International Journal of Mathematics and
Computer Science, **16**(2021), no. 4, 1469–1477

Design of an Alternative NTRU Encryption with High Secure and Efficient

Hadeel Hadi Abo-Alsood, Hassan Rashed Yassein

Department of Mathematics
College of Education
University of Al-Qadisiyah
Al-Diwaniyah, Iraq

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

(Received March 25, 2021, Accepted April 26, 2021)

Abstract

With the need to store a huge amount of personal information, Computer hardware has become extremely vital nowadays. However, some challenges follow this expansion; for instance, solving the problem of maintaining security challenges by using high-security algorithms. As a result, a high-security cryptosystem with low computation power is needed. One of the lattice-based cryptosystems that meet these requirements is NTRU. Since the NTRU cryptosystem proposal, many variants were proposed by researchers using different algebraic structures. In this paper, we design a new cryptosystem variant of NTRU, called BOTRU, which is a high-performing system based on bi-octonion subalgebra and it has good resistance to some well-known attacks, such as a brute force attack. The creation of two public keys in the system proposed has differentiated it from NTRU and NTRU like cryptosystems. Some arithmetic operations are used for comparing the efficiency of BOTRU with the OTRU cryptosystem. Based on arithmetic assessment, the comparison reveals that the BOTRU has a higher speed than the OTRU.

Key words and phrases: NTRU, bi-octonion subalgebra, OTRU, BOTRU.
AMS (MOS) Subject Classifications: 94A60.
ISSN 1814-0432, 2021, http://ijmcs.future-in-tech.net

1 Introduction

In 1996, Hoffstein et al. [1] introduced the NTRU public key cryptosystem that operates in the ring of truncated polynomials $Z[x]/\left(x^N-1\right)$. Its name NTRU indicates the use of number theory and rings. It is the first system thatis not based on complicated mathematical problems. NTRU is dependent on the shortest vector problem in a lattice. The speed of NTRU is one of its considerable features. Compared to RSA and ECC, NTRU executes drastically faster and its key is significantly smaller.

Since NTRU was proposed, many researchers have improved its performance over the past two decades. This was done by developing its algebraic structure. In 2002, Gaborit et al. [2] introduced an analog of NTRU, called CTRU, based on a polynomial ring on $F_2[x]$. In 2005, Coglianese and Goi [3] presented an analog of NTRU, called MaTRU. This system operates in the ring of $k \times k$ matrices of polynomials in $Z[x]/(x^n-1)$. In 2009, Malekian et al. [4] gave a four-dimensional cryptosystem, QTRU, depending on quaternion algebra. In 2010, Malekian et al. [5] introduced a multi-dimensional cryptosystem, OTRU, based on non-associative and non-commutative algebra; namely, octonion algebra. In 2011, K. Jarvis [6] introduced ETRU based on Eisenstein integer ring $Z[\omega]$. In 2016, Yassein and Al-Saidi [7-10] introduced analogs to the NTRU cryptosystem called HXDTRU and BITRU, defined by the hexadecnion and binary algebras. For BITRU, its design relies on establishing two public keys, which in turn helps increase the security and complexity of BITRU. In 2018, Yassein and Al-Saidi [11, 12] also designed another multidimensional NTRU-like cryptosystem, called BCTRU, which relies on Bi-cartesian algebra. In the same year, Atani et al. [13] introduced a new NETRU cryptosystem that operates over the ring $\boldsymbol{M} = M_k(Z_p)[T,x]/(X^n - I_{k\times k})$ of $k \times k$ matrices of elements in the ring $R = Z_p[T,x]/(x^n-1)$. In 2020, Yassein et al. [14] proposed a new NTRU-analogue called QOB_{TRU} based on carternion algebra. In the same year, Yassein et al. [15] introduced a new multi-dimensional public key cryptosystem, called NTRTE, based on a commutative quaternion algebra with a new structure. In 2021 Yassein et al. [16] introduced an analog QTRU cryptosystem, called QMNTR, by designing a new mathematical structure.
In this study, we present a new public key cryptosystem, called BOTRU, based on the bi-octonion subalgebra with a new mathematical structure and we compare its performance with OTRU.

2 BI-OCTONION SUBALGEBRA

In this section, the real bi-octonion subalgebra and its properties are introduced. Let $\mathbb{O}$ be an octonion algebra defined as follows $\mathbb{O} = \{x \setminus x = x_0 + \sum_{i=1}^{7} x_i \, .e_i \setminus x_0, \ldots, x_7 \ \in \mathbb{R}\}$. Define the real bi-octonion subalgebra $B\mathbb{O}_{\mathbb{R}}$ of dimension two as follows:

$B\mathbb{O}_{\mathbb{R}} = \{a + be_1 \setminus a, b \in \mathbb{R}\}$ such that $e_1^2 = -1$, where $\{1, e_1\}$ form the basis of the bi-octonion subalgebra. This algebra is associative and commutative. Assume $\mathcal{F}$ be an arbitrary finite ring of $char\,(\mathcal{F}) \neq 2$. We define the bi-octonion subalgebra $B\mathbb{O}_{\mathcal{F}}$ over $\mathcal{F}$ as follows:

$$B\mathbb{O}_{\mathcal{F}} = \{a + be_1 \setminus \ a, b \in \mathcal{F}\},$$

with the same operations, which are defined in the octonion algebra. Now, if we have three truncated polynomial rings

$$\mathcal{K} = Z\,[x] \,/\, \left(x^N - 1\right), \ \mathcal{K}_p = (Z/pZ)\,[x] \,/\, \left(x^N - 1\right), \ \mathcal{K}_q = (Z/qZ)\,[x] \,/\, \left(x^N - 1\right).$$

We can define three bi-octonionic subalgebras Ω, Ω_p, *and* Ω_q as follows:

$\Omega = \{f_0 + f_1 e_1 \setminus \ f_0, f_1 \in \mathcal{K}\}$, $\Omega_p = \{f_0 + f_1 e_1 \setminus \ f_0, f_1 \in \mathcal{K}_p\}$, and $\Omega_q = \{f_0 + f_1 e_1 \setminus \ f_0, f_1 \in \mathcal{K}_q\}$.

3 THE PROPOSED BOTRU

The parameters of the BOTRU cryptosystem consist of the integers N, p, q as defined in OTRU and the subsets $\mathcal{L}_F$, $\mathcal{L}_V$, $\mathcal{L}_G$, $\mathcal{L}_J$, $\mathcal{L}_M$, $\mathcal{L}_\theta$, and $\mathcal{L}_R \subset \Omega$ are defined in Table 1.

where $\ell\,(d_1, d_2) = \{f \in \mathcal{K} \setminus f$ has d_1 coefficients equal 1, d_2 coefficients equal -1, the remaining equal 0$\}$. The constants d_f, d_v, d_g, d_j, d_m, d_θ, and d_r are defined in a similar role as in OTRU. The BOTRU cryptosystem can be described through the following three phases:

Key Creation

To create BOTRU keys, we select four polynomials $F \in \mathcal{L}_F$, $V \in \mathcal{L}_V$, $G \in \mathcal{L}_G$, and $J \in \mathcal{L}_J$, such that, F should be invertible modulo p and q, V invertible modulo q, and J invertible modulo p, denoted by F_p^{-1}, F_q^{-1}, V_q^{-1}, J_p^{-1} respectively.

$$F_q^{-1} * F \equiv I \ (mod\ q), F * F_p^{-1} \equiv I \ (mod\ p)$$

Table 1: Subsets of BOTRU

Notation	**Definition**
$\mathcal{L}_F$	$\{f_0(x)+f_1(x)e_1 \in \Omega \backslash f_0\ ,\ f_1 \in \mathcal{K}$ satisfy $\ell(d_f, d_f-1)\}$
$\mathcal{L}_V$	$\{v_0(x)+v_1(x)e_1 \in \Omega \backslash v_0\ ,\ v_1 \in \mathcal{K}$ satisfy $\ell(d_v, d_v-1)\}$
$\mathcal{L}_G$	$\{g_0(x)+g_1(x)e_1 \in \Omega \backslash g_0\ ,\ g_1 \in \mathcal{K}$satisfy $\ell(d_g, d_g)\}$
$\mathcal{L}_J$	$\{j_0(x)+j_1(x)e_1 \in \Omega \backslash j_0\ ,\ j_1 \in \mathcal{K}$ satisfy $\ell(d_j, d_j-1)\}$
$\mathcal{L}_\theta$	$\{\theta_0(x)+\theta_1(x)e_1 \in \Omega \backslash \theta_0\ ,\ \theta_1 \in \mathcal{K}$satisfy $\ell(d_\theta, d_\theta)\ \}$
$\mathcal{L}_R$	$\{r_0(x)+r_1(x)e_1 \in \Omega \backslash r_0\ ,\ r_1 \in \mathcal{K}$satisfy $\ell(d_r, d_r)\}$
$\mathcal{L}_M$	$\{m_0(x)+m_1(x)e_1 \in \Omega \backslash$ coefficients of $m_0\ ,\ m_1 \in \mathcal{K}$ are the chosen modulo between $-p/2$ and $p/2\ \}$.

$$V_q^{-1} * V \equiv I\ (mod\ q), J * J_p^{-1} \equiv I\ (mod\ p).$$

The public keys are computed as follows:

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

Therefore, the private key is $\{F,\ \ G,\ \ J,\ \ V\}$.

Encryption

After converting the original message M to bi-octonion form, we choose random polynomials $\theta \in \mathcal{L}_\theta$ and $R \in \mathcal{L}_R$. Now, compute E by the law

$$E = p(H * \theta + R) + M * K\ \ (mod\ q).$$

Decryption

To get the original message after receiving the ciphertext from the sender, we follow the following process:

a. **Multiple Private Keys**

$$\begin{aligned} B &= F * E * V\ \ (mod\ q) \\ &= F * (p(H * \theta + R) + M * K) * V\ \ (mod\ q) \\ &= pF * H * \theta * V + pF * R * V + F * M * K * V\ \ (mod\ q) \\ &= pF * F_q^{-1} * G * \theta * V + pF * R * V + F * M * J * V_q^{-1} * V\ \ (mod\ q) \\ &= pG * \theta * V + pF * R * V + F * M * J\ \ (mod\ q). \end{aligned}$$

such that the coefficient of $pG * \theta * V + pF * R * V + F * M * J$ lie in the interval $(-q/2,\ \ q/2]$.

b. **Convert modulo q to modulo p.**

$$\begin{aligned} &Convert\ B = pG * \theta * V + pF * R * V + F * M * J\ \ (mod\ q)\ to\ modulo\ p \\ &B\ (\ mod\ p) = pG * \theta * V + pF * R * V + F * M * J\ \ (mod\ p) \\ &\qquad\qquad = F * M * J\ (mod\ p). \end{aligned}$$

c. **Multiple Inverses**

$$F_p^{-1} * B * J_p^{-1}\,(mod\ p) = M\ \ (mod\ p)\,,$$

and the resulting coefficients are adjusted to lie in the interval $(-p/2,\ \ p/2]$.

4 SECURITY ANALYSIS

In BOTRU an attacker who knows the public key,

$$H = F_q^{-1} * G\ (mod\ q),\ \ K = J * V_q^{-1}\ (mod\ q),$$

the public parameters must search in $\mathcal{L}_F$ and $\mathcal{L}_V$ to find the private keys $F,\ \ V$ or (search in $\mathcal{L}_G$ and $\mathcal{L}_J$ to find the private keys $G,\ \ J$), till a short key for the decryption is found. By a brute force attack, the total space for the four subsets $\mathcal{L}_F,\ \ \mathcal{L}_V,\ \ \mathcal{L}_G$, and $\mathcal{L}_J$ are calculated as follows:

$$|\mathcal{L}_F| = \left(\frac{N!}{(d_f!)^2\,(N-2d_f)!}\right)^2, |\mathcal{L}_V| = \left(\frac{N!}{(d_v!)^2\,(N-2d_v)!}\right)^2,$$

$$|\mathcal{L}_G| = \left(\frac{N!}{(d_g!)^2\,(N-2d_g)!}\right)^2, |\mathcal{L}_J| = \left(\frac{N!}{(d_j!)^2\,(N-2d_j)!}\right)^2.$$

Therefore, the key space is equal to the following:

$$\frac{(N!)^4}{(d_g!)^4((N-2d_g)!)^2(d_j!)^4((N-2d_j)!)^2}.$$

Similarly, to find the original message, an attacker must search in $\mathcal{L}_\theta$ and $\mathcal{L}_R$ such that

Table 2: space of the private key and message

N	d_f	d_v	d_g	d_1	d_θ	d_r	Key space	Message space
107	12	12	12	12	5	5	3.3696×10^{120}	6.1472×10^{63}
107	20	20	20	20	10	10	1.0421×10^{163}	3.8134×10^{106}
149	12	12	12	12	10	10	6.0452×10^{135}	1.1432×10^{119}
149	25	25	25	25	20	20	8.2799×10^{216}	3.9455×10^{190}
167	18	18	18	18	18	18	3.5153×10^{186}	3.5153×10^{186}
167	27	27	27	27	22	22	1.0436×10^{239}	9.2180×10^{211}
211	20	20	20	20	18	18	8.5378×10^{217}	5.5077×10^{202}
211	34	34	34	34	22	22	1.9513×10^{303}	1.9088×10^{232}
257	20	20	20	20	18	18	8.6085×10^{232}	1.2893×10^{216}
257	24	24	24	24	24	24	1.6681×10^{264}	1.6681×10^{264}

$$|\mathcal{L}_\theta| = \left(\frac{N!}{(d_\theta!)^2\,(N-2d_\theta)!}\right)^2, |\mathcal{L}_R| = \left(\frac{N!}{(d_r!)^2\,(N-2d_r)!}\right)^2.$$

Therefore, the message space is equal to the following:

$$\frac{(N!)^4}{(d_\theta!)^4((N-2d_\theta)!)^2(d_r!)^4((N-2d_r)!)^2}.$$

The security level of the private key space and the message space according to public parameters in BOTRU are shown in Table 2.

5 Comparison of BOTRU and OTRU

Key and Message Security

We compare the level of security of the keyspace and the message space of BOTRU with the OTRU cryptosystem, as shown in Table 3, according to the general parameters provided in Table 2. Consequently, the key and message security of the system OTRU is twice the key and message security of the system BOTRU.

Table 3: Comparison of BOTRU, and OTRU

Message Space of BOTRU	**Message Space of OTRU**	**Key Space of BOTRU**	**Key Space of OTRU**
6.1472×10^{63}	3.7788×10^{127}	3.3696×10^{120}	1.1354×10^{241}
3.8134×10^{106}	1.4542×10^{213}	1.0421×10^{163}	1.0859×10^{326}
1.1432×10^{119}	1.3068×10^{238}	6.0452×10^{135}	3.6544×10^{271}
3.9455×10^{190}	1.5567×10^{381}	8.2799×10^{216}	6.8557×10^{433}
3.5153×10^{186}	1.2357×10^{373}	3.5153×10^{186}	1.2357×10^{373}
9.2180×10^{211}	8.4972×10^{423}	1.0436×10^{239}	1.0891×10^{478}
5.5077×10^{202}	3.0335×10^{405}	8.5378×10^{217}	7.2895×10^{435}
1.9088×10^{232}	3.6438×10^{464}	1.9513×10^{303}	3.8076×10^{606}
1.2893×10^{216}	1.6622×10^{432}	8.6085×10^{232}	7.4107×10^{465}
1.6681×10^{264}	2.7825×10^{528}	1.6681×10^{264}	2.7825×10^{528}

Computational Efficiency

Compared the arithmetic operations (addition and convolution multiplication) of BOTRU and OTRU are shown in Table 4. Therefore, the speed of key creation, encryption, and decryption of BOTRU are faster than those of OTRU.

Table 4: Convolution multiplication and addition of BORTU, and OTRU

	BOTRU	**OTRU**
Key Generation	8β	64β
Encryption	8β and 4γ	64β and 8γ
Decryption	24β and 4γ	1024β and 8γ

such that β is the convolution multiplication and γ is the polynomial addition. Suppose that t is the time of convolution multiplication and t_1 is the time of polynomial addition. Based on Table 4, the speed of BOTRU and OTRU are compared in Table 5.

Table 5: Speed of BOTRU,and OTRU

	BOTRU	**OTRU**
Speed	$40t + 8t_1$	$1152t + 16t_1$

6 Conclusion

In this study, we introduced BOTRU as an alternative to NTRU. It is based on bi-octonion subalgebra. This system, being multi-dimensional, makes it possible to encrypt two messages from the same source or two independent messages from two different sources at the same time which is an important feature in certain applications. When the coefficient e_1 is equal to zero, BOTRU converts to NTRU. The speed of the BOTRU system is faster than that of OTRU with the same parameters, where speed is important for many applications. We have seen that the BOTRU system has a low-security level compared with the OTRU cryptosystem.

References

[1] J. Hoffstein, J. Pipher, J. Silverman, NTRU: A ring based public key cryptosystem. Proceeding of ANTS III, LNCS, Springer Verlag, (1998), 267–288.

[2] P. Gaborit, J. Ohler, P. Soli, CTRU, a polynomial analogue of NTRU, INRIA, Rapport de recherché, N. 4621, (2002).

[3] M. Coglianese, B. Goi, MaTRU: A new NTRU based cryptosystem, Springer Verlag Berlin Heidelberg, (2005), 232–243.

[4] E. Malekian, A. Zakerolhsooeini, A. Mashatan, QTRU: a lattice attack resistant version of NTRU PCKS based on quaternion algebra, The ISC Int'l Journal of Information Security, **3,** no. 1, (2011), 29–42.

[5] E. Malekian, A. Zakerolhsooeini, OTRU: A non-associative and high speed public key cryptosystem. IEEE Computer Society, (2010), 83–90.

[6] K. Jarvis, NTRU over the Eisenstein Integers, M. Sc. thesis, University of Ottawa, (2011).

[7] H. R. Yassein, N. M. Al-Saidi, HXDTRU Cryptosystem Based on Hexadecnion Algebra. In proceeding of 5th international cryptology and information security conference, (2016).

[8] N. M. Al-Saidi, H. R. Yassein, A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure, Malaysian Journal of Mathematical Sciences, **11,** (S), (2017), 29–43.

[9] H. R. Yassein, N. M. Al-Saidi, BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra, International Journal of Advanced Computer Science and Applications, **7,** no. 11, (2016), 1–6.

[10] H. R. Yassein, N. M. G. Al-Saidi, A Comparative Performance Analysis of NTRU and Its Variant Cryptosystems, Proceeding of International Conference on Current Research in Computer Science and Information Technology, (2017), 115–120.

[11] H. R. Yassein, N. M. Al-Saidi, BCTRU: A New Secure NTRUCrypt Public Key System Based on a Newly Multidimensional Algebra. In proceeding of 6th international cryptology and information security conference, (2018).

[12] H. R. Yassein, N. M. Al-Saidi, An Innovative Bi-Cartesian Algebra for Designing of Highly Performed NTRU Like Cryptosystem, Malaysian Journal of Mathematical Sciences, **13,** (S), (2019), 29–43.

[13] R. E. Atani, S. E. Atani, A. H. Karbasi, NETRU: A Non-commutative and Secure Variant of CTRU Cryptosystem, The ISC International Journal of Information Security, **10,** no. 1, (2018), 45–53.

[14] 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, Journal of Discrete Mathematical Sciences and Cryptography, **23,** no. 2 ,(2020) 1–20.

[15] H. R. Yassein, N. M. Al-Saidi, A. K. Jabber, A MultidimensionalAlgebra for Designing an Improved NTRU Cryptosystem, Eurasian Journal of Mathematical and Computer Applications, **8,** no. 4, (2020), 97–107.

[16] H. R. Yassein, A. A. Abidalzahra, N. M. G. Al-Saidi, A New Design of NTRU Encryption with High Security and Performance Level, AIP Conf. Proc. Istanbul Turkey, (2021), 080005- 1- 080005- 4.