QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra

H. H. Abo-Alsood and H. R. Yassein

1University of Al-Qadisiyah, College of Education, Iraq

Email: math.post12@qu.edu.iq , hassan.yaseen@qu.edu.iq

Abstract. NTRU is an open-source public key cryptosystem that encrypts and decrypts data using lattice-based cryptography. It is more resistant to attacks than other common public-key cryptosystems, and its performance has been demonstrated to be significantly higher. Any cryptosystem that uses non-commutative computations in its encryption and decryption processes becomes a highly lattice attack-resistant system as a result of Shamir's conclusion. This paper presents a new multidimensional public-key cryptosystem which is a non-commutative variant of the NTRU called QOTRU. It operates in the subalgebra of octonion algebra called Qu-octonion subalgebra with a new mathematical structure of two public keys and five private keys. This new structure has enhanced the public key system to be more secure and complex.

1. Introduction

Today, there is a rapid spread in the need for public-key encryption as more people use computer networks to exchange confidential documents and access sensitive data. In fact, without the availability of a secure and efficient public-key cryptosystem, several of these tasks would be impossible to achieve. Many public-key cryptosystems have been proposed as RSA, and ECC which are based on factorization and discrete algorithm problems. In 1996, Hoffstein et al. [1] designed a group of fast public key cryptosystems, called NTRU cryptosystem. It is a public key cryptosystem that works in the ring \( \mathbb{Z}[x]/(x^N - 1) \). In comparison with RSA and ECC, NTRU is faster and has considerably smaller keys. The possibility of a decryption failure is one weakness of NTRU; however, parameters may be chosen to minimize or eliminate this error. NTRU’s security has been and continues to be scrutinized by the cryptographic community, as a result of which the original design has undergone many improvements.

In 2002, Gaborite et al. [2] presented a generalization of NTRU by the ring of polynomials over the binary field \( F_2 \) which is called CTRU. In 2005, Coglianese and Goi [3] presented an analogue of NTRU called MaTRU; this system operates in the ring of all square matrices with polynomial entries. In 2009, Malekian et al. [4] presented QTRU cryptosystem, based on quaternion algebra. In 2010, Malekian et al. [5] introduced a cryptosystem called OTRU, depends on the octonion algebra. In 2011, K. Jarvis [6,7] introduced ETRU depends on Eisenstein integer ring \( \mathbb{Z}[\omega] \). In 2015, Majeed [8] proposed a new multidimensional system variant to NTRU based on the commutative quaternion called CQTRU. In 2016, Yassein and Al-Saidi [9-11] presented a new cryptosystems, called HXDTRU and BITRU, based on their hexadecenion and binary algebras. In 2018, Yassein and Al-Saidi [12,13] introduced a new NTRU like cryptosystem based on the bi-cartesian algebra; she called
it BCTRU. In the same year, Atani et al. [14] introduced a new NETRU cryptosystem that operates over the ring $M = M_k(Z_p)[T, x]/(x^n - I_{k,k})$ of $k \times k$ matrices of elements in the ring $R = Z_p[T, x]/(x^n - 1)$. In 2020, Yassein et al. [15] proposed a new NTRU cryptosystem using multidimensional carternion algebra called QOB\textsubscript{TRU}. In same year, Yassein et al. [16] proposed new multidimensional public key cryptosystem, called NTRTE based on a commutative quaternion algebra with a new structure. In 2021, Yassein et al. [17] also presented QMTRU an improvement of QTRU by using a new mathematical structure.

In this paper, we designed a new version of NTRU, called QOTRU depends on the subalgebra of octonion algebra, namely Qu-octonion algebra with a new mathematical structure.

This study is structured as follows. Qu-octonion algebra was introduced in Section 2. The QOTRU cryptosystem, defined in section 3, is constructed using this algebra. The security analysis of the QOTRU is discussed in section 4. Finally, Comparisons are performed with OTRU and QOTRU in section 5.

2. Qu-Octonion Subalgebra

Let $\mathfrak{O}$ be real octonion algebra which define as follows:

$$\mathfrak{O} = \{x \ | x = x_0 + \sum_{i=1}^{7} x_i e_i \ | x_0, ..., x_7 \in R \}. [18]$$

Now, the real qu-octonion subalgebra $\mathfrak{O}_R$ is a vector space of dimension four over the real numbers $R$ as follows:

$$\mathfrak{O}_R = \{a + b e_2 + c e_4 + d e_6 \ | a, b, c, d \in R \} \text{ such that } e_2^2 = e_4^2 = e_6^2 = -1 \text{ and } e_2 e_4 = -e_4 e_2 = e_6,$$

where $\{1, e_2, e_4, e_6\}$ form the basis of the qu-octonion subalgebra. Note that the qu-octonion subalgebra is associative and non commutative.

Let $F$ be a finite ring with $\text{char}(F) \neq 2$. We define the qu-octonion subalgebra $\mathfrak{O}_F$ over $F$ as follows: $\mathfrak{O}_F = \{a + b e_2 + c e_4 + d e_6 \ | a, b, c, d \in F \}$, with the same operations defined for the real octonion. Now, consider the three truncated polynomial rings:

$$\mathfrak{K}(x) = Z[x] / (x^N - 1), \quad \mathfrak{K}_p(x) = Z_p[x] / (x^N - 1) \quad \text{and} \quad \mathfrak{K}_q(x) = Z_q[x] / (x^N - 1).$$

The qu-octonionic subalgebras $\psi, \psi_p, \psi_q$ are defined as follows:

$$\psi = \{f_0 + f_1 e_2 + f_2 e_4 + f_3 e_6 \ | f_0, f_1, f_2, f_3 \in \mathfrak{K}\},$$

$$\psi_p = \{f_0 + f_1 e_2 + f_2 e_4 + f_3 e_6 \ | f_0, f_1, f_2, f_3 \in \mathfrak{K}_p\},$$

$$\psi_q = \{f_0 + f_1 e_2 + f_2 e_4 + f_3 e_6 \ | f_0, f_1, f_2, f_3 \in \mathfrak{K}_q\}.$$  

3. QOTRU Cryptosystem

3.1. Parameter creation

QOTRU scheme utilizes three positive integer $(N, p, q)$ as defined in OTRU and eight subsets $(\mathcal{L}_F, \mathcal{L}_G, \mathcal{L}_L, \mathcal{L}_T, \mathcal{L}_W, \mathcal{L}_R, \mathcal{L}_\theta, \mathcal{L}_M) \subset \psi$ are defined in table 1.

| Notation | Definition |
|----------|------------|
| $\mathcal{L}_F$ | $\{f_0(x) + f_1(x)e_2 + f_2(x)e_4 + f_3(x)e_6 \in \psi \ | f_0(x) \in \mathfrak{K} \text{ satisfy } \ell(d_f, d_f - 1)\}$ |
| $\mathcal{L}_G$ | $\{g_0(x) + g_1(x)e_2 + g_2(x)e_4 + g_3(x)e_6 \in \psi \ | g_0(x) \in \mathfrak{K} \text{ satisfy } \ell(d_g, d_g)\}$ |
| $\mathcal{L}_L$ | $\{u_0(x) + u_1(x)e_2 + u_2(x)e_4 + u_3(x)e_6 \in \psi \ | u_0(x) \in \mathfrak{K} \text{ satisfy } \ell(d_u, d_u)\}$ |
| $\mathcal{L}_T$ | $\{t_0(x) + t_1(x)e_2 + t_2(x)e_4 + t_3(x)e_6 \in \psi \ | t_0(x) \in \mathfrak{K} \text{ satisfy } \ell(d_t, d_t - 1)\}$ |
| $\mathcal{L}_W$ | $\{w_0(x) + w_1(x)e_2 + w_2(x)e_4 + w_3(x)e_6 \in \psi \ | w_0(x) \in \mathfrak{K} \text{ satisfy } \ell(d_w, d_w - 1)\}$ |
| $\mathcal{L}_R$ | $\{r_0(x) + r_1(x)e_2 + r_2(x)e_4 + r_3(x)e_6 \in \psi \ | r_0(x) \in \mathfrak{K} \text{ satisfy } \ell(d_r, d_r)\}$ |
| $\mathcal{L}_\theta$ | $\{\theta_0(x) + \theta_1(x)e_2 + \theta_2(x)e_4 + \theta_3(x)e_6 \in \psi \ | \theta_0(x) \in \mathfrak{K} \text{ satisfy } \ell(d_\theta, d_\theta)\}$ |
| $\mathcal{L}_M$ | $\{m_0(x) + m_1(x)e_2 + m_2(x)e_4 + m_3(x)e_6 \in \psi \ | \text{coefficients of } m_i(x) \in \mathfrak{K} \text{ are the chosen modulo between } -p/2 \text{ and } p/2\}$ |


Where \( \{(d_x, d_y) = \{ f \in \mathcal{K} : f \text{ has } d_x \text{ coeff.} = 1, d_y \text{ coeff.} = -1 \text{, and rest } 0 \}\}.

### 3.2. Key generation algorithm

After randomly choosing five small qu-octonions \( F \in \mathcal{L}_F, G \in \mathcal{L}_G, U \in \mathcal{L}_U, T \in \mathcal{L}_T \) and \( W \in \mathcal{L}_W \), the keys are generated, as shown in algorithm 1.

**Algorithm 1: Key generation**

- **Input:** \( N, p, q, d_f, d_g, d_u, d_w, d_t \)
- **Output:** public keys \( H, K \)

\[
egin{align*}
F_q^{-1} &= \text{inverse } F \mod q \\
F_p^{-1} &= \text{inverse } F \mod p \\
T_q^{-1} &= \text{inverse } T \mod q \\
W_p^{-1} &= \text{inverse } W \mod p \\
H &= F_q^{-1} \ast G \ast U \mod q \\
K &= W \ast T_q^{-1} \mod q
\end{align*}
\]

Therefore \( \{F, G, U, W, T\} \) is set of private key.

### 3.3. Encryption algorithm

After selects a random \( R \in \mathcal{L}_R \) and \( \theta \in \mathcal{L}_\theta \), and converts the original message \( M \) to qu-octonion form. Algorithm 2 explains how the encryption is designed.

**Algorithm 2: Encryption**

- **Input:** \( N, p, q, d_r, d_o, \) the message \( M \), the public keys \( H, K \)
- **Output:** the encryption message \( E \)

\[
E = p(H \ast \theta + R) + M \ast K \mod q
\]

### 3.4. Decryption algorithm

The decryption is executed through the following proposed algorithm.

**Algorithm 3: Decryption**

- **Input:** \( N, q, p, F, F_p^{-1}, T, W_p^{-1}, E \)
- **Output:** \( M \)

\[
egin{align*}
A_1 &= F \ast E \mod q \\
A_2 &= A_1 \ast T \mod q \\
\text{for } i &= 1 \text{ to } 4 \\
\text{for } j &= 1 \text{ to } N \\
\text{if } A_2(i, j) \leq -q/2 \\
A_2(i, j) &= A_2(i, j) + q \\
\text{else if } A_2(i, j) > q/2 \\
A_2(i, j) &= A_2(i, j) - q \\
\text{end if}
\end{align*}
\]

\[
A_3 = A_2 \mod p \\
A_4 = F_p^{-1} \ast A_3 \mod p \\
A_5 = A_4 \ast W_p^{-1} \mod p \\
\text{for } i &= 1 \text{ to } 4
\]
4. Security Analysis

To conduct a brute force attack against QOTRU, attackers who know the general parameters and the public key \( H = F_q^{-1} \ast G \ast U \mod q \) and \( K = W \ast T_q^{-1} \mod q \). It is necessary to find the private keys \( F, T \) from the set \( L_F, L_T \) or find the private keys \( G, U, W \) from the sets \( L_G, L_U, L_W \) and a short key using these private keys. The size of the subsets \( L_F, L_G, L_U, L_W \) and \( L_T \) is equal to

\[
|L_F| = \left( \frac{N!}{(d_f!)^2(N-2d_f)!} \right)^4,
\]

\[
|L_G| = \left( \frac{N!}{(d_g!)^2(N-2d_g)!} \right)^4,
\]

\[
|L_U| = \left( \frac{N!}{(d_u!)^2(N-2d_u)!} \right)^4,
\]

\[
|L_W| = \left( \frac{N!}{(d_w!)^2(N-2d_w)!} \right)^4,
\]

\[
|L_T| = \left( \frac{N!}{(d_t!)^2(N-2d_t)!} \right)^4.
\]

Therefore, the total number of attempts to find the private keys \( G, U \) and \( W \) is equal to

\[
\frac{N^{12}}{(d_g!d_u!d_w!)^8((N-2d_g)!(N-2d_u)!(N-2d_w)!)^{10}}.
\]

Similarly, it is necessary to find \( \theta, R \) from the sets \( L_\theta, L_R \) until the original message is found. The size of the subsets \( L_\theta, L_R \) is equal to

\[
|L_\theta| = \left( \frac{N!}{(d_\theta!)^2(N-2d_\theta)!} \right)^4,
\]

\[
|L_R| = \left( \frac{N!}{(d_r!)^2(N-2d_r)!} \right)^4.
\]

Therefore, the total number of attempts to find \( \theta, R \) is equal to

\[
\frac{N^8}{(d_\theta!d_r!)^8((N-2d_\theta)!(N-2d_r)!)^{10}}.
\]

Table 2 shows the security level of the private key space and message space according to general parameters in QOTRU.
Table 2. Space of the private key and message

| N   | $d_f$ | $d_i$ | $d_g$ | $d_u$ | $d_w$ | $d_o$ | $d_r$ | Key space       | Message space       |
|-----|-------|-------|-------|-------|-------|-------|-------|-----------------|---------------------|
| 107 | 12    | 12    | 12    | 12    | 12    | 5     | 5     | $3.8261 \times 10^{361}$ | $3.7788 \times 10^{127}$ |
| 107 | 20    | 20    | 20    | 20    | 20    | 10    | 10    | $1.1316 \times 10^{489}$ | $1.4542 \times 10^{213}$ |
| 149 | 12    | 12    | 12    | 12    | 12    | 10    | 10    | $2.2092 \times 10^{407}$ | $1.3068 \times 10^{238}$ |
| 149 | 25    | 25    | 25    | 25    | 25    | 20    | 20    | $5.6765 \times 10^{650}$ | $1.5567 \times 10^{381}$ |
| 167 | 18    | 18    | 18    | 18    | 18    | 18    | 18    | $4.3439 \times 10^{559}$ | $1.2357 \times 10^{373}$ |
| 167 | 27    | 27    | 27    | 27    | 27    | 22    | 22    | $1.1366 \times 10^{717}$ | $8.4972 \times 10^{423}$ |
| 211 | 20    | 20    | 20    | 20    | 20    | 18    | 18    | $6.2237 \times 10^{653}$ | $3.0335 \times 10^{405}$ |
| 211 | 34    | 34    | 34    | 34    | 34    | 22    | 22    | $7.4299 \times 10^{909}$ | $3.6438 \times 10^{664}$ |
| 257 | 20    | 20    | 20    | 20    | 20    | 18    | 18    | $6.3795 \times 10^{698}$ | $1.6622 \times 10^{432}$ |
| 257 | 24    | 24    | 24    | 24    | 24    | 24    | 24    | $4.6413 \times 10^{792}$ | $2.7825 \times 10^{528}$ |

5. Comparison Between QOTRU with OTRU

In this section, comparison of the QOTRU and the OTRU is described from where a efficiency and security.

5.1. Key and message security level

A comparison between key security and message security in both QOTRU and OTRU systems shows that QOTRU security is better than OTRU security. In table 3, a comparison between the QOTRU and OTRU in terms of security for the key and the message is introduced, depending on the generic parameters.

Table 3. Comparison between QOTRU with OTRU

| Message Space of QOTRU | Message Space of OTRU | Key Space of QOTRU | Key Space of OTRU |
|------------------------|-----------------------|-------------------|-------------------|
| $3.7788 \times 10^{127}$ | $3.7788 \times 10^{127}$ | $3.8261 \times 10^{361}$ | $1.1354 \times 10^{241}$ |
| $1.4542 \times 10^{213}$ | $1.4542 \times 10^{213}$ | $1.1316 \times 10^{489}$ | $1.0859 \times 10^{326}$ |
| $1.3068 \times 10^{238}$ | $1.3068 \times 10^{238}$ | $2.2092 \times 10^{407}$ | $3.6544 \times 10^{271}$ |
| $1.5567 \times 10^{381}$ | $1.5567 \times 10^{381}$ | $5.6765 \times 10^{650}$ | $6.8557 \times 10^{433}$ |
| $1.2357 \times 10^{373}$ | $1.2357 \times 10^{373}$ | $4.3439 \times 10^{559}$ | $1.2357 \times 10^{373}$ |
| $8.4972 \times 10^{423}$ | $8.4972 \times 10^{423}$ | $1.1366 \times 10^{717}$ | $1.0891 \times 10^{478}$ |
| $3.0335 \times 10^{405}$ | $3.0335 \times 10^{405}$ | $6.2237 \times 10^{653}$ | $7.2895 \times 10^{435}$ |
| $3.6438 \times 10^{464}$ | $3.6438 \times 10^{464}$ | $7.4299 \times 10^{909}$ | $3.8076 \times 10^{606}$ |
| $1.6622 \times 10^{432}$ | $1.6622 \times 10^{432}$ | $6.3795 \times 10^{698}$ | $7.4107 \times 10^{465}$ |
| $2.7825 \times 10^{528}$ | $2.7825 \times 10^{528}$ | $4.6413 \times 10^{792}$ | $2.7825 \times 10^{528}$ |
With the same coefficients, the security level of the key of QOTRU is higher than OTRU and the security level of the message is the same.

5.2. Computational efficiency
We compare the arithmetic operations (addition and convolution multiplication) of QOTRU with those of OTRU, as shown in Table 4.

| Table 4. Convolution multiplication and addition of QOTRU, and OTRU |
|---------------------------------------------------------------|
| QOTRU | OTRU |
| Key generation | 80C | 64C |
| Encryption | 32C and 8A | 64C and 8A |
| Decryption | 384C and 8A | 1024C and 8A |

Where C refers to the convolution multiplication, A refers to the addition. Moreover, the system QOTRU is also efficient in terms of speed compared to the OTRU.

Table 5 compares the speed of QOTRU and OTRU based on Table 4.

| Table 5. Speed of QOTRU, and OTRU |
|-----------------------------------|
| QOTRU | OTRU |
| Speed | 496t + 16t₁ | 1152t + 16t₁ |

Such that t is the time of convolution multiplication and t₁ is the time of polynomial addition.

6. Conclusion
The OTRU cryptosystem is based on octonion algebra, and by relying on subalgebra from the octonion algebra, a QOTRU multi-dimensional cryptosystem was introduced with high security and high speed compared to OTRU. Therefore, QOTRU will have very high security compared to the original system NTRU. Also, this method ensures that data is generated from one or different sources and this makes it successful in many applications that require multiple data sources.

References
[1] Hoffstein J, Pipher J and Silverman J 1998 NTRU: a ring based public key cryptosystem Int. Algorithmic Number Theory Symp. (LNCS vol 1423) ed J P Buhler (London: Springer) pp 267-288.
[2] Gaborit P, Ohler J and Soli P 2002 CTRU, a polynomial analogue of NTRU INRIA Rapport de recherche N. 4621.
[3] Coglianese M and Goi B 2005 MaTRU: A new NTRU based cryptosystem Int. conf. on cryptoloogy in India (LNCS vol 3797) ed S Maitra et al (Dalian: Springer) pp 232-243.
[4] Malekian E, Zakerollhosoeini A and Mashatan A 2011 QTRU: quaternion version of the NTRU public-key cryptosystems The ISC Int’l J. Information Security 3 29-42.
[5] Malekian E and Zakerollhosoeini A 2010 OTRU: a non-associative and high speed public key cryptosystem In 2010 15th CSI Int. Symp. On Computer Architecture and Digital Systems (Tehran: IEEE Computer Society) pp 83-90.
[6] Jarvis K 2011 NTRU over the Eisenstein Integers M. Sc. thesis University of Ottawa.
[7] Jarvis K and Nevins M 2015 ETRU: NTRU over the Eisenstein integers Designs Codes and Cryptography 74 219-242.
[8] Majeed A A 2015 CQTRU cryptosystem based on commutative rings of quaternion M.Sc.
Thesis University of Technology Iraq.

[9] Yassein H R and Al-Saidi N M 2016 HXDTRU cryptosystem based on hexadecinion algebra in Proc. 5th Int. Cryptology and Information Security Conf. vol 5 (Sabah) pp 1-14.

[10] Al-Saidi N M and Yassein H R 2017 A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure *Malaysian J. Mathematical Sci.* 11 29-43.

[11] Yassein H R and Al-Saidi N M 2016 BITRU: binary version of the NTRU public key cryptosystem via binary algebra *Int. J. Advanced Computer Sci. and Applications* 7 1-6.

[12] Yassein H R and Al-Saidi N M 2018 BCTRU: a new secure NTRUcrypt public key system based on a newly multidimensional algebra proc. 6th Int. Cryptology and Information Security conf. vol 6 (Negeri Sembilan) pp 1-11.

[13] Yassein H R and Al-Saidi N M 2019 An innovative bi-cartesian algebra for designing of highly performed NTRU like cryptosystem *Malaysian J. Mathematical Sci.* 13 77-91.

[14] Atani R E, Atani S E and Karbasi A H 2018 NETRU: a non-commutative and secure variant of CTRU cryptosystem *The ISC Int’l J. Information Security* 10 45-53.

[15] Yassein H R, Al-Saidi N M and Farhan A K 2020 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.

[16] Yassein H R, Al-Saidi N M and Jabber A K 2020 A multi-dimensional algebra for designing an improved NTRU cryptosystem Eurasian *J. Mathematical and Computer Applications* 8 97-107.

[17] Yassein H R, Abidalzahra A A and Al-Saidi N M 2021 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.

[18] Saraiva P, Beites P D, Fernandes J, Costa C and Vitoria J 2015 Best Pair of Two Skew Lines over the Octonions Society *J. Advances in Applied Clifford Algebras*. 25 657-672.