Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 2, pp. 557-564
DOI : 10.47974/JDMSC-2255

HH-MRSA : Designing an improvement of MRSA with high security

Mohammed Hassan Hamza *
Department of Mathematics
General Directorate of Al-Muthanna Education
Al-Muthanna 66001
Iraq

and

Department of Computer Technical Engineering
College of Information Technology
Imam Ja'afar Al-Sadiq University
Al-Muthanna 66001
Iraq

Hadeel Hadi Abo-Alsood †
Department of Mathematics
Collage of Education for Pure Sciences
Al-Muthanna University
Al-Muthanna 66001
Iraq

Sahab Mohsen Abboud §
Department of Mathematics
College of Basic Education
University of Babylon
Babylon 11702
Iraq

---

* *ORCID-ID:* **0009-0006-3916-6456**
† *ORCID-ID:* **0009-0006-0069-2248**

---

* *E-mail:* **edu-math.post16@qu.edu.iq (Corresponding Author)**
† *E-mail:* **hadeel.hadi@mu.edu.iq**
§ *E-mail:* **bsc.sahab.jwer@uobabylon.edu.iq**

Hassan Rashed Yassein [‡]
Department of Mathematics
Collage of Education
University of Al-Qadisiyah
Al-Qadisiyah 54004
Iraq

Zahraa Salih Shareef [@]
Department of Computer Technical Engineering
College of Information Technology
Imam Ja'afar Al-Sadiq University
Al-Muthanna 66001
Iraq

Abstract

Modern technology has become a means of exchanging data but at the same time it helps hackers to access the data exchanged over the Internet, and the development of encryption techniques and ways to enhance security has become necessary to avoid such breaches. In this work, we have introduced a new system to improve MRSA using HH-Real algebra in the mathematical construction of the method, which gave a high level of security to its phases.

Subject Classification (2020): *94A60.*

Keywords: *RSA encryption system, QOTRU, BOTRU.*

1. Introduction

In 1978, Rivets et al. introduced the RSA encryption system based on the factorization problem [1]. In 1996, Hoffstein et al. proposed NTRU which using truncated polynomials ring [2]. Several researchers have presented a number of researches on the improvement RSA. Also, in 2012, Levy et al. developed RSA algorithm encryption [3]. In 2015, Using polynomials instead of integers, Gafitoiu proposed the polynomial RSA [4]. A number of researchers have made developments to NTRU, including: in 2010, Malakian et al. presented NTRU-like, it is called the OTRU via octonion algebra instead truncated polynomials ring [5]. In 2016 Yassein and Al- Saidi, proposed HXDTRU via Hexadecenoin algebra and BITRU via binary algebras as replacements for NTRU [6-8]. Also, they proposed BCTRU depend on Bi-cartesian algebra [9]. In 2021, Yassein et al. presented QOTRU, BOTRU and QMNTR via qu-octonion subalgebra,

[‡] *E-mail:* **hassan.yaseen@qu.edu.iq**
[@] *E-mail:* **zahraasalih1997@gmail.com**

bioctonion subalgebra, quaternion algebra respectively [10-12]. In 2022, Al-Awadi introduced QP- RSA via quaternion algebra [13]. Shihadi and Yassein [14] proposed an upgraded NTRU cryptosystem called NTRTRN. TOTRU, a cryptosystem distinguished by its efficiency and security presented by Abo-Alsood and Yassein [15]. In 2023, Atea and Yassein introduced PMRSA via a ring of polynomials [16]. Yassein et al. introduced QuiTRU based on multidimensional algebra [17]. In 2024, Abboud and Yassein, introduced OTRCQ via octonion and quaternion algebras [18]. In same year, Abo-Alsood et al. proposed HH-RSA based on QuiTRU polynomial algebra. Also, Abaas and Yassein proposed TPRSA based on Tri- cartesian algebra [19, 20]. Abboud at el. proposed OP-RSA based on octonion polynomials [21-26].

2. HH-MRSA Cryptosystem

A public key HH-MRSA uses a parameter similar to polynomial RSA, but it employs HH-Real algebra [17] instead of the polynomial ring $Z_q[x]$. Suppose that $\psi = D/< N(x) >=$ {each possible remainder with any polynomial belong to D divided by $N(x)$}, such that $D = Z_q[x]$. The subsets L_F, L_G, L_T, and L_V are defined by the Table 1.

Table 1
Subsets of HH-MRSA.

Set	Definition
L_F	$\{\sum_{i=0}^{4} f_i\tau_i \in D \setminus f_0(x), \dots, f_4(x)\ satisfy\ l(d_f, d_f)\}$
L_G	$\{\sum_{i=0}^{4} g_i\tau_i \in D \setminus g_0(x), \dots, g_4(x)\ satisfy\ l(d_g, d_g)\}$
L_J	$\{\sum_{i=0}^{4} j_i\tau_i \in D \setminus j_0(x), \dots, j_4(x)\ satisfy\ l(d_j, d_j)\}$
L_V	$\{\sum_{i=0}^{4} v_i\tau_i \in D \setminus v_0(x), \dots, v_4(x)\ satisfy\ l(d_v, d_v)\}$

Where $l(d_\alpha, d_\beta) = \{f \in D$ has d_α, d_β coeff. Equal $1, -1$ respectively, rest $0\}$.

The HH-MRSA system consists following steps.

2.1. *Generation of Key*

To create the key, the following steps are followed:

1. Choose four not associated and irreducible polynomials $\mathrm{F(x)} = \mathrm{f_0\tau_0} + \mathrm{f_1\tau_1} + \mathrm{f_2\tau_2} + \mathrm{f_3\tau_3} + \mathrm{f_4\tau_4}$, $\mathrm{G(x)} = \mathrm{g_0\tau_0} + \mathrm{g_1\tau_1} + \mathrm{g_2\tau_2} + \mathrm{g_3\tau_3} + \mathrm{g_4\tau_4}$, $\mathrm{J(x)} = \mathrm{j_0\tau_0} + \mathrm{j_1\tau_1} + \mathrm{j_2\tau_2} + \mathrm{j_3\tau_3} + \mathrm{j_4\tau_4}$ and $\mathrm{V(x)} = \mathrm{v_0\tau_0} + \mathrm{v_1\tau_1} + \mathrm{v_2\tau_2} + \mathrm{v_3\tau_3} + \mathrm{v_4\tau_4}$ from the sets $\mathrm{L_F}$, $\mathrm{L_G}$, $\mathrm{L_J}$ and $\mathrm{L_V}$ respectively.
2. Calculate $\mathrm{N_1(x)} = \mathrm{F(x)J(x)}$, $\mathrm{N_2(x)} = \mathrm{G(x)V(x)}$, $\mathrm{s_1} = (\sigma^{\mathrm{m}} - 1)(\sigma^{\mathrm{n}} - 1)$ and $\mathrm{s_2} = (\sigma^{\mathrm{r}} - 1)(\sigma^{\mathrm{t}} - 1)$ are number of invertible elements in $\psi \bmod \mathrm{N_1(x)}$ and $\bmod \mathrm{N_2(x)}$ respectively.
3. Compute $\mathrm{N(x)} = \mathrm{F(x)J(x)G(x)V(x)}$ in which $\mathrm{s} = (\sigma^{\mathrm{m}} - 1)(\sigma^{\mathrm{n}} - 1)(\sigma^{\mathrm{r}} - 1)(\sigma^{\mathrm{t}} - 1)$ number of elements which invariable in $\psi \bmod \mathrm{N(x)}$.

4. Choose e_1, e_2 belong to Z_s when $g.c.d(e_1, s) = 1, g.c.d(e_2, s) = 1$
5. Find d_1 with $d_1 e_1 = 1 \bmod s$ ($d_1 = e_1^{-1} \bmod s$), $e_1 d_1 = k_1 s + 1$ and d_2 with $d_2 e_2 = 1 \bmod s$ ($d_2 = e_2^{-1} \bmod s$) $e_2 d_2 = k_2 s + 1$.

2.2. *Encryption*

The original message $P(x)$ is transformed into ciphertext through the utilization of the formula:

$$C(x) \equiv \left([(\sum_{i=0}^{4} m_i(x)\tau_i)]^{e_1} mod\ N(x)\right)^{e_2} mod\ N(x).$$

2.3. *Decryption*

To get the plaintext $P(x)$ from the encrypted message $C(x)$, the recipient follows the steps below:

$$(C(x))^{d_1 d_2} \bmod N(x) \equiv ([(\sum_{i=0}^{4} m_i(x)\tau_i)]^{e_1 e_2})^{d_1 d_2} \bmod N(x)$$
$$\equiv \left([(\sum_{i=0}^{4} m_i(x)\tau_i)]^{e_1 d_1 e_2}\right)^{d_2} \bmod N(x)$$
$$\equiv \left([(\sum_{i=0}^{4} m_i(x)\tau_i)]^{(k_1 s+1)e_2}\right)^{d_2} \bmod N(x)$$
$$\equiv \left(\left((\sum_{i=0}^{4} m_i(x)\tau_i)\right)^{(k_1 e_2)}\left((\sum_{i=0}^{4} m_i(x)\tau_i)\right)^{e_2}\right)^{d_2} \bmod N(x)$$
$$\equiv \left((\sum_{i=0}^{4} m_i(x)\tau_i)\right)^{e_2 d_2} \bmod N(x) \equiv \left((\sum_{i=0}^{4} m_i(x)\tau_i)\right)^{sk_2+1} \bmod N(x)$$
$$\equiv \left((\sum_{i=0}^{4} m_i(x)\tau_i)\right)^{sk_2} (\sum_{i=0}^{4} m_i(x)\tau_i) \bmod N(x)$$
$$\equiv (\sum_{i=0}^{4} m_i(x)\tau_i) \bmod N(x).$$

If $P(x)$ does not have an inverse $\bmod N(x)$ then $F(x), J(x), G(x), \text{and } V(x)$ can be substituted for s, respectively.

$$(C(x))^{d_1 d_2} \bmod N(x) \equiv ([P(x)]^{e_1 e_2})^{d_1 d_2} \bmod F(x)$$
$$\equiv ([P(x)]^{e_1 e_2})^{d_1 d_2} \bmod J(x)$$
$$\equiv ([P(x)]^{e_1 e_2})^{d_1 d_2} \bmod G(x) \equiv ([P(x)]^{e_1 e_2})^{d_1 d_2} \bmod V(x)$$

By replacing s into the previous formula

$$(C(x))^{d_1 d_2} \bmod N(x) \equiv \left([P(x)]^{(sk_1+1)e_2}\right)^{d_1}$$
$$\equiv \left([P(x)]^{(((\sigma^m-1)(\sigma^n-1)(\sigma^r-1)(\sigma^t-1))k_1+1)e_2}\right)^{d_2} \bmod F(x)$$
$$\equiv \left([P(x)]^{(\sigma^m-1)(\sigma^n-1)(\sigma^r-1)(\sigma^t-1)k_1 e_2}\right)^{d_2} [P(x)]^{e_2 d_2} \bmod F(x)$$
$$\equiv \left(\left[P(x)^{(\sigma^m-1)}\right]^{(\sigma^n-1)(\sigma^r-1)(\sigma^t-1)k_1 e_2}\right)^{d_2} [P(x)]^{e_2 d_2} \bmod F(x)$$
$$\equiv (1)^{(\sigma^n-1)(\sigma^r-1)(\sigma^t-1)k_1 e_2 d_2} [P(x)]^{e_2 d_2} \bmod F(x)$$
$$\equiv [P(x)]^{e_2 d_2} \bmod F(x) \equiv [P(x)]^{sk_2+1} \bmod F(x)$$

$$\equiv [P(x)]^{sk_2}\ P(x) \bmod F(x)$$

$$\equiv [P(x)]^{(\sigma^m-1)(\sigma^n-1)(\sigma^r-1)(\sigma^t-1)k_2}\ P(x) \bmod F(x)$$

$$\equiv \left[P(x)^{(\sigma^m-1)}\right]^{(\sigma^n-1)(\sigma^r-1)(\sigma^t-1)k_2}\ P(x) \bmod F(x)$$

$$\equiv [1]^{(\sigma^n-1)(\sigma^r-1)(\sigma^t-1)k_2}\ P(x) \bmod F(x)\ \equiv\ P(x) \bmod F(x).$$

Similarly, $(C(x))^{d_1 d_2} \bmod N(x) \equiv \left([P(x)]^{(sk_1+1)e_2}\right)^{d_2}$

$$\equiv \left([P(x)]^{(((\sigma^m-1)(\sigma^n-1)(\sigma^r-1)(\sigma^t-1))k_1+1)e_2}\right)^{d_2} \bmod J(x)$$

$$\equiv [1]^{(\sigma^n-1)(\sigma^r-1)(\sigma^t-1)k_2}\ P(x) \bmod J(x)\ \equiv\ P(x) \bmod J(x)$$

$$(C(x))^{d_1 d_2} \bmod N(x) \equiv \left([P(x)]^{(sk_1+1)e_2}\right)^{d_2}$$

$$\equiv \left([P(x)]^{(((\sigma^m-1)(\sigma^n-1)(\sigma^r-1)(\sigma^t-1))k_1+1)e_2}\right)^{d_2} \bmod G(x)$$

$$\equiv [1]^{(\sigma^n-1)(\sigma^r-1)(\sigma^t-1)k_2}\ P(x) \bmod G(x)\ \equiv\ P(x) \bmod G(x).$$

$$(C(x))^{d_1 d_2} \bmod N(x) \equiv \left([P(x)]^{(sk_1+1)e_2}\right)^{d_2}$$

$$\equiv \left([P(x)]^{(((\sigma^m-1)(\sigma^n-1)(\sigma^r-1)(\sigma^t-1))k_1+1)e_2}\right)^{d_2} \bmod V(x)$$

$$\equiv [1]^{(\sigma^n-1)(\sigma^r-1)(\sigma^t-1)k_2}\ P(x) \bmod V(x)\ \equiv\ P(x) \bmod V(x).$$

3. Security Analysis of HH-MRSA

In HH-MRSA an attacker tries to getting the three private keys from the sets L_F, L_G, L_J, L_V to getting the original message. Assume the space of L_V greater than L_F, L_G, L_J then by brute force attack, therefore, the total key space is calculated as follows:

$$\left(\frac{n_1!}{(d_f!)^2(n_1-2d_f)!}\right)^5 \left(\frac{n_2!}{(d_j!)^2(n_2-2d_j)!}\right)^5 \left(\frac{n_3!}{(d_g!)^2(n_3-2d_g)!}\right)^5.$$

4. Conclusion

HH-MRSA is exhibits superior security levels compared to RSA and polynomial RSA. This superiority is attributed to its reliance on the product of four elements of the HH-Real algebra: $F(x)$, $G(x)$, $J(x)$, and $V(x) \in D$. The complexity associated with cracking the key, coupled with the increased time required due to the expanding key space, underscores how this technology enhances efficiency, dependability, and security across networks.

References

[1] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the*

ACM, vol. 21, no. 2, pp. 120-126 (1978), [Online]. Available: https://doi.org/10.1145/359340.359342.

[2] J. Hoffstein, J. Pipher, and J.H. Silverman, "NTRU: A ring-based public key cryptosystem," *Lecture Notes in Computer Science*, vol. 1423, pp. 267-288 (1998), [Online]. Available: https://doi.org/10.1007/bfb0054868.

[3] B.P.U. lvy, P. Mandiwa and M. Kumar, A modified RSA cryptosystem based on "n " prime numbers, *Int. J. Comput. Sci. Eng*, vol. 06, no. 03, pp. 78-90 (2018), [Online]. Available: https://doi.org/10.4236/jcc.2018.63006.

[4] I. B. Gafitoiu, Polynomial based RSA, B. Sc, Linnaeus University, Sweden, (2015).

[5] 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, 83-90 (2010).

[6] H.R. Yassein and N. M. Al- Saidi, HXDTRU Cryptosystem Based on Hexadecnion Algebra, Cryptology Conference (2016).

[7] N.M. Al-Saidi and H.R. Yassein, BITRU: Binary Version of the NTRU Public Key Cryptosystem via binary algebra, *Int. J. Adv. Comput. Sci. Appl.,* vol. 7, no. 11 (2016), [Online]. Available: https://doi.org/10.14569/ijacsa.2016.071101.

[8] N.M. Al-Saidi and H.R. Yassein, A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure, *Malays. J. Math. Sci.*, vol. 11, pp. 29-43 (2017).

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

[10] H.H. Abo-Alsood and H.R. Yassein, QOTRU: A new design of NTRU public key encryption via Qu- Octonion subalgebra, J. Phys. Conf. Ser., vol. 1999, no. 1, pp. 012097-012097, [Online]. Available: https://doi.org/10.1088/1742-6596/1999/1/012097.

[11] S.H. Shihadi and H.R. Yassein. A new Design of NTRU Encrypt- analogue Cryptosystem with high security and Performance level via Trip ternion algebra, *Int. J. Math. Comput. Sci.,* vol. 16, no. 4, pp. 1515-

1522 (2021), [Online]. Available: https://future-in-tech.net/16.4/r-HassanYasein.pdf

[12] H.R. Yassein, A.A. Abidalzahra and N. M. Al-Saidi, A new design of NTRU encryption with security and performance level, AIP Conference Proceedings, vol. 2334, no. 1, 08005-08009 (2021), https://doi.org/10.1063/5.0042312.

[13] M.H. Al-Awadi, Designing an Efficient and Scure Cryptosystems Similar to MaTRU and RSA, M. SC. Thesis, University of Al-Qadisiya, Iraq, (2022).

[14] S.H. Shihadi and H.R. Yassein, "An innovative tripternion algebra for designing NTRU-like cryptosystem with high security", AIP Conference Proceedings, vol. 2386, pp. 60009-1-60009-6 (2022). https://doi.org/10.1063/5.0067023

[15] H.H. Abo-alsood and H.R. Yassein, "Analogue to NTRU public key cryptosystem by multi-dimension algebra with high security'', AIP Conference Proceedings, vol. 2386, pp. 600091-600096 (2022), [Online]. Available: https://doi.org/10.1063/5.0067033.

[16] F.R. Atea and H.R. Yassein, PMRSA: Designing an Efficient and Secure Public-Key Similar to RSA Based on Polynomial Ring, Appl. Math. Info. Sci., vol. 17, no. 3, pp. 535-538, May (2023), [Online]. Available: https://doi.org/10.18576/amis/170321.

[17] 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, Appl. Math. Info. Sci., vol. 17, no. 1, pp. 49-53, Jan. (2023), [Online]. Available: https://doi.org/10.18576/amis/170107.

[18] S. M. Abboud and H.R. Yassein, Improvement Multi-Dimensional Public key OTRU Cryptosystem, *Int. J. Math. Comput. Sci.,* vol. 19, no. 4, pp. 1071-1076 (2024),

[19] H.H. Abo-Alsood, M.H. Hamza, S. A. Al-Bairmani and H.R. Yassein, HH-RSA: Development of Public key Cryptosystem RSA via multidimensional algebra, *Int. J. Math. Comput. Sci.*, vol. 19, no. 4, pp. 1177-1182 (2024). [Online]. Available: https://future-in-tech.net/19.4/R-Abo-Alsood-Hamz-Al-Bairmani-Yassein.pdf.

[20] B.N. Abaas 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, Feb. (2024),

[21] S.M. Abboud, R.K. Ajeena and H.R. Yassein, Octonion Polynomials for a More Secure RSA Public Key Cryptosystem. *Int. J. Math. Comput. Sci.*, vol. 20, no.1, pp. 281-284 (2025), [Online]. Available: https://doi.org/10.69793/ijmcs/01.2025/yassein.

[22] F. Afzal, S. Rukh, D. Afzal, M.R. Farahani, M. Cancan and S. Ediz, "A study of non-commutative Von-Neumann regular rings," *J. Inf. Optim. Sci.,* vol. 42, no. 7, pp. 1425-1436 (2021). [Online] Available: https://doi.org/10.1080/02522667.2021.1896650.

[23] M. Nadeem, S. Ahmad, M.K. Siddiqui, M.A. Ali, M.R. Farahani and A.J.M. Khalaf, "On some applications related with algebraic structures through different well known graphs," *J. Discrete Math. Sci. Cryptography,* vol. 24, no. 2, pp. 451-471 (2021). [Online] Available: https://doi.org/10.1080/0972052.

[24] S. Ediz, M. Cancan 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).

[25] 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).

[26] F.O. Oduol and I.O. Okoth, "Counting vertices among all noncross¬ing trees by levels and degrees," *Commun. Combinatorics Cryptogr. Comput. Sci.,* vol. 2024, no. 2, pp. 193-212 (2024).

Received November, 2024