Malaysian Journal of Mathematical Sciences 11(S) August: 29 - 43 (2017)
Special Issue: The 5th International Cryptology and Information Security Conference (New Ideas in Cryptology)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

A New Alternative to NTRU cryptosystem based on Highly Dimensional Algebra with Dense Lattice Structure

Al-Saidi, N. M. G.[1] and **Yassein, H. R** *[2]

[1] *Department of Applied Sciences, University of Technology, Iraq*
[2] *Department of Mathematics, College of Education, Al-Qadisiyah University, Iraq*

E-mail: hassan.yaseen@qu.edu.iq
**Corresponding author*

ABSTRACT

NTRU public key is a cryptosystem with hard mathematical structure and short key size relies in its security on the hardness of lattice based cryptosystems. Its smallest key size made it highly performed system and grant it an advantageous over other numbers theoretical based cryptosystems. Due to Shamir's conclusion about the dnon commutative computations in encryption and decryption processes of any cryptosystem leads to turn it into a highly lattice attack resist system. In this paper, a new alternative non associative, non-commutative multidimensional system is proposed under the same principle of NTRU cryptosystem. It is called HXDTRU, where its operations taken place in a specially designed high dimensional algebra called hexadecnion algebra. The proposed system is implemented, and its security and efficiency are analyzed.

Keywords: NTRU, HXDTRU, hexadecnion algebra, lattice hexadecnion algebra.

1. Introduction

With the developing information technology, a new secure and highly performed protection mechanism is of high and continuous demand. In 1996, a new public key cryptosystem called NTRU (number theory research unit) was founded by three mathematicians Jeffery Hoffstein, Joseph H. Silverman and Jill Piper (Hoffstein et al., 1998). Its importance was granted due to its hard mathematical structure with short key size, where its operations are taken place in a truncated polynomial ring of degree $N-1$ with integer coefficients in $Z[x]/(x^N-1)$. It is the first public key cryptosystem that did not depend on factorization (as RSA cryptosystem) or discrete algorithmic problems (as EL Gamal cryptosystem and ECC cryptosystem) (Blömer and May, 2001, Hoffstein et al., 2008). In comparison with RSA cryptosystem and ECC cryptosystems, NTRU is faster and has significantly smaller keys.

Based on the same construction structure of NTRU, many good alternatives to it were introduced since that time. They were designed to improve its performance by replacing the original polynomial ring over Z (Nevins et al., 2010), by many variant polynomial rings other than Z. All of them aimed to design of NTRU like cryptosystem with short key size and secure against lattice attack (Coppersmith and Shamir, 1997). Some of these attempts are presented as follows:

In 2002, P.Gaborit et al., introduced CTRU based on the ring of the polynomials in one variable over a finite field (Gaborit et al., 2002). In 2005, M.Coglianese and B.Goi, presented a new cryptosystem called MaTRU by using ring of $k \times k$ matrices of polynomials of order n (Coglianese and Goi, 2005). In 2009, Malekian et al., introduced QTRU cryptosystem based on quaternion algebra (Malekian et al., 2009). They also introduced OTRU cryptosystem based on octonions algebra (Malekian and Zakerolhosseini, 2010a,b). In this year also, Vats introduced NNRU, a new variant of NTRU with non-commutative operations over the non-commutative ring $\mathcal{M} = M_k(Z[x])/(X^n - I_{k\times k})$ (Vats, 2009). He showed that his proposed system is completely secure against lattice attack. In 2011, K.Jarvis presented ETRU based on Eisenstein integers (Jarvis, 2011, Jarvis and Nevins, 2015). In 2015, Majeed introduced CQTRU cryptosystem based on commutative quaternions algebra (Alsaidi et al., 2015, Majeed, 2015). In 2015, Atani et al. introduced EEH, a GGH like public key system based on Eisenstein integers $Z[\zeta_3]$, where $Z[\zeta_3]$ is a primitive cube root of unity. They demonstrated an improvement of their proposed system has an improvement over GGH in terms of security and efficiency (Ebrahimi Atani et al., 2016). In 2016, Thakur and Tripathi introduced BTRU, a new like NTRU cryptosystem, that replaces Z by a ring of polynomial with one variable α over a rational field. They conveyed faster than NTRU (Thakur and Tripathi, 2016).

In this paper, we presented a new multidimensional public key cryptosystem HXDTRU based on Hexadecnion algebra. This multidimensional algebra is used to serve in constructing of a highly performed public key system which is highly secured with small key size. This system was first introduced in Cryptology 2016 by Yassein and Alsaidi (Yassein and AlSaidi, 2016), but in this work, it is extended with more details.

In addition to this introductory section, the rest of this paper is structured as follows; Section 2 is devoted to introduce the mathematical description of the Hexadecnion algebra with its algebraic structure. The proposed HXDTRU cryptosystem is described in Section 3. The proof of successful decryption is presented in this section too. The security analysis of the proposed system is investigated in Section 4, and the paper is finally concluded in Section 5.

2. 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.

2.1 HEXADECNION ALGEBRA (HD)

In this section, we define hexadecnion algebra and its properties. It is a vector space of sixteen dimension over the real number R defined as follows: HD= $\{w|w = r_0 + \sum_{i=1}^{15} r_i x_i | r_0, r_1, \cdots, r_{15} \in R\}$
where $\beta = \{1, x_1, x_2, \cdots, x_{15}\}$ form the basis of the hexadecnion algebra and r_i s are scalars in a set of real number. Let w_1 , w_2 $\in$HD such that: $w_1 = r_0+r_1x_1+r_2x_2+...+r_{14}x_{14}+r_{15}x_{15}$, $w_2 = r'_0+r'_1x_1+r'_2x_2+...+r'_{14}x_{14}+r'_{15}x_{15}$
The addition of w_1 and w_2 is found by adding their corresponding coefficients such that; $w_1 + w_2 = (r_0 + r'_0) + (r_1 + r'_1)x_1 + (r_2 + r'_2)x_2 + \cdots + (r_{14} + r'_{14})x_{14} + (r_{15} + r'_{15})x_{15}$.
The multiplication table shown in Table 1 is given to define the multiplication between w_i and w_j, where w_i and w_j $\in$HD, and $x_i^2 = -1, x_i x_j = -x_j x_i, i \neq j$, and $i, j = 1, 2, \cdots, 15$. The multiplication is non commutative and non associative but it is alternative.

*	1	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}
1	1	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}
x_1	x_1	-1	x_3	$-x_2$	x_5	$-x_4$	$-x_7$	x_6	x_9	$-x_8$	x_{11}	$-x_{10}$	x_{13}	$-x_{12}$	x_{15}	$-x_{14}$
x_2	x_2	$-x_3$	-1	x_1	x_6	x_7	$-x_4$	$-x_5$	x_{10}	$-x_{11}$	$-x_8$	x_9	x_{14}	$-x_{15}$	$-x_{12}$	x_{11}
x_3	x_3	x_2	$-x_1$	-1	x_7	$-x_6$	x_5	$-x_4$	x_{11}	x_{10}	$-x_9$	$-x_8$	x_{15}	x_{14}	$-x_{13}$	$-x_{12}$
x_4	x_4	$-x_5$	$-x_6$	$-x_7$	-1	x_1	x_2	x_3	x_{12}	$-x_{13}$	$-x_{14}$	$-x_{15}$	x_8	x_9	x_{10}	x_{11}
x_5	x_5	x_4	$-x_7$	x_6	$-x_1$	-1	$-x_3$	x_2	x_{13}	x_{12}	$-x_{15}$	x_{14}	$-x_9$	$-x_8$	x_{11}	$-x_{10}$
x_6	x_6	x_7	x_4	$-x_5$	$-x_2$	x_3	-1	$-x_1$	x_{14}	x_{15}	x_{12}	$-x_{13}$	$-x_{10}$	$-x_{11}$	$-x_8$	x_9
x_7	x_7	$-x_6$	x_5	x_4	$-x_3$	$-x_2$	x_1	-1	x_{15}	$-x_{14}$	x_{13}	x_{12}	$-x_{11}$	x_{10}	$-x_9$	$-x_8$
x_8	x_8	$-x_9$	$-x_{10}$	$-x_{11}$	$-x_{12}$	$-x_{13}$	$-x_{14}$	$-x_{15}$	-1	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_9	x_9	x_8	x_{11}	$-x_{10}$	x_{13}	$-x_{12}$	x_{15}	x_{14}	$-x_1$	-1	x_3	$-x_2$	x_5	$-x_4$	x_7	$-x_6$
x_{10}	x_{10}	$-x_{11}$	x_8	x_9	x_{14}	x_{15}	$-x_{12}$	$-x_{13}$	$-x_2$	$-x_3$	-1	x_1	x_6	$-x_7$	$-x_4$	x_5
x_{11}	x_{11}	x_{10}	$-x_9$	x_8	x_{15}	$-x_{14}$	x_{13}	$-x_{12}$	$-x_3$	x_2	$-x_1$	-1	x_7	x_6	$-x_5$	$-x_4$
x_{12}	x_{12}	$-x_{13}$	$-x_{14}$	$-x_{15}$	x_8	x_9	x_{10}	x_{11}	$-x_4$	$-x_5$	$-x_6$	$-x_7$	-1	x_1	x_2	x_3
x_{13}	x_{13}	x_{12}	x_{15}	$-x_{14}$	$-x_9$	x_8	x_{11}	$-x_{10}$	$-x_5$	x_4	x_7	$-x_6$	$-x_1$	-1	x_3	$-x_2$
x_{14}	x_{14}	$-x_{15}$	x_{12}	x_{13}	$-x_{10}$	$-x_{11}$	x_8	x_9	$-x_6$	$-x_7$	x_4	x_5	$-x_2$	$-x_3$	-1	x_1
x_{15}	x_{15}	x_{14}	x_{13}	x_{12}	$-x_{11}$	x_{10}	$-x_9$	x_8	$-x_7$	x_6	$-x_5$	x_4	x_3	x_2	$-x_1$	-1

$H_{16NX16N} =$

$$\left|\begin{array}{cccccccccccccccc}
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_{15} & -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_0 & -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{array}\right|$$

Table 1: The Multiplication Table

For any scalar α, we have,

$$\alpha w = \alpha(r_0 + r_1x_1 + r_2x_2 + \cdots + r_{14}x_{14} + r_{15}x_{15})$$

$$= \alpha r_0 + \alpha r_1x_1 + \alpha r_2x_2 + \cdots + \alpha r_{14}x_{14} + \alpha r_{15}x_{15}$$

The conjugate of a hexadecnion $w = r_0 + \sum_{i=1}^{15} r_ix_i$ is defined as follows $\overline{w} = r_0 - \sum_{i=1}^{15} r_ix_i$ and the square norm is given by $N(w) = w\overline{w} = \sum_{i=1}^{15} {r_i}^2$. The multiplicative inverse of any non zero element w in HD is given by

$$w^{-1} = N(w)^{-1}\overline{w}$$

.

2.2 ALGEBRAIC STRUCTURE OF HXDTRU

Let K be any arbitrary finite ring of characteristic is not equal to 2, we define the hexadecnion algebra Ψ over K as follows:

$$\Psi = \{r_0 + \sum_{i=1}^{15} r_ix_i | r_0, r_1, \cdots, r_{15} \in K\}$$

Where the multiplication, the multiplicative inverse and the norm has the same properties as the real hexadecnion algebra HD. Note that Ψ is a non associative and since the usual multiplication of matrices is associative then it does not have any matrix representation. Now, consider the truncated polynomial rings $K_p(x) = (Z/pZ)[x]/(x^N - 1)$ and $K_q(x) = (Z/qZ)[x]/(x^N - 1)$. We define three hexadecnion algebras Ψ, Ψ_p and Ψ_q as follows:

$$\Psi = \{f_0 + \sum_{i=1}^{15} f_i(x)x_i | f_0, f_1, \ldots, f_{15} \in K\}$$

$$\Psi_p = \{f_0 + \sum_{i=1}^{15} f_i(x)x_i | f_0, f_1, \ldots, f_{15} \in K_p\}$$

$$\Psi_q = \{f_0 + \sum_{i=1}^{15} f_i(x)x_i | f_0, f_1, \ldots, f_{15} \in K_q\}$$

Now, let Φ_1 , $\Phi_2 \in \Psi_p$ or Ψ_q such that;

$$\Phi_1 = f_0(x) + f_1(x)x_1 + f_2(x)x_2 + \cdots + f_{14}(x)x_{14} + f_{15}(x)x_{15}$$

$$\Phi_2 = g_0(x) + g_1(x)x_1 + g_2(x)x_2 + \cdots + g_{14}(x)x_{14} + g_{15}(x)x_{15}$$

where f_i , $g_i \in K_p$ or K_q.
The addition of $\Phi_1$and Φ_2 is done by adding their corresponding coefficients including $16N$, *mod p* or *mod q*

$$\begin{aligned}\Phi_1 + \Phi_2 = f_0(x) + g_0(x) + (f_1(x) + g_1(x))x_1 + (f_2(x) + g_2(x))x_2 + \cdots +\\ (f_{14}(x) + g_{14}(x))x_{14} + (f_{15}(x) + g_{15}(x))x_{15}\end{aligned}$$

The multiplication of Φ_1 and Φ_2 is defined as follows:

$$\begin{aligned}\Phi_1 \circ \Phi_2 = (f_0 * g_0 - f_1 * g_1 - f_2 * g_2 - f_3 * g_3 - f_4 * g_4 - f_5 * g_5 - f_6 * g_6 - f_7 * g_7 - f_8 * g_8\\ - f_9 * g_9 - f_{10} * g_{10} - f_{11} * g_{11} - f_{12} * g_{12} - f_{13} * g_{13} - f_{14} * g_{14} - f_{15} * g_{15})\\ +(f_0 * g_1 + f_1 * g_0 + f_2 * g_3 + f_3 * g_5 + f_4 * g_5 - f_5 * g_4 - f_6 * g_7 + f_7 * g_6 + f_8 * g_9 - f_9 * g_8 + f_{10} * g_{11}\\ - f_{11} * g_{10} + f_{12} * g_{13} - f_{13} * g_{12} + f_{14} * g_{15} - f_{15} * g_{14})x_1 + \cdots + (f_0 * g_{15} + f_1 * g_{14}\\ - f_2 * g_1 3 + f_3 * g_{12} - f_4 * g_{11} - f_5 * g_{10} + f_6 * g_9 + f_7 * g_8 - f_8 * g_7 - f_9 * g_6\\ + f_{10} * g_5 + f_{11} * g_4 - f_{12} * g_3 + f_{13} * g_2 - f_{14} * g_1 + f_{15} * g_0)x_{15}\end{aligned}$$

such that $*$ is a convolution product.

2.3 The PROPOSED 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. The subsets $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_m$ and $\mathcal{L}_\Phi \subset \Psi$ are defined as follows:

$\mathcal{L}_f = \{f_0(x) + f_1(x)x_1 + f_2(x)x_2 + \ldots + f_{14}(x)x_{14} + f_{15}(x)x_{15} \in \Psi |\ f_i \in K$ has d_f coefficients equal to $+1$, $(d_f - 1)$ equal to -1,the rest are 0 $\}$,
$\mathcal{L}_g = \{g_0(x) + g_1(x)x_1 + g_2(x)x_2 + \ldots + g_{14}(x)x_{14} + g_{15}(x)x_{15} \in \Psi | g_i \in K$ has d_g coefficients equal to $+1$, d_g equal to -1,the rest are 0 $\}$,
$\mathcal{L}_m = \{m_0(x) + m_1(x)x_1 + m_2(x)x_2 + \ldots + m_{14}(x)x_{14} + m_{15}(x)x_{15} \in \Psi |$ coefficients of $m_i(x) \in \Psi$ are chosen modulo p, between $-p/2$ and $p/2\}$ and
$\mathcal{L}_\Phi = \{\Phi_0(x) + \Phi_1(x)x_1 + \Phi_2(x)x_2 + \ldots + \Phi_{14}(x)x_{14} + \Phi_{15}(x)x_{15} \in \Psi | \Phi_i \in k$ 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 to those in NTRU. Then HXDTRU can be described through three phases:

a) KEY GENERATION

To generate the public key and the private key, two small norm F and $G \in \Psi$ are randomly generated, such that:

$$F = f_0(x) + f_1(x)x_1 + f_2(x)x_2 + \cdots + f_{14}(x)x_{14} + f_{15}(x)x_{15},$$

$$f_0, f_1, f_2, \cdots, f_{14}, f_{15} \in \mathcal{L}_f$$

$$G = g_0(x) + g_1(x)x_1 + g_2(x)x_2 + \cdots + g_{14}(x)x_{14} + g_{15}(x)x_{15},$$

$$g_0, g_1, g_2, \cdots, g_{14}, g_{15} \in \mathcal{L}_g$$

Here, F must have multiplication inverses over Ψ_p and Ψ_q. If F is not invertible (when the inverse of $\sum_{i=1}^{15} f_i^2(x)$, is not existed in K_p or K_q) then a new hexadecnion F should be chosen. The inverses of F are denoted by F_P and F_q over algebra Ψ_p and Ψ_q respectively. Now, the public key is calculated as follows:

$H = F_q \cdot G \in \Psi_q$
$= (f_{q_0}(x) + f_{q_1}(x)x_1 + f_{q_2}(x)x_2 + \cdots + f_{q_{14}}(x)x_{14} + f_{q_{15}}(x)x_{15}) \cdot (g_0(x) + g_1(x)x_1 + g_2(x)x_2 + \cdots + g_{14}(x)x_{14} + g_{15}(x)x_{15})$
$= f_{q_0}*g_0 - f_{q_1}*g_1 - f_{q_2}*g_2 - f_{q_3}*g_3 - f_{q_4}*g_4 - f_{q_5}*g_5 - f_{q_6}*g_6 - f_{q_7}*g_7 - f_{q_8}*g_8 - f_{q_9}*g_9 - f_{q_{10}}*g_{10} - f_{q_{11}}*g_{11} - f_{q_{12}}*g_{12} - f_{q_{13}}*g_{13} - f_{q_{14}}*g_{14} - f_{q_{15}}*g_{15}$
$+(f_{q_0}*g_1 - f_{q_1}*g_0 - f_{q_2}*g_3 - f_{q_3}*g_2 + f_{q_4}*g_5 - f_{q_5}*g_4 - f_{q_6}*g_7 + f_{q_7}*g_6 + f_{q_8}*g_9 - f_{q_9}*g_8 + f_{q_{10}}*g_{11} - f_{q_{11}}*g_{10} + f_{q_{12}}*g_{13} - f_{q_{13}}*g_{12} + f_{q_{14}}*g_{15} - f_{q_{15}}*g_{14}) \cdot x_1$
$\vdots$
$+(f_{q_0}*g_{14} - f_{q_1}*g_{15} + f_{q_2}*g_{12} + f_{q_3}*g_{14} - f_{q_4}*g_{10} + f_{q_5}*g_{11} + f_{q_6}*g_8 - f_{q_7}*g_9 - f_{q_8}*g_6 + f_{q_9}*g_7 + f_{q_{10}}*g_4 - f_{q_{11}}*g_5 - f_{q_{12}}*g_2 - f_{q_{13}}*g_3 + f_{q_{14}}*g_0 + f_{q_{15}}*g_1) \cdot x_{14}$
$+(f_{q_0}*g_{15} + f_{q_1}*g_{14} - f_{q_2}*g_{13} + f_{q_3}*g_{12} - f_{q_4}*g_{11} - f_{q_5}*g_{10} + f_{q_6}*g_9 + f_{q_7}*g_8 - f_{q_8}*g_7 - f_{q_9}*g_6 + f_{q_{10}}*g_5 + f_{q_{11}}*g_4 - f_{q_{12}}*g_3 + f_{q_{13}}*g_2 - f_{q_{14}}*g_1 + f_{q_{15}}*g_0) \cdot x_{15}$
$= h_0(x) + h_1(x)x_1 + h_2(x)x_2 + ... + h_{14}(x)x_{14} + h_{15}(x)x_{15}$. F, F_P and F_q must be kept secret in order to be used in decryption phase. When the same parameters N, p and q are used in NTRU and HXDTRU, the key generation phase of NTRU is faster than that of HXDTRU, but the computational time of this phase depends on the computation of the inverses which is greater than the time of this phase in traditional NTRU with the same parameters.

b) ENYCRYPTION

At the beginning of the encryption process, the message M should be converted to the form, $M = m_0(x) + m_1(x)x_1 + m_2(x)x_2 + \cdots + m_{14}(x)x_{14} + m_{15}(x)x_{15}$

where $m_i(x) \in \mathcal{L}_m$, $i = 0, 1, \cdots, 15$ and Φ is another small hexadecnion that is randomly chosen. It computes the encrypted message M as follows:

$$E = pH \circ \Phi + M \in \Psi_q,$$

the encryption in HXDTRU needs one hexadecnion multiplication including 256 convolution multiplication and 16 polynomial additions.

c) DECRYPTION

After receiving the encrypted message E, the receiver decrypt the message through the following steps: At the first, E is multiplied by the private key F on the left and then on right as follows:

$A = (F \circ E) \circ F \in \Psi_q$

$= (F \circ (pH \circ \Phi + M)) \circ F \circ \Psi_q$

$= p(F \circ (H \circ \Phi)) \circ F + (F \circ M) \circ F \in \Psi_q$

$= p(F \circ H) \circ (\Phi \circ F) + (F \circ M) \circ F \in \Psi_q$ (by moufang identity)

$= p(F \circ (F_q \circ G)) \circ (\Phi \circ F) + (F \circ M) \circ F \in \Psi_q$

$= pG \circ (\Phi \circ F) + (F \circ M) \circ F \in \Psi_q$

The coefficients of sixteen polynomial in $pG \circ (\Phi \circ F) + (F \circ M) \circ F$ must lie in the intervals $(-q/2, q/2]$ and the last reduction mod q does not required. When the term $(\Phi \circ F) + (F \circ M) \circ F$ is reduced mod p, the term $F \circ M \pmod{p}$ remains and $pG \circ (\Phi \circ F)$ vanishes.

Hence, $A = F \circ M \in \Psi_p$. Multiplying $A = F \circ M \pmod{p}$ by F_p, the message $M = F_p \circ A$ is constructed and its coefficients are adjusted to lying in the interval $(-p/2, p/2]$.

2.4 SUCCESSFUL DECRYPTION

If all hexadecnion coefficients of $pG \circ (\Phi \circ F) + (F \circ M) \circ F$ lies within the interval $(-q/2, q/2]$ then the probability of successful decryption is increased, and can be computed in the following proposition.

Proposition 1: $Pr(| \, a_{i,k} \, | \leq \frac{q-1}{2}) = Pr(-\frac{q-1}{2} \leq a_{i,k} \leq \frac{q-1}{2}) = 2\mathcal{N}\frac{q-1}{2\sigma}$, where $\mathcal{N}$ denotes the normal distribution, $i, k = 0, 1, 2, \cdots, 15$ and $\sigma = \sqrt{\frac{2048p^2 d_f d_g d_\Phi}{N} + 20d_{f^2}(p-1)(p+1) + \frac{16d_{f^2}(N-1)(P-1)(p+1)}{3N} + \frac{8d_f(p-1)(p+1)}{3}}$

Proof: Let $A = pG \circ (\Phi \circ F) + (F \circ M) \circ F$ which can be written in the form,

$$A = a_0(x) + a_1(x)x_1 + a_2(x)x_2 + \cdots + a_{14}(x)x_{14} + a_{15}(x)x_{15}.$$

The polynomial $a_0(x)$ represents the constant coefficients of A such that;

$$a_0 = p(g_0\Phi_0 f_0 - g_0\Phi_1 f_1 - g_0\Phi_2 f_2 - g_0\Phi_3 f_3 - g_0\Phi_4 f_4 - g_0\Phi_5 f_5 - g_0\Phi_6 f_6 - g_0\Phi_7 f_7 - g_0\Phi_8 f_8 - g_0\Phi_9 f_9 - g_0\Phi_{10} f_{10} - g_0\Phi_{11} f_{11} - g_0\Phi_{12} f_{12} - g_0\Phi_{13} f_{13} - g_0\Phi_{14} f_{14} - g_0\Phi_{15} f_{15} - g_1\Phi_0 f_1 - g_1\Phi_1 f_0 - g_1\Phi_2 f_3 + g_1\Phi_3 f_2 - g_1\Phi_4 f_5 + g_1\Phi_5 f_4 + g_1\Phi_6 f_7 - g_1\Phi_7 f_6 - g_1\Phi_8 f_9 + g_1\Phi_9 f_8 - g_1\Phi_{10} f_{11} + g_1\Phi_{11} f_{10} - g_1\Phi_{12} f_{13} + g_1\Phi_{13} f_{12} - g_1\Phi_{14} f_{15} + g_1\Phi_{15} f_{14}$$
$$+ \ldots - g_{15}\Phi_0 f_{15} - g_{15}\Phi_1 f_{14} - g_{15}\Phi_2 f_{13} - g_{15}\Phi_3 f_{12} - g_{15}\Phi_4 f_{11} - g_{15}\Phi_5 f_{10} + g_{15}\Phi_6 f_9 - g_{15}\Phi_7 f_8 - g_{15}\Phi_8 f_7 - g_{15}\Phi_9 f_6 + g_{15}\Phi_{10} f_5 - g_{15}\Phi_{11} f_4 - g_{15}\Phi_{12} f_3 - g_{15}\Phi_{13} f_2 + g_{15}\Phi_{14} f_1 - g_{15}\Phi_{15} f_0) + (f_0^2 m_0 + f_1^2 m_0 + f_2^2 m_0 + f_3^2 m_0 + f_4^2 m_0 + f_5^2 m_0 + f_6^2 m_0 + f_7^2 m_0 + f_8^2 m_0 + f_9^2 m_0 + f_{10}^2 m_0 + f_{11}^2 m_0 + f_{12}^2 m_0 + f_{13}^2 m_0 + f_{14}^2 m_0 + f_{15}^2 m_0$$
$$= [a_{0,0}, a_{0,1}, a_{0,2}, \ldots, a_{0,N-1}]$$

Each polynomial of $a_1, a_2, \ldots, a_{15}$ is calculated in the similar method. Now, by the definition of $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_m$ and $\mathcal{L}_\Phi$ we obtain,
$f_i = [f_{i,0}, f_{i,1}, f_{i,2}, \cdots, f_{i,N-1}] \quad i = 0, 1, 2, \cdots, 15$

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

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

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

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

$$Pr(\Phi_{i,j} = 1) = Pr(\Phi_{i,j} = -1) = \tfrac{d_\Phi}{N}, \quad Pr(\Phi_{i,j} = 0) = 1 - \tfrac{2d_\Phi}{N}$$

$$Pr(m_{i,j} = \gamma) = \tfrac{1}{p}, \text{ where } \gamma \in (-p/2, p/2], \quad i, j = 0, 1, 2, \ldots, 15$$

Assume that all $f_{i,s}$, $g_{j,t}$ and $\Phi_{k,u}$ are pairwise independent random variables. For $s, t, u = 0, 1, \ldots, N-1$ and $i, j, k = 0, 1, 2, \ldots, 15$ and $\gamma = -\frac{p-1}{2}, \ldots, \frac{p-1}{2}$

$$Pr(f_{i.s} \cdot g_{j,t} . \Phi_{k.u} = \mp 1) = \tfrac{8 d_f d_g d_\Phi}{N^3}$$

$$Pr(f_{i.s} \cdot g_{j,t} . \Phi_{k.u} = 0) = 1 - \tfrac{8 d_f d_g d_\Phi}{N^3}$$

$$Pr(f_{i.s} \cdot f_{j.t} . m_{k.u} = \gamma) = \tfrac{4 d_{f2}}{p N^2}, \qquad (i \neq j \vee s \neq t) \wedge (\gamma \neq 0)$$

$$Pr(f_{i.s} \cdot f_{i.t} . m_{k.u} = \gamma) = \tfrac{2 d_f (d_f - 1) + 2 d_{f2}}{p N (N-1)} \quad (s \neq t) \wedge (\gamma \neq 0)$$

Under the above assumptions, we get $E(f_{i.s}.g_{j,t}.\Phi_{k.u}) = 0$, and $E(f_{i.s}.f_{j.t}.m_{k.u}) = 0$

$Var(f_{i.s}.g_{j,t}.\Phi_{k.u}) = \frac{8d_f d_g d_\Phi}{N^3}$, $Var(f_{i.s}.f_{j.t}.m_{k.u}) = \frac{d_f^2(P-1)(P+1)}{3N^2}$ and

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

Assume that the covariance of $f_{i.s}$ and $f_{i.t}$ is negligible, the final result is obtained as follows:

$$Var((f_{i.s}.g_{j,t}.\Phi_{k.u})y) = Var(\Sigma\Sigma_{s+t+u=y(modN)} f_{i.s}g_{j.t}\Phi_{k.u}) = \frac{8d_f d_g d_\Phi}{N}$$

$$Var((f_i.f_j.m_k)y) = Var(\Sigma\Sigma_{s+t+u=y(modN)} f_{i.s}g_{j.t}m_{k.u}) = \frac{d_f^2(p-1)(p+1)}{3}$$

$$Var((f_i^2 m_k)y) = Var(\Sigma\Sigma_{s+t+u=y(modN)} f_{i.s}g_{j.t}m_{k.u}) \approx \frac{d_f^2(N-1)(P-1)(p+1)}{3N} + \frac{d_f(p-1)(p+1)}{6}$$

Therefore,

$$Var(a_0, k) \approx \frac{2048p^2 d_f d_g d_\Phi}{N} + 20d_f^2(p-1)(p+1) + \frac{16d_f^2(N-1)(P-1)(p+1)}{3N} + \frac{8d_f(p-1)(p+1)}{3}$$

By applying the same procedure, we obtain

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

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

If the probability of all coefficients a_{ik} lie within $[(-q+1)/2 \ldots (q+1)/2]$, then the successful decryption is acheived.

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

$$Pr(\mid a_{i,k} \mid \leq \tfrac{q-1}{2}) = Pr(-\tfrac{q-1}{2} \leq a_{i,k} \leq \tfrac{q-1}{2}) = 2\mathcal{N}\tfrac{q-1}{2\sigma} \ ,$$

where σ equal amount

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

Corollary 2 :

i) The probability for any one of the messages $M_0, M_1, \ldots, M_{15}$ to be successfully decrypted is $(2\mathcal{N}(\frac{q-1}{2\sigma}) - 1)^N$

ii) The probability for all the messages $M_0, M_1, \ldots, M_{15}$ to be successfully decrypt $(2\mathcal{N}(\frac{q-1}{2\sigma}) - 1)^{16N}$

3. Security Analysis

In this section, some of the known attacks are discussed to show the security improvement of the proposed cryptosystem upon the classical NTRU.

3.1 BRUTE FORCE ATTACK

In HXDTRU an attacker who knows the public parameters, as well as, the public key $H = Fq \circ G$, must try all possible hexadecnion $F \in \mathcal{L}_f$ and check to see if $F \circ H$ turns into hexadecnion with small coefficients until find private key, the size of the subset $\mathcal{L}_f$ is calculated as follows: $\mid \mathcal{L}_f \mid = (\frac{N!}{(d_f!)^2(N-2d_f)!})^{16}$. Similarly, the attacker can search in the space $\mathcal{L}_\Phi$ to get the message original from the ciphertext and this search must be done in the order of the space $\mathcal{L}_\Phi$, where its size is calculated as follows: $\mid \mathcal{L}_\Phi \mid = (\frac{N!}{(d_\Phi!)^2(N-2d_\Phi)!})^{16}$

3.2 ALTERNATE KEYS ATTACK

An attacker trying to decrypt a message encrypted by the HXDTRU needs to find the alternate private key $F^{'}$ to F with the same properties. Hence, an attacker in the HXDTRU needs sixteen polynomials $f_0^{'}, f_1^{'}, \ldots, f_{15}^{'}$ with the same properties of polynomials $f_0, f_1, \ldots, f_{15}$ of F. However, an attacker in the NTRU only needs one polynomial in L_f with the same properties of the private key. In this method, the attacker in the HXDTRU needs sixteen times more attempts than those required by the NTRU to decrypt the message.

3.3 LATTICE BASED ATTACKS

The lattice attack against HXDTRU is more difficult because it is a non-commutative algebra and has dimension 16. When the attacker succeeds to obtain hexadecnion F satisfying $H = Fq \circ G \in \Psi_q$, the HXDTRU cryptosystem is broken. The only way for attacking the HXDTRU cryptosystem is by diffusion $H = F_q \circ G$ as follows:

$$f_0 * h_0 - f_1 * h_1 - f_2 * h_2 - f_3 * h_3 - f_4 * h_4 - f_5 * h_5 - f_6 * h_6 - f_7 * h_7 - f_8 * h_8 - f_9 * h_9 - f_{10} * h_{10} - f_{11} * h_1 - f_{12} * h12 - f_{13} * h_{13} - f_{14} * h_{14} - f_{15} * h_{15} = g_0 + qv_0$$

$$f_0 * h_1 + f_1 * h_0 + f_2 * h_3 - f_3 * h_2 + f_4 * h_5 - f_5 * h_4 - f_6 * h_7 + f_7 * h_6 + f_8 * h_9 - f_9 * h_8 + f_{10} * h_{11} - f_{11} * h_{10} + f_{12} * h_{13} - f_{13} * h_{12} + f_{14} * h_{15} - f_{15} * h_{14} = g_1 + qv_1$$

$$\vdots$$

$$f_0 * h_{14} - f_1 * h_{15} + f_2 * h_{12} + f_3 * h_{14} - f_4 * h_{10} + f_5 * h_{11} + f_6 * h_8 - f_7 * h_9 - f_8 * h_6 + f_9 * h_7 + f_{10} * h_4 - f_{11} * h_5 - f_{12} * h_2 - f_{13} * h_3 + f_{14} * h_0 + f_{15} * h_1 = g_{14} + qv_{14}$$

$$f_0 * h_{15} + f_1 * h_{14} - f_2 * h_{13} + f_3 * h_{12} - f_4 * h_{11} - f_5 * h_{10} + f_6 * h_9 + f_7 * h_8 - f_8 * h_7 - f_9 * h_6 + f_{10} * h_5 + f_{11} * h_4 - f_{12} * h_3 + f_{13} * h_2 - f_{14} * h_1 + f_{15} * h_0 = g_{15} + qv_{15}$$

All polynomials $h_0, h_1, \ldots, h_{15}$ can be represented in their matrix isomorphic representation as follows:

$$(H_i)_{N \times N} = \begin{pmatrix} h_{i,0} & h_{i,1} & \cdots & h_{i,N-1} \\ h_{i,N-1} & h_{i,0} & \cdots & h_{i,N-2} \\ h_{i,N-2} & h_{i,N-1} & \cdots & h_{i,N-3} \\ \vdots & \vdots & \ddots & \vdots \\ h_{i,2} & h_{i,3} & \cdots & h_{i,1} \\ h_{i,1} & h_{i,2} & \cdots & h_{i,0} \end{pmatrix}$$

Under the above assumptions, we can describe the HXDTRU lattice of dimension $32N$ spanned by the rows of the matrix $\mathcal{M}_{32N \times 32N} = \begin{pmatrix} I_{16N \times 16N} & H_{16N \times 16N} \\ 0_{16N \times 16N} & qI_{16N \times 16N} \end{pmatrix}$ such that H is the fundamental matrix for the h_i's satisfied $F \circ H = G$, which is described in Appendix , where I denoted the identity matrix, qI denotes q times the identity matrix and 0 denoted zero matrix. The vector $(f_0, f_1, \ldots, f_{15}, g_0, g_1, \ldots, g_{15})_{1 \times 32N}$ belong to the HXDTRU lattice which is denoted by $\mathcal{L}_{HXDTRU}$. Using a lattice reduction algorithm, a short vector in HXDTRU lattice can be found. For simplicity assuming $d = d_f = d_g = d_\Phi \approx N/3$, since the determinant of $\mathcal{L}_{HXDTRU}$ is equal to the determinant of $\mathcal{M}_{32N\times 32N}$ which is an upper triangle matrix, so its determinant equal to q^{16N}, $\parallel (f_0, f_1, \dots, f_{15}, g_0, g_1, \dots, g_{15}) \parallel \approx \sqrt{64d} \approx 4.62\sqrt{N}$. The Gaussian heuristic expected that the length of the shortest nonzero vector in HXDTRU lattice is calculated as $\delta(\mathcal{L}_{HXDTRU}) = \sqrt{\frac{16N}{\pi e}}\sqrt{q} \approx 1.369\sqrt{Nq}$. Also $\frac{\|(f_0,f_1,\dots,f_{15},g_0,g_1,\dots,g_{15})\|}{\delta} = \frac{4.62\sqrt{N}}{1.369\sqrt{Nq}} \approx \frac{3.37}{\sqrt{q}}$, hence the proposed vectors in $\mathcal{L}_{HXDTRU}$ are shorter than that expected by the Gaussian heuristic, also the dimension of $\mathcal{L}_{HXDTRU}$ is sixteen times larger than the dimension of $\mathcal{L}_{NTRU}$ with the same value of N. Therefore, the resistance of the HXDTRU against lattice attacks is much more than NTRU.

4. CONCLUSIONS

In this paper, the HXDTRU cryptosystem based on Hexadecnion algebra, which is a non-commutative, non-associative and alternative is proposed. The speed of HXDTRU is slower than NTRU with same parameter, but we can overtake this problem by taking small N. The HXDTRU is a multi dimension cryptosystem which has the ability to encrypt message of length $16N$ in one round (i.e. sixteen messages from a single source or sixteen independent messages from sixteen different sources). This property may be important in some applications such as electronic voting. When the coefficients of $x_1, x_2, \dots, x_{15}$ are equal to zero, HXDTRU converts to NTRU. The security of HXDTRU with dimension N has been similar to that of NTRU with dimension $16N$. Many attacks can threaten the security of the NTRU or NTRU-like cryptosystems. However, the most serious threat comes from the lattice attack. We have shown that the proposed HXDTRU can resist brute force, alternative, and lattice attacks

References

Alsaidi, N., Saed, M., Sadiq, A., and Majeed, A. A. (2015). An improved NTRU Cryptosystem via Commutative Quaternions Algebra. In *Proceedings of the International Conference on Security and Management (SAM)*, page 198. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Blömer, J. and May, A. (2001). Low secret exponent RSA revisited. In *Cryptography and Lattices*, pages 4–19. Springer.

Coglianese, M. and Goi, B.-M. (2005). MaTRU: A new NTRU-based cryptosystem. In *International Conference on Cryptology in India*, pages 232–243. Springer.

Coppersmith, D. and Shamir, A. (1997). Lattice attacks on NTRU. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 52–61. Springer.

Ebrahimi Atani, R., Ebrahimi Atani, S., and Hassani Karbasi, A. (2016). EEH: AGGH-like public key cryptosystem over the Eisenstein Integers using polynomial representations. *The ISC International Journal of Information Security*, 7(2):115–126.

Gaborit, P., Ohler, J., and Solé, P. (2002). *CTRU, a polynomial analogue of NTRU*. PhD thesis, INRIA.

Hoffstein, J., Pipher, J., and Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium*, pages 267–288. Springer.

Hoffstein, J., Pipher, J., Silverman, J. H., and Silverman, J. H. (2008). *An introduction to mathematical cryptography*, volume 1. Springer.

Jarvis, K. (2011). *NTRU over the Eisenstein integers*. PhD thesis, Université d'Ottawa/University of Ottawa.

Jarvis, K. and Nevins, M. (2015). ETRU: NTRU over the Eisenstein integers. *Designs, Codes and Cryptography*, 74(1):219–242.

Majeed, A. A. (2015). *CQTRU Cryptosystem Pased on Commutative Rings of Quaternion*. PhD thesis, University of Technology,IBaghdad.

Malekian, E. and Zakerolhosseini, A. (2010a). NTRU-like public key cryptosystems beyond dedekind domain up to alternative algebra. In *Transactions on computational science X*, pages 25–41. Springer.

Malekian, E. and Zakerolhosseini, A. (2010b). OTRU: A non-associative and high speed public key cryptosystem. In *Computer Architecture and Digital Systems (CADS), 2010 15th CSI International Symposium on*, pages 83–90. IEEE.

Malekian, E., Zakerolhosseini, A., and Mashatan, A. (2009). QTRU: A Lattice Attack Resistant Version of NTRU PKCS Based on Quaternion Algebra. *preprint, Available from the Cryptology ePrint Archive: http://eprint. iacr. org/2009/386. pdf.*

Nevins, M., Karimianpour, C., and Miri, A. (2010). NTRU over rings beyond. *Designs, Codes and Cryptography*, 56(1):65–78.

Thakur, K. and Tripathi, B. P. (2016). BTRU, A Rational Polynomial Analogue of NTRU Cryptosystem. *International Journal of Computer Applications, Foundation of Computer Science (FCS)*, 145(12):22–24.

Vats, N. (2009). NNRU, a noncommutative analogue of NTRU. *arXiv preprint arXiv:0902.1891*.

Yassein, R. and AlSaidi, N. (2016). HXDTRU Crytosystem Based On Hexadecnion Algebra. In *5th International Cryptology and Information Security Conference*, pages 1–10.