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

(3s.) **v. 2025 (43) 3** : 1–4.
ISSN-0037-8712
doi:10.5269/bspm.78684

Developing MRSA Encryption Based on Triptrion Algebra

Alaa Kamil Jabber

ABSTRACT: Encryption algorithms are a pressing need for protecting sensitive information and data, as well as for establishing infrastructure in technology security, electronic communication methods, and internet security. The RSA algorithm is one of the most important algorithms for protecting information through the process it performs. In this paper we present the development of the MRSA by adopting the triptrion algebra in building the proposed system.

Key Words: MRSA, triptrion algebra, security analysis.

Contents

1. Introduction

RSA cryptosystem proposed in 1978 by Rivest, et al. [1], utilizes larger keys and requires more complex encryption and decryption operations, demanding significant memory and time to achieve a comparable level of security. Glenn et al., 2002 [2] proposed a cryptanalysis of RSA using algebraic and lattice methods of RSA. Atea and Yassein proposed a new system by mixing NTRU and RSA to enhance safety and efficiency [3]. Abass and Yassein proposed TPRSA via Tri-Cartesian algebra and polynomials as an alternative to the modified RSA 2024 [4]. Also, they are presented a comparison between three public ket cryptostems [5]. Abo-Alsood et al, presented an improvements to RSA by using HH-Real algebra to increase security [6]. In 2025, Abboud et al. [7] introduced new version of the RSA public key cryptosystem via octonion polynomials. Also, Shareef et al. suggested HH-MRSA system via HH-Real algebra [8]. Abdul-Zahra and Yassein introduced a new cryptosystem based on polynomial RSA and a new multidimensional algebra [9]. Hamza et al. [10] introduced a modified RSA cryptosystem by octonion algebra and a new mathematical structure of the modified RSA.

Abbas and Yassein [11], introduced a new cryptosystems PH-RSA based on hexadecnion Polynomials and TPRSA which an alternative to the modified RSA encryption [12].

2. TPMRS Cryptosystem

TPMR (Triptrion Polynomial Modified RSA) depend on the same generic parameters in polynomial RSA, and the ring of polynomials

$$Z_\tau\left[\varphi\right] = \left\{z_0 + z_1\varphi + z_2\varphi^2 + ... + z_j\varphi^j | j \geq 0, z_j \in Z_\tau\right\}$$

where τ is a prime and the addition and multiplication operations are done modulo a polynomial replaced by tripternion algebra and the subsets $\Delta_1, \Delta_2, \Delta_3$ *and* $\Delta_4 \subset \mathbb{T}$ are defined as:

$$\Delta_1 = \left\{v_0(\varphi) + v_1(\varphi)x + v_2(\varphi)x^2 \; | v_0, v_1, v_2 \in Z_\tau\left[\varphi\right]\right\},$$

$$\Delta_2 = \left\{\vartheta_0(\varphi) + \vartheta_1(\varphi)x + \vartheta_2(\varphi)x^2 \; | \vartheta_0, \vartheta_1, \vartheta_2 \in Z_\tau\left[\varphi\right]\right\},$$

2010 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted August 29, 2025. Published October 07, 2025

$$\Delta_3 = \left\{\theta_0(\varphi) + \theta_1(\varphi)x + \theta_2(\varphi)x^2 \ |\theta_0, \theta_1, \theta_2 \in Z_\tau\left[\varphi\right]\right\},$$

$$\Delta_4 = \left\{\eta_0(\varphi) + \eta_1(\varphi)x + \eta_2(\varphi)x^2 \ |\eta_0, \eta_1, \eta_2 \in Z_\tau\left[\varphi\right]\right\},$$

Description of the proposed system:

I. Key Generation

By random selection of items $\wp_1(\varphi) \in \Delta_1, \wp_2(\varphi) \in \Delta_2, \wp_3(\varphi) \in \Delta_3, and \wp_4(\varphi) \in \Delta_4$, such that:

$$\wp_1(\varphi) = v_0(\varphi) + v_1(\varphi)x + v_2(\varphi)x^2$$
$$\wp_2(\varphi) = \vartheta_0(\varphi) + \vartheta_1(\varphi)x + \vartheta_2(\varphi)x^2$$
$$\wp_3(\varphi) = \theta_0(\varphi) + \theta_1(\varphi)x + \theta_2(\varphi)x^2$$

and

$$\wp_4(\varphi) = \eta_0(\varphi) + \eta_1(\varphi)x + \eta_2(\varphi)x^2$$

then compute $\mathbb{N}_1(\varphi) = \wp_1(\varphi)\wp_2(\varphi)$ and $\mathbb{N}_2(\varphi) = \wp_3(\varphi)\wp_4(\varphi)$, which is the number of the invertible elements in TPMR modulo $\mathbb{N}_1(\varphi)$ and $\mathbb{N}_2(\varphi)$ respectively such that $\sigma_1 = (\tau^{n_1} - 1)(\tau^{n_2} - 1)$ and $\sigma_2 = (\tau^{n_3} - 1)(\tau^{n_4} - 1)$ where t degree of $\wp_1$, c degree of $\wp_2$, d degree of $\wp_3$ and g degree of $\wp_4$.

Now, compute $\mathbb{N}(\varphi) = \wp_1(\varphi)\wp_2(\varphi)\wp_3(\varphi)\wp_4(\varphi)$ such that

$$\sigma = (\tau^{n_1} - 1)(\tau^{n_2} - 1)(\tau^{n_3} - 1)(\tau^{n_4} - 1)$$

Suppose Ψ such that

$\Psi = \mathbb{T}/ < \mathbb{N}(\varphi) >= \{All\ choices\ remainders\ where\ every\ polynomial \in \mathbb{T}\ is\ divided\ by\ \mathbb{N}(\varphi)\}$.

Select $1 \leq \varrho < \sigma$ such that $gcd(\varrho,\ \sigma) = 1$ such that $\mathfrak{T}$ is multiplication inverse of ϱ.

II. Encryption To convert plaintext $\mathcal{M} = \varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2$ to ciphertext $\mathbb{C}\ (\varphi)$ we use the following formula:

$$\mathbb{C}(\varphi) \equiv (\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2)^\varrho \ mod\ \mathbb{N}(\varphi).$$

III. Decryption After the encrypted message reaches the recipient through the transmission medium, in order for him to understand its contents, he follows a number of steps, as follows:

$$\mathbb{C}(\varphi) \equiv ((\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2)^\varrho)^{\mathfrak{T}} \ mod\ \mathbb{N}(\varphi).$$

Since,

$$\mathfrak{T}\varrho \equiv 1\ mod\ \sigma\ then\ \mathfrak{T}\varrho = \sigma\eta + 1,$$
$$(\mathbb{C}(\varphi))^{\mathfrak{T}} = ((\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2)^\varrho)^\eta \ mod\ \mathbb{N}(\varphi).$$

If $\mathcal{M}$ is invertible mod $\mathbb{N}(\varphi)$ then

$$(\mathbb{C}(\varphi))^{\mathfrak{T}} \equiv ((\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2)^\varrho)^\eta(\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2) \ mod\ \mathbb{N}(\varphi).$$
$$\equiv (1)^\eta(\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2) \ mod\ \mathbb{N}(\varphi). \qquad .$$
$$\equiv (\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2) \ mod\ \mathbb{N}(\varphi). \qquad .$$

If $\mathcal{M}$ has no inverse modulo $\mathbb{N}(\varphi)$ then

$$((\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2)^{(\tau^{n_1}-1)(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)})^\eta(\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2) \ mod\ \wp_1(\varphi)$$

$$\equiv ((\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2)^{(\tau^{n_1}-1))})^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2) \ mod\ \wp_1(\varphi)$$

$$\equiv (-1)^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2) \ mod\ \wp_1(\varphi).$$

$$((\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2)^{(\tau^{n_1}-1)(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)})^\eta(\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2) \ mod\ \wp_2(\varphi)$$

$$\equiv ((\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2)^{(\tau^{n_1}-1))})^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2) \ mod\ \wp_2(\varphi)$$

$$\equiv (-1)^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi) + \varpi_1(\varphi)x + \varpi_2(\varphi)x^2) \ mod\ \wp_2(\varphi).$$

$$((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{(\tau^{n_1}-1)(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)})^{\eta}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_3(\varphi)$$
$$\equiv((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{(\tau^{n_1}-1))})^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_3(\varphi)$$
$$\equiv(-1)^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_3(\varphi).$$
$$((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{(\tau^{n_1}-1)(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)})^{\eta}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_4(\varphi)$$
$$\equiv((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{(\tau^{n_1}-1))})^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_4(\varphi)$$
$$\equiv(-1)^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_4(\varphi).$$

Therefore,

$$(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}\equiv(-1)^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_1(\varphi)$$
$$(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}\equiv(-1)^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_2(\varphi)$$
$$(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}\equiv(-1)^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_3(\varphi)$$
$$(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}\equiv(-1)^{\eta(\tau^{n_2}-1)(\tau^{n_3}-1)(\tau^{n_4}-1)}(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)\ mod\ \wp_4(\varphi)$$

Hence,

$$((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}-(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2))\equiv 0\ mod\ \wp_1(\varphi)$$
$$((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}-(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2))\equiv 0\ mod\ \wp_2(\varphi)$$
$$((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}-(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2))\equiv 0\ mod\ \wp_3(\varphi)$$
$$((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}-(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2))\equiv 0\ mod\ \wp_4(\varphi)$$

Therefore,
$((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}-(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2))$ divisible by $\wp_1(\varphi), \wp_2(\varphi), \wp_3(\varphi), \wp_4(\varphi)$
And so

$$((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}-(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2))\equiv 0\ mod\ \mathbb{N}(\varphi)$$
$$((\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2)^{\mathfrak{T}_{\varrho}}\equiv(\varpi_0(\varphi)+\varpi_1(\varphi)x+\varpi_2(\varphi)x^2))\ mod\ \mathbb{N}(\varphi)$$

3. Security of TPMR

An attacker using the TPMR ciphertext needs to know three of the four private keys $\wp_1(u), \wp_2(u), wp_3(u), \wp_4(u)$. Therefore, the security of this method depends on the sample space $(|\ |)$ for each set of private keys. Therefore, the number of attempts if $\wp_1(u), \wp_2(u), \wp_3(u)$ are selected is as follows:

$$(|\wp_1(u)|\wp_2(u)|\wp_3(u)|)^3$$

(The appearance of the number 3 in the exponent of the law is due to the fact that each element in triptrion algebra consists of three elements)

This is the case for the remaining key selections the attacker is looking for. This method is considered more secure than RSA and many of its improvements, as well as MRSA and some of its improvements.

4. Conclusions

The proposed TPMR system is an improvement of the MRSA system by relying on the analysis of polynomials instead of integers through multi-dimensional triptrion algebra, which greatly increases the level of security compared to RSA and MRSA, taking into account that MRSA is a special case of TPMR when the coefficients of x and x^2 equal one, in addition to the advantage of multiple encrypted messages at the same time due to the multi-dimensionality of the algebra.

References

1. R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, 1978, 21(2), 120-126.

2. G. Durfee, *Cryptanalysis of RSA using algebraic and lattice methods*, Doctoral dissertation, Stanford University, 2002.

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. B. N. Abass and H. R. Yassein, *Design of an alternative to polynomial modified RSA algorithm*, Int. J. Math. Comput. Sci, Vol.19, no. 3, 2024, pp. 693-696.

5. B. N. Abass and H. R. Yassein, *Comparison between NTRU, Polynomial RSA, and PH-RSA*, E3S Web of Conferences, vol. 508,2024, pp. 1-5.

6. H. H. Abo-Alsood, M.H. Hamza, S. A. Al-Bairmani, and H. R. Yassein, *Development of Public Key Cryptosystem RSA via Multidimensional Algebra*, International Journal of Mathematics and Computer Science, vol.19, no. 4, 2024, pp. 1177-1182.

7. S. M. Abboud, R. K. K. Ajeena, and H. R. Yassein, *Octonion Polynomials for a More Secure RSA Public Key Cryptosystem*, 2025.

8. 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, Vol. 28, no. 2, 2025, pp. 557-564.

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.

10. 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 Volume 20, Issue no. 1, (2025), 459–464.

11. B. N. Abbas, and H. R. Yassein, *A High-Security Encryption Based on Hexadecnion Polynomials*, Computer Science, 2024, 19(1), 37-40.

12. B. N. Abbas, and H. R. Yassein, *Design of an Alternative to Polynomial Modified RSA Algorithm*, Computer Science, 2024, 19(3), 693-696.

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