

Proposed development of RSA via new multidimensional algebra

Dalael Saad Abdul-Zahra *

*Department of Mathematics
Faculty of Education for Girls
University of Kufa
Kufa
Al Najaf 540011
Iraq*

Hassan Rashed Yassein [†]

*Department of Mathematics
Faculty of Education
University of Al-Qadisiyah
Al-Diwaniya 58003
Iraq*

Abstract

With the exponential growth of technology and increasing reliance on digital platforms, the security of our personal and sensitive information is constantly at risk. Data breaches and cyber threats have become very common, making it necessary for individuals and organizations to take proactive measures to protect their data by encrypting it. In this study, a new encryption method is introduced via the polynomial RSA using a new multidimensional algebra, which provides a high level of security.

Subject Classification: 94A60, 68P25.

Keywords: RSA, Polynomial-RSA, Size of security space.

* ORCID-ID: 0000-0001-5949-0671

[†] ORCID-ID: 0000-0002-6788-0247

* E-mail: dalael20175@gmail.com (corresponding Author)

[†] E-mail: hassan.yassein@qu.edu.iq

1. Introduction

In 1978, by Rivest et al. [8], RSA was invented. Public key encryption has become the most widely used and well-known system. The public key parameters in the RSA cryptosystem are based on the product N of two large prime p and q , and the public exponent e . Numerous studies on the creation of RSA were presented by the academics, including this one from 2012, in which Ivy et al. updated the RSA cypher system's algorithm to handle prime numbers and offer security by employing a prime number that is difficult to crack [5]. The polynomial RSA encryption method, which Gafitoui proposed in 2015, enhanced security by providing intricate mathematical operations for both encryption and decryption [3]. Some variables in the RSA encryption system depend on several systems, including elliptic curves such as KMOV systems [9]. Although there are some weaknesses in these systems, the basic equation of the Demetko system has been studied before in [7]. Mumtaz and Ping's latest survey [6] provides additional information on a range of RSA attacks.

A multidimensional algebra was presented by Yassein and Al-Saidi in 2016 in order to create a better cypher scheme for NTRU [11, 12]. In 2020, Yassein et al. used Carternion algebra to propose QOBTRU [13]. In 2021, Imine et al. introduced McEliece encryption via non-permutation equivalent polar codes [4]. Several researchers presented an efficient and secure public key in 2023 [10, 14-18]. In 2024, Yassein et al. proposed new cryptosystem, hexadecnon polynomial RSA (PH-RSA) [1]. In the same year, they also developed the TPRSA cryptosystem based on Tri-Cartesian algebra and polynomials [2].

In this paper, details are provided $DAH - Nin$ algebra in second section and in third section description of our submitted $DORSA$ cryptosystem, finally $DORSA$ security was introduced.

2. DAH-NIN Algebra

A new multidimensional algebra $DAH-Nin$ is introduced in this section, denoted by the symbol by $\mathcal{DO}$ and defined as follows:

$$\mathcal{DO} = \{A: A = \sum_{\alpha=0}^8 x_{\alpha} \gamma_{\alpha} \mid x_0, x_1, x_2, \dots, x_8 \in F, \gamma_0 = 1\},$$

and three operations addition (+), multiplication (*) and multiplication by scalar (.) are defined as follows:

Suppose $A, B \in \mathcal{DO}$ and $r \in F$ such that $A = \sum_{\alpha=0}^8 x_{\alpha} \gamma_{\alpha}$, $B = \sum_{\alpha=0}^8 y_{\alpha} \gamma_{\alpha}$ then

$$A + B = \sum_{\alpha=0}^8 x_{\alpha} \gamma_{\alpha} + \sum_{\alpha=0}^8 y_{\alpha} \gamma_{\alpha} = \sum_{\alpha=0}^8 (x_{\alpha} + y_{\alpha}) \gamma_{\alpha},$$

$$A * B = \sum_{\alpha=0}^8 (x_{\alpha} y_{\alpha}) \gamma_{\alpha},$$

$$\text{and } r.A = r.(\sum_{\alpha=0}^8 x_{\alpha} \gamma_{\alpha}) = \sum_{\alpha=0}^8 r.x_{\alpha} \gamma_{\alpha}.$$

$\{\gamma_0 = 1, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6, \gamma_7, \gamma_8\}$ represents the basis of the $\mathcal{DO}$ algebra.

It is clear that $\mathcal{DO}$ is a associative and commutative algebra.

3. The **DORSA** Cryptosystem

In this section, the **DORSA** Cryptosystem is defined by defining the general parameters and three phases of the system as follows:

$$Z_p[x] = \{z_0 + z_1x + z_2x^2 + \dots + z_nx^n | n \geq 0, z_i \in Z_p\}$$

where p is a prime, the operations addition and multiplication are calculate modulo a polynomial and the same parameters are used in polynomial RSA, but $\mathcal{DO}$ algebra was used instead of the polynomial ring $Z_p[x]$. The subsets L_Ω, L_ϕ , and $L_\varphi \subset \mathcal{DO}$ are defined by:

$$L_\Omega = \{f_0(x) + \sum_{i=1}^8 f_i(x)\gamma_i | f_i \in Z_p[x]\},$$

$$L_\phi = \{g_0(x) + \sum_{i=1}^8 g_i(x)\gamma_i | g_i \in Z_p[x]\}, \text{ and}$$

$$L_\varphi = \{h_0(x) + \sum_{i=1}^8 h_i(x)\gamma_i | h_i \in Z_p[x]\}.$$

The phases of the **DORSA** cryptosystem is described as follows:

I. Key generation

The key is generated through the following steps

- Choose three irreducible polynomials, associated $A_1(x) \in L_\Omega, A_2(x) \in L_\phi$ and $A_3(x) \in L_\varphi$ such that:

$$A_1(x) = f_0(x) + \sum_{i=1}^8 f_i(x)x_i,$$

$$A_2(x) = g_0(x) + \sum_{i=1}^8 g_i(x)x_i, \text{ and}$$

$$A_3(x) = h_0(x) + \sum_{i=1}^8 h_i(x)x_i$$

- Compute $N(x) = A_1(x)A_2(x)A_3(x)$ such that $s = (p^n - 1)(p^m - 1)(p^r - 1)$ number of the invertible elements in $\mathcal{DO}$ modulo $N(x)$ where n degree of $f(x)$, m degree of $g(x)$, and r degree of $h(x)$.
- Take $\Re$ such that $\Re = \mathcal{DO} / \langle N(x) \rangle = \{\text{all possible remainders such that } N(x) \text{ divides any polynomial in } \mathcal{DO}\}$.
- Choose $0 \leq e < s$ such that $\gcd(e, s) = 1$.
- Compute the multiplication inverse δ of $e \bmod s$ (i.e., $\delta e \equiv 1 \bmod s$).

II. Encryption

To get the ciphertext $C(x)$ of the original message $M(x) = m_0 + \sum_{i=1}^8 m_i(x)x_i$, the following formula is used:

$$C(x) = (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^e \bmod N(x).$$

III. Decryption

Once the ciphertext $C = C_0 + \sum_{i=1}^8 C_i(x)\gamma_i \bmod N(x)$ was obtained, to recover the original text, the recipient should complete the following steps:

$$C[x]^\delta \equiv (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^e)^{\delta} \bmod N(x).$$

Since $\delta e \equiv 1 \bmod s$ then $\delta e = sk + 1$,

$C[x]^{\delta} \equiv ((m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^s)^k (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod N(x)$ If $M(x)$ is invertible modulo $N(x)$ then,

$$\begin{aligned} C[x]^{\delta} &\equiv ((m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^s)^k (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod N(x) \\ &\equiv (1)^k (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod N(x) \\ &\equiv (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod N(x) \end{aligned}$$

If $M(x)$ has no inverse modulo $N(x)$ then,

$$\begin{aligned} &((m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^s)^k (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod A_1(x) \\ &\equiv \left((m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{(p^9-1)^2} \right)^{k(p^9-1)} (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod A_1(x), \\ &((m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^s)^k (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod A_2(x) \\ &\equiv ((m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{(p^9-1)^2})^{k(p^9-1)} (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod A_2(x), \\ &((m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^s)^k (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod A_3(x) \\ &\equiv ((m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{(p^9-1)^2})^{k(p^9-1)} (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod A_3(x), \\ &(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} \equiv (1)^{k(p^9-1)} (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod A_1(x), \\ &(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} \equiv (1)^{k(p^9-1)} (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod A_2(x), \\ &(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} \equiv (1)^{k(p^9-1)} (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod A_3(x). \end{aligned}$$

Therefore,

$$\begin{aligned} &(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} - (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \equiv 0 \bmod A_1(x), \\ &(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} - (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \equiv 0 \bmod A_2(x), \\ &(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} - (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \equiv 0 \bmod A_3(x). \end{aligned}$$

Hence, $(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} - (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)$ divisible by $A_1(x), A_2(x)$, and $A_3(x)$, it follows that

$(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} - (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)$ is divisible by $A_1(x)A_2(x)A_3(x)$ (because $A_1(x), A_2(x)$, and $A_3(x)$ are not associated and irreducible).

Therefore,

$$\begin{aligned} &(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} - (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \equiv 0 \bmod N(x), \\ &(m_0 + \sum_{i=1}^8 m_i(x)\gamma_i)^{\delta e} \equiv (m_0 + \sum_{i=1}^8 m_i(x)\gamma_i) \bmod N(x). \end{aligned}$$

4. Security of $\mathcal{DORSA}$

The security level of $\mathcal{DORSA}$ depends on the size of the space of the subsets of each of the keys that make up the public key $N(x)$. Therefore, the attacker tries two of the three keys $A_1(x), A_2(x)$ and $A_3(x)$ given that the public key is known. Therefore, the size of the key security space that constitutes the

security of the $\mathcal{DORSA}$ is as follows: $(|L_\Omega|)^9(|L_\phi|)^9$ assuming that the size of space L_ϕ is greater than the size of spaces L_Ω and L_ϕ which $| \cdot |$ denotes the size of space.

5. Conclusions

The $\mathcal{DORSA}$ cryptosystem is based on the difficulty of factoring numbers, and when factoring polynomials is used, that difficulty increases. However, in this paper, new algebra $\mathcal{DO}$ was used to increase that difficulty through each element consisting of nine polynomials, which contributes to a very high level of security, which makes this method desirable. In many electronic transactions sent via an unsecured medium.

References

- [1] B. N. Abbas and H. R. Yassein, "A high-security encryption based on hexadecion polynomials," *Int. J. Math. Comput. Sci.*, vol. 19, no. 1, pp. 37-40 (2024).
- [2] B. N. Abbas and H. R. Yassein, "Design of an alternative to polynomial modified RSA algorithm," *Int. J. Math. Comput. Sci.*, vol. 19, no. 3, pp. 693-696 (2024).
- [3] I. B. Gafitciu, Polynomial based RSA, B. Sc. Thesis, Linnaeus University, Sweden (2015).
- [4] B. Imine, N. Hadj-Said, and A. Ali-Pacha, "New McEliece cryptosystem based on non-permutation equivalent polar codes," *J. Discrete Math. Sci. Cryptogr.*, Aug. (2021). [Online]. Available: <https://doi.org/10.1080/09720529.2021.1933706>.
- [5] B. Ivy, P. Mandiwa, and M. Kumar, "A modified RSA cryptosystem based on 'n' prime numbers," *Int. J. Eng. Comput. Sci.*, vol. 1, no. 2, pp. 63-66 (2012).
- [6] M. Mumtaz and L. Ping, "Forty years of attacks on the RSA cryptosystem: A brief survey," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 1, pp. 9-29 (2019). [Online]. Available: <https://doi.org/10.1080/09720529.2018.1564201>.
- [7] A. Nitaj and E. Fouotsa, "A new attack on RSA and Demytko's elliptic curve cryptosystem," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 3, pp. 391-409 (2019). [Online]. Available: <https://doi.org/10.1080/09720529.2019.1587827>.
- [8] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120-126 (1978). [Online]. Available: <https://doi.org/10.1145/359340.359342>.

- [9] M. C. Semmouni, A. Nitaj, and M. Belkasmi, "Cryptanalysis of RSA with smooth prime sum," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 8, pp. 1-21 (2022). [Online]. Available: <https://doi.org/10.1080/09720529.2021.2000152>.
- [10] H. S. Salman and H. R. Yassein, "An innovative HSS algebra for designing a secure like-NTRU encryption," *Math. Statist. Eng. Appl.*, vol. 71, no. 4, pp. 6098-6113 (2022). [Online]. Available: <https://doi.org/10.17762/msea.v71i4.1208>.
- [11] H. R. Yassein and N. M. Al-Saidi, "BITRU: Binary version of the NTRU public key cryptosystem via binary algebra," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 11, pp. 1-6 (2016). [Online]. Available: <https://doi.org/10.14569/IJACSA.2016.071101>.
- [12] H. R. Yassein and N. M. Al-Saidi, "HXDTRU cryptosystem based on hexadecinion algebra," *Proc. 5th Int. Cryptol. Inf. Security Conf.*, Kota Kinabalu, Malaysia (2016).
- [13] H. R. Yassein, N. M. G. Al-Saidi, and A. K. Farhan, "A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 2, pp. 523-542 (2020). [Online]. Available: <https://doi.org/10.1080/09720529.2020.1741218>.
- [14] H. R. Yassein and H. A. Ali, "HUDTRU: An enhanced NTRU for data security via quintuple algebra," *Int. J. Math. Comput. Sci.*, vol. 18, no. 2, pp. 199-204 (2023).
- [15] A. H. Alwan, "Small intersection graph of subsemimodules of a semi-module," *Commun. Combinatorics Cryptogr. Comput. Sci.*, vol. 2022, no. 1, pp. 15-22 (2022).
- [16] S. Ediza, M. Cancana, and M. R. Farahani, "Eccentric connectivity and connective eccentricity indices of generalized Petersen graphs," *Commun. Combinatorics Cryptogr. Comput. Sci.*, vol. 2021, no. 1, pp. 1-6 (2021).
- [17] R. Ponraj, S. Prabhu, and M. Sivakumar, "Pair mean cordial labeling of total graph of some graphs and prism related graphs," *Commun. Combinatorics Cryptogr. Comput. Sci.*, vol. 2024, no. 2, pp. 181-192 (2024).
- [18] F. O. Oduol and I. O. Okoth, "Counting vertices among all noncrossing trees by levels and degrees," *Commun. Combinatorics Cryptogr. Comput. Sci.*, vol. 2024, no. 2, pp. 193-212 (2024).

Received May, 2024