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

(3s.) **v. 2025 (43) 3** : 1–3.
ISSN-0037-8712
doi:10.5269/bspm.78827

Building a More Secure Cryptosystem Using Tripternion Algebra and Polynomials

Alaa Kamil Jabber

ABSTRACT: There are many modern encryption methods, but the rapid development in the field of software and algorithm design has made the development of these methods or the design of new encryption methods a necessity. In this paper, we have developed a multidimensional encryption system based on the analysis of polynomials and triangular algebra to obtain an efficient system.

Key Words: Tripternion algebra, security analysis.

Contents

1. Introduction

A number of researchers have conducted numerous studies in the field of developing encryption methods that rely on polynomials in order to meet the challenges of maintaining data confidentiality. The most important of these studies are:

Svensson proposed polynomials RSA based on ring of polynomials, 2015 [1]. Shahhadi and Yassein introduced tripternion algebra to design NTRsh cryptosystem with high security, 2021 [2]. Atea and Yassein proposed new system by mixed NTRU and MRSA to getting efficiency system, 2023 [3]. Zhang et al. proposed public key via RSA and chebyshev polynomials, 2024 [4]. Also, in the same year Hamza et al. using octonion algebra with eight dimension to develop MRSA [5]. Abass and Yassein, proposed improvement of MRSA by tri-cartsian algebra to increase security and presented comparison between polynomial RSA, NTRU, and PH-RSA in terms of the security [6,7]. In 2025, Ajeena et al. presented OP-RSA cryptosystem via algebra of octonion to getting more efficacy [8]. Also, Abdul-Zahra and Yassein suggest new system based on multidimensional algebra to improved polynomial RSA cryptosystem [9].

2. TNPRS Cryptosystem

TNPRS (Tripternion polynomial RSA) public key cryptosystem depends on the tripternion algebra $\mathbb{T} = \{a + bx + cx^2 \; where \; a, b, c \in Z_p\left[\gamma\right]\}$ [2] where $Z_p\left[\gamma\right] = \{a_0 + a_1\gamma + a_2\gamma^2 + \ldots + a_\tau\gamma^\tau | a_0 \in Z_p, \tau \geq 1, \; p \; is \; prime \; number\}$ is polynomials ring with addition and multiplication modulo a polynomial [1].

The following three phases constitute the construction of this system.

I. Key Generation

Select $\mathcal{T}\left(\gamma\right), \mathcal{J}\left(\gamma\right) \in \mathbb{T}$ irreducible polynomial and not associated where
$\mathcal{T}\left(\gamma\right) = \vartheta_0(\gamma) + \vartheta_1\left(\gamma\right)x + \vartheta_2(\gamma)x^2$ and
$\mathcal{J}\left(\gamma\right) = \xi_0(\gamma) + \; \xi_1\left(\gamma\right)x + \xi_2(\gamma)x^2$ such that
$\vartheta_0\left(\gamma\right), \; \vartheta_1\left(\gamma\right), \; \vartheta_2\left(\gamma\right), \; \xi_0\left(\gamma\right), \; \xi_1\left(\gamma\right), \; \xi_2(\gamma) \in Z_p[\gamma]$

- Compute $\mathfrak{U}\left(\gamma\right) = \mathcal{T}\left(\gamma\right)\mathcal{J}\left(\gamma\right)$ and take $\mathfrak{V} = \mathcal{T}\left(x\right)/\mathfrak{U}\left(\gamma\right) = \{$all possible remainders when any polynomial in $\mathbb{T}$ is divided by $\mathfrak{U}\left(\gamma\right)\}$ and $\mathfrak{d} =$ number elements in $\mathfrak{V}$ which invariable modulo $\mathfrak{U}\left(\gamma\right)$.

2010 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted September 07, 2025. Published October 07, 2025

- Choose $\mathfrak{x} \in Z_{\mathfrak{d}} = \{1, 2, \ldots,\ \mathfrak{d} - 1\}$ such that $\gcd(\mathfrak{x}, \mathfrak{d}\ ) = 1$ and find $\mathfrak{q} \in Z_{\mathfrak{d}}$ such that $\mathfrak{x}\mathfrak{q} \equiv 1\ mod\ \mathfrak{d}\,(\mathfrak{x}\mathfrak{q} = \mathfrak{d}k + 1\ ,\ k\ \ an\ integer)$.

II. Encryption

First, the original text $\mathbb{M}(\gamma)$ is converted to the following format:
$\mathbb{M}\,(\gamma) = m_0(\gamma) +\ m_1\,(\gamma)\,x + m_2(\gamma)x^2$
The ciphertext compute as the formula

$$\mathcal{C}\,(\gamma) \equiv (m_0\,(\gamma) +\ m_1\,(\gamma)\,x + m_2\,(\gamma)\,x^2\ )^e\ mod\ \mathfrak{U}\,(\gamma)$$

III- Decryption

To convert the encrypted text to plain text, we perform the following steps:

$$[\mathcal{C}(\gamma)]^q \equiv [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{x}\mathfrak{q}}\ mod\ \mathfrak{U}\,(\gamma)$$

$$\equiv [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{d}k+1}\ mod\ \mathfrak{U}\,(\gamma)$$

$$\equiv [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{d}k+1}[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]\ mod\ \mathfrak{U}\,(\gamma)$$

$$\equiv [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{d}k}[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]\ mod\ \mathfrak{U}\,(\gamma)$$

If $\mathbb{M}\,(\gamma)$ has no inverse modulo $\mathfrak{U}\,(\gamma)$ then substituting $\mathfrak{d}$ by congruence modulo $\mathcal{T}\,(\gamma)$ and $\mathcal{J}\,(\gamma)$ respectively:
$[[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{(p^r-1)(p^s-1)}]^k[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]$

$$\equiv [[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{(p^r-1)}]^{k(p^s-1)}[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]\ mod\ \mathcal{T}\,(\gamma)$$

$$[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{x}\mathfrak{q}}\ \equiv [1]^{k(p^s-1)}[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]\ mod\ \mathcal{T}\,(\gamma)$$

$$[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{x}\mathfrak{q}}\ \equiv [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]\ mod\ \mathcal{T}\,(\gamma)$$

$$[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{x}\mathfrak{q}}\ - [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2] \equiv 0\ mod\ \mathcal{T}\,(\gamma)$$

Like same way
$[[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{(p^r-1)(p^s-1)}]^k[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]$

$$\equiv [[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{(p^s-1)}]^{k(p^r-1)}[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]\ mod\ \mathcal{J}\,(\gamma)$$

$$[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{x}\mathfrak{q}}\ \equiv [1]^{k(p^r-1)}[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]\ mod\ \mathcal{J}\,(\gamma)$$

$$[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{x}\mathfrak{q}}\ \equiv [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]\ mod\ \mathcal{J}\,(\gamma)$$

$$[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{x}\mathfrak{q}}\ - [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2] \equiv 0\ mod\ \mathcal{J}\,(\gamma)$$

Therefore,

$$[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{x}\mathfrak{q}}\ - [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2] \equiv 0\ mod\ \mathcal{T}\,(\gamma)\,\mathcal{J}\,(\gamma)$$

$$[m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]^{\mathfrak{x}\mathfrak{q}}\ \equiv [m_0(\gamma) + m_0(\gamma)x + m_0(\gamma)x^2]\ mod\ \mathcal{J}\,(\gamma)$$

3. Security Analysis

The security of any encryption system depends on the size of the sample space for the private keys. The larger the space, the more work the attacker has to do to reach the correct key that leads him to the original text. Given that the proposed system relies on three-dimensional algebra, which increases the size of the space significantly, if we assume that the size of the space is #, the security of the method is as follows:

$$(\#, (\mathcal{T}\,(\gamma))^3\ or\ (\#(\mathcal{J}\,(\gamma))^3.$$

4. Conclusions

The world is witnessing rapid developments in data technology and its transmission via various media, making it vulnerable to numerous hacking methods. This necessitates constantly evolving encryption systems to keep pace with the improvements made by other parties. The TNPRS method, which relies on polynomial analysis, a challenging problem, has significantly enhanced security compared to previous methods such as RSA and polynomial RSA, making it effective for many organizations whose data requires encryption

References

1. N. per-Svensson, *polynomial based RSA*, Linnaeus university, Bachelor Thesis, 2015.
2. S. H. shahhadi and H. R. Yassein, *NTRsh: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra*, Journal of physics conference series, vol. 1999, pp. 2-6, 2021.
3. F. R. Atea and H. R. Yassein, *PMRSA: Designing an Efficient and Secure Public-Key Similar to RSA Based on Polynomial Ring*, Applied Mathematics & Information Sciences, vol. 17, 2023, pp. 535-538.
4. C. Zhang, Y. Liang , A. Tavares, L. Wang, T. Gomes, and S. Pinto, *An Improved Public Key Cryptographic Algorithm Based on Chebyshev Polynomials and RSA*, Symmetry, 16(30) pp.1-15, 2024.
5. M. H. Hamza, S. M. Abboud, and, H. R. Yassein, *Development of Modified RSA Cryptosystem via Octonion Algebra*, [5] 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 Vol. 20, no. 1, (2025), 459–464.
6. B. N. Abass and H. R. Yassein, *Comparison between NTRU, Polynomial RSA, and PH-RSA*, E3s Web of Conferences, 2024.
7. B. N. Abbas, and H. R. Yassein, *Design of an Alternative to Polynomial Modified RSA Algorithm*, Computer Science, 2024, 19(3), 693-696.
8. 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, Vol. 20, no. 1, (2025), 281–284.
9. D. S. Abdul-Zahra and H. R. Yassein, *Proposed development of RSA via new multidimensional algebra*, Journal of Discrete Mathematical Sciences and Cryptography, vol. 28, no. 2, 2025, pp. 375-380.

Alaa Kamil Jabber,
Department of Mathematics,
College of Education, University of Al-Qadisiyah,
Iraq.
E-mail address: alaa_almosawi@qu.edu.iq