A New Public Key Encryption Based on Hexadecnion Algebra with Neutrosophic Integer Coefficients

Sahab Mohsen Abboud[1,*], Mohammed Hassan Hamza[2], Hassan Rashed Yassein[3]

[1]Department of Mathematics, College of Basic Education, University of Babylon, Hillah, Iraq

[2]General Directorate of Al-Muthanna Education, Al-Muthanna, Iraq

[3]Department of Mathematics College of Education, University of Al-Qadisiyah, Al-Qadisiya, Iraq

Emails: bsc.sahab.jwer@uobabylon.edu.iq; edu-math.post16@qu.edu.iq; hassan.yaseen@qu.edu.iq

Abstract

HXDTRU is a multidimensional public key encryption system with sixteen encrypted data vectors at each step. In this work, we propose HXDHS, an improved version of HXDTRU based on hexadecnion algebra with neutrosophic integer coefficients, as well as a new mathematical construction includes three private keys with one public key to enhance the security and robustness of the public-key system. HXDHS is suitable for applications that require concurrent operation from multiple sources.

Keywords: Neutrosophic Integer; HXDTRU; Hexadecnion Algebra; Security Analysis

1. Introduction

Any encryption system its main goal is to conceal sensitive information in a way that makes it unknown to anyone not authorized to access it. The NTRU encryption system plays a big role in providing high levels of security. Three mathematicians Hoff stein et al [1]. Introduced it in 1996, it is faster compared to RSA and ECC encryption systems. The mathematical structure of NTRU has been the focus of many studies aimed at improving its performance. Specifically, NTRU mainly relies on the ring of truncated polynomial with degree $N-1$ represented as $Z[x]/(x^N-1)$. In 2005, Coglianese and Goi introduced MaTRU, a variant of NTRU that operates in ring M of $k*k$ matrices of polynomials $Z[x]/(x^N-1)$, providing an analog approach [2]. In 2009, Malkian et al. proposed a system called QTRU based on quaternary algebra [3]. In 2010 Malakai et al. [3].

Presented an encryption system called OTRU, which is a multi-dimensional encryption system, depended of Octonion algebra. In 2011 and 2015 Jarvis [4, 5] proposed an ETRU via integer Z[W] loop of Leisenstein. It is a faster system and contains smaller keys with the same security level or higher than NTRU. In 2016 and 2017, Yassin and Al-Saeedi [6, 7] presented multi-dimensional systems are called HXDTRU and BITRU used on hexadecimal and binary algebra respectively. Yassein and Al-Saidi [8, 9] presented the BCTRU system, in 2018 and 2019, which is based on algebra of bi-Cartesian. In 2021, Yassein et al. [10] also proposed QMTRU with a new mathematical structure as an improvement for QTRU. In addition, Shihadi and Yassein [11] introduced NTRSH, a novel public key system via tripternion algebra, which analogous NTRU. As well as Abo-Alsood and Yassein [12] proposed an octonion algebra subalgebra named Qu-octonion subalgebra, which is non-commutative and associative. This algebra is used to build the QOTRU cryptosystem.

In 2022, Shihadi and Yassein [13] proposed an upgraded NTRU cryptosystem called NTRTRN. In the same year, Abo-Alsood and Yassein [14] presented TOTRU, an encryption system distinguished by its security and efficiency. Also, Al-Awadi [15] proposed MaTRUD as an improvement to the MaTRU. In 2023, Yassein et al. suggest QuiTRU via a multi-dimensional algebra [16]. In 2024, Abboud et al. using octonion and quaternion algebras to introduced OTRCQ [17]. Abo-Alsood et al. based on HH-Real algebra and RS proposed HH-RSA

DOI: https://doi.org/10.54216/IJNS.260411

system [18]. In 2025, Abboud et al. improved the RSA through the octonion polynomials [19]. Hamza et al. development of MRSA via algebra of octonion [20]. If Z is the ring of integers and I an indeterminacy with the property $I^2 = I$, then $Z(I) = \{a + bI;\ a, b \in Z\}$ is said to be the neutrosophic ring of integers, the elements of $Z(I)$ are said to be neutrosophic integers [21].
The usage of neutrosophic structures in cryptography can be seen in [22].

2. Related Work

Hexadecnion algebra is a vector space of sixteen dimension over the real number R defined as follows: $HD = \{\, w | w = r_0 \ + \sum_{i=1}^{15} r_i \tau_i, r_0, r_1, \dots, r_{15} \in R\}$ [6].

where $\beta = \{1, \tau_1, \tau_2, \dots, \tau_{15}\}$ is the basis and r_i's are scalars in a set of real number. Suppose $w_1, w_2 \in HD$ where

$$w_1 = r_0 + r_1\tau_1 + r_2\tau_2 + \cdots + r_{14}\tau_{14} + r_{15}\tau_{15},$$

$$w_2 = r_o^{'} + r_1^{'}\tau_1 + r_2^{'}\tau_2 + \cdots + r_{14}^{'}\tau_{14} + r_{15}^{'}\tau_{15}.$$

The addition of w_1 and w_2 is defined by adding their corresponding coefficients, such that;

$$w_1 + w_2 = \left(r_0 + r_o^{'}\right) + \left(r_1 + r_1^{'}\right)\tau_1 + \cdots + (r_{14} + r_{14}^{'})\tau_{14} + (r_{15} + r_{15}^{'})\tau_{15}$$

Table 1 is designed to define the multiplication between w_i and w_j where w_i and $w_j \in HD$, and $\tau_i^2 = -1$, $\tau_i\tau_j = -\tau_j\tau_i$ and $i \neq j$, $i, j = 1,2, \dots ,15$.

Table 1: (Multiplication Table)

$*$	1	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8	τ_9	τ_{10}	τ_{11}	τ_{12}	τ_{13}	τ_{14}	τ_{15}
1	1	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8	τ_9	τ_{10}	τ_{11}	τ_{12}	τ_{13}	τ_{14}	τ_{15}
τ_1	τ_1	-1	τ_3	$-\tau_2$	τ_5	$-\tau_4$	$-\tau_7$	τ_6	τ_9	$-\tau_8$	τ_{11}	$-\tau_{10}$	τ_{13}	$-\tau_{12}$	τ_{15}	$-\tau_{14}$
τ_2	τ_2	$-\tau_3$	-1	τ_1	τ_6	τ_7	$-\tau_4$	$-\tau_5$	τ_{10}	$-\tau_{11}$	$-\tau_8$	τ_9	τ_{14}	$-\tau_{15}$	$-\tau_{12}$	τ_{11}
τ_3	τ_3	τ_2	$-\tau_1$	-1	τ_7	$-\tau_6$	τ_5	$-\tau_4$	τ_{11}	τ_{10}	$-\tau_9$	$-\tau_8$	τ_{15}	τ_{14}	$-\tau_{13}$	$-\tau_{12}$
τ_4	τ_4	$-\tau_5$	$-\tau_6$	$-\tau_7$	-1	τ_1	τ_2	τ_3	τ_{12}	$-\tau_{13}$	$-\tau_{14}$	$-\tau_{15}$	τ_8	τ_9	τ_{10}	τ_{11}
τ_5	τ_5	τ_4	$-\tau_7$	τ_6	$-\tau_1$	-1	$-\tau_3$	τ_2	τ_{13}	τ_{12}	$-\tau_{15}$	τ_{14}	$-\tau_9$	$-\tau_8$	τ_{11}	$-\tau_{10}$
τ_6	τ_6	τ_7	τ_4	$-\tau_5$	$-\tau_2$	τ_3	-1	$-\tau_1$	τ_{14}	τ_{15}	τ_{12}	$-\tau_{13}$	$-\tau_{10}$	$-\tau_{11}$	$-\tau_8$	τ_9
τ_7	τ_7	$-\tau_6$	τ_5	τ_4	$-\tau_3$	$-\tau_2$	τ_1	-1	τ_{15}	$-\tau_{14}$	τ_{13}	τ_{12}	$-\tau_{11}$	τ_{10}	$-\tau_9$	$-\tau_8$
τ_8	τ_8	$-\tau_9$	$-\tau_{10}$	$-\tau_{11}$	$-\tau_{12}$	$-\tau_{13}$	$-\tau_{14}$	$-\tau_{15}$	-1	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7
τ_9	τ_9	τ_8	τ_{11}	$-\tau_{10}$	τ_{13}	$-\tau_{12}$	τ_{15}	τ_{14}	$-\tau_1$	-1	τ_3	$-\tau_2$	τ_5	$-\tau_4$	τ_7	$-\tau_6$
τ_{10}	τ_{10}	$-\tau_{11}$	τ_8	τ_9	τ_{14}	τ_{15}	$-\tau_{12}$	$-\tau_{13}$	$-\tau_2$	$-\tau_3$	-1	τ_1	τ_6	$-\tau_7$	$-\tau_4$	τ_5
τ_{11}	τ_{11}	τ_{10}	$-\tau_9$	τ_8	τ_{15}	$-\tau_{14}$	τ_{13}	$-\tau_{12}$	$-\tau_3$	τ_2	$-\tau_1$	-1	τ_7	τ_6	$-\tau_5$	$-\tau_4$
τ_{12}	τ_{12}	$-\tau_{13}$	$-\tau_{14}$	$-\tau_{15}$	τ_8	τ_9	τ_{10}	τ_{11}	$-\tau_4$	$-\tau_5$	$-\tau_6$	$-\tau_7$	-1	τ_1	τ_2	τ_3
τ_{13}	τ_{13}	τ_{12}	τ_{15}	$-\tau_{14}$	$-\tau_9$	τ_8	τ_{11}	$-\tau_{10}$	$-\tau_5$	τ_4	τ_7	$-\tau_6$	$-\tau_1$	-1	τ_3	$-\tau_2$
τ_{14}	τ_{14}	$-\tau_{15}$	τ_{12}	τ_{13}	$-\tau_{10}$	$-\tau_{11}$	τ_8	τ_9	$-\tau_6$	$-\tau_7$	τ_4	τ_5	$-\tau_2$	$-\tau_3$	-1	τ_1
τ_{15}	τ_{15}	τ_{14}	τ_{13}	τ_{12}	$-\tau_{11}$	τ_{10}	$-\tau_9$	τ_8	$-\tau_7$	τ_6	$-\tau_5$	τ_4	τ_3	τ_2	$-\tau_1$	-1

DOI: https://doi.org/10.54216/IJNS.260411

The multiplication is alternative but non-associative and non- commutative.

For any scalar α, we have, $\alpha w = \alpha(r_0 + r_1\tau_1 + \cdots + r_{14}\tau_{14} + r_{15}\tau_{15})$

$$= \alpha r_0 + \alpha r_1\tau_1 + \cdots + \alpha r_{14}\tau_{14} + \alpha r_{15}\tau_{15},$$

the conjugate of a hexadecnion $w = r_0 + \sum_{i=1}^{15} r_i\tau_i$ is defined as follows

$$\overline{w} = r_0 - \sum_{i=1}^{15} r_i\tau_i,$$

and the square norm is given by $N(w) = w\overline{w} = \sum_{i=0}^{15} {r_i}^2$.

The multiplicative inverse of $0 \neq w$ equal to:

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

3. Proposed Cryptosystem HXDHS Using Neutrosophic integers

HXDHS cryptosystem depends on algebras $\varphi = \left\{\sum_{i=0}^{15} f_i\,\beta_i\,;\ f_i \in \mathfrak{R}\right\}, \varphi_p = \left\{\sum_{i=0}^{15} f_i\,\beta_i\,;\ f_i \in \mathfrak{R}_p\right\}$, $\varphi_q = \left\{\sum_{i=0}^{15} f_i\,\beta_i\,;\ f_i \in \mathfrak{R}_q\right\}$ where $\mathfrak{R} = Z(I)[x]/(x^N - 1)$, $\mathfrak{R}_p = Z_p(I)[x]/(x^N - 1)$, and $\mathfrak{R}_q = Z_q(I)[x]/(x^N - 1)$ be truncated polynomials rings with neutrosophic integer coefficients, three positive integer parameters (N, p, q) defined as HXDTRU and five sets L_F, L_G, L_S, L_W and $L_M \subset \varphi$, which' defined as follows:

$L_F = \{f_0(x) + f_1(x)\tau_1 + \cdots + f_{15}(x)\tau_{15} + I(z_0(x) + z_1(x)\tau_1 + \cdots + z_{15}(x)\tau_{15}) | f_i(x) + Iz_i(x) \in \mathfrak{R}$ satisfy $\ell(d_f, d_f - 1)\}$,

$L_G = \{g_0(x) + g_1(x)\tau_1 + \cdots + g_{15}(x)\tau_{15} + I(\{k_0(x) + k_1(x)\tau_1 + \cdots + k_{15}(x)\tau_{15}) |\ g_i(x) + Ik_i(x) \in \mathfrak{R}$ satisfy $\ell(d_g, d_g)\}$,

$L_S = \{s_0(x) + s_1(x)\tau_1 + \cdots + s_{15}(x)\tau_{15} + I(c_0(x) + c_1(x)\tau_1 + \cdots + c_{15}(x)\tau_{15}) | s_i(x) + Ic_i(x) \in \mathfrak{R}$ satisfy $\ell(d_s, d_s)\}$,

$L_W = \{w_0(x) + w_1(x)\tau_1 + \cdots + w_{15}(x)\tau_{15} + I(b_0(x) + b_1(x)\tau_1 + \cdots + b_{15}(x)\tau_{15}) | w_i(x) + Ib_i(x) \in \mathfrak{R}$ satisfy $\ell(d_w, d_w)\}$,

$L_M = \{m_0(x) + m_1(x)\tau_1 + \cdots + m_{15}(x)\tau_{15} + I(a_0(x) + a_1(x)\tau_1 + \cdots + a_{15}(x)\tau_{15}) |$ coefficients of $m_i(x), a_i(x)$ re the

chosen modulo between $-p/2$ and $p/2$ },

where, $\ell(d_a, d_b) = \{f | f\ has\ d_a$ coefficients equal 1+I, d_b coefficients equal -1-I, other value equal I}.

The phases of HXDHS are described as below:

I- Key Generation

By using the mathematical formulas of multiplication and inversing modulo neutrosophic integers, we can generate a public key as follows:
choose $F \in L_F,\ G \in L_G,\ S \in L_S\ and\ R \in L_R$ where F invertible modulo p and q denoted by ${F_p}^{-1}\ and\ F_q^{-1}$ respectively. The public key H computed by the formula
$H \equiv {F_q}^{-1} * (G * S) \pmod q$.
We can summarize the method of generating the key with the following pseudocode (1):

Pseudocode 1: demonstrate the key generation phase of HXDHS:

Input: N, p, q, d_f, d_g, d_s.
Output: H
Compute $F_q^{-1} = inverse\ of\ F \pmod q$.
Compute $H_1 \equiv G * S \pmod q$.
Compute $H \equiv {F_q}^{-1} * H_1 \pmod q$
End.

II- **Encryption**

To convert the original text M to encrypted text, choose randomly $W \in L_W$ and use the following formula to getting the ciphertext E

$E \equiv pH * W + M \pmod q$.
Where the coefficients of E belong to interval $\left(-\frac{p}{2}, \frac{p}{2}\right]$.
We can summarize the method of encryption with the following pseudocode (2):

DOI: https://doi.org/10.54216/IJNS.260411

Pseudocode 2: demonstrates the encryption phase of HXDHS:

Input: N, d_w, H, M

Output: $(Encryption\ text)\ E$

Compute $E_1 \equiv H * W (mod\ q)$.

Compute $E \equiv pE_1 + M (mod\ q)$

for $\varepsilon = 0,1, \dots ,15$.

for $\zeta = 1\ to\ N$

if $E(\varepsilon, \zeta) \leq -q/2$

$E(\varepsilon, \zeta) = E(\varepsilon, \zeta) + q$

else $E(\varepsilon, \zeta) > q/2$

$E(\varepsilon, \zeta) = E(\varepsilon, \zeta) - q$

end if

end for

end for

end.

III- Decryption

In order for the recipient to recover the original text M through the encrypted text E, he\she must follow the following steps:

Compete $\beta \equiv F * E\ (mod\ q)$

$$\equiv F * (pH * W + M)\ (mod\ q)$$
$$\equiv p(F * F_q^{-1} * G * S * W) + (F * M)\quad (mod\ q)$$
$$\equiv p(G * S * W) + (F * M)\quad (mod\ q).$$

Where the coefficients of β belong to interval $\left(-\frac{q}{2}, \frac{q}{2}\right]$.

Take $\delta \equiv \beta\ (mod\ p)$.

$$F_p^{-1} * \delta\ (mod\ p) \equiv F_p^{-1} * (F * M)\ (mod\ p)$$
$$\equiv M\ \ (mod\ p).$$

Where the coefficients belong to interval $\left(-\frac{p}{2}, \frac{p}{2}\right]$.

We can summarize the phase of decryption HXDHS with the following pseudocode (3):

Pseudocode 3: demonstrates the decryption phase of HXDHS:

Input: N, p, q, W, F_p^{-1}, E .

Output: $(\ message\ M)$.

Compute $\beta \equiv F * E (mod\ q)$.

for $\varepsilon = 0,1, \dots ,15$.

for $\zeta = 1\ to\ N$

if $\beta(\varepsilon, \zeta) \leq -q/2$

$\beta(\varepsilon, \zeta) = \beta(\varepsilon, \zeta) + q$

else $\beta(\varepsilon, \zeta) > q/2$

$\beta(\varepsilon, \zeta) = \beta(\varepsilon, \zeta) - q$

end if

end for

DOI: https://doi.org/10.54216/IJNS.260411

end for

$\beta_1 \equiv \beta \ (mod\ p)$

$\delta \equiv F_p^{-1} * \beta_1 \ (mod\ p)$

for $\varepsilon = 0,1, \dots ,15$.

for $\zeta = 1\ to\ N$

if $\delta(\varepsilon,\zeta) \leq -p/2$

$\delta(\varepsilon,\zeta) = \delta(\varepsilon,\zeta) + p$

else if $\delta(\varepsilon,\zeta) > p/2$

$\delta(\varepsilon,\zeta) = \delta(\varepsilon,\zeta) - p$

end if

end for

end for

$M = \delta$

end.

4. Performance Analysis of HXDHS

4.1. Space of Security

By brute force attack, an attacker tries to get two of three private keys ($F,\ G,\ S$) that make up the public key. Suppose that the space of is greater than of (L_G, L_S) therefore, the space of L_G, L_S equal to

$\left(\frac{N!}{(d_G\,!)^2\,(N-2d_G)!}\right)^{16}, \left(\frac{N!}{(d_S\,!)^2\,(N-2d_S)!}\right)^{16}$ respectively.

Since the coefficients of G and S are neutrosophic integers, therefore the space of key equal to

$\left(\frac{N!}{(d_G\,!)^2\,(N-2d_G)!}\right)^{32} \left(\frac{N!}{(d_S\,!)^2\,(N-2d_S)!}\right)^{32}$.

The attacker can also access the original text by searching for the private key W which belong to L_W in the encrypted text. The space of L_W equal to

$\left(\frac{N!}{(d_W!\,)^2\,(N-2d_W)!}\right)^{16}$.

Hence, the space of message equal to:

$\left(\frac{N!}{(d_W!\,)^2\,(N-2d_W)!}\right)^{32}$.

4.2. Execution Time

Table (2) shows the execution time of HXDHS according to the addition and multiplication of polynomials in the all phases.

Table 2: Execution time of HXDHS

Phase	Time
Key generation	$4096t_1$
Encryption	$256t_1 + 16t_0$
Decryption	$4352t_1 + 16t_0$
Total	$4448t_1 + 23t_0$

Where t_1, t_0 are the time of multiplication and addition of polynomials respectively.

DOI: https://doi.org/10.54216/IJNS.260411

5. Comparative Between HXDTRU and HXDHS

The Tables (3) and (4) show a comparison between the new method HXDHS and the method HXDTRU in terms of the space of the key and the message, which gives the HXDHS method a significant advantage in the space of the key and the message, making it more efficient and usable.

Table 3: Space of key of HXDHS and HXDTRU

Cryptosystem	Space of key
HXDHS	$\left(\frac{N!}{(d_G!)^2\,(N-2d_G)!}\right)^{32}\left(\frac{N!}{(d_S!)^2\,(N-2d_S)!}\right)^{32}$
HXDTRU	$\left(\frac{N!}{(d_G!)^2\,(N-2d_G)!}\right)^{16}$

Table 4: Space of message of HXDHS and HXDTRU

Cryptosystem	Space of message
HXDHS	$\left(\frac{N!}{(d_W!)^2\,(N-2d_W)!}\right)^{32}$
HXDTRU	$\left(\frac{N!}{(d_W!)^2\,(N-2d_W)!}\right)^{16}$

Tables (6) and (7) explain key space and message security of HXDTRU and HXDHS depends on the values in Table (5) respectively.

Table 5: Generic parameters

N	d_G	d_S	d_W
103	10	10	3
103	18	18	8
139	10	10	8
139	23	23	18
163	16	16	16
163	25	25	20
199	18	18	16
199	32	32	20
251	18	18	16
251	22	22	22

DOI: https://doi.org/10.54216/IJNS.260411

Table 6: Key space security of HXDHS and HXDTRU

Key Space of $\boldsymbol{HDXTRU}$	Key Space of $\boldsymbol{HXDHS}$
$\mathbf{3.0345 \times 10^{420}}$	8.4797×10^{1681}
$\mathbf{1.3743 \times 10^{605}}$	3.5675×10^{2420}
$\mathbf{7.5142 \times 10^{465}}$	3.1882×10^{1563}
$\mathbf{3.2803 \times 10^{801}}$	1.1578×10^{3206}
$\mathbf{5.3037 \times 10^{683}}$	7.9068×10^{2734}
$\mathbf{1.4272 \times 10^{905}}$	4.1496×10^{3620}
$\mathbf{7.9264 \times 10^{794}}$	3.9474×10^{3197}
$\mathbf{1.6254 \times 10^{1141}}$	6.9808×10^{4564}
$\mathbf{1.3086 \times 10^{858}}$	2.1342×10^{3432}
$\mathbf{7.8916 \times 10^{987}}$	3.8788×10^{3951}

Table 7: Message space security of HXDHS and HXDTRU

Message space of $\boldsymbol{HDXTRU}$	*Message space of* $\boldsymbol{HXDHS}$
$\mathbf{3.0345 \times 10^{420}}$	9.2085×10^{840}
$\mathbf{1.3743 \times 10^{605}}$	1.8887×10^{1210}
$\mathbf{7.5142 \times 10^{465}}$	5.6464×10^{931}
$\mathbf{3.2803 \times 10^{801}}$	1.0760×10^{1603}
$\mathbf{5.3037 \times 10^{683}}$	2.8119×10^{1367}
$\mathbf{1.4272 \times 10^{905}}$	2.037×10^{1810}
$\mathbf{7.9264 \times 10^{794}}$	6.3829×10^{1589}
$\mathbf{1.6254 \times 10^{1141}}$	3.6421×10^{2282}
$\mathbf{1.3086 \times 10^{858}}$	1.4609×10^{1716}
$\mathbf{7.8916 \times 10^{987}}$	6.2378×10^{1975}

Figure (1) shows key space security of HXDHS and HXDTRU depending on the value in Table (6).

DOI: https://doi.org/10.54216/IJNS.260411

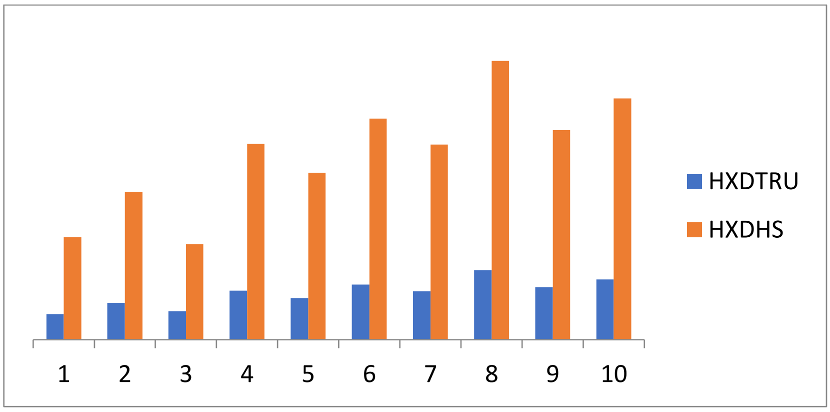

Figure 1. Key space security of HXDHS and HXDTRU.

Figure (2) shows message space security of HXDHS and HXDTRU depending on the value in Table (7).

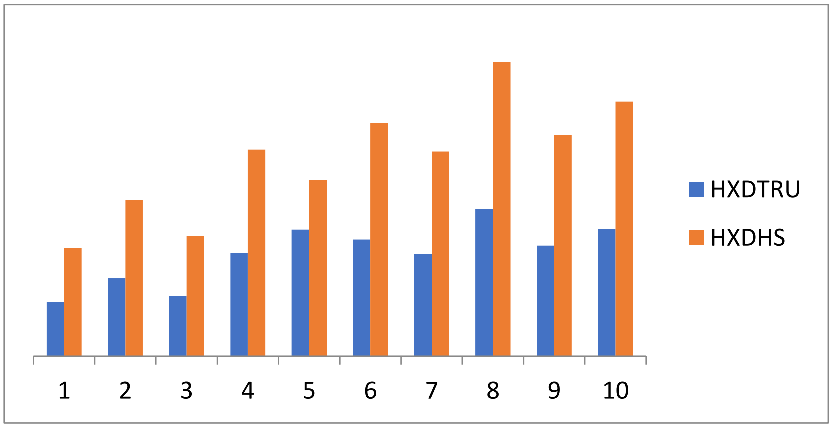

Figure 2. Message space security of HXDHS and HXDTRU.

Table (8) shows a comparison between HXDHS and HXDTRU in terms of execution time.

Table 8: Execution time of HXDHS and HXDTRU

Cryptosystem	Execution time
HXDHS	$4448t_1 + 23t_0$
HXDTRU	$8704t_1 + 32t_0$

HXDHS is obviously faster than HXDTRU.

6. Conclusion

The proposed method, HXDHS, which is based on introducing integer Neutrosophic coefficients, has had a significant impact on increasing the level of security for both the private keys that generate public key and private key used to convert the plaintext to ciphertext, making it a suitable method for encrypting multi-source data. HXDTRU method is a special case of HXDHS in the case of $s = 1$ and $b = 0$ in the Neutrosophic element $a + bI$.

References

[1] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *International Algorithmic Number Theory Symposium*, 1998, pp. 267–288.

[2] M. Coglianese and B.-M. Goi, "MaTRU: A new NTRU-based cryptosystem," in *Progress in Cryptology-INDOCRYPT 2005: 6th International Conference on Cryptology in India*, Bangalore, India, December 10-12, 2005. Proceedings 6, 2005, pp. 232–243.

DOI: https://doi.org/10.54216/IJNS.260411

[3] E. Malekian, A. Zakerolhosseini, and A. Mashatan, "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, 2009.

[4] K. Jarvis, *NTRU over the Eisenstein Integers*. University of Ottawa (Canada), 2011.

[5] K. Jarvis and M. Nevins, "ETRU: NTRU over the Eisenstein integers," *Designs, Codes and Cryptography*, vol. 74, no. 1, pp. 219–242, 2015.

[6] H. R. Yassein and N. M. Al-Saidi, "HXDTRU cryptosystem based on hexadecnion algebra," in *Proceedings of the 5th International Cryptology and Information Security Conference*, Kota Kinabalu, Malaysia, 2016, vol. 31.

[7] N. M. G. Al-Saidi and H. R. Yassein, "A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure," *Malaysian Journal of Mathematical Sciences*, vol. 11, pp. 29–43, 2017.

[8] H. R. Yassein and N. M. G. Al-Saidi, "BCTRU: a new secure NTRUcrypt public key system based on a newly multidimensional algebra," in *Proceedings of the 6th International Cryptology and Information Security Conference*, 2018, pp. 1–11.

[9] H. R. Yassein and N. M. G. Al-Saidi, "An innovative bi-cartesian algebra for designing of highly performed NTRU like cryptosystem," *Malaysian Journal of Mathematical Sciences*, vol. 13, no. S, pp. 77–91, 2019.

[10] H. R. Yassein, A. A. Abidalzahra, and N. M. G. Al-Saidi, "A new design of NTRU encryption with high security and performance level," in *AIP Conference Proceedings*, 2021, vol. 2334, no. 1, p. 80005.

[11] S. H. Shahhadi and H. R. Yassein, "NTRsh: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra," *Journal of Physics Conference Series*, vol. 1999, pp. 2-6, 2021.

[12] H. H. Abo-Alsood and H. R. Yassein, "QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra," *Journal of Physics Conference Series*, vol. 1999, pp. 2-7, 2021.

[13] S. H. Shihadi and H. R. Yassein, "An innovative tripternion algebra for designing NTRU-like cryptosystem with high security," *AIP Conference Proceedings*, vol. 2386, pp. 60009-1-60009-6, 2022.

[14] H. H. Abo-Alsood and H. R. Yassein, "Analogue to NTRU public key cryptosystem by multi-dimension algebra with high security," *AIP Conference Proceedings*, vol. 2386, pp. 600091-600096, 2022.

[15] M. H. Al-Awadi, "Designing an Efficient and Secure Cryptosystems Similar to MaTRU and RSA," M. Sc. Thesis, University of Al-Qadisiyah, Iraq, 2022.

[16] H. R. Yassein, H. N. Zaky, H. H. Abo-Alsoo, I. A. Mageed, and W. I. El-Sobky, "QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra," *Applied Mathematics*, vol. 17, no. 1, pp. 49–53, 2023.

[17] S. M. Abboud, H. R. Yassein, R. K. Alhamido, and S. Deir-ez-Zor, "Improvement of a Multi-Dimensional Public-Key OTRU Cryptosystem," *Computer Science*, vol. 19, no. 4, pp. 1071–1076, 2024.

[18] H. H. Abo-Alsood, M. H. Hamza, S. A. Al-Bairmani, and H. R. Yassein, "Development of Public Key Cryptosystem RSA via Multidimensional Algebra," *Computer Science*, vol. 19, no. 4, pp. 1177–1182, 2024.

[19] S. M. Abboud, R. K. K. Ajeena, and H. R. Yassein, "Octonion Polynomials for a More Secure RSA Public Key Cryptosystem," *International Journal of Mathematics & Computer Science*, vol. 20, no. 1, 2025.

[20] M. H. Hamza, S. M. Abboud, and H. R. Yassein, "Development of Modified RSA Cryptosystem via Octonion Algebra."

[21] M. Abobala, "Foundations of neutrosophic number theory," *Neutrosophic Sets and Systems*, vol. 39, no. 1, p. 10, 2021.

[22] A. N. Smith and B. J. Lee, "Secure Data Transmission Using Quantum Key Distribution: A Comprehensive Review," *Journal of Quantum Information Processing*, vol. 20, no. 3, pp. 123-145, 2022.

DOI: https://doi.org/10.54216/IJNS.260411