Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/170107

QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra

Hassan Rashed Yassein[1,], Hany Nasry Zaky[2], Hadeel Hadi Abo-Alsoo[1], Ismail A Mageed[3] and Wageda I. El-Sobky[4]*

[1]Department of Mathematics, College of Education, University of Al-Qadisiyah, Dewaniyah, Iraq
[2]Mathematics Department, Military Technical College, Cairo, Egypt
[3]Department of Computer Science, Faculty of engineering and Informatics, University of Bradford, Bradford, United Kingdom
[4]Department of Basic Engineering Sciences, Benha Faculty of Engineering, Benha University, Benha 13511, Egypt

Received: 23 Sep. 2022, Revised: 12 Nov. 2022, Accepted: 13 Dec. 2022
Published online: 1 Jan. 2023

Abstract: The NTRU public-key cryptosystem is based on time complexity and efficient computations. Many researchers were stimulated to improve NTRU performance by changing mathematical structure with new algebraic structures and replacing the truncated polynomial ring, such as OTRU, QTRU. In this paper, we proposed QuiTRU as a new version of the NTRU. It's a five-dimensional cryptosystem based on a new algebraic structure. As well, QuiTRU was compared with NTRU, QTRU, and OTRU.

Keywords: NTRU, QTRU, OTRU, QuiTRU.

1 Introduction

The first NTRU version was suggested by [1]. It has been assessed recently as the fastest public-key cryptosystems, its operations are in the truncated polynomial ring with coefficients in Z. Many studies were published to improve NTRU, some of them were focused on security improvement through the replacement of the original ring. [2] presented a generalization of NTRU by the ring of polynomials over the binary field F_2 which is called CTRU. [3] presented an analog of NTRU called MaTRU; this system operates in the ring of $k \times k$ matrices of polynomials in $Z[x]/(x^n-1)$. [4] presented a system called QTRU that relies on quaternion algebra. [5] presented a cryptosystem called OTRU, which depends on the octonion algebra. [6,7] introduced ETRU depends on Eisenstein integer ring $Z[\omega]$. [8] proposed a new multidimensional public key cryptosystem called CQTRU that operates in commutative quaternion algebra. [9,10, 11], presented new cryptosystems, called HXDTRU and BITRU, based on their hexadecenion and binary algebras. [12,13] introduced a new NTRU-like cryptosystem that depends on the bi-cartesian algebra; they called it BCTRU. [14] introduced a new NETRU cryptosystem that operates over the ring $M = M_k(Z_p)[T,x]/(X^n - I_{k*k})$ of $k*k$ matrices of elements in the ring $R = Z_p[T,x]/(x^n-1)$. [15] introduced a new NTRU-analog cryptosystem using multidimensional carternion algebra called QOB$_{TRU}$. [16] proposed a new multi-dimensional public key cryptosystem, called NTRTE which relies on a commutative quaternion algebra with a new structure. [17] presented QMTRU with a new mathematical structure as an improvement for QTRU. This paper designed a new version of NTRU, called QuiTRU depends on the new algebra, namely HH-Real algebra with a new mathematical structure. This paper is structured as follows. HH-Real algebra was introduced in Section 2. The QuiTRU cryptosystem is defined in section 3, the security analysis of QuiTRU is discussed in section 4. The comparison is carried out in Section 5 with QuiTRU, NTRU, QTRU, and OTRU. Finally, some conclusions are in section 6.

2 HH-REAL ALGEBRA

The following is the describes of a new HH-Real algebra, which is a five-dimensional vector space over the real number $\mathbb{R}$:

$$HH = \{a_0\tau_0 + a_1\tau_1 + a_2\tau_2 + a_3\tau_3 + a_4\tau_4 \;\; a_0,\ldots,a_4 \in \mathbb{R}\}.$$

* Corresponding author e-mail: hassan.yaseen@qu.edu.iq

It is called real HH-Real algebra with basis $\{\tau_0,\tau_1,\tau_2,\tau_3,\tau_4\}$ such that $\tau_0=(1,0,0,0,0)$, $\tau_1=(0,1,0,0,0)$, $\tau_2=(0,0,1,0,0)$, $\tau_3=(0,0,0,1,0)$, $\tau_4=(0,0,0,0,1)$.

Let $p_0=a_0\tau_0+a_1\tau_1+a_2\tau_2+a_3\tau_3+a_4\tau_4$ and $p_1=b_0\tau_0+b_1\tau_1+b_2\tau_2+b_3\tau_3+b_4\tau_4\in$ HH, then the operations on this algebra are defined as follows: The addition:

$$p_0+p_1=(a_0+b_0)\,\tau_0+(a_1+b_1)\,\tau_1+(a_2+b_2)\,\tau_2 \\ +(a_3+b_3)\,\tau_3+(a_4+b_4)\,\tau_4.$$

The multiplication:

$$p_0*p_1=(a_0b_0)\,\tau_0+(a_1b_1)\,\tau_1+(a_2b_2)\,\tau_2 \\ +(a_3b_3)\,\tau_3+(a_4b_4)\,\tau_4$$

where $*$ is the HH-Real algebra product.This multiplication is associative and commutative. The multiplicative inverse is defined as follows:

$$p_0^{-1}=c_0\tau_0+c_1\tau_1+c_2\tau_2+c_3\tau_3+c_4\tau_4$$

Such that:

$$c_0=\frac{1}{a_0},\; c_1=\frac{1}{a_1},\; c_2=\frac{1}{a_2}, \\ c_3=\frac{1}{a_3},\; c_4=\frac{1}{a_4}\; \text{ and } \; a_0,\ldots,a_4\neq 0.$$

Consider the rings $\mathcal{K}=Z[x]/\left(x^N-1\right)$, $\mathcal{K}_p=Z_p[x]/\left(x^N-1\right)$, and $\mathcal{K}_q=Z_q[x]/\left(x^N-1\right)$. The HH-Real algebras $\mathcal{D}$, $\mathcal{D}_p$, and $\mathcal{D}_q$ are defined as follows:

$$\mathcal{D}=\{f_0\tau_0+f_1\tau_1+f_2\tau_2+f_3\tau_3+f_4\tau_4 \quad f_0,\ldots,f_4\in\mathcal{K}\}$$

$$\mathcal{D}_p=\left\{f_0\tau_0+f_1\tau_1+f_2\tau_2+f_3\tau_3+f_4\tau_4 \quad f_0,\ldots,f_4\in\mathcal{K}_p\right\},$$

$$\mathcal{D}_q=\left\{f_0\tau_0+f_1\tau_1+f_2\tau_2+f_3\tau_3+f_4\tau_4 \quad f_0,\ldots,f_4\in\mathcal{K}_q\right\}.$$

3 The QuiTRU Cryptosystem

3.1 Parameter Creation

As in NTRU, QuiTRU has three parameters N,p,q defined in the same manner, and the subsets $\left(\mathcal{L}_F,\mathcal{L}_G,\ \mathcal{L}_J,\ \mathcal{L}_R,\ \mathcal{L}_\phi,\ \mathcal{L}_M\right)\subset\mathcal{D}$ are defined in Table 1.

Table 1: Subsets of QuiTRU

Notation	Definition
$\mathcal{L}_F$	$\{f_0(x)\,\tau_0+f_1(x)\,\tau_1+f_2(x)\,\tau_2+f_3(x)\,\tau_3+f_4(x)\,\tau_4$ $\in\mathcal{D}\setminus f_0(x),\ldots,f_4(x)\in\mathcal{K}\; satisfy\; \ell\left(d_f,d_f-1\right)\}$
$\mathcal{L}_G$	$\{g_0(x)\,\tau_0+g_1(x)\,\tau_1+g_2(x)\,\tau_2+g_3(x)\,\tau_3+g_4(x)\,\tau_4$ $\in\mathcal{D}\setminus g_0(x),\ldots,g_4(x)\in\mathcal{K}\; satisfy\; \ell\left(d_g,d_g\right)\}$
$\mathcal{L}_J$	$\{j_0(x)\,\tau_0+j_1(x)\,\tau_1+j_2(x)\,\tau_2+j_3(x)\,\tau_3+j_4(x)\,\tau_4$ $\in\mathcal{D}\setminus j_0(x),\ldots,j_4(x)\in\mathcal{K}\; satisfy\; \ell\left(d_j,d_j\right)\}$
$\mathcal{L}_R$	$\{r_0(x)\,\tau_0+r_1(x)\,\tau_1+r_2(x)\,\tau_2+r_3(x)\,\tau_3+r_4(x)\,\tau_4$ $\in\mathcal{D}\setminus r_0(x),\ldots,r_4(x)\in\mathcal{K}\; satisfy\; \ell\left(d_r,d_r\right)\}$
$\mathcal{L}_\phi$	$\{\phi_0(x)\,\tau_0+\phi_1(x)\,\tau_1+\phi_2(x)\,\tau_2+\phi_3(x)\,\tau_3+\phi_4(x)\,\tau_4$ $\in\mathcal{D}\setminus\phi_0(x),\ldots,\phi_4(x)\in\mathcal{K}\; satisfy\; \ell(d_\phi,d_\phi)\}$
$\mathcal{L}_M$	$\{m_0(x)\,\tau_0+m_1(x)\,\tau_1+m_2(x)\,\tau_2+m_3(x)\,\tau_3$ $+m_4(x)\,\tau_4\in\mathcal{D}\setminus cofficients\; of\; m_0(x),\ldots,m_4(x)$ $\in\mathcal{K}$ are the chosen modulo between $-p/2$ and $p/2\}$

where $\ell\left(d_x,d_y\right)=\Big\{f\in\mathcal{K}\setminus f$ has d_x coeff.equal to $1,\ d_y$ coeff.equal to $-1,$ and the rest are $0\Big\}$.

3.2 Key Generation

To generate the keys, first, we randomly choose $F\in\mathcal{L}_F$, $G\in\mathcal{L}_G$, and $J\in\mathcal{L}_J$, such that F should be invertible under mod q and p. Let the inverses be denoted by F_q^{-1} and F_p^{-1}.
An algorithm below illustrates public key generation in the proposed QuiTRU.

Algorithm 1 The proposed QuiTRU: Keys Generation Process

Input: $N,\ p,\ q,\ F,\ G,\ J$
Output: public key H
1: Choose randomly $\in\mathcal{L}_F$, $G\in\mathcal{L}_G$, and $J\in\mathcal{L}_J$
2: Compute $F_q^{-1}=$ inverse of $F\ (mod\ q)$
3: Compute $H=F_q^{-1}*G*J\ (mod\ q)$
4: Return H as a public key and $\{F,\ G,\ J\}$ is a set of the private keys
5: end

3.3 Encryption

Initially, we choose $\phi\in\mathcal{L}_\phi$, $R\in\mathcal{L}_R$, to encrypt the message $M\in\mathcal{L}_M$, it should be convert to HH-Real algebra form. Then, the encrypted message is

$$E=p\,(H*\phi+R)+M\ \ (mod\ q)\,.$$

An algorithm below illustrates encryption in the proposed QuiTRU.

Algorithm 2 The proposed QuiTRU: Encryption process

Input: $N,\ p,\ q,\ F,\ G,\ J$
Output: The encryption E of message M

chooses message $M \in \mathcal{L}_M$
converts a message M into a HH-Real algebra form.
computes the ciphertext $E = p(H * \Phi + R) + M(mod\ \mathrm{q})$
Return E as a ciphertext $E = p(H * \Phi + R) + M(mod\ \mathrm{q})$.
end

3.4 Decryption

Upon receiving the first user to the ciphertext, he/ she wants to decrypt it and recover the original message M. So, the decryption process can be explained by Algorithm (3).

Algorithm 3 The proposed QuiTRU: Encryption process

```
Input: N, q, p, F, F_p^{-1}, E
Output: A message M
chooses message M ∈ L_M
Compute D = F * E (mod q)
for i = 1 to 5 do
    for i = 1 to 5 do
        if D_2(i, j) <= -p/2 then
            Compute D_2(i, j) = D_2(i, j) + p
        else if D_2(i, j) > p/2 then
            Compute D_2(i, j) = D_2(i, j) - p
        end if
    end for
end for
Return M = D_2
end
```

4 Security analysis

There are many attacks that have been used to analyze NTRU and their variance cryptosystems. The most used one is the brute force attack, the attacker who know the public parameters and the public key $H = F_q^{-1} * G * J$ $mod\ q$ is tried to find the private key F from the set $\mathcal{L}_F$ (or find the private keys $G,\ J$ from the sets $\mathcal{L}_G,\ \ \mathcal{L}_J$).This helps to find a decryption short key, or the random polynomials $\phi,\ R$ from the set $\mathcal{L}_\phi$,$\mathcal{L}_R$, which leads to find the message. The size of the subsets$\mathcal{L}_F,\ \ \mathcal{L}_G,\ \mathcal{L}_J,\ \mathcal{L}_\phi,\ \mathcal{L}_R$is equal to

$$|\mathcal{L}_F| = \left(\frac{N!}{(d_f!)^2 (N-2d_f)!}\right)^5, |\mathcal{L}_G| = \left(\frac{N!}{(d_g!)^2 (N-2d_g)!}\right)^5,$$
$$|\mathcal{L}_J| = \left(\frac{N!}{(d_j!)^2 (N-2d_j)!}\right)^5, |\mathcal{L}_\phi| = \left(\frac{N!}{(d_\phi!)^2 (N-2d_\phi)!}\right)^5,$$
$$|\mathcal{L}_R| = \left(\frac{N!}{(d_r!)^2 (N-2d_r)!}\right)^5.$$

Therefore, the size of the search space of finding the private keys $G,\ J$ is

$$\frac{(N!)^{10}}{(d_g!\ d_j!)^{10} \left((N-2d_g)!\ (N-2d_j)!\right)^5}.$$

Similarly, the size of the search space to find the polynomials $R,\ \ \phi$ is

$$\frac{(N!)^{10}}{\left(d_r!\ d_\phi!\right)^{10} \left((N-2d_r)!\ \left(N-2d_\phi\right)!\right)^5}.$$

Table 2 shows the security level of the private key space and message space according to the general parameters in QuiTRU and $p = 3$

Table 2: The Space of the Private Key and the Message

d_r	d_ϕ	d_j	d_g	d_f	N	Key space	Message space
5	5	12	12	12	107	2.0843×10^{301}	2.9627×10^{159}
10	10	20	20	20	107	3.5056×10^{407}	2.8397×10^{266}
10	10	12	12	12	149	2.8413×10^{339}	4.4184×10^{297}
20	20	25	25	25	149	1.9727×10^{542}	3.0923×10^{476}
18	18	18	18	18	167	2.3168×10^{466}	2.3168×10^{466}
22	22	27	27	27	167	3.5184×10^{597}	8.1583×10^{529}
18	18	20	20	20	211	6.7356×10^{544}	7.1192×10^{506}
22	22	34	34	34	211	1.6819×10^{758}	5.0344×10^{580}
18	18	20	20	20	257	2.1743×10^{582}	1.8873×10^{540}
24	24	24	24	24	257	3.5936×10^{660}	3.5936×10^{660}

5 Comparing NTRU, QTRU, OTRU, and QuiTRU

We now compare the proposed QuiTRU with the original NTRU, and QTRU, OTRU because the dimensional of QuiTRU between the dimensional of QTRU and OTRU according to some main criteria such as, level of security of the key and the message, efficiency.

5.1 Level of Security

In Tables 3 and 4, a comparison between the QuiTRU and NTRU, QTRU, and OTRU in terms of security level for the key and the message is introduced depending on the generic parameters. Thus, the comparison between key security and message security in the QuiTRU, NTRU, QTRU, and OTRU systems shows that the security level of QuiTRU is better than that of the NTRU, QTRU, and OTRU.

Table 3: Key Space in QuiTRU, NTRU, QTRU, and OTRU

Key Space			
QuiTRU	NTRU	QTRU	OTRU
2.0843×10^{301}	1.3549×10^{30}	3.3696×10^{120}	1.1355×10^{241}
3.5056×10^{407}	5.6817×10^{40}	1.0421×10^{163}	1.0859×10^{326}
2.8413×10^{339}	8.8176×10^{33}	6.0452×10^{135}	3.6544×10^{271}
1.9727×10^{542}	1.6963×10^{54}	8.2799×10^{216}	6.8557×10^{433}
2.3168×10^{466}	4.3300×10^{46}	3.5153×10^{186}	1.2357×10^{373}
3.5184×10^{597}	5.6837×10^{59}	1.0436×10^{239}	1.0891×10^{478}
6.7356×10^{544}	3.0397×10^{54}	8.5378×10^{217}	7.2895×10^{435}
1.6819×10^{758}	6.6463×10^{75}	1.9513×10^{303}	3.8076×10^{606}
2.1743×10^{582}	1.7129×10^{58}	8.6085×10^{232}	7.4107×10^{465}
3.5936×10^{660}	1.1358×10^{66}	1.6681×10^{264}	2.7825×10^{528}

Table 4: Message Space in QuiTRU, NTRU, QTRU, and OTRU

Message Space			
QuiTRU	**NTRU**	**QTRU**	**OTRU**
2.9627×10^{159}	8.8546×10^{15}	6.1472×10^{63}	3.7788×10^{127}
2.8397×10^{266}	4.4190×10^{26}	3.8134×10^{106}	1.4542×10^{213}
4.4184×10^{297}	5.8147×10^{29}	1.1432×10^{119}	1.3068×10^{238}
3.0923×10^{476}	4.4568×10^{47}	3.9455×10^{190}	1.5567×10^{381}
2.3168×10^{466}	4.3300×10^{46}	3.5153×10^{186}	1.2357×10^{373}
8.1583×10^{529}	9.7985×10^{52}	9.2180×10^{211}	8.4972×10^{423}
7.1192×10^{506}	4.8444×10^{50}	5.5077×10^{202}	3.0335×10^{405}
5.0344×10^{580}	1.1754×10^{58}	1.9088×10^{232}	3.6438×10^{464}
1.8873×10^{540}	1.0656×10^{54}	1.2893×10^{216}	1.6622×10^{432}
3.5936×10^{660}	1.1358×10^{66}	1.6681×10^{264}	2.7825×10^{528}

5.2 Mathematical Operations

In this subsection, a comparison of the QuiTRU, NTRU, QTRU, and the OTRU is described as shown in Table 5 according to the mathematical operations (polynomial addition and convolution (conv.) multiplication). Therefore, for key generation, encryption, and decryption of QuiTRU is performed faster than QTRU and OTRU, and slower than NTRU.

Table 5: Convolution multiplication and addition of QuiTRU, NTRU, QTRU, and OTRU

	QuiTRU	**NTRU**	**QTRU**	**OTRU**
Key Creation	10 conv. multiplications	one conv. multiplications	16 conv. multiplications	64 conv. multiplications
Encryption	five conv. multiplications, 10 polynomial addition	one conv. multiplications, one polynomial addition	16 conv. multiplications, four polynomial addition	64 conv. multiplications, eight polynomial addition
Decryption	20 conv. multiplications, 10 polynomial addition	two conv. multiplications, one polynomial addition	32 conv. multiplications, four polynomial addition	1024 conv. multiplications, eight polynomial addition

Table 6 compares the speed of QuiTRU, NTRU, QTRU, and OTRU based on Table 5, such that t is the time of convolution multiplication and $t_1$is the time of polynomial addition.

Table 6: Speed of QuiTRU, NTRU, QTRU, and OTRU

	QuiTRU	**NTRU**	**QTRU**	**OTRU**
Speed	$35t+20t_1$	$4t+2t_1$	$64t+8t_1$	$1152t+16t_1$

So, QuiTRU has higher security than NTRU, QTRU, and OTRU, but NTRU is faster.

6 Conclusion

We presented here a multi-dimensional analog of NTRU, called QuiTRU. It is based on newly generated HH-Real algebra. This system enjoys a very high security level compared to the three systems NTRU, QTRU, and OTRU. Also, QuiTRU can encrypt five messages in parallel. These messages may be created from a single source or several sources, because of HH-Real algebra has five dimensional . This feature may be important in some applications, for example, in electronic voting. The speed of QuiTRU is faster than QTRU and OTRU, and slower than NTRU.

Acknowledgement

Authors of this article wish to extend their cordial thanks to professor Nadia M. G. Al-Saidi, department of applied sciences University of Technology for her generous guidance in preparing this paper.

References

[1] J. Hoffstein, J. Pipher , J. Silverman, NTRU: a ring based public key cryptosystem, Int. Algorithmic Number Theory Symp **1423**, 267-288 (1998).
[2] P. Gaborit, J. Ohler, P. Solé, CTRU, a polynomial analogue of NTRU (Doctoral dissertation, Inria), N 4621, inria-00071964ff (2002).
[3] M. Coglianese, B. Goi, MaTRU: A new NTRU based cryptosystem, Int. conf. on cryptology in India **3797**, 232-243 (2005).
[4] E. Malekian, A. Zakerolhsooeini, A. Mashatan, QTRU: quaternion version of the NTRU public-key cryptosystems, The ISC Int'l J. Information Security **3**, 29-42 (2011).
[5] E. Malekian, A. Zakerolhsooeini, OTRU: a non-associative and high speed public key cryptosystem, In 2010 15th CSI Int. Symp. On Computer Architecture and Digital Systems 83-90 (2010).
[6] K. Jarvis, NTRU over the Eisenstein Integers M. Sc (Doctoral dissertation, thesis University of Ottawa), 2011.
[7] K. Jarvis, M. Nevins, ETRU: NTRU over the Eisenstein integers, Designs Codes and Cryptography **74**,219-242 (2015).
[8] N M. AlSaidi, M. Said,A T. Sadiq, A A. Majeed A A. An improved NTRU cryptosystem via commutative quaternions algebra, Int. Conf. Security and Management SAM, 27 - 30 (2015).
[9] N M. Al-Saidi, H R. Yassein, A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure, Malaysian J. Mathematical Sci.**11**, 29-43 (2017).
[10] H R. Yassein, N M. Al-Saidi, HXDTRU cryptosystem based on hexadecnion algebra, Proc. 5th Int. Cryptology and Information Security Conf. **5**:1-14 (2016a).
[11] H. R. Yassein, N. M. Al-Saidi, BITRU: binary version of the NTRU public key cryptosystem via binary algebra, Int. J. Advanced Computer Sci. and Applications **7**,1-6 (2016b).

[12] H. R. Yassein, N. M. Al-Saidi, BCTRU: a new secure NTRUcrypt public key system based on a newly multidimensional algebra, proc. 6th Int. Cryptology and Information Security conf. **6**,1-11 (2018).
[13] H R. Yassein, N M. Al-Saidi, An innovative bi-cartesian algebra for designing of highly performed NTRU like cryptosystem, Malaysian J. Mathematical Sci. **13**, 77-91 (2019).
[14] R. E. Atani, S. E. Atani, A H. Karbasi, NETRU: a non-commutative and secure variant of CTRU cryptosystem, The ISC Int'l J. Information Security **10**, 45-53 (2018).
[15] H. R. Yassein, N. M. Al-Saidi, A. K. Jabber, A multi-dimensional algebra for designing an improved NTRU cryptosystem Eurasian, J. Mathematical and Computer Applications **8**, 97-107 (2020).
[16] H. R. Yassein, N. M. Al-Saidi, A. K. Farhan, A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure, J. Discrete Mathematical Sci. and Cryptography **23**, 1-20 (2020).
[17] H. R. Yassein , A. A. Abidalzahra, N. M. Al-Saidi, A new design of NTRU encryption with security and performance level, 4th Int. conf. Mathematical Sci. **2334**:080005-1-080005-4 (2021).

Hassan Rashed Yassein completed his doctorate in cryptography at the college of the science university of Baghdad, Iraq in 2017. His research interests include algebra, security, representation theory, cryptography, applied mathematics, fuzzy algebra, and abstract algebra. In 2017 he has been elected as Secretary of the Administrative Board of the Iraqi Mathematical Society. He supervised many postgraduate students, masters, and doctorates.

Hany Nasry Zaky was born in Giza, Egypt, on August 8. 1974. He received his B.Sc. degree in Electrical and Communications Engineering from Military Technical College, Cairo, Egypt in 1997. He received his M.Sc. degree in Clifford algebra and applied mathematics from Military Technical College, Cairo, Egypt in 2003. He received the Ph.D. degree in Mechatronics and Teleoperation of unmanned vehicles from Beijing Institute of Technology, Beijing, China in 2013. He has been the head of engineering mathematics department in Military Technical College since 2013 till 2017. He is the head of postgraduate expatriates in Military Technical College. Currently, He is a member of Liaison Technical Center for Research and Development.

Hadeel Hadi Abo-alsood completed the B.Sc. degree in mathematics from college of education for pure science Al-Muthanna University in 2018. She completed his master in cryptography at the college of education university of Al-Qadisiyah, Iraq in 2021. Her interests include algebra, security, and cryptography

Ismail A Mageed (FRSS, INTISCC, IAENG) completed his doctorate in Applied Probability at The University of Bradford, United Kingdom. His leading research on the relativisation of queuing theory and discovering the geodesic equation of motion for transient queues was greatly received by the world research community. Dr Mageed has published numerous papers in many highly reputable journals and IEEE conferences. He is also a reviewer and a co-editor to several prestigious journals. Dr Mageed has published a chapter in a book of the best eight queueing theorists in the world by ISTE WILLEY. He is currently leading several international research teams.

Wageda I. El Sobky was born in Egypt in 1981. She received the B.Sc. degree in communications and computers from Benha faculty of engineering in 2003. She received the B.Sc. degree in science from Benha faculty of science in 2008. She received the M.Sc. in applied mathematics from Benha University, Cairo, Egypt, in 2012 and the Ph.D. degree in cryptography from Ain Shams University, Cairo, Egypt, in 2017. She is currently a doctor in basic engineering sciences, at Benha Faculty of Engineering, Benha University, Egypt. Her current research interests include data security, and cryptography.