Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

QOC_{NTR}: Improved NTRU Public Key based on a New Algebraic Structure

Eqbal Naji Hameed [#1], Hassan Rashed Yassein[2]
[1]Department of Mathematics, College of Computer Sciences and Mathematics, University of Kufa, Al Najaf, 54001, Iraq
[2]Department of Mathematics, College of Education, University of Al-Qadisiyah, Al-Qadisiyah, 58002, Iraq
e-mail: iqbaln.alkerawi@uokufa.edu.iq[1]
hassan.yaseen@qu.edu.iq[2]

Article Info
Page Number: 5627-5633
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 March 2022
Revised: 30 April 2022
Accepted: 15 June 2022
Publication: 19 August 2022

Abstract
This study proposes QOC_{NTR}, a new multidimensional public key cryptosystem based on q-octonion algebra that improves security through a multidimensional approach. The proposed cryptosystem features two public keys, which distinguishes it from previous cryptosystems. This cryptosystem can encrypt thirty-two messages simultaneously from thirty-two different or independent sources, which is useful in certain applications. QOC_{NTR} was shown to outperform NTRU, QTRU, and OTRU in terms of security. Finally, because the suggested system has a very high level of security, the results are considered extremely suitable.

Keywords: - NTRU; QTRU; OTRU; QOC_{NTR}.

Introduction

The objective of cryptography is to keep information private when it is shared in a hostile environment. As a result, the proper implementation of standard, high-quality cryptography enables users to access safe apps while protecting the security of both systems of information and the data they handle. Because they provide outstanding security in a new era of network security, the creation of cryptographic systems that offer high-security levels has gained favor. For example, Rivest et al. [1] described RSA in 1978 based on the integer factorization problem. T. ElGamal [2] proposed an El Gamal cryptosystem in 1985 based on Diffie–Hellman key exchange [3]. R. Schoof [4] introduced ECC in 1987 based on the elliptic curve discrete logarithm problem. Hoffstein et al. [5] established NTRU in 1996 based on a truncated polynomial ring. NTRU's advantages make it a suitable option for various applications that encourage researchers to improve it. Meanwhile, many researchers have improved the NTRU system both in terms of algebraic and mathematical structures. For example, in 2002, Gaborit et al. [6] presented CTRU by using the ring of polynomials over the binary field F_2. Coglianese and Goi [7] presented MaTRU, an analog of NTRU that operates in the ring of polynomial matrices $Z[x]/(x^N - 1)$.
Malekian et al. [8] in 2008 improved NTRU by using quaternion algebra to replace the ring of a truncated polynomial. OTRU is also a novel NTRU cryptosystem that uses octonion

algebra, which was created by Malekian et al. [9]. Jarvis introduced a novel cryptosystem similar to NTRU in 2011, using Eisenstein integers, known as ETRU [10]. Al-Saidi et al. [11] proposed CQTRU, a multidimensional public key cryptosystem variation based on a commutative quaternion, in 2015. Using binary, hexadecnion, bi-cartesian, carternion, quaternion, bi-octonion, tripternion and Qu-octonion, and algebra to improve NTRU, which are referred to as BITRU, HXDTRU, BCTRU, QOBTRU, QMNTR, BOTRU, NTRS, NTRsh, and QOTRU, respectively [12-23].

This paper proposes a novel NTRU cryptosystem, which is built in a distinct way of increasing the security of the keys and was named QOC_{NTR}. It has been demonstrated that it is a more secure cryptosystem than the other three (NTRU, QTRU, and OTRU).

Q-octonion Algebra

A novel multidimensional associative and commutative algebra, over an arbitrary field F with char(F) $\neq 2$, which is called q-octonion algebra denoted by QOc, is provided in this section. Consider the four-dimensional vector space over an arbitrary field F which is defined as follows:

QOc = { $\mathrm{Ą} : \mathrm{Ą} = a + bi + cj + dk; a, b, c, d \in$ octonion algebra}, with the basis $\{1, i, j, k\}$. Assume that $A, B \in$ QOc, such that: $A = a + bi + cj + dk$, $B = \tilde{a} + \eth i + c'j + d_{\circ}k$ where $a, b, c, d, \tilde{a}, \eth, c', d_{\circ} \in$ octonion algebra,

$a = a_0 + \sum_{n=1}^{7} a_n e_n$, $b = b_0 + \sum_{n=1}^{7} b_n e_n$, $c = c_0 + \sum_{n=1}^{7} c_n e_n$, $d = d_o + \sum_{n=1}^{7} d_n e_n$, $\tilde{a} = \tilde{a}_0 + \sum_{n=1}^{7} \tilde{a}_n e_n$, $\eth = \eth_0 + \sum_{n=1}^{7} \eth_n e_n$, $c' = c'_0 + \sum_{n=1}^{7} c'_n e_n$, and $d_{\circ} = d_{\circ 0} + \sum_{n=1}^{7} d_{\circ n} e_n$, $a_n, b_n, c_n, d_n, \tilde{a}_n, \eth_n, c'_n, d_{\circ n} \in F$, $n = 0, 1, \ldots, 7$.

The addition +, multiplication $*$, scalar multiplication μ, identity I, and the inverse of any non-zero element are defined by:

$A+B = ((a_0+\tilde{a}_0)+\sum_{n=1}^{7}(a_n+\tilde{a}_n)e_n) + ((b_0+\eth_0) + \sum_{n=1}^{7}(b_n+\eth_n) e_n)i + ((c_0+c'_0) + \sum_{n=1}^{7}(c_n+c'_n) e_n)j + ((d_0+d_{\circ 0})+\sum_{n=1}^{7}(d_n+d_{\circ n}) e_n)k$

$A * B = ((a_0\tilde{a}_0)+\sum_{n=1}^{7}(a_n\tilde{a}_n) e_n) + ((b_0\eth_0)+\sum_{n=1}^{7}(b_n\eth_n) e_n)i + ((c_0c'_0)+\sum_{n=1}^{7}(cc'_n) e_n)j + ((d_0d_{\circ 0})+\sum_{n=1}^{7}(d_nd_{\circ n}) e_n)k$

$\mu A = \mu a + \mu bi + \mu cj + \mu dk; \ \mu \in F$

$I = (1+\sum_{n=1}^{7} e_n) + (1+\sum_{n=1}^{7} e_n)i + (1+\sum_{n=1}^{7} e_n)j + (1+\sum_{n=1}^{7} e_n))k$

$A^{-1} = (a_0^{-1}+\sum_{n=1}^{7} a_n^{-1} e_n) + (b_0^{-1}+\sum_{n=1}^{7} b_n^{-1} e_n)i + (c_0^{-1}+\sum_{n=1}^{7} c_n^{-1} e_n)j + (d_0^{-1}+\sum_{n=1}^{7} d_n^{-1} e_n)k; \ a_n, b_n, c_n, d_n \neq 0.$

Note that q-octonion is associative and commutative algebra.

Suppose that: $A = Z[x]/(x^N-1)$, $A_p = (Z/pZ)[x]/(x^N-1)$, and $A_q = (Z/qZ)[x]/(x^N-1)$ are rings of truncated polynomials, where N is a prime number, p and q are relatively prime

numbers. Now, we define the following q-octonion algebra $\mathfrak{Q}$, $\mathfrak{Q}_p$ and $\mathfrak{Q}_q$ over the rings of truncated polynomials A, A_p, A_q as follows:

$\mathfrak{Q}$= $\{(f_0+ \sum_{n=1}^{7} f_n e_n)+ (g_0+ \sum_{n=1}^{7} g_n e_n)i + (w_0+\sum_{n=1}^{7} w_n e_n)j + (v_0+ \sum_{n=1}^{7} v_n e_n)k ; f_n, g_n, w_n, v_n \in A\}$.

$\mathfrak{Q}_p$=$\{(f_0+ \sum_{n=1}^{7} f_n e_n)+ (g_0+ \sum_{n=1}^{7} g_n e_n)i + (w_0+\sum_{n=1}^{7} w_n e_n)j + (v_0+ \sum_{n=1}^{7} v_n e_n)k ; f_n, g_n, w_n, v_n \in A_p\}$.

$\mathfrak{Q}_q$=$\{(f_0+ \sum_{n=1}^{7} f_n e_n)+ (g_0+ \sum_{n=1}^{7} g_n e_n)i + (w_0+\sum_{n=1}^{7} w_n e_n)j + (v_0+ \sum_{n=1}^{7} v_n e_n)k ; f_n, g_n, w_n, v_n \in A_q\}$.

All operations on algebra $\mathfrak{Q}$, $\mathfrak{Q}_p$, and $\mathfrak{Q}_q$ are the same above.

Proposed Scheme: QOC_{NTR} crypto system

QOC_{NTR} cryptosystem depends on the same parameters in NTRU(N, p, q) and five subsets L_F, $L_U, L_G, L_\Phi, L_M \subset \mathfrak{Q}$, which are defined below:

Let $d_\alpha, d_\beta, d_\gamma$ and d_δ be constants less than N

L_F ={F∈$\mathfrak{Q}$ \ F has d_α coefficients equal to 1, $(d_\alpha - 1)$ equal to -1 such that α is octonion elements, the rest 0}

L_U={U ∈ $\mathfrak{Q}$ \ Uhas d_β coefficients equal to1coefficients equal to 1, $(d_\beta - 1)$ equal to-1 such that β is octonion elements, the rest 0}

L_G={ G ∈ $\mathfrak{Q}$ \ G hasd$_\gamma$ coefficients equal to 1, d_γ equal to – 1 such that γ is octonion elements, the rest 0},

L_Φ={ Φ∈ $\mathfrak{Q}$ \ Φ hasd$_\delta$ coefficients equal to 1, d_δ equal to-1 such that δ is octonion elements, the rest 0}, and

L_M= {M ∈ $\mathfrak{Q}$ \ coefficients of octonion elements of M are chosen between $-p/2$ and$p/2$}.

The following is a description of how QOC_{NTR} works:

1) **Key-generation:** In the first step, the recipient chooses three polynomials F ∈ L_F, U and G ∈ L_G that F and U are invertible in both $\mathfrak{Q}_q$ and $\mathfrak{Q}_p$ respectively. Assume F_q and U_p denote the inverses of F and U respectively meaning that:

$F * F_q \equiv I \bmod q$, $U_p * U \equiv I \bmod p$.
The recipient applies the following two formulas to get the public keys:

$\mathbf{H} = F_q * G \pmod q$, $\mathbf{K} = F_q * U \pmod q$

Here, the polynomials F and U will be saved as secret keys.

2) **Encryption:** The encryption procedure begins from the sender in which the first step is to choose a random polynomial Φ that belongs to the set L_{Φ}.

The second step is to express the secret message M in the form of a polynomial that belongs to L_M.

Finally, to obtain ciphertext, use the formula as follows:

$$E = (pH * \Phi + K * M) \bmod q$$

3) **Decryption:** The following steps were taken to retrieve the original message from the ciphertext:

- Multiply E by the secret key F

$$A = F * E \,(\text{mod } q) = F * (pH * \Phi + K * M)(\text{mod } q)$$

$$= p(F * H * \Phi) + F * K * M(\text{mod } q) = p(F * F_q * G * \Phi) + F * F_q * U * M(\text{mod } q)$$

$$= p(G * \Phi) + U * M(\text{mod } q)$$

- Reduce the coefficient of modulo p. Hence, the term $p(G * \Phi)$ vanishes and $U * M(\text{mod } p)$ remains.

- To extract the message M multiply $U * M(\text{mod } p)$ by U_p from left.

Results and Discussion

This section discusses the advantages of the proposed cryptosystem in terms of its high level of security for both the message and the keys, as shown in the tables below, with the same parameters. In addition, through the mathematical structure, which is used, it was found that the cryptosystem can encrypt thirty-two messages from one source or independent sources. Comparatively, the NTRU cryptosystem can encrypt only one message, QTRU can encrypt four messages, and OTRU can encrypt eight messages. Furthermore, the speed of the proposed system is compared with the other cryptosystems.

A. Security of QOC_{NTR} and Some NTRU-like

Table I compares the key space and message space security levels of the QOC_{NTR} and other cryptosystems, as well as some NTRU-like according to some public parameters.

TABLE I: COMPARISON OF KEY AND MESSAGE SECURITY LEVELS BETWEEN QOC_{NTR} AND SOME NTRU-LIKE

Title	**NTRU**	**QTRU**	**OTRU**	**QOC_{NTR}**	
Key space	$\frac{N!}{(d_g!)^2(N-d_g)!}$	$\left(\frac{N!}{(d_g!)^2(N-d_g)!}\right.$	$\left(\frac{N!}{(d_g!)^2(N-d_g)!}\right.$	$\left(\frac{N!}{(d_g!)^2(N-d_g)!}\right)^{32}$	$\left(\frac{N!}{(d_u!)^2(N-d_u)!}\right.$
Message	$\left(\frac{N!}{(d_\Phi!)^2(N-d_\Phi}\right.$	$\left(\frac{N!}{(d_\Phi!)^2(N-d_\Phi)!}\right.$	$\left(\frac{N!}{(d_\Phi!)^2(N-d_\Phi)}\right.$	$\left(\frac{N!}{(d_\Phi!)^2(N-d_\Phi)!}\right)^{32}$	

space

B. Speed of QOC_{NTR} and Some NTRU-like

The speed is determined by the mathematical operations of key generation, encryption, and decryption. Table II shows a comparison of speed between QOC_{NTR}, NTRU, QTRU, and OTRU cryptosystems

TABLE II: COMPARISON of SPEED BETWEEN QOCNTR and SOME NTRU-LIKE

Cryptosystem	NTRU	QTRU	OTRU	QOC_{NTR}
Speed	$4t + 2t`$	$64t + 8t`$	$1152t + 16t`$	$192t + 64t`$

Where t is the time of convolution multiplication while t` is the time of polynomial addition

Conclusion

QOC_{NTR}, a new multi-dimensional public key cryptosystem based on newly developed q-octonion algebra to improve security is presented in this study. Because this system is multi-dimensional, it may encrypt 32 messages from 32 distinct or independent sources at the same time, which is useful in some applications. When QOC_{NTR} is compared to the NTRU, QTRU, and OTRU cryptosystems, the QOC_{NTR} system is shown to have a high level of security. QOC_{NTR} is slower than NTRU and QTRU (the effect of this problem can be reduced by decreasing the value N). However, with the same parameters, it is faster than OTRU.

References

1. R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signature and public key cryptosystems”, Communications of the ACM, vol. 21, no.2, p.p.120-126, Feb.1978.
2. T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithm,” IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, Jul. 1985.
3. W. Diffie, M. Hellman, “New directions in cryptography”,IEEE Transactions on Information Theory, vol.22, no.6, p.p.644-654, Nov.1976.
4. R. Schoof“Elliptic curve over finite fields and the computation of square roots mod p,”Mathematics of computation, vol.44, no.170, pp. 483-494, Apr.1985.
5. J. Hoffstein, J. Pipher, and J. Silverman,“NTRU: A ring based public key cryptosystem,” in Proc. ANTS III, LNCS, Springer Verlag. 1998, pp. 267-288.
6. P. Gaborit J. Ohler, P. Soli, “CTRU, a polynomial Analogue of NTRU,”INRIA. Rapport de recherche, no. 4621, Nov.2002

7. M. Coglianese, and B. Goi, “MaTRU: A new NTRU based cryptosystem”, Springer Verlag Berlin Heidelberg, vol 3797 p.p. 232-243, Dec.2005.
8. 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, Jan. 2011.
9. E. Malecian, et al., “OTRU: A non-associative and high speed public key cryptosystem,” IEEE Computer Society, 2010, pp.83- 90.
10. K. Jarvis, “NTRU over the Eisenstein Integers,Master's Thesis, University of Ottawa, 2011.
11. N. M. G. AlSaidi, M. Said, A. T. Sadiq, and A.A. Majeed, “An improved NTRU cryptosystem via commutative quaternions algebra,”in Proc. Int. Conf. Security and Management SAM'15, Las Vegas, USA, 2015, pp. 198–203.
12. N. M. G. Al-Saidi and H. R. Yassein, “BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra,” International Journal of Advanced Computer Science and Applications, vol. 7, no. 11, pp. 1-6, 2016.
13. H. R. Yassein and N. M. G. Al-Saidi, “HXDTRU Cryptosystem Based on Hexadecnion Algebra,”in Proc. 6th International Cryptology and Information Security Conference,Sabah,Malaysia, 2016, pp. 1–10.
14. N. M. G. Al-Saidi and H. R. Yassein, “ A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure,” Malaysian Journal of Mathematical Sciences, vol. 11, no. S, pp. 29-43, Aug. 2017.
15. H. R. Yassein and N. M. Al-Saidi, “A comparative performance analysis of NTRU and its variant cryptosystems,” in Proc. (ICCIT), IEEE,Bangladesh,2017, pp. 115–120.
16. H. R. Yassein and N. M. G. Al-Saidi, “BCTRU: A New Secure NTRUCrypt Public Key System Based on a Newly multidimensional Algebra,” in Proc. the 6th International Cryptology and Information Security Conference,Negeri Sembilan, Malaysia, 2018, pp. 1–11.
17. H. R. Yassein and N. M. G. Al-Saidi, “An Innovative Bi-Cartesian Algebra for Designing of Highly Performed NTRU Like Cryptosystem,” Malaysian Journal of Mathematical Sciences, vol. 13, no. S, pp. 77-91, Aug. 2019.
18. H. R. Yassein, N. M. G. Al-Saidi. and A. K. Farhan, “A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure,” Journal of Discrete Mathematical Sciences & Cryptography, vol. 23, no. 2, pp. 1-20, May. 2020.
19. H. R. Yassein, A. A. Abidalzahra and N. M. G. Al-Saidi, “A New Design of NTRU Encryption with High Security and Performance Level,” in Proc. AIP Conf. Proc. Istanbul Turkey, 2021, pp. 080005- 1- 080005- 4.
20. H. H. Abo-Alsood and H. R. Yassein, “Design of an Alternative NTRU Encryption with High Secure and Efficient,” International Journal of Mathematics and Computer Science, vol. 16, no. 4, pp. 1469-1477, Apr. 2021.
21. S. H. Shahhadi, and 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, vol. 16, no. 4, pp. 1515-1522, 2021.

22. S. H. shahhadi and H. R. Yassein, “NTRsh: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra,” Journal of Physics: Conference Series, , vol.1999, pp. 1-6, 2021.
23. H. H. Abo-Alsood and H. R. Yassein, “QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra,” Journal of Physics: Conference Series, vol. 1999, pp. 1-7, 2021.