Malaysian Journal of Mathematical Sciences 13(S) August: 77–91 (2019)
Special Issue: The 6th International Cryptology and Information Security Conference (CRYPTOLOGY2018)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

An Innovative Bicartisian Algebra for Designing of Highly Performed NTRU Like Cryptosystem

Yassein, H.R.*[1] and Al-Saidi, N.M.G.[2]

[1]*Department of Mathematics, College of Education, University of Al-Qadisiyah , Iraq*
[2]*Department of Applied Sciences, University of Technology, Iraq*

E-mail: hassan.yaseen@qu.edu.iq
**Corresponding author*

ABSTRACT

With the rapid developing of quantum computers, the needs of the highly secure cryptographic system are of great demand. NTRU is proved as a good performed and secure public key system for such developed technology because it is lattice-based cryptosystem. Therefore, designing of the finite field with high complexity and good resistance against linear algebra attacks is the primary objective for developing of highly secure NTRU like systems. In this paper, we construct a new algebraic structure to replace the classical NTRU polynomial ring; we called it bicartesian algebra. It is designed to be commutative and associative to generate BCTRU, which is an innovative high dimensional NTRU variant cryptosystem. Its probability of successful decryption is demonstrated. BCTRU exhibits appropriate security levels due to its ability to withstand some public attacks for such types of public key systems.

Keywords: NTRU , BCTRU, bicartesian algebra, security analysis.

1. Introduction

Cryptographic systems with high-security level and low implementation cost gained great attraction because it offers excellent security for our new network security era. Nowadays, NTRU is considered one of the highly used cryptosystems. It gains the popularity due to its efficient computational speed with low cost. Moreover, on the same security level, NTRU exceeds the classical cryptosystems by more than two orders of magnitude (An et al., 2018).

Most of the modern cryptographic techniques are best on arithmetic operations that defined on commutative algebraic structure which is considered nowadays as weak due to the fast increasing in computing process of newly computer devices.The developments in cryptosystems started from using symmetric cryptography such as stream ciphers and asymmetric cryptosystem such as RSA in (Rivest et al., 1978). An alternate fast public key system is a challenge and of great demand. In 1996 at crypt.96 conference, three J. start mathematicians researchers in (Hoffstein et al., 1998) introduced as to a new filed of research called non commutative algebraic cryptography through introducing of NTRU (Number Theory Research Unit) cryptosystem.

They aimed to develop the cryptographic technique based on a non-commutative algebraic structures. It was generalized by many researchers through developing of its algebraic structure. Some of those developed protocols based on different Euclidean ring free modules and algebras beyond Z are as follows: Basic collection of objects used by the NTRU public key cryptosystem occurs in a truncated polynomial ring of degree $N-1$ with integer coefficients that belong to $Z[x]/(x^N-1)$. NRTU is the first public key cryptosystem that does not depend on factorization and discrete log problems. Compared with the RSA and ECC cryptosystems, NTRU is faster and exhibits significantly smaller keys (Rivest et al., 1978, Schoof, 1985).

Based on polynomial ring on $F_2[x]$ is proposed by Gaborit et al. (2002). They constructed a CTRU which is a NTRU variant cryptosystem. Matrices of polynomials of size $k \times k$ in $Z[x]/(x^N-1)$ is proposed by Coglianese and Goi (2005). This NTRU analog is called MaTRU.

Suri and Puri (2007) presented the concept of crossbred technology using symmetric key as a stream cipher for encryption and decryption. NTRU public key cryptosystem was used in sending the secret key. Accordingly, the studies doubled the security, thereby avoiding brute force attacks because the attacker needs first to find the secret key that was encrypted through public key cryptography. In the same year, Malekian and Zakerolhosseini (2010) used

the actual performance results of NTRU with respect to current asymmetrical cryptosystems.

Atici et al. (2008) presented a low-power and compact NTRU design that was suitable for security applications such as, RFID and sensor nods. Their design involved two architectures, namely, one that can perform both encryption and decryption and another for encryption only. The researchers compared the design with the original NTRU and found that the new design saves a factor of more than two. This design improved the speed of NTRU.

Other NTRU variant cryptosystem was proposed by Malekian et al.,in 2009 and 2010 respectively (Malekian and Zakerolhosseini, 2010, Malekian et al., 2009). They rely in designing of their cryptosytems on Quaterion algebra and Octonion algebra respectively. In the same period, Vats (2009) introduced NTRU variant which is operated in the non-commutative ring $M = M_k(Z)[x]/(x^N - -I_{k\times k})$, where M is a matrix ring of the $k \times k$ matrices of polynomials in $Z[x]/(x^N - 1)$.

Another generalized framework is proposed by Pan and Deng (2011). They used hiding the trapdoor technique, that is led to design of a new lattice-based cryptosystem, which helps to solve the closest vector problem.

Kumar et al. introduced complex problems into the existing implementation; efficiency could be achieved through reduced implementation of polynomial multiplication of inverse computation.

A new ring of cubic root of unity called Eisensteian ring Z[w] is used to construct a new framework to NTRU called ETRU which is proposed by Jarvis and Nevins (2015). CQTRU is another NTRU variant cryptosystem proposed by Alsaidi et al. (2015). In (Thakur and Tripathi, 2016) Thakur and Tripathi utilized the rational field to construct a ring with polynomials of one variable over this filed to be used in introducing of new NTRU alternative cryptosystem called BTRU. After that Yassein and Al-Saidi constructed several high dimensional algebra as and utilized them in proposing of different NTRU analog cryptosystems presented in Al-Saidi and Yassein (2017), Alsaidi and Yassein (2016), Yassein and Al-Saidi (2016, 2017).

Atani et al. (2018) improved the CTRU by replacing the ring of polynomials $Z[x]/(x^N-1)$ by finite field Z_p and it operates over the ring $M = M_k(Z_p)[T,x]/(x^N - I_{k\times k})$, where M is a matrix ring of the $k \times k$.

In this paper, a new algebra is constructed, we called bicartesian algebra.It is used to construct BCTRU which is a new NTRU like cryptosystem. It is also multidimensional public key system, because it is produced two public key. This is resulted in increasing the security of the proposed cryptosystem. On comparing to its variant with the same structures, BCTRU has the ability to encrypt four messages sent by a single origin or four independent messages sent by four different sources. With this important property, the proposed system will be considered as an ultimate fast new public key cryptosystem to be as a best fit in many applications with limited resources, for examples smart cards, cellular phones and many others.

This study is organized as follows. Section 2 introduced new algebra called bicartesian algebra. This innovative algebra is used to design BCTRU cryptosystem, which is described in the section 3. The probability of successful decryption of BCTRU is discussed in section 4, and its security analysis is discussed in section 5. Finally, section 6 is dedicated for the most important conclusions.

2. Bicartesian Algebra

The bicartesian algebra is defined by utilizing the same parameters N, p and q used in NTRU, taking in our consideration that the integer constants d_f, d_g, d_m and d_ϕ should be less than N. Also, the truncated polynomial ring is defined as $K = Z[x]/(x^N - 1)$ with degree $N - 1$. We define a new algebra as follows:
The bicartesian algebra is introduced in this section as a vector space of dimension two over the field F. Let $BC = \{(a,b)(1,1) + (c,d)(k,1) | a,\ b,\ c,\ d \in F\} k^2 = 1$ where $\{$ (1,1), (k,1)$\}$ forms the basis of this algebra. The operation on this space is defined as follows:
Let x, $y \in BC$, such that $x = (a,b)(1,1) + (c,d)(k,1)$ and $y = (a_1,b_1)(1,1) + (c_1,d_1)(k,1)$, the addition is then defined by

$$x + y = (a + a_1, b + b_1)(1,1) + (c + c_1, d + d_1)(k,1).$$

The multiplication $x * y$ can be determined using Table 1 as follows

$$x * y = (aa_1 + cc_1, bb_1 + dd_1)(1,1) + (ac_1 + ca_1, bd_1 + db_1)(k,1)$$

$*$	(1,1)	(k,1)
(1,1)	(1,1)	(k,1)
(k,1)	(k,1)	(1,1)

For any scalar α, the scalar multiplication is defined by $\alpha x = (\alpha a, \alpha b)$. It is clear that the multiplication is commutative and associative. We now consider the truncated polynomial rings
$K(x) = (Z/Z)[x]/(x^N - 1)$, $K_p(x) = (Z/pZ)[x]/(x^N - 1)$
and $K_q(x) = (Z/qZ)[x]/(x^N - 1)$ and define three bicartesian algebra ψ, ψ_p and ψ_q as follows:

$$\psi = \{(f_0, f_1)(1,1) + (f_2, f_3)(k,1) | f_0,\ f_1,\ f_2,\ f_3 \in K\}$$

$$\psi_p = \{(f_0, f_1)(1,1) + (f_2, f_3)(k,1) | f_0,\ f_1,\ f_2,\ f_3 \in K_p\}$$

$$\psi_q = \{(f_0, f_1)(1,1) + (f_2, f_3)(k,1) | f_0,\ f_1,\ f_2,\ f_3 \in K_q\}.$$

The parameters N, p, and q are fixed similar to the NTRU parameters. The constants d_f, d_g, d_ϕ and d_m are defined in a similar role as in NTRU.

Let F and G $\in \psi_p$ or ψ_q , such that:

$$F = (f_0, f_1)(1,1) + (f_2, f_3)(k,1)$$

$$G = (g_0, g_1)(1,1) + (g_2, g_3)(k,1)$$

where f_0, f_1, f_2, f_3 and g_0 , g_1, g_2, $g_3 \in \psi_p$ or ψ_q.

The addition of F and G is performed by adding the corresponding coefficients mod p or mod q, such that

$$F + G = (f_0 + g_0, f_1 + g_1)(1,1) + (f_2 + g_2, f_3 + g_3)(k,1)$$

the multiplication of F and G is defined as follows:

$$F * G = (f_0 g_0 + f_2 g_2, f_1 g_1 + f_3 g_3)(1,1) + (f_0 g_2 + f_2 g_0, f_1 g_3 + f_3 g_1)(k,1)$$

The multiplicative inverse of any non zero element F in BC is given by:

$$F^{-1} = ((f_0^2 - f_2^2)^{-1} f_0, (f_2^2 - f_0^2)^{-1} f_2)(1,1)$$
$$+((f_1^2 - f_3^2)^{-1} f_1, (f_3^2 - f_1^2)^{-1} f_3)(k,1)$$

3. BCTRU Cryptosystem

Similar to NTRU, the BCTRU cryptosystem is constructed based on the same parameters, a prime number N, and two relatively prime numbers p, and

q, in which q is much larger than p. The four main subsets that NTRU and any NTRU variant cryptosystem depends on are defined as follows:

Definition 1: The subsets L_F, L_G, L_ϕ and $L_M \subset \Psi$ are called the subsets of BCTRU, and these subsets are defined as follows:

Notation	Definition
L_F	$\{ (f_0, f_1)(1,1) + (f_2, f_3)(k,1) \in K \mid f_i$ has d_f coefficients equal to $+1$, $(d_f - 1)$ coefficients equal to -1, and the rest are 0$\}$
L_G	$\{(g_0, g_1)(1,1) + (g_2, g_3)(k,1) \in K \mid g_i$ has d_g coefficients equal to $+1$, d_g coefficients equal to -1, and the rest are 0$\}$
L_ϕ	$\{(\phi_0, \phi_1)(1,1) + (\phi_2, \phi_3)(k,1) \in K \mid \phi_i$ has d_ϕ coefficients equal to $+1$, d_ϕ coefficients equal to -1, and the rest are 0$\}$
L_M	$\{(m_0, m_1)(1,1) + (m_2, m_3)(k,1) \in K \mid$ coefficients of m_i are chosen modulo p between $-p/2$ and $p/2$ $\}$

d_f, d_g and d_ϕ are also constant parameters similar to those defined in NTRU. The main cryptosystem parts of BCTRU are:

A. KEY GENERATION

In this phase, the sender is able to generate the public key by choosing F and U randomly from the set L_F and G randomly from the set LG such that,
$F = (f_0, f_1)(1,1) + (f_2, f_3)(k,1)$, $G = (g_0, g_1)(1,1) + (g_2, g_3)(k,1)$
and $U = (u_0, u_1)(1,1) + (u_2, u_3)(k,1)$

By considering that F must have multiplicative inverse modulo p and q refered to as F_p^{-1}, F_q^{-1} respectively, and U must have multiplicative inverse modulo p refered to as U_p^{-1}, the public keys are given by:

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

where F, G and U are the private keys. BCTRU key generation needs sixteen convolution multiplications and eight polynomial additions.

B. ENCRYPTION

Before performing of the encryption process, the message M should be expressed by the elements of the bicartesian algebra as:

$$M = (m_0, m_1)(1,1) + (m_2, m_3)(k,1).$$

We choose $\phi \in L_\phi$, which is called the blinding value to encrypt the message $M \in L_M$:

$$E = pH * \phi + M \ * \ K \ \ (mod\ q)$$

BCTRU encryption needs sixteen convolution multiplications and eight polynomial additions. Therefore, the speed of the key generation is faster than that of encryption.

C. DECRYPTION

After receiving E, it is multiplied by from both left and right sides, then

$$\begin{aligned} A &= F * E * F(mod\ q) = F * (pH * \phi + M * K) * F \ \ (mod\ q) \\ &= pF * H * \phi * F + F * M * K * F \ \ (mod\ q) \\ &= pF * F_q^{-1} * G * \phi * F + F * M * U * F_q^{-1} * F \ \ (mod\ q) \\ &= pG * \phi * F + F * M * U \ \ (mod\ q) \end{aligned}$$

Let $B = A\,(mod\ p) = pG * \phi * F + F * M * U \ \ (mod\ p)\,.$
Since the first term is equal to zero modulo p (because it contains p), then

$$B = F * M * U \ \ (mod\ p)\,, \quad F_p^{-1} * B * U_p^{-1} = M\,(mod\ p)$$

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

BCTRU decryption needs thirty two convolution multiplications and twelve polynomial additions. As a result, the speed of encryption is more than twice as fast as that of decryption.

4. Probability of Successful Decryption

The successful decryption of BCTRU depends on the probability of all coefficients of $A = pG * \phi * F + F * M * U$ belongs to the interval $\left[\frac{-q+1}{2}, \frac{q-1}{2}\right]$, which are calculated in the following theorem:

Theorem 4.1. *$Pr\left(|A_{j,\tau}| \leq \frac{q-1}{2}\right) = 2\,\mathcal{N}(\frac{q-1}{2\sqrt{\frac{32p^2 d_g d_\phi d_f}{N} + \frac{32 d_f d_u (p-1)(p+1)}{3}}})$, where $\mathcal{N}$ denotes the normal distribution, and $j, \tau = 0, 1, 2, 3$.*

Proof. To compute this probability, A should be written in a BCTRU form, such that,

$A = pG * \phi * F + F * M * U \ = (A_0, A_1)\,(1,1) + (A_2, A_3)\,(k,1)\,,$
$F = (f_0, f_1)\,(1,1) + (f_2, f_3)\,(k,1)\,,$
$G = (g_0, g_1)\,(1,1) + (g_2, g_3)\,(k,1)\,,$
$U = (u_0, u_1)\,(1,1) + (u_2, u_3)\,(k,1)\,,$
$\phi = (\phi_0, \phi_1)\,(1,1) + (\phi_2, \phi_3)\,(k,1)\,,$
$M = (m_0, m_1)\,(1,1) + (m_2, m_3)\,(k,1)\,,$
$A_0, A_1, A_2, A_3, f_0, f_1, f_2, f_3, g_0, g_1, g_2, g_3, u_0, u_1, u_2, u_3, \phi_0, \phi_1, \phi_2, \phi_3, m_0, m_1$
$, m_2, m_3$ which are polynomials of degree N where

$$\begin{aligned}
A_0 = \ & p\,(g_0\phi_0 f_0 + g_0\phi_2 f_2 + \ g_2\phi_0 f_2 + g_2\phi_2 f_0\ ) + (f_0 m_0 u_0 + f_0 m_2 u_2 + \\
& f_2 m_0 u_2 + f_2 m_2 u_0\ ) = \ [\ A_{0,0},\ A_{0,1},\ A_{0,2},\ \ldots,\ A_{0,N-1}], \\
A_1 = \ & p\,(g_1\phi_1 f_1 + g_1\phi_3 f_3 + \ g_3\phi_1 f_3 + g_3\phi_3 f_1\ ) + (f_1 m_1 u_1 + f_1 m_3 u_3 + \\
& f_3 m_1 u_3 + f_3 m_3 u_1\ ) \ = \ [\ A_{1,0},\ A_{1,1},\ A_{1,2},\ \ldots,\ A_{1,N-1}], \\
A_2 = \ & p\,(g_0\phi_0 f_2 + g_0\phi_2 f_0 + \ g_2\phi_2 f_0 + g_2\phi_2 f_2\ ) + (f_0 m_0 u_0 + f_0 m_2 u_0 + \\
& f_2 m_2 u_0 + f_2 m_2 u_2\ ) \ = \ [\ A_{2,0},\ A_{2,1},\ A_{2,2},\ \ldots,\ A_{2,N-1}], \\
A_3 = \ & p\,(g_1\phi_1 f_3 + g_1\phi_3 f_1 + \ g_3\phi_1 f_1 + g_3\phi_3 f_3\ ) + (f_1 m_1 u_1 + f_1 m_3 u_1 + \\
& f_3 m_1 u_1 + f_3 m_3 u_3\ ) \ = \ [\ A_{3,0},\ A_{3,1},\ A_{3,2},\ \ldots,\ A_{3,N-1}],
\end{aligned}$$

Based on the definition of $L_F, L_M,$ and L_ϕ, the following is obtained:

$$f_j \ = [f_{j,0},\ f_{j,1},\ f_{j,2},\ \ldots,\ f_{j,N-1}]$$

$$g_j = [g_{j,0},\ g_{j,1},\ g_{j,2},\ \ldots,\ g_{j,N-1}]$$

$$\phi_j = [\phi_{j,0},\ \phi_{j,1},\ \phi_{j,2},\ \ldots,\ \phi_{j,N-1}]$$

$Pr\,(f_{j,k} = 1) \ = \ \frac{d_f}{N}\ ,$ and $Pr\,(f_{j,k} = -1) = \frac{d_f - 1}{N} \approx \frac{d_f}{N}$
$Pr\ (f_{j,k} = 0) = 1 - \ \frac{2\ d_f}{N}$
$Pr\,(u_{j,k} = 1) \ = \ \frac{d_u}{N}\ ,$ and $Pr\,(u_{j,k} = -1) = \frac{d_u - 1}{N} \approx \frac{d_u}{N}$
$Pr\ (u_{j,k} = 0) = 1 - \ \frac{2\ d_u}{N}$

$$Pr\,(g_{j,k} = 1) \ = Pr\,(g_{j,k} = -1) \ = \frac{d_g}{N}\ , Pr\ (g_{j,k} = 0) = 1 - \ \frac{2\ d_g}{N},$$

$$Pr\,(\phi_{j,k} = 1) \ = Pr\,(\phi_{j,k} = -1) \ = \frac{d_\phi}{N}\ , Pr\,(\phi_{j,k} = 0) \ = 1 - \ \frac{2\ d_\phi}{N},$$

$$Pr\,(m_{j,k} = \gamma) \ = \frac{1}{p} \qquad \gamma \in \Big[-\ \frac{p}{2}\ ,\ \frac{p}{2}\ \Big], \qquad j, k \ = \ 0, 1, 2, 3.$$

We assume that all $f_{j,\alpha},\ g_{k,\beta}$ and $\phi_{t,\lambda}$ are pairwise independent random variables.

For $\alpha, \beta,\ \lambda = 0, 1, \ldots\ , N-1$,

$$\gamma = \ -\ \frac{p-1}{2},\ \ldots\ , \frac{p-1}{2},\ \text{ and } j, k, t = 0, 1, 2, 3.$$

Therefore,

$$Pr\ (g_{j,\alpha}.\ \phi_{k,\beta}.\ f_{t,\lambda}\ = \mp\ 1)\ =\ \ \frac{8 d_g d_\phi d_f}{N^3},$$

$$Pr\ \ (g_{j,\alpha}.\ \phi_{k,\beta}.\ f_{t,\lambda}\ = 0) = 1 -\ \frac{8 d_g d_\phi d_f}{N^3},$$

$$Pr\,(f_{j,\alpha}.\ m_{k,\beta}.\ u_{t,\lambda}\ = \gamma)\ =\ \frac{4 d_f d_u}{p N^2}\ .$$

Based on the preceding assumptions and after a number of computations, the following is obtained:

$$Var\ (g_{j,\alpha}.\ \phi_{k,\beta}.\ f_{t,\lambda})_y\ = Var(\sum \sum_{\alpha+\beta+\lambda=y(mod\ N)} g_{j,\alpha}.\ \phi_{k,\beta}.\ f_{t,\lambda})$$

$$= \frac{8 d_g d_\phi d_f}{N},$$

$$Var\ (f_{j,\alpha}.\ m_{k,\beta}.\ u_{t,\lambda})_y\ = Var(\sum \sum_{\alpha+\beta+\lambda=y(mod\ N)} f_{j,\alpha}.\ m_{k,\beta}.\ u_{t,\lambda})$$

$$= \frac{d_f d_u\,(p-1)\,(p+1)}{3},$$

$$Var\ \ (A_0,\ \tau) = \ \frac{32 p^2 d_g d_\phi d_f}{N}\ \ +\ \ \frac{32 d_f d_u\,(p-1)\,(p+1)}{3}.$$

Moreover, $Var\ \ (A_1,\ \tau) = Var\ \ (A_2,\ \tau) = Var\ \ (A_3,\ \tau)$ are equal to $\frac{32 p^2 d_g d_\phi d_f}{N}\ \ +\ \ \frac{32 d_f d_u (p-1)(p+1)}{3}$ obtained in a similar manner when the probabilities of all coefficients $A_{0.i},\ \ A_{1.i},\ A_{2.i}\ A_{3.i}$ are belong to $[\frac{-q+1}{2}\ ,\ \frac{q+1}{2}]$. Therefore, the successful decryption is performed to obtain,

$$Pr\left(|A_{i,\tau}|\ \leq \frac{q-1}{2}\ \right)\ = Pr\left(-\frac{q-1}{2} \leq A_{j,\tau} \leq \frac{q-1}{2}\ \right)\ = 2\,\mathcal{N}\ (\frac{q-1}{2\sigma}),$$

where $\sigma = \sqrt{\frac{32 p^2 d_g d_\phi d_f}{N}\ \ +\ \ \frac{32 d_f d_u (p-1)(p+1)}{3}}$,

$i = 0, 1, 2, 3$ and $\tau = 0, 1, \ldots, N-1$

□

Corollary 4.1. *1. The probability for any of the messages* M_0, M_1, M_2 *and* M_3 *to be successfully decrypted is*

$$(2\mathcal{N}\ (\frac{q-1}{2\sqrt{\frac{32p^2d_g d_\phi d_f}{N} + \frac{32d_f d_u(p-1)(p+1)}{3}}}) - 1)^N$$

2. The probability for both of the messages M_0, M_1, M_2 *and* M_3 *to be successfully decrypted is*

$$(2\mathcal{N}\ (\frac{q-1}{2\sqrt{\frac{32p^2d_g d_\phi d_f}{N} + \frac{32d_f d_u(p-1)(p+1)}{3}}}) - 1)^{4N}.$$

5. Security Analysis

To prove the security of the BCTRU cryptosystems, some of the known attacks are discussed such as brute force attack, alternate keys attack, multiple transmission attacks and finally, lattice-based attack.

A. ALTERNATE KEY ATTACK

The main objective of this attacker is to find the alternate private keys in order to decrypt the received encrypted media. Therefore, the attacker task is an attempt to find the following keys:

$$\acute{F} = (\acute{f}_0, \acute{f}_1)(1,1) + (\acute{f}_2, \acute{f}_3)(k,1)$$
$$\acute{G} = (\acute{g}_0, \acute{g}_1)(1,1) + (\acute{g}_2, \acute{g}_3)(k,1)$$
$$\acute{U} = (\acute{u}_0, \acute{u}_1)(1,1) + (\acute{u}_2, \acute{u}_3)(k,1)$$

alternate to F, G and U respectively, such that $\acute{F}$ must have multiplicative inverse modulo p and q also, $\acute{U}$ must have multiplicative inverse modulo p .

Thus, an attacker to BCTRU needs twelve polynomials $\acute{f}_0$, $\acute{f}_1$, $\acute{f}_2$, $\acute{f}_3$, $\acute{g}_0$, $\acute{g}_1$, $\acute{g}_2$ $\acute{g}_3$, $\acute{u}_0$, $\acute{u}_1$, $\acute{u}_2$, $\acute{u}_3$, with the same properties of polynomials f_0, f_1, f_2, f_3, g_0 , g_1, g_2, g_3, u_0, u_1, u_2, u_3 respectively. However, an attacker to NTRU only needs extra attempts to find the private key (in this case twelve) than those used to decrypt NTRU, which needs only one polynomial in L_F with the same properties of the private key.

B. BRUTE FORCE ATTACK

An attacker to BCTRU that knows the public parameters, as well as the public key

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

which are equivalent to the following hidden equations:

$$FH = G \mod (q), \tag{1}$$

$$KF = U \mod (q), \tag{2}$$

All the polynomials $F \epsilon L_F$ (hard mathematical problem) are tested and determine if Eqs. (1) and (2) turn into bicartesian algebra with small coefficients until the private key is found. The size of the subset L_F is calculated as follows:

$$|L_F| = \left(\frac{N!}{(d_f!)^2 (N-2d_f)!}\right)^4.$$

Accordingly, the number of all attempts to find the private keys F, G and U is equal to

$$\frac{N!^{12}}{(d_f! d_g! d_u!)^2 ((N-2d_f)!(N-2d_g)!(N-2d_u)!)^4}.$$

C. MULTIPLE TRANSMISSION ATTACK

This attack is based on sending a single message several times with the same public key. In BCTRU, when the sender sends one message M many times using different âblinding values of ϕ and the same public keys H, K, then the attacker âcan recover a large part of the message M . Suppose the sender transmits âthe message M in the form

$$E_i = pH * \phi_i + M * K \ (mod\ q)$$

for $i = 1, 2, \ldots, s$.â Then, the attacker can compute

$$H^{-1}(E_i - E_1) \ (mod\ q).$$

Therefore, the attacker can ârecovere

$$(R_i - R_1) \ (mod\ q).$$

However, the coefficients of R are âsmall such that, the attacker recovers exactly $R_i - R_1$. Thus, the attacker âcan recover many coefficients of R_1. BITRU is multidimensional and is âtherefore more resistant to attacks than NTRU.â

D. ANALYZING LATTICE ATTACKS AGAINST BCTRU

The majority of some attacks to threaten BCTRU has been investigated to prove its security. The most powerful for such type of cryptosystem that based on polynomial algebra is the lattice attack, in which the shortest vector in the lattice vector space of the proposed cryptosystem represents the private key, which can be found by approximate solution for the corresponding vector matrix. Some of these attacks are discussed as follows.
The BCTRU cryptosystem is broken when the attacker succeeds to find F or G, this means finding the shortest vector in the BCTRU lattice, which satisfies $F * H = G$ and $K * F = I$ and as follows:â

$$\begin{aligned}
f_0h_0 &+ f_2h_2 &&= g_0 + ql_0\\
f_1h_1 &+ f_3h_3 &&= g_1 + ql_1\\
f_0h_2 &+ f_2h_0 &&= g_2 + ql_2\\
f_1h_3 &+ f_3h_1 &&= g_3 + ql_3\\
f_0k_0 &+ f_2k_2 &&= i_0 + qw_0\\
f_1k_1 &+ f_3k_3 &&= i_1 + qw_1\\
f_0k_2 &+ f_2k_0 &&= i_2 + qw_2\\
f_1k_3 &+ f_3k_1 &&= i_3 + qw_3
\end{aligned}$$

We can represent the polynomials h_0, h_1, h_2, h_3 and k_0, k_1, k_1, k_3 in the following matrices respectively â

$$(H_i)_{N\times N} = \begin{pmatrix}
h_{i,o} & h_{i,1} & h_{i,2} & \dots & h_{i,N-1}\\
h_{i,N-1} & h_{i,0} & h_{i,1} & \dots & h_{i,N-2}\\
h_{i,N-2} & h_{i,N-1} & h_{i,0} & \dots & h_{i,N-3}\\
\vdots & \vdots & & \vdots & \vdots\\
h_{i,2} & h_{i,3} & h_{i,4} & \dots & h_{i,1}\\
h_{i,1} & h_{i,2} & h_{i,3} & \dots & h_{i,0}
\end{pmatrix}$$

$$(K_i)_{N\times N} = \begin{pmatrix}
k_{i,o} & k_{i,1} & k_{i,2} & \dots & k_{i,N-1}\\
k_{i,N-1} & k_{i,0} & k_{i,1} & \dots & k_{i,N-2}\\
k_{i,N-2} & k_{i,N-1} & k_{i,0} & \dots & k_{i,N-3}\\
\vdots & \vdots & & \vdots & \vdots\\
k_{i,2} & k_{i,3} & k_{i,4} & \dots & k_{i,1}\\
k_{i,1} & k_{i,2} & k_{i,3} & \dots & k_{i,0}
\end{pmatrix}$$

Depending on the above, we can constitute representing by $\pounds^H_{BCTRU}$ â and

$\pounds^K_{BCTRU}$ of dimension $4N$ are spanned by the ârows of matrices

$$(M^H_{4N\times 4N}) = \begin{pmatrix} I_{2N\times 2N} & H_0 & H_1 \\ & H_1 & H_0 \\ 0_{2N\times 2N} & qI_{2N\times 2N} & \end{pmatrix}$$

and

$$(M^K_{4N\times 4N}) = \begin{pmatrix} I_{2N\times 2N} & K_0 & K_1 \\ & K_1 & K_0 \\ 0_{2N\times 2N} & qI_{2N\times 2N} & \end{pmatrix}$$

where I denoted identity matrix , 0 denoted zero matrix with âbicartesian entries and
$H_0 = (h_{0,0} + h_{0,1}x + \cdots + h_{0,N-1}x^{N-1}, h_{1,0} + h_{1,1}x + \cdots + h_{1,N-1}x^{N-1})$
$K_0 = (k_{0,0} + k_{0,1}x + \cdots + k_{0,N-1}x^{N-1}, k_{1,0} + k_{1,1}x + \cdots + k_{1,N-1}x^{N-1})$
Assuming $d = d_f = d_g = d_u = d_\phi \approx \frac{N}{3}$. â We have $||\mathbf{M}^H_{4N\times 4N}|| = 2q^{4N}$, based on the âshortest vector problem to find the length of the shortest non zero vector âwith respect to H is equal to $0.48\sqrt{N}q(2)^{\frac{1}{4N}}$.
By the same âaway, the length of the shortest non zero vector with respect to K is equal âto $0.48\sqrt{N}q(2)^{\frac{1}{4N}}$. Therefore, the attacker is trying to find âtwo non zero vector every one of length $0.48\sqrt{N}q(2)^{\frac{1}{4N}}$. âHence, BCTRU is good resistance against lattice attacks. â

6. Conclusions

In this paper, we introduced BCTRU public key cryptosystem that depends on new generated bicartesian algebra to enhance the security through discussing of some attacks. We demonstrated that, the security of BCTRU is four times mor than NTRU, and it shows certain resistance against attacks.
When designing NTRU like cryptosystems, the most crucial point that should be taken in the consideration is the non-commutative calculation during the encryption and decryption process, which led to design a secure cryptosystem against the lattice-based attacks because the attacker needs to try two non-zero vectors, each of length $0.48\sqrt{N}q(2)^{\frac{1}{4N}}$. Also, BCTRU has the ability to encrypt four messages of length N in each round, which granted it a good speed facility that is important for many application.

References

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 Journal of Mathematical Sciences*, 11:29–43.

Alsaidi, N., Saed, M., Sadiq, A., and Majeed, A. A. (2015). An improved ntru cryptosystem via commutative quaternions algebra. In *Proceedings of the International Conference on Security and Management (SAM)*, page 198. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Alsaidi, N. M. and Yassein, H. R. (2016). BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra. *International Journal of Advanced Computer Science and Applications*, 7(11):1–6.

An, S., Kim, S., Jin, S., Kim, H., and Kim, H. (2018). Single trace side channel analysis on ntru implementation. *Applied Sciences*, 8(11):2014.

Atani, R. E., Atani, S. E., and Karbasi, A. H. (2018). Netru: A non-commutative and secure variant of ctru cryptosystem. *ISeCure*, 10(1).

Atici, A. C., Batina, L., Fan, J., Verbauwhede, I., and Yalcin, S. B. O. (2008). Low-cost implementations of NTRU for pervasive security. In *Application-Specific Systems, Architectures and Processors, 2008. ASAP 2008. International Conference on*, pages 79–84. IEEE.

Coglianese, M. and Goi, B.-M. (2005). MaTRU: A new NTRU-based cryptosystem. In *International Conference on Cryptology in India*, pages 232–243. Springer.

Gaborit, P., Ohler, J., and Solé, P. (2002). *CTRU, a polynomial analogue of NTRU*. PhD thesis, INRIA.

Hoffstein, J., Pipher, J., and Silverman, J. H. (1998). Ntru: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium*, pages 267–288. Springer.

Jarvis, K. and Nevins, M. (2015). ETRU: NTRU over the Eisenstein Integers. *Designs, Codes and Cryptography*, 74(1):219–242.

Kumar, S., Pal, S. K., et al. An Improved Post-Quantum Cryptographic Scheme Based on NTRU. *International Journal of Computer Applications Technology and Research*, 2(4):499–meta.

Malekian, E. and Zakerolhosseini, A. (2010). OTRU: A non-associative and high speed public key cryptosystem. In *Computer Architecture and Digital Systems (CADS), 2010 15th CSI International Symposium on*, pages 83–90. IEEE.

Malekian, E., Zakerolhosseini, A., and Mashatan, A. (2009). QTRU: A Lattice Attack Resistant Version of NTRU PKCS Based on Quaternion Algebra. *preprint, Available from the Cryptology ePrint Archive: http://eprint. iacr. org/2009/386. pdf.*

Pan, Y. and Deng, Y. (2011). A general NTRU-Like framework for constructing lattice-based public-key cryptosystems. In *International Workshop on Information Security Applications*, pages 109–120. Springer.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod ð. *Mathematics of computation*, 44(170):483–494.

Suri, P. and Puri, P. (2007). Application of LFSR with NTRU Algorithm. In *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*, pages 369–373. Springer.

Thakur, K. and Tripathi, B. (2016). BTRU, A Rational Polynomial Analogue of NTRU Cryptosystem. *International Journal of Computer Applications, Foundation of Computer Science (FCS), NY, USA*, 145(12).

Vats, N. (2009). NNRU, a noncommutative analogue of NTRU. *arXiv preprint arXiv:0902.1891.*

Yassein, H. R. and Al-Saidi, N. M. (2016). HXDTRU Cryptosystem Based On Hexadecnion Algebra. In *Proceeding of the 5th International Cryptology and Information Security Conference, Kota Kinabalu, Malaysia.*

Yassein, H. R. and Al-Saidi, N. M. (2017). A comparative performance analysis of NTRU and its variant cryptosystems. In *Current Research in Computer Science and Information Technology (ICCIT), 2017 International Conference on*, pages 115–120. IEEE.