International Journal of Mathematics and
Computer Science, **19**(2024), no. 4, 1071–1076

Improvement of a Multi-Dimensional Public-Key OTRU Cryptosystem

Sahab Mohsen Abboud[1], **Hassan Rashed Yassein**[2], **Riad Khidr Alhamido**[3]

[1]Department of Mathematics
College of Basic Education
University of Babylon
Babylon, Iraq

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

[3]Department of Mathematics
College of Science
University of Alfurat
Deir-ez-Zor, Syria

email: bsc.sahab.jwer@uobabylon.edu.iq, hassan.yaseen@qu.edu.iq,
Riad-hamido1983@alfuratuniv.edu.sy

(Received March 1, 2024, Accepted April 1, 2024,
Published June 1, 2024)

Abstract

OTRU is a multi-dimensional public-key cryptosystem which depends on octonions algebra. In this paper, we present a new multi-dimensional public-key cryptosystem, an improvement to the OTRU called OTRCQ, based on octonions algebra, commutative quaternion algebra and a new mathematical structure, with more security.

Key words and phrases: OTRU, Octonions algebra, Commutative quaternion algebra.
AMS (MOS) Subject Classifications: 94A60, 68P25.
ISSN 1814-0432, 2024, http://ijmcs.future-in-tech.net

1 Introduction

The OTRU public key cryptosystem was introduced in 2010 based on non–commutative octonions algebra with ligh level of security [1]. In 2021, Abo-Alsood and Yassein proposed QOTRU and BOTRU which depend on qu-octonion subalgebra and bi-octonion subalgebra of octonions algebra respectively [2, 3]. Also, Shahhadi and Yaasein proposed two public key cryptosystems called NTRS and NTR_{sh} which depend on tripternion algebra [4, 5]. In 2022, Yaasein et al. presented TOTRU, NTR_{TRN}, and AH_{QTR} public key based on octonions algebra, tripternion algebra, and quaternion algebra respectively [6, 7, 8]. In 2023, Yassein and et al. introduced $Q_{ui}TRU$ and HUDTRU that use quintuple algebra and HH- real algebra [9, 10]. In 2024, Abidalzahra and Yassein presented ASTRU depending on AS algebra.

2 Algebraic Structure of the OTRCQ Cryptosystem

The OTRCQ cryptosystem is based on octonions algebra with coefficients of commutative quaternion.

The set of commutative quaternions algebra is a four-dimensional vector space defined as: $CQ = \{q = t_0 + t_1 i + t_2 j + t_3 k : t_0, t_1, t_2, t_3 \in R\}$ such that $\{1, i, j, k\}$ from the basis of commutative quaternion, where R is the set of real numbers and i, j, k satisfy the following multiplication rules: $i^2 = k^2 = -1, j^2 = 1, ij = ji = k$ [11].

Let F be a field with $Char(F) \neq 2$. Then the octonions algebra over F is as follows:

$\mathbb{O}_F = \left\{r_0 + \sum_{n=1}^{7} r_n e_n\right\}$, where $r_0, r_1, \ldots r_7 \in F$, and $\{1, e_1, e_2, \ \ldots, \ e_7\}$ form the basis of this algebra. (i.e., algebra of eight dimensions) [1].

Suppose that $A = Z[x]/\left(x^N - 1\right), A_p = Z_p[x]/\left(x^N - 1\right)$ and $A_q = Z_q[x]/\left(x^N - 1\right)$ are truncated polynomial rings. Let Ω, Ω_p and Ω_q be three octonions algebras defined as follows:

$$\Omega = \Big\{ \big(f_{(0,0)} + f_{(0,1)}i + f_{(0,2)}j + f_{(0,3)}k\big) + \big(f_{(1,0)} + f_{(1,1)}i + f_{(1,2)}j + f_{(1,3)}k\big)\, e_1 + \ldots + \big(f_{(7,0)} + f_{(7,1)}i + f_{(7,2)}j + f_{(7,3)}k\big)\, e_7 \ \setminus\ f_{(0,0)}, f_{(0,1)}, \ldots, f_{(7,3)} \in A \Big\}.$$

$$\Omega_p = \Big\{ \big(f_{(0,0)} + f_{(0,1)}i + f_{(0,2)}j + f_{(0,3)}k\big) + \big(f_{(1,0)} + f_{(1,1)}i + f_{(1,2)}j + f_{(1,3)}k\big)\, e_1 + \ldots + \big(f_{(7,0)} + f_{(7,1)}i + f_{(7,2)}j + f_{(7,3)k}\big)\, e_7 \ \setminus\ f_{(0,0)}, f_{(0,1)}, \ldots, f_{(7,3)} \in A_p \Big\}.$$

$$\Omega_q = \Big\{ \big(f_{(0,0)} + f_{(0,1)}i + f_{(0,2)}j + f_{(0,3)}k\big) + \big(f_{(1,0)} + f_{(1,1)}i + f_{(1,2)}j + f_{(1,3)}k\big)\, e_1 + \ldots + \big(f_{(7,0)} + f_{(7,1)}i + f_{(7,2)}j + f_{(7,3)}k\big)\, e_7 \ \setminus\ f_{(0,0)}, f_{(0,1)}, \ldots, f_{(7,3)} \in A_q \Big\}.$$

3 The Proposed Scheme OTRCQ Cryptosystem

The OTRCQ public key cryptosystem depends on parameters N, p and q as defined in OTRU and the subsets L_f, L_g, L_s, L_r and $L_m \subset \Omega$ are defined as follow:

$$L_f = \Big\{ \big(f_{(0,0)} + f_{(0,1)}i + f_{(0,2)}j + f_{(0,3)}k\big) + \big(f_{(1,0)} + f_{(1,1)}i + f_{(1,2)}j + f_{(1,3)}k\big)\, e_1 + \ldots + \big(f_{(7,0)} + f_{(7,1)}i + f_{(7,2)}j + f_{(7,3)}\big)\, e_7 \ \in \Omega \setminus f_i \in A \text{ has } d_f \text{ coefficients equal to } +1,\ (d_f - 1) \text{ coefficients equal to -1, and the rest are } 0 \Big\}.$$

$$L_g = \Big\{ \big(g_{(0,0)} + g_{(0,1)}i + g_{(0,2)}j + g_{(0,3)}k\big) + \big(g_{(1,0)} + g_{(1,1)}i + g_{(1,2)}j + g_{(1,3)}k\big)\, e_1 + \ldots + \big(g_{(7,0)} + g_{(7,1)}i + g_{(7,2)}j + g_{(7,3)}\big)\, e_7 \ \in \Omega \setminus g_i \in A \text{ has } d_g \text{ coefficients equal to } +1,\ d_g \text{ coefficients equal to -1, and the rest are } 0 \Big\}.$$

$$L_s = \Big\{ \big(s_{(0,0)} + s_{(0,1)}i + s_{(0,2)}j + s_{(0,3)}k\big) + \big(s_{(1,0)} + s_{(1,1)}i + s_{(1,2)}j + s_{(1,3)}k\big)\, e_1 + \ldots + \big(s_{(7,0)} + s_{(7,1)}i + s_{(7,2)}j + s_{(7,3)}\big)\, e_7 \in \Omega \setminus s_i \in A \text{ has } d_s \text{ coefficients equal to } +1,\ d_s \text{ coefficients equal to -1, and the rest are } 0 \Big\}.$$

$$L_r = \Big\{ \big(r_{(0,0)} + r_{(0,1)}i + r_{(0,2)}j + r_{(0,3)}k\big) + \big(r_{(1,0)} + r_{(1,1)}i + r_{(1,2)}j + r_{(1,3)}k\big)\, e_1 + \ldots + \big(r_{(7,0)} + r_{(7,1)}i + r_{(7,2)}j + r_{(7,3)}\big)\, e_7 \in \Omega \setminus r_i \in A \text{ has } d_r \text{ coefficients equal to 1, } d_r \text{ coefficients equal to -1, and the rest are } 0 \Big\}.$$

$$L_m = \Big\{ \big(m_{(0,0)} + m_{(0,1)}i + m_{(0,2)}j + m_{(0,3)}k\big) + \big(m_{(1,0)} + m_{(1,1)}i + m_{(1,2)}j + m_{(1,3)}k\big)\, e_1 + \ldots + \big(m_{(7,0)} + m_{(7,1)}i + m_{(7,2)}j + m_{(7,3)}\big)\, e_7 \in \Omega \setminus m_i \in A, \text{ coefficients of } m_{(\alpha,\beta)} \text{ are chosen between -p/2 and p/2} \Big\}.$$

The OTRCQ can be described by three phases:

i. Key Generation phase
To generate the public key, first choose randomly three octonions F, G and S, such that $F \in L_f, G \in L_g$ and $S \in L_s$, and F must have multiplicative inverse modulo p and q. The public key H is calculated as follows: $H = F_q * G * S \pmod q$.

ii. Encryption phase
To encrypt a message $M \in L_m$, select a random octonions $R \in L_r$, and the ciphertext E is computed by $E = pH * R + M \pmod q$.

iii. Decryption phase
In order to recover the original text, the recipient performs the following steps on the encrypted text:

$$\begin{aligned} V = F * E * F \,(\text{mod } q) &= F * (pH * R + M) * F (\text{mod } q) \\ &= (pF * (F_q * G * S * R) * F + F * M * F \pmod q \\ &= pG * S * R * F + F * M * F (\text{mod } q), \end{aligned}$$

such that the coefficients of the last term belong to $(-q/2, q/2]$. Take $U = V \pmod p = F * M * F \pmod p$,

$F_p * U * F_p = F_p * (F * M * F) * F_p \pmod p = M \pmod p$, such that the coefficients belong to $(-p/2, p/2]$.

4 Discussion

The characteristics of the proposed cryptosystem are discussed in terms of key security based on the site of the space of L_g and L_s (assuming that the subset L_f is larger) which are calculated as follows:

$$|L_g| = \binom{N}{d_g}^{32} \binom{N - d_g}{d_g}^{32}, |L_s| = \binom{N}{d_s}^{32} \binom{N - d_s}{d_s}^{32}.$$

As for security of the message, it depends on the site of the space of the subset L_r, which is equal to $|L_r| = \binom{N}{d_r}^{32}\binom{N-d_r}{d_r}^{32}$. As for the time taken for the OTRCQ it is done by calculating the time required for each of the three phases based on the convolution multiplication and addition operations, which is equal to $58368\, t{+}64t_1$, where t represents the convolution polynomial multiplication and t_1 represents the addition time.

5 Conclusion

The proposed multi-dimensional encryption based on a combination of octonions algebra and commutative quaternion algebra by adopting commutative quaternion algebra as coefficients for octonions algebra, which given higher security compared to OTRU, but slower with the possibility of reducing that slowness by reducing the degree of the polynomials. OTRCQ can be applied to multiple source data, where 32 message can be encrypt at the same time.

References

[1] E. Malecian, A. Zakerolhsooeini, OTRU: A non- associative and high speed public key cryptosystem, in 15th CSI International Symposium on Computer Architecture and Digital Systems, (2010), 83–90.

[2] H. H. Aboo-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), 2–7.

[3] H. H. Aboo-Alsood, H. R. Yassein, Design of an Alternative NTRU Encryption with High Secure and Efficient, International Journal of Mathematics and Computer Science, **16,** no. 4, (2021), 1469–1477.

[4] S. H. shahhadi, H. R. Yassein, NTRsh: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra, Journal of Physics conference series, **1999,** no. 1, (2021), 2–6.

[5] S. H. shahhadi, H. R. Yassein, A New Design of NTRUEncrypt – analog Cryptosystem with High Security and Performance level via Tripternion Algebra, International Journal of Mathematics and Computer Science, **16,** no. 4,(2021), 1515–1522.

[6] H. H. Abo-Alsood, H. R. Yassein, Analogue to NTRU public key cryptosystem by multi-dimension algebra with high security, AIP Conference Proceedings, **2386**, no. 1, (2022), 600091-600096.

[7] S. H. shahhadi, H. R. Yassein, An innovative Tripternion Algebra for Designing NTRU-like cryptosystem with High Security, AIP Conference Proceedings, **2386,** no. 1, (2022), 60009-1-60009-6.

[8] H. R. Yassein, A. H. Reshan, N. M. G. Al-Saidi, AHQTR: A New NTRU Variant based on Quaternion algebra, in Proceeding of 8th International Cryptology and Information Security Conference, (2022), 100–108.

[9] H. R. Yassein, H. N. Zaky, H. H. Abo-Alsoo, I. A. Mageed, W. I. El-Sobky, QuiTRU: Design Secure variant of NTRUencrypt via a New Multi-Dimensional Algebra, Applied Mathematics and Information Sciences, **17,** no. 1, (2023), 1–5.

[10] H. R. Yassein, H. A. Ali, HUDTRU: An Enhanced NTRU for Data Security via Quintuple algebra, International Journal of Mathematics and Computer Science, **18,** no. 2, (2023), 199–204.

[11] F. Catoni, R. Cannata, P. Zampetti, An Introduction to Commutative Quaternions, Advances in Applied Clifford Algebras, **16,** (2006), 1–28.