A Novel Application of Symbolic 2-Plithogenic Integers and Refined Neutrosophic Numbers in Public Key Encryption Based On Hexadecnion Algebra

Maha Alsaoudi[1], Gharib M. Gharib[2,*], Fadil A. Jaradat[3,*], Ahmad A. Abubaker[4], Ahmed Atallah Alsaraireh[5]

[1]Department of Science, Applied Science Private University, Jordan

[2]Department of Mathematics, Zarqa University, Zarqa , Jordan

[3]Faculty of Information Technology, Abu Dhabi University, Abu Dhabi, United Arab Emirates

[4]Faculty of Computer Studies, Arab Open University, Saudi Arabia

[5] The University of Jordan, Aqaba, Department of computer information systems, Jordan

Emails: m_alsoudi@asu.edu.jo; ggharib@zu.edu.jo; Fadil.jaradat@adu.ac.ae; a.abubaker@arabou.edu.sa; a.alsarairah@ju.edu.jo

Abstract

In this work, we use the symbolic 2-plithogenic integers and refined neutrosophic numbers to get a generalized version of HXDTRU with a strict approach includes three symbolic 2-plithogenic and refined neutrosophic private keys with one public symbolic 2-pithogenic and refined neutrosophic key to improve the security. In addition, we analyse the complexity of the generalized systems numerically.

Keywords: Refined neutrosophic number; Symbolic 2-plithogenic number; Hexadecnion 2-plithogenic Algebra; Complexity; Encryption

1. Introduction

Cryptography is the science of securing information by transforming it into an unreadable format, accessible only to those with a secret key. It plays a vital role in protecting data in communication, finance, and digital security. Modern cryptography relies on complex mathematical algorithms to ensure confidentiality and integrity. [2-3]
In [6], authors present the HXDTRU cryptosystem, which utilizes hexadecnion algebra to enhance security and complexity. Results show improved resistance to algebraic and analytical attacks compared to traditional schemes like NTRU [1].

The use of neutrosophic numbers in cryptography has provided a valuable tool for extending well-known traditional algorithms and constructing more complex models, as it has contributed to the development of generalized versions of the RSA and El-Gamal algorithms [4-5,7].
Refined neutrosophic numbers and symbolic 2-plithogenic numbers are defined as extensions of classical numbers with many interesting algebraic properties, see [8-12].

In this work, we use the symbolic 2-plithogenic integers and refined neutrosophic numbers to get a generalized version of HXDTRU with a strict approach includes three symbolic 2-plithogenic and refined neutrosophic private keys with one public symbolic 2-pithogenic and refined neutrosophic key to improve the security. In addition, we analyse the complexity of the generalized systems numerically.

DOI: https://doi.org/10.54216/IJNS.270217

2. Preliminaries

Hexadecnion algebra is a vector space of sixteen dimension over the real number R defined as follows: $HD = \{ s | s = c_0 + \sum_{i=1}^{15} c_i \tau_i, r_0, c_1, \ldots, c_{15} \in R\}$ [6].

where $M = \{1, v_1, v_2, \ldots, v_{15}\}$ is the basis and c_i's .

For $s_1, s_2 \in HD$ where

$$s_1 = c_0 + c_1 v_1 + c_2 v_2 + \cdots + c_{14} v_{14} + c_{15} v_{15},$$

$$s_2 = c_o' + c_1' v_1 + c_2' v_2 + \cdots + c_{14}' v_{14} + c_{15}' v_{15}.$$

The conjugate of a hexadecnion $s = c_0 + \sum_{i=1}^{15} c_i v_i$ is defined as follows

$$\bar{s} = c_0 - \sum_{i=1}^{15} c_i v_i,$$

- **Refined neutrosophic numbers/symbolic 2-plithogenic numbers [8-10]**

Feature	Refined Neutrosophic Numbers	Symbolic 2-Plithogenic Numbers
Definition	An extension of neutrosophic numbers where truth, indeterminacy, and falsity are refined into multiple subcomponents.	An advanced symbolic structure based on two attributes with multiple sub-values, blending plithogenic and symbolic logic.
Components	Triplet: where each sub-component can be subdivided into refined values.	Multiple degrees for each attribute value under two dimensions or aspects.
Uncertainty Modeling	Handles more granular indeterminacy using refined degrees.	Manages uncertainty through symbolic aggregation across dual attributes.
Mathematical Complexity	Moderate; primarily additive/multiplicative rules extended from neutrosophy.	Higher; uses complex symbolic operators, set relationships, and contradiction degrees.
Use in Cryptography	Applied in generalized RSA, El-Gamal, and key-exchange models.	Emerging potential; less explored in cryptographic schemes but useful in decision layers.
Logical Basis	Based on neutrosophic logic: true, indeterminate, false.	Based on plithogenic logic: contradictory degrees + symbolic semantics.
Flexibility	High in modeling uncertain numeric data.	Very high in modeling multi-attribute symbolic reasoning.
Application Areas	Cryptography, decision-making, data fusion.	Symbolic AI, fuzzy decision systems, theoretical frameworks.

- **Proposed Cryptosystem Based on Symbolic 2-Plithogenic integers**

Consider the algebras:

$2 - SP\varphi = \{\sum_{i=0}^{15}(a_i + b_i P_1 + c_i P_2)\, v_i \,;\, a_i, b_i, c_i \in 2 - SP\mathfrak{R}\}$, $2 - SP\varphi_p = \{\sum_{i=0}^{15}(a_i + b_i P_1 + c_i P_2)\, v_i \,;\, a_i, b_i, c_i \in 2 - SP\mathfrak{R}_p\}$, $2 - SP\varphi_q = \{\sum_{i=0}^{15}(a_i + b_i P_1 + c_i P_2)\, v_i \,;\, a_i, b_i, c_i \in 2 - SP\mathfrak{R}_q\}$ where $2 - SP\mathfrak{R} = Z(P_1, P_2)[x + yP_1 + zP_2]/((x + yP_1 + zP_2)^N - 1)$, $2 - SP\mathfrak{R}_p = Z_p(P_1, P_2)[x + yP_1 + zP_2]/((x + yP_1 + zP_2)^N - 1)$, and 2-SP$\mathfrak{R}_q = Z_q(P_1, P_2)[x + yP_1 + zP_2]/((x + yP_1 + zP_2)^N - 1)$ be truncated polynomials rings with symbolic 2-plithogenic 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:

DOI: https://doi.org/10.54216/IJNS.270217

$L_F = \{(a+bP_1+cP_2)_0\,(x+yP_1+zP_2)+(a+bP_1+cP_2)_1(x+yP_1+zP_2)v_1+\cdots+(a+bP_1+cP_2)_{15}(x+yP_1+zP_2)v_{15} | (a+bP_1+cP_2)_i(x+yP_1+zP_2) \in 2-SP\mathfrak{R}$ satisfies $\ell(d_f, d_f-1)\}$,

$L_G = \{(m+nP_1+tP_2)_0\,(x+yP_1+zP_2)+(m+nP_1+tP_2)_1(x+yP_1+zP_2)v_1+\cdots+(m+nP_1+tP_2)_{15}(x+yP_1+zP_2)v_{15} | (m+nP_1+tP_2)_i(x+yP_1+zP_2) \in 2-SP\mathfrak{R}$ satisfy $\ell(d_g, d_g)\}$,

$L_S = \{(f+gP_1+hP_2)_0\,(x+yP_1+zP_2)+(f+gP_1+hP_2)_1(x+yP_1+zP_2)v_1+\cdots+(f+gP_1+hP_2)_{15}(x+yP_1+zP_2)v_{15} | (f+gP_1+hP_2)_i(x+yP_1+zP_2) \in 2-SP\mathfrak{R}$ satisfy $\ell(d_s, d_s)\}$,

$L_W = \{(r+sP_1+kP_2)_0\,(x+yP_1+zP_2)+(r+sP_1+kP_2)_1(x+yP_1+zP_2)v_1+\cdots+(r+sP_1+kP_2)_{15}(x+yP_1+zP_2)v_{15} | (r+sP_1+kP_2)_i(x+yP_1+zP_2) \in 2-SP\mathfrak{R}$ satisfy $\ell(d_w, d_w)\}$,

$L_M = \{\{(q+pP_1+sP_2)_0\,(x+yP_1+zP_2)+(q+pP_1+sP_2)_1(x+yP_1+zP_2)v_1+\cdots+(q+pP_1+sP_2)_{15}(x+yP_1+zP_2)v_{15})|$ coefficients of $(q+pP_1+sP_2)_i(x+yP_1+zP_2)$

- **Key Generation**

we can generate a public key as follows:
choose $K \in L_{F,}\ J \in L_G,\ I \in L_S$ *and* $U \in L_R$ where K invertible modulo p and q denoted by ${K_p}^{-1}$ *and* ${K_q}^{-1}$ respectively. The public key H computed by the formula
$H \equiv {K_q}^{-1} * (J * I) \quad (mod\ q)$.
We can summarize the method of generating the key with the following pseudocode (1):

Pseudocode 1: demonstrate the key generation phase of the plithogenic method:
Input: N, p, q, d_f, d_g, d_s.
Output: H
Compute $K_q^{-1} = inverse\ of\ K\ (mod\ q)$.
Compute $H_1 \equiv J * I\ (mod\ q)$.
Compute $H \equiv {K_q}^{-1} * H_1\ (mod\ q)$
End.

Encryption

Let the original text be (C) to encrypted text, choose randomly $D \in L_W$ and use the following formula to getting the ciphertext E

$E \equiv\ pH * D + C \quad (mod\ q)$.
Where the coefficients are taken of E from $\left(-\frac{p}{2},\frac{p}{2}\right]$.
Decryption

For the recipient to recover the original text C through the encrypted text E, he\she must follow the following steps:

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

$$\begin{aligned} &\equiv K * (pH * D + C)\ (mod\ q) \\ &\equiv p(K * {K_q}^{-1} * J * I * D) + (K * C) \quad (mod\ q) \\ &\equiv p(J * I * D) + (F * C) \quad (mod\ q). \end{aligned}$$

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

Take $\delta\ \equiv \beta\ (mod\ p)$.
$K_p^{-1} * \delta\ (mod\ p)\ \equiv K_p^{-1} * (K * C)\ (mod\ p)$
$\equiv C\ \ (mod\ p)$.
Performance Analysis of the plithogenic method
.
Execution Time
Table (1) shows the execution time of the plithogenic method according to the addition and multiplication of plithogenic polynomials in the all phases.

DOI: https://doi.org/10.54216/IJNS.270217

Table 1: Execution time of plitho-version

Phase	Time
Key generation	$(4096o_1)^3$
Encryption	$(\mathbf{256o_1} + \mathbf{16o_0})^3$
Decryption	$(4352o_1 + 16o_{0)}{}^3$
Total	$(4448o_1 + 23o_0)^3$

Where o_1, o_0 are the time of multiplication and addition of polynomials respectively.

- **Comparative Between HXDTRU and the plithogenic version**

Table 2: Space of key of the two methods

Cryptosystem	Space of key
Plitho-version	$\left(\frac{N!}{(d_G\,!)^2\,(N-2d_G)!}\right)^{96}$
HXDTRU	$\left(\frac{N!}{(d_G!\,)^2\,(N-2d_G)!}\right)^{16}$

Table 3: Space of message of HXDHS and HXDTRU

Cryptosystem	Space of message
Plitho-version	$\left(\frac{N!}{(d_W!\,)^2\,(N-2d_W)!}\right)^{48}$
HXDTRU	$\left(\frac{N!}{(d_W!\,)^2\,(N-2d_W)!}\right)^{16}$

Table 4: Generic parameters

N	d_G	d_S	d_W
108	$10+10P_1+10P_2$	$10+10P_1+10P_2$	$3+3P_1+P_2$
124	$18+8P_1+5P_2$	$18+8P_1+5P_2$	$8+P_1+7P_2$
144	$10+P_1+3P_2$	$10+P_1+3P_2$	$8+3P_1+11P_2$
144	$23+8P_1+2P_2$	$23+8P_1+2P_2$	$18+P_1+P_2$

DOI: https://doi.org/10.54216/IJNS.270217

171	16+P_1 + P_2	16+P_1 + 9P_2	16+3P_1 + 3P_2
171	25+7P_1 + 11P_2	25+7P_1 + 11P_2	20+P_1 + 11P_2
206	18+P_1 + 21P_2	18+P_1 + 21P_2	16+3P_1 + P_2
206	32+13P_1 + 14P_2	32+13P_1 + 14P_2	20+P_1 + 7P_2

Table 5: Key space security of both methods

Key Space of $\boldsymbol{HDXTRU}$	Key Space of $\boldsymbol{plitho-version}$
$\mathbf{3.1215 \times 10^{440}}$	8.4687×10^{1861}
$\mathbf{1.3463 \times 10^{705}}$	3.6415×10^{2960}
$\mathbf{7.5241 \times 10^{563}}$	3.1262×10^{1843}
$\mathbf{3.2471 \times 10^{821}}$	1.1657×10^{3408}
$\mathbf{5.2215 \times 10^{699}}$	7.9004×10^{3003}
$\mathbf{1.4581 \times 10^{945}}$	4.1891×10^{3830}
$\mathbf{7.97271 \times 10^{802}}$	3.92391×10^{3391}
$\mathbf{1.6778 \times 10^{1205}}$	6.9989×10^{4616}

Table 6: Message space security of both methods

$\boldsymbol{Message\ space\ of\ HDXTRU}$	$\boldsymbol{Message\ space\ of\ plitho-version}$
$\mathbf{3.1215 \times 10^{440}}$	8.4687×10^{1861}
$\mathbf{1.3463 \times 10^{705}}$	3.6415×10^{2960}
$\mathbf{7.5241 \times 10^{563}}$	3.1262×10^{1843}
$\mathbf{3.2471 \times 10^{821}}$	1.1657×10^{3408}
$\mathbf{5.2215 \times 10^{699}}$	7.9004×10^{3003}
$\mathbf{1.4581 \times 10^{945}}$	4.1891×10^{3830}
$\mathbf{7.97271 \times 10^{802}}$	3.92391×10^{3391}
$\mathbf{1.6778 \times 10^{1205}}$	6.9989×10^{4616}

DOI: https://doi.org/10.54216/IJNS.270217

Table 7: Execution time of both methods

Cryptosystem	Execution time
Plitho-version	$(4448o_1 + 23o_0)(4467o_1 + 213o_0)$
HXDTRU	$8704o_1 + 32o_0$

- **Proposed Cryptosystem Based On refined neutrosophic integers**

Consider the algebras:

$R(I_1, I_2)\varphi = \{\sum_{i=0}^{15}(a_i + b_iI_1 + c_iI_2)\, v_i\, ;\ a_i, b_i, c_i \in R(I_1, I_2)\mathfrak{R}\}$, $R(I_1, I_2)\varphi_p = \{\sum_{i=0}^{15}(a_i + b_iI_1 + c_iI_2)\, v_i\, ;\ a_i, b_i, c_i \in R(I_1, I_2)\mathfrak{R}_p\}$, $R(I_1, I_2)\varphi_q = \{\sum_{i=0}^{15}(a_i + b_iI_1 + c_iI_2)\, v_i\, ;\ a_i, b_i, c_i \in R(I_1, I_2)\mathfrak{R}_q\}$ where $R(I_1, I_2)\mathfrak{R} = Z(I_1, I_2)[x + yI_1 + zI_2]/((x + yI_1 + zI_2)^N - 1)$, $R(I_1, I_2)\mathfrak{R}_p = Z_p(I_1, I_2)[x + yI_1 + zI_2]/((x + yI_1 + zI_2)^N - 1)$, and $R(I_1, I_2)\mathfrak{R}_q = Z_q(I_1, I_2)[x + yI_1 + zP_2]/((x + yI_1 + zI_2)^N - 1)$ be truncated polynomials rings with symbolic 2-plithogenic 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:

$L_F = \{(a + bI_1 + cI_2)_0\,(x + yI_1 + zI_2) + (a + bI_1 + cI_2)_1(x + yI_1 + zI_2)v_1 + \cdots + (a + bI_1 + cI_2)_{15}(x + yI_1 + zI_2)v_{15} | (a + bI_1 + cI_2)_i(x + yI_1 + zI_2) \in R(I_1, I_2)\mathfrak{R}$ satisfies $\ell(d_f, d_f - 1)\}$,

$L_G = \{(m + nI_1 + tI_2)_0\,(x + yI_1 + zI_2) + (m + nI_1 + tI_2)_1(x + yI_1 + zI_2)v_1 + \cdots + (m + nI_1 + tI_2)_{15}(x + yI_1 + zI_2)v_{15} |\ (m + nI_1 + tI)_i(x + yI_1 + zI_2) \in R(I_1, I_2)\mathfrak{R}$ satisfy $\ell(d_g, d_g)\}$,

$L_S = \{(f + gI_1 + hI_2)_0\,(x + yI_1 + zI_2) + (f + gI_1 + hI_2)_1(x + yI_1 + zI_2)v_1 + \cdots + (f + gI_1 + hI_2)_{15}(x + yI_1 + zI_2)v_{15} | (f + gI_1 + hI_2)_i(x + yI_1 + zI) \in R(I_1, I_2)\mathfrak{R}$ satisfy $\ell(d_s, d_s)\}$,

$L_W = \{(r + sI_1 + kI_2)_0\,(x + yI_1 + zI_2) + (r + sI_1 + kI_2)_1(x + yI_1 + zI_2)v_1 + \cdots + (r + sI_1 + kI_2)_{15}(x + yI_1 + zI_2)v_{15} | (r + sI_1 + kI_2)_i(x + yI_1 + zI_2) \in R(I_1, I_2)\mathfrak{R}$ satisfy $\ell(d_w, d_w)\}$,

$$L_M = \{\{(q + pI_1 + sI_2)_0\,(x + yI_1 + zI) + (q + pI_1 + sP_2)_1(x + yI_1 + zI_2)v_1 + \cdots + (q + pI_1 + sI_2)_{15}(x + yI_1 + zI_2)v_{15})\}$$

Key Generation

we can generate a public key as follows:
choose $K \in L_{F,}\ J \in L_G,\ I \in L_S$ *and* $U \in L_R$ where K invertible modulo p and q denoted by $K_p{}^{-1}$ *and* $K_q{}^{-1}$ respectively. The public key H computed by the formula
$H \equiv\ K_q{}^{-1} * (J * I) \quad (mod\ q)$.
We can summarize the method of generating the key with the following pseudocode (1):

Encryption

Let the original text be (C) to encrypted text, choose randomly $D \in L_W$ and use the following formula to getting the ciphertext E

$E \equiv\ pH * D + C \quad (mod\ q)$.
Where the coefficients are taken of E from $\left(-\frac{p}{2}, \frac{p}{2}\right]$.

Decryption

For the recipient to recover the original text C through the encrypted text E, he\she must follow the following steps:

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

$\equiv K * (pH * D + C)\ \ (mod\ q)$
$\equiv p(K * K_q{}^{-1} * J * I * D) + (K * C) \quad (mod\ q)$
$\equiv p(J * I * D) + (F * C) \quad (mod\ q)$.
Where the coefficients of β belong to interval $\left(-\frac{q}{2}, \frac{q}{2}\right]$.

Take $\delta\ \equiv \beta\ (mod\ p)$.
$K_p^{-1} * \delta\ (mod\ p)\ \equiv K_p^{-1} * (K * C)\ (mod\ p)$
$\equiv C\ \ (mod\ p)$.

DOI: https://doi.org/10.54216/IJNS.270217

Performance Analysis of the refined neutrosophic method

Execution Time

Table (1) shows the execution time of the refined neutrosophic method according to the addition and multiplication of refined neutrosophic polynomials in the all phases.

Table 8: Execution time of refined neutrosophic-version

Phase	**Time**
Key generation	$(4096o_1)^3$
Encryption	$(\mathbf{256}\boldsymbol{o_1} + \mathbf{16}\boldsymbol{o_0})^3$
Decryption	$(4352o_1 + 16o_{0)}{}^3$
Total	$(4448o_1 + 23o_0)^3$

Where o_1, o_0 are the time of multiplication and addition of polynomials respectively.

- **Comparative between HXDTRU and the refined neutrosophic version**

Table 9: Space of key of the two methods

Cryptosystem	Space of key
Plitho-version	$\left(\frac{N_!}{(d_G\,!)^2\,(N-2d_G)!}\right)^{96}$
Refined neutrosophic version	$\left(\frac{N_!}{(d_G\,!)^2\,(N-2d_G)!}\right)^{96}$

Table 10: Space of message of HXDHS and HXDTRU

Cryptosystem	Space of message
Plitho-version	$\left(\frac{N_!}{(d_W!\,)^2\,(N-2d_W)!}\right)^{48}$
Refined neutrosophic version	$\left(\frac{N_!}{(d_W!\,)^2\,(N-2d_W)!}\right)^{48}$

DOI: https://doi.org/10.54216/IJNS.270217

Table 11: Generic parameters

N	d_G	d_S	d_W
108	10+10I_1 + 10I_2	10+10I_1 + 10I_2	3+3I_1 + I_2
124	18+8I_1 + 5I_2	18+8I_1 + 5I_2	8+I_1 + 7I_2
144	10+I_1 + 3I_2	10+I_1 + 3I_2	8+3I_1 + 11I_2
144	23+8I_1 + 2I_2	23+8I_1 + 2I_2	18+I_1 + I_2
171	16+I_1 + I_2	16+I_1 + 9I_2	16+3I + 3I_2
171	25+7I_1 + 11I_2	25+7I_1 + 11I_2	20+I_1 + 11I_2
206	18+I_1 + 21I_2	18+I_1 + 21I_2	16+3I_1 + I_2
206	32+13I_1 + 14I_2	32+13I_1 + 14I_2	20+I_1 + 7I_2

Table 12: Key space security of both methods

Key Space of $\boldsymbol{refined\ version}$	**Key Space of** $\boldsymbol{plitho - version}$
$\mathbf{8.4687 \times 10^{1861}}$	8.4687×10^{1861}
$\mathbf{3.6415 \times 10^{2960}}$	3.6415×10^{2960}
$\mathbf{3.1262 \times 10^{1843}}$	3.1262×10^{1843}
$\mathbf{1.1657 \times 10^{3408}}$	1.1657×10^{3408}
$\mathbf{7.9004 \times 10^{3003}}$	7.9004×10^{3003}
$\mathbf{4.1891 \times 10^{3830}}$	4.1891×10^{3830}
$\mathbf{3.92391 \times 10^{3391}}$	3.92391×10^{3391}
$\mathbf{6.9989 \times 10^{4616}}$	6.9989×10^{4616}

Table 13: Message space security of both methods

Message space of $\boldsymbol{refined\ version}$	***Message space of*** $\boldsymbol{plitho - version}$
$\mathbf{8.4687 \times 10^{1861}}$	8.4687×10^{1861}
$\mathbf{3.6415 \times 10^{2960}}$	3.6415×10^{2960}
$\mathbf{3.1262 \times 10^{1843}}$	3.1262×10^{1843}

DOI: https://doi.org/10.54216/IJNS.270217

$\mathbf{1.1657 \times 10^{3408}}$	1.1657×10^{3408}
$\mathbf{7.9004 \times 10^{3003}}$	7.9004×10^{3003}
$\mathbf{4.1891 \times 10^{3830}}$	4.1891×10^{3830}
$\mathbf{3.92391 \times 10^{3391}}$	3.92391×10^{3391}
$\mathbf{6.9989 \times 10^{4616}}$	6.9989×10^{4616}

Table 14: Execution time of both methods

Cryptosystem	Execution time
Plitho-version	$(4448o_1 + 23o_0)(4467o_1 + 213o_0)$
Refined version	$4448o_1 + 23o_0)(4467o_1 + 213o_0)$

3. Conclusion

In this work, we used the symbolic 2-plithogenic integers and refined neutrosophic numbers to get a generalized version of HXDTRU with a strict approach includes three symbolic 2-plithogenic and refined neutrosophic private keys with one public symbolic 2-pithogenic and refined neutrosophic key to improve the security. In addition, we analysed the complexity of the generalized systems numerically.

Acknowledgement: The authors extend their appreciation to the Arab Open University for supporting this work.

References

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

[2] Y. A. Alhasan *et al.*, "On a novel security algorithm for the encryption of 3x3 fuzzy matrices with rational entries based on the symbolic 2-plithogenic integers and El-Gamal algorithm," *Int. J. Neutrosophic Sci.*, vol. 21, no. 1, pp. 88–95, 2023, doi: 10.54216/IJNS.210108.

[3] Allouf, "A Review on the Neutrosophic Number Theory Based Cryptography and Neutrosophic Public Key Crypto-Systems," *Int. J. Adv. Appl. Comput. Intell*, pp. 30-35, 2024, doi: https://doi.org/10.54216/IJAACI.060103.

[4] M. Abobala, H. Sankari, and M. B. Zeina, "On Novel Security Systems Based on the 2-Cyclic Refined Integers and the Foundations of 2-Cyclic Refined Number Theory," *J. Fuzzy Extension Appl.*, 2024.

[5] M. Abobala and A. Allouf, "On A Novel Security Scheme for The Encryption and Decryption Of 2×2 Fuzzy Matrices with Rational Entries Based on The Algebra of Neutrosophic Integers and El-Gamal Crypto-System," *Neutrosophic Sets Syst.*, vol. 54, 2023.

[6] H. R. Yassein and N. M. Al-Saidi, "HXDTRU cryptosystem based on hexadecnion algebra," in *Proc. 5th Int. Cryptol. Inf. Secur. Conf.*, Kota Kinabalu, Malaysia, 2016, vol. 31.

[7] Z. Djedid *et al.*, "On solutions of differential and integral equations using new fixed point results in cone Eb-metric spaces," *Partial Differ. Equations Appl. Math.*, vol. 8, p. 100559, 2023.

[8] D. Alrwashdeh *et al.*, "On Two Novel Generalized Versions of Diffie-Hellman Key Exchange Algorithm Based on Neutrosophic and Split-Complex Integers and their Complexity Analysis," *Int. J. Neutrosophic Sci.*, pp. 01-10, 2025, doi: https://doi.org/10.54216/IJNS.250201.

[9] F. Smarandache, *Plithogeny, Plithogenic Set, Logic, Probability, and Statistics*. Brussels, Belgium: Pons Editions, 2017.

[10] R. Saadeh *et al.*, "Linear Fractional Differential Equations for Modeling Nonlinear Hydro Environmental Phenomena," *Eng. Lett*, vol. 33, no. 6, 2025.

[11] M. Celik and A. Hatip, "On The Refined AH-Isometry And Its Applications In Refined Neutrosophic Surfaces," *Galoisica J. Math. Struct. Appl.*, 2022.

[12] E. O. Adeleke, A. A. A. Agboola, and F. Smarandache, "Refined Neutrosophic Rings I", *Int. J. Neutrosophic Sci.*, vol. 2, no. 2, pp. 77-81, 2020.

DOI: https://doi.org/10.54216/IJNS.270217