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

(3s.) **v. 2026 (44) 11** : 1–6.
ISSN-0037-8712
doi:10.5269/bspm.81035

Designing an Encryption System Using MAL-Eleven Algebra and Pythagorean Quadruples

Reem Nayef Alahmad, Basel Hamdo Alarnous, Abdulbaset Alkhatib and Hassan Rashed Yassein*

ABSTRACT: The pace of the technological race is accelerating at an unprecedented rate, driven by fierce competition among information security institutions to meet the demands of the digital market for encryption methods that fulfill its aspirations. This paper employs a mathematical construct to design an efficient encryption method by combining an algebraic structure with the concept of Pythagorean quadruples.

Keywords: MAL-Eleven algebra, Pythagorean quadruples, space security.

Contents

1. Introduction

By employing a truncated polynomials rin, Hoffstein et al. presented a method for NTRU public-key encryption as an alternative to methods that rely on factorization integersproblem and the discrete logarithm problem [1].

Malecian et al. developed NTRU by relying on quaternion algebraic structure, resulting in high efficiency [2]. Malecian and Zakerolhosseini, however, proposed an improvement to NTRU by using an octonions algebraic structure in the system phases, which increased its security level [3]. Several researchers have presented numerous improvements to Nitro, which prompted Yassein and Al-Saidi to make a comparison between some of those improvements [4]. Tripternion algebra opened the door to the design of new encryption systems, introduced by Shihadi and Yassein called NTRsh, NTRS, NTRTRN [5,6,7].

Abo-alsood and Yassein designed multi-dimensional public key encryption systems based on different algebras, which are characterized by a high level of security with features that allow for the encryption of more than one text from more than one source at the same time [8,9,10]. The HUDTRU system was designed by Yassein and Ali based on quintuple algebra and was introduced as a development of the NTRU system [11].

* Corresponding author.
2020 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted December 26, 2025. Published March 13, 2026

Typeset by $\mathcal{B}^{S}\mathcal{P}_{\mathcal{M}}$ style.
© Soc. Paran. de Mat.

2. MAL-Eleven Algebra and Pythagorean Quadruples

2.1. MAL-Eleven Algebra

MAL-Eleven algebra denoted by M_{ae} is defined [12], as follows:
Let F be a field (in this paper take F is real numbers) and

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

The operations addition $(+)$, multiplication $(*)$ and scalar multiplication $(\cdot)$ are defined as follows:
Suppose $m_1, m_2 \in M_{ae}$ such that $m_1 = a_0 + \sum_{i=1}^{10} a_i w_i$, $m_2 = b_0 + \sum_{i=1}^{10} b_i w_i$ and a scalar $\alpha \in \Re$ then

$$m_1 + m_2 = (a_0 + b_0) + \sum_{i=1}^{10} (a_i + b_i) w_i,$$

$$m_1 * m_2 = (a_0 \cdot b_0) + \sum_{i=1}^{10} (a_i \cdot b_i)\, w_i,$$

and

$$\alpha \cdot m_i = (\alpha a_0) + \sum_{i=1}^{10} (\alpha a_i)\, w_i.$$

Respectively, if

$$a_0 + \sum_{i=1}^{10} a_i w_i = b_0 + \sum_{i=1}^{10} b_i w_i$$

implies that $a_i = b_i$.

1. $\{1, w_1, w_2, \ldots, w_{10}\}$ is basis.
2. The identity element of M_{ae} algebra is $1 + w_1 + w_2 + \ldots + w_{10}$.
3. The inverse of $m_1 = a_0 + \sum_{i=1}^{10} a_i w_i$ equal to ${m_1}^{-1} = a_0^{-1} + \sum_{i=1}^{10} a_i^{-1} w_i$ such that $a_i \neq 0$ for all $i = 0, \ldots, 10$.

2.2. Pythagorean quadruples

Let a, b, c be integer numbers [13], then

$$Q = \begin{pmatrix} \frac{-1+a^2+b^2-c^2}{1+a^2+b^2+c^2} & \frac{2(-a+bc)}{1+a^2+b^2+c^2} & \frac{-2(b+ac)}{1+a^2+b^2+c^2} \\ \frac{2(a+bc)}{1+a^2+b^2+c^2} & \frac{-1+a^2-b^2+c^2}{1+a^2+b^2+c^2} & \frac{-2(c-ab)}{1+a^2+b^2+c^2} \\ \frac{2(b-ac)}{1+a^2+b^2+c^2} & \frac{2(c+ab)}{1+a^2+b^2+c^2} & \frac{-1-a^2+b^2+c^2}{1+a^2+b^2+c^2} \end{pmatrix}$$

is a regular orthonormal matrix and the quadruples,

$$\left(-1 + a^2 + b^2 - c^2, 2\,(a + bc)\,, 2\,(b - ac)\,, 1 + a^2 + b^2 + c^2\ \right),$$

$$\left(2\,(-a + bc)\,, -1 + a^2 - b^2 + c^2, 2\,(c + ab)\,, 1 + a^2 + b^2 + c^2\ \right),$$

$$\left(-2\,(b + ac)\,, -2\,(c - ab)\,, -1 - a^2 + b^2 + c^2, 1 + a^2 + b^2 + c^2\ \right)$$

are Pythagorean.

It is clear that the fourth component of these Pythagorean quadruples is equal to $1 + a^2 + b^2 + c^2$.

We form the following sequence:

$$v_0 = -1 + a^2 + b^2 - c^2, v_1 = 2\,(a + bc)\,, v_2 = 2\,(b - ac)\,, v_3 = 2\,(-a + bc)$$
$$v_4 = -1 + a^2 - b^2 + c^2, v_5 = 2\,(c + ab)\,, v_6 = -2\,(b + ac)\,,$$
$$v_7 = -2\,(c - ab)\,, v_8 = -1 - a^2 + b^2 + c^2, v_9 = 1 + a^2 + b^2 + c^2$$

such that the first three terms, v_0, v_1, v_2 are from the first Pythagorean quadruple, v_3, v_4, v_5 from the second Pythagorean quadruples, v_6, v_7, v_8 from the third Pythagorean quadruple, and v_9 is the common fourth Pythagorean quadruple term. Suppose $V = \{v_0, v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9\}$.

3. MPQN Cryptosystem

In this section, we introduce MPQN cryptosystem based on the MAL-Eleven algebra (M_{ae}) with same parameters (N, p, q) of the NTRU, as well as the truncated polynomials rings $\Theta = Z\,[x]\,/(x^N - 1), \Theta_p = Z_p\,[x]\,/(x^N - 1), \Theta_q = Z_q\,[x]\,/(x^N - 1)$, and the following algebras

$$\zeta = \left\{ \alpha_0 + \sum_{i=1}^{10} \eta_i w_i; \eta_i \in \Theta \right\},$$

$$\zeta_p = \left\{ \alpha_0 + \sum_{i=1}^{10} \eta_i w_i; \eta_i \in \Theta_p \right\},$$

and

$$\zeta_q = \left\{ \alpha_0 + \sum_{i=1}^{10} \eta_i w_i; \eta_i \in \Theta_q \right\}.$$

The following subsets are also known:

$\mathcal{L}_\mathfrak{f}, \mathcal{L}_\mathcal{G}, \mathcal{L}_M, \mathcal{L}_U \subset$ where ζ

$\mathcal{L}_\mathcal{G} = \{\mathfrak{f} \in \zeta \mid \mathfrak{f} = f_0 + \sum_{i=1}^{10} f_i w_i,\ f_0, f_1, \ldots, f_{10}$ has cofficients d_{f_i} equal one, d_{f_i} equal negative one, other values zero$\}$,

$\mathcal{L}_\mathcal{G} = \{\mathcal{G} \in \zeta \mid \mathcal{G} = g_0 + \sum_{i=1}^{10} g_i w_i, g_0, g_1, \ldots, g_{10}$ has cofficients d_{g_i} equal one, $d_{g_i} - 1$ equal negative one, other values zero$\}$,

$\mathcal{L}_m = \{M = m_0 + \sum_{i=1}^{10} m_i w_i$, the cofficients of $m_0, m_1, \ldots, m_{10}$ lies between $-\frac{p}{2}$ and $\frac{p}{2}\}$, and $\mathcal{L}_U$ is defined similar to $\mathcal{L}_\mathfrak{f}$.

This system works as follows:

3.1. Key Generation

The recipient chooses two polynomials $\mathfrak{f} \in \mathcal{L}_\mathfrak{f}$ and $\mathcal{G} \in \mathcal{L}_\mathcal{G}$ of the form:

$$\mathfrak{f} = f_0 + \sum_{i=1}^{10} f_i w_i,\ \ \mathcal{G} = g_0 + \sum_{i=1}^{10} g_i w_i$$

where $\mathcal{G}$ has inverses of modulo p and q, denoted ${\mathcal{G}_p}^{-1}$ and ${\mathcal{G}_q}^{-1}$ respectively to build the public key, proceed as follows

$$\mathcal{I} \equiv \mathfrak{f} * {\mathcal{G}_q}^{-1}\ mod\ q.$$

3.2. Encryption

To send an encrypted text message m, the sender writes in the form $m_0 + \sum_{i=1}^{10} m_i w_i$, then selects $U \in \mathcal{L}_U$. Also, selects $S = s_0 + \sum_{i=1}^{10} s_i w_i, s_i \in V$ and then uses the following formula:

$$\mathfrak{E}\ \equiv p\,(U * \mathcal{I} + S) + M\ mod\ q,$$

with coefficients belong to $\left(-\frac{q}{2}, \frac{q}{2}\right]$.

4. Decryption

The next steps taken by the recipient lead to the explicit text:
Take

$$\begin{aligned}\Lambda &\equiv \mathfrak{E} * \mathcal{G} \ mod\ q \\ &\equiv p\,(U * \mathcal{I} + S) * \mathcal{G} + M * \mathcal{G} \ mod\ q \\ &\equiv p\left(U * (\mathfrak{f} * {\mathcal{G}_q}^{-1}) + S\right) * \mathcal{G} + M * \mathcal{G} \ mod\ q \\ &\equiv p\left(U * \left(\mathfrak{f} * {\mathcal{G}_q}^{-1}\right) * \mathcal{G} + S * \mathcal{G}\right) + M * \mathcal{G} \ mod\ q \\ &\equiv p\,(U * \mathfrak{f} + S * \mathcal{G}) + M * \mathcal{G} \ mod\ q\end{aligned}$$

with coefficients lie in the interval $\left(-\frac{q}{2}, \frac{q}{2}\right]$.

Now, convert Λ from $mod\ q$ to$mod\ p$, then

$$\begin{aligned}\Gamma &\equiv \Lambda \ mod\ p \\ &\equiv p\,(U * \mathfrak{f} + S * \mathcal{G}) + M * \mathcal{G} \ mod\ p \\ &\equiv M * \mathcal{G} \ mod\ p\end{aligned}$$

Hence, $M \equiv \Gamma * {\mathcal{G}_p}^{-1}\ mod\ p$, where the coefficients lie in the interval $\left(-\frac{p}{2}, \frac{p}{2}\right]$.

5. Security Analysis

The attacker has the public key $\mathcal{I}$ and wants to know the private keys to complete the remaining steps of the system to retrieve the original message. This is done by searching the number of public operations in $\mathcal{L}_\mathfrak{f}$ to find the private key $\mathfrak{f}$, or in $\mathcal{L}_\mathcal{G}$ to find the private key $\mathcal{G}$. Assuming $\mathcal{L}_\mathcal{G} > \mathcal{L}_\mathfrak{f}$, then the key space size is calculated as follows:

$$\left(\binom{N}{d_f}\binom{N-d_f}{d_f}\right)^{11} = \left(\left(\frac{N!}{d_f!\,(N-d_f)!}\right)\left(\frac{(N-d_f)!}{d_f!\,(N-2d_f)!}\right)\right)^{11} = \left(\frac{N!}{(d_f!)^2\,(N-2d_f)!}\right)^{11}.$$

The attacker can also find the original message from the ciphertext $\mathfrak{E}$ by searching $\mathcal{L}_U$ and V to obtain the keys U and S respectively. Therefore, the message space size is as follows:

$$\begin{aligned}(\text{size of space of } \mathcal{L}_U)\mathfrak{X} &= \left(\binom{N}{d_u}\binom{N-d_u}{d_u}\right)^{11}\mathfrak{X} \\ &= \left(\left(\frac{N!}{d_g!\,(N-d_g)!}\right)\left(\frac{(N-d_g)!}{d_g!\,(N-2d_g)!}\right)\right)^{11}\mathfrak{X} \\ &= \left(\frac{N!}{(d_g!)^2\,(N-2d_g)!}\right)^{11}\mathfrak{X},\end{aligned}$$

where $\mathfrak{X}$ is the size of space of V.

6. Conclusions

The MPQN system is an evolution of the original NTRU system, enhancing its security capabilities and making it more difficult to attack communication channels and intercept data transmitted over the network. Furthermore, it can encrypt multiple messages into a single message due to the dimensional of algebra used in its construction, thus increasing the speed of delivery to the recipient. This system can also be used in cybersecurity to protect data even if attackers manage to bypass the firewall.

References

1. 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.
2. E. Malecian, A. Zakerolhsooeini, and A. Mashatan. QTRU: Quaternionic version of the NTRU public-key cryptosystems. *The ISC International Journal of Information Security*, 3(1):29–42, 2011.
3. 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.
4. H. R. Yassein and N. M. G. Al-Saidi. A comparative performance analysis of NTRU and its variant cryptosystems. In *Proceedings of the International Conference on Current Research in Computer Science and Information Technology*, pages 115–120, Sulaymaniyah, Iraq, 2017.
5. S. H. Shihadi and H. R. Yassein. A new design of NTRUEncrypt-analog cryptosystem with high security and performance level via tripternion algebra. *International Journal of Mathematics and Computer Science*, 16(4):1515–1522, 2021.
6. S. H. Shahhadi and H. R. Yassein. NTRSH: A new secure variant of NTRUEncrypt based on tripternion algebra. *Journal of Physics: Conference Series*, 1999(1):012092, 2021.
7. S. H. Shahhadi and H. R. Yassein. An innovative tripternion algebra for designing NTRU-like cryptosystem with high security. *AIP Conference Proceedings*, 2386(1):060009, 2022.
8. H. H. Abo-Alsood and H. R. Yassein. Design of an alternative NTRU encryption with high secure and efficient. *International Journal of Mathematics and Computer Science*, 16(4):1469–1477, 2021.
9. 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.
10. H. H. Abo-Alsood and H. R. Yassein. Analogue to NTRU public key cryptosystem by multi-dimensional algebra with high security. *AIP Conference Proceedings*, 2386:060006, 2022.
11. H. R. Yassein and H. A. Ali. HUDTRU: An enhanced NTRU for data security via quintuple algebra. *International Journal of Mathematics and Computer Science*, 18(2):199–204, 2023.
12. M. Y. Almustafa, B. H. Alarnous, and H. R. Yassein. ELTRU: Development of NTRU via newly eleventh-dimensional algebra. *Boletim da Sociedade Paranaense de Matemática*, 43(3s):1–7, 2025.
13. R. N. Alahmad, A. A. Alkhatib, and B. H. Alarnous. Generation of orthonormal matrices and pythagorean tuples using the cayley transform. *Homs University Journal for Basic Sciences*, 2025.

Reem Nayef Alahmad,
Department of Mathematics,
College of Science, Homs University,
Syria.
E-mail address: r-alahmad@homs-univ.edu.sy

and

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

and

Abdulbaset Alkhatib,
Department of Mathematics,
College of Science, Homs University,
Syria.
E-mail address: aalkhteb@homs-univ.edu.sy

and

Hassan Rashed Yassein,

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