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

(3s.) **v. 2026 (44)** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.77263

Novel Encryption System via AT and Quaternion Algebras

Amna Abdul Karim Sahib and Hassan Rashed Yassein*

ABSTRACT: Due to the increasing and sophisticated attacks on data transmitted in encrypted transmission media, it has become necessary to find new encryption methods that are more secure than existing methods to maintain and protect data confidentiality. In this paper, we present a new encryption system, QTRAT, which is a comprehensive development of QTRU using AT algebra. It is compared with NTRU, QTRU, HXDTRU, and ATTRU in terms of message and key security, and execution time.

Key Words: Quaternion algebra, key security, message security, execution time.

Contents

1. Introduction

With the increasing advent of the Internet and its use to transmit and store data and the increase in cyber-attacks, the need for new encryption methods has emerged that are difficult to break easily, as many cryptosystems have been developed.

In 1997, Hoffstein et al. presented NTRU cryptosystem, a public key cryptosystem that is one of the most widely used cryptosystems. It was designed to provide strong security against computational attacks. Choosing the appropriate parameters is crucial to achieving a balance between performance and security in NTRU [6]. In 2010, Malekian and Zakerolhosseini [7] presented a high-security OTRU cryptosystem, which is based on non-associative and non-commutative octonions algebra.

In 2011, Malekian et al. [8] presented QTRU cryptosystem, which is based on non-commutative quaternion algebra and is more resistant to attacks than NTRU. In 2014, UbaidurRahman [18] presented a technology based on biological simulation for encoding and decoding DNA and possesses performing power for algorithms high. In 2016, Yassein and Al-Saidi [11] presented HXDTRU cryptosystem, which is based on non-commutative, non-associative and alternative hexadecnion algebra. In 2022, Ali and Yassein [13] presented QTNTR cryptosystem, which is based on commutative and associative quintuple algebra. In 2023, Yassein et al. [4] presented QuiTRU cryptosystem, which is based on HH-Real algebra. In same year, Yassein and Abo-Alsoo [16], and Yassein and shahhadi [17] presented comparison between NTRU and QTRU with four methods NTRU-like in terms of security.

* Corresponding author.
2020 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted June 09, 2025. Published January 20, 2026

In 2023 Yassein and Ali presented SQNTRU cryptosystem [12], which is based on commutative and associative subalgebra of Quintuple algebra, and HUDTRU cryptosystem [14], which is based on commutative and associative quintuple algebra. In same year, Salman and Yassein presented TRUFT cryptosystem [10], which is based on commutative and associative FTH algebra and TRUHSH cryptosystem [15], which is based on hexat algebra.

In 2024, Fadeel and Yassein [5], presented HAQTR cryptosystem, which is based on non-commutative quaternion algebra. In same year, Abidalzahra and Yassein [2] presented ASTRU cryptosystem, which is based on associative and commutative AS algebra. Also, Abboud et al. [1] presented OTRCQ which is a multi-dimensional public-key cryptosystem is based on octonions algebra with coefficients of commutative quaternion. In 2025, Al-Bairmani et al. [3] presented KPNTR cryptosystem, which is based on para-quaternion with coefficients in KAH-Octo algebra. Also, Sahib and Yassein proposed encryption system via a multi-dimensional algebra AT, which called ATTRU [9].

2. QTRAT Cryptosystem

QTRAT depended on AT algebra [18] with coefficients of quaternion and the same parameters in ATTRU and three AT algebras:

$$\sigma = \left\{ \left(f_{(0,0)} + f_{(0,1)}i + f_{(0,2)}j + f_{(0,3)}k\right) + \sum_{n=1}^{11} \left(f_{(n,0)} + f_{(n,1)}i + f_{(n,2)}j + f_{(n,3)}k\right)\beta_n | f_{(n,0)}, f_{(n,1)}, f_{(n,2)}, f_{(n,3)} \in \mathcal{K}, n = 0, 1, \ldots, 11\right\},$$

$$\sigma_p = \left\{ \left(f_{(0,0)} + f_{(0,1)}i + f_{(0,2)}j + f_{(0,3)}k\right) + \sum_{n=1}^{11} \left(f_{(n,0)} + f_{(n,1)}i + f_{(n,2)}j + f_{(n,3)}k\right)\beta_n | f_{(n,0)}, f_{(n,1)}, f_{(n,2)}, f_{(n,3)} \in \mathcal{K}_p, n = 0, 1, \ldots, 11\right\},]$$

$$\sigma_q = \left\{ \left(f_{(0,0)} + f_{(0,1)}i + f_{(0,2)}j + f_{(0,3)}k\right) + \sum_{n=1}^{11} \left(f_{(n,0)} + f_{(n,1)}i + f_{(n,2)}j + f_{(n,3)}k\right)\beta_n | f_{(n,0)}, f_{(n,1)}, f_{(n,2)}, f_{(n,3)} \in \mathcal{K}_q, n = 0, 1, \ldots, 11\right\}$$

$\mathcal{K} \cong \mathbb{Z}[x]/(x^N - 1)$, $\mathcal{K}_p \cong \mathbb{Z}_p[x]/(x^N - 1)$, and $\mathcal{K}_q \cong \mathbb{Z}_q[x]/(x^N - 1)$ are the truncated polynomial rings,

The four subsets $\ell_{\mathcal{F}}, \ell_{\mathcal{G}}, \ell_{\mathcal{M}}$, and $\ell_{\mathcal{R}} \subseteq \sigma$ defined as the following:

$\ell_{\mathcal{F}} = \{\mathcal{F} \in \sigma | f_{(n,\Delta)}, \Delta = 0, 1, 2, 3, n = 0, 1, \ldots 11$ has d_f coefficients equal to 1, $(d_f - 1)$ equal to -1 and 0 for other values $\}$

$\ell_{\mathcal{G}} = \{\mathcal{G} \in \sigma | \mathcal{G}_{(n,\Delta)}, \Delta = 0, 1, 2, 3, n = 0, 1, \ldots 11$ has $d_{\mathcal{G}}$ coefficients equal to 1, $(d_{\mathcal{G}} - 1)$ equal to -1 and 0 for other values $\}$

$\ell_{\mathcal{M}} = \{\mathcal{M} \in \sigma | \mathcal{M}_{(n,\Delta)}, \Delta = 0, 1, 2, 3, n = 0, 1, \ldots 11$, are chosen modulo between $\frac{-p}{2}$ and $\frac{p}{2}$ $\}$,

and the subset $\ell_{\mathcal{R}}$ defined similar to $\ell_{\mathcal{G}}$.

QTRAT designed goes through the following three phases:

2.1. Key Generation

The recipient at this phase chooses $\mathcal{F} = \sum_{n=0}^{11} \mathcal{F}_n \beta_n \in \ell_{\mathcal{F}}$ such that it had an inverse over σ_p and σ_q where

$$\mathcal{F}_t = \sum_{n=0}^{11} \left(f_{(n,0)} + f_{(n,1)}i + f_{(n,2)}j + f_{(n,3)}k\right)\beta_n \ , t = 0, 1, \ldots, 11,$$

and chooses $\mathcal{G} \in \ell_{\mathcal{G}}$.

After that, compute public key $\mathcal{H}$ as follows:

$$\mathcal{H} \equiv \mathcal{F}_q^{-1} * \mathcal{G} \ \ (mod\ q)$$

where $\mathcal{F}, \mathcal{G}$is a private keys.

2.2. Encryption

The sender at this phase, after receiving $\mathcal{H}$, writes the message $\mathcal{m}$ in the form

$$\left(m_{(0,0)} + m_{(0,1)}i + m_{(0,2)}j + m_{(0,3)}k\right) + \sum_{n=1}^{11} \left(m_{(n,0)} + m_{(n,1)}i + m_{(n,2)}j + m_{(n,3)}k\right) \beta_n \in \ell_{\mathcal{m}}$$

and chooses $\mathcal{R} \in \ell_{\mathcal{R}}$ as private key.

Compute $\mathcal{E}$ the encrypted text of the message as follows:

$$\mathcal{E} \equiv p\mathcal{H} * \mathcal{R} + \mathcal{m} \ \ (mod\ q)\,,$$

all the coefficients belong to $(-{}^{q}/_{2}, {}^{q}/_{2}]$.

2.3. Decryption

The recipient at this phase, after receiving the encrypted text $\mathcal{E}$, Performs the following steps:

$$\begin{aligned}
\mathcal{A} &\equiv \mathcal{F} * \mathcal{E} \ \ (mod\ q)\\
&\equiv \mathcal{F} * (p\mathcal{H} * \mathcal{R} + \mathcal{m}\ )\ (mod\ q)\\
&\equiv (p\mathcal{F} * \mathcal{H}) * \mathcal{R} + \mathcal{F} * \mathcal{m} \ \ (mod\ q)\\
&\equiv \left(\left(p\mathcal{F} * \mathcal{F}_q^{-1}\right) * \mathcal{G}\right) * \mathcal{R} + \mathcal{F} * \mathcal{m} \ \ (mod\ q)\\
&\equiv p\mathcal{G} * \mathcal{R} + \mathcal{F} * \mathcal{m} \ \ (mod\ q)\,,
\end{aligned}$$

and adjust the resulting coefficients within the interval $(\frac{-q}{2}, \frac{q}{2}]$.

Covert $\mathcal{A}$ from $mod\ q$ to $mod\ p$.

Thus, $\mathcal{A}_1 \equiv \mathcal{A}\ (mod\ p)$, therefore $\mathcal{m} \equiv \mathcal{F}_p^{-1} * \mathcal{A}_1 \ \ (mod\ p)$. All coefficients of the last term within the interval $(\frac{-p}{2}, \frac{p}{2}]$.

3. Performance Analysis

Given the known public parameters, an attacker can obtain the original text of the encrypted message by searching for the private key of the public key or by using the private key during the encryption phase.

Searching for one of the two private keys, $\mathcal{F}$ or $\mathcal{G}$, represents the security space of the key. If we assume that the space of $\mathcal{G}$ is less than $\mathcal{F}$, attempts to access the original text through a brute force attack are calculated as follows:

$$\left(\binom{N}{d_g}\binom{N-d_g}{d_g}\right)^{48} = \left(\frac{N!}{(d_g!)^2\,(N-2d_g)!}\right)^{48}.$$

The same applies when searching for key $\mathcal{R}$, which represents the security space of the message, which is calculated as follows:

$$\left(\binom{N}{d_{\mathfrak{r}}}\binom{N-d_{\mathfrak{r}}}{d_{\mathfrak{r}}}\right)^{48} = \left(\frac{N!}{(d_{\mathfrak{r}}!)^2\,(N-2d_{\mathfrak{r}})!}\right)^{48}.$$

4. Comparison of QTRAT with NTRU and Some of its Improvements

Comparison of QTRAT public key cryptosystem with NTRU and some of its improvements such as QTRU, ATTRU and HXDTRU cryptosystems, the comparison includes security and execution time.

4.1. Comparison Execution Time

Table 1 shows comparison between the execution time of the NTRU cryptosystem and some of its improvements such as QTRAT, QTRU, ATTRU and HXDTRU.

Table 1: Execution Time of NTRU, QTRU, ATTRU, HXDTRU and QTRAT

Phase	NTRU	QTRU	ATTRU	HXDTRU	QTRAT
Key generation	One Convolution multiplication	16 Convolution multiplication	12 Convolution multiplication	256 Convolution multiplication	192 Convolution multiplication
Encryption	One Convolution multiplication One Polynomial addition	16 Convolution multiplications Four Polynomial additions	12 Convolution multiplication 12 Polynomial addition	256 Convolution multiplication 16 Polynomial addition	192 Convolution multiplications 48 Polynomial addition
Decryption	Two Convolution multiplications One Polynomial addition	32 Convolution multiplications Four Polynomial addition	24 Convolution multiplication 12 Polynomial addition	8192 Convolution multiplication 16 Polynomial addition	384 Convolution multiplications 48 Polynomial addition
Total Time	$4\mathcal{T} + 2\mathcal{T}_1$	$64\mathcal{T} + 8\mathcal{T}_1$	$48\mathcal{T} + 24\mathcal{T}_1$	$8704\mathcal{T} + 32\mathcal{T}_1$	$768\mathcal{T} + 96\mathcal{T}_1$

Where $\mathcal{T}_1$ is the addition times, and $\mathcal{T}$ is the convolution multiplication time. Therefore, QTRAT is faster than HXDRTU but slower than NTRU, QTRU, and ATTRU.

4.2. Space of Security

Table 2 shows a comparison of space security between NTRU, QTRAT, QTRU, ATTRU and HXDTRU cryptosystems. This comparison is about space of key security and space of message security.

Table 2: Space of security of NTRU, QTRU, ATTRU, HXDTRU and QTRAT

Cryptosystem	Space of key security	Space of message security
NTRU	$\frac{N!}{(d_g!)^2(N-2d_g)!}$	$\frac{N!}{(d_{\mathfrak{r}}!)^2(N-2d_{\mathfrak{r}})!}$
QTRU	$\left(\frac{N!}{(d_g!)^2(N-2d_g)!}\right)^4$	$\left(\frac{N!}{(d_{\mathfrak{r}}!)^2(N-2d_{\mathfrak{r}})!}\right)^4$
ATTRU	$\left(\frac{N!}{(d_g!)^2(N-2d_g)!}\right)^{12}$	$\left(\frac{N!}{(d_{\mathfrak{r}}!)^2(N-2d_{\mathfrak{r}})!}\right)^{12}$
HXDTRU	$\left(\frac{N!}{(d_g!)^2(N-2d_g)!}\right)^{16}$	$\left(\frac{N!}{(d_{\mathfrak{r}}!)^2(N-2d_{\mathfrak{r}})!}\right)^{16}$
QTRAT	$\left(\frac{N!}{(d_g!)^2(N-2d_g)!}\right)^{48}$	$\left(\frac{N!}{(d_{\mathfrak{r}}!)^2(N-2d_{\mathfrak{r}})!}\right)^{48}$

According to the Table 2, the space of security of QTRAT is greater than that of the NTRU, QTRU, ATTRU and HXDTRU.

Table 3 show the key space and message space of QTRAT respectively according some values

We will take the same values for all methods to compare the key and message space in Table (4), Table (5), Figure (1), and Figure (2), respectively.

Table 3: Key space and essage space of QTRAT

N	d_g	d_r	Key space	Message space
107	12	12	2.1430×10^{1446}	2.1430×10^{1446}
107	20	20	1.6401×10^{1956}	1.6401×10^{1956}
149	12	12	2.3818×10^{1629}	2.3818×10^{1629}
149	25	25	1.0383×10^{2603}	1.0383×10^{2603}
167	18	18	3.5608×10^{2238}	3.5608×10^{2238}
167	27	27	1.6690×10^{2868}	1.6690×10^{2868}
211	20	20	1.5004×10^{2615}	1.5004×10^{2615}
211	34	34	3.0476×10^{3639}	3.0476×10^{3639}
257	20	20	1.6564×10^{2795}	1.6564×10^{2795}
257	24	24	4.6405×10^{3170}	4.6405×10^{3170}

Table 4: Key space and essage space of QTRAT

NTRU	QTRU	ATTRU	HXDTRU	QTRAT
1.3549×10^{30}	3.370×10^{120}	3.8273×10^{361}	1.2898×10^{482}	2.1430×10^{1446}
5.6817×10^{40}	1.0421×10^{163}	1.1317×10^{489}	1.1794×10^{652}	1.6401×10^{1956}
8.8176×10^{33}	6.0451×10^{135}	2.2090×10^{407}	1.3354×10^{543}	2.3818×10^{1629}
1.6963×10^{54}	8.2796×10^{216}	5.6759×10^{650}	4.6994×10^{867}	1.0383×10^{2603}
4.3300×10^{46}	3.5152×10^{186}	4.3436×10^{559}	1.5269×10^{746}	3.5608×10^{2238}
5.6837×10^{59}	1.0436×10^{239}	1.1365×10^{717}	1.1860×10^{956}	1.6690×10^{2868}
3.0397×10^{54}	8.5373×10^{217}	6.2226×10^{653}	5.3152×10^{871}	1.5004×10^{2615}
6.6463×10^{75}	1.9513×10^{303}	7.4295×10^{909}	1.4497×10^{1213}	3.0476×10^{3639}
1.1713×10^{58}	1.8822×10^{232}	6.6683×10^{696}	1.2551×10^{929}	1.6564×10^{2795}
1.1366×10^{66}	1.6689×10^{264}	4.6483×10^{792}	7.7575×10^{1056}	4.6405×10^{3170}

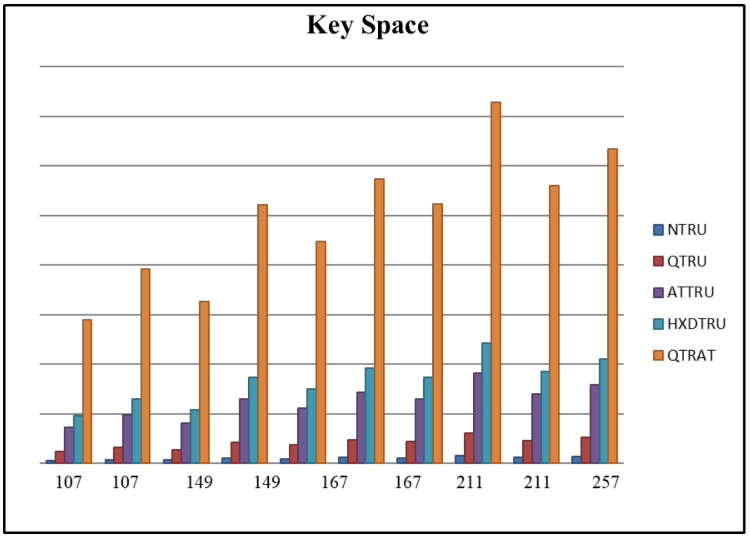

Figure 1: Space of key security of NTRU, QTRU, ATTRU, HXDTRU and QTRAT

Table 5: Space of message security of NTRU, QTRU, ATTRU, HXDTRU and QTRAT

NTRU	QTRU	ATTRU	HXDTRU	QTRAT
1.3549×10^{30}	3.3700×10^{120}	3.8273×10^{361}	1.2898×10^{482}	2.1430×10^{1446}
5.6817×10^{40}	1.0421×10^{163}	1.1317×10^{489}	1.1794×10^{652}	1.6401×10^{1956}
8.8176×10^{33}	6.0451×10^{135}	2.2090×10^{407}	1.3354×10^{543}	2.3818×10^{1629}
1.6963×10^{54}	8.2796×10^{216}	5.6759×10^{650}	4.6994×10^{867}	1.0383×10^{2603}
4.3300×10^{46}	3.5152×10^{186}	4.3436×10^{559}	1.5269×10^{746}	3.5608×10^{2238}
5.6837×10^{59}	1.0436×10^{239}	1.1365×10^{717}	1.1860×10^{956}	1.6690×10^{2868}
3.0397×10^{54}	8.5373×10^{217}	6.2226×10^{653}	5.3152×10^{871}	1.5004×10^{2615}
6.6463×10^{75}	1.9513×10^{303}	7.4295×10^{909}	1.4497×10^{1213}	3.0476×10^{3639}
1.1713×10^{58}	1.8822×10^{232}	6.6683×10^{696}	1.2551×10^{929}	1.6564×10^{2795}
1.1366×10^{66}	1.6689×10^{264}	4.6483×10^{792}	7.7575×10^{1056}	4.6405×10^{3170}

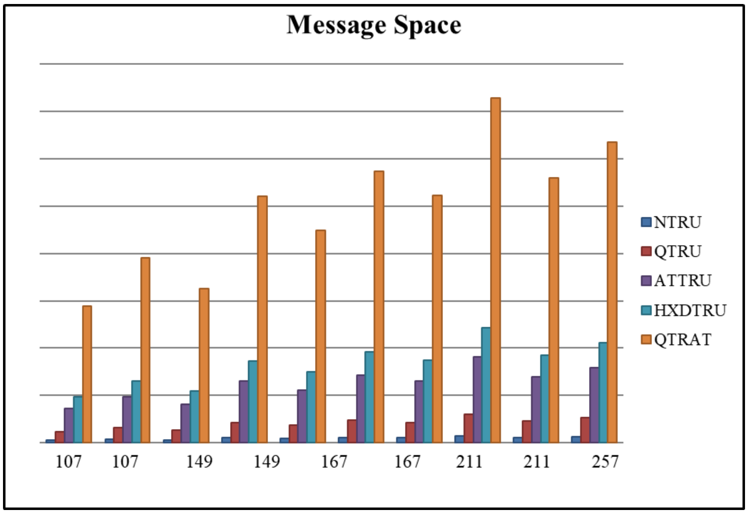

Figure 2: Space of message security of NTRU, QTRU, ATTRU, HXDTRU and QTRAT

5. Conclusions

The QTRAT method presented in this paper is based on the idea of combining two algebras at the same time, one of which is the basic algebra, which is AT, and the other is the quaternion algebra, which is the coefficients of the first algebra, which greatly increases its security level compared to other methods, and its execution time is somewhat acceptable. In addition, there is another advantage in that it is a multidimensional method, which makes it possible to send multiple messages at the same time, up to 48 different messages, which makes this method a requirement for organizations operating in different directions using different transmission media.

References

1. S. M. Abboud, H. R. Yassein, and R. K. Alhamido, *Improvement of a multi-dimensional public-key otru cryptosystem*, International Journal of Mathematics and Computer Science **19** (2024), no. 4, 1071–1076.

2. A. A. Abidalzahra and H. R. Yassein, *Proposed development of ntru encryption*, International Journal of Mathematics and Computer Science **19** (2024), no. 3, 715–719.

3. S. A. Al-Bairmani, N. N. Hani, and H. R. Yassein, *A new high-performance public-key encryption scheme using two algebras*, International Journal of Mathematics and Computer Science **20** (2025), no. 1, 435–438.

4. H. A. Ali and H. R. Yassein, *QTNTR: A New Secure NTRUEncrypt Alternative with a High Level of Security*, Mathematical Statistician and Engineering Applications **71** (2022), no. 4, 5634–5639.

5. A. C. Fadeel and H. R. Yassein, *Haqtr: Ntru-like public key*, International Journal of Mathematics and Computer Science **19** (2024), no. 1, 1–4.

6. J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A Ring-Based Public Key Cryptosystem*, International Algorithmic Number Theory Symposium, Springer, 1998, pp. 267–288.

7. E. Malekian and A. Zakerolhosseini, *OTRU: A Non-Associative and High Speed Public Key Cryptosystem*, 2010 15th CSI International Symposium on Computer Architecture and Digital Systems (CADS) (Tehran, Iran), IEEE, September 2010, pp. 83–90.

8. E. Malekian, A. Zakerolhosseini, and A. Mashatan, *QTRU: Quaternionic Version of the NTRU Public–Key Cryptosystems*, The ISC International Journal of Information Security **3** (2011), no. 1, 29–42.

9. A. A. Sahib and H. R. Yassein, *Novel encryption system via a new multi-dimensional algebra*, International Journal of Mathematics and Computer Science **20** (2025), no. 1, 507–509.

10. H. S. Salman and H. R. Yassein, *Truhsh: Developing ntru cryptosystem in terms of security and performance*, Applied Mathematics and Information Sciences an International Journal **17** (2023), no. 4, 723–725.

11. N. H. UbaidurRahman, C. Balamurugan, and R. Mariappan, *A Novel DNA Computing Based Encryption and Decryption Algorithm*, Procedia Computer Science **46** (2015), 463–475.

12. H. R. Yassein and H. H. Abo-Alsood, *Performance analysis of some analog ntru public key*, AIP Conference Proceedings **2845** (2023), no. 1, 050038.

13. H. R. Yassein and N. M. Al-Saidi, *HXDTRU Cryptosystem Based on Hexadecnion Algebra*, Proceedings of the 5th International Cryptology and Information Security Conference (Cryptology2016) (Malaysia), 2016.

14. H. R. Yassein and H. A. Ali, *Hudtru: An enhanced ntru for data security via quintuple algebra*, International Journal of Mathematics and Computer Science **18** (2023), no. 2, 199–204.

15. H. R. Yassein and S. H. Shahhadi, *A comparative analysis between ntru and its some ntru-like cryptosystems*, AIP Conference Proceedings **2845** (2023), no. 1, 050039.

16. H. R. Yassein, H. N. Zaky, H. H. Abo-alsoo, I. A. Mageed, and W. I. ElSobky, *Quitru: Design secure variant of ntruencrypt via a new multi-dimensional algebra*, Applied Mathematics and Information Sciences an International Journal **17** (2023), no. 1, 1–5.

17. H.R. Yassein and H. A. Ali, *Sqntru: New public key encryption*, International Journal of Mathematics and Computer Science **18** (2023), no. 3, 381–385.

18. Z. Yunpeng, Z. Yu, W. Zhong, and R. O. Sinnott, *Index-based symmetric dna encryption algorithm*, 2011 4th International Congress on Image and Signal Processing (Shanghai, China), vol. 5, IEEE, 2011, pp. 2290–2294.

Amna Abdul Karim Sahib,
Department of Mathematics,
College of Education, University of Al-Qadisiyah,
Iraq.
E-mail address: edu.math.post24.24@qu.edu.iq

and

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