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

(3s.) **v. 2025 (43) 3** : 1–3.
ISSN-0037-8712
doi:10.5269/bspm.78627

Designing an Efficient Cryptosystem via Tripternion Algebra and Nitrosophic Integers

Alaa Kamil Jabber

ABSTRACT: The exchange of information between two parties always requires protecting its confidentiality from any unauthorized third party, which requires sending it encrypted using a secure cryptographic system. In this paper, we present a cryptosystem based on quaternion algebra with neutrosophic integer coefficients, an evolution of the QTRU system with features that make this system effective and desirable for many organizations concerned with information security.

Key Words: Neutrosophic integer, tripternion algebra, security analysis.

Contents

1. Introduction

Digital transactions have entered our daily lives through the transformation of institutions, companies, markets, and even the social level to the digital side and away from traditional or paper-based transactions. This requires that we protect this digital information from intruders by sending it according to more secure encryption systems. Currently, there are many efficient encryption systems, such as NTRU [1], which works to transfer data in an encrypted form through an insecure transmission medium. Those interested in this field have competed to develop this system by relying on algebraic structures with a specific composition and different algebraic properties. Among these developments: Gaborit et al. 2002, [2] proposed CTRU generalization of NTRU uses polynomials ring in single variable in finite field F_2 with the same public parameters. In 2006, the core algorithm for NTRU was developed using special parameter values and privacy keys by Slaibi [3]. In 2010, Nevins et al. [4] developed a like NTRU cryptosystem in which the original NTRU ring is replaced with the Einstein integers ring. Yassein and Al-Saeedi, 2017 presented a comparison between the NTRU method and three of its improvements in terms of safety level [5]. In 2019, Lyubashevsky and Seiler [6] proposed NTTRU, that generate public keys and cipher text with an approximate size of 1.25 .KB by the number theoretic transform (NTT) over the cyclotomic ring. Abo-Alsood and Yassein, 2021 [7] proposed an octonion algebra subalgebra named Qu-octonion subalgebra, which is associative and noncommutative which used to suggested QOTRU cryptosystem. Abo-Alsood and Yassein, 2022 [8] presented TOTRU, an encryption system distinguished by its security and efficiency. In 2023, Yassein et al. [9] proposed a QuiTRU via HH-real algebra with a new mathematical structure.

2. Proposed NSPTr Cryptosystem

The cryptosystem NSPTr is based on the tripternion algebra $\mathbb{T} = \{a+ bx+cx^2 \ where \ a, b, c \ \in F\}$ [10] with coefficients is the neutrosophic integers (If Z is the ring of integers numbers and I an indeterminacy with the property $I^2 = I$, then $Z(I) = \{a + bI; a, b \in Z\}$ is said to be neutrosophic ring of integers, the elements of $Z(I)$ are said to be neutrosophic integers) [11] and the general parameters in the NTRU, we know the three algebras as follows:

For any positive integers μ_1 and μ_2, we define the set

2010 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted August 25, 2025. Published October 07, 2025

$$\Gamma\left(\mu_1,\ \mu_2\right)=\left\{\alpha_0(y)+\ \alpha_1(y)x+\alpha_2(y)x^2\ \in\mathbb{T}:\begin{array}{r}\alpha_i\left(y\right) has\ \mu_1\ coefficients\ equal\ to\ 1\\ \alpha_i\left(y\right) has\ \mu_2\ coefficients\ equal\ to-1\\ \alpha_i\left(y\right)\ has\ all\ other\ coefficients\ equal\ to\ 0\end{array}\right\}$$

For $i=0,1,2,\alpha_i\left(y\right)\in\beta$, with coefficients is neutrosophic integers where

$\beta=Z[y]/(yN-1)$ is truncated polynomial ring, $\beta_p=Z_p[y]/(yN-1)$ and $\beta_q=Z_q[y]/(yN-1)$ are truncated polynomial ring modulo p and q respectively. Three tripternion algebras which are defined as:

$\mathfrak{Y}=\{\mathcal{I}_{0,0}\left(y\right)+\mathcal{I}_{0,1}\left(y\right)I+(\mathcal{I}_{1,0}\left(y\right)+\mathcal{I}_{1,1}\left(y\right)I)x+(\mathcal{I}_{2,0}\left(y\right)+\mathcal{I}_{2,1}\left(y\right)I)x^2|\mathcal{I}_{i,j}\left(y\right)\in\beta,\ i=0,1\ and\ j=0,1,2\}$,

$\mathfrak{Y}_p=\{\mathcal{I}_{0,0}\left(y\right)+\mathcal{I}_{0,1}\left(y\right)I+(\mathcal{I}_{1,0}\left(y\right)+\mathcal{I}_{1,1}\left(y\right)I)x+(\mathcal{I}_{2,0}\left(y\right)+\mathcal{I}_{2,1}\left(y\right)I)x^2|\mathcal{I}_{i,j}\left(y\right)\in\beta_p,\ i=0,1\ and\ j=0,1,2\}$,

$\mathfrak{Y}_q=\{\mathcal{I}_{0,0}\left(y\right)+\mathcal{I}_{0,1}\left(y\right)I+(\mathcal{I}_{1,0}\left(y\right)+\mathcal{I}_{1,1}\left(y\right)I)x+(\mathcal{I}_{2,0}\left(y\right)+\mathcal{I}_{2,1}\left(y\right)I)x^2|\mathcal{I}_{i,j}\left(y\right)\in\beta_q,\ i=0,1\ and\ j=0,1,2\}$,

The phases of building this method are as follows:

I. Key generation

Items $\mathfrak{k}\in\Gamma\left(\mu_1,\ \mu_{2-1}\right)$, $\mathfrak{s}\in\Gamma\left(\mu_1,\ \mu_2\right)$, and $\vartheta\in\Gamma\left(\mu_1,\ \mu_2\right)$ are randomly selected by the recipient and then the declared key is calculated as follows:

$$\mathcal{W}=\mathfrak{k}^{-1}*\mathfrak{s}*\vartheta\ mod\ p.$$

II. Encryption

To convert the original text to an encrypted one, the sender performs the following steps:

The disappearing element $\mathfrak{x}\in\Gamma\left(\mu_1,\ \mu_2\right)$ is selected

The original text $\mathfrak{M}$ is converted to the elements of the set $\mathfrak{Y}$

The encrypted text is calculated as follows:

$$\mathfrak{Z}=p\mathcal{W}*\mathfrak{x}+\ \mathfrak{M}\ mod\ q.$$

The coefficients of $\mathfrak{Z}$ must be between $-\frac{q}{2}$ and $\frac{q}{2}$.

III. Decryption

After the encrypted text reaches the recipient, he performs a number of steps until he retrieves the understood text:

$\mathfrak{k}*\mathfrak{Z}\ mod\ q\ \equiv\mathfrak{k}*(p\mathcal{W}*\mathfrak{x}+\ \mathfrak{M}\ )\ mod\ q$

. $\equiv p\mathfrak{k}*\left(\mathfrak{k}^{-1}*\mathfrak{s}*\vartheta\right)*\mathfrak{x}+\mathfrak{k}*\mathfrak{M}\ \ mod\ q$

. $\equiv p\left(\mathfrak{s}*\vartheta\right)*\mathfrak{x}+\mathfrak{k}*\mathfrak{M}\ \ mod\ q$

Convert $\mathfrak{k}*\mathfrak{Z}\ mod\ q\ to\ mod\ p\ \equiv p\left(\mathfrak{s}*\vartheta\right)*\mathfrak{x}+\mathfrak{k}*\mathfrak{M}\ mod\ p$

. $\equiv\ \mathfrak{k}*\mathfrak{M}\ mod\ p$

$\mathfrak{k}^{-1}*\left(\mathfrak{k}*\mathfrak{M}\right)\ mod\ p\equiv\ \mathfrak{M}\ \ mod\ p.$

The coefficients of last amount belong to $(-\frac{p}{2},\frac{p}{2}]$.

3. Security Analysis

Encrypted messages are vulnerable to attacks by hackers and intruders seeking to access and view the information sent by the source for other purposes, such as espionage, warfare, or to obtain money. This is achieved by testing all possible options. Assuming that the possible possibilities for the two keys, $\mathfrak{s}$ and ϑ, are less than $\mathfrak{k}$ (and given that each element is a triple element with binary coefficients), the security level of the keys is as follows:

$$\left(\binom{N}{d_{\mathfrak{s}}}\binom{N-d_{\mathfrak{s}}}{d_{\mathfrak{s}}}\binom{N}{d_{\vartheta}}\binom{N-d_{\vartheta}}{d_{\vartheta}}\right)^6=\left(\frac{N!}{\left(d_{\mathfrak{s}}!\right)^2\left(N-2d_{\mathfrak{s}}\right)!}\frac{N!}{\left(d_{\vartheta}!\right)^2\left(N-2d_{\vartheta}\right)!}\right)^6.$$

The probability of obtaining the original text through the ciphertext is also possible by considering all possible possibilities for the key $\mathfrak{x}$

$$\left(\binom{N}{d_{\mathfrak{r}}}\binom{N-d_{\mathfrak{r}}}{d_{\mathfrak{r}}}\right)^{6}=\left(\frac{N!}{(d_{\mathfrak{r}}!)^{2}\,(N-2d_{\mathfrak{r}})!}\right)^{6}.$$

This makes this system highly secure, making it popular in the job market. It is clear that NSPTr more security of NTRU, NTRSH, QTRU, and OTRU.

4. Conclusions

The dual algebraic structure of the NSPTr system (tripternion algebra and neutrosophic integers) gives it positive points through the multiple transmission of information six messages at once, whether from six different sources or from one source, which allows for the speed of sending data from multiple sources, similar to other methods that cannot send this information at the same time, in addition to the time taken to take the probabilities of each key with the rest of the other keys for each attempt. All of this makes this method more efficient, whether in terms of security or the time of sending multiple messages.

References

1. J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A ring-based public key cryptosystem*, International algorithmic number theory symposium, 1998, pp. 267–288.
2. P. Gaborit, J. Ohler, and P. Solé, *CTRU, a polynomial analogue of NTRU*, Inria, 2002.
3. T. S. Slaibi, *Improved NTRU Cryptosystem*, University of Technology, 2006.
4. M. Nevins, C. KarimianPour and A. Miri, *NTRU over rings beyond Z*, Designs, Codes and Cryptography, vol. 56, no.1, pp. 65-78, 2010.
5. Yassein, H.R., Al-Saidi, N.M.G, *A comparative performance analysis of NTRU and its variant cryptosystems International Conference on Current Research in*, Computer Science and Information Technology, 2017, pp. 115–120.
6. V. Lyubashevsky, G. Seiler, *NTTRU: Truly Fast NTRU Using NTT*, IACR Transactions on Cryptographic Hardware and Embedded Systems, no. 3, pp. 180-201, 2019.
7. 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.
8. H. H. Abo-Alsood, H. R. Yassein, *Analogue to NTRU Public Key Cryptosystem by Multi-Dimensional Algebra with High Security*, AIP Conference Proceedings, 2022, 2386, 1-6.
9. 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*, Appl. Math, vol. 17, no. 1, pp. 49–53, 2023.
10. 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.
11. M. Abobala, *Foundations of neutrosophic number theory* , Neutrosophic Sets and Systems, vol. 39, no. 1, pp. 10, 2021.

Alaa Kamil Jabber,
Department of Mathematics,
College of Education, University of Al-Qadisiyah,
Iraq.
E-mail address: alaa _ almosawi@qu.edu.iq