International Journal of Mathematics and
Computer Science, **19**(2024), no. 3, 693–696

Design of an Alternative to Polynomial Modified RSA Algorithm

Banen Najah Abass[1], Hassan Rashed Yassein[2]

[1]Department of Mathematics
Faculty of Education for Girls
University of Kufa
Al Najaf, Iraq.

[2]Department of Mathematics
College of Education
University of Al-Qadisiyah
Al-Qadisiyah, Iraq.

Email: banenn.alkuzai@uokufa.edu.iq, hassan.yaseen@qu.edu.iq

(Received December 2, 2023, Accepted January 6, 2024,
Published February 12, 2024)

Abstract

The modified RSA provides high efficiency against attacks and, as a result, it is considered the ideal choice for many applications. In this paper, we introduce an alternative to the modified RSA key encryption system called TPRSA, based on Tri-Cartesian algebra and polynomials, by modifying the mathematical structure of text encryption and decryption keys to obtain a high level of security.

1 Introduction

In 1978, Rivest et al. proposed the famous RSA algorithm which is widely used in many applications, including cryptography in secure online communications and securing data and financial transactions online [1]. In 1996,

Key words and phrases: Polynomial RSA, Tri-Cartesian algebra, modified RSA, security of key.
AMS (MOS) Subject Classifications: 94A60, 68P25.
ISSN 1814-0432, 2024, http://ijmcs.future-in-tech.net

Hoffstein et al. introduced the NTRU public key cryptosystem by using the ring of truncated polynomials $Z[x]/(x^N - 1)$ [2].

Many researchers have made many improvements to the NTRU by replacing the ring $Z[x]/(x^N - 1)$ with a different algebraic structure or a different mathematical structure. Some of those improvements are OTRU, HXDTRU, BCTRU, QTNTR, using octonion algebra, hexadecnion, bi-cartesian and quintuple algebra respectively which greatly increased security [3, 4, 5, 6]. In 2012, Ivy et al. presented a modified version of the RSA that relies on a set of "n" prime integers [7]. Also, Dhakar et al. proposed a modified RSA encryption algorithm [8]. In 2015, Gafitoiu introduced polynomial-based RSA, based on additive homomorphic properties, by replacing numbers with polynomials [9]. In 2023, Atea and Yassein designed a public key PMRSA based on a polynomial ring [10].

In this paper, we used a modified RSA encryption system which is an algorithm to deal with polynomials and provide security.

2 Proposed TPRSA Cryptosystem

A public key TPRSA cryptosystem is determined by the same parameters as polynomial RAS but the polynomial ring $Z_p[x]$ is replaced by tri-cartesian algebra $TC = \{\phi_0, \phi_1, \phi_2(1+1) + (\phi_3, \phi_4, \phi_5)(k, 1) \mid \phi_0, \ldots, \phi_5 \in F\}$ [10]. The subsets L_V, L_Q, L_W and L_G are defined as:
$L_V = \{(v_0, v_1, v_2)(1, 1) + (v_3, v_4, v_5)(k, 1) \in TC$ satisfying $\tau(d_V, d_{V-1})\}$ and
$L_Q = \{(q_0, q_1, q_2)\ (1, 1) + (q_3, q_4, q_5)(k, 1) \in TC$ satisfying $\tau(d_Q, d_{Q-1})\}$,
L_W, L_G are subsets defined as L_Q, where $\tau(d_x, d_y) = \{d_x$ coefficients equal to 1, d_y coefficients equal to -1, and the rest are $0\}$.
This cryptosystem goes through three phases that are explained below:

I. **Key Generation Phase:** In this phase, the key is generated as follows:

(a) Choose four polynomials as well as unrelated $V(x) \in L_V, Q(x) \in L_Q, W(x) \in L_W$ and $G(x) \in L_G$, do the following:
$V(x) = (v_0, v_1, v_2)(1, 1) + (v_3, v_4, v_5)(k, 1)$,
$Q(x) = (q_0, q_1, q_2)(1, 1) + (q_3, q_4, q_5)(k, 1)$,
$W(x) = (w_0, w_1, w_2)(1, 1) + (w_3, w_4, w_5)(k, 1)$ and
$G(x) = (g_0, g_1, g_2)(1, 1) + (g_3, g_4, g_5)(k, 1)$
Such that $V(x)Q(x)W(x)G(x) = N(x)$

(b) Take R, S such that $R = TC/ < N(x) >$ and S = number of invariable elements in R modulo $N(x)$.

(c) Select $e \in Z_s$ such that $g.c.d(e, s) = 1$

(d) Find $d \in Z_s$ such that $de = 1 \ mod \ s$.

II. **Encryption:** Message $M(x)$ is encrypted with the public key e and the following formula:
$C(x) = [(m_0, m_1, m_2)(1, 1) + (m_3, m_4, m_5)(k, 1)]^e \ mod \ N(x)$.

III. **Decryption:** In order to recover the original message $M(x)$, the recipient at this phase uses the following formula:
$C[x]^d = (m_0, m_1, m_2)(1, 1) + (m_3, m_4, m_5)(k, 1)$.

3 Security Analysis of TPRSA

In a brute force attack, assault takes advantage of public parameters and $N(x) = \{(\alpha_0, \alpha_1, \alpha_2)(1, 1) + (\alpha_3, \alpha_4, \alpha_5)(k, 1) \mid \alpha_0, \ldots, \alpha_5 \in F\}$.

Since there were four polynomials involved, the hacker would have to search three sets of the four sets $V(x), Q(x), W(x), G(x)$. The space security of each of $V(x), Q(x), W(x)$, and $G(x)$ is calculated as follows:
$\left(\frac{n_1!}{(d_v!)^2(n_1-2d_v)!}\right)^6, 1 \leq n_1 < n-1,$
$\left(\frac{n_2!}{(d_q!)^2(n_2-2d_q)!}\right)^6, 1 \leq n_2 < n-1,$
$\left(\frac{n_3!}{(d_w!)^2(n_3-2d_w)!}\right)^6, 1 \leq n_3 < n-1,$
$\left(\frac{n_4!}{(d_g!)^2(n_4-2d_g)!}\right)^6, 1 \leq n_4 < n-1.$

4 Conclusion

In this article, we presented a new encryption method TPRSA that is superior to polynomial RSA and modified RSA in terms of security level due to its dependence on tri-cartesian algebra. With the feature of encrypting six messages simultaneously, this characteristic renders it valuable in several applications that necessitate the utilization of various sources of messages.

References

[1] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communication of the Association for Computing Machinery, **21,** no. 2, (1978), 120–126.

[2] J. Hoffstein, J. Pipher, J. H. Silverman, NTRU: A ring-based public key cryptosystem, in Algorithmic Number Theory, Proceedings of the Third International Symposium, (1998), 267–288.

[3] E. Malecian, A. Zakerolhosseini, OTRU: A non-associative and high speed public key cryptosystem, Proceeding of the 15th CSI international symposium on computer architecture and digital systems, (2010), 83–90.

[4] H. R. Yassein, N. M. Al-Saidi, HXDTRU Cryptosystem Based on Hexadecnion Algebra, Proceeding of the 6th International Cryptology and Information Security Conference, Malaysia, (2016), 1–10.

[5] H. R. Yassein, N. M. G. Al-Saidi, BCTRU: A New Secure NTRUCrypt Public Key System Based on a Newly multidimensional Algebra, Proceeding of the 6th International Cryptology and Information Security Conference, Malaysia, (2018), 1–11.

[6] H. A. Ali, H. R. Yassein, QTNTR: A New Secure NTRU Encrypt Alternative with a High Level of Security, Mathematical Statistician and Engineering Applications, **71,** no. 4, (2022), 5634–5639.

[7] B. P. Urbana Ivy, P. Mandiwa, M. Kumar, A modified RSA cryptosystem based on 'n' prime numbers, International Journal of Engineering and Computer Science, **1,** no. 2, (2012), 63–66.

[8] R. S. Dhakar, A. K. Gupta, P. sharma, Modified RSA Encryption Algorithm, Proceeding of the 2nd International Conference on Advanced Computing and Communication Technologies, (2012), 426–429.

[9] I. B. Gafitoiu, Polynomial based RSA, Bachelor Thesis, Linnaeus University, Sweden, (2015).

[10] F. R. Atea, H. R. Yassein, PMRSA: Designing an Efficient and Secure Public-Key Similar to RSA Based on Polynomial Ring, Applied Mathematics & Information Sciences, **17,** no. 3, (2023), 535–538