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

(3s.) **v. 2025 (43)** : 1–7.
ISSN-0037-8712
doi:10.5269/bspm.66031

TrQtNTR: A New Algebra for Establishing Secure Public-Key NTRU

Hassan R. Yassein* and Sarah H. Shahhadi

ABSTRACT: NTRU has been proven computationally efficient and can be implemented at low cost. In addition, it does not depend on factorization integer problems or discrete logarithm problems, it depends on truncated polynomials ring. This paper presents the design of the TrQtNTR public key cryptosystem. It is based on qua-tripternion, a novel algebra with a distinctive mathematical structure. High security and efficiency are ensured by the new system, which is thought to be ideal for various applications.

Key Words: NTRU, QTRU, TrQtNTR, Qua-tripternion algebra.

Contents

1. Introduction

After the rapid development of the technology, encryption became the backbone that provides a safe environment for transferring information, maintaining its confidentiality, and not accessing it or changing it by persons who are not allowed to access or know it. Since this information is sent over the Internet. It makes it insecure and vulnerable to hackers. With the great development that cryptography is witnessing, its goal is one and constant, to preserve information and its confidentiality and achieve high security for this information. Hoffstein et al. [4] are founded a public key cryptosystem NTRU to be used for such purposes. It is based on the convolution polynomials ring of the degree $N-1$ denoted by $Z[x]/(x^N-1)$. Some researchers presented several studies on NTRU, which are summarized as follows.

* Corresponding author

Submitted November 27, 2022. Published July 04, 2023
2010 *Mathematics Subject Classification:* 94A60, 68P25.

Kouzmenko [8] designed a system GNTRU that depends on Gaussian integers. Also, by replacing the ring of polynomials with the ring of $k \times k$ matrices of polynomials, Coglianese and Goi [3] introduced the MaTRU cryptosystem. Nevins et al. [7] proposed a new variant, to NTRU by replacing the original NTRU ring with Einstein integers. Also, Malekian et al. [5] introduced a public key cryptosystem QTRU depends on the Quaternion. NTRU is less resistant to some attacks compared to QTRU. (Malekian et al. [6] proposed an alternative of NTRU which is called OTRU by replacing the origin ring of NTRU with octonion algebra. It encrypts eight data carriers per round and has a secure, and complex core. In 2016 [9,1,2] introduced HXDTRU and BITRU depend on the hexadecnion and binary algebras, respectively. Yassein and Al-Saidi et al. [11,13] introduced another multidimensional analog NTRU called BCTRU using bicartesian algebra. Yassein et al. [12] introduced the QOBTRU cryptosystem based on carternion algebra. Yassein et al. [10] introduced a new NTRU alternative cryptosystem called NTRTE that depends on a commutative quaternion algebra with a new structure, which is multi-dimensional. In this paper, a new encryption system was created based on qua-tripternion algebra, whose coefficients belong to quaternion algebra, two public keys and six private keys is used in this system which are characterized by a high security.

2. NTRU Cryptosystem

NTRU cryptosystem depends on a truncated polynomial ring of degree $N-1$ denoted by $K = Z[x]/(x^N-1)$, such that N is a prime number. The rings of truncated polynomial $mod\ p$ is denoted by $K_p = Z_p[x]/(x^N-1)$ and the rings of truncated polynomial $mod\ q$ is denoted by $K_q = Z_q[x]/(x^N-1)$, such that p, q are integers number and gcd $(p,q) = 1$, where p is smaller than q. The subset L_f, L_g, L_r, and L_m are defined as follow:

$L_f = \{f \in K : f \text{ satisfy } \ell_{(d_f, d_f-1)}\}$

$L_g = \{g \in K : g \text{ satisfy } \ell_{(d_g, d_g)}\}$

$L_r = \{r \in K : r \text{ satisfy } \ell_{(d_r, d_r)}\}$

$L_m = \{m \in K :$ coefficients of m are chosen $mod\ p$ between $-p/2$ and $p/2\}$ where $\ell_{(d_x,d_y)} = \{f \epsilon\ K \backslash f$ has d_x coefficients equal to 1, d_y coefficients equal to -1, the remaining are equal to $0\}$

The NTRU cryptosystem is passed three phases :

2.1. Key Generation

We randomly choose two polynomials f, g from L_f, L_g such that, f has an inverse concerning p and q. f_p^{-1} denotes the inverse of f concerning p and f_q^{-1} denotes the inverse of f concerning q such that, $f * f_p^{-1} = 1$, $f * f_q^{-1} = 1$, the public key is calculated by the law $h = f_q^{-1} * g(mod\ q)$.

2.2. Encryption

The message $m \in L_m$ is encryption after selecting of a random polynomial $r \in L_r$ and using the formula $e = ph * r + m(mod\ q)$.

2.3. Decryption

After receiving the encrypted text, the original plaintext is obtained through steps $f * e\,(mod\ q) = (pf * h * r + f * m)\,(mod\ q)$.

$$\begin{aligned} \text{Take } z &= f * e\ (mod\ p) \\ &= pg * r + f * m\ (mod\ p) \\ &= f * m\ (mod\ p) \end{aligned}$$

$f_p^{-1} * z = m(mod\ p)$.

3. QTRU Cryptosystem

QTRU cryptosystem [5] is based on the quaternion algebra instead of $Z[x]/(x^N-1)$ that is used in the NTRU with the same parameters. Let θ be a field with $char(\theta\ ) \neq 2$, then the quaternion algebra H is defined over θ as follows:

$$H = \{\rho + \tau i + \sigma j + \mu k : \sigma, \tau, \rho, \mu \in \theta\}$$

with the basis $\{1, i, j, k\}$ such that, $i^2 = a$, $j^2 = b, ij = k = -ji$. The QTRU cryptosystem is passed through the following three phases:

3.1. Key Generation

The key is generated in the QTRU by selecting the two quaternion polynomials F and G such that, F has an inverse with respect to p and q and is calculated by the following formula

$$H = F_q^{-1} * G(mod\ q).$$

3.2. Encryption

The plaintext or the message M is encrypted by choosing the polynomial $r \in L_R$ and it is encrypted by the following law: $E = pH * R + M(mod\ q)$

3.3. Decryption

The encrypted text is decrypted as follows

$$\begin{aligned} F * E\,(mod\ q) &= F * pH * R + F * M(mod\ q) \\ &= pG * R + F * M(mod\ q) \\ F * E(mod\ p) &= F * M(mod\ p) \\ \text{Take } B &= F * M(mod\ p) \\ F_p^{-1} * B &= M(mod\ p). \end{aligned}$$

4. QUA-TRIPTERNION Algebra

In this section we introduce a new multidimensional algebra over the field θ which called qui-tripternion algebra QT describes as follows:

$QT = \{a + bx + cx^2 : a, b, c \in$ quaternion algebra$\}$ such that
$a = \sigma_1 + \mu_1 i + \delta_1 j + \tau_1 k$
$b = \sigma_2 + \mu_2 i + \delta_2 j + \tau_2 k$
$c = \sigma_3 + \mu_3 i + \delta_3 j + \tau_3 k.$

Let $A, B \in QT$, then
$A = (\sigma_1 + \mu_1 i + \delta_1 j + \tau_1 k) + (\sigma_2 + \mu_2 i + \delta_2 j + \tau_2 k)x + (\sigma_3 + \mu_3 i + \delta_3 j + \tau_3 k)x^2$
$B = (\sigma_4 + \mu_4 i + \delta_4 j + \tau_4 k) + (\sigma_5 + \mu_5 i + \delta_5 j + \tau_5 k)x + (\sigma_6 + \mu_6 i + \delta_6 j + \tau_6 k)x^2$. The addition, multiplication of two qui-tripternions, scalar multiplication and inverse multiplication are defined by:

$$\begin{aligned} A + B =& ((\sigma_1 + \sigma_4) + (\mu_1 + \mu_4)i + (\delta_1 + \delta_4)j + (\tau_1 + \tau_4)k) + ((\sigma_2 + \sigma_5) + (\mu_2 + \mu_5)\,i \\ &+ (\delta_2 + \delta_5)j + (\tau_2 + \tau_5)k)x + ((\sigma_3 + \sigma_6) + (\mu_3 + \mu_6)i + (\delta_3 + \delta_6)j + (\tau_3 + \tau_6)k)x^2 \end{aligned}$$

$$\begin{aligned} A * B =& ((\sigma_1\sigma_4) + (\mu_1\mu_4)i + (\delta_1\delta_4)j + (\tau_1\tau_4)k) + ((\ \sigma_2\sigma_5) + (\mu_2\mu_5)\,i + (\delta_2\delta_5)\,j \\ &+ (\tau_2\tau_5)k)x + ((\sigma_3\sigma_6) + (\mu_3\mu_6)i + (\delta_3\delta_6)j + (\tau_3\tau_6)k)x^2 \end{aligned}$$

$$\begin{aligned} \rho A &= \rho(\sigma_1 + \mu_1 i + \delta_1 j + \tau_1 k) + \rho(\sigma_2 + \mu_2 i + \delta_2 j + \tau_2 k)x + \rho(\sigma_3 + \mu_3 i + \delta_3 j + \tau_3 k)x^2 \\ &= (\rho + \rho\mu_1 i + \rho\delta_1 j + \rho\tau_1 k) + (\rho\ \sigma_2 + \rho\mu_2 i + \rho\delta_2 j + \rho\tau_2 k)x + (\rho\sigma_3 + \rho\mu_3 i + \rho\delta_3 j + \rho\tau_3 k)x^2 \end{aligned}$$

$$A^{-1} = \left(\frac{1}{\sigma_1} + \frac{1}{\mu_1}i + \frac{1}{\delta_1}j + \frac{1}{\tau_1}k\right) + \left(\frac{1}{\sigma_2} + \frac{1}{\mu_2}i + \frac{1}{\delta_2}j + \frac{1}{\tau_2}k\right)x + \left(\frac{1}{\sigma_3} + \frac{1}{\mu_3}i + \frac{1}{\delta_3}j + \frac{1}{\tau_3}k\right)x^2,$$
$$\sigma_\gamma, \delta_\gamma, \tau_\gamma \neq 0, \forall\gamma = 1, 2, 3$$

where the identity element in QT is given by $(1 + i + j + k) + (1 + i + j + k)x + (1 + i + j + k)x^2$. It is clear that the multiplication is associative.

5. TrQtNTR Cryptosystem

TrQtNTR cryptosystem depends on qua-tripternion algebra. The rings of truncated polynomial is denoted by $A = Z[x]/(x^N - 1)$ the rings of truncated polynomial *mod* p is denoted by $A_p = Z_p[x]/(x^N - 1)$ and the rings of truncated polynomial *mod* q is denoted by $A_q = Z_q[x]/(x^N - 1)$, such that p, q are integers number and $\gcd(p, q) = 1$, where p is smaller than q. Now, define three qua-tripternion algebras

$$\Omega = \{(\sigma_0 + \sigma_1 i + \sigma_2 j + \sigma_3 k) + \left(\mu_0 + \mu_1 i + \mu_2 j + \mu_3 k)x + (\delta_0 + \delta_1 i + \delta_2 j + \delta_3 k)x^2\right) | \sigma_0, \sigma_1,$$
$$\sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2, \mu_3, \delta_0, \delta_1, \delta_2, \delta_3 \in A\}$$

$$\Omega_p = \{(\sigma_0 + \sigma_1 i + \sigma_2 j + \sigma_3 k) + \left(\mu_0 + \mu_1 i + \mu_2 j + \mu_3 k)x + (\delta_0 + \delta_1 i + \delta_2 j + \delta_3 k)x^2\right) | \sigma_0,$$
$$\sigma_1, \sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2, \mu_3, \delta_0, \delta_1, \delta_2, \delta_3 \in A_p\}$$

$$\Omega_q = \{(\sigma_0 + \sigma_1 i + \sigma_2 j + \sigma_3 k) + \left(\mu_0 + \mu_1 i + \mu_2 j + \mu_3 k)x + (\delta_0 + \delta_1 i + \delta_2 j + \delta_3 k)x^2\right) | \sigma_0,$$
$$\sigma_1, \sigma_2, \sigma_3, \mu_0, \mu_1, \mu_2, \mu_3, \delta_0, \delta_1, \delta_2, \delta_3 \in A_q\}.$$

The subset $L_F, L_V, L_U, L_G, L_R, L_S, L_C,$ and L_M are define as follow:

$L_F = \{f_0 + f_1 x + f_2 x^2 \in \Omega$ satisfy $\ell_{(d_f, d_f - 1)}\}$
$L_V = \{v_0 + v_1 x + v_2 x^2 \in \Omega$ satisfy $\ell_{(d_v, d_v - 1)}\}$
$L_U = \{u_0 + u_1 x + u_2 x^2 \in \Omega$ satisfy $\ell_{(d_u, d_u)}\}$
$L_G = \{g_0 + g_1 x + g_2 x^2 \in \Omega$ satisfy $\ell_{(d_g, d_g)}\}$
$L_R = \left\{r_0 + r_1 x + r_2 x^2 \in \Omega$ satisfy $\ell_{(d_r, d_r)}\right\}$
$L_S = s_0 + s_1 x + s_2 x^2 \in \Omega\ satisfy\ \ell_{(d_s, d_s - 1)}$
$L_C = \{c_0 + c_1 x + c_2 x^2 \in \Omega\ satisfy\ \ell_{(d_c, d_c)}\}$
$L_M = \{m_0 + m_1 x + m_2 x^2 |$then the coefficients m_i are chosen *mod* p between $-p/2$ and $p/2\}$

where $\ell(d_x, d_y) = \{f \in \Omega | f$ has d_x coefficients equal 1, d_y coefficients equal to -1, the remaining are equal to 0$\}$. The TrQtNTR cryptosystem is passed through the following three phases:

5.1. Key Generation

The keys are constructed as follows: we randomly choose six polynomials F, G, U, S, and V from L_F, L_G, L_U, L_S, and L_V, respectively such that F must be invertible *mod* q. Their inverses is denoted by F_q^{-1} such that $F * F_q^{-1} = 1$, and V must be invertible *mod* p their inverses are denoted by V_p^{-1} such that $V_p^{-1} * V = 1$. Also, S must be invertible *mod* p their inverses are denoted by S_p^{-1} such that $S_p^{-1} * S = 1$.
The public key H, K are computed in the following manner:
$H = F_q^{-1} * G * U(modq)$
$K = F_q^{-1} * V * S(modq)$.
The set $\{F, G, U, V, S\}$ is private keys.

5.2. Encryption

The sender selects a random polynomial $R \in L_R$ and $C \in L_c$ which is called the ephemeral polynomial. The ciphertext of the plaintext $M \in L_M$ is computed as follows:
$E = p(H + R * C) + (K * M)(mod\ q)$.

5.3. Decryption

To recover the original message, the following steps must be followed:
After receiving the encrypted text, the original plaintext is obtained through the following steps

$$E = p\,(H + R * C) + K * M (mod\ q)$$
$$F * E\,(mod\ q) = p\left(F * F_q^{-1} * G * U + F * R * C\right) + F * F_q^{-1} * V * S * M\,(mod\ q)$$
$$F * E\,(mod\ q) = p\,(G * U + F * R * C) + V * S * M\ \ (mod\ q)$$
$$F * E\,(mod\ p) = V * S * M\ \ (mod\ p)$$

Take $Z = F * E\,(mod\ p)$
Then $S^{-1} * V^{-1} * Z\,(mod\ p) = M$.

6. Security Analysis

In TrQtNTR an attacker who knows the public parameters, as well as, the public keys $H = F_q^{-1} * G * U$ and $K = F_q^{-1} * V * S$, finds two of the qua-tripternion set $\{F, G, U\}$ and finds two of the qua-tripternion set $\{F, V, S\}$ (if not choose F previously), the private key can be easily computed. By brute force attack, the size of the subset L_F, L_G, L_U, L_V, and L_S is calculated as follows:

$$|L_F| = \left(\frac{N!}{(d_f!)^2\,(N-2d_f)!}\right)^{12},$$
$$|L_G| = \left(\frac{N!}{(dg!)^2\,(N-2d_g)!}\right)^{12},$$
$$|L_U| = \left(\frac{N!}{(d_u!)^2\,(N-2d_u)!}\right)^{12}$$
$$|L_V| = \left(\frac{N!}{(d_v!)^2\,(N-2d_v)!}\right)^{12},$$
$$|L_S| = \left(\frac{N!}{(d_s!)^2\,(N-2d_s)!}\right)^{12},$$

Therefore, the size of the search space of finding the private keys G, U, V, S is

$$\left(\frac{N!}{(dg!)^2\,(N-2d_g)!}\right)^{12}\left(\frac{N!}{(d_u!)^2\,(N-2d_u)!}\right)^{12}\left(\frac{N!}{(d_v!)^2\,(N-2d_v)!}\right)^{12}\left(\frac{N!}{(d_s!)^2\,(N-2d_s)!}\right)^{12}.$$

Similarly, the attacker can search in the space L_R and L_C to get the message original from the ciphertext and this search must be done in the order of the space L_R and L_C where its size is calculated as follows:

$$|L_R| = \left(\frac{N!}{(d_r!)^2\,(N-2d_r)!}\right)^{12}$$

$$|L_C| = \left(\frac{N!}{(d_c!)^2\,(N-2d_c)!}\right)^{12}.$$

Therefore, the size of the search space of finding the polynomials R, C is

$$\left(\frac{N!}{(d_r!)^2\,(N-2d_r)!}\right)^{12}\left(\frac{N!}{(d_c!)^2\,(N-2d_c)!}\right)^{12}.$$

7. Comparative Between QTRU, NTRU, TrQtNTR

7.1. Mathematical Operation

Through 5.1, 5.2, and 5.3 from section 5, the comparison of the mathematical operations of creating the key, the encryption, and the decryption between QTRU, NTRU, and TrQtNTR are shown in Table 1.

Table 1: Convolution multiplications and addition of QTRU, NTRU, and TrQtNTR

	QTRU	NTRU	TrQtNTR
Key Generate	16 convolution multiplications	one convolution multiplications	48 convolution multiplications
Encryption	16 convolution multiplications, four polynomials addition	one convolution multiplications, one polynomial addition	24 convolution multiplications, 24 polynomials addition
Decryption	32 convolution multiplications, four polynomials addition	two convolution multiplications, one polynomial addition	60 convolution multiplications, 24 polynomials addition

The speed of QTRU, NTRU, and TrQtNTR is described in Table 2. The multiplication, time is denoted by t, and the addition time is denoted by t_1. It is calculated as follows

Table 2: Speed of QTRU, NTRU, and TrQtNTR

	QTRU	NTRU	TrQtNTR
Speed	$64t + 8t_1$	$4t + 2t_1$	$132t + 48t_1$

We conclude that TrQtNTR is slower than NTRU and QTRU.

7.2. Level of Security

By brute force attack, the level of security comparison of the key and the message between QTRU, NTRU, and TrQtNTR is abstracted in Table 3.

Table 3: Level of Security of QTRU, NTRU, and TrQtNTR

	Security Space of key	Security Space of message
QTRU	$(\frac{N!}{(d_g!)^2(N-2d_g)!})^4$	$(\frac{N!}{(d_r!)^2(N-2d_r)!})^4$
NTRU	$(\frac{N!}{(d_g!)^2(N-2d_g)!})$	$(\frac{N!}{(d_r!)^2(N-2d_r)!})$
TrQtNTR	$(\frac{N!}{(dg!)^2(N-2d_g)!})^{12}(\frac{N!}{(d_s!)^2(N-2d_s)!})^{12}$ $(\frac{N!}{(d_u!)^2(N-2d_u)!})^{12}(\frac{N!}{(d_v!)^2(N-2d_v)!})^{12}$	$(\frac{N!}{(d_r!)^2(N-2d_r)!})^{12}$ $(\frac{N!}{(d_c!)^2(N-2d_c)!})^{12}$

8. Conclusion

TrQtNTR cryptosystem is better than NTRU and QTRU in terms of security. It provides security for the key and the message, as the security of the key in this system is forty-eight times for the key compared to the NTRU and twelve times to QTRU, and twenty four times for the message compared to the NTRU and six times in comparing QTRU. But, it is slower than NTRU and QTRU. It has many applications, including electronic voting.

References

1. N. M. 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 **7** (2016), no. 11, 1–6.

2. N. M. AlSaidi and H. R. Yassein, *A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure*, Malaysian Journal of Mathematical Sciences **11** (2017), 29–43.

3. M. Coglianese and B.-M. Goi, *MaTRU: A new NTRU-based cryptosystem*, Progress in Cryptology-INDOCRYPT 2005: 6th International Conference on Cryptology in India, Bangalore, India, December 10-12, 2005. Proceedings 6, Springer, 2005, pp. 232–243.

4. 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.

5. E. Malekian and A. Zakerolhosseini, *OTRU: A non-associative and high speed public key cryptosystem. a. computer architecture and digital systems (cads)*, 2010 15th CSI International Symposium on Computer Architecture and Digital Systems, Tehran, 2009, pp. 83–90.

6. E. Malekian, A. Zakerolhosseini, and A. Mashatan, *QTRU: Quaternionic version of the ntru public-key cryptosystems.*, ISeCure **3** (2011), no. 1, 29–42.

7. M. Nevins, C. Karimianpour, and A. Miri, *NTRU over rings beyond*, Designs, Codes and Cryptography **56** (2009), no. 1, 65–78.

8. Kouzmenko R., *Generalizations of the NTRU cryptosystem*, Diploma project, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, 2006.

9. H. R. Yassein and N. M. Al-Saidi, *HXDTRU cryptosystem based on hexadecnion algebra*, Cryptology 2016 Conference, vol. 30, 2016, pp. 1–14.

10. 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*, Journal of Discrete Mathematical Sciences and Cryptography **25** (2020), no. 2, 523–542.

11. H. R. Yassein and N. M. AlSaidi, *BCTRU: A new secure ntru crypt public key system based on a newly multidimensional algebra*, proceeding of 6th international cryptology and information security conference, 2018, pp. 1–11.

12. H.R. Yassein, N. M. Al-Saidi, and A. K. Almosawi, *A multi-dimensional algebra for designing an improved NTRU cryptosystem*, Eurasian journal of mathematical and computer applications **8** (2020), no. 4, 97–107.

13. H.R. Yassein and N.M. Al-Saidi, *An innovative bi-cartesian algebra for designing of highly performed NTRU like cryptosystem*, Malaysian Journal of Mathematical Sciences **13** (2019), no. S, 77–91.

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

and

Sarah H. Shahhadi,
Department of Mathematics,
College of Education, University of Al-Qadisiyah,
Dewaniyah, Iraq.
E-mail address: math.post05@qu.edu.iq