International Journal of Mathematics and Computer Science
Volume **20,** Issue no. 1, (2025), 459–464
DOI: https://doi.org/10.69793/ijmcs/01.2025/hamza

Development of Modified RSA Cryptosystem via Octonion Algebra

Mohammed Hassan Hamza[1], **Sahab Mohsen Abboud**[2], **Hassan Rashed Yassein**[3]

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

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

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

email: edu-math.post16@qu.edu.iq, bsc.sahab.jwer@uobabylon.edu.iq, hassan.yaseen@qu.edu.iq

(Received December 2, 2024, Accepted January 2, 2025, Published January 4, 2025)

Abstract

Researchers and those interested in data encryption are constantly working to provide new methods that increase security against attacks that seek to access the original data or by developing methods that currently work well. In this paper, we present a new method by using octonion algebra to develop the mathematical structure of the modified RSA, which increases its security and all its phases in the face of various attacks.

Keywords and phrases: RSA, Polynomial RSA, Modified RSA, Octonion Algebra.
AMS (MOS) Subject Classifications: 94A60, 68P25.
ISSN 1814-0432, 2025, https://future-in-tech.net

1 Introduction

The RSA cryptosystem was introduced in 1977 depending on the parameters derived from the prime. In 1978, Rivest et al. [1] proposed a public-key cryptosystem RSA that was dependent on the factoring problem. It was a relatively slow algorithm. In 1996, Hoffstein et al. [2] introduced NTRU that was dependent on a ring of truncated polynomials . Later, many researchers presented many studies on the development of RSA including, in 2012, Lvy et al. who used a modified algorithm of the RSA cipher system [3]. In 2015, Gafitoiu proposed a polynomial RSA by using polynomials instead of integers [4]. Also, many researchers have made improvements to NTRU. Some of those improvements were achieved by Malakian et al. who, in 2010, presented an alternative to NTRU, called OTRU, by replacing the original ring of NTRU with Octonion algebra [5]. In 2021, Abo-Alsood and Yassein presented QOTRU which was dependent on Qu-Octonion subalgebra [6]. In 2023, Atea and Yassein proposed PMRSA which was based on a polynomial ring [7]. In 2024, Abboud et al. [8] proposed OTRCQ based on Octonion algebra and Quaternion algebra.

2 Proposed OT-MRSA Cryptosystem

2.1 Key generation

To generate the public key, choose four octonion polynomials $\mathcal{F}\left(x\right) \in L_{\mathcal{F}}, \mathcal{B}\left(x\right) \in L_{\mathcal{B}}, \varkappa\left(x\right) \in L_{\varkappa}$ and $\}(x) \in L_{\}}$, such that $N_1\left(x\right) = \mathcal{F}\left(x\right)\mathcal{B}\left(x\right), N_2\left(x\right) = \varkappa\left(x\right)\}\left(x\right)$, and $N\left(x\right) = \mathcal{F}\left(x\right)\mathcal{B}\left(x\right)\ V\left(x\right)\}\left(x\right)$. Select $R = \mathbb{O} < N(x) >$ and $S = (p^m - 1)(p^n - 1)(p^r - 1)(p^t - 1)$ number of invariable elements in R modulo $N(x)$. Select $e_1, e_2 \in Z_s, 0 \leq e_1, e_2 < S$ and $gcd\ (e_1, e_2, S) = 1$. Find $d, g \in Z_s$ such that $de_1 = 1\ mod\ S$ and $ge_2 = 1\ mod\ S$, where $d = {e_1}^{-1} mod\ S$ and $g = {e_2}^{-1}\ mod\ S)$ are multiplication inverses.

2.2 Encryption phase

For any massage $M\left(x\right) = \ m_0 + \sum_{i=1}^{7}\ m_i e_i$, there is an encrypted public key e_1, e_2 given by the following formula:
$C\left(x\right) = \left[\left(m_0 + \sum_{i=1}^{7} m_i e_i\right)^{e_1}\ mod\ N(x)\right]^{e_2}\ mod\ N(x)$.

2.3 Decryption

To retrieve the original message $M(x)$, the recipient at this phase uses the following formula:

$$\begin{aligned}
M\left(x\right) &\equiv \left(C\left(x\right)\right)^{dg}\ \ mod\ N(x) \\
&\equiv \left(\left[\ m_0 + \sum_{i=1}^{7}\ m_i e_i\right]^{e_1 e_2}\right)^{dg}\ \ mod\ N(x) \\
&\equiv \left(\left[\ m_0 + \sum_{i=1}^{7} m_i e_i\right]^{(Sk_1+1)e_2}\right)^{g}\ \ mod\ N(x) \\
&\equiv \left(\left(\left[m_0 + \sum_{i=1}^{7}\ m_i e_i\right]^{(Sk_1 e_2)}\right)(m_0 + \sum_{i=1}^{7} m_i e_i)^{e_2}\right)^{g} mod\ N(x) \\
&\equiv \left[m_0 + \sum_{i=1}^{7}\ m_i e_i\right]^{e_2 g}\ \ mod\ N(x) \\
&\equiv \left(\left[m_0 + \sum_{i=1}^{7} m_i e_i\right]^{(Sk_2+1)}\right)\ mod\ N(x) \\
&\equiv (\left(\ m_0 + \sum_{i=1}^{7} m_i e_i\right)^{Sk_2}\ (m_0 + \sum_{i=1}^{7} m_i e_i))\ mod\ N(x) \\
&\equiv (\ m_0 + \sum_{i=1}^{7}\ m_i e_i) mod\ N\left(x\right).
\end{aligned}$$

Now, write the decryption formula modulo $\mathcal{F}(x), \mathcal{B}(x), \varkappa(x)$ and $\}(x)$ respectively

$$
\begin{aligned}
(C\,(x))^{dg} &\equiv \left(\left[m_0+\sum_{i=1}^{7}m_ie_i\right]^{\left(\left((p^m-1)(p^n-1)(p^r-1)\left(p^t-1\right)\right)k_1+1\right)e_2}\right)^{g} \ mod\ \mathcal{F}(x)\\
&\equiv (1)^{\left(((p^m-1)(p^n-1)(p^r-1)(p^t-1))k_1e_2g\right)}\left[\ m_0+\sum_{i=1}^{7}m_ie_i\right]^{e_2g} \ mod\ \mathcal{F}(x)\\
&\equiv \left[\ m_0+\sum_{i=1}^{7}\ m_ie_i\right]^{e_2g} \ mod\ \mathcal{F}(x) \equiv \left[\ m_0+\sum_{i=1}^{7}\ m_ie_i\right]^{Sk_2+1} \ mod\ \mathcal{F}(x)\\
&\equiv \left([M\,(x)]^{(p^m-1)(p^n-1)(p^r-1)\left(p^t1\right)k_2}\ \left(m_0+\sum_{i=1}^{7}\ m_ie_i\right)\right)\ mod\ \mathcal{F}(x)\\
&\equiv [1]^{(p^n-1)(p^r-1)(p^t-1)k_2}\ \left(m_0+\sum_{i=1}^{7}\ m_ie_i\right) mod\ \mathcal{F}(x)\\
&\equiv (\ m_0+\sum_{i=1}^{7}\ m_ie_i)\ mod\ \mathcal{F}(x) \equiv M\,(x)\ \ mod\ \mathcal{F}(x).
\end{aligned}
$$

In the same way,

$$
\begin{aligned}
(C\,(x))^{dg} &\equiv \left(\left[m_0+\sum_{i=1}^{7}\ m_ie_i\right]^{\left(\left((p^m-1)(p^n-1)(p^r-1)\left(p^t-1\right)\right)k_1+1\right)e_2}\right)^{g} \ mod\ \mathcal{B}(x)\\
&\equiv (\ m_0+\sum_{i=1}^{7}\ m_ie_i)\ mod\ \mathcal{B}(x) \equiv M\,(x)\ \ mod\ \mathcal{B}(x)
\end{aligned}
$$

Also, $(C\,(x))^{dg} \equiv M\,(x)\ \ mod\ \varkappa(x), (C\,(x))^{dg} \equiv M\,(x)\ \ mod\ \}\,(x)\,.$

3 Security Analysis for OT-MRSA

The public parameters and $N(x) = \{n_0(x) + n_1(x)e_1 + \ldots n_7(x)e_7 \in \mathbb{O}\}$, are used by the attacker in a brute force attack. Since the presence four polynomials involved, need for the hacker to search three sets of the four sets $\mathcal{F}(x), \mathcal{B}(x), \varkappa(x)$ and $\}(x)$. The space security of each of $\mathcal{F}(x), \mathcal{B}(x), \varkappa(x)$ and $\}(x)$ is calculated as follows:

$$\left(\frac{m!}{(d_{\mathcal{F}}!)^2(m-2d_{\mathcal{F}})!}\right)^8 \left(\frac{n!}{(d_{\mathcal{B}}!)^2(n-2d_{\mathcal{B}})!}\right)^8 \left(\frac{r!}{(d_{\}}!)^2(r-2d_{\}})!}\right)^8.$$

4 Conclusions

In this study, we presented a new encryption method called OT-MRSA dependence on octonion algebra which is superior to polynomial RSA and modified RSA. This method provided efficiency, reliability, and increased security, with the addition to the advantage of encrypting eight messages at the same time which made it useful for many applications that require the use of different sources of messages.

References

[1] R. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, **21,** no. 4, (1978), 120–126.

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

[3] B. Persis Urbana lvy, P. Mandiwa, M. Kumar, A modified RSA cryptosystem based on ”n” prime numbers, International Journal of Engineering and Computer Science, **1,** (2012), 63–66.

[4] I.B. Gafitoiu, Polynomial based RSA, B. Sc. thesis, 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, (2010), 83–90.

[6] 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.

[7] 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.

[8] S.M. Abboud, H.R. Yassein, R.K. Alhamido, Improvement Multi-Dimensional Public key OTRU Cryptosystem, International Journal of Mathematics and Computer Science, **19,** no. 4, (2024), 1071–1076.