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.78456

ELQTR: More Secure Encryption System Based on MAL-Eleven Algebra with Quaternion Coefficients

Mariam Yosef Almustafa, Basel Hamdo Alarnous and Hassan Rashed Yassein*

ABSTRACT: Our traditional world is transforming into a digital world at a very rapid pace, which requires the need to encrypt data at the same or greater speed. In this paper, we will present an improved NTRU encryption scheme called ELQTR, which is based on the eleven-dimensional M_ae algebra. As a special case, we will take the coefficients from the quaternion algebra, which gives a significant difference in security compared to NTRU and some of its improvements. We will also provide some comparisons between the new scheme and some other schemes in terms of message security, key security, and speed

Key Words: QTRU, MAL-Eleven algebra, Space security of key, Space security of Message.

Contents

1. Introduction

Cryptography researchers are constantly working to develop new, effective encryption methods or improve existing methods to keep pace with digital developments. Among the methods that are still in use today are RSA [12] and NTRU [6], the most important improvements made to these two methods by replacing the algebra [7] or mathematical construction can be summarized as follows:

Sari and Puri, 2007 [14] used the same key to encryption and decryption phases by cipher stream. Based on quaternion algebra, Malekian et al., 2009 [10] introduced cryptosystem QTRU. Nevins et al., 2010 [11] using Einstein integers ring to proposed a new version of the NTRU. Also, Malekian and Zakerolhosseini [9] proposed OTRU public key based on algebra of octonion.

Lei and Liao, 2013 [8] introduced a new NTRU key exchange protocol. Yassein and Al-Saidi compared HXDTRU, BITRU and PQTRU in terms of security [16].

Via the bi-octonion subalgebra of octonion algebra, Abo-alsood and Yassein 2021 [15] proposed the QOTRU system. Also, through tripternion algebra, the NTRSH system was proposed by Shihadi and Yassein [3]. In 2022, Shihadi and Yassein, 2022 [13] developed the NTRU by proposed NTRTRN via tripternion algebra. Abo-alsood and Yassein [4] introduced TOTRU via algebra of octonion. Yassein et al., 2023 [17] proposed public key cryptosystem depends on HH-Real algebra which called QuiTRU. Also, Atea and Yassein, [5] suggests PMRSA system based on Polynomial Ring. Abboud et al., 2024 [2] proposed OTRCQ, via octonions algebra. Abboud et al., 2025 [1] introduced OP-RSA via the octonion polynomials

* Corresponding author.
2010 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted August 17, 2025. Published October 07, 2025

2. MAL-Eleven Algebra

The set MAL-Eleven algebra denoted by M_{ae} is defined as follows:

$$M_{ae} = \left\{ a_0 + \sum_{i=1}^{10} a_i w_i | a_i \in F \right\},$$

where F is a field.

The operations addition $(+)$, multiplication $(*)$ and scalar multiplication $(\cdot)$ are defined as follows: Suppose $x, y \in M_{ae}$ such that $x = x_0 + \sum_{i=1}^{10} x_i w_i$, $y = y_0 + \sum_{i=1}^{10} y_i w_i$ and a scalar $\gamma \in F$ then

$$x + y = (x_0 + y_0) + \sum_{i=1}^{10} (x_i + y_i) w_i,$$

$$x * y = (x_0 \cdot y_0) + \sum_{i=1}^{10} (x_i \cdot y_i)\, w_i,$$

and

$$\gamma \cdot y = (\gamma y_0) + \sum_{i=1}^{10} (\gamma y_i)\, w_i$$

respectively, if $x_0 + \sum_{i=1}^{10} x_i w_i = y_0 + \sum_{i=1}^{10} y_i w_i$ implies that $x_i = y_i$.

A vector space $(M_{ae}, +, \cdot, *)$ is commutative and associative algebra with identity element $1 + w_1 + w_2 + \ldots + w_{10}$ and the inverse of $x = x_0 + \sum_{i=1}^{10} x_i w_i$ equal to $x^{-1} = x_0^{-1} + \sum_{i=1}^{10} x_i^{-1} w_i$ such that $x \neq 0$ for all $i = 0, \ldots, 10$. Also, $\{1, w_1, w_2, \ldots, w_{10}\}$ is basis.

3. Proposed ELQTR System

ELQTR is a multidimensional public-key cryptosystem based on the eleventh algebra Mae with coefficients from the quaternion algebra with general parameters (N, p, q) such that $gcd(p, q) = 1$ and $q >> p$ and rings of truncated polynomials $\varsigma = Z[x]/(x^N - 1), \varsigma_p = Z_p[x]/(x^N - 1), \varsigma_q = Z_q[x]/(x^N - 1)$. Also, define algebras

$$K = \left\{ \left(f_{(0,0)} + f_{(0,1)} i + f_{(0,2)} j + f_{(0,3)} k \right) + \sum_{n=1}^{10} \left(f_{(n,0)} + f_{(n,1)} i + f_{(n,2)} j + f_{(n,3)} k \right) w_n | f_{(n,0)}, f_{(n,1)}, f_{(n,2)}, f_{(n,3)} \in \varsigma,\ n = 0, 1, \ldots, 10 \right\}$$

$$K_p = \left\{ \left(f_{(0,0)} + f_{(0,1)} i + f_{(0,2)} j + f_{(0,3)} k \right) + \sum_{n=1}^{10} \left(f_{(n,0)} + f_{(n,1)} i + f_{(n,2)} j + f_{(n,3)} k \right) w_n | f_{(n,0)}, f_{(n,1)}, f_{(n,2)}, f_{(n,3)} \in \varsigma, n = 0, 1, \ldots, 10 \right\},$$

$$K_q = \left\{ \left(f_{(0,0)} + f_{(0,1)} i + f_{(0,2)} j + f_{(0,3)} k \right) \sum_{n=1}^{10} \left(f_{(n,0)} + f_{(n,1)} i + f_{(n,2)} j + f_{(n,3)} k \right) w_n | f_{(n,0)}, f_{(n,1)}, f_{(n,2)}, f_{(n,3)} \in \varsigma,\ n = 0, 1, \ldots, 10 \right\},$$

and subsets $\mathcal{L}_F, \mathcal{L}_G, \mathcal{L}_M, \mathcal{L}_\Phi, \mathcal{L}_\psi, \mathcal{L}_S \subset K$

$\mathcal{L}_F = \{ F \in K |\ F = \left(f_{(0,0)} + f_{(0,1)} i + f_{(0,2)} j + f_{(0,3)} k \right) + \sum_{n=1}^{10} \left(f_{(n,0)} + f_{(n,1)} i + f_{(n,2)} j + f_{(n,3)} k \right) w_n |$ $f_{(n,0)}, f_{(n,1)}, f_{(n,2)}, f_{(n,3)} \in \varsigma,\ n = 0, 1, \ldots, 10$ has cofficients d_{f_i} equal one, $d_{f_i} - 1$ equal negative one, other values zero$\}$,

$\mathcal{L}_G = \{G \in K |\ G = \left(g_{(0,0)} + g_{(0,1)}i + g_{(0,2)}j + g_{(0,3)}k\right) + \sum_{n=1}^{10}\left(g_{(n,0)} + g_{(n,1)}i + g_{(n,2)}j + g_{(n,3)}k\right)w_n |$ $g_{(n,0)}, g_{(n,1)}, g_{(n,2)}, g_{(n,3)} \in \varsigma,\ n = 0, 1, \ldots, 10$ has cofficients d_{g_i} equal one, d_{g_i} equal negative one, other values zero$\}$,

$\mathcal{L}_\Phi = \{\Phi \in K |\ G = \left(\Phi_{(0,0)} + \Phi_{(0,1)}i + \Phi_{(0,2)}j + \Phi_{(0,3)}k\right) + \sum_{n=1}^{10}\left(\Phi_{(n,0)} + \Phi_{(n,1)}i + \Phi_{(n,2)}j + \Phi_{(n,3)}k\right)w_n |$ $\Phi_{(n,0)}, \Phi_{(n,1)}, \Phi_{(n,2)}, \Phi_{(n,3)} \in \varsigma, n = 0, 1, \ldots, 10$ has cofficients d_{Φ_i} equal one, d_{Φ_i} equal negative one, other values zero$\}$,

$\mathcal{L}_\psi = \{\psi \in K |\ \psi = \left(\psi_{(0,0)} + \psi_{(0,1)}i + \psi_{(0,2)}j + \psi_{(0,3)}k\right) + \sum_{n=1}^{10}\left(\psi_{(n,0)} + \psi_{(n,1)}i + \psi_{(n,2)}j + \psi_{(n,3)}k\right)w_n |$ $\psi_{(n,0)}, \psi_{(n,1)}, \psi_{(n,2)}, \psi_{(n,3)} \in \varsigma,\ n = 0, 1, \ldots, 10$ has cofficients d_{ψ_i} equal one, d_{ψ_i} equal negative one, other values zero$\}$,

$\mathcal{L}_S = \{S \in K |\ S = \left(s_{(0,0)} + s_{(0,1)}i + s_{(0,2)}j + s_{(0,3)}k\right) + \sum_{n=1}^{10}\left(s_{(n,0)} + s_{(n,1)}i + s_{(n,2)}j + s_{(n,3)}k\right)w_n |$ $s_{(n,0)}, s_{(n,1)}, s_{(n,2)}, , s_{(n,3)} \in \varsigma,\ n = 0, 1, \ldots, 10$ has cofficients d_{s_i} equal one, d_{s_i} equal negative one, other values zero$\}$, and

$\mathcal{L}_M = \{M \in K |\ M = \left(m_{(0,0)} + m_{(0,1)}i + m_{(0,2)}j + m_{(0,3)}k\right) + \sum_{n=1}^{10}\left(m_{(n,0)} + m_{(n,1)}i + m_{(n,2)}j + m_{(n,3)}k\right)w_n | m_{(n,0)}, m_{(n,1)}, m_{(n,2)}, m_{(n,3)} \in \varsigma, n = 0, 1 \ldots, 10$ has cofficients, the cofficients of $m_{(n,0)}, m_{(n,1)}, m_{(n,2)}, m_{(n,3)} \in \varsigma,\ n = 0, 1.., 10$ lies between $-\frac{p}{2}$ and $\frac{p}{2}\}$.

Now we explain how the proposed ELQTR cryptosystem works through the following phases:

3.1. Generation of Key

Now we explain how the proposed ELQTR cryptosystem works through the following stages: In order to generate the public key H by the recipient, he chooses three elements, $F \in \mathcal{L}_f, G \in \mathcal{L}_g$, and $S \in \mathcal{L}_S$, as follows:

$$F = \left(f_{(0,0)} + f_{(0,1)}i + f_{(0,2)}j + f_{(0,3)}k\right) + \sum_{n=1}^{10}\left(f_{(n,0)} + f_{(n,1)}i + f_{(n,2)}j + f_{(n,3)}k\right)w_n,$$

$$G = \left(g_{(0,0)} + g_{(0,1)}i + g_{(0,2)}j + g_{(0,3)}k\right) + \sum_{n=1}^{10}\left(g_{(n,0)} + g_{(n,1)}i + g_{(n,2)}j + g_{(n,3)}k\right)w_n,$$

$$S = \left(s_{(0,0)} + s_{(0,1)}i + s_{(0,2)}j + s_{(0,3)}k\right) + \sum_{n=1}^{10}\left(s_{(n,0)} + s_{(n,1)}i + s_{(n,2)}j + s_{(n,3)}k\right)w_n,$$

and compute H by formula $H = F_q^{-1} * G * S \ mod\ q$, where F_q^{-1} is the inverse of $F \ mod\ q$. Note that multiplying the coefficients represents multiplication in quaternion algebra (the convolution multiplication).

3.2. Encryption

When the sender receives the public key, he converts his plaintext message into $\mathcal{L}_M$ elements, then randomly selects the elements $\Phi \in \mathcal{L}_\Phi$ and $\psi \in \mathcal{L}_\psi$ (vanishing), and then uses the following formula to obtain the ciphertext:

$$E \equiv \left(p\left(H * \Phi + \psi\right) + M\right)\ mod\ q,$$

such that the coefficients of E belong to $(-\frac{q}{2}, \frac{q}{2}]$.

3.3. Decryption

In order to recover the plaintext message from the encrypted text, the recipient performs the following steps:

$$\begin{aligned}
\text{Take } a &\equiv (F * E)\ mod\ q \\
&\equiv (\ F * (p\left(H * \Phi + \psi\right) + M))\ mod\ q \\
&\equiv (F * pH * \Phi + F * p\psi + F * M)\ mod\ q \\
&\equiv \left(pF * \left(F_q^{-1} * G\ * S\right) * \Phi + F * p\psi + F * M\right) mod\ q, \\
&\equiv (pG * S * \Phi + F * p\psi + F * M)\ mod\ q.
\end{aligned}$$

$$\begin{aligned}\text{Suppose } b &\equiv a \ (mod\ p)\\ &\equiv \ (pG * S * \Phi + F * p\psi + F * M)\, mod\ p\\ &\equiv 0 + 0 + \ F * M mod\ p.\end{aligned}$$

Therefore, $M \equiv \left(F_p^{-1} * b\right) mod\ p$ where F_p^{-1} is the inverse of $F\ mod\ p$ such that the coefficients of M belong to $(-\frac{p}{2},\ \frac{p}{2}]$.

4. Analysis of Security

The security of the Nitro method depends on the level of access to the private keys in the public key (key security) or the ciphertext (message security) by searching the subsets of each private key.

4.1. The Key Security Level

Assuming the size of both $\mathcal{L}_S(|\mathcal{L}_S|)$ and $\mathcal{L}_G$ $(|\mathcal{L}_G|)$ is less than $\mathcal{L}_F(|\mathcal{L}_F|)$ then

$$|\mathcal{L}_s| = \left(\binom{N}{d_S}\binom{N-d_S}{d_S}\right)^{44} = \left(\frac{N!}{d_S!\,(N-d_S)!}\right)\left(\frac{(N-d_S)!}{d_S!\,(N-2d_S)!}\right)^{44},$$

$$|\mathcal{L}_g| = \left(\binom{N}{d_d}\binom{N-d_g}{d_g}\right)^{44} = \left(\left(\frac{N!}{d_g!\,(N-d_g)!}\right)\left(\frac{(N-d_g)!}{d_g!\,(N-2d_g)!}\right)\right)^{44},$$

Therefore the space of key security equal to

$$\left(\frac{N!}{d_S!\,(N-d_S)!}\right)\left(\frac{(N-d_S)!}{d_S!\,(N-2d_S)!}\right)^{44}\left(\left(\frac{N!}{d_g!\,(N-d_g)!}\right)\left(\frac{(N-d_g)!}{d_g!\,(N-2d_g)!}\right)\right)^{44}.$$

4.2. The Message Security Level

Assuming the size of both $\mathcal{L}_\Phi(|\mathcal{L}_\Phi|)$ and $\mathcal{L}_\psi$ $(|\mathcal{L}_\psi|))$ then

$$|\mathcal{L}_\Phi| = \left(\binom{N}{d_\Phi}\binom{N-d_\Phi}{d_\Phi}\right)^{44} = \left(\left(\frac{N!}{d_\Phi!\,(N-d_\Phi)!}\right)\left(\frac{(N-d_\Phi)!}{d_\Phi!\,(N-2d_\Phi)!}\right)\right)^{44},$$

$$|\mathcal{L}_\psi| = \left(\binom{N}{d_\psi}\binom{N-d_\psi}{d_\psi}\right)^{44} = \left(\left(\frac{N!}{d_\psi!\,(N-d_\psi)!}\right)\left(\frac{(N-d_\psi)!}{d_\psi!\,(N-2d_\psi)!}\right)\right)^{44},$$

Therefore the space of key security equal to

$$\left(\left(\frac{N!}{d_\Phi!\,(N-d_\Phi)!}\right)\left(\frac{(N-d_\Phi)!}{d_\Phi!\,(N-2d_\Phi)!}\right)\right)^{44}\left(\left(\frac{N!}{d_\psi!\,(N-d_\psi)!}\right)\left(\frac{(N-d_\psi)!}{d_\psi!\,(N-2d_\psi)!}\right)\right)^{44}$$

5. Conclusions

The system proposed in this paper has several advantages over the NTRU cryptosystem, in addition to several other improvements, such as those of QTRU and OTRU. The most important of these is the level of security and the ability to process different messages from a single or multiple sources. It contains eleven dimensions, each containing four dimensions representing a quadrilateral algebra, making it a target for many institutions and companies with multiple data sources. However, the implementation time is longer, and this problem can be addressed by reducing the degree of the polynomials without compromising security.

References

1. S. M. Abboud, R. K. K. Ajeena, and H. R. Yassein, *Octonion polynomials for a more secure rsa public key cryptosystem*, International Journal of Mathematics and Computer Science **20** (2025), no. 1, 281–284.
2. S. M. Abboud, H. R. Yassein, and R. K. Alhamido, *Improvement of a multi-dimensional public-key otru cryptosystem*, International Journal of Mathematics and Computer Science **19** (2024), no. 4, 1071–1076.
3. 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, 012097.
4. 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** (2022), no. 1, 060006.
5. F. R. Atea and H. R. Yassein, *Pmrsa: Designing an efficient and secure public-key similar to rsa based on polynomial ring*, Applied Mathematics and Information Sciences **17** (2023), no. 3, 535–538.
6. 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.
7. B. Y. Hussein, *Equivalent locally martingale measure for the deflator process on ordered banach algebra*, Journal of Mathematics **2020** (2020), no. 1, 5785098.
8. X. Lei and X. Liao, *Ntru-ke: A lattice-based public key exchange protocol*, IACR Cryptology ePrint Archive **718** (2013).
9. 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 (Tehran, Iran), IEEE, 2010, pp. 83–90.
10. E. Malekian, A. Zakerolhosseini, and A. Mashatan, *Qtru: Quaternionic version of the ntru public-key cryptosystems*, ISeCure **3** (2011), no. 1, 29–42.
11. M. Nevins, C. Karimianpour, and A. Miri, *Ntru over rings beyond*, Designs, Codes and Cryptography **56** (2010), no. 1, 65–78.
12. R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126.
13. S.H. Shahhadi and H.R. Yassein, *An innovative tripternion algebra for designing ntru-like cryptosystem with high security*, AIP Conference Proceedings **2386** (2022), no. 1, 060009.
14. P. R. Suri and P. Puri, *Application of lfsr with ntru algorithm*, Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, Springer, 2007, pp. 369–373.
15. H. R. Yassein, *Ntrsh: A new secure variant of ntruencrypt based on tripternion algebra*, Journal of Physics: Conference Series **1999** (2021), no. 1, 012092.
16. H. R. Yassein and N. M. G. Al-Saidi, *A comparative performance analysis of ntru and its variant cryptosystems*, 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT) (Sulaymaniyah, Iraq), IEEE, 2017, pp. 115–120.
17. H. R. Yassein, H. N. Zaky, H. H. Abo-Alsood, I. A. Mageed, and W. I. El-Sobky, *Quitru: Design secure variant of ntruencrypt via a new multi-dimensional algebra*, Applied Mathematics **17** (2023), no. 1, 49–53.

Mariam Yosef Almustafa,
Department of Mathematics,
College of Science, Homs University,
Syria.
E-mail address: mariamalmustafa588@gmail.com

and

Basel Hamdo Alarnous,
Department of Mathematics,
College of Science, Homs University,
Syria.
E-mail address: barnous@homs-univ.edu.sy

and

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