24,1,56,15,2)$.

We notice that $|G|^2=0 \bmod r$, $|H|^2=0 \bmod r$,

$GH=(0,174,1802,605,920,339,237,1428)$,

$HG=(0,312,1208,1075,1077,1654,813,639)$,

Example of $F(X)=\{f_{ij}\}$ is omitted here.

2) User A selects secret key $a\in R$ and calculates $F^a(X)$ to be user A's public-key.
User A sends public-key $F^a(X)$ with (d_{aij}), α_a and β_a to system centre.

3) User B selects secret key $b\in R$ and calculates $F^b(X)$ to be a part of user B's public-key.

User B sends $F^b(X)$ with (d_{bij}), α_b and β_b to system centre.

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

where

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

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

$(d_{bij})=(1865,482,1705\ ;\ 1111,733,1747\ ;\ 253,1802,1462)$.

4) User B downloads user A's public-key $F^a(X)$ from system centre and generates common enciphering function $F_{AB}(X,Y)=F^{-ab}(YF^{ab}(X)) \bmod r$.

5) User B selects $[({}^{i}k_b),({}^{i}l_b),({}^{i}w_b, {}^{i}z_b), s_b,t_b]$ to be secret
where
$({}^{i}k_b)=(7,9,13)$, $({}^{i}l_b)=(11,17,19)$,
$({}^{1}w_{b1},{}^{1}z_{b1})=(2,3)$, $({}^{2}w_{b1},{}^{2}z_{b1})=(3,11)$, $({}^{3}w_{b1},{}^{3}z_{b1})=(7,13)$,
$({}^{1}w_{b2},{}^{1}z_{b2})=(2,1)$, $({}^{2}w_{b2},{}^{2}z_{b2})=(1,2)$, $({}^{3}w_{b2},{}^{3}z_{b2})=(3,1)$,
$s_b=59$, $t_b=1818$,

6) User B selects the plaintexts $(m_1, m_2)=(313,1915)$ which he has.

7) User B calculates $(u_1,v_1)=(111,234)$, $(u_2,v_2)=(12,95)$ which satisfy the following equations,
$m_1= s_bu_1+t_bv_1 \bmod r=59*111+1818*234 =313 \bmod r$,
$m_2= s_bu_2+t_bv_2 \bmod r=59*12+1818*95 =1915 \bmod r$.

8) By using the plaintexts $(m_1, m_2)=(313,1915)$ 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
${}^{1}M_1={}^{1}k_bu_1\mathbf{1}+{}^{1}l_bv_1G+{}^{1}w_{b1}GH+{}^{1}z_{b1}HG \bmod r=(298,1438,1629,595,1231,506,986,919)$,
${}^{2}M_1={}^{2}k_bu_1\mathbf{1}+{}^{2}l_bv_1G+{}^{2}w_{b1}GH+{}^{2}z_{b1}HG \bmod r=(1485,1161,1304,617,234,1107,1192,282)$,
${}^{3}M_1={}^{3}k_bu_1\mathbf{1}+{}^{3}l_bv_1G+{}^{3}w_{b1}GH+{}^{3}z_{b1}HG \bmod r=(966,1686,1304,716,1020,1343,666,960)$,
${}^{1}M_2={}^{1}k_bu_2\mathbf{1}+{}^{1}l_bv_2G+{}^{1}w_{b2}GH+{}^{1}z_{b2}HG \bmod r=(46,459,1246,1566,271,1450,1287,1568)$,
${}^{2}M_2={}^{2}k_bu_2\mathbf{1}+{}^{2}l_bv_2G+{}^{2}w_{b2}GH+{}^{2}z_{b2}HG \bmod r=(750,137,1685,1819,211,1408,1863,779)$,
${}^{3}M_2={}^{3}k_bu_2\mathbf{1}+{}^{3}l_bv_2G+{}^{3}w_{b2}GH+{}^{3}z_{b2}HG \bmod r=(1667,662,1856,597,1544,622,1524,1069)$.

9) 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 cipher texts $C(m_1,X)=(F_{AB}(X,{}^{1}M_1), F_{AB}(X,{}^{2}M_1), F_{AB}(X,{}^{3}M_1))$, $C(m_2,X)=(F_{AB}(X,{}^{1}M_2), F_{AB}(X,{}^{2}M_2), F_{AB}(X,{}^{3}M_2))$.

10) User B sends $C(m_1, X)$, $C(m_2, X)$ to user A.

11) User A receives $C(m_1, X)$, $C(m_2, X)$ from user B.

12) User A downloads user B's public-key $[F^{b}(X), (d_{bij}), \alpha_b, \beta_b]$ from system centre and generates common enciphering function $F_{AB}(X,Y)=F^{-ab}(YF^{ab}(X)) \bmod r$.

13) User A deciphers $C(m_i, X):=(F_{AB}(X,{}^{1}M_i), F_{AB}(X,{}^{2}M_i), F_{AB}(X,{}^{3}M_i))$ (i=1,2) to obtain m_1,m_2 as follows.

$$F^{ba}(F_{AB}(F^{-ba}(\mathbf{1}),{}^{e}M_i))$$
$$= F^{ba}(F^{-ab}({}^{e}M_i F^{ab}(F^{-ba}(\mathbf{1})))) \bmod r$$
$$={}^{e}M_i,$$
$$m_i=\alpha_b[{}^{1}M_i]_0 +\beta_b[{}^{2}M_i]_0 \bmod r \text{ (i=1,2)}.$$

[Data processing]

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

He generates another encryption function $F_{B*}(X,Y)=F^{-yb}(YF^{yb}(X)) \bmod r$.

He calculates $C^*(m_1,X)$, $C^*(m_2,X)$ such that

$C^*(m_1,X):=(F_{B*}(X,{}^1M_1), F_{B*}(X,{}^2M_1), F_{B*}(X,{}^3M_1)), C^*(m_2,X):=(F_{B*}(X,{}^1M_2), F_{B*}(X,{}^2M_2), F_{B*}(X,{}^3M_2))$.

15) User B sends his ciphered data $C^*(m_1, X)$, $C^*(m_2,X)$ with the method for processing to data processing centre D. He requires to have $C^*(m_1+m_2, X)$, $C^*(m_1m_2,X)$.

16) Data processing centre D receives user B's ciphered data $C^*(m_1, X)$, $C^*(m_2, X)$ with the method for processing.

17) Data processing centre D downloads user B's public-key $[F^b(X), (d_{bij}), \alpha_b, \beta_b]$. He uses only (d_{bij}). Data processing centre D calculates $C^*(m_1+m_2, X)$, $C^*(m_1m_2,X)$ without knowing ${}^1M_1,{}^1M_2,{}^2M_1,{}^2M_2,{}^3M_1,{}^3M_2$ and so on as follows.

$C^*(m_1+m_2,X):=(F_{B*}(X,{}^1M_1)+F_{B*}(X,{}^1M_2),F_{B*}(X,{}^2M_1)+F_{B*}(X,{}^2M_2),F_{B*}(X,{}^3M_1)+FB_{B*}(X,{}^3M_2))$,

$=(F_{B*}(X,{}^1M_1+{}^1M_2),F_{B*}(X,{}^2M_1+{}^2M_2),F_{B*}(X,{}^3M_1+M_2))$,

$= (F_{B*}(X,(344,1897,948,234,1502,29,346,560))$,

$F_{B*}(X,(308,1298,1062,509,445,588,1128,1061))$,

$F_{B*}(X,(706,421,1233,1313,637,38,263,102)))$,

$K_1(X):= F_{B*}((F_{B*}(X, Y)=(X, {}^1M_2)), {}^1M_1)= F_{B*}(X,{}^1M_1{}^1M_2) \bmod r$

$= F_{B*}(X,(1078,1474,1153,162,391,850,157,1640))$

$K_2(X):= F_{B*}((F_{B*}(X,Y)=(X,{}^2M_2)),{}^2M_1)= F_{B*}(X,{}^2M_1{}^2M_2) \bmod r$

$= F_{B*}(X,(1709,233,1247,992,604,1703,634,562))$

$K_3(X):= F_{B*}((F_{UB}(X,Y)=(X,{}^3M_2)),{}^3M_1)= F_{B*}(X,{}^3M_1{}^3M_2) \bmod r$

$= F_{B*}(X,(1228,1401,474,1590,988,1391,1693,1377))$

${}^1K_{12}(X):= d_{11}K_1(X)+d_{12} K_2(X)+d_{13} K_3(X)$

$= F_{B*}(X, d_{11}{}^1M_1{}^1M_2+ d_{12}{}^2M_1{}^2M_2+ d_{13}{}^3M_1{}^3M_2) \bmod r$

$= F_{B*}(X,(609,873,400,1427,1302,718,942,327))$

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

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

$= F_{B*}(X,(1703,1134,1576,424,1719,1780,1038,1316))$

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

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

$= F_{B*}(X,(671,652,212,465,1432,905,1836,1123))$

$C^*(m_1m_2, X):= ({}^1K_{12}(X), {}^2K_{12}(X), {}^3K_{12}(X))$.

18) Data processing centre D sends $C^*(m_1+m_2, X)$, $C^*(m_1m_2, X)$ to user B.

19) User B receives $C^*(m_1+m_2, X)$, $C^*(m_1m_2, X)$ from Data processing centre D.

20) User B deciphers $C^*(m_1+m_2, X)$ to obtain m_1+m_2 as follows.

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

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

$= F^{yb}(F^{-yb}({}^{e}M_1F^{yb}(F^{-yb}(\mathbf{1}))))+F^{yb}(F^{-yb}({}^{e}M_2F^{yb}(F^{-yb}(\mathbf{1})))) \bmod r$

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

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

$=2[344]+5[308] \bmod r,$

$=301$

[verification]

$m_1+m_2=313+1915=301=m_{1+2} \bmod r,$

21) User B deciphers $C^*(m_1m_2, X)$ to obtain m_1m_2 as follows.

$F^{yb}({}^{e}K_{12}(F^{-yb}(\mathbf{1})))$

$= F^{yb}(F^{-yb}((d_{e1}{}^{1}M_1{}^{1}M_2+d_{e2}{}^{2}M_1{}^{2}M_2+d_{e3}{}^{3}M_1{}^{3}M_2)F^{yb}(F^{-yb}(\mathbf{1})))) \bmod r$

$= d_{e1}{}^{1}M_1{}^{1}M_2+d_{e2}{}^{2}M_1{}^{2}M_2+d_{e3}{}^{3}M_1{}^{3}M_2,\ (e=1,2,3)$

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

$=2[609]+5[1703] \bmod r,$

$=98$

[verification]

$m_1m_2=313*1915=98 \bmod r=m_{12},$

§6. Analysis of proposed scheme

Here we analyze the proposed fully homomorphic public-key encryption scheme described in section 5.

§6.1 Computing plaintext *m* from coefficients of ciphertext $F_{AB}(X,M)$

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

$$F_{AB}(X,{}^{k}M_n)=F^{-ba}({}^{k}M_nF^{ba}(X)) \bmod r\in O[X]$$

$$=({}^{k}c_{n00}x_0+{}^{k}c_{n01}x_1+\ldots+{}^{k}c_{n07}x_7,$$

$${}^{k}c_{n10}x_0+{}^{k}c_{n11}x_1+\ldots+{}^{k}c_{n17}x_7,$$

$$\ldots\qquad\ldots$$

$${}^{k}c_{n70}x_0+{}^{k}c_{n71}x_1+\ldots+{}^{k}c_{n77}x_7) \bmod r,$$

$=\{{}^{k}c_{nij}\}(i,j=0,\ldots,7;n=1,2,\ldots;\ \mathrm{k}=1,2,3)$

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

where

$${}^{1}M_n={}^{1}k\ u_n\mathbf{1}+{}^{1}lv_nG+{}^{1}w_nGH+{}^{1}z_nHG \bmod r\in O,$$

$${}^{2}M_n={}^{2}k\ u_n\mathbf{1}+{}^{2}lv_nG+{}^{2}w_nGH+{}^{2}z_nHG \bmod r\in O,$$

$${}^{3}M_n={}^{3}k\ u_n\mathbf{1}+{}^{3}lv_nG+{}^{3}w_nGH+{}^{3}z_nHG \bmod r\in O,$$

$$u_n,v_n,\ {}^{1}w_n,\ {}^{1}z_n,{}^{2}w_n,\ {}^{2}z_n,{}^{3}w_n,\ {}^{3}z_n\in R\ (n=0,\ldots,7).$$

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

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

$$=(\gamma_{000}x_0y_0+\gamma_{001}x_0y_1+\ldots+\gamma_{077}x_7y_7,$$

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

$$\ldots\qquad\ldots$$

$$\gamma_{700}x_0y_0+\gamma_{701}x_0y_1+\ldots+\gamma_{777}x_7y_7) \bmod r,$$

$$=\{\gamma_{ijh}\}(i,j,h=0,\ldots,7)$$

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 ${}^{k}M_n=({}^{k}m_{n0},\ldots,{}^{k}m_{n7})$ from $\{{}^{k}c_{nij}\}(i,j=0,\ldots,7;n=1,2,3;\mathrm{k}=1,2,3)$ 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 $F_{\mathrm{AB}}(X, {}^{k}M_n)$ where $\gamma_{ijh}(i,j,h=0,\ldots,7)$ and $({}^{k}m_{n0},\ldots,{}^{k}m_{n7})$ are unknown variables.

$$\begin{cases}\gamma_{i00}{}^{k}m_{n0}+\gamma_{i01}{}^{k}m_{n1}+\ldots+\gamma_{i07}{}^{k}m_{n7}={}^{k}c_{ni0} \bmod r\\ \gamma_{i10}{}^{k}m_{n0}+\gamma_{i11}{}^{k}m_{n1}+\ldots+\gamma_{i17}{}^{k}m_{n7}={}^{k}c_{ni1} \bmod r\\ \ldots\\ \ldots\\ \gamma_{i70}{}^{k}m_{n0}+\gamma_{i71}{}^{k}m_{n1}+\ldots+\gamma_{i77}{}^{k}m_{n7}={}^{k}c_{ni7} \bmod r\end{cases}$$

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

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

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

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

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

$$G_{reb}>G_{reb}'=({}_{576+dreg}C_{dreg})^{w}=({}_{847}C_{271})^{w}=2^{1818}>>2^{80},$$

where G_{reb}' is the complexity required for solving 576 simultaneous quadratic algebraic equations with 576 variables by using Gröbner basis,

where w=2.39, and

$$d_{reg} = 271(=576*(2-1)/2 - 1\sqrt{\ }(576*(4-1)/6)\ ).$$

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

§6.2 Attack by using the ciphertext of *m* and -*m*

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

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

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

where

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

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

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

$m:= su+tv \bmod r\in R$

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

where

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

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

Let

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

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

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

$m_- := -m = su_- + tv_- \bmod r \in R,$

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

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

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

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

As $m + m_- = s(u + u_-) + t(v + v_-) = 0 \bmod r$, we have

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

$$^1M + {}^1N$$

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

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

Then we have

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

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

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

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

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

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

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

From (27a)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§6.3 Attack by using ${}^{i}k$, ${}^{i}l$ (i=1,2,3)

We try to obtain the plaintext m directly from the ciphertext $C(m, X) = (F_{AB}(X, {}^{1}M), F_{AB}(X, {}^{2}M), F_{AB}(X, {}^{3}M))$ by using ${}^{i}k$, ${}^{i}l$ (i=1,2,3) where

$F_{AB}(X,Y) = F^{-ba}(YF^{ba}(X)),$

$m=su+tv \bmod r \in R,$

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

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

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

The public parameters (d_{ij}) are given as follows.

$$\begin{cases} d_{11}({}^1k)^2 + d_{12}({}^2k)^2 + d_{13}({}^3k)^2 = {}^1k\, s \bmod r \\ d_{11}{}^1k{}^1l + d_{12}{}^2k{}^2l + d_{13}{}^3k{}^3l = {}^1l\, s \bmod r \\ d_{11}({}^1l)^2 + d_{12}\,({}^2l)^2 + d_{13}({}^3l)^2 = {}^1l\, t/(2g_0) \bmod r \end{cases} \quad (31a)$$

$$\begin{cases} d_{21}({}^1k)^2 + d_{22}({}^2k)^2 + d_{23}({}^3k)^2 = {}^2k\, s \bmod r \\ d_{21}{}^1k{}^1l + d_{22}{}^2k{}^2l + d_{23}{}^3k{}^3l = {}^2l\, s \bmod r \\ d_{21}({}^1l)^2 + d_{22}\,({}^2l)^2 + d_{23}({}^3l)^2 = {}^2l\, t/(2g_0) \bmod r \end{cases} \quad (31b)$$

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

We try to obtain ${}^ik$, ${}^il$ (i=1,2,3) from public parameters (d_{ij}) where s,and t are unknown parameters.

Let

${}^ik={}^ik_pkq+{}^ik_qhp \bmod r$, ${}^il={}^il_pkq+{}^ik_qhp \bmod r$(i=1,2,3),$s=s_pkq+s_qhp \bmod r$, $t=t_pkq+t_qhp \bmod r$,

${}^ik'={}^ik_pkq-{}^ik_qhp \bmod r$, ${}^il'={}^il_pkq-{}^ik_qhp \bmod r$(i=1,2,3),$s'=s_pkq-s_qhp \bmod r$, $t'=t_pkq-t_qhp \bmod r$,

${}^ik''=-{}^ik_pkq+{}^ik_qhp \bmod r$, ${}^il''=-{}^il_pkq+{}^ik_qhp \bmod r$(i=1,2,3),$s''=-s_pkq+s_qhp \bmod r$, $t''=-t_pkq+t_qhp \bmod r$,

${}^ik'''=-{}^ik_pkq-{}^ik_qhp \bmod r$, ${}^il'''=-{}^il_pkq-{}^ik_qhp \bmod r$(i=1,2,3),$s'''=-s_pkq-s_qhp \bmod r$, $t'''=-t_pkq-t_qhp \bmod r$,

where

$kq+hp \bmod r=1, r=pq$,

${}^ik_p := {}^ik \bmod p$, ${}^ik_q := {}^ik \bmod q$, ${}^il_p := {}^il \bmod p$, ${}^il_q := {}^il \bmod q$, (i=1,2,3)

$s_p := s \bmod p$, $s_q := s \bmod q$, $t_p := t \bmod p$, $t_q := t \bmod q$.

Let ALSQE be the PPT algorithm for solving the above simultaneous equations.

If a tuple of (${}^ik$, ${}^il$,s,t) (i=1,2,3) satisfies above equations, (${}^ik'$, ${}^il'$,s',t'), (${}^ik''$, ${}^il''$,s'',t'') and (${}^ik'''$, ${}^il'''$,s''',t''') satisfy above equations because

$({}^ik)^2=({}^ik')^2=({}^ik'')^2=({}^ik''')^2 \bmod r$ (i=1,2,3),

$({}^il)^2=({}^il')^2=({}^il'')^2=({}^il''')^2 \bmod r$ (i=1,2,3),

${}^ik{}^il={}^ik'{}^il'={}^ik''{}^il''={}^ik'''{}^il''' \bmod r$ (i=1,2,3),

${}^{i}ks={}^{i}k's'={}^{i}k''s''={}^{i}k'''s'''$ mod r (i=1,2,3),

${}^{i}ls={}^{i}l's'={}^{i}l''s''={}^{i}l'''s'''$ mod r (i=1,2,3),

${}^{i}lt={}^{i}l't'={}^{i}l''t''={}^{i}l'''t'''$ mod r (i=1,2,3).

If the PPT algorithm exists, by using ALSQE we can solve the following equations.

$$\begin{cases} d_{i1}({}^{1}k)^2 + d_{i2}({}^{2}k)^2 + d_{i3}({}^{3}k)^2 = -{}^{i}k\, s \bmod r \\ d_{i1}{}^{1}k^{1}l + d_{i2}{}^{2}k^{2}l + d_{i3}{}^{3}k^{3}l = -{}^{i}l\, s \bmod r \\ d_{i1}({}^{1}l)^2 + d_{i2}({}^{2}l)^2 + d_{i3}({}^{3}l)^2 = -{}^{i}l\, t/(2g_0) \bmod r \end{cases} \quad (32)$$

(i=1,2,3).

We have (${}^{i}k'$, ${}^{i}l'$,s'',t''), (${}^{i}k''$, ${}^{i}l''$,s',t'), (${}^{i}k$, ${}^{i}l$, s''',t''') or (${}^{i}k'''$, ${}^{i}l'''$,s,t) as the solutions of above simultaneous equation with a quarter probability each.

For example, we can factorize r from (${}^{i}k$, ${}^{i}l$,s,t) and (${}^{i}k'$, ${}^{i}l'$,s'',t'') such that

$GCD({}^{i}k+{}^{i}k', r) = GCD({}^{i}k_p kq+{}^{i}k_q hp+{}^{i}k_p kq-{}^{i}k_q hp, r) = GCD(2\,{}^{i}k_p kq, r)=q$.

To solve the above equation (31a)~(32) is as difficult as factorizing modulus r. It is said that the attack by using ${}^{i}k$, ${}^{i}l$ (i=1,2,3) is not efficient.

§6.4 Attack by using α and β

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

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

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

If $F^{-ba}(X)$ is known, we can obtain the plaintext m directly from the ciphertext $C(m,X)$ as follows.

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

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

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

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

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

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

$m=\alpha[^1M]_0+\beta[^2M]_0 \bmod r$ (= $su+tv \bmod r$).

But the adversary A_d does not know $F^{-ba}(X)$. Though he knows α and β, he cannot obtain the plaintext m directly from the ciphertext $C(m,X)$.

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

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

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

§7. The size of the modulus *r* and the complexity for enciphering/deciphering

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

Theorem 2 shows that the order l of an element $A\in O$ is LCM { p^2-1, q^2-1} in general. The complexity required for obtaining the discrete logarithm of $A^x\in O$ is O($sqrt(l)$) where l is the order of an element $A\in O$[25]. We select the size of r such that O($sqrt(l)$) is larger than 2^{2000}. Then we need to select modulus r such as $O(r)=2^{2000}$.

We calculate the size of the parameter and the complexity required for the opration in k=8 of $F(X)=(S_k((\ldots((S_1X)T_1))\ldots))T_k \bmod r=\{f_{ij}\}$ $(i,j=0,\ldots,7)\in O[X]$.

1) The size of $f_{ij}\in R(i,j=0,\ldots,7)$ which are the coefficients of elements in $F(X) \bmod r\in O[X]$ is (64)($\log_2 r$) bits =128kbits,
2) The size of $f_{aij}\in R(i,j=0,\ldots,7)$ which are the coefficients of elements in $F^a(X) \bmod q\in O[X]$ is (64)($\log_2 r$) bits =128kbits, and the size of system parameters $(r,G,H;F(X))$ is as large as 162kbits.
3) The complexity G_1 to obtain $F(X)$ is $(64*8*15)(\log_2 r)^2=2^{35}$ bit-operations.
4) The size of $F_{AB}(X,M)=F^{-ba}(YF^{ba}(X))\in O[X,Y]$ is (512)($\log_2 r$) bits =1024 kbits.
5) The complexity G_2 to obtain $F^a(X)$, $f_{aij}\in R$ $(i,j=0,\ldots,7)$ from $F(X)$ and a, is

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

6) The complexity G_3 to obtain $F^{-1}(X)$ from $F(X)$ by using Gaussian elimination is

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

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

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

7) The complexity G_4 to obtain $F^{ab}(X)$ from $F^a(X)$ and b, is

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

8) The complexity G_5 to obtain $F_{UV}(X,Y):= F^{-ba}(YF^{ba}(X))$ from $F^{ba}(X)$ is

$G_3+(512*8)*(\log_2 r)^2 = 2^{37}$ bit-operations.

9) The complexity $G_{encipher}$ for enciphering to calculate $C(m, X)=(F_{AB}(X,{}^1M), F_{AB}(X,{}^2M)$, $F_{AB}(X,{}^3M))$ from $F_{AB}(X,Y)$, ${}^1M$,${}^2M$ and ${}^3M$ is $3*(64*8)*(\log_2 r)^2 = 2^{33}$ bit-operations.

The size of $C(m, X)=(F_{AB}(X,{}^1M), F_{AB}(X,{}^2M), F_{AB}(X,{}^3M))$ is $(64*3)* (\log_2 r)$ bits =384kbits.

We notice that the complexity $G_{encipher}$ required for enciphering every plaintext m is only 2^{33} bit-operations.

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

As

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

$$F^{ba}(F_{AB}(F^{-ba}(\mathbf{1}),{}^eM))$$

$$= F^{ba}(F^{-ab}({}^eMF^{ab}(F^{-ba}(\mathbf{1})))) \bmod r$$

$$={}^eM,$$

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

the complexity $G_{decipher}$ is $(64*2+2)(\log_2 r)^2= 2^{29}$ bit-operations.

11) The complexity G_{multi} required for generating $C(m_1m_2,X)$ from $C(m_1,X)$ and $C(m_2,X)$ is given as follows.

As

$$C(m_1m_2,X) = (F_{AB}(X,{}^1M_{12}),F_{AB}(X,{}^2M_{12}) ,F_{AB}(X,{}^3M_{12}))$$

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

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

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

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

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

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

the complexity G_{multi} is $(512*3+64*3*3)(\log_2 r)^2= 2^{33}$ 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.

§8. Conclusion

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

As theoretically a part of the system parameter G and H needs not to be published, G and H are able to be belonged to user's secret keys. In this case the system parameter is $[r, F(X)]$.

§9.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 [26]. I thank for the publisher (Lambert Academic, Germany) for kindly providing an opportunity to accomplish the task.

§10.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] 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.

[14] 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.

[15] 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/.

[16] 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.

[17] 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/.

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

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

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

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

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

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

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

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

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

Appendix A:

Octinv(A) --

S ← $a_0^2+a_1^2+\ldots+a_7^2$ mod r.

% S^{-1} mod r

r[1] ← r div S ;% integer part of r/S

Res[1] ← r mod S ;% Residue

k ←1

r[0] ← r

Res[0] ← S

while Res[k] $\neq$ 0

begin

k← k + 1

r[k] ← Res[k−2] div Res[k−1]

Res[k] ← res[k−2] mod Res[k−1]

end

Q [k−1] ← (-1)*r[k−1]

L[k−1] ← 1

i ← k−1

while i > 1

begin

Q[i−1] ← (-1)*Q[i] *r[i−1] + L[i]

L[i−1] ← Q[i]

i← i−1

end

invS ← Q[1] mod r

invA[0] ← a_0*invS mod r

For i=1,…,7,

invA[i] ← (-1)*a_i*invS mod r

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

Appendix B:
Theorem 1

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

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

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

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

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

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

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

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

(*Proof*:)

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

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

as was required. q.e.d.

Appendix C:

Theorem 2

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

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

where

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

(*Proof*:)

From (8) and (9) it comes that

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

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

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

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

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

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

We can calculate β^{q^2} as follows.

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

In the same manner we obtain

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

Then we obtain

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

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

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

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

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

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

$$\beta^q=\beta \bmod q,$$

$$\alpha^q=\alpha \bmod q.$$

Then we have

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

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

$$=a_{10} \bmod q,$$

$$b_q=(\beta^q-\alpha^q)/(\beta- \alpha)=1 \bmod q.$$

Then we have

$$a^q=(a_{q0}, b_qa_{11},\ldots,b_qa_{17})$$

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

We therefore arrive at the equation such as

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

where

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

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)

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

then we have

$$a_{n0}= a_{10}^{\ n} \bmod q\ ,(n=1,2,\ldots).$$

$$a_{q0}= a_{10}^{\ q}= a_{10} \bmod q.$$

From (9)

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

$$= a_{10}^{\ n-1}+ b_{n-1}a_{10} \bmod q$$

$$= 2a_{10}^{\ n-1}+ b_{n-2}a_{10}^{2} \bmod q$$

$$\ldots \qquad \ldots$$

$$= (n-1)a_{10}^{\ n-1}+ b_1a_{10}^{\mathrm{n-1}} \bmod q$$

$$= na_{10}^{\ n-1} \bmod q.$$

Then we have

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

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

Appendix D:

Lemma 2

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

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

(*Proof*:)

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

$$AB \bmod r$$

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

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

$$\begin{aligned}
= \{\, & a_0(a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7) \\
& + a_1(a_0b_1 + a_1b_0 + a_2b_4 + a_3b_7 - a_4b_2 + a_5b_6 - a_6b_5 - a_7b_3) \\
& + a_2(a_0b_2 - a_1b_4 + a_2b_0 + a_3b_5 + a_4b_1 - a_5b_3 + a_6b_7 - a_7b_6) \\
& + a_3(a_0b_3 - a_1b_7 - a_2b_5 + a_3b_0 + a_4b_6 + a_5b_2 - a_6b_4 + a_7b_1) \\
& + a_4(a_0b_4 + a_1b_2 - a_2b_1 - a_3b_6 + a_4b_0 + a_5b_7 + a_6b_3 - a_7b_5) \\
& + a_5(a_0b_5 - a_1b_6 + a_2b_3 - a_3b_2 - a_4b_7 + a_5b_0 + a_6b_1 + a_7b_4) \\
& + a_6(a_0b_6 + a_1b_5 - a_2b_7 + a_3b_4 - a_4b_3 - a_5b_1 + a_6b_0 + a_7b_2) \\
& + a_7(a_0b_7 + a_1b_3 + a_2b_6 - a_3b_1 + a_4b_5 - a_5b_4 - a_6b_2 + a_7b_0)\} / |A|^2 \bmod r \\
= \{ & (a_0^2 + a_1^2 + \ldots + a_7^2)\, b_0\} / |A|^2 = b_0 \bmod r
\end{aligned}$$

where $[M]_i$ denotes the i-th element of $M \in O$.

$$
\begin{aligned}
&[A^{-1}(AB)]_1 \\
&=\{ a_0(a_0b_1+a_1b_0+a_2b_4+a_3b_7-a_4b_2+a_5b_6-a_6b_5-a_7b_3) \\
&\quad -a_1(a_0b_0-a_1b_1-a_2b_2-a_3b_3-a_4b_4-a_5b_5-a_6b_6-a_7b_7) \\
&\quad -a_2(a_0b_4+a_1b_2-a_2b_1-a_3b_6+a_4b_0+a_5b_7+a_6b_3-a_7b_5) \\
&\quad -a_3(a_0b_7+a_1b_3+a_2b_6-a_3b_1+a_4b_5-a_5b_4-a_6b_2+a_7b_0) \\
&\quad +a_4(a_0b_2-a_1b_4+a_2b_0+a_3b_5+a_4b_1-a_5b_3+a_6b_7-a_7b_6) \\
&\quad -a_5(a_0b_6+a_1b_5-a_2b_7+a_3b_4-a_4b_3-a_5b_1+a_6b_0+a_7b_2) \\
&\quad +a_6(a_0b_5-a_1b_6+a_2b_3-a_3b_2-a_4b_7+a_5b_0+a_6b_1+a_7b_4) \\
&\quad +a_7(a_0b_3-a_1b_7-a_2b_5+a_3b_0+a_4b_6+a_5b_2-a_6b_4+a_7b_1)\} /|A|^2 \bmod r \\
&=\{(a_0^2+a_1^2+\ldots+a_7^2) b_1\} /|A|^2=b_1 \bmod r.
\end{aligned}
$$

Similarly we have

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

Then

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

Appendix E:

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

Power(A,n,r) --

$P \leftarrow 1$

while $n \neq 0$

begin

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

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

end

Return P

Appendix F:

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

Power($A(X)$,n,r) --

$P(X) \leftarrow \mathbf{1} \in O$

while $n \neq 0$

begin

if n is even then $A(X) \leftarrow A(A(X)) \bmod r$, $n \leftarrow n/2$

otherwise $P(X) \leftarrow A(P(X)) \bmod r$, $n \leftarrow n-1$

end

Return $P(X)$

Appendix G:

Theorem 6

Let O be the octonion ring over a finite ring 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

$$h_0=0 \bmod r,$$

$$g_0^2+g_1^2+\ldots+g_7^2=0 \bmod r,$$

$$h_0^2+h_1^2+\ldots+h_7^2=0 \bmod r$$

and

$$g_1h_1+g_2h_2+g_3h_3+{}_4h_4+g_5h_5+g_6h_6+g_7h_7=0 \bmod r.$$

A,B satisfy the following equations.

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

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

(*Proof*:)

$$GH \bmod r$$

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

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

$= (g_0h_0 - g_1h_1- g_2h_2- g_3h_3-g_4h_4- g_5h_5-g_6h_6-g_7h_7) g_0$

$-(g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3) g_1$

$-(g_0h_2-g_1h_4+g_2h_0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6) g_2$

$-(g_0h_3-g_1h_7-g_2h_5+g_3h_0+g_4h_6+g_5h_2-g_6h_4+g_7h_1) g_3$

$-(g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+g_4h_0+g_5h_7+ g_6h_3 -g_7h_5) g_4,$

$-(g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+g_5h_0+g_6h_1+g_7h_4) g_5$

$-(g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+g_6h_0 +g_7h_2) g_6,$

$-(g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+g_7h_0) g_7) \bmod r$

As

$h_0=0 \bmod r$,

$g_0^2+g_1^2+\ldots+g_7^2=0 \bmod r,$

$h_0^2+h_1^2+\ldots+h_7^2=0 \bmod r$

and

$g_1h_1+ g_2h_2+g_3h_3+{}_4h_4+ g_5h_5+g_6h_6+g_7h_7=0 \bmod r,$

we have

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

$=(g_0h_0 - g_1h_1- g_2h_2- g_3h_3-g_4h_4- g_5h_5-g_6h_6-g_7h_7) g_0$

$-(g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3) g_1$

$-(g_0h_2-g_1h_4+g_2h_0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6) g_2$

$-(g_0h_3-g_1h_7-g_2h_5+g_3h_0+g_4h_6+g_5h_2-g_6h_4+g_7h_1) g_3$

$-(g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+g_4h_0+g_5h_7+ g_6h_3 -g_7h_5) g_4,$

$-(g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+g_5h_0+g_6h_1+g_7h_4) g_5$

$-(g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+g_6h_0 +g_7h_2) g_6$

$-(g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+g_7h_0) g_7$

$=(g_00- 0) g_0$

$- g_0 (g_1 h_1+g_2h_2+g_3h_3+g_4h_4+g_5h_5+g_6h_6+g_7h_7)$

$- g_1(g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3-g_2h_4-g_3h_7+g_4h_2 -g_5h_6+g_6h_5+g_7h_3)$

$- g_2 (g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6-g_3h_5-g_4h_1+g_5h_3-g_6h_7+g_7h_6)$

$- g_3 (g_4h_6+g_5h_2-g_6h_4+g_7h_1-g_4h_6 -g_5h_2+ g_6h_4-g_7h_1)$

$- g_4 (g_5h_7+ g_6h_3 -g_7h_5-g_5h_7- g_6h_3+g_7h_5)$

$- g_5 (g_6h_1+g_7h_4-g_6h_1-g_7h_4)$

$-(g_7h_2) g_6-(-g_6h_2) g_7$

$=0 \bmod r,$

$[(GH)G]_1 \bmod r$

$= (g_0h_0 - g_1h_1- g_2h_2- g_3h_3-g_4h_4- g_5h_5-g_6h_6-g_7h_7)g_1$

$+(g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3)g_0$

$+(g_0h_2-g_1h_4+g_2h_0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6)g_4$

$+(g_0h_3-g_1h_7-g_2h_5+g_3h_0+g_4h_6+g_5h_2-g_6h_4+g_7h_1)g_7$

$-(g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+g_4h_0+g_5h_7+ g_6h_3 -g_7h_5)g_2$

$+(g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+g_5h_0+g_6h_1+g_7h_4)g_6$

$-(g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+g_6h_0 +g_7h_2)g_5$

$-(g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+g_7h_0)g_3$

$= (g_00-g_1h_1- g_2h_2- g_3h_3-g_4h_4- g_5h_5-g_6h_6-g_7h_7)g_1$

$+2(g_1h_1+g_2h_2+g_3h_3+g_4h_4+g_5h_5+g_6h_6+g_7h_7)g_1$

$+(g_0h_1+0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3)g_0$

$+(g_0h_2-g_1h_4+0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6)g_4$

$+(g_0h_3-g_1h_7-g_2h_5+0+g_4h_6+g_5h_2-g_6h_4+g_7h_1)g_7$

$-(g_0h_4+g_1h_2 -g_2h_1 -g_3h_6+0+g_5h_7+ g_6h_3 -g_7h_5)g_2$

$+(g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+0+g_6h_1+g_7h_4)g_6$

$-(g_0h_6+g_1h_5 -g_2h_7+g_3h_4 -g_4h_3 -g_5h_1+0 +g_7h_2)g_5$

$$-(g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+0)g_3$$

$$= \quad h_1\,(g_1^2+g_0^2+g_4^2+g_7^2+g_2^2+g_6^2+g_5^2+g_3^2)$$

$$+\,h_2\,(g_2g_1-g_4g_0+g_0g_4+g_5g_7-g_1g_2-g_3g_6-g_7g_5+g_6g_3)$$

$$+\,h_3\,(g_3g_1-g_7g_0-g_5g_4+g_0g_7-g_6g_2+g_2g_6+g_4h_5-g_1g_3)$$

$$+\,h_4\,(g_4g_1+g_2g_0-g_1g_4-g_6g_7-g_0g_2+g_7g_6-g_3g_5+g_5g_3)$$

$$+h_5\,(g_5g_1-g_6g_0+g_3g_4-g_2g_7+g_7g_2+g_0g_6-g_1g_5-g_4g_3)$$

$$+\,h_6\,(g_6g_1+g_5g_0-g_7g_4+g_4g_7+g_3g_2-g_1g_6-g_0g_5-g_2g_3)$$

$$+\,h_7(g_7g_1+g_3g_0+g_6g_4-g_1g_7-g_5g_2-g_4g_6+g_2g_5-g_0g_3)$$

$$=0 \bmod r.$$

In the same manner we have

$$[(GH)G]_i=0 \bmod r \; (i=2,\ldots,7).$$

Then we have

$$(GH)G=\mathbf{0} \bmod r.$$

In the same manner we have

$$(HG)H=\mathbf{0} \bmod r. \qquad \text{q.e.d.}$$

Appendix H:

Theorem 7

Let O be the octonion ring over a finite ring 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

$$h_0=0 \bmod r\,,$$

$$g_0^2+g_1^2+\ldots+g_7^2=0 \bmod r,$$

$$h_0^2+h_1^2+\ldots+h_7^2=0 \bmod r$$

and

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

G,H satisfy the following equations.

$$GH+HG=2g_0H \bmod r.$$

(*Proof*:)

$$GH \bmod r$$

$$= (\ g_0h_0-g_1h_1-g_2h_2-g_3h_3-g_4h_4-g_5h_5-g_6h_6-g_7h_7 \bmod r,$$

$$g_0h_1+g_1h_0+g_2h_4+g_3h_7-g_4h_2+g_5h_6-g_6h_5-g_7h_3 \bmod r,$$

$$g_0h_2-g_1h_4+g_2h_0+g_3h_5+g_4h_1-g_5h_3+g_6h_7-g_7h_6 \bmod r,$$

$$g_0h_3-g_1h_7-g_2h_5+g_3h_0+g_4h_6+g_5h_2-g_6h_4+g_7h_1 \bmod r,$$

$$g_0h_4+g_1h_2-g_2h_1-g_3h_6+g_4h_0+g_5h_7+g_6h_3-g_7h_5 \bmod r,$$

$$g_0h_5-g_1h_6+g_2h_3-g_3h_2-g_4h_7+g_5h_0+g_6h_1+g_7h_4 \bmod r,$$

$$g_0h_6+g_1h_5-g_2h_7+g_3h_4-g_4h_3-g_5h_1+g_6h_0+g_7h_2 \bmod r,$$

$$g_0h_7+g_1h_3+g_2h_6-g_3h_1+g_4h_5-g_5h_4-g_6h_2+g_7h_0 \bmod r),$$

$HG \bmod r$

$$= (h_0g_0 - h_1g_1 - h_2g_2 - h_3g_3 - h_4g_4 - h_5g_5 - h_6g_6 - h_7g_7 \bmod r,$$

$$h_0g_1 + h_1g_0 + h_2g_4 + h_3g_7 - h_4g_2 + h_5g_6 - h_6g_5 - h_7g_3 \bmod r,$$

$$h_0g_2 - h_1g_4 + h_2g_0 + h_3g_5 + h_4g_1 - h_5g_3 + h_6g_7 - h_7g_6 \bmod r,$$

$$h_0g_3 - h_1g_7 - h_2g_5 + h_3g_0 + h_4g_6 + h_5g_2 - h_6g_4 + h_7g_1 \bmod r,$$

$$h_0g_4 + h_1g_2 - h_2g_1 - h_3g_6 + h_4g_0 + h_5g_7 + h_6g_3 - h_7g_5 \bmod r,$$

$$h_0g_5 - h_1g_6 + h_2g_3 - h_3g_2 - h_4g_7 + h_5g_0 + h_6g_1 + h_7g_4 \bmod r,$$

$$h_0g_6 + h_1g_5 - h_2g_7 + h_3g_4 - h_4g_3 - h_5g_1 + h_6g_0 + h_7g_2 \bmod r,$$

$$h_0g_7 + h_1g_3 + h_2g_6 - h_3g_1 + h_4g_5 - h_5g_4 - h_6g_2 + h_7g_0 \bmod r).$$

$$[GH + HG]_0 = g_0h_0 - g_1h_1 - g_2h_2 - g_3h_3 - g_4h_4 - g_5h_5 - g_6h_6 - g_7h_7$$

$$+ h_0g_0 - h_1g_1 - h_2g_2 - h_3g_3 - h_4g_4 - h_5g_5 - h_6g_6 - h_7g_7$$

$$= 0 - 0 + 0 - 0 = 0 = 2g_0h_0 \bmod r.$$

$$[GH + HG]_1 = g_0h_1 + g_1h_0 + g_2h_4 + g_3h_7 - g_4h_2 + g_5h_6 - g_6h_5 - g_7h_3$$

$$+ h_0g_1 + h_1g_0 + h_2g_4 + h_3g_7 - h_4g_2 + h_5g_6 - h_6g_5 - h_7g_3$$

$$= 2g_0h_1 \bmod r.$$

In the same manner

$$[GH + HG]_i = 2g_0h_i \quad (i = 2, \ldots, 7).$$

We have

$$GH + HG = 2g_0H \bmod r. \qquad \text{q.e.d.}$$