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

(3s.) **v. 2025 (43) 3** : 1–5.
ISSN-0037-8712
doi:10.5269/bspm.79071

OTRUD: A New Multidimensional Public Key Encryption Based on Octonion Algebra

Mohammed Hassan Hamza, Adnan Awadh Oudah, Sahab Mohsen Abboud and Hassan Rashed Yassein*

ABSTRACT: OTRU is a multi-dimensional public key cryptographic with eight data vectors encrypted at each step. In our research, we introduce OTRUD, an enhanced version of OTRU, which utilizes a new mathematical construct of four private keys and two public keys to strengthen the security of public key system. OTRUD is suitable to applications which require simultaneous operation from multiple sources, such as electronic voting.

Key Words: NTRU, OTRU, octonion algebra.

Contents

1. Introduction

The main objective of any cryptosystem is to obscure sensitive information in a manner that renders it incomprehensible to anyone without authorized access. Encryption is primarily utilized to either safeguard data in a digital file or transfer it securely over an unsecured network, such as the Internet. The NTRU encryption system plays a big role in providing high levels of security. Three mathematicians Hoffstein et al. [14] introduced it in 1996. It is considered this is the initial system that is not reliant on discrete algorithmic issues or factors. 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 truncated polynomials ring with degree N-1 represented as $Z[X]/(X^N - 1)$.

In 2002, Jaborit et al. [11] We introduce CTRU, a polynomial loop over the binary domain F, which extends NIRU and provides a more generalized approach. In 2005, Coglianese and Goi introduced MaTRU, a variant of NTRU that operates in ring M of $n \times n$ matrices of polynomials $Z[X]/(X^N - 1)$, providing an analog approach [9]. In 2009 [18] Malkian et al proposed a system called QTRU used quaternion algebra. In 2010 Malakai et al. [10]. Presented an encryption system called OTRU, which is a multi-dimensional encryption system with one public key with the property of encrypting in each step, there are eight data vectors [10,17]. In 2011 and 2015 Jarvis [15,16] prposed ETRU via integer $Z[\omega]$ 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, Yassein and Al-Saidi [21,8] proposed multi-dimensional HXDTRU and BITRU via hexadecimal and binary algebra respectively. In 2017, Yassein and Al-Saidi [26] presented a comparison between three mathematical structures as alternatives to NTRU. Yassein and Al-Saidi [25,23] suggested the BCTRU cryptosystem in 2018 and 2019, which is based on algebra of bi-Cartesian. Yassein et al. [22] introduced the QOBTRU cryptosystem in 2020, which utilizes a new multi-dimensional algebra known

* Corresponding author.

2010 *Mathematics Subject Classification:* 94A60, 68P25.
Submitted September 19, 2025. Published December 20, 2025

as Carterion algebra. In 2021, Yassein et al. [20] introduced QMTRU as developments of QTRU. Abo-Alsood and Yassein presented QOTRU via Qu- Octonion subalgebra [5]. In 2022, Al-Awadi [7] proposed MaTRUD as an improvement to the MaTRU. In the same year Al-Awadi, introduced QP-RSA that used quaternion algebra. Shihadi and Yassein presented NTRTRN which based on tripternion algebra [19]. Abo-alsood and Yassein suggested TOTRU via algebra of octonion [6].

In 2023, Yassein et al. introduced QuiTRU via multi-dimensional algebra [24]. In 2024, Abboud et al. using octonion and quaternion algebras to introduced OTRCQ [3], Abo-Alsood at al. based on HH-Real algebra and RSA proposed HH-RSA system [4]. In 2025, Abboud et al. improved the RSA through the octonion polynomials [1], Hamza et al. development of MRSA via algebra of octonion [12]. Also, Abboud et al. an proposed HXDHS via hexadecnion algebra with neutrosophic integer coefficients [2]. Hamza et al. develop MRSA via HH-Real algebra [13].

2. The Proposed Scheme OTRUD

Similar to OTRU in search. The OTRUD cryptosystem depends on three positive integer N, p, q as define in NTRU and six subsets $L_{\mathcal{F}}, L_g, L_{\hbar}, L_{б}, L_j, L_{\Delta}$ and L_m, are define as follows:

Table 1: OTRUD subsets

Subset	Description
$L_{\mathcal{F}}$	$\{\mathcal{F}_0(x) + \mathcal{F}_1(x)e_1 + \ldots + \mathcal{F}_7(x)e_7, \mathcal{F}_i(x)$ satisfy $\ell(d_{\mathcal{F}}, d_{\mathcal{F}} - 1)\}$
L_g	$\{g_0(x) + g_1(x)e_1 + \ldots + g_7(x)e_7, g_i(x)$ satisfy $\ell(d_g, d_g)\}$
$L_{\hbar}$	$\{\hbar_0(x) + \hbar_1(x)e_1 + \ldots + \hbar_7(x)e_7, \hbar_i(x)$ satisfy $\ell(d_{\hbar}, d_{\hbar})\}$
$L_{б}$	$\{б_0(x) + б_1(x)e_1 + \ldots + б_7(x)e_7, б_i(x)$ satisfy $\ell(d_{б}, d_{б} - 1)\}$
L_j	$\{j_0(x) + j_1(x)e_1 + \ldots + j_7(x)e_7, j_i(x)$ satisfy $\ell(d_j, d_j)\}$
L_{Δ}	$\{\Delta_0(x) + \Delta_1(x)e_1 + \ldots + \Delta_7(x)e_7, \Delta_i(x)$ satisfy $\ell(d_{\Delta}, d_{\Delta} - 1)\}$
L_m	$\{m_0(x) + m_1(x)e_1 + \ldots + m_7(x)e_7, m_i(x)$ has coefficients lie between $-p/2$ and $p/2\}$

The $\mathscr{L}(d_z, d_s)$ is defined by {The number of coefficients $\mathcal{F}$ whose value is 1 is d_z, and whose value is -1 is d_s, the rest 0}. OTRUD is described by:

2.1. Generate of key

To generate a public key, select $\mathcal{F} \in L_{\mathcal{F}}, g \in L_g, \hbar \in L_{\hbar}, j \in L_j$ and $б \in L_{б}, \Delta \in L_{\Delta}$ with $\mathcal{F}, \Delta$ and $б$ invertible denoted by $\mathcal{F}_p^{-1}, \Delta_p^{-1}$ and $б_p^{-1}$ respectively. Also $\mathcal{F}$ invert denote by $\mathcal{F}_q^{-1}$ respectively.

Compute $\mathcal{H} = \mathcal{F}_q^{-1} * g * \hbar \,(mod\ q)$ and $\mathfrak{R} = б * \Delta_q^{-1}\ (mod\ q)$.

2.2. Encryption

To encrypt a message $m \in L_m$

1. We randomly generate $j \in L_j$.

2. Competes the encrypted massage as follows:

$$£ = p\mathcal{H} * j + m * \mathfrak{R}\ (mod\ q).$$

2.3. Decryption

To decrypt the cipher text £, we do the following:

- Compete

$$\begin{aligned}\eth &= \mathscr{F} * \mathscr{L} * \Delta \ mod\ q\\ &= \mathscr{F} * (p\mathscr{H} * j + m * \mathfrak{R}) * \Delta\, (mod\ q)\\ &= \mathscr{F}\left(\left(p\mathscr{F}_q^{-1} * g * \hbar\right) * j + m * \left(\mathscr{b} * \Delta_q^{-1}\right)\right) * \Delta\ (mod\ q)\\ &= pg * \hbar * j * \Delta + \mathscr{F} * m * \mathscr{b}\ (mod\ q)\end{aligned}$$

- Take

$$\begin{aligned}\mathscr{B} &= \eth\, (mod\ p)\\ &= \mathscr{F} * m * \mathscr{b}\ \ (mod\ p)\\ &= \mathscr{F}_p^{-1} * \mathscr{B} * \mathscr{b}_p^{-1}\ \ (mod\ p)\\ &= m\ \ (mod\ p)\end{aligned}$$

3. Performance of OTRUD

By brute force attack, the hacker who know the public keys $\mathscr{H} = \mathscr{F}_q^{-1} * g * \hbar, \mathfrak{R} = \mathscr{b} * \mathscr{F}_q^{-1}$ and either try to obtain the private key $\mathscr{F}$ from the set $L_{\mathscr{F}}$ (or obtain private keys $g, \hbar, \mathscr{b}$ from the sets $(L_g, L_\hbar, L_{\mathscr{b}})$, to find a decryption short key. Such that all of polynomials have degree $n-1$ therefore, the security key of OTRUD equal

$$\begin{aligned}\text{Space of Key} &= \left(\frac{N_!}{(dg_!)^2\ \ (N-2dg)_!}\right)^8 \left(\frac{N_!}{(d\mathscr{b}_!)^2\,(N-2d\mathscr{b})_!}\right)^8\\ &= \left(\frac{(N_!)^{16}}{(dg_!d\mathscr{b}_!)^{16}\ \ ((N-2dg)_!\,(N-2d\mathscr{b})_!)^8}\right)\end{aligned}$$

Because the time of OTRUD depends on convolution multiplication time (t) and addition time (t_1), then the time of OTRUD equal 1600 $t + 16\ t_1$.

4. Conclusions

We have presented OTRUD and shown that level of security is comparable to OTRU with respect to brute force attack. Because OTRUD use two public keys instead one public key in OTRU and four private key in OTRU then OTRUD is slower than OTRU but the key security of OTRUD more than of OTRU and the message security of OTRUD equal to OTRU, such that OTRU special case of OTRUD when $(\mathscr{b} = \mathscr{F}, \hbar = 1)$.

References

1. S. M. Abboud, R. K. Ajeena, and H. R. Yassein, *Octonion polynomials for a more secure RSA public key cryptosystem*, International Journal of Mathematics and Computer Science (2025), no. 1, 281–284.
2. S. M. Abboud, M. H. Hamza, and H. R. Yassein, *A new public key encryption based on Hexadecnion algebra with neutrosophic integer coefficients*, International Journal of Neutrosophic Science **26** (2025), no. 4, 113–121.
3. S. M. Abboud, H. R. Yassein, and R. K. Alhamido, *Improvement of multi-dimensional public key OTRU cryptosystem*, International Journal of Mathematics and Computer Science **19** (2024), no. 4, 1071–1076.
4. H. H. Abo-Alsood, M. H. Hamza, S. A. Al-Bairmani, and H. R. Yassein, *Development of public key cryptosystem RSA via multidimensional algebra*, Journal of Mathematics and Computer Science **19** (2024), no. 4, 1177–1182.
5. 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** (2021), no. 1, 1–7.
6. H.H. Abo-Alsood and H.R. Yassein, *Analogue to NTRU public key cryptosystem by multi-dimension algebra with high security*, AIP Conference Proceedings **2386** (2022), 600091–600096.
7. M. H. Al-Awadi, *Designing an efficient and secure cryptosystem similar to MaTRU and RSA*, M. sc. thesis, University of Al-Qadisiya, Al-Qadisiya, Iraq, 2022.

8. N. M. 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 **11** (2017), 29–43.

9. M. Coglianese and B.M. Goi, *Matru: A new ntru-based cryptosystem*, Progress in Cryptology – INDOCRYPT 2005 (Berlin, Heidelberg) (S. Maitra, C.E. Veni Madhavan, and R. Venkatesan, eds.), Lecture Notes in Computer Science, vol. 3797, Springer, 2005.

10. E.Malekian and A. Zakerolhosseini, *OTRU: A Non-Associative and High Speed Public Key Cryptosystem*, 2010 15th CSI International Symposium on Computer Architecture and Digital Systems (CADS) (Tehran, Iran), IEEE, September 2010, pp. 83–90.

11. P. Gaborit, J. Ohler, and P. Sole, *CTRU, a polynomial analogue of NTRU*, Tech. Report RR-4621, INRIA, France, 2002, Available at ftp://ftp.inria.fr/INRIA/publication/publi-pdf/RR/RR-4621.pdf.

12. M. H. Hamza, S. M. Abboud, and H. R. Yassein, *Development of modified RSA cryptosystem via Octonion algebra*, International Journal of Mathematics and Computer Science **20** (2025), no. 1, 459–464.

13. M. H. Hamza, H. H. Abo-Alsood, S. M. Abboud, H. R. Yassein, and Z. S. Shareef, *HH-MRSA: Designing an improvement of MRSA with high security*, Journal of Discrete Mathematical Sciences and Cryptography **28** (2025), no. 2, 557–564.

14. J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A Ring-Based Public Key Cryptosystem*, International Algorithmic Number Theory Symposium, Springer, 1998, pp. 267–288.

15. K. Jarvis, *NTRU over the Eisenstein integers*, Master's thesis, University of Ottawa, 2011.

16. K. Jarvis and M. Nevins, *ETRU: NTRU over the Eisenstein integers*, Designs, Codes and Cryptography **74** (2015), no. 1, 219–242.

17. E. Malekian and A. Zakerolhosseini, *NTRU-Like Public Key Cryptosystems beyond Dedekind Domain up to Alternative Algebra*, Transactions on Computational Science X (M. L. Gavrilova, C. J. K. Tan, and E. D. Moreno, eds.), Lecture Notes in Computer Science, vol. 6340, Springer, Berlin, Heidelberg, 2010.

18. E. Malekian, A. Zakerolhosseini, and A. Mashatan, *QTRU: A lattice attack resistant version of NTRU PKCS based on quaternion algebra*, The ISC International Journal of Information Security **3** (2011), no. 1, 29–42.

19. S.H. Shihadi and H.R. Yassein, *An innovative tripternion algebra for designing NTRU-like cryptosystem with high security*, AIP Conference Proceedings **2386** (2022), 60009–1–60009–6.

20. H. R. Yassein, A. A. Abidalzahra, and N. M. Al-Saidi, *A new design of NTRU encryption with security and performance level*, AIP Conference Proceedings **2334** (2021), no. 1, 080005–1–080005–4.

21. H. R. Yassein and N. M. Al-Saidi, *HXDTRU cryptosystem based on hexadecnion algebra*, Proceedings of the 5th International Cryptology and Information Security Conference (Malaysia), 2016.

22. H. R. Yassein, N. M. Al-Saidi, and A. K. Farhan, *A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure*, Journal of Discrete Mathematical Sciences and Cryptography **25** (2022), no. 2, 523–542.

23. H. R. Yassein and N.M. Al-Saidi, *An innovative Bi-Cartesian algebra for designing of highly performed NTRU like cryptosystem*, Malaysian Journal of Mathematical Sciences **13** (2019), 77–91.

24. 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** (2023), no. 1, 49–53.

25. H.R. Yassein and N. M. Al-Saidi, *BCTRU: A new secure NTRU crypt public key system based on a newly multidimensional algebra*, Proceedings of the 6th International Cryptology and Information Security Conference, 2018, pp. 1–11.

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

Mohammed H. Hamza,
General Directorate of Al-Muthanna Education,
Iraq.
E-mail address: muhammad_hassan@ijsu.edu.iq

and

Adnan A. Oudah,
General Directorate of Al-Muthanna Education,
Iraq.
E-mail address: adnann8@gmail.com

and

Sahab M. Abboud,
Department of Mathematics,
College of Basic Education, University of Babylon,
Iraq.
E-mail address: bsc.sahab.jwer@uobabylon.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