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

(3s.) **v. 2025 (43)** : 1–7.
ISSN-0037-8712
doi:10.5269/bspm.78333

# ELTRU: Development of NTRU via Newly Eleventh-Dimensional Algebra

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

ABSTRACT: Rapid technological development has transformed our transactions from classical to digital, making them risky due to their interception by intruders. This has made it essential for transmitted data to be secure through modern, advanced, and efficient encryption methods that can withstand intruders' attempts. In this paper, a multidimensional algebra has been created for use in building a new, more secure encryption system with features that make it efficient.

Key Words: OTRU, MAL-Eleven algebra, space security of key, Space security of message.

## Contents



## 1. Introduction

Researchers are racing to provide new methods for encrypting data or developing existing methods to ensure that data continues to be sent safely from hackers. Among the most important approved methods are RSA [14], Al-Gamal [7], Elliptic Curve cryptosystem [15], and NTRU [8]. The most important improvements made to NTRU by changing the algebra [9] or mathematical construction can be summarized as follows:

Coppersmith and Shamir, 1997 [6] demonstrated the NTRU encryption system's effectiveness against Lattice attacks. Sari and Puri, 2007 [18] used the same key to encryption phase and decryption phase by using a stream of ciphers. A quaternion-based public key cryptosystem QTRU is proposed by Malekian et al., 2009 [12]. A new version of the NTRU was introduced by Nevins et al., 2010 [13] using Einstein integers ring. Also, Malekian and Zakerolhosseini [11] suggested OTRU cryptosystem via algebra of octonion with eight dimension. Lei and Liao, 2013 [10] create a new NTRU key exchange protocol. In 2016, Yassein and Al-saidi, 2016 [20,5,4] presented the binary and hexadecnion algebras to introduced BITRU and HXDTRU, respectively. Yassein and Al-Saidi compared HXDTRU, PQTRU and BITRU in terms of safety [21].

Shihadi and Yassein, 2021 [16] introduced a public key cryptosystem NTRS via tripternion algebra. Also, Abo-alsood and Yassein [2,19] suggested BOTRU and QOTRU systems via the bi-octonion subalgebra of octonion algebra and Qu-octonion subalgebra. Shihadi and Yassein [1] proposed NTRSH system based on tripternion algebra. In 2022, Shihadi and Yassein, 2022 [17] suggested NTRTRN system a development of NTRU. Also, Abo-alsood and Yassein [3] proposed TOTRU based on octonion algebra. Yassein et al. introduced QuiTRU and HUDTRU cryptosystem via HH-Real algebra, and quintuple algebra respectively [23,22].

* Corresponding author.
2010 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted August 09, 2025. Published October 29, 2025

## 2. MAL-Eleven Algebra

In this section, a new multidimensional MAL-Eleven algebra denoted by $M_{ae}$ is defined as follows: Let $F$ be a field and

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

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 $\alpha \in F$ then

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

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

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

Respectively, if $a_0 + \sum_{i=1}^{10} a_i w_i = b_0 + \sum_{i=1}^{10} b_i w_i$ implies that $a_i = b_i$.

Then $(M_{ae}, +, \cdot)$ is a vector space with a basis $\{1, w_1, w_2, \ldots, w_{10}\}$.

**Proposition 2.1** *A vector space $(M_{ae}, +, \cdot, *)$ is an algebra.*

**Proof:** Let $m_1, m_2, m_3 \in M_{ae}$ and $\alpha \in F$ such that,

$$m_1 = a_0 + \sum_{i=1}^{10} a_i w_i, m_2 = b_0 + \sum_{i=1}^{10} b_i w_i, m_3 = c_0 + \sum_{i=1}^{10} c_i w_i.$$

$$\begin{aligned}
(m_1 + m_2) * m_3 &= \left( (a_0 + b_0) + \sum_{i=1}^{10} (a_i + b_i)\, w_i \right) * \left( c_0 + \sum_{i=1}^{10} c_i w_i \right) \\
&= ((a_0 + b_0) \cdot c_0) + \sum_{i=1}^{10} ((a_i + b_i) \cdot c_i)\, w_i \\
&= ((a_0 \cdot c_0) + (b_0 \cdot c_0)) + \sum_{i=1}^{10} ((a_i \cdot c_i) + (b_i \cdot c_i))\, w_i \\
&= (a_0 \cdot c_0) + \sum_{i=1}^{10} (a_i \cdot c_i) w_i + (b_0 \cdot c_0) + \sum_{i=1}^{10} (b_i \cdot c_i) w_i \\
&= m_1 * m_3 + m_2 * m_3 \cdot \ (\cdot \text{ multiplication operation in } F)
\end{aligned}$$

$$\begin{aligned}
m_1 * (m_2 + m_3) &= \left( a_0 + \sum_{i=1}^{10} a_i w_i \right) * \left( (b_0 + c_0) + \sum_{i=1}^{10} (b_i + c_i)\, w_i \right) \\
&= (a_0 \cdot (b_0 + c_0)) + \sum_{i=1}^{10} (a_i \cdot (b_i + c_i) w_i \\
&= (a_0 \cdot b_0) + (a_0 \cdot c_0) + \sum_{i=1}^{10} (a_i \cdot b_i) w_i + \sum_{i=1}^{10} (a_i \cdot c_i) w_i \\
&= m_1 * m_2 + m_1 * m_3.
\end{aligned}$$

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

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

Therefore, $(M_{ae}, +, \cdot, *)$ is an algebra. □

**Proposition 2.2** *Algebra $(M_{ae}, +, \cdot, *)$ is commutative and associative.*

**Proof:** Let $m_1, m_2, m_3 \in M_{ae} \in M_{ae}$ such that

$$m_1 = a_0 + \sum_{i=1}^{10} a_i w_i, m_2 = b_0 + \sum_{i=1}^{10} b_i w_i, m_3 = c_0 + \sum_{i=1}^{10} c_i w_i$$

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

Therefore $(M_{ae}, +, \cdot, *)$ is commutative.

$$(m_1 * m_2) * m_3 = \left((a_0 \cdot b_0) + \sum_{i=1}^{10} (a_i \cdot b_i)\, w_i\right) * \left(c_0 + \sum_{i=1}^{10} c_i w_i\right)$$
$$= ((a_0 \cdot b_0) \cdot c_0) + \sum_{i=1}^{10} ((a_i \cdot b_i) \cdot c_i)\ \ w_i$$
$$= (a_0 \cdot (b_0 \cdot c_0)) + \sum_{i=1}^{10} (a_i \cdot (b_i \cdot c_i))\ \ w_i$$
$$= \left(a_0 + \sum_{i=1}^{10} a_i w_i\right) * \left((b_0 \cdot c_0) + \sum_{i=1}^{10} (b_i \cdot c_i)\, w_i\right)$$
$$= m_1 * (m_2 * m_3).$$

Therefore, $(M_{ae}, +, \cdot, *)$ is associative. □

**Corollary 2.3**

1. *The identity element of $M_{ae}$ algebra is $1 + w_1 + w_2 + \ldots + w_{10}$*
2. *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 $i = 0, \ldots, 10$.*

## 3. Proposed ELTRU System

In this section, we introduce ELTRU, a multidimensional public-key cryptosystem based on the eleventh using the general parameters (N,p,q) of the NTRU, as well as the three rings of truncated polynomials $\Gamma = Z[x]/(x^N-1)$, $\Gamma_p = Z_p[x]/(x^N-1)$, $\Gamma_q = Z_q[x]/(x^N-1)$, and the following algebras

$$K = \left\{ \alpha_0 + \sum_{i=1}^{10} \mathfrak{h}_i w_i;\ \mathfrak{h}_i \in \Gamma \right\}$$

$$K_1 = \left\{ \beta_0 + \sum_{i=1}^{10} \mathfrak{h}_i w_i;\ \mathfrak{h}_i \in \Gamma_p \right\},$$

$$K_2 = \left\{ \gamma_0 + \sum_{i=1}^{10} \mathfrak{h}_i w_i; \mathfrak{h}_i \in \Gamma_q \right\}.$$

The following subsets are also known:

$$\mathcal{L}_f\ ,\ \mathcal{L}_g, \mathcal{L}_m,\ \mathcal{L}_\Phi \subset K$$

where

$\mathcal{L}_F = \{ F \in K | F = f_0 + \sum_{i=1}^{10} f_i w_i, f_0, f_1, \ldots, f_{10}$ has cofficients $d_{f_i}$ equal one, $d_{f_i} - 1$ equal negative one, other values zero$\}$,

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

$\mathcal{L}_m = \{ M \in K | M = m_0 + \sum_{i=1}^{10} m_i w_i,$ the cofficients of $m_0, m_1, \ldots, m_{10}$ lies between $-\frac{p}{2}$ and $\frac{p}{2}\}$, and $\mathcal{L}_\Phi$ is defined similarly to $\mathcal{L}_g$.

Here's a description of how ELTRU works.

### 3.1. Key Generation

The recipient randomly selects two polynomials $F \in \mathcal{L}_F\ and G \in \mathcal{L}_G$ of the form:

$$F \in K|\ F = f_0 + \sum_{i=1}^{10} f_i w_i, G \in K|\ G = g_0 + \sum_{i=1}^{10} g_i w_i$$

where $F$ has inverses of modulo $p$ and $q$, denoted ${F_p}^{-1} F$ and ${F_q}^{-1}$ respectively.

To generate the public key, the recipient calculates:

$$\mathfrak{U} \equiv {F_q}^{-1} * G\ mod\ q.$$

### 3.2. Encryption

Assuming the sender wants to send a message $M$ to the recipient, he will perform the following steps:
The message $M$ must be converted to MAL-Eleven algebra form as follows:

$$M = m_0 + \sum_{i=1}^{10} m_i w_i,$$

then, a (vanishing) polynomial $\Phi = \Phi_0 + \sum_{i=1}^{10} \Phi_i w_i \in \mathcal{L}_\Phi$ is randomly selected (Here, we mentioned that the polynomial is vanishing because it is only used in this phase and then removed in the decryption phase).

Finally, the public key $\mathfrak{U}$ is used to calculate the ciphertext $\mathfrak{E}$ as follows:

$$\mathfrak{E}\ \equiv p\mathfrak{U} * \Phi + M\ mod\ q.$$

*3.2.1. Decryption.* In the decryption stage, the private key F is multiplied by the ciphertext $\mathfrak{E}$ from the left as follows:
Take

$$\begin{aligned}\mathfrak{V} &\equiv (F * \mathfrak{E}) \ mod\ q \\ &\equiv (F * (p\mathfrak{U} * \Phi + M)) \ mod\ q \\ &\equiv (F * p\mathfrak{U} * \Phi + F * M) \ mod\ q \\ &\equiv (pF * {F_q}^{-1} * \mathfrak{G} \ * \Phi + F * M) \ mod\ q \\ &\equiv (p\mathfrak{G} * \Phi + F * M) \ mod\ q,\end{aligned}$$

So that the coefficients of the last quantity lie in the interval $\left(-\frac{q}{2}, \frac{q}{2}\right]$.

Convert $\mathfrak{V}$ from *mod* $q$ to *mod* $p$, then

$$\begin{aligned}\mathfrak{Y} &\equiv \mathfrak{V} \ mod\ p \\ &\equiv (p\mathfrak{G} * \Phi + F * M) \ \ mod\ p \\ &\equiv F * M \ mod\ p\end{aligned}$$

Hence, $M \equiv {F_p}^{-1}\mathfrak{Y}$ *mod* $p$, where the coefficients of the last quantity lie in the interval $\left(-\frac{p}{2}, \frac{p}{2}\right]$.

## 4. Space Security of Key and Message

The security level of ELTRU depends on the sample space of the subsets to which the private keys belong, both during the key generation phase (key security level) and during the encryption phase (message security level). Attackers attempt to test keys for each subset until they reach a plaintext or a readable text. Assuming that subset $\mathcal{L}_G$ is smaller than $\mathcal{L}_F$, the sample space for key security is as follows:

$$\begin{aligned}\binom{N}{d_d}\binom{N-d_g}{d_g} &= \left(\frac{N!}{d_g!\,(N-d_g)!}\right)\left(\frac{(N-d_g)!}{d_g!\,(N-2d_g)!}\right) \\ &= \frac{N!}{(d_g!)^2\,(N-2d_g)!}.\end{aligned}$$

The message security level, which depends on the sample space of subset $\mathcal{L}_\Phi$ to which key $\Phi$ belongs, is as follows:

$$\begin{aligned}\binom{N}{d_\Phi}\binom{N-d_\Phi}{d_\Phi} &= \left(\frac{N!}{d_\Phi!\,(N-d_\Phi)!}\right)\left(\frac{(N-d_\Phi)!}{d_\Phi!\,(N-2d_\Phi)!}\right) \\ &= \frac{N!}{(d_\Phi!)^2\,(N-2d_\Phi)!}.\end{aligned}$$

## 5. Conclusions

ELTRU is an advanced alternative to NTRU, capable of processing multiple data streams from a single or multiple sources simultaneously and with high efficiency. This is a vital feature for the modern business market, which increasingly requires solutions capable of handling large and complex data. From a security perspective, ELTRU achieves a higher level of security than the original NTRU and outperforms other alternative encryption systems such as QTRU and OTRU. In terms of performance, it is faster than QTRU and OTRU due to the reduced number of boundary multiplications required in the three-stage multiplication process, but slower than NTRU. Together, these features represent a paradigm shift in multidimensional encryption methods, as ELTRU combines security with execution time, making it a promising candidate for use in modern applications that require secure and efficient processing of data from multiple sources.

## References


1. 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.
2. 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.
3. 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(1):060006, 2022.
4. N. M. Al-Saidi and H. R. Yassein. Bitru: Binary version of the ntru public key cryptosystem via binary algebra. *International Journal of Advanced Computer Science and Applications*, 7(11):1–6, 2016.
5. N. M. G. 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*, 11:29–43, 2017.
6. D. Coppersmith and A. Shamir. Lattice attacks on ntru. In W. Fumy, editor, *Advances in Cryptology — EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 52–61, Berlin, Heidelberg, 1997. Springer.
7. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.
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. B. Y. Hussein. Equivalent locally martingale measure for the deflator process on ordered banach algebra. *Journal of Mathematics*, 2020(1):5785098, 2020.
10. X. Lei and X. Liao. Ntru-ke: A lattice-based public key exchange protocol. *IACR Cryptology ePrint Archive*, 718, 2013.
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*, pages 83–90, Tehran, Iran, 2010. IEEE.
12. E. Malekian, A. Zakerolhosseini, and A. Mashatan. Qtru: Quaternionic version of the ntru public-key cryptosystems. *ISeCure*, 3(1):29–42, 2011.
13. M. Nevins, C. Karimianpour, and A. Miri. Ntru over rings beyond. *Designs, Codes and Cryptography*, 56(1):65–78, 2010.
14. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
15. R. Schoof. Elliptic curves over finite fields and the computation of square roots *mod p*. *Mathematics of Computation*, 44(170):483–494, 1985.
16. S. H. Shahhadi and H. R. Yassein. A new design of ntru encrypt-analog cryptosystem with high security and performance level via tripternion algebra. *International Journal of Mathematics and Computer Science*, 16(4):1515–1522, 2021.
17. 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.
18. 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, 2007.
19. H. R. Yassein. Ntrsh: A new secure variant of ntruencrypt based on tripternion algebra. *Journal of Physics: Conference Series*, 1999(1):012092, 2021.
20. H. R. Yassein and N. M. Al-Saidi. HXDTRU Cryptosystem Based on Hexadecnion Algebra. In *Proceedings of the 5th International Cryptology and Information Security Conference (Cryptology2016)*, Malaysia, 2016.
21. H. R. Yassein and N. M. G. Al-Saidi. A comparative performance analysis of ntru and its variant cryptosystems. In *2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, pages 115–120, Sulaymaniyah, Iraq, 2017. IEEE.
22. 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.
23. 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(1):49–53, 2023.


*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