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

QTNTR: A New Secure NTRUEncrypt Alternative with a High Level of Security

Huda Abdulateef Ali [#1], Hassan Rashed Yassein[2]
[1]Department of Mathematics, Faculty of Education for Girls, University of Kufa, Al Najaf, Iraq
[2]Department of Mathematics, College of Education, University of Al-Qadisiyah, Al-Qadisiyah, Iraq
e-mail: hudaalrobayee75@gmail.com[1]
hassan.yaseen@qu.edu.iq[2]

Article Info
Page Number: 5634-5639
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
Due to its efficiency in resisting attacks, the encryption algorithm, NTRUEncrypt has received a lot of attention. Many researchers have improved the performance of the NTRU cryptosystem. This paper introduces QTNTR, a commutative and associative multidimensional public-key cryptosystem. It is built on quintuple algebra, with one public key and two private keys as the mathematical structure. Also, it has a good resistance against attacks, and its performance is significantly different from that of conventional public-key cryptosystems.

Keywords: NTRU, BCTRU, QOB_{TRU}, QTNTR, and Quintuple algebra

1. Introduction

Public-key cryptography is built on one-way functions that are easy to compute but difficult to invert [1]. Diffie and Hellman [2] invented public-key cryptosystems in 1976, including the Diffie-Hellman key exchange protocol, which is based on a discrete logarithm problem. In 1978, Rivest et al. [3] introduced the RSA cryptosystem, which is built on factoring large integers into prime factors. El Gamal [4] introduced the El Gamal cryptosystem in 1985, which is predicated on a discrete logarithm. In 1985, Koblitz [5] and Miller [6] proposed the Elliptic Curves Cryptosystem (ECC), a discrete logarithm problem defined by points on an elliptic curve over a finite field, which arises from the elliptic curve logarithm. Hoffstein et al. [7] introduced NRTU, the first public-key cryptosystem that does not rely on factorization or discrete log issues. It is built on a ring of truncated polynomials of degree $N-1$ with integer coefficients $(Z[X]) / (X^N - 1)$ over finite fields.

Several researchers have attempted to improve the NTRU cryptosystem by employing a new ring and a more efficient linear transformation. CTRU, for example, was developed by Gaborit et al. in 2002 and is centered on the ring of polynomials in one variable over a finite field [8]. In 2005, a new cryptosystem called MaTRU was presented by Coglianese and Goi, which depends on the ring $k \times k$ matrices of polynomials of order n [9]. Malekian et al. proposed the QTRU cryptosystem in 2009, which is founded on non-commutative and associative quaternion algebra [10]. Malekian et al. [11] presented OTRU, an octonion algebra-based cryptosystem, in 2010. In 2011, K. Jarvis [12] proposed ETRU, a novel

cryptosystem centered on the Eisenstein integer ring. Majeed et al. [13] presented a novel multidimensional system termed CQTRU in 2015, which is analogous to NTRU in terms of the commutative quaternion. Yassein and AlSaidi [14-16] proposed the HXDTRU and BITRU cryptosystems in 2016, based on their hexadecenoic and binary algebra, respectively. Yassein and Al-Saidi proposed BCTRU, a novel NTRU-like cryptosystem based on bi-cartesian algebra, in 2018 [17,18]. After that, Yassein et al. introduced many improvements to the NTRU, which proved its efficiency in terms of security and speed [19-27].

2. Quintuple algebra

A new algebra was introduced in this section, which is a five-dimensional vector space over the real number set R, which has the following definition:

$QU = \{(a_1, b_1)(1,1) + (a_2, b_2)(1, i) + (a_3, b_3)(1, j) + (a_4, b_4)(1, k) + (a_5, b_5)(1, h) | a_i, b_i, i = 1,2,3,4,5\}$, where $\{(1,1), (1, i), (1, j), (1, k), (1, h)\}$, forms the basis of this algebra.

Let $x, y \in QU$, such that $x = (a_1, b_1)(1,1) + (a_2, b_2)(1, i) + (a_3, b_3)(1, j) + (a_4, b_4)(1, k) + (a_5, b_5)(1, h)$, and

$$y = (c_1, d_1)(1,1) + (c_2, d_2)(1, i) + (c_3, d_3)(1, j) + (c_4, d_4)(1, k) + (c_5, d_5)(1, h)$$

The addition to this algebra is defined by:

$$x + y = (a_1 + c_1, b_1 + d_1)(1,1) + (a_2 + c_2, b_2 + d_2)(1, i) + (a_3 + c_3, b_3 + d_3)(1, j) + (a_4 + c_4, b_4 + d_4)(1, k) + (a_5 c_5 +, b_5 + d_5)(1, h).$$

The multiplication of x and y is then defined by:

$$x * y = (a_1 c_1, b_1 d_1)(1,1) + (a_2 c_2, b_2 d_2)(1, i) + (a_3 c_3, b_3 d_3)(1, j) + (a_4 c_4, b_4 d_4)(1, k) + (a_5 c_5, b_5 d_5)(1, h)$$

This multiplication is both associative and commutative.

The most important operation in any designed algebraic structure is finding the inverse of the elements, as a result, for the quintuple elements, the inverse is determined as follows:

$qu^{-1} = (s_1, t_1)(1,1) + (s_2, t_2)(1, i) + (s_3, t_3)(1, j) + (s_4, t_4)(1, k) + (s_5, t_5)(1, h)$, where, $s_i = \frac{1}{c_i}$, $t_i = \frac{1}{d_i}$

The identity of quintuple elements is defined as follows:

$$qu_{identity} = (1,1)(1,1) + (1,1)(1, i) + (1,1)(1, j) + (1,1)(1, k) + (1,1)(1, h)$$

Assume that F be an arbitrary field with $\text{char}(F) \neq 2$. The quintuple algebra $\mathbb{Q}$ over F is defined as follows:

$\mathbb{Q} = \{(\tau_0, \tau_1)(1,1) + (\tau_2, \tau_3)(1, i) + (\tau_4, \tau_5)(1, j) + (\tau_6, \tau_7) + (\tau_8, \tau_9)(1, h) | \tau_0, \tau_1, \tau_2, \tau_3, \tau_4, \tau_5 \in F\}$, with the same operations defined in QU.

If we have three convolutions polynomial rings $\delta = Z[x]/(x^N - 1)$, $\delta_P = Z[x] / (x^N - 1)$, $\delta_q = Z[x] / (x^N - 1)$, we can define three quintuple algebras:

$$\varphi = \{(\tau_0, \tau_1)(1,1) + (\tau_2, \tau_3)(1, i) + (\tau_4, \tau_5)(1, j) + (\tau_6, \tau_7)(1, k) + (\tau_8, \tau_9)(1, h) | \tau_i \in \delta, i = 1,2, \dots .9\}$$

$$\varphi_p = \{(\tau_0, \tau_1)(1,1) + (\tau_2, \tau_3)(1, i) + (\tau_4, \tau_5)(1, j) + (\tau_6, \tau_7)(1, k) + (\tau_8, \tau_9)(1, h) | \tau_i \in \delta_P , i = 1,2, \dots .9 \}$$

$$\varphi_q = \{(\tau_0, \tau_1)(1,1) + (\tau_2, \tau_3)(1, i) + (\tau_4, \tau_5)(1, j) + (\tau_6, \tau_7)(1, k) + (\tau_8, \tau_9)(1, h) | \tau_i \in \delta_q, i = 1,2, \dots .9 \}$$

The elements of this new algebra are utilized to build the QUATRU cryptosystem, which is explained, using these mathematical definitions.

3. QTNTR Cryptosystem Proposal

The QTNTR cryptosystem variables are the integers N, p, and q as defined in NTRU, with the subsets $\mathcal{L}_F, \mathcal{L}_M, \mathcal{L}_G$ and $\mathcal{L}_V \subset \mathbb{Q}$ as shown in Table 1.

Table 1: The subsets of Quintuple algebra

Symbol of subsets	Definition
$\mathcal{L}_F$	$\{(f_0, f_1)(1,1) + (f_2, f_3)(1, i) + (f_4, f_5)(1, j) + (f_6 , f_7)(1, k) + (f_8 , f_9)(1, h) \mid f_i \in \delta, i = 1,2, \dots ,9$ has d_f coefficients of 1, and $d_f - 1$ of -1, and the rest are $0\}$
$\mathcal{L}_M$	$\{(m_0, m_1)(1,1) + (m_2, m_3)(1, i) + (m_4, m_5)(1, j) + (m_6 , m_7)(1, k) + (m_8 , m_9)(1, h) \mid f_i \in \delta, i = 1,2, \dots ,9$ has m_i coefficients are chosen modulo p between $p/2$ and $-p/2\}$

$\mathcal{L}_G$ and $\mathcal{L}_V$ have the same definition $\mathcal{L}_F$ except has $d_g - 1$ coefficients of -1. $d_v - 1$ coefficients of -1, respectively. d_g and d_v are constant variables similar to those defined in NTRU. The QTNTR cryptosystem consists of three stages

I. Generation of Key

Two polynomials, F and G, were chosen at random to create the public and private keys, such that $F \in \mathcal{L}_F$ and $G \in \mathcal{L}_G$, and F must have multiplicative inverse modulo p and q. The following is how the public keys are generated:

$$\mathcal{H} = F_q * G (\mathrm{mod}\ q).$$

The private key is $\{F, G\}$.

II. Encryption

To convert the message $M \in \mathcal{L}_M$ to ciphertext E, choose blinding polynomial $V \in \mathcal{L}_V$ and computes E by the law:

$$E = pV * \mathcal{H} + M (\mathrm{mod}\ q).$$

III. Decryption

The receiver decrypts the ciphertext using the following procedure after receiving E:

$$D = F * E(mod\ q)$$

$$= F * (pV * \mathcal{H} + M)(mod\ q)$$

$$= p\ G * V + F * M(mod\ q)$$

Let $W = D(mod\ p) = F * M(mod\ p)$

$$F_p * W = F_p\ * F * M(mod\ p) = M(mod\ p).$$

4. Comparison of some NTRU improvements

In this section, some of the NTRU improvements were compared. This comparison is about the space security of a key, space security of a message, and speed. The key space and message space of NTRU, BCTRU, QOB_{TRU}, and QTNTR as shown in Table 2.

Table 2: Message space and key space of NTRU, BCTRU, QOB_{TRU}, and QNTRU

	Key space	Message space
NTRU	$\left(\frac{N!}{(dg!)^2(N-2dg)!}\right)$	$\left(\frac{N!}{(dr!)^2(N-2dr)!}\right)$
BCTRU	$\left(\frac{N!}{(d_t!)^2(N-2d_t)!}\right)^4\left(\frac{N!}{(d_v!)^2(N-2d_v)!}\right)^4$	$\left(\frac{N!}{(d_\emptyset!)^2(N-2d_\emptyset)!}\right)^4$
QOB_{TRU}	$\left(\frac{N!}{(d_t!)^2(N-2d_t)!}\right)^8\left(\frac{N!}{(d_v!)^2(N-2d_v)!}\right)^8$	$\left(\frac{N!}{(d_\emptyset!)^2(N-2d_\emptyset)!}\right)^8$
QTNTR	$\left(\frac{N!}{(d_g!)^2(N-2d_g)!}\right)^{10}$	$\left(\frac{N!}{(d_v!)^2(N-2d_v)!}\right)^{10}$

The speed of the NTRU, BCTRU, QOB_{TRU}, and QNTRU cryptosystems is compared in this section based on mathematical operations (polynomial addition and convolution multiplication) in key generation, encryption, and decryption phases. The speed of NTRU and its Improvements showed in Table 3, such that t is the time of convolution multiplication and t_1 the time of polynomial addition.

Table 3: Speed of NTRU and some of its improvements

Title	NTRU	BCTRU	QOB_{TRU}	QTNTR
Speed	$4\ t\ +\ 2\ t_1$	$64t + 20\ t_1$	$384t\ +\ 16\ t_1$	$40t\ +\ 20t_1$

The time of key generation, encryption, and Decryption of QTNTR is faster than BCTRU, QOB_{TRU} but is slower than NTRU**.**

5. Conclusion

The QTNTR cryptosystem is predicated on commutative and associative quintuple algebra. In comparison to BCTRU and QOBTRU, the QTNTR multi-dimensional cryptosystem with great security and speed was introduced. As a result, QTNTR will have a much higher level of security than the original NTRU. In addition, the QTNTR cryptosystem can encrypt ten messages of length N in each round, which gives it a good advantage in many applications such as election commission and communications.

References

1. Q. M. Hussein, "Recover the Private Keys of NTRU Cryptosystem from Known Public Information and Public Key", Ph.D. thesis, University of Technology, 2009.
2. W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory IT-22, pp. 644-654, 1976.
3. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Commune. ACM 21, pp.120-126, 1978.
4. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE transactions on information theory, 31(4): 469–472, 1985.
5. N. Koblitz, "Elliptic curve cryptosystems, Mathematics of Computation", 48, pp. 203- 209, 1987.
6. V. Miller, "Uses of elliptic curves in cryptography, Advances in Cryptology"- CRYPTO '85, Lecture Notes in Computer Science, 218, pp. 417-426, 1986.
7. J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem", in Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, Proceedings, pp.267-288, 1998.
8. P. Gaborit, J. Ohler and P. Soli, "CTRU, a polynomial analogue of NTRU", INRIA. Rapport de recherche, N. 4621, 2002.
9. M. Coglianese and B. Goi, "MaTRU: A new NTRU based cryptosystem", Int. conf. on cryptology in India (LNCS vol 3797) ed S Maitra et al (Dalian: Springer) pp. 232-243, 2005.
10. E. Malecian, A. Zakerolhsooeini, and A. Mashatan, "QTRU: a lattice attack resistant version of NTRU PCKS based on quaternion algebra", The ISC Int'l Journal of Information Security, vol. 3, no. 1, (pp. 29–42), 2011.
11. E. Malecian and A. Zakerolhsooeini, "OTRU: A non-associative and high speed public key cryptosystem", Proceeding of the 15th CSI International Symposium Computer Architecture and Digital Systems, Iran, 23-24 September, IEEE xplore, pp. 83-90, 2010.
12. K. Jarvis, "NTRU over the Eisenstein Integers", M. Sc. Thesis, University of Ottawa, 2011.
13. N. M. G. AlSaidi, M. Said, A. T. Sadiq, and A.A. Majeed, An improved NTRU cryptosystem via commutative quaternions algebra, Proceeding of Int. Conf. Security and Management SAM'15, (2015), pp.198-203.

14. H. R. Yassein and N. M. AlSaidi, "HXDTRU Cryptosystem Based On Hexadecnion Algebra", 5th International Cryptology and Information Security Conference, 2016.
15. H. R. Yassein and N. M. AlSaidi, "BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra", International Journal of Advanced Computer Science and Application, vol. 7, no. 11, pp. 1-6, 2016.
16. H. R. Yassein, and N. M. AlSaidi, "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, 2017.
17. H. R. Yassein and N. M Al-Saidi, "BCTRU: a new secure NTRUcrypt public key system based on a newly multidimensional algebra", 6th Int. Cryptology and Information Security conf. vol 6, pp 1-11, 2018.
18. H. R. Yassein and N. M. Al-Saidi, "An innovative bi-cartesian algebra for designing of highly performed NTRU like cryptosystem", Malaysian J. Mathematical Sci. 13, pp. 77-91, 2019.
19. H. R. Yassein, N. M. Al-Saidi, and 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.
20. H. R. Yassein, N. M. Al-Saidi and A. K. Jabber, "A multi-dimensional algebra for designing an improved NTRU cryptosystem", Eurasian J. Mathematical and Computer Applications 8 97-107, 2020.
21. H. R. Yassein, A. A. Abidalzahra, and N. M. Al-Saidi," A new design of NTRU encryption with security and performance level", 4th Int. conf. Mathematical Sci. (ICMS 2020) vol 2334 (Istanbul) pp. 080005- 1-080005-4, 2021.
22. S. H. Shihadi, 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.
23. 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, 2021.
24. 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, 2021, pp. 1-6.
25. 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, 2021, pp. 1-7.
26. S. H. Shihadi, H. R. Yassein, "An innovative tripternion algebra for designing NTRU-like cryptosystem with high security," AIP Conference Proceedings 2386, 060009 (2022).
27. H. H. Abo-alsood, H.R. Yassein, "Analogue to NTRU public key cryptosystem by multi-dimensional algebra with high security," AIP Conference Proceedings 2386, 060006 (2022).