Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 13** : 1–6.
ISSN-0037-8712
doi:10.5269/bspm.79987

Designing a Secure Cryptosystem via Neutrosophic Integers Octonions Algebra

Majida H. Majeed, Abdullah Mhmood Jasim and Hassan Rashed Yassein

ABSTRACT: The development of methods and technology for exchanging information and storing, or what is known as data transfer over a network from one party to another, has made the security of this and information and data a paramount concern and a vital objective for all countries and organizations. This paper aims to design a more secure encryption system via algebra of octonion with neutrosophic integer coefficients.

Keywords: Neutrosophic integer, OTRU, octonion algebra, analysis of security.

Contents

1. Introduction

In 1998, Hoffstein et al. proposed the first public key encryption system NTRU used a truncated polynomials ring with integer coefficients. As a result of its efficiency, many researchers interested in the field of data encryption introduced new methods based on the truncated polynomials ring to keep pace with the development of data transmission [4].

The OTRU cryptosystem, proposed by Malekian and Zakerolhosseini in 2010 based on algebra of octonion with bases $\{\xi_0, \xi_1, \xi_2, \xi_3, \ \xi_4, \xi_5, \xi_6, \xi_7\}$ [5]. A comparison was presented between the NTRU and two of its enhancements in terms of level of level by Yassein and Al-Saidi in 2017 [8]. The NTRsh encryption was designed in 2021 by Yassein and Shahhadi via a tripternion algebra construction instead of the structure used in the original system [6]. The QOTRU system was proposed by Abo-Alsood and Yassein through the use of a subalgebraic structure from octonion algebra to improve the efficiency of the original system [1]. In 2022, Abo-Alsood and Yassein developed the NTRU system by introducing a more efficient multi-dimensional encryption system suitable for many uses [2].

In 2023, Yassein et al. [7] using HH-real algebra with different mathematical structure to design QuiTRU system. If I an indeterminacy with the property $I^2 = I$, then $Z(I) = \{x + yI; x, y \in Z\}$ is said to be neutrosophic ring of integers, the elements of $Z(I)$ are said to be neutrosophic integers where Z integer numbers ring [3].

2. Proposed NSOT Cryptosystem

The proposed system NSOT , which is an improvement on the OTRU system, relies on the same parameters, algebras, and subsets as the OTRO system, but the coefficients of the polynomials are neutrosophic integers.

2020 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted November 08, 2025. Published April 28, 2026.

Let $\mathfrak{n} = Z[\mathfrak{b}]/(\mathfrak{b}^N - 1), \mathfrak{n}_p = Z_p[\mathfrak{b}]/(\mathfrak{b}^N - 1)$ and $\mathfrak{n}_q = Z_q[\mathfrak{b}]/(\mathfrak{b}^N - 1)$ be a truncated polynomial rings such that $\mathfrak{n}_p and \mathfrak{n}_q$ are truncated polynomial ring modulo p and q respectively. Define three algebras of neutrosophic integers octonion which are defined as:

$$\gamma = \left\{ \sum_{i=0}^{7} (\mathcal{L}_{i,0}(v) + \mathcal{L}_{i,1}(v) I)\xi_i | \mathcal{L}_{i,\mathfrak{Z}}(v) \in \mathfrak{n}, \mathfrak{Z} = 0, 1 \right\}$$

$$\gamma_p = \left\{ \sum_{i=0}^{7} (\mathcal{L}_{i,0}(v) + \mathcal{L}_{i,1}(v) I)\xi_i | \mathcal{L}_{i,\mathfrak{Z}}(v) \in \mathfrak{n}, \mathfrak{Z} = 0, 1 \right\}$$

$$\gamma_q = \left\{ \sum_{i=0}^{7} (\mathcal{L}_{i,0}(v) + \mathcal{L}_{i,1}(v) I)\xi_i | \mathcal{L}_{i,\mathfrak{Z}}(v) \in \mathfrak{n}, \ \mathfrak{Z} = 0, 1 \right\}$$

As well as five subsets of γ defined by the form: $\mathcal{T}_{\mathcal{L}} = \{\sum_{i=0}^{7} (\mathcal{L}_{i,0}(v) + \mathcal{L}_{i,1}(v) I)\xi_i$, such that $f_{\sigma,\tau}(v)$ has the number of coefficients equal to 1 is greater than the number equal to -1 by 1, and the other values 0$\}$,
$\mathcal{T}_{\mathcal{G}} = \{\sum_{i=0}^{7} (\mathcal{G}_{i,0}(v) + \mathcal{G}_{i,1}(v) I)\xi_i$, such that $\mathcal{G}_{\sigma,\tau}(v)$ has the same number of coefficients, equal to 1 and -1, and the other values 0$\}$,
$\mathcal{T}_{\mathfrak{r}} = \{\sum_{i=0}^{7} (\mathfrak{r}_{i,0}(v) + \mathfrak{r}_{i,1}(v) I)\xi_i$, such that $\mathfrak{r}_{\sigma,\tau}(v)$ has the same number of coefficients, equal to 1 and -1, and the other values 0$\}$,
$\mathcal{T}_{\varpi} = \{\sum_{i=0}^{7} (\varpi_{i,0}(v) + \varpi_{i,1}(v) I)\xi_i$, such that $\varpi_{\sigma,\tau}(v)$ has the same number of coefficients, equal to 1 and -1, and the other values 0$\}$,
$\mathcal{T}_{\mathfrak{w}} = \{\sum_{i=0}^{7} (\mathfrak{w}_{i,0}(v) + \mathfrak{w}_{i,1}(v) I)\xi_i$, such that the coefficients between $-p/2$ and $p/2\}$.

The phase that the NSOT goes through are as follows:

2.1. Key Generation

To build the NSOT system, the receiver must generate a public key $\mathfrak{H}$ using two private keys $\mathcal{L} \in \mathcal{T}_{\mathcal{L}}$ and $\mathcal{G} \in \mathcal{T}_{\mathcal{G}}$ send its to the sender to be used in encrypting the text, as in the Algorithm 1.

Algorithm 1 Generate of key

Input: $d_{\mathcal{L}}, d_{\mathcal{G}}, N, q$
Output: $\mathfrak{H}$
Compute: $\mathcal{L}_q^{-1} = inverse\ \mathcal{L}\ mod\ q$
Compute: $\mathfrak{H} = \mathcal{L}_q^{-1} * \mathcal{G}\ mod\ q$
End.

Where d is the number of coefficients that equal one.

2.2. Encryption

To encrypt plaintext $\mathfrak{w}$, the sender converts it to form in $\mathcal{T}_{\mathfrak{w}}$ and then chooses two private keys $\mathfrak{r} \in \mathcal{T}_{\mathfrak{r}}, \varpi \in \mathcal{T}_{\varpi}$, using the public key $\mathfrak{H}$ according to Algorithm 2.

Algorithm 2 Encryption.

Input: $N, p, q, d_{\mathfrak{r}}, d_{\varpi}, h, \mathfrak{w}$
Output: ciphertext $\mathfrak{c}$
Compute: $\mathfrak{c} = p(\varpi + \mathfrak{H} * \mathfrak{r}) + \mathfrak{w}(mod\ q)$
  for $\eta = 1$ to N **do**
    for $i = 0$ to 7 **do**
      for $\mathfrak{k} = 0$ to 1 **do**
        if $\mathfrak{c}_{i,\mathfrak{k}} <= {}^{-q}/_{2}$ **then**
          $\mathfrak{c}_{i,\mathfrak{k}} = q + \mathfrak{c}_{i,\mathfrak{k}}$
        else
          if $\mathfrak{c}_{i,\mathfrak{k}} > {}^{q}/_{2}$ **then**
            $\mathfrak{c}_{i,\mathfrak{k}} = \mathfrak{c}_{i,\mathfrak{k}} - q$
          end if
        end if
      end for
    end for
  end for
  End.

2.3. Decryption

Restoring clear text requires the recipient to apply Algorithm 3 steps.

Algorithm 3 Decryption phase.

Input: $N, p, q, \mathfrak{c}$
Output: the message $\mathfrak{w}$
Compute: $\mathfrak{e} = \mathcal{L} * (e * \mathcal{L})(mod\ q)$
  for $\eta = 1$ to N **do**
    for $i = 0$ to 7 **do**
      for $\mathfrak{k} = 0$ to 1 **do**
        if $\mathfrak{e}_{i,\mathfrak{k}} <= {}^{-q}/_{2}$ **then**
          $\mathfrak{e}_{i,\mathfrak{k}} = q + \mathfrak{e}_{i,\mathfrak{k}}$
        else
          if $\mathfrak{e}_{i,\mathfrak{k}} > {}^{q}/_{2}$ **then**
            $\mathfrak{e}_{i,\mathfrak{k}} = \mathfrak{e}_{i,\mathfrak{k}} - q$
          end if
        end if
      end for
    end for
  end for
Compute: $\mathbb{S} = \mathfrak{e}\ \ (mod\ p)$
Compute: $\mathfrak{U} \equiv (\mathcal{L}_p^{-1} * \mathbb{S}) * \mathcal{L}_p^{-1} (mod\ p)$
  for $\eta = 1$ to N **do**
    for $i = 0$ to 7 **do**
      for $\mathfrak{k} = 0$ to 1 **do**
        if $\mathfrak{U}_{i,\mathfrak{k}} <= {}^{-p}/_{2}$ **then**
          $\mathfrak{U}_{i,\mathfrak{k}} = p + \mathfrak{U}_{i,\mathfrak{k}}$
        else
          if $\mathfrak{U}_{i,\mathfrak{k}} > {}^{p}/_{2}$ **then**
            $\mathfrak{U}_{i,\mathfrak{k}} = \mathfrak{U}_{i,\mathfrak{k}} - p$
          end if
        end if
      end for
    end for
  end for
  $\mathfrak{w} = \mathfrak{U}$
  End.

3. Security of Analysis of NSOT

The security level of an encryption system depends on the strength of the private keys, both in the public key and the encrypted message. An unauthorized party attempts to access the plaintext by knowing one of the private keys of the public key and the two private keys of the encrypted message. When the attacker targets the smallest of the two private key combinations, $\mathcal{L} \in \mathcal{T}_{\mathcal{L}}$ and $\mathcal{G} \in \mathcal{T}_{\mathcal{G}}$ (assuming combination $\mathcal{T}_{\mathcal{G}}$ is the smallest), the space within combination $\mathcal{T}_{\mathcal{G}}$ is called the key security level, calculated as follows:

$$|L_f| = \left(\binom{N}{d_{\mathcal{G}}} \binom{N - d_{\mathcal{G}}}{d_{\mathcal{G}}} \right)^{16} = \left(\frac{N!}{\left(d_{\mathcal{G}}!\right)^2 \left(N - 2d_{\mathcal{G}}\right)!} \right)^{16},$$

However, if the attacker attempts to decipher the encrypted message and accesses the two private keys, $\varpi \in \mathcal{T}_{\varpi}$ and $\mathfrak{r} \in \mathcal{T}_{\mathfrak{r}}$, which constitute the message security level, the calculation is as follows:

$$\left(\binom{N}{d_{\varpi}} \binom{N - d_{\varpi}}{d_{\varpi}} \binom{N}{d_{\mathfrak{r}}} \binom{N - d_{\mathfrak{r}}}{d_{\mathfrak{r}}} \right)^{16} = \left(\frac{N!}{(d_{\varpi}!)^2 (N - 2d_{\varpi})!} \right)^{16} \left(\frac{N!}{(d_{\mathfrak{r}}!)^2 (N - 2d_{\mathfrak{r}})!} \right)^{16},$$

4. Comparison of Security Between NSOT and OTRU

Tables 1 and 2 show the comparison between the proposed NSOT encryption system and the original OTRU system with respect to the key and message levels.

Table 1: Security space of key of NSOT and OTRU

System	Security space of key
NSOT	$\left(\frac{N!}{\left(d_{\mathcal{G}}!\right)^2(N-2d_{\mathcal{G}})!}\right)^{16}$
OTRU	$\left(\frac{N!}{(d_g!)^2(N-2d_g)!}\right)^{8}$

Table 2: Security space of message of NSOT and OTRU

System	Security space of message
NSOT	$\left(\frac{N!}{(d_{\mathfrak{r}}!)^2(N-2d_{\mathfrak{r}})!}\right)^{16}\left(\frac{N!}{(d_{\varpi}!)^2(N-2d_{\varpi})!}\right)^{16}$
OTRU	$\left(\frac{N!}{(d_r!)^2(N-2d_r)!}\right)^{8}$

Therefore, the new system provides a higher level of security compared to OTRU in terms of key and message.

5. Conclusions

The combined structure of Neutrosophic integers and octal algebra in the proposed system offers a significant improvement in security compared to the original OTRU method. Furthermore, it allows for the simultaneous transmission of up to 16 messages, making it suitable for large datasets. Additionally, the original method becomes a special case of the proposed system by setting the I coefficients to zero.

References

1. 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*, 1999(1):012097, 2021.
2. H.H. Abo-Alsood and H.R. Yassein. Analogue to NTRU public key cryptosystem by multi-dimensional algebra with high security. *AIP Conference Proceedings*, 2386(1):060006, 2022.
3. M. Abobala. Foundations of neutrosophic number theory. *Neutrosophic Sets and Systems*, 39(1):10, 2021.
4. J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In *International Algorithmic Number Theory Symposium*, pages 267–288. Springer, 1998.
5. E. Malekian and A. Zakerolhosseini. OTRU: A Non-Associative and High Speed Public Key Cryptosystem. In *2010 15th CSI International Symposium on Computer Architecture and Digital Systems (CADS)*, pages 83–90, Tehran, Iran, September 2010. IEEE.
6. S. H. Shahhadi and H. R. Yassein. NTR$_{SH}$: A new secure variant of NTRUEncrypt based on tripternion algebra. *Journal of Physics: Conference Series*, 1999(1):012092, 2021.
7. H. R. Yassein, H. N. Zaky, H. H. Abo-alsoo, I. A. Mageed, and W. I. ElSobky. QuiTRU: Design secure variant of ntruencrypt via a new multi-dimensional algebra. *Applied Mathematics and Information Sciences an International Journal*, 17(1):49–53, 2023.
8. H.R. Yassein and N.M. Al-Saidi. A comparative performance analysis of NTRU and its variant cryptosystems. In *Proceeding of International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, pages 115–120, Sulaymaniyah, Iraq, April 2017. IEEE.

Majida H. Majeed,

Al-Qadisiyah Education Directorate,

Al-Qadisiyah, Iraq.

E-mail address: majida.majeed@qu.edu.iq

and

Abdullah Mhmood Jasim,

Department of Mathematics,
College of Education-Tuzkhurmatu, Tikrit University
Iraq.
E-mail address: abdullah.jasem122@st.tu.edu.iq

and

Hassan Rashed Yassein,
Department of Mathematics,
Collage of Education, University of Al-Qadisiyah,
Iraq.
E-mail address: hassan.yaseen@qu.edu.iq