University of AL-Qadisiyah

College Of Education

Department of Mathematics

HXDTRU Cryptosystem Based On Hexadecnion Algebra

A research

Submitted to mathematic Department/College of education

University of Al- Qadisiyah As a Partial Fulfillment of the Requirements

for the Degree Of Bachelor of Science in Mathematics

By

Riam Riad Murad

Supervised By

2018-2019

CHAPTER ONE

NTRU Cryptosystem

CHAPTER TWO

QUTR Cryptosystem

CHAPTER THREE

HXDTRU Cryptosystem

الاهداء

الهي لا يطيب الليل الا بشكرك ولا يطيب النهار الا بطاعتك ولا تطيب اللحظات الا بذكرك ولا تطيب الجنة الا برؤيتك .

الله جل جلاله . . .

الى من بلغ الرسالة وأدى الأمانة ونصح الأمة الى نبي الرحمة سيدنا

محمد (صل الله عليه واله وسلم) .

الى من كلله بالهيبة والوقار ، الى من علمني العطاء دون انتظار ، الى من احمل اسمه بكل افتخار .

والدي العزيز . . .

الى ملاكي في الحياة الى معنى الحياة ومعنى الحب ومعنى التفاني ، الى من كان دعائها سر نجاحي .

امي الحنونة . . .

شكر وتقدير

الحمد لله على ما انعم والشكر على هنيء عطائك ومحمود بلائك وجليل اللائك ، ثم جزيل الشكر والامتنان الى مشرف البحث الدكتور

(حسن راشد ياسين)

بما بذله من جهد وفقه الله لما يحب ويرضى .

والشكر الموصول الى رئيس القسم والاساتذة الكرام الذين ساهموا وأشرفوا في تكوين الدفعة الرابعة .

والشكر والتقدير الى جميع من كان له يد العون في هذا البحث .

الباحث

هُوَ اللَّهُ الَّذِي لَا إِلَٰهَ إِلَّا هُوَ الْمَلِكُ الْقُدُّوسُ
السَّلَامُ الْمُؤْمِنُ الْمُهَيْمِنُ الْعَزِيزُ الْجَبَّارُ الْمُتَكَبِّرُ
سُبْحَانَ اللَّهِ عَمَّا يُشْرِكُونَ ﴿٢٣﴾

صدق الله العلي العظيم

سورة الحشر

الآية(٢٣)

Table Of Contents

ABSTRACT

In this reaserch, we surevy a public key cryptosystem based on hexadecimal algebra, which is a non-associative, non-commutative and alternativ; which called HXDTRU. The security of HXDTRU with N dimension equals the security of NTRU with the $16N$ dimension, and HXDTRU with N dimension is sixteen times faster Ulan NTRU with the $16N$ dimensions, which is a respectable improvement especially for large N.

1. INTRODUCTION

The NTRU (number theory research unit) public key cryptosystem was founded in 1996 by-three mathematicians Jeffery Hoffstein, Joseph H. Silverman and Jill Piper, the basic collection of objects used by the NTRU public key cryptosystem take place in a truncated polynomial ring of degree $N-1$ with integer coefficients in $Z[x]/(xN-1)$ (1). It is the first public key cryptosystem that do not depend on factorization (as RSA cryptosystem) or discrete algorithmic problems (as ELgamal cryptosystem and Ecc cryptosystem).

Many researchers have tried to improve the NTRU cryptosystem through choosing a different ring and applying a more efficient linear transformation. In 2005, M.Coglianese and BiGoi, presented a new cryptosystern called MaTRU by using ring of $k \star k$ matrices of polynomials of order n (2). In 2009, Malekian et al., introduced QTRU cryptosystem based on quaternion algebra (3, 4), They also introduced OTRU cryptosystern based on octonions algebra (4,5). In 2015, Majeed introduced CQTRU cryptosystem based on commutative quatemions algebra (6). In this paper, we presented a new multidimensional public key cryptosystem HXDTRU by using hexadecnion algebra.

1.1. Description of the NTRU algorithm

NTRU cryptosystem depends on three integer parameters (N, p, q) and four sets $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_\phi, \mathcal{L}_m$ of polynomials of degree $N-1$ with integer coefficients. Note that p and q need not be prime, but we will assume that $gcd(p,q) = 1$, and q will always be considerably larger than p. We work in the ring

$R = Z[X]/(X^N - 1)$. An element $F \in R$ will be written as a polynomial or a vector,

$$F = L \sum_{i=0}^{N-1} F_i x^i = [F_0, F_1, \ldots, . F_{N-1}].$$

We write $\circledast$ to denote multiplication in R. This star multiplication is given explicitly as a cyclic convolution product,

$$F \circledast G = H \; with \; H_k = \sum_{i=0}^{k} F_i G_{k-i} + \sum_{i=k+1}^{N-1} F_i G_{N+k-i} = \sum_{i+j \equiv k \; (mod \; N)} F_i G_j.$$

When we do a multiplication modulo (say) q, we mean to reduce the coefficients modulo q.

Remark:

In principle, computation of a product $F \circledast G$ requires N^2 multiplications. However, for a typical product used by NTRU, one of F or G has small coefficients, so the computation of $F \circledast G$ is very fast. On the other hand, if N is taken to be large, then it might be faster to use Fast Fourier Transforms to comp e products $F \circledast G$ in $O(N \; log \; N)$ operations.

1.2. Key Creation.

To create an NTRU key, Ali randomly chooses two polynomials $f, g \in \mathcal{L}_g$. The polynomial f must satisfy the additional requirement that it have inverses modulo q and modulo p. For suitable parameter choices, this will be true for most choices of f, and the actual computation of these inverses is easy using a modification of the Euclidean algorithm. We will denote these inverses by F_q and F_p, that is,

$$F_q \circledast f = 1 \,(mod\, q) \text{ and } F_p \circledast f = 1 \,(mod\, p). \qquad (1)$$

Ali next computes the quantity

$$h \equiv F_q \circledast g \,(mod\, q). \qquad (2)$$

Ali 's public key is the polynomial h. Ali 's private key is the polynomial f, although in practice he will also want to store F_p.

1.3. Encryption.

Suppose that Ahmed (the encrypter) wants to send a message to Ali (the decrypter). She begins by selecting a message m from the set of plaintexts $\mathcal{L}_m$. Next she randomly chooses a polynomial $\phi \in \mathcal{L}_\phi$, and uses Ali 's public key h to compute

$$e \equiv p\phi \circledast h + m \,(mod\, q).$$

This is the encrypted message which Ahmed transmits to Ali.

1.4. Decryption.

Suppose that Ali has received the message e from Ahmed and wants to decrypt it using his private key $f\cdot$ To do this efficiently, Ali should have precomputed the polynomial F_p described in Section 1.1.

In order to decrypt e, Ali first computes

$$A \equiv f \circledast e(mod\, q),$$

where he chooses the coefficients of a in the interval from $-q/2$ to $q/2$. Now treating a as a polynomial with integer coefficients, Ali recovers the message by computing

$$F_p \circledast a\ (mod\, p).$$

Remark:

For appropriate parameter values, there is an extremely high probability that the decryption procedure will recover the original message. However, some parameter choices may cause occasional decryption failure, so one should probably include a few check bits in each message block. The usual cause of decryption failure will be that the message is improperly centered. In this case Ali will be able to recover the message by choosing the coefficients of $A \equiv f \circledast e(mod\, q)$ in a slightly different interval, for example from $-q/2 + x$ to $q/2 + x$ for some small (positive or negative) value of x. If no value of x works, then we say that we have gap failure and the message cannot be decrypted as

easily. For w osen parameter values, this will occur so rarely that it can be ignored in practice.

1.5. Why Decryption Works.

The polynomial a that Ali computes satisfies

$$A \equiv f \circledast e \equiv f \circledast p\phi \circledast h + f \circledast m \,(mod\, q)$$

$$= f \circledast p\phi \circledast F_q \circledast g + f \circledast m \,(mod\, q) \quad from\,(2),$$

$$= p\phi \circledast g + f \circledast m \,(mod\, q) \qquad from(1)$$

Consider this last polynomial $p\phi \circledast g + f \circledast m$. For appropriate parameter choices, we can ensure that (almost always) all of its coefficients lie between $-q/2$ and $q/2$, so that it doesn't change if its coefficients are reduced modulo q. This means that when Dan reduces the coefficients of $f \circledast e$ modulo q into the interval from $-q/2$ to $q/2$, he recovers exactly the polynomial

$$A = p\phi \circledast g + f \circledast m \in Z[X]/(X^N - 1).$$

Reducing a modulo p then gives him the polynomial $f \circledast m \,(mod\, p)$, and multiplication by F_p retrieves the message $m \,(mod\, p)$.

2.1. Proposed Scheme: QTRU

Similar to NTRU, the security of the QTRU cryptosystem depends on three parameters (N, P, q) and four subsets $\mathcal{L}_f$, $\mathcal{L}_m$, $\mathcal{L}_\phi$, $\mathcal{L}_g \subset \mathbb{A}$ $(\mathbb{A} = (\frac{-1,-1}{\mathbb{Z}[x]/(x^N-1)}))$· Here, N, p and q are constant parameters which playa role similar to the equivalent parameters in NTRU. The constants d_f, d_g, d_ϕ , and d_m and the subsets $\mathcal{L}_f, \mathcal{L}_\phi$, $\mathcal{L}_g$ and $\mathcal{L}_m$, are defined exactly as in Table 1. Since ell'fryption and decryption are taking place in a multi-dimensional vector space, the following notations and symbols are required

$$\vec{F} = f_0 + f_1.i + f_2.j + f_3.k \in (\frac{-1,-1}{\mathbb{Z}[x]/(x^N-1)}) \text{ and}$$

$$\{ f_0 \triangleq f_0(x), f_1 \triangleq f_1(x), f_2 \triangleq f_2(x), f_2 \triangleq f_3(x) \} \in \mathbb{Z}[x]/(x^N - 1).$$

The symbol $\star$ denotes the quatemionic multiplication and is defined as follows

$$\vec{F} \star \vec{G} = (f_0 + f_1.i + f_2.j + f_3.k) \star (g_0 + g_1.i + g_2.j + g_3.k)$$

$$= (f_0 \star g_0 - f_1 \star g_1 - f_3 \star g_3 - f_2 \star g_2)$$

$$+ (f_0 \star g_1 + f_1 \star g_0 - f_3 \star g_2 + f_2 \star g_3) \cdot i$$

$$+ (f_3 \star g_1 + f_2 \star g_0 + f_0 \star g_2 - f_1 \star g_3) \cdot j$$

$$+ (f_1 \star g_2 + f_0 \star g_3 - f_2 \star g_1 + f_3 \star g_0) \cdot k,$$

where $\star$ denotes the convolution product. We denote the conjugate of a quaternion $\vec{F}$ by $\vec{F}^*$. QTRU can now be described as follows.

2.2. Key Generation.

In order to generate a pair of public and private keys, two small quaternion (i.e., quaternions with small norm) $\vec{F}$ and $\vec{G}$ are randomly generated.

$\vec{F} = f_0 + f_1.i + f_2.j + f_3.k$, such that $f_0, f_1, f_2, f_3 \in \mathcal{L}_f$,

$\vec{G} = g_0 + g_1.i + g_2.j + g_3.k$, such that $g_0, g_1, g_2, g_3 \in \mathcal{L}_g$.

The quaternion $\vec{F}$ must be invertible over $\mathbb{A}_0 = (\frac{-1,-1}{\mathbb{Z}_p[x]/(x^N-1)})$ and $\mathbb{A}_1 = (\frac{-1,-1}{\mathbb{Z}_p[x]/(x^N-1)})$. As mentioned in the previous section, the necessary and sufficient condition for $\vec{F}$ to be invertible over $\mathbb{A}_0$ and $\mathbb{A}_1$ is that the polynomial $\|\vec{F}\| = (f_0^2 + f_1^2 + f_2^2 + f_3^2)$ be invertible over the rings $\mathbb{Z}_p[x]/(x^N - 1)$ and $\mathbb{Z}_q[x]/(x^N - 1)$. Given the fact that invertiblilty of quaternion $\vec{F}$ depends on the four polynomials f_0, f_1, f_2, f_3, there is more freedom in selection of these polynomials. For example, there is no necessity for selecting all the polynomials from $\mathcal{L}_f$ as it is sufficient to have $f_0^2 + f_1^2 + f_2^2 + f_3^2|_{x=1} \neq 0 \pmod{p \text{ and } q}$. If the generated quaternion is not invertible over $\mathbb{A}_0$ and $\mathbb{A}_1$, a new quaternion can easily be generated.

After generation of $\vec{F}$ and $\vec{G}$, the inverses of $\vec{F}$ (denoted by $\vec{F}_p$ and $\vec{F}_q$) will be computed in the following way

$$\vec{F}_p = \omega_0 + \omega_1.i + \omega_2.j + \omega_3.k,$$

$$\vec{F}_q = \tau_0 + \tau_1.i + \tau_2.j + \tau_3.k,$$

Now, the public key, which is a quaternion, is calculated and then made public as follows

$$\vec{H} = \vec{F}_q \star \vec{G} =$$

$$= (\tau_0 \star g_0 - \tau_1 \star g_1 - \tau_3 \star g_3 - \tau_2 \star g_2)$$

$$+ (\tau_0 \star g_1 + \tau_1 \star g_0 - \tau_3 \star g_2 + \tau_2 \star g_3) \cdot i$$

$$+ (\tau_3 \star g_1 + \tau_2 \star g_0 + \tau_0 \star g_2 - \tau_1 \star g_3) \cdot j$$

$$+ (\tau_1 \star g_2 + \tau_0 \star g_3 - \tau_2 \star g_1 + \tau_3 \star g_0) \cdot k,$$

The quaternions $\vec{F}$, $\vec{F}_p$and $\vec{F}_q$ will be kept secret in order to be used in the decryption phase.

2.3. Encryption.

In the encryption process in the first the conversion of the incoming message (s) into one quaternion, the ciphertext will be computed and sent in the following way.

Data Quaternion

$$\vec{M} = m_0 + m_1.i + m_2.j + m_3.k,$$

Blinding Quaternion

$$\vec{\Phi} = \phi_0 + \phi_1.i + \phi_2.i + \phi_3.k,$$

Ciphertext

$$\vec{\mathrm{E}} = P \cdot \vec{\mathrm{H}} \star \vec{\Phi} + \vec{M}$$

Encryption needs one quaternionic multiplication including 16 convolution multiplications with $O(N^2)$ complexity, and 4 polynomial additions with $O(N)$complexity. In the encryption phase, a total of four data vectors are encrypted at once.

2.4. Decryption.

The received quaternion E is first multiplied by the private key P

$$\vec{\mathrm{F}} \star \vec{\mathrm{E}} = \left(\vec{\mathrm{F}} \star \left(P \cdot \vec{\mathrm{H}} \star \vec{\Phi} + \vec{M}\right)\right) mod\ q$$

$$= (\vec{\mathrm{F}} \star P \cdot \vec{\mathrm{H}} \star \vec{\Phi} + \vec{\mathrm{F}} \star \vec{M})\ mod\ q$$

$$= \left(P \cdot \vec{\mathrm{F}} \star \vec{F}_q \star \vec{\mathrm{G}} \star \vec{\Phi} + \vec{\mathrm{F}} \star \vec{M}\right) mod\ q$$

$$= \left(P \cdot \vec{\mathrm{G}} \star \vec{\Phi} + \vec{\mathrm{F}} \star \vec{M}\right).$$

Take $\mathbb{A} = P \cdot \vec{\mathrm{G}} \star \vec{\Phi} + \vec{\mathrm{F}} \star \vec{M}\ (mod\ q)$

$$\mathbb{B} = \mathbb{A}(mod\ p)$$

$$= \vec{\mathrm{F}} \star \vec{M}\ (mod\ p)$$

$$\mathbb{M} = \vec{F}_p \star\ \mathbb{B}\ (mod\ p)$$

Theorem: Successful Decryption. Probability of successful decryption in QTRU is

$$Pr\left(\left|a_{i,k}\right| \leq \frac{q-1}{2}\right) = Pr\left(-\frac{q-1}{2} \leq a_{i,k} \leq \frac{q-1}{2}\right)$$

$$= 2\Phi\left(\frac{q-1}{2\sigma}\right) - 1$$

where Φ denotes the distribution of the standard normal variable and $\sigma = \sqrt{\frac{16P^2 d_\phi d_g}{N} + \frac{4d_f(P-1)(P+1)}{6}}$.

Corollary(1): The probability for each of the messages $m_0, m_1, m_2, or\ m_3$ to be correctly decrypted is

$$\left(2\Phi(\frac{q-1}{2\sigma})-1\right)^N$$

Corollary(2): The probability for all the messages $m_0, m_1, m_2, and\ m_3$ to be correctly decrypted is

$$\left(2\Phi(\frac{q-1}{2\sigma})-1\right)^{4\cdot N}$$

2.5. Brute Force Attack.

In QTRU, an attacker knows the constant and public parameters, namely $d_\phi, d_g, d_f, q, p,$ and N, as well as, the public key $\vec{H} = \vec{F}_q \star \vec{G} = h_0 + h_{1\cdot i} + h_{2\cdot j} + h_{3\cdot k}$. If the attacker finds one of the quaternions $\vec{G} \in \mathcal{L}_g\ or\ \vec{F} \in \mathcal{L}_f$, the private key can e easily computed.

In order to find $\vec{G}$ or $\vec{F}$ using a brute force attack, the attacker can try all possible values and check to see if $\vec{F} \star \vec{H}$ $(\vec{G} \star \vec{H}^{-1})$ turns into a quaternion with small coefficients or not. The total state space for the two subsets $\mathcal{L}_f$ and $\mathcal{L}_g$ is calculated as follows

$$|\mathcal{L}_f| = \binom{N}{d_f}^4 \binom{N-d_f+1}{d_f}^4 = \frac{(N!)^4}{(d_f!)^8 (N-2d_f)!^4}.$$

3.1. THE PROPOSED HXDTRU CRYPTOSYSTEM

The parameters N, p and q are similar to the parameters in NTRU, the constant d_f, d_g, d_m and d_Φ are integers less than N. Let $K = Z[x]/(x^N - 1)$ be the truncated polynomials ring of degree $N-1$. We define a new algebra as follows:

3.2. HEXADECNION ALGEBRA(HD)

In this section, we define hexadecnion and properties. A vector space of sixteen dimensions over real number defined as follows

$$HD = \{w \mid w=r_0+\sum_{i=1}^{15} r_i y_i \; l \; r_0, r_1, \ldots, r_{15} \epsilon R\}$$

Where $\beta= \{1, y_1, y_2, \ldots, y_{15}\}$ form basis of hexadecnion algebra and r_i's are scalar in a set of real number .Let w_1 and $w_2 \epsilon H$ such that

$$w_1 = r_0+r_1y_1+r_2y_2+ \ldots + r_{14}y_{14}+r_{15}y_{15}$$

$$w_2= \acute{r}_0+ \acute{r}_1y_1+ \acute{r}_2y_2+ \ldots + \acute{r}_{14}y_{14}+ \acute{r}_{15}y_{15}$$

Addition of w_1 and w_2 adding corresponding coefficients

$w_1+ w_2 = (r_0+\acute{r}_0)+(r_1+\acute{r}_1)y_1+(r_2+\acute{r}_2)y_2+ \ldots + r_{14}+r_0+r_1y_1+r_2y_2+ \ldots + (r_{14}+ \acute{r}_{14})y_{14} +(r_{15}+\acute{r}_{15})y_{15}$.

Multiplication of w_1 and w_2 can be determined by the following multiplication table $3y_1$

$$y_i^{\,2}= -1 \text{ and } y_iy_j = - y_jy_i \quad i \neq j \quad i, j = 1,2, \ldots ,15$$

and the multiplication is non-commutative and non-associative $((y_5y_2)\, y_{11} \neq y_5(\, y_2 y_{11}))$ but is alternative .For any scalar α then

$$\alpha w = \alpha\, (r_0+r_1y_1+r_2y_2+ \ldots + r_{14}y_{14}+r_{15}y_{15})$$

$$= \alpha r_0+ \alpha r_1y_1+ \alpha r_2y_2+ \ldots + \alpha\, r_{14}y_{14}+ \alpha r_{15}y_{15}$$

The conjugate of a hexadecnion $w=r_0+\sum_{i=1}^{15} r_i y_i$ is defined as follows $\overline{w} = r_0 -\sum_{i=1}^{15} r_i y_i$ and the square norm is given by $N(w) = w\, \overline{w} = \sum_{i=1}^{15} r_i^{\,2}$.

The multiplication inverse of any non zero element w in HD such that $gcd\,(N(w), 15) = 1$ is defined as follows $w^{-1} = N(w)^{-1}\,\overline{w}$.

3.3. ALGEBRA STRUCTURE OF HXDTRU

Let R be a finite ring with char $(R) \neq 2$, we define the hexadecnion algebra ψ over R as follows $\psi = \{r_0 + \sum_{i=1}^{15} r_i\, y_i \; l \; r_0, r_1, \ldots, r_{15} \epsilon\, R\}$ with multiplication, multiplication inverse and a norm has the like qualities of HD. Note that ψ is a non-associative and because usual multiplication of matrices is associative then it doesn't have any matrix representation. Now, consider truncated polynomial rings $R = Z[y]/\,(y^N-1)$, $R_p(y) = (Z/pZ)\,[y]/\,(y^N-1)$ and $R_q(y) = (Z/qZ)\,[y]/\,(y^N-1)$ which. We define three hexadecnion algebras ψ, ψ_p and ψ_q as follows

$$\Psi = \{f_0 + \sum_{i=1}^{15} f_i(y)\, y_i \; l \; f_0, f_1, \ldots, f_{15} \epsilon\, R\}$$

$$\Psi_p = \{f_0 + \sum_{i=1}^{15} f_i(y)\, y_i \; l \; f_0, f_1, \ldots, f_{15} \epsilon\, R_p\}$$

$$\Psi_q = \{f_0 + \sum_{i=1}^{15} f_i(y)\, y_i \; l \; f_0, f_1, \ldots, f_{15} \epsilon\, R_q\}$$

The parameters N, p and q are similar to the parameters in NTRU .The constant d_f, d_g, d_m and d_ϕ are defined as the table Now, let ϕ_1 and $\phi_2 \epsilon\, \Psi_p$ or Ψ_q such that

$$\phi_1 = f_0(y) + f_1(y)\, y_1 + f_2(y)\, y_2 + \ldots + f_{14}(y)\, y_{14} + f_{15}(y)\, y_{15}$$

$$\phi_2 = g_0(y) + g_1(y)\, y_1 + g_2(y)\, y_2 + \ldots + g_{14}(y)\, y_{14} + g_{15}(y)\, y_{15}$$

where f_i and $g_i \epsilon\, R_p$ or R_q.

The addition of $\phi_1$and ϕ_2 is adding corresponding coefficients including $16N$ modular addition mod p or mod q

$$\phi_1 + \phi_2 = f_0(y) + g_0(y) + (f_1(y) + g_1(y))\, y_1 + (f_2(y) + g_2(y))\, y_2 + \ldots + (f_{14}(y) + g_{14}(y))\, y_{14} + (f_{15}(y) + g_{15}(y))\, y_{15}$$

The multiplication of ϕ_1 and ϕ_2 is defined

$\phi_1 \circ \phi_2 = (f_0*g_0 - f_1*g_1 - f_2*g_2 - f_3*g_3 - f_4*g_4 - f_5*g_5 - f_6*g_6 - f_7*g_7 - f_8*g_8 - f_9*g_9 - f_{10}*g_{10} - f_{11}*g_{11} - f_{12}*g_{12} - f_{13}*g_{13} - f_{14}*g_{14} - f_{15}*g_{15}) + (f_0*g_1 + f_1*g_0 + f_2*g_3 + f_3*g_5 + f_4*g_5 - f_5*g_4 - f_6*g_7 + f_7*g_6 + f_8*g_9 - f_9*g_8 + f_{10}*g_{11} - f_{11}*g_{10} + f_{12}*g_{13} - f_{13}*g_{12} + f_{14}*g_{15} - f_{15}*g_{14})y_1 + \ldots + (f_0*g_{15} + f_1*g_{14} - f_2*g_{13} + f_3*g_{12} - f_4*g_{11} - f_5*g_{10} + f_6*g_9 + f_7*g_8 - f_8*g_7 - f_9*g_6 + f_{10}*g_5 + f_{11}*g_4 - f_{12}*g_3 + f_{13}*g_2 - f_{14}*g_1 + f_{15}*g_0)y_{15},$

such that * is convolution product

3.4. The PROPSED HXDTRU

The security of HXDTRU cryptosystem depended on the parameters N, p and q (where N is a prime, $gcd(p, q) = 1$) and q much larger than p) and the subsets L_f, L_g, L_m and $L_\phi \subset \Psi$ as defined as follows:

$L_f = \{f_0(x) + f_1(x)x_1 + f_2(x)x_2 + \ldots + f_{14}(x)x_{14} + f_{15}(x)x_{15} \in \Psi \mid f_i \in K$ has d_f coefficients equal to $+1$, $(d_f - 1)$ equal to -1, the rest are 0 $\}$,

$L_g = \{g_0(x) + g_1(x)x_1 + g_2(x)x_2 + \ldots + g_{14}(x)x_{14} + g_{15}(x)x_{15} \in \Psi \mid g_i \in K$ has d_g coefficients equal to $+1$, d_g equal to -1, the rest are 0 $\}$,

$L_m = \{m_0(x) + m_1(x)x_1 + m_2(x)x_2 + \ldots + m_{14}(x)x_{14} + m_{15}(x)x_{15} \in \Psi \mid$ coefficients of $m_i(x) \in \Psi$ are chosen modulo p, between $p/2$ and $p/2\}$ and

$L_\Phi = \{\Phi_0(x) + \Phi_1(x)x_1 + \Phi_2(x)x_2 + \ldots + \Phi_{14}(x)x_{14} + \Phi_{15}(x)x_{15} \in \Psi \mid \Phi_i \in k$ has d_Φ coefficients equal to $+1$, d_Φ equal to -1, the rest are 0 $\}$ Also, d_f, d_g and d_ϕ are constant parameters similar role as in NTRU.

HXDTRU can now be depicted beneath:

a) KEY GENERATION

To generate the public key and private key two small (small norm) F and G ϵ Ψ are randomly generated

$$F = f_0(y) + f_1(y)\, y_1 + f_2(y)\, y_2 + \ldots + f_{14}(y)\, y_{14} + f_{15}(y)\, y_{15},$$

$$f_0, f_1, f_2, \ldots, f_{14}, f_{15} \epsilon L_f$$

$$G = g_0(y) + g_1(y)\, y_1 + g_2(y)\, y_2 + \ldots + g_{14}(y)\, y_{14} + g_{15}(y)\, y_{15},$$

$$g_0, g_1, g_2, \ldots, g_{14}, g_{15} \epsilon L_g$$

Such that F must be has multiplication inverse over Ψ_p and Ψ_q. If F is not invertible (when the inverse of $\sum_{i=1}^{15} f_i^2(y)$ is not exist in $Z_p[y]/(y^N-1)$ or $Z_q[y]/(y^N-1)$ then a new hexadecnion F will choose. The inverse of F is denoted by F_P and F_q over algebra Ψ_p and Ψ_q respectively. Now, the public key is calculated as follows:

$$H = F_q \circ G \epsilon \Psi_q$$

$$= h_0(y) + h_1(y)\, y_1 + h_2(y)\, y_2 + \ldots + h_{14}(y)\, y_{14} + h_{15}(y)\, y_{15}$$

F, F_P and F_q must be kept secret in order to be employ decryption stage. When the like parameters N, p and q are employ NTRU and HXDTRU, the key generation of NTRU faster than that of HXDTRU, but the speed key generation of HXDTRU with N, p and q is equal the speed key generation of NTRU with $16N$, p and q.

b) ENYCRYPTION

At the beginning of encryption process, convert the message M to the form

$$M = m_0(y) + m_1(y)\, y_1 + m_2(y)\, y_2 + \ldots + m_{14}(y)\, y_{14} + m_{15}(y)\, y_{15}$$

Where $m_i(y) \epsilon L_m$, $i=0, 1, \ldots, 15$ and randomly chooses another small heyadecnion ϕ.

Computes the encrypted message M as follows:

$$E = pH \circ \phi + M \epsilon \Psi_q,$$

the encryption in HXDTRU needs one hexadecnion multiplication including 256 convolution multiplication.

c) DECRYPTION

Fatima received massage E from Tiba and would like to decrypted it.

Multiplied by her private key F on the left and then on right as follows:

$$A = (F \circ E) \circ F \epsilon \Psi_q$$
$$= (F \circ (pH \circ \phi + M)) \circ F \epsilon \Psi_q$$
$$= p\,(F \circ (H \circ \phi)) \circ F + (F \circ M) \circ F \epsilon \Psi_q$$
$$= p\,(F \circ H) \circ (\phi \circ F) + (F \circ M) \circ F \epsilon \Psi_q \quad \text{(by moufang identity)}$$
$$= p\,(F \circ (F_q \circ G)) \circ (\phi \circ F) + (F \circ M) \circ F \epsilon \Psi_q$$
$$= p\,G \circ (\phi \circ F) + (F \circ M) \circ F \epsilon \Psi_q$$

The coefficients of sixteen polynomial in $p\,G \circ (\phi \circ F) + (F \circ M) \circ F$ must be lie in the intervals $(-q/2, q/2]$ and the last reduction mod q will not be required. When reduced $(\phi \circ F) + (F \circ M) \circ F$ to $mod\ p$, the term $F \circ M\ (mod\ p)$ remains and $pG \circ (\phi \circ F)$ vanishes.

$$A = F \circ M \epsilon \Psi_P.$$

By multiply $A = F \circ M\ (mod\ p)$ by F_P, she get $M = F_P \circ A$ and adjust the coefficients lie in the interval $[-p/2, p/2]$.

3.5. SUCCESSFUL DECRYPTION

If all hexadecnion coefficients of $p\,G \circ (\phi \circ F) + (F \circ M) \circ F$ belong to the interval $(-q/2, q/2]$ then the probability of successful decryption is increase. Now, to compute this probability, first, write

$$A = pG \circ (\phi \circ F) + (F \circ M) \circ F \text{ in the form}$$

$$A = a_0(y) + a_1(y)\, y_1 + a_2(y)\, y_2 + \ldots + a_{14}(y)\, y_{14} + a_{15}(y)\, y_{15}.$$

The polynomial $a_0(y)$

$$a_0 = p\,(g_0 \phi_0 f_0 - g_0 \phi_1 f_1 - g_0 \phi_2 f_2 - g_0 \phi_3 f_3 - g_0 \phi_4 f_4 - g_0 \phi_5 f_5 - g_0 \phi_6 f_6 - g_0 \phi_7 f_7 - g_0 \phi_8 f_8 - g_0 \phi_9 f_9 - g_0 \phi_{10} f_{10} - g_0 \phi_{11} f_{11} - g_0 \phi_{12} f_{12} - g_0 \phi_{13} f_{13} - g_0 \phi_{14} f_{14} - g_0 \phi_{15} f_{15} + \ldots + g_{15} \phi_0 f_{15} + g_{15} \phi_1 f_{14} - g_{15} \phi_2 f_{13} + g_{15} \phi_3 f_{12} - g_{15} \phi_4 f_{11} - g_{15} \phi_5 f_{10} + g_{15} \phi_6 f_9 + g_{15} \phi_7 f_8 - g_{15} \phi_8 f_7 - g_{15} \phi_9 f_6 + g_{15} \phi_{10} f_5 + g_{15} \phi_{11} f_4 - g_{15} \phi_{12} f_3 + g_{15} \phi_{13} f_2 - g_{15} \phi_{14} f_1 + g_{15} \phi_{15} f_0) + \ldots + (f_0^{\,2} m_0 + f_1^{\,2} m_0 + f_2^{\,2} m_0 + f_3^{\,2} m_0 + f_4^{\,2} m_0 + f_5^{\,2} m_0 + f_6^{\,2} m_0 + f_7^{\,2} m_0 + f_8^{\,2} m_0 + f_9^{\,2} m_0 + f_{10}^{\,2} m_0 + f_{11}^{\,2} m_0 + f_{12}^{\,2} m_0 + f_{13}^{\,2} m_0 + f_{14}^{\,2} m_0 + f_{15}^{\,2} m_0$$

$$= [\, a_{0,0}, a_{0,1}, a_{0,2}, \ldots, a_{0,N-1}].$$

Each polynomial of $a_0, a_1, a_2, \ldots, a_{15}$ is calculated in the similar method.

Now, by definition of the L_f, L_g, L_m and L_ϕ we obtain

$$f_i = [f_{i,0}, f_{i,1}, f_{i,2}, \ldots, f_{i,N-1}] \quad i = 0,1,2, \ldots, 15$$

$$g_i = [g_{i,0}, g_{i,1}, g_{i,2}, \ldots, g_{i,N-1}] \quad i = 0,1,2, \ldots, 15$$

$$\phi_i = [\, \phi_{i,0}, \phi_{i,1}, \phi_{i,2}, \ldots, \phi_{i,N-1}] \quad i = 0,1,2, \ldots, 15$$

$$Pr\,(f_{i,j} = 1) = \frac{d_f}{N}, \quad Pr\,(f_{i,j} = -1) = \frac{d_f - 1}{N} \cong \frac{df}{N}, \quad Pr\,(f_{i,j} = 0) = 1 - \frac{2\, d_f}{N}$$

$$Pr\,(g_{i,j}=1)=Pr\,(g_{i,j}=-1)=\frac{d_g}{N}\,,\ Pr\,(g_{i,j}=0)=1-\frac{2\,d_g}{N}$$

$$Pr\,(\phi_{i,j}=1)=Pr\,(\phi_{i,j}=1)=\frac{d_\Phi}{N}\,,\ Pr\,(\phi_{i,j}=0)=1-\frac{2\,d_\Phi}{N}$$

$$Pr\,(m_{i,j}=\gamma)=\frac{1}{p}\quad \gamma\epsilon\,[-\frac{p}{2}\,,\frac{p}{2}\,]\,,\ i,j=0,1,2,\ \dots\,,15$$

Assume that all $f_{i,\alpha}$, $g_{j,\beta}$ and $\phi_{k,\delta}$ are pairwise independent random variables.

For $\alpha,\beta,\delta=0,1,\dots,N-1$ and $i,j,k=0,1,2,\dots,15$ and $\gamma=-\frac{p-1}{2},\dots,\frac{p-1}{2}$

$$Pr\,(f_{i.\alpha}\,.g_{j,\beta}.\,\phi_{k.\delta}=\mp\,1)=\frac{8d_f d_g d_\Phi}{N^3}$$

$$Pr\,(f_{i.\alpha}\,.g_{j,\beta}.\,\phi_{k.\delta}=0\,)=1-\frac{8d_f d_g d_\Phi}{N^3}$$

$$Pr\,(f_{i.\alpha}\,.f_{j.\beta}.\,m_{k.\delta}=\gamma)=\frac{4{d_f}^2}{pN^2}\,,\ (i\neq j\vee\alpha\neq\beta)\wedge(\gamma\neq 0)$$

$$Pr\,(f_{i.\alpha}\,.f_{i.\beta}.\,m_{k.\delta}=\gamma)=\frac{2d_f(d_f-1)+2{d_f}^2}{pN(N-1)}\quad(\alpha\neq\beta)\wedge(\gamma\neq 0)$$

Under the above assumptions, we get

$$E\,(f_{i.\alpha}\,.g_{j,\beta}.\,\phi_{k.\delta})=0\,,\ E\,(f_{i.\alpha}\,.f_{j.\beta}.\,m_{k.\delta})=0$$

$$Var\,(f_{i.\alpha}\,.g_{j,\beta}.\,\phi_{k.\delta})=\frac{8d_f d_g d_\Phi}{N^3}\,,\ Var\,(f_{i.\alpha}\,.f_{j.\beta}.\,m_{k.\delta})=\frac{{d_f}^2(P-1)(P+1)}{3N^2},$$

$$Var\,({f_{i.s}}^2 m_{k.u})=\frac{d_f(p-1)(p+1)}{6N}$$

Assume that the covariance of $f_{i.\alpha}$ and $f_{i.\beta}$ are negligible we get the final result

$$Var\,((f_{i.\alpha}\,.g_{j,\beta}.\,\phi_{k.\delta})_y)=Var\,(\sum\sum_{\alpha+\beta+\delta\equiv y\ (mod\ N)} f_{i.\alpha}g_{j.\beta}\,\phi_{k.\delta})=\frac{8d_f d_g d_\Phi}{N}$$

$$Var\left((f_i . f_j . m_k)_y\right) = Var\left(\sum\sum_{\alpha+\beta+\delta\equiv y\ (mod\ N)} f_{i.s} f_{j.t}\ m_{k.\delta}\right) = \frac{{d_f}^2(p-1)(p+1)}{3}$$

$$Var\left(({f_i}^2 m_k)_y\right) = Var\left(\sum\sum_{\alpha+\beta+\delta\equiv y\ (mod\ N)} f_{i.s} f_{i.t}\ m_{k.\delta}\right) \approx$$

$$\frac{{d_f}^2(N-1)(P-1)(p+1)}{3N} + \frac{d_f(p-1)(p+1)}{6}$$

Now, obtain

$$Var\left(a_{0,k}\right) \approx \frac{2048p^2 d_f d_g d_\Phi}{N} + 20{d_f}^2(p-1)(p+1) +$$

$$\frac{16{d_f}^2(N-1)(P-1)(p+1)}{3N} + \frac{8d_f(p-1)(p+1)}{3}$$

In the similar method, we obtain

$$Var\left(a_{0,k}\right) = Var\left(a_{1,k}\right) = Var\left(a_{2,k}\right) = \ldots = Var\left(a_{15,k}\right)$$

$$\approx \frac{2048p^2 d_f d_g d_\Phi}{N} + 20{d_f}^2(p-1)(p+1) + \frac{16{d_f}^2(N-1)(P-1)(p+1)}{3N} +$$

$$\frac{8d_f(p-1)(p+1)}{3}$$

When the probability of all coefficients a_{ik} belong to $[\frac{-q+1}{2} \ldots \frac{q+1}{2}]$, the successful decryption.

With the supposition that $a_{ik}s$ are independent random variable and have normal distribution $N(0, \sigma^2)$ we obtain

$$Pr\left(\left|a_{i,k}\right| \leq \frac{q-1}{2}\right) = Pr\left(-\frac{q-1}{2} \leq a_{i,k} \leq \frac{q-1}{2}\right) = 2N\left(\frac{q-1}{2\sigma}\right),$$

where σ

=

$$\sqrt{\frac{2048p^2 d_f d_g d_\Phi}{N} + 20{d_f}^2(p-1)(p+1) + \frac{16{d_f}^2(N-1)(P-1)(p+1)}{3N} + \frac{8d_f(p-1)(p+1)}{3}}$$

,

the probability for successful decryption in HXDTRU may be calculated by the following tow observation

i) The probability for any one of the message $M_0, M_1, \dots, M_{15}$ to be successfully decrypted is

$$(2N\left(\frac{q-1}{2\sigma}\right) - 1)^N$$

ii) The probability all the message $M_0, M_1, \dots, M_{15}$ to be successfully decrypt

$$(2N\left(\frac{q-1}{2\sigma}\right) - 1)^{16}.$$

3.6. BRUTE FORCE ATTACK

In HXDTRU an attacker who knows the public parameters ,as well as, the public key $H=F_q \circ G$ have to attempt all maybe hexadecnion $F \epsilon L_f$ and check to see if $F \circ H$ turns into hexadecnion with small coefficients until find private key ,the size of the subset L_f is calculated as follows:

$$|L_f| = \left(\frac{N!}{(d_f!)^2 (N-2d_f)!}\right)^{16}.$$

An attacker can use another way by try all possible hexadecnion $G \epsilon L_g$ and check if $G \circ H^{-1} (mod\ q)$ has small coefficients.
Similarly, the attacker can search in space L_ϕ to get the message original from the ciphertext and this search must be done in the order of the space L_ϕ which the size is calculated as follows:

$$|L_\phi| = \left(\frac{N!}{(d_\phi!)^2 (N-2d_\phi)!}\right)^{16}.$$

3.7. CONCLUSION

In this paper, HXDTRU cryptosystem based on Hexadecnion algebra which is a non-commutative, non-associative and alternative. The speed of HXDTRU is slower than NTRU with same parameter but we

can exceed that problem by lowering of N. The HXDTRU is a multi-dimension cryptosystem which encrypted message can consist from sixteen messages from a single origin or sixteen independent messages from sixteen different origins and this property can be important in some applications as electronic voting. When the coefficients of y_1, y_2, …, y_{15} are equal to zero, HXDTRU

converts to NTRU. The security of HXDTRU with dimension N has same to that of NTRU with dimension 16N.

REFERENCES

1- J. Hoffstein, J. Pipher, and J. Silverman, "NTRU: A ring based public key cryptosystem " in Lecture Notes in Computer science. Springer Verlag, 1998, p.p. 267-288.

2- M. Coglianese and B.M. Goi, "MaTRU: A new NTRU based cryptosystem", Springer Verlag Berlin Heidelberg, 2005, p.p. 232-243.

3- Malecian E., Zakerolhsooeini A., Mashatan A. " QTRU: a lattice attack resistant version of NTRU PCKS based on quaternion algebra. Available from the cryptology eprint Archive: http://eprint.Iacr. org/2009/386.pdf. Accessed Sep. 2012.

4- Malecian E., Zakerolhsooeini A., " OTRU: A Non Associative and high Speed Public Key Cryptosystem ", IEEE Computer Society, 2010, p.p.83-90.

5- Malecian E., Zakerolhsooeini A., "NTRU- Like Public Key Cryptosystems beyond Dedekind Domain up to Alternative Algebra ", Springer Verlag Berlin Heidelberg, 2010, p.p. 25-41.

6- Nadia. ALs. Mustafa. S., Ali.A.M, "An improved NTRU Cryptosystem via Commutative Quaternions Algebra", Int'l Conf. Security and Management SAM'15, 2015, P.P.198-203.

7- M. Nevins, C. Karimianpour, and A. Miri. "Ntru over ring beyond z" accepted to Designs, Codes and Cryptography, May 2009.

8- D. Coppersmith and A. Shamir, "Lattice attacks on NTRU" Springer Verlag Berlin Heidelberg, 1997, p.p. 52-61.

9- J. Hoffstein, J. Pipher, and J. Silverman, "An Introduction to Mathematical cryptography" ser, Science+BusinessMedia, LLC. Springe, 2008.

5 Appendix

Table 1: The Multiplication Table

*	1	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8	y_9	y_{10}	y_{11}	y_{12}	y_{13}	y_{14}	y_{15}
1	1	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8	y_9	y_{10}	y_{11}	y_{12}	y_{13}	y_{14}	y_{15}
y_1	y_1	-1	y_3	$-y_2$	y_5	$-y_4$	$-y_7$	y_6	y_9	$-y_8$	y_{11}	$-y_{10}$	y_{13}	$-y_{12}$	y_{15}	$-y_{14}$
y_2	y_2	$-y_3$	-1	y_1	y_6	y_7	$-y_4$	$-y_5$	y_{10}	$-y_{11}$	$-y_8$	y_9	y_{14}	$-y_{15}$	y_{12}	y_{13}
y_3	y_3	y_2	$-y_1$	-1	y_7	$-y_6$	y_5	$-y_4$	y_{11}	y_{10}	$-y_9$	$-y_8$	y_{15}	y_{14}	$-y_{13}$	$-y_{12}$
y_4	y_4	$-y_5$	$-y_6$	$-y_7$	-1	y_1	y_2	y_3	y_{12}	$-y_{13}$	$-y_{14}$	$-y_{15}$	$-y_8$	y_9	y_{10}	y_{11}
y_5	y_5	y_4	$-y_7$	y_6	$-y_1$	-1	$-y_3$	y_2	y_{13}	y_{12}	$-y_{15}$	y_{14}	$-y_9$	$-y_8$	y_{11}	$-y_{10}$
y_6	y_6	y_7	y_4	$-y_5$	$-y_2$	y_3	-1	$-y_1$	y_{14}	y_{15}	y_{12}	$-y_{13}$	$-y_{10}$	$-y_{11}$	$-y_8$	y_9
y_7	y_7	$-y_6$	y_5	y_4	$-y_3$	$-y_2$	y_1	-1	y_{15}	$-y_{14}$	y_{13}	y_{12}	$-y_{11}$	y_{10}	$-y_9$	$-y_8$
y_8	y_8	$-y_9$	$-y_{10}$	$-y_{11}$	$-y_{12}$	$-y_{13}$	$-y_{14}$	$-y_{15}$	-1	y_1	y_2	y_3	y_4	y_5	y_6	y_7
y_9	y_9	y_8	y_{11}	$-y_{10}$	y_{13}	$-y_{12}$	$-y_{15}$	y_{14}	$-y_1$	-1	y_3	$-y_2$	y_5	$-y_4$	y_7	$-y_6$
y_{10}	y_{10}	$-y_{11}$	y_8	y_9	y_{14}	y_{15}	$-y_{12}$	$-y_{13}$	$-y_2$	$-y_3$	-1	y_1	y_6	$-y_7$	$-y_4$	y_5
y_{11}	y_{11}	y_{10}	$-y_9$	y_8	y_{15}	$-y_{14}$	y_{13}	$-y_{12}$	$-y_3$	y_2	$-y_1$	-1	y_7	y_6	$-y_5$	$-y_4$
y_{12}	y_{12}	$-y_{13}$	$-y_{14}$	$-y_{15}$	y_8	y_9	y_{10}	y_{11}	$-y_4$	$-y_5$	$-y_6$	$-y_7$	-1	y_1	y_2	y_3
y_{13}	y_{13}	y_{12}	y_{15}	$-y_{14}$	$-y_9$	y_8	y_{11}	$-y_{10}$	$-y_5$	y_4	y_7	$-y_6$	$-y_1$	-1	y_3	$-y_2$
y_{14}	y_{14}	$-y_{15}$	y_{12}	y_{13}	$-y_{10}$	$-y_{11}$	y_8	y_9	$-y_6$	$-y_7$	y_4	y_5	$-y_2$	$-y_3$	-1	y_1
y_{15}	y_{15}	y_{14}	y_{13}	y_{12}	$-y_{11}$	y_{10}	$-y_9$	y_8	$-y_7$	y_6	$-y_5$	y_4	$-y_3$	y_2	$-y_1$	-1

$H_{16Nx16N}$ =

$$\begin{bmatrix}
H_0 & H_1 & H_2 & H_3 & H_4 & H_5 & H_6 & H_7 & H_8 & H_9 & H_{10} & H_{11} & H_{12} & H_{13} & H_{14} & H_{15} \\
-H_1 & H_0 & -H_3 & H_2 & -H_5 & H_4 & H_7 & -H_6 & -H_9 & H_8 & -H_{11} & H_{10} & -H_{13} & H_{12} & -H_{15} & H_{14} \\
-H_2 & -H_3 & H_0 & -H_1 & -H_6 & -H_7 & H_4 & H_5 & -H_{10} & H_{11} & H_8 & -H_9 & -H_{14} & H_{15} & H_{12} & -H_{13} \\
-H_3 & -H_2 & H_1 & H_0 & -H_7 & H_6 & -H_5 & H_4 & -H_{11} & -H_{10} & H_9 & H_8 & -H_{15} & -H_{14} & H_{13} & H_{12} \\
-H_4 & H_5 & H_6 & H_7 & H_0 & H_1 & -H_2 & -H_3 & -H_{12} & H_{13} & H_{14} & H_{15} & H_8 & -H_9 & -H_{10} & -H_{11} \\
-H_5 & -H_4 & H_7 & -H_6 & H_1 & H_0 & H_3 & -H_2 & -H_{13} & -H_{12} & H_{15} & -H_{14} & H_9 & H_8 & -H_{11} & H_{10} \\
-H_6 & -H_7 & -H_4 & H_5 & H_2 & -H_3 & H_0 & H_1 & -H_{14} & -H_{15} & -H_{12} & -H_{13} & H_{10} & H_{11} & H_8 & -H_9 \\
-H_7 & H_6 & -H_5 & -H_4 & -H_3 & H_2 & -H_1 & H_0 & -H_{15} & H_{14} & -H_{13} & -H_{12} & H_{11} & -H_{10} & H_9 & H_8 \\
-H_8 & H_9 & H_{10} & H_{11} & H_{12} & H_{13} & H_{14} & H_{15} & H_{10} & -H_1 & -H_2 & -H_3 & -H_4 & -H_5 & -H_6 & -H_8 \\
-H_9 & -H_8 & -H_{11} & H_{10} & -H_{13} & H_{12} & H_{15} & -H_{14} & H_1 & H_0 & -H_3 & H_2 & -H_5 & H_4 & -H_7 & H_6 \\
-H_{10} & H_{11} & -H_8 & -H_9 & -H_{14} & -H_{15} & H_{12} & H_{13} & H_2 & H_3 & H_0 & -H_1 & -H_6 & H_7 & H_4 & -H_5 \\
-H_{11} & -H_{10} & H_9 & -H_8 & -H_{15} & H_{14} & -H_{13} & H_{12} & H_3 & -H_2 & H_1 & H_0 & -H_7 & -H_6 & H_5 & H_4 \\
-H_{12} & H_{13} & H_{14} & H_{15} & -H_8 & -H_9 & -H_{10} & -H_{11} & H_4 & H_5 & H_6 & H_7 & H_0 & -H_1 & -H_2 & -H_3 \\
-H_{13} & -H_{12} & -H_{15} & H_{14} & H_9 & -H_8 & -H_{11} & H_{10} & H_5 & -H_4 & H_7 & H_6 & H_1 & H_0 & -H_3 & H_2 \\
-H_{14} & H_{15} & -H_{12} & -H_{13} & H_{10} & H_{11} & -H_8 & -H_9 & H_6 & H_7 & -H_4 & -H_5 & H_2 & H_3 & H_0 & -H_1 \\
-H_{15} & -H_{14} & -H_{13} & -H_{12} & H_{11} & -H_{10} & H_9 & -H_8 & H_7 & -H_6 & H_5 & -H_4 & H_3 & -H_2 & H_1 & H_0
\end{bmatrix}$$