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

(3s.) **v. 2025 (43) 3** : 1–6.
ISSN-0037-8712
doi:10.5269/bspm.78271

Designing a Secure Mathematical Cryptosystem via Two Multi-Dimensional Algebras

Abdullah Mhmood Jasim and Hassan Rashed Yassein*

ABSTRACT: Electronic transactions of all kinds have become prevalent in many countries, and the exchange of information via social media accounts has spread to almost every corner of the world. This has opened the door to the development of highly secure and efficient encryption systems to provide reliable protection for users. In this paper, we present a new encryption system based on the combination of two multidimensional algebras, each with a dimension of eight, making this method popular in the job market.

Key Words: OTRU, octonion Algebra, KOH Algebra, security analysis.

Contents

1. Introduction

One of the most famous encryption systems used in electronic transmissions is the NTRU encryption system. NTRU is ideal for a wide range of applications which is the first encryption system that uses polynomials as a public key, where it was used truncated polynomial ring of degree $N-1$, denoted by $Z[x]/x^N-1$ presented by Hoffistein et al. in 1998 [8]. This list presents some studies to improve of the NTRU cryptosystem by changing the algebra, mathematical construction, or both. In 1997, Coppersmith and Shamir [2] apply new lattice to find either the original secret key or an alternative secret key to decryption the ciphertexts. In 2000, Leier et al. [9] introduced two different types of coding methods based on binary strands of DNA where double strand DNA strands was used to hide information. In 2002, Gaborit et al. [5] introduce CTRU generalization of NTRU which uses polynomials ring over a finite field F_2 in one variable. For the same value of N, NTRU and CTRU have the same encryption and decryption speeds.

In 2005, Coglianese and Goi [3], NTRU development submission called MaTRU as a public key cryptosystem that use a more efficient linear transformation with a security level in comparable to NTRU. In 2006, Slaibi [14] improved the basic algorithm by employing special values for parameters and privet keys. In 2007, Sari and Puri [15] use a stream of ciphers in keys of encryption and decryption. In 2010, Malekian et al. [11] QTRU, a cipher system based on NTRU, was proposed using quaternion algebra, where the basic algebraic structure of NTRU was changed to a non-commutative algebraic structure. In 2015, Majeed [10] presented cryptosystem CQTRU improvement of NTRU used on algebra of commutative quaternion, it is more four times better than resistens to attacks. In 2016, Yassein

[*] Corresponding author.

2010 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted August 04, 2025. Published October 16, 2025

and Al- Saidi [17] introduced a cooperation between NTRU and some methods. In 2023, Yassein and Ali, proposed public key cryptosystem SQNTRU [18] improvement to NTRU, the first depended on the quintuple algebra, and the second based on subalgebra of quintuple algebra. And Yassein et al. [16] proposed a QuiTRU based on an HH-real algebra with a new mathematical structure. As well as, Salman and Yassein present three new cryptosystem, TRUFT, TRUHIB, and TRUHSH by relying on multidimensional algebras to ensure a high level of security [19,13,12].

In 2024, Yassein and Fadeel, [4] constructed HAQTR which is a public key system using algebra of non-commutative quaternion with new mathematical structure. In 2025, Sahib and Yassein [1] presented a new algebra called AT to build ATTRU cryptosystem. Also, Yassein and Shahhadi, [20] design TrQtNTR public key cryptosystem, based on novel qua-tripternion algebra. Also, Hassoon, introduced two mehods KAOTR, and KSQOT via KAH-Octo algebra [6,7].

2. Octonion algebra

The octonion algebra over a field F an eight-dimension is defined as follows:

$$O = \left\{ \alpha_0 + \sum_{i=1}^{7} \alpha_i e_i : \ \alpha_0, \ldots, \alpha_7 \in F \right\}$$

with $\{r_0 = 1, r_1, r_2, r_3, r_4, r_5, r_6, r_7\}$ basis of the algebra and $\alpha_i \in F$ are scalars. The addition is performed on the basis of adding the corresponding to the usual addition of eight polynomials.

But the multiplication $(*)$ process follows the following rules:

$$e_i^2 = -1, \ i = 1, \ldots, 7$$

$e_i * e_j = -e_j * e_i$, with $i \neq j$ and $i, j = 1, \ldots, 7$
$e_i * e_j = e_k \mapsto e_{i+1} * e_{j+1} = e_{k+1}$ where $i \neq j$ and $i, j = 1, \ldots, 7$
$e_i * e_j = e_k \mapsto e_{2i} * e_{2j} = e_{2k}$, $i \neq j$ and $i, j = 1, \ldots, 7$.

It is clear that the multiplication octonion algebra is a non-commutative and a non-associative but is alternative with the multiplicative identity is 1 . The square norm $N(x)$ and conjugate $\bar{x}$ of x are defined as follow: $N(x) = x\bar{x} = \sum_{i=0}^{7} \alpha_i^2$ and $\bar{x} = \alpha_0 - \sum_{i=1}^{7} \alpha_i$ respectively. The multiplicative inverse of a non-zero element $x \in O$ defined as $(N(x))^{-1} \bar{x}$ [8].

3. KAH-Octo Algebra

Let F be a field, a KAH-Octo algebra which denoted by KO is defined by:

$$KO = \left\{ x = \sum_{i=0}^{7} x_i \beta_i \middle| \ x_0, \ldots, x_7 \in F, \beta_0 = 1 \right\},$$

with a basis $\{\beta_0 = 1, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7\}$

such that the addition, multiplication, and scalar multiplication are defined as follows:

If x, y in KO and a in F such that

$$x = \sum_{i=0}^{7} x_i \beta_i$$

and

$$y = \sum_{i=0}^{7} y_i \beta_i,$$

then

$$\begin{aligned}
&x + y = \sum_{i=0}^{7} x_i \beta_i + \sum_{i=0}^{7} y_i \beta_i = \sum_{i=0}^{7} (x_i + y_i)\, \beta_i,\\
&x * y = \sum_{i=0}^{7} (x_i y_i)\, \beta_i,\\
&a \cdot x = a \cdot \left(\sum_{i=0}^{7} x_i \beta_i \right) = \sum_{i=0}^{7} (a x_i)\, \beta_i, \text{ respectively.}
\end{aligned}$$

It is clear that $(KO, +, \cdot)$ is a vector space. It is clear that KO is a commutative and associative algebra with multiplication $*$.

4. Proposed KOTR cryptosystem

The KOTR cryptosystem is via octonion algebra with coefficients in KAH-Octo algebra with truncated polynomial rings $\varsigma = Z[\chi]/(\chi^N - 1), \varsigma_p = Z_p[\chi]/(\chi^N - 1), \varsigma_q = Z_{q}[\chi]/(\chi^N - 1)$, and octonnion algebras:

$$\begin{aligned}
\Gamma &= \left\{ \sum_{j=0}^{7} f_j \beta_j + \sum_{i=1}^{7} \left(\sum_{j=0}^{7} f_j \beta_j \right) e_i : f_j \in \varsigma \right\},\\
\Gamma_p &= \left\{ \sum_{j=0}^{7} f_j \beta_j + \sum_{i=1}^{7} \left(\sum_{j=0}^{7} f_j \beta_j \right) e_i : f_j \in \varsigma_p \right\},\\
\Gamma_q &= \left\{ \sum_{j=0}^{7} f_j \beta_j + \sum_{i=1}^{7} \left(\sum_{j=0}^{7} f_j \beta_j \right) e_i : f_j \in \varsigma_q \right\},
\end{aligned}$$

Also, define the subsets:

$L_f = \{\sum_{j=0}^{7} f_j \beta_j + \sum_{i=1}^{7} \left(\sum_{j=0}^{7} f_j \beta_j \right) e_i : f_j \in \varsigma |$ such that f_j has d_f coefficient equal to $+1$, d_f equal -1 and the other values $0\}$,

$L_g = \{\sum_{j=0}^{7} g_j \beta_j + \sum_{i=1}^{7} \left(\sum_{j=0}^{7} g_j \beta_j \right) e_i : g_j \in \varsigma |$ such that g_j has d_g coefficient equal to $+1$, $d_g - 1$ equal -1 and the other values $0\}$,

$L_{\mathfrak{W}} = \{\sum_{j=0}^{7} \mathfrak{W}_j \beta_j + \sum_{i=1}^{7} \left(\sum_{j=0}^{7} \mathfrak{W}_j \beta_j \right) e_i : \mathfrak{W}_j \in \varsigma |$ such that coefficients of $\mathfrak{W}_j \in (-p/2, p/2)\}$, and L_v defined as L_f.

The phases of NSQTR explain as the following:

4.1. Key generate

The recipient chooses randomly secret keys $f \in L_f$ and $g \in L_g$, the public key $\wp$ that is exchanged between the two parties is calculated using the following equation:

$$\wp = f * g^{-1}\ mod\ q.$$

4.2. Encryption

When sending the message $\mathfrak{W}$ to the other party, we convert it to the form $\sum_{j=0}^{7} \mathfrak{W}_j \beta_j + \sum_{i=1}^{7} \left(\sum_{j=0}^{7} \mathfrak{W}_j \beta_j \right) e_i$ and then choose $\mathcal{V}$ (a vanishing element) from the subset L_v and then convert it to the ciphertext as follows:

$$\mathfrak{L} \equiv p\, (\mathcal{V} *\ \wp + \mathfrak{W})\, mod\ q,$$

such that the coefficients of the polynomials lie in the interval $(-\frac{q}{2},\ \frac{q}{2}]$.

4.3. Decryption

When receiving the encrypted message, to obtain the original text, we follow the following steps:

- Multiply the encrypted text $\mathfrak{L}$ by the key g from the right as follows:

$$\begin{aligned}\mathfrak{L} * g \ (\ mod\ q) &\equiv p\,(\mathcal{V} * \ \wp + \mathfrak{W}) * g\ (mod\ q)\\ &\equiv p\,(\mathcal{V} * \wp) * g + \mathfrak{W} * g\ (mod\ q)\\ &\equiv \ p\left(\mathcal{V} * f * g^{-1}\right) * g + \mathfrak{W} * g\ (\ mod\ q)\\ &\equiv p\,(\mathcal{V} * f) + \mathfrak{W} * g\ (mod\ q)\end{aligned}$$

  where the coefficients of the polynomials of the last expression $p\,(\mathcal{V} * f) + \mathfrak{W} * g = \mathcal{S}$ within the interval $\left(-\frac{q}{2}, \frac{q}{2}\right]$.

- Convert the coefficients of the expression $p\,(\mathcal{V} * f) + \mathfrak{W} * g = \mathcal{S}$ from modulo p to modulo q, therefore

$$\begin{aligned}\mathcal{S} &\equiv p\,(\mathcal{V} * f) + \mathfrak{W} * g\ (mod\ p)\\ &\equiv \mathfrak{W} * g\ (\ mod\ p).\end{aligned}$$

- Multiply the encrypted text $\mathcal{S}$ by the key g^{-1} from the right as follows:

$$\begin{aligned}\mathcal{S} * g^{-1} &\equiv (\mathfrak{W} * g) * \ g^{-1}\ (\ mod\ p)\\ &\equiv \ \mathfrak{W}\ (mod\ p),\end{aligned}$$

  with coefficients of the polynomials of the last expression within the interval $\left(-\frac{q}{2}, \frac{q}{2}\right]$.

5. Analysis of NSQTR

In terms of the security, the encrypted text sent between two parties is not permitted to be accessed by the other party. Hackers between the two parties attempt to obtain the original text, view its original data, and use it for their own personal purposes. In this method, the hacker takes two paths: either through the public key, by taking the possible probabilities for one of the two keys, f or g. If we assume that the sample space f is smaller than the sample space g, then the number of probabilities for key f is as follows:

$$|L_f| = \left(\binom{N}{d_f}\binom{N-d_f}{d_f}\right)^{64} = \left(\frac{N!}{(d_f!)^2\,(N-2d_f)!}\right)^{64},$$

The second path is through the encrypted text, which the hacker can access through the medium that transmits it. In this case, the hacker works on all possible probabilities for key $\mathcal{V}$, which equals:

$$|L_{\mathcal{V}}| = \left(\binom{N}{d_{\mathcal{V}}}\binom{N-d_{\mathcal{V}}}{d_{\mathcal{V}}}\right)^{64} = \left(\frac{N!}{(d_{\mathcal{V}}!)^2\,(N-2d_{\mathcal{V}})!}\right)^{64},$$

As for the time required to implement the three phases of the system, it depends on the multiplication (Con. Multi) and addition operations in each phase, and thus the Table 1 explains that.

Table 1: Mathematical operations of NSQTR

Phases	Mathematical operations
Key generate	512 Con. Multi
Encryption	512 Con. Multi and 64 polynomial additions
Decryption	1024 Con. Multi and 64 polynomial addition

Execution time is equal to $2048t + 124t_1$, such that t_1 is number of addition times and t multiplication times.

6. Conclusions

The proposed method offers a very high level of security due to its reliance on algebra resulting from the combination of octonion algebra and KAH-Octo algebra algebra. Therefore, it has a higher level of security for both the key and the message compared to the OTRU method, which relies on octonion algebra, and the KAOTR and KSQOT methods, which rely on KAH-Octo algebra. However, in terms of execution time, it is slower than OTRU, KAOTR, and KSQOT methods, but its speed can be increased by reducing the degree of polynomials. This method provides another positive point in that it is used to encrypt and send multiple messages simultaneously, up to 64 messages together, due to the algebraic structure used in its construction, which opens the door to making it a popular method in banks, communication networks, or corporate network systems, etc.

References

1. A. A. Abidalzahra and H. R. Yassein. Proposed development of ntru encryption. *International Journal of Mathematics and Computer Science*, 19(3):715–719, 2024.

2. M. Albrecht and L. Ducas. *Lattice Attacks on NTRU and LWE: A History of Refinements*. Cambridge University Press, Cambridge, UK, 2021.

3. M. Coglianese and B.M. Goi. Matru: A new ntru-based cryptosystem. In S. Maitra, C.E. Veni Madhavan, and R. Venkatesan, editors, *Progress in Cryptology – INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Computer Science*, Berlin, Heidelberg, 2005. Springer.

4. A. C. Fadeel and H. R. Yassein. Haqtr: Ntru-like public key. *International Journal of Mathematics and Computer Science*, 19(1):1–4, 2024.

5. P. Gaborit, J. Ohler, and P. Solé. *CTRU, a polynomial analogue of NTRU*. PhD thesis, Inria, 2002.

6. K.A. Hassoon. A new algebra with its application in a cryptosystem. M.sc. thesis, University of Kufa, Iraq, 2025.

7. K.A. Hassoon and H.R. Yassein. A new multi-dimensional public key cryptosystem via kah-octo algebra. *J. Discrete Math. Sci. Cryptogr.*, 28(2):349–354, 2025.

8. 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.

9. A. Leier, C. Richter, W. Banzhaf, and H. Rauhe. Cryptography with dna binary strands. *Biosystems*, 57(1):13–22, 2000.

10. A. Majeed. Cqtru cryptosystem based on commutative ring of quaternion. M.sc. thesis, University of Technology, Iraq, 2015.

11. 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.

12. H. S. Salman and H. R. Yassein. Truhsh: Developing ntru cryptosystem in terms of security and performance. *Applied Mathematics and Information Sciences an International Journal*, 17(4):723–725, 2023.

13. H.S. Salman and H.R. Yassein. Structure a public-key cryptosystem based on hss algebra. *Appl. Math. Inf. Sci.*, 17(4):659–661, 2023.

14. T.S. Slaibi. *Improved NTRU Cryptosystem*. Ph.d. thesis, University of Technology, Iraq, 2006.

15. P.R. Suri and P. Puri. Application of lfsr with ntru algorithm. In *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*, pages 369–373. Springer Netherlands, Dordrecht, 2007.

16. 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.

17. H.R. Yassein and N.M. Al-Saidi. A comparative performance analysis of ntru and its variant cryptosystems. In *Proc. Int. Conf. Current Research in Computer Science and Information Technology (ICCIT)*, pages 115–120, Sulaymaniyah, Iraq, April 2017. IEEE.

18. H.R. Yassein and H. A. Ali. Sqntru: New public key encryption. *International Journal of Mathematics and Computer Science*, 18(3):381–385, 2023.

19. H.R. Yassein and H.S. Salman. Truft: A new public key cryptosystem based on novel fth algebra. *Int. J. Math. Comput. Sci.*, 18(4):589–593, 2023.

20. H.R. Yassein and S.H. Shahhadi. Trqttru: A new algebra for establishing secure public-key ntru. *Bol. Soc. Paran. Mat.*, 43:1–7, 2025.

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

and

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