Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43)** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.77672

A Novel Development of OTRU Cryptosystem

Kawthar A. Hassoon and Hassan R. Yassein*

ABSTRACT: In the light of the tremendous development in data exchanging, maintaining its confidentiality has become extremely vital when transferring it in an insecure medium, so there is a constant need to develop encryption systems. One of these encryption systems is NTRU, which was developed by OTRU encryption. In this paper, we presented a development of OTRU, which is called KSQOT, by using KAH-octo algebra with partial coefficients of quaternion algebra instead of octonion algebra (a mix between octonion algebra and quaternion algebra) with eight dimensions but with sixteen partial elements for each element and different mathematical constructions of the phases (key generation, encryption, and decryption) of the system which allude a very high level of security by augmenting the private keys with the public key and an acceptable speed by the number of mathematical operations used in constructing the method.

Key Words: KSQOT Cryptosystem, Brute Force Attack, Alternate Keys Attacks, OTRU, TOTRU, BOTRU, NTRS, $\mathrm{NTR_{SH}}$, $\mathrm{NTR_{TRN}}$.

Contents

1. Introduction

The growth of various encryption methods can improve the security of information transmission in insecure channels which is the objective. In 1998, the NTRU cryptosystem was presented by Hoffstein et al. such as the four sets of polynomials of degree $N-1$ with integer coefficients and three integer parameters $(N, p,$ and $q)$ are required for the NTRU cryptosystem [1]. In 2002, Gaborit et al. [2, 3], introduced a new cipher system analogous to NTRU called CTRU, which is based on the $\frac{F_2[x]}{x^N-1}$. In 2005, Coglianese and Goi [4] presented an improved cipher system for NTRU called MaTRU, which uses a more efficient linear transformation with a security level similar to that of NTRU. The use of the concept of algebra [5, 6] in many fields has encouraged researchers to adopt these algebraic structures in developing encryption methods. In 2009, a quaternion-based public key cryptosystem QTRU is constructed by Malekian et al. [7], the conclusion is that QTRU is more resistant to some attacks than NTRU. In 2010, Malekian and Zakerolhosseini presented the OTRU cryptosystem and pointed out that it was similar to the NTRU cryptosystem and required four subsets; but its coefficients belong to the octonions algebra [8]. In 2015, Alsaidi et al. introduced the CQTRU system through the use of commutative quaternion algebra [9]. In 2019, Lyubashevsky and Seiler [10] created NTTRU, which creates public keys and cipher text with an approximate size of 1.25 $.KB$ at the 128−, bit security level using the number theoretic transform over the cyclotomic ring $\frac{Z_{7681}[x]}{(x^{768}-x^{384}+1)}$. In 2021, Abo-Alsood and Yassein presented the BOTRU cryptosystem based on bi-octonion subalgebra [11]. The NTRS cryptosystem was presented by Shahhadi and Yassein [12], and the $\mathrm{NTR_{SH}}$ cryptosystem was also presented by Shahhadi and Yassein [13]. In 2022,

* Corresponding author

Submitted July 04, 2025. Published August 10, 2025
2010 *Mathematics Subject Classification:* 94A60, 11T71.

the TOTRU cryptosystem was presented by Abo-Alsood and Yassein and depends on octonions algebra with two public keys [14]. The $\mathrm{NTR}_{\mathrm{TRN}}$ cryptosystem was presented by Shahhadi and Yassein [15]. In 2023, Yassein at el. suggestion a new version of the NTRU called QuiTRU [16]. In the current study, we introduce the KSQOT cryptosystem based on KAH-Octo algebra [17] and show how it has a very high level of security and acceptable speed. In addition to this section, this paper is structured as follows: In second Section, introduce KSQOT, a novel public-key cryptosystem based on KAH-Octo algebra with coefficients belonging to quaternion algebra. The third section discusses the security of the new system through two types of attacks. The fourth section compares KSQOT and six new cryptosystems in terms of key and message security, and speed, and presents the results in tabular form. The fifth Section presents a summary of the paper results.

2. KSQOT Cryptosystem

In this section, a new public-key cryptosystem KSQOT is proposed that is based on the KAH-Octo algebra with coefficients belonging to quaternion algebra [18] such that i=j=0 (i.e., commutative and associative). Also, the public parameters N,p,q are positive integers such that p and q coprime and three KAH-Octo algebras are defined as follows:

$$KO = \left\{ (f_{0,0} + f_{0,1}k) + \sum_{\alpha=1}^{7} (f_{\alpha,0} + f_{\alpha,1})\,\beta_\alpha \;\middle|\; f_{\alpha,0}, f_{\alpha,1} \in A \right\}$$

$$KO_p = \left\{ (f_{0,0} + f_{0,1}k) + \sum_{\alpha=1}^{7} (f_{\alpha,0} + f_{\alpha,1})\,\beta_\alpha \;\middle|\; f_{\alpha,0}, f_{\alpha,1} \in A_p \right\}$$

$$KO_q = \left\{ (f_{0,0} + f_{0,1}k) + \sum_{\alpha=1}^{7} (f_{\alpha,0} + f_{\alpha,1})\,\beta_\alpha \;\middle|\; f_{\alpha,0}, f_{\alpha,1} \in A_q \right\}$$

Such that $A = \mathbb{Z}[x]/(x^N - 1), \quad A_p = \mathbb{Z}_p[x]/(x^N - 1), \quad A_q = \mathbb{Z}_q[x]/(x^N - 1)$
and six subsets $L_F, L_G, L_S, L_\phi, L_R$ and $L_M \in KO$

$$L_F = \left\{ (f_{0,0} + f_{0,1}k) + \sum_{\alpha=1}^{7} (f_{\alpha,0} + f_{\alpha,1})\,\beta_\alpha \;\middle|\; f_{\alpha,0}, f_{\alpha,1} \in A, L_{(d_f, d_{(f-1)})} \right\}$$

$$L_G = \left\{ (g_{0,0} + g_{0,1}k) + \sum_{\alpha=1}^{7} (g_{\alpha,0} + g_{\alpha,1})\,\beta_\alpha \;\middle|\; g_{\alpha,0}, g_{\alpha,1} \in A, L_{(d_g, d_g)} \right\}$$

$$L_S = \left\{ (s_{0,0} + s_{0,1}k) + \sum_{\alpha=1}^{7} (s_{\alpha,0} + s_{\alpha,1})\,\beta_\alpha \;\middle|\; s_{\alpha,0}, s_{\alpha,1} \in A, L_{(d_s, d_s)} \right\}$$

$$L_\phi = \left\{ (\phi_{0,0} + \phi_{0,1}k) + \sum_{\alpha=1}^{7} (\phi_{\alpha,0} + \phi_{\alpha,1})\,\beta_\alpha \;\middle|\; \phi_{\alpha,0}, \phi_{\alpha,1} \in A, L_{(d_\phi, d_\phi)} \right\}$$

$$L_R = \left\{ (r_{0,0} + r_{0,1}k) + \sum_{\alpha=1}^{7} (r_{\alpha,0} + r_{\alpha,1})\,\beta_\alpha \;\middle|\; r_{\alpha,0}, r_{\alpha,1} \in A, L_{(d_r, d_r)} \right\}$$

$$L_M = \left\{ (m_{0,0} + m_{0,1}k) + \sum_{\alpha=1}^{7} (m_{\alpha,0} + m_{\alpha,1})\,\beta_\alpha \;\middle|\; m_{\alpha,0}, m_{\alpha,1} \in A, \text{modulo pbetween } \frac{(-p)}{2} \text{ and } \frac{p}{2} \right\}$$

such that

$$L_{(d_x, d_y)} = \{ f \in K; f \text{ has } d_x \text{ coefficients equal } 1, d_y \text{ coefficients equal } -1, \text{ and the remaining equal } 0 \}$$

3. The KSQOT Cryptosystem's Phases:

I. **Key Generation** The recipient generates the public key H and sends it to the sender by selecting three elements $F \in L_F$, $G \in L_G$, and $S \in L_S$ and calculating it through the following formula $H = {F_q}^{-1} * G * S \mod q$, where F_q^{-1} represents the inverse of F modulo q. The key generation phase involves 128 convolution multiplications.

II. **Encryption** After receiving the public key H from the recipient by the sender, to send the original message M in an encrypted form E, the sender chooses $\phi \in L_\phi, R \in L_R$ and calculates E, as follows: $E = p(H * \phi + R) + M \mod q$. The encryption phase needs 32 convolution multiplications and 32 additions of polynomials.

III. **Decryption** After receiving the encrypted message from the sender and for the purpose of converting it to the original text M,
he/she takes the following steps:

$$\begin{aligned} D &= F * E \mod q \\ &= F * \Big(p\big(H * \phi + R\big) + M\Big) \mod q \\ &= F * \bigg(\Big(p\big(F_q^{-1} * G * S\big) * \phi + R\Big) + M\bigg) \mod q \\ &= p\bigg(\Big(\big(F * F_q^{-1}\big) * G * S\Big) * \phi + R\bigg) + F * M \mod q \\ &= p\Big(\big(G * S\big) * \phi + F * R\Big) + F * M \mod q \end{aligned}$$

Such that the coefficients of the last value belong to the interval $(-q/2, q/2]$. Now, convert $D \mod q$ to

$$D \mod p = p\bigg(\Big(\big(F * F_q^{-1}\big) * G * S\Big) * \phi + R\bigg) + F * M \mod p$$

,

since $p = 0 \mod p$ then

$$D \mod p = F * M \mod p$$

Therefore, $M = F_p^{-1} * D \mod p$ where F_p^{-1} represents the inverse of F modulo p and the coefficients in the interval $(-p/2, p/2]$. This phase needs 192 convolution multiplications and 32 polynomial additions.

4. Security Analysis

I. **Brute Force Attack** If we take into account that the general parameters are known to the attacker, then the original message can be accessed in two ways. First, to search for the private keys that generated the public key H, which are G and S (considering that the size of space of the subset L_F is greater than L_G and L_S). In a brute force attack, the size of the key space is equal to

$$\left(\binom{N}{d_g}\binom{N-d_g}{d_g}\binom{N}{d_s}\binom{N-d_s}{d_s}\right)^{16}$$

The second way is to search for the keys for the encryption phase, which are ϕ and R. Accordingly, the size of the message space is equal to

$$\left(\binom{N}{d_\phi}\binom{N-d_\phi}{d_\phi}\binom{N}{d_r}\binom{N-d_r}{d_r}\right)^{16}$$

Table 1: **The size of the key space and the message space of KSQOT**

N	d_g	d_s	d_ϕ	d_r	Key space	Message space
107	12	12	5	5	1.6622×10^{964}	2.0391×10^{510}
107	20	20	10	10	1.3907×10^{1304}	4.4720×10^{852}
149	12	12	10	10	1.7835×10^{1086}	2.9164×10^{952}
149	25	25	20	20	2.2092×10^{1735}	5.8735×10^{1524}
167	18	18	18	18	2.3318×10^{1492}	2.3318×10^{1492}
167	27	27	22	22	1.4070×10^{1912}	5.2133×10^{1695}
211	20	20	18	18	2.8236×10^{1743}	8.4680×10^{1621}
211	34	34	22	22	2.1020×10^{2426}	1.7629×10^{1858}
257	20	20	18	18	3.0161×10^{1863}	7.6330×10^{1728}
257	24	24	24	24	5.9939×10^{2113}	5.9939×10^{2113}

The size of the key space and the message space of KSQOT with optional numerical values are shown in Table 1.

All calculations in Table 1 were performed using MATLAB R2021a.

II. **Alternate Keys Attacks** The attacker can access the original text by finding alternative keys for the keys G and S (considering that the size of space of the subset L_F is greater than L_G and L_S), which requires him to find 32 alternative keys, as follows:

$$\hat{g}_{0,0}, \hat{g}_{0,1}, \hat{g}_{1,0}, \hat{g}_{1,1}, \hat{g}_{2,0}, \hat{g}_{2,1}, \hat{g}_{3,0}, \hat{g}_{3,1} \hat{g}_{4,0}, \hat{g}_{4,1}, \hat{g}_{5,0}, \hat{g}_{5,1}, \hat{g}_{6,0}, \hat{g}_{6,1}, \hat{g}_{7,0}, \hat{g}_{7,1}$$

and

$$\hat{s}_{0,0}, \hat{s}_{0,1}, \hat{s}_{1,0}, \hat{s}_{1,1}, \hat{s}_{2,0}, \hat{s}_{2,1}, \hat{s}_{3,0}, \hat{s}_{3,1} \hat{s}_{4,0}, \hat{s}_{4,1}, \hat{s}_{5,0}, \hat{s}_{5,1}, \hat{s}_{6,0}, \hat{s}_{6,1}, \hat{s}_{7,0}, \hat{s}_{7,1}$$

of the keys

$$g_{0,0}, g_{0,1}, g_{1,0}, g_{1,1}, g_{2,0}, g_{2,1}, g_{3,0}, g_{3,1}, g_{4,0}, g_{4,1}, g_{5,0}, g_{5,1}, g_{6,0}, g_{6,1}, g_{7,0}, g_{7,1}$$

and

$$s_{0,0}, s_{0,1}, s_{1,0}, s_{1,1}, s_{2,0}, s_{2,1}, s_{3,0}, s_{3,1}, s_{4,0}, s_{4,1}, s_{5,0}, s_{5,1}, s_{6,0}, s_{6,1}, s_{7,0}, s_{7,1}$$

.

Which requires more time. Therefore ,this method has a high level of security against this type of attack.

5. Comparison Between KSQOT and Some Improvements of NTRU

In this section, the key security, message security spaces, and algebraic structures used as a basis for construction for KSQOT and some previous cryptosystems OTRU, TOTRU, BOTRU, NTRS, NTR_{SH}, and NTR_{TRN} will be compared based on the same parameter values mentioned above, so that what the recipient will choose will be equal to $d_g = d_s$, and what the sender will choose will be equal to $d_\phi = d_r$, without focusing on the need for the inverse of the parameters in the decryption phase in TOTRU, BOTRU, NTRS, NTR_{SH}, and NTR_{TRN}. In addition, we make a comparison in terms of execution time for the three phases of each system. In addition, we made a comparison in terms of execution time for the three phases of each system depending on the number of operations, convolution multiplication, and addition polynomials for the polynomials. See (Table 2) which shows the size of the key security space

and the space of message security of KSQOT and the cryptosystems it compares with, (Table 3) which shows the algebraic structure each cryptosystem relies on, and (Table 4) which summarizes the execution time for each cryptosystem listed below in sequence.

Table 2: **The size of the key security space and the space of message security of KSQOT and some improvements**

Cryptosystem	Size of key space	Size of message space
OTRU	$\left(\binom{N}{d_g}\binom{N-d_g}{d_g}\right)^8$	$\left(\binom{N}{d_\phi}\binom{N-d_\phi}{d_\phi}\right)^8$
TOTRU	$\left(\binom{N}{d_g}\binom{N-d_g}{d_g}\binom{N}{d_s}(\binom{N-d_s}{d_s}\right)^8$	$\left(\binom{N}{d_\phi}\binom{N-d_\phi}{d_\phi}\binom{N}{d_r}\binom{N-d_r}{d_r}\right)^8$
BOTRU	$\left(\binom{N}{d_g}\binom{N-d_g}{d_g}\binom{N}{d_j}\binom{N-d_j}{d_j}\right)^2$	$\left(\binom{N}{d_\phi}\binom{N-d_\phi}{d_\phi}\binom{N}{d_r}\binom{N-d_r}{d_r}\right)^2$
NTRS	$\left(\binom{N}{d_g}\binom{N-d_g}{d_g}\binom{N}{d_v}\binom{N-d_v}{d_v}\binom{N}{d_u}\binom{N-d_u}{d_u}\right)^3$	$\left(\binom{N}{d_\phi}\binom{N-d_\phi}{d_\phi}\binom{N}{d_r}\binom{N-d_r}{d_r}\right)^3$
NTR_{SH}	$\left(\binom{N}{d_g}\binom{N-d_g}{d_g}\binom{N}{d_u}\binom{(N-d_u}{d_u}\binom{N}{d_s}(\binom{N-d_s}{d_s}\binom{N}{d_v}\binom{N-d_v}{d_v}\right)^3$	$\left(\binom{N}{d_c}\binom{N-d_c}{d_c}\binom{N}{d_r}\binom{N-d_r}{d_r}\right)^3$
NTR_{TRN}	$\left(\binom{N}{d_g}\binom{N-d_g}{d_g}\binom{N}{d_u}\binom{N-d_u}{d_u}\right)^3$	$\left(\binom{N}{d_r}\binom{N-d_r}{d_r}\right)^3$
KSQOT	$\left(\binom{N}{d_g}\binom{N-d_g}{d_g}\binom{N}{d_s}(\binom{N-d_s}{d_s}\right)^{16}$	$\left(\binom{N}{d_\phi}\binom{N-d_\phi}{d_\phi}\binom{N}{d_r}\binom{N-d_r}{d_r}\right)^{16}$

Table 3: **Algebraic structure of KSQOT and some improvements**

Cryptoststem	algebraic structures
OTRU	octonions
TOTRU	octonions
BOTRU	bi-octonions
NTRS	tripternion
NTR_{SH}	tripternion
NTR_{TRN}	tripternion
KSQOT	KAH-Octo

where t_0 is the time of convolution multiplication while t_1 is time of polynomial addition. Using MATLAB R2021a, we will mention a numerical comparison between KSQOT and some improvements of NTRU mentioned in this section, in Tables 5 and 6. Therefore, Table 5 contains a comparison of their size of key spaces.

Table 6 explains the comparison of the size of message spaces for them.

All calculations in Tables 5 and 6 based on the same parameter values in Table 1.

Table 4: **Execution time of KSQOT and some improvements**

	OTRU	**TOTRU**	**BOTRU**	**NTRS**	**NTR_{SH}**	**NTR_{TRN}**	**KSQOT**
Key generation	$64t_0$	$128t_0$	$8t_0$	$36t_0$	$54t_0$	$18t_0$	$128t_0$
Encryption	$64t_0 + 8t_1$	$128t_0 + 16t_1$	$8t_0 + 4t_1$	$18t_0 + 6t_1$	$18t_0 + 6t_1$	$18t_0 + 3t_1$	$32t_0 + 32t_1$
decryption	$1024t_0 + 8t_1$	$1536t_0 + 16t_1$	$24t_0 + 4t_1$	$45t_0 + 6t_1$	$198t_0 + 6t_1$	$54t_0 + 3t_1$	$192t_0 + 32t_1$
Total speed	$1152t_0 + 16t_1$	$1792t_0 + 32t_1$	$40t_0 + 8t_1$	$99t_0 + 12t_1$	$261t_0 + 12t_1$	$90t_0 + 6t_1$	$352t_0 + 64t_1$

Table 5: **Size of key spaces of KSQOT and some improvements**

OTRU	**TOTRU**	**BOTRU**	**NTRS**	**NTR_{SH}**	**NTR_{TRN}**	**KSQOT**
1.1355×10^{241}	1.2893×10^{482}	3.3696×10^{120}	1.5384×10^{271}	3.8261×10^{361}	6.1855×10^{180}	1.6622×10^{964}
1.0860×10^{326}	1.1793×10^{652}	1.0421×10^{163}	6.1700×10^{366}	1.1317×10^{489}	3.3640×10^{244}	1.3907×10^{1304}
3.6544×10^{271}	1.3355×10^{543}	6.0452×10^{135}	3.2223×10^{305}	2.2092×10^{407}	4.7002×10^{203}	1.7835×10^{1086}
6.8558×10^{433}	4.7002×10^{867}	8.2800×10^{216}	1.1630×10^{488}	5.6766×10^{650}	2.3826×10^{325}	2.2092×10^{1735}
1.2357×10^{373}	1.5270×10^{746}	3.5153×10^{186}	5.3508×10^{419}	4.3440×10^{559}	6.5909×10^{279}	2.3318×10^{1492}
1.0891×10^{478}	1.1862×10^{956}	1.0436×10^{239}	6.1903×10^{537}	1.1366×10^{717}	3.3714×10^{358}	1.4070×10^{1912}
7.2896×10^{435}	5.3138×10^{871}	8.5379×10^{217}	2.2158×10^{490}	6.2238×10^{653}	7.8891×10^{326}	2.8236×10^{1743}
3.8077×10^{606}	1.4498×10^{1213}	1.9513×10^{303}	2.5307×10^{682}	7.4300×10^{909}	8.6197×10^{454}	2.1020×10^{2426}
7.4107×10^{465}	5.4919×10^{931}	8.6086×10^{232}	1.2694×10^{524}	6.3796×10^{698}	2.5258×10^{349}	3.0161×10^{1863}
2.7825×10^{528}	7.7421×10^{1056}	1.6681×10^{264}	3.1621×10^{594}	4.6413×10^{792}	2.1544×10^{396}	5.9939×10^{2113}

6. Conclusions

KSQOT has a very high key and message security compared to OTRU, TOTRU, BOTRU, NTRS, NTR_{SH}, and NTR_{TRN}. In terms of time, KSQOT is faster than OTRU and TOTRU, but slower than BOTRU, NTRS, NTR_{SH}, and NTR_{TRN}, this slowness can be addressed by minimizing the degree of the polynomials while maintaining security. OTRU can be considered a special case of KSQOT when $f_{\alpha,1} = 0$ for all $\alpha = 0, 1, \ldots, 7$ and $S = 1, R = 0$. Since each element in KAH-Octo algebra consists of 16 elements, it makes it possible to send 16 different messages:

$$m_{0,0}, m_{0,1}, m_{1,0}, m_{1,1}, m_{2,0}, m_{2,1}, m_{3,0}, m_{3,1}, m_{4,0}, m_{4,1}, m_{5,0}, m_{5,1}, m_{6,0}, m_{6,1}, m_{7,0}, m_{7,1}$$

Simultaneously. These properties make it a suitable option for many types of electronic transactions.

References

1. J. Hoffstein, J. Pipher, J. H. Silverman, D. Lieman, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in International algorithmic number theory symposium, Springer, 1998, pp. 267–288.

2. P. Gaborit, J. Ohler and P. Soli, "CTRU, a polynomial Analogue of NTRU," INRIA. Rapport de recherche, no. 4621, 2002.

3. M. Coglianese and B. Goi, "MaTRU: A new NTRU based cryptosystem", Springer Verlag Berlin Heidelberg, vol. 3797 p.p. 232-243, 2005.

4. E. Malecian, A. Zakerolhsooeini and A. Mashatan, "QTRU: Quaternionic Version of the NTRU Public-Key Cryptosystems," The ISC Int'l Journal of Information Security, vol. 3, no. 1, pp. 29-42, 2011.

Table 6: **Size of message spaces of KSQOT and some improvements**

OTRU	**TOTRU**	**BOTRU**	**NTRS**	**NTR$_{SH}$**	**NTR$_{TRN}$**	**KSQOT**
3.7788×10^{127}	1.4280×10^{255}	6.1472×10^{63}	4.8197×10^{95}	4.8197×10^{95}	6.9424×10^{47}	2.0391×10^{510}
1.4542×10^{213}	2.1147×10^{426}	3.8134×10^{106}	7.4468×10^{159}	7.4468×10^{159}	8.6295×10^{79}	4.4720×10^{852}
1.3068×10^{238}	1.7077×10^{476}	1.1432×10^{119}	3.8651×10^{178}	3.8651×10^{178}	1.9660×10^{89}	2.9164×10^{952}
1.5568×10^{381}	2.4235×10^{762}	3.9456×10^{190}	7.8373×10^{285}	7.8373×10^{285}	8.8529×10^{142}	5.8735×10^{1524}
1.2357×10^{373}	1.5270×10^{746}	3.5153×10^{186}	6.5909×10^{279}	6.5909×10^{279}	8.1184×10^{139}	2.3318×10^{1492}
8.4972×10^{423}	7.2203×10^{847}	9.2180×10^{211}	8.8503×10^{317}	8.8503×10^{317}	9.4076×10^{158}	5.2133×10^{1695}
3.0335×10^{405}	9.2021×10^{810}	5.5077×10^{202}	1.2926×10^{304}	1.2926×10^{304}	1.1369×10^{152}	8.4680×10^{1621}
3.6438×10^{464}	1.3278×10^{929}	1.9089×10^{232}	2.6374×10^{348}	2.6374×10^{348}	1.6240×10^{174}	1.7629×10^{1858}
1.6622×10^{432}	2.7628×10^{864}	1.2893×10^{216}	1.4639×10^{324}	1.4639×10^{324}	1.2099×10^{162}	7.6330×10^{1728}
2.7825×10^{528}	7.7421×10^{1056}	1.6681×10^{264}	2.1544×10^{396}	2.1544×10^{396}	1.4678×10^{198}	5.9939×10^{2113}

5. B. Y. Hussein, Equivalent Locally Martingale Measure for the DeflatorProcess on Ordered Banach Algebra, Journal of Mathematics, Vol. 2020, pp. 1-7, 2020.
6. H. A. Wshayeh and B.Y. Hussein, On δ-characterization in symmetric Δ-Banach algebra with Hermitian properties, AIP Conference Proceedings, Vol. 2386. pp. 1-8, 2022
7. D. Eberly, "Quaternion algebra and calculus," Magic Softw. Inc, vol. 26, pp. 1–8, 2002.
8. E. Malekian and A. Zakerolhosseini, "OTRU: A non-associative and high speed public key cryptosystem," in 2010 15th CSI International Symposium on Computer Architecture and Digital Systems, IEEE, 2010, pp. 83–90.
9. N. Alsaidi, M. Saed, A. Sadiq, and A. A. Majeed "An improved NTRU Cryptosystem via Commutative Quaternions Algebra," Int'l Conf. Security and Management (SAM'15), 2015, pp. 198–203.
10. V. Lyubashevsky, G. Seiler, "NTTRU: Truly Fast NTRU Using NTT," IACR Transactions on Cryptographic Hardware and Embedded Systems, no. 3, pp. 180-201, 2019.
11. H. H. Abo-Alsood and H. R. Yassein, "Design of an alternative NTRU Encryption with High Secure and Efficient," Int. J. Math. Comput. Sci., vol. 16, no. 4, pp. 1469–1477, 2021.
12. S. H. Shahhadi and H. R. Yassein, "NTRsh: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra," Journal of Physics: Conference Series, 2021, pp. 1–6.
13. S. H. Shahhadi and H. R. Yassein, "A New Design of NTRU Encrypt-analog Cryptosystem with High Security and Performance Level via Tripternion Algebra," Int. J. Math. Comput. Sci., vol. 16, no. 4, pp. 1515–1522, 2021.
14. H. H. Abo-Alsood and H. R. Yassein, "Analogue to NTRU public key cryptosystem by multi-dimensional algebra with high security," AIP Conference Proceedings, AIP Publishing LLC, 2022, pp. 1–6.
15. S. H. Shahhadi and H. R. Yassein, "An innovative tripternion algebra for designing NTRU-like cryptosystem with high security," AIP Conference Proceedings, AIP Publishing, 2022, pp. 1–6.
16. Hassan Rashed Yassein, Hany Nasry Zaky, Hadeel Hadi Abo-Alsoo, Ismail A Mageed, Wageda I El-Sobky, QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra, Applied Mathematics and Information Sciences, Vol. 17, no. 1, pp. 49-53, 2023
17. K. A. Hassoon and H. R. Yassein, "Proposed Multi-Dimensional Algebra," Int. J. Math. Comput. Sci., vol. 19, no. 3, pp. 765–770, 2024.

Kawthar A. Hassoon,
Department of Mathematics,
Faculty of Education for Women, University of Kufa,
Iraq.
E-mail address: kawthara.alshammari@student.uokufa.edu.iq

and

Hassan R. Yassein,
Department of Mathematics,
College of Education, University of Al-Qadisiyah,
Iraq.
E-mail address: hassan.yaseen@qu.edu.iq