International Journal of Mathematics and
Computer Science, **19**(2024), no. 4, 1177–1182

Development of Public Key Cryptosystem RSA via Multidimensional Algebra

Hadeel Hadi Abo-Alsood[1], Mohammed Hassan Hamza[2], Sukaina Abdullah Al-Bairmani[3], Hassan Rashed Yassein[4]

[1]Department of Mathematics
Collage of Education for Pure Science
Al-Muthanna University
Al-Muthanna, Iraq

[2]General Directorate of Al-Muthanna Education
Al-Muthanna, Iraq

[3]Department of Mathematics
Collage of Basic Education
University of Babylon
Hillah, Iraq

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

email: hadeel.hadi@mu.edu.iq, edu-math.post16@qu.edu.iq,
sukaina.albairmani@uobabylon.edu.iq, hassan.yaseen@qu.edu.iq

(Received April 5, 2024, Accepted May 5, 2024,
Published June 1, 2024)

Abstract

When data is shared over the public Internet, there is a possibility that it can be hacked by hackers. To prevent this, cryptosystems can be used to ensure the secure transmission of this. In this paper, we

Keywords and phrases: RSA, HH-RSA, Space of key.
AMS (MOS) Subject Classifications: 94A60, 68P25.
ISSN 1814-0432, 2024, http://ijmcs.future-in-tech.net

introduce a new public key HH-RSA that is based on five-dimensions to get high security through key creation, encryption, and decryption.

1 Introduction

The RSA cryptosystem was introduced in 1977 depending on the parameters derived from the prime [1]. In 1996, Hoffstein et al. introduced NTRU that depends on a ring of truncated polynomials [2]. Later, many studies came to develop the NTRU including MaTRU that was presented in 2005 by Coglianese and Goi depending on a ring of k by k matrices of polynomials [3]. In 2016, Yassein and Al-Saidi presented HXDTRU defined by hexadecnion algebra, and BITRU defined by binary algebra as analogs of the NTRU [4, 5, 6]. In 2017, Yassein and Al-Saidi provided a comparison of the performance of NTRU and some improvements of it [7]. Also, they proposed a new like-NTRU depends on bi-cartesian algebra called BCTRU [8, 9]. In 2020, Yassein et. al. presented tow like-NTRU which are called QOBTRU and NTRTE depending on carternion algebra and commutative quaternion algebra, respectively [10, 11]. In 2021, Yassein et. al. presented five like-NTRU called QMNTR, BOTRU, NTRS, QOTRU, and NTRSH depend on quaternon algebra, bi-octonion subalgebra, tripternion algebra, Qu-octonion subalgebra, and tripternion algebra respectively [12, 13, 14, 15, 16]. In 2022, Al-Awadi [17] proposed the public key cryptosystems MaTRUD and PQ-RSA that depend on the same algebraic structure for MaTRU and quaternion algebra. In 2023, Yassein et al. [18] proposed the public key QuiTRU using a new algebraic structure.

2 The HH-RSA Cryptosystem

The HH-RSA cryptosystem depends on the same parameter in polynomial RSA but replaces the ring of polynomial $Z_P[x]$ with HH-Real algebra [18]. Let $\Omega = D \ < N(x) >= \{$all possible remainders such that all polynomial in D divided by $N(x)\}$. The phases of HH-RSA are described as follows:

I. **Key generation:** To generate the key, we need to use the following steps:

- Select two irreducible polynomials $P(x)$ and $Q(x)$ not associated from the sets L_P, L_Q respectively, such that $P(x) = \sum_{i=0}^{4} p_i(x)\,\tau_i$ and $Q(x) = \sum_{i=0}^{4} q_i(x)\,\tau_i$

- Compute $N(x) = P(x)Q(x)$ in D and $\mathcal{S}=$ number of invariable elements in Ω modulo $N(x)$.
- Choose $e \in Z_{\mathcal{S}} = \{0, 1, 2, \ldots, \mathcal{S}-1\}$ such that $gcd\ (e,\ \mathcal{S})\ = 1$.
- Find $d \in Z_{\mathcal{S}}$ such that $ed \equiv 1\ mod\ \mathcal{S}\ (d = e^{-1}\ mod\ \mathcal{S})$.

II. **Encryption:** For any message $M(x) = \sum_{i=0}^{4} m_i(x)\,\tau_i \in \Omega$, the ciphertext $C(x)$ is computed as follows:
$C(x)\ \equiv \left(\sum_{i=0}^{4} m_i(x)\,\tau_i\right)^e\ mod\ N(x)$.

III. **Decryption:** After the encrypted text is received and the sender obtains the plaintext, he\she takes the following steps:

- If $M(x)$ is invertible modulo $N(x)$, then
$C[x]^d\ mod\ N(x) \equiv \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{ed}\ mod\ N(x)$
$\equiv \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{sk+1}\ mod\ N(x)$
$\equiv \left[\left(\sum_{i=0}^{4} m_i(x)\,\tau_i\right)^{s}\right]^{k}\ \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]\ mod\ N(x)$
$\equiv \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]\ mod\ N(x)$.
- If $M(x)$ has no inverse $mod\ N(x)$, then substituting $\mathcal{S}$ by congruence $mod\ P(x)$ and $mod\ Q(x)$ respectively:

$$C[x]^d\ mod\ N(x)\ \equiv\ \left[\left(\sum_{i=0}^{4} m_i(x)\,\tau_i\right)^{(p^m-1)(p^n-1)}\right]^{k}\ \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]\ mod\ P(x)$$

$$\equiv\ \left[\left(\sum_{i=0}^{4} m_i(x)\,\tau_i\right)^{(p^n-1)}\right]^{k(p^m-1)}\ \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]\ mod\ P(x),$$

$$C[x]^d\ mod\ N(x)\ \equiv\ \left[\left(\sum_{i=0}^{4} m_i(x)\,\tau_i\right)^{(p^m-1)(p^n-1)}\right]^{k}\ \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]$$

$$\equiv\ \left[\left(\sum_{i=0}^{4} m_i(x)\,\tau_i\right)^{(p^m-1)}\right]^{k(p^n-1)}\ \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]\ mod\ Q(x)$$

$$C[x]^d\ mod\ N(x)\ \equiv\ \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{ed}\ \equiv\ 1^{k(p^m-1)}\ \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]$$

$$\equiv \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right] \ mod\ P\,(x)\,,$$

$$\left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{ed} - \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right] \equiv 0\ mod\ P(x)$$

$$C\,[x]^d\ mod\ N\,(x) \equiv \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{ed} \equiv 1^{k(p^n-1)} \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]$$

$$\equiv \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right] \ mod\ Q\,(x)\,,$$

$$\left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{ed} - \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right] \equiv 0\ mod\ Q(x)$$

therefore,

$$\left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{ed} - \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right] \text{ is divisible by } P\,(x)\,and Q\,(x)\,.$$

Since $P\,(x)\,, Q\,(x)$ irreducible and associated, $\left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{ed} - \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]$ divisible by $P\,(x)\,Q\,(x)$. Hence $\left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{ed} - \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right] \equiv 0\ mod\ P(x)Q(x)$. and $\left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]^{ed} \equiv \left[\sum_{i=0}^{4} m_i(x)\,\tau_i\right]\ mod\ N(x)$.

3 Security Analysis

To perform a brute force attack against HH-RSA, attackers use general parameters and $N\,(x) = \sum_{i=0}^{4} a_i(x)\,\tau_i$, for the purpose of obtaining private keys $P\,(x)\ \epsilon L_P$ or $Q\,(x)\ \epsilon L_Q$. The space of key is equal to:
$\left(\frac{n_1!}{(d_p!)^2(n_1-2d_p)!}\right)^5, 1 \le n_1 \le n-1 or \left(\frac{n_2!}{(d_q!)^2(n_2-2d_q)!}\right)^5, 1 \le n_2 \le n-1.$

4 Conclusions

In this study, we introduced a new encryption algorithm called HH-RSA which relies on the HH-Real algebra. It utilizes the same structure as the original RSA but with high difficulty in polynomial factorization. The HH-RSA system enjoys a high security level compared with NTRU, polynomial

RSA, and PQ-RSA systems. It is suitable for many applications that rely on multiple data sources.

References

[1] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signature and public key cryptosystems, Communications of the ACM, **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] M. Coglianese, B. Goi, MaTRU: A new NTRU based cryptosystem, 6th International Conference on Cryptology in India, (2005), 232–243.

[4] H. R. Yassein, N. M. Al-Saidi, HXDTRU cryptosystem based on hexadecnion algebra, Proceedings of the 5th International Cryptology and Information Security Conference, (2016), 1–14.

[5] H. R. Yassein, N. M. Al-Saidi, BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra, International Journal of Advanced Computer Science and Applications, **7,** no. 11, (2016).

[6] N. M. Al-Saidi, H. R. Yassein, A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure, Malaysian Journal of Mathematical Sciences, **11,** (2017), 29–43.

[7] H. R. Yassein, N. M. Al-Saidi, A comparative performance analysis of NTRU and its variant cryptosystems, Proceeding of International Conference on Current Research in Computer Science and Information Technology, (2017), 115–120.

[8] H. R. Yassein, N. M. 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, (2018), 1–11.

[9] H. R. Yassein, N. M. Al-Saidi, An Innovative Bi-Cartesian Algebra for Designing of Highly Performed NTRU Like Cryptosystem, Malaysian Journal of Mathematical Sciences, **13,** (2019), 77–91.

[10] H. R. Yassein, N. M. G. Al-Saidi, A. K. Farhan, A new NTRU cryptosystem outperforms three highly secured NTRUanalog systems through an innovational algebraic structure, Journal of Discrete Mathematical Sciences and Cryptography, **23,** (2020), 1–20.

[11] H. R. Yassein, N. M. Al-Saidi, A. K. Jabber, A multidimensional algebra for designing an improved NTRU cryptosystem Eurasian, Journal of Mathematical and Computer Applications, **8,** (2020), 97–107.

[12] H. R. Yassein, A. A. Abidalzahra, N. M. Al-Saidi, A new design of NTRU encryption with security and performance level, AIP Conference Proceedings, 2334, no. 1, (2021), 080005.

[13] S. H. Shihadi, H. R. Yassein, A New Design of NTRU Encrypt-analogue Cryptosystem with High Security and Performance Level via Tripternion Algebra, Int. J. Math. Comput. Sci., **16,** (2021), 1515–1522.

[14] S. H. Shahhadi, H. R. Yassein, NTRsh: A New Secure Variant of NTRU Encrypt Based on Tripternion Algebra, Journal of physics conference series, 1999, no. 1, (2021), 2–6.

[15] H. H. Abo-Alsood, H. R. Yassein, QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra, Journal of Physics: Conference Series, 1999, no. 1, (2021), 1–7.

[16] H. H. Abo-Alsood, H. R. Yassein, Design of an Alternative NTRU Encryption with High Secure and Efficient, Int. J. Math. Comput. Sci., **16,** no. 4, (2021), 1469–1477.

[17] M. H. Al-Awadi, Designing an Efficient and Secure Cryptosystem Similar to MaTRU and RSA, M.Sc. Thesis, University of Al-Qadisiyah, Iraq, (2022).

[18] H. R. Yassein, H. N. Zaky, H. H. Abo-Alsood, I. A. Mageed, W. I. El-Sobky, QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra, Applied Mathematics & Information Sciences, **17,** no. 1, (2023), 1–5.