# BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra

Nadia M.G. Alsaidi
Department of applied Sciences
University of Technology
Baghdad, Iraq

Hassan R. Yassein
Department of Mathematics
College of Education, Al-Qadisiyah University
AL-Dewaniya, Iraq

***Abstract*—New terms such as closest vector problem (CVP) and the shortest vector problem (SVP), which have been illustrated as NP-hard problem, emerged, leading to a new hope for designing public key cryptosystem based on certain lattice hardness. A new cryptosystem called NTRU is proven computationally efficient and it can be implemented with low cost. With these characteristics, NTRU possesses advantage over others system that rely on number-theoretical problem in a finite field (e.g. integer factorization problem or discrete logarithm problem). These advantages make NTRU a good choice for many applications. After the adaptation of NTRU, many attempts to generalize its algebraic structure have appeared. In this study, a new variant of the NTRU public key cryptosystem called BITRU is proposed. BITRU is based on a new algebraic structure used as an alternative to NTRU-mathematical structure called binary algebra. This commutative and associative. Establishing two public keys in the proposed system has distinguished it from NTRU and those similar to NTRU cryptosystems. This new structure helps to increase the security and complexity of BITRU. The clauses of BITRU, which include key generation, encryption, decryption, and decryption failure, are explained in details. Its suitability of the proposed system is proven and its security is demonstrated by comparing it with NTRU.**

***Keywords*—NTRU; BITRU; polynomial ring; binary algebra**

## I. INTRODUCTION

With the rapid development of wireless communication system widely deployed in recent years, security has become a crucial issue. Cryptography to solve this issue; it is used to meet the requirements of data and network communication security, namely, confidentiality, integrity, authentication, and non-repudiation [1]. The designing of high-performed algorithms is greatly demanded, which leads to security risk and heightens the need for analysis and investigation. Many public key cryptosystems have been developed since the Diffie Hellman seminal paper [2] was presented in 1976. Most of these cryptosystem are based on two mathematical hard problems: factorization and discrete logarithm problems (e.g., RSA [3], ElGamal cryptosystem [4], ECC [5], and many others [6]). From a practical perspective, most of these systems are costly because of their space complexity and high computation. This problem can be resolved by looking for new fast cryptosystems based on different hard problems.

The number theory research unit (NTRU) public key cryptosystem is a new generation of public key cryptosystems based on lattice hard problem introduced in 1996 by three mathematicians, namely Jeffery Hoffstein, Joseph Silverman, and Jill Piper [7]. It is the first public key cryptosystem that does not depend on the factorization and discrete algorithm problems aforementioned mathematical problems. Unfortunately, similar to many other public key systems, its security is unguaranteed although it is closely based on lattice problem. The basic collection of objects used by the NTRU public key cryptosystem occurs in a truncated polynomial ring of degree $N-1$ with integer coefficients belonging to $Z[x]/(x^N-1)$. NTRU is faster and has significantly smaller keys than the RSA and ECC cryptosystem.

Many researchers have improved the performance of NTRU by developing of its algebraic structure. In 2002, Gaborit et al. [8] introduced a NTRU-like cryptosystem called CTRU by replacing the base ring of the NTRU with a polynomial ring over a binary field F2[x]. They proved that their system is successfully decrypted. In 2005, Kouzmenko [9] showed that CTRU is weak under a time attack and proposed the GNTRU cryptosystem based on Gaussian integers Z[i] rather Z or $F_2[x]$. In the same year, Coglianese et al. [10] introduced an analog to the NTRU cryptosystem called MaTRU. MaTRU is based on a ring of all square matrices with polynomial entries. In 2009, Malekian et al. introduced the QTRU cryptosystem based on quaternion algebra [11]. They also introduced the OTRU cryptosystem in 2010 based on Octonion algebra [12]. Afterward, Vats [13] presented a new a non-commutative NTRU analog. His system 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 $Z[x]/(x^N-1)$. He proved that the speed is improved by a factor of $O(k^{1.624})$ over NTRU. In 2011, N. Zhao and S. Su [14] improved the algorithm of seeking the inverse of polynomial in NTRU. Also, they designed a new algorithm to judge whether the polynomial is invertible or not by computing $\gcd(\det(A), w)$. If it equals to 1, it is invertible, otherwise, the polynomial has no inverse in modulo w, and this algorithm use a matrix of an *N*–cyclic (A) corresponding to coefficients of polynomial of order N.

In 2012, Y. Bin Pan and Y. Deng in [15] focused on the technique of hiding the trapdoor of NTRU cryptosystem. So, they presented general NTRU – like framework. This framework has constructed new lattice based public key cryptosystem to find some particular kinds of easy closest vector problems (CVPs). They proposed a new lattice based public key cryptosystem as an application of their framework.

In 2013, Jarvis et al. [16] proposed a new framework based on the ring of a cubic root of unity known as the Eisenstein ring Z[w], whose coefficient integers belong to Z. They called it ETRU.

In 2014, P. Gauravaram, H. Narumanchi and N. Emmadi [17] present our analytical study on the implementation of NTRU encryption scheme which serves as a guideline for security practitioners who are novice to lattice based cryptographic implementations. In the same year, D. Cabarcas, P. Weiden, and J. Buchmann in [18] focused on the relationship between two embedding's ideals into geometric space and the shortest vector problem in principal ideal lattice.

In 2015, S. C. Batson in [19] focused on the relationship between two embedding's ideals into geometric space and the shortest vector problem in principal ideal lattice. In the same year, Alsaidi et al. [20] introduced the CQTRU cryptosystem based on commutative quaternion algebra.

In 2016, Thakur and Tripathi introduced BTRU, a new NTRU-like cryptosystem that replaces Z by a ring of polynomial with one variable over a rational field. They conveyed faster than NTRU [21]. In the same year, Yassein and Alsaidi [22] introduced an analog to the NTRU cryptosystem called HXDTRU, where the operations occur in the specially designed high-dimensional algebra called hexadecnion algebra.

In this study, we present a new multidimensional public key cryptosystem BITRU based on binary algebra. The mathematical structure of the proposed system results in two public keys, which in turn helps increase the BITRU security in comparison to its equivalents with identical structure.

This work is organized as follows. The summary of the original NTRU based on the arbitrary polynomial ring $Z[x]/(x^N - 1)$ is briefly introduced in Section II. The binary algebra used to construct the new NTRU-like cryptosystem, with its algebraic structure is provided in Section III. An analog of the NTRU cryptosystem called BITRU is proposed in Section IV. The successful decryption of the proposed system is proven through two propositions in Section V. The security and complexity analysis of the BITRU is discussed in Section VI. The study is concluded in Section VII.

## II. NTRU Cryptosystem

A simple description of the NTRU cryptosystem is explained in this section. This cryptosystem depends on the addition and multiplication in the ring of a truncated polynomial of degree N denoted by $K = Z[X]/(X^N - 1)$, where N is a prime. Let $K_p(x) = (Z/pZ)[x]/(X^N - 1)$ and $K_q(x) = (Z/qZ)[x]/(X^N - 1)$denotes the rings of truncated polynomial modulo p and q respectively, where p and q are integers number, such that, $\gcd(p, q) = 1$ and q is significantly larger than p. Let $d_f$, $d_g$, $d_m$, and $d_\phi$ be constant integers less than N. Let $L_f, L_g, L_m$ and $L_\phi \subset R$ be defined in Table 1.

TABLE I. Definition of the Public NTRU Parameters

| Notation | Definition |
|---|---|
| $L_f$ | {f$\epsilon$ R \| f has $d_f$ coefficients equal to +1, ($d_f - 1$) equal to -1, the rest 0} |
| $L_g$ | {g$\epsilon$ R \| g has $d_g$ coefficients equal to +1, $d_g$equal to -1, the rest 0} |
| $L_m$ | {m$\epsilon$ R \| coefficients of m are chosen modulo p, between $-p/2$ and $p/2$} |
| $L_\phi$ | {$\phi\epsilon$ R \| $\phi$ has $d_\phi$ coefficients equal to +1, $d_\phi$ equal to -1, the rest 0} |

A rough outline of the key creation, encryption, and decryption processes is presented as follows:

### A. Key Generation

Public and private keys are generated by having the sender initially randomly choose two small polynomials f and g from $L_f$ and $L_g$, respectively, such that f must be invertible modulo p and q denoted by $F_p$ and $F_q$, respectively, where $f * F_p = 1$ and $f * F_q = 1$. A new polynomial f can be chosen if probable f is not invertible. Parameters f and g must be kept confidential. The public key h is computed in the following manner:

$$h = F_q * g \pmod q,$$

where f, $F_p$, $F_q$, and g are kept confidential (i.e., sender private key).

### B. Encryption

Encryption is performed as follows:

For any given message $m \in L_m$, the public key h is used to compute the ciphertext e, such that,

$e = p\phi * h + m \pmod q$, where $\phi \in L_\phi$ is randomly chosen.

### C. Decryption

Decryption is performed after the second party receives e. The receiver must find a, such that

$a = f * e \pmod q$, to derive the message. The coefficients of $a \epsilon K_q$ should be adjusted to lie in the interval $\left(-\frac{q}{2}, \frac{q}{2}\right]$, thus the unnecessary reduction of mod q.

$$\begin{aligned} a &= f * e \pmod q \\ &= f * (p\phi * h + m) \pmod q \\ &= pf * \phi * h + f * m \pmod q \\ &= pf * \phi * (F_q * g) + f * m \pmod q \\ &= p\phi * g + f * m \pmod q \end{aligned}$$

The resulting polynomial $p\phi * g + f * m$ obtains coefficients in the interval $(-q/2, q/2]$. It does not change if its coefficients are reduced to modulo q. The receiver computes the polynomial as follows:

$$b = a \pmod p$$

$$= p\phi * g + f * m \pmod p$$
$$= f * m \pmod p$$

The result is then multiplied by $F_p$ to construct message m.

$$F_p * b = F_p * f * m \pmod p = m \pmod p,$$

the resulting coefficients are adjusted within the interval $[-q/2, q/2)$.

## III. Binary Algebra

In this section, a real binary algebra and its properties are introduced. It is a vector space of two dimensions over the real numbers R defined as follows:

$BN_R = \{a + bj \,|a, b \in R\}$, where $j^2 = 1$ and R is the set of real numbers. The operation on this algebra is defined as follows:

Let $w_1, w_2 \in BN_R$, such that $w_1 = a_1 + b_1 j$ and $w_2 = a_2 + b_2 j$, the addition is then defined by

$w_1 + w_2 = (a_1 + a_2) + (b_1 + b_2)j$, the multiplication is then defined by

$w_1 . w_2 = (a_1 * a_2 + b_1 * b_2) + (a_1 * b_2 + b_1 * a_2)j$, and for any scalar r, the scalar multiplication is defined by $rw = ra + (rb)j$. This algebra is associative and commutative.

Every non zero element in $BN_R$ $a + bj$ contains a unique multiplication inverse that is given by

$(a + bj)^{-1} = (\frac{b^2}{a(a^2-b^2)} + \frac{1}{a} - \frac{b}{a^2-b^2} j)$ such that $a^2 \neq b^2$.

Let F be a finite field of $\text{char}(F) \neq 2$. We define the binary algebra $BN_F$ over F as follows: $BN_F = \{ a + bj \,|a, b \in F \}$, with addition, scalar multiplication, multiplication, and square norm as defined in the real binary algebra. We now consider the truncated polynomial ring

$K = Z[x]/(x^N - 1)$, $K_p(x) = (Z/pZ)[x]/(x^N 1)$ and $K_q(x) = (Z/qZ)[x]/(x^N - 1)$.

We define three binary algebras $\psi$, $\psi_p$, and $\psi_q$ as follows:

$$\Psi = \{ f_0(x) + f_1(x)j \mid f_0, f_1 \in K \}$$
$$\Psi p = \{ f_0(x) + f_1(x)j \mid f_0, f_1 \in K_p \}$$
$$\Psi q = \{ f_0(x) + f_1(x)j \mid f_0, f_1 \in K_q \}.$$

Let $\phi_1$ and $\phi_2 \in \psi_p$ or $\psi_q$, such that:

$$\phi_1 = f_0(x) + f_1(x)j$$
$$\phi_2 = g_0(x) + g_1(x)j,$$

where $f_0, f_1$ and $g_0, g_1 \in K_p$ or $K_q$.

The addition of $\phi_1$ and $\phi_2$ is performed by adding the corresponding coefficients mod p or mod q, such that $\phi_1 + \phi_2 = (f_0(x) + g_0(x)) + (f_1(x) + g_2(x))j$.

The multiplication of $\phi_1$ and $\phi_2$ is defined as follows:

$$\phi_1 * \phi_2 = (f_0 * g_0 + f_1 * g_1) + (f_0 * g_1 + f_1 * g_0)j,$$

where $*$ is the convolution product, the scalar multiplication is defined by $r\phi_1 = rf_0(x) + rf_1(x)j$ for any scalar $r$, and the same multiplication inverse is defined for the $BN_R$.

## IV. Proposed BITRU Cryptosystem

The BITRU cryptosystem is set up by integers N, p, and q such that N is a prime, p and q are relatively prime and q is significantly larger than p. It also depends on five subsets define as follows

Definition 1: The subsets $L_f, L_w, L_m, L_\phi$ and $L_r \subset \Psi$ are called the subsets of BITRU defined as follows:

$L_f = \{f_0(x) + f_1(x)j \in \Psi \,|f_i(x)$ has $d_f$ coefficients equal to 1, $d_f - 1$ equal to $-1$, the rest are $0\}$,

$L_w = \{w_0(x) + w_1(x)j \in \Psi | w_i(x)$ has $d_w$ coefficients equal to 1, $d_w - 1$ equal to $-1$, the rest are $0\}$,

$L_m = \{m_0(x) + m_1(x)j \in \Psi \,|m_i(x)$ are chosen modulo p, between $-p/2$ and $p/2\}$,

$L_\phi = \{\phi_0(x) + \phi_1(x)j \in \Psi \,|\phi_i(x)$ has $d_\phi$ coefficients equal to 1, $d_\phi$ equal to $-1$, the rest are $0\}$ and

$L_r = \{r_0(x) + r_1(x)j \in \Psi \,|r_i(x)$ has $d_r$ coefficients equal to +1, $d_r$ equal to $-1$, the rest are $0\}$,

where $d_f, d_w, d_\phi$ and $d_r$ are also constant parameters similar to those defined in the NTRU.

The BITRU cryptosystem is introduced based on the binary algebra and defined through four main phases described as follows:

### A. Key Generation

The public and private keys are generated by making the sender randomly choose $f, g \in L_f, w \in L_w$, and $\phi \in L_\phi$, such that, f and g must have multiplicative inverse modulo p and q denoted by $f_p, f_q$ and $g_p, g_q$ respectively, and w have multiplicative inverse modulo p denoted by $w_p$.

The public keys are computed as follows:

$h = \phi f_q \pmod q$ ……. (1)
$k = g_q w \bmod (q)$ ……. (2)

where $f, g, \phi$, and w are the private keys.

Algorithm 1 is designed for generating the first key set $h = [h_0, h_1]$

Algorithm 1: Ceatekey $[h_0, h_1]$

Input: $p, q, n, f_0, f_1, g_0, g_1$

1- $[Fq, Fq1] = \text{bininvq}\ (p, q, n, f_0, f_1)$
2- $[c_0, c_1] = \text{multbin}\ (g_0, g_1, Fq, F1, n, p)$
3- for i=1 to n
4- if $c_0(i) < 0$
5- $c_0(i) = c_0(i) + q$
6- end if
7- $c_0(i) = c_0(i) * p \pmod q$
8- end for
9- $h_0 = c_0$
10- for i = 1 to n

```
11-    if c1(i) < 0
12-      c1(i) = c1(i) + q
13-    end if
14-    c1(i) = c1(i) * p(mod q)
15- end for
16- h1 = c1
```

Algorithm 2 that is designed for generating of the second set $k = [k_0, k_1]$

Algorithm 2: generatekey $[k_0, k_1]$

Input: $p, q, n, f_0, f_1, g_0, g_1$

```
1-  [Fq, Fq1] = bininvq (p, q, n, f0, f1)
2-  [c0, c1] = multbin (g0, g1, Fq, F1, n, p)
3-  for i=1 to n
4-      if c0(i) < 0
5-        c0(i) = c0(i) + q
6-      end if
7-      c0(i) = c0(i) * p(mod q)
8-  end for
9-  k0 = c0
10- for i = 1 to n
11-    if c1(i) < 0
12-      c1(i) = c1(i) + q
13-    end if
14-    c1(i) = c1(i) * p(mod q)
15- end for
16- k1 = c1
```

*B. Encryption*

At the beginning of encryption, message m is converted to the binary algebra form, such that $m = m_0(x) + m_1(x)i$, where $m_i(x) \epsilon L_m$.

We choose $r \epsilon L_r$ which required the blinding value to encrypt the message $m \epsilon L_m$:

$$e = pr * h + m * k \,(\text{mod } q) \qquad \ldots\ldots\ldots (3)$$

Algorithm 1 is designed for encryption process

Algorithm 3: encryp $[e_0, e_1]$

Input: $n, m, q, m_0, m_1, h_0, h_1, k_0, k_1, r_0, r_1$

```
1- x = multbin(r0, r1, h0, h1, n, m)
2- y = multbin (m0, m1, k0, k1, n, m)
3- e0 = x mod q
4- e1 = y mod q
```

*C. Decryption*

After receiving e, it is left-multiplied by g and right-multiplied by f. Therefore,

$$a = g * e * f (\text{mod } q) \qquad \ldots\ldots\ldots (4)$$

where the coefficients of the polynomial a lie in the interval of $(-q/2 \text{ to } q/2]$.

$$b = a \,(\text{mod } p)$$

$$= w * m * f \,(\text{mod } p)$$

Compute $d = w_p * b * f_p \,(\text{mod } p)$.

Algorithm 4 that is designed for decryption

Algorithm 4: decryp $[d_0, d_1]$

Input: $n, p, q, f_0, f_1, g_0, g_1, w_0, w_1, e_0, e_1$

```
1-  [u0, u1] = multbin(g0, g1, e0, e1, n, q)
2-  [v0, v1] = multbin (u0, u1, f0, f1, n, q)
3-  [Fp0, Fp1] = bininvp (f0, f1, n, q)
4-  [wp0, wp1] = bininvp (w0, w1, n, q)
5-  for i=1 to n
6-      if v0(i) < 0
7-        v0(i) = v0(i) + q
8-      end if
9-    if v0(i) > (q/2)
10-     v0(i) = v0(i) − q
11-   end if
12- end for
13- for i=1 to n
14-     if v1(i) < 0
15-       v1(i) = v1(i) + q
16-     end if
17-     if v1(i) > (q/2)
18-       v1(i) = v1(i) − q
19-     end if
20- end for
21- [s0, s1] = multbin (w0, w1, v0, v1n, p)
22- [t0, t1] = multbin (s0, s1, Fp0, Fp1, n, p)
23- d0 = t0, d1 = t1
```

## V. SUCCESSFUL DECRYPTION

Proposition: The polynomial d is computed by the receiver, and it is equal to the sender plaintext m.

Proof: $a = g * e * f \,(\text{mod } q)$

$$= g(pr * h + k * m) f \,(\text{mod } q) \qquad \text{from (3)}$$

$$= pg * r * h * f + g * k * m * f \,(\text{mod } q)$$

$$= pg * r * \phi * f_q * f + g * g_q * w * m * f \,(\text{mod } q)$$

from (1) and (2)

$$= pg * r * \phi + w * m * f \,(\text{mod } q).$$

Let $b = a \,(\text{mod } p)$

$$= pg * r * \phi + w * m * f \,(\text{mod } p).$$

The first term is equal to zero modulo p because it contains p.

$$b = w * m * f \,(\text{mod } p).$$

Then $d = w_p * b * f_p \,(\text{mod } p)$.

$$= w_p * w * m * f * f_p \,(\text{mod } p)$$

$$= m \,(\text{mod } p). \qquad \square$$

## VI. LATTICE-BASED ATTACKS

To prove the security of BITRU, different attacks have been investigated to show that they are without major effects. In such cryptosystems that based on polynomial ring, the lattice is defined from the relation between the public key and the private key, where the private key represents the shortest vector in this lattice and can be found by solving the approximate matrix for that vector. The attacker must recover the private keys f and g from the public keys h and k, respectively, to attack BITRU. This move is equivalent to finding the shortest vector in the BITRU lattice denoted by $\mathcal{L}_{\mathrm{BITRU}}$.

The attacker first spreads $hf = \phi \pmod q$, $gk = w \pmod q$ as follows:

$$h_0 * f_0 + h_1 * f_1 = \phi_0 + qu_0$$
$$h_0 * f_1 + h_1 * f_0 = \phi_1 + qu_1$$

and

$$g_0 * k_0 + g_1 * k_1 = w_0 + qv_0$$
$$g_0 * k_1 + g_1 * k_0 = w_1 + qv_1.$$

All the polynomials $h_0, h_1$ and $k_0, k_1$ can be represented in their matrix isomorphic representation as follows:

$$(H_i)_{N\times N}=\begin{bmatrix} h_{j,0} & h_{j,1} & \dots & h_{j,N-1} \\ h_{j,N-1} & h_{j,0} & \dots & h_{j,N-2} \\ h_{j,N-2} & h_{j,N-1} & \dots & h_{j,N-3} \\ \vdots & & \ddots & \vdots \\ h_{j,2} & h_{j,3} & \dots & h_{j,1} \\ h_{j,1} & h_{j,2} & \dots & h_{j,0} \end{bmatrix}$$

and

$$(K_i)_{N\times N}=\begin{bmatrix} k_{j,0} & k_{j,1} & \dots & k_{j,N-1} \\ k_{j,N-1} & k_{j,0} & \dots & k_{j,N-2} \\ k_{j,N-2} & k_{j,N-1} & \dots & k_{j,N-3} \\ \vdots & & \ddots & \vdots \\ k_{j,2} & k_{j,3} & \dots & k_{j,1} \\ k_{j,1} & k_{j,2} & \dots & k_{j,0} \end{bmatrix} \quad j = 0,1$$

Therefore, $\mathcal{L}_{\mathrm{BITRU}}$ represented by $\mathcal{L}^{h}_{\mathrm{BITRU}}$ and $\mathcal{L}^{k}_{\mathrm{BITRU}}$ of dimension 8N are spanned by the rows of matrices

$$\mathcal{M}^{h}_{4N\times 4N} = \begin{bmatrix} I_{2Nx2N} & H_{2Nx2N} \\ 0_{2Nx2N} & qI_{2Nx2N} \end{bmatrix}$$

and

$$\mathcal{M}^{k}_{4N\times 4N} = \begin{bmatrix} I_{2Nx2N} & K_{2Nx2N} \\ 0_{2Nx2N} & qI_{2Nx2N} \end{bmatrix} \text{ respectively,}$$

where I denoted the identity matrix, qI denotes q times the identity matrix, 0 denotes zero matrix, and H, K are described as follows:

$$H_{2Nx2N} = \begin{bmatrix} h_0 & h_1 \\ -h_1 & -h_0 \end{bmatrix}$$

$$K_{2Nx2N} = \begin{bmatrix} k_0 & k_1 \\ -k_1 & -k_0 \end{bmatrix}$$

Therefore, the vectors $(\phi_0, \phi_1, f_0, f_1)$ and $(g_0, g_1, w_0, w_1)$ belong to $\mathcal{L}^{h}_{\mathrm{BITRU}}$ and $\mathcal{L}^{k}_{\mathrm{BITRU}}$, respectively. A short vector in $\mathcal{L}^{h}_{\mathrm{BITRU}}$ and $\mathcal{L}^{k}_{\mathrm{BITRU}}$ can be found by a lattice reduction algorithm, which demonstrates that BITRU can resist lattice attacks significantly more than the NTRU. For simplicity, we assume that $d = df = d\phi = dw = dr \approx N/3$ because the determinant $\mathcal{L}^{h}_{\mathrm{BITRU}}$ is equal to the determinant of $\mathcal{M}^{h}_{4N\times 4N}$ which is an upper triangle matrix, and that its determinant is equal to $q^{2N}$, $\|(\phi_0, \phi_1, f_0, f_1)\| \approx \sqrt{8d} \approx 1.63\sqrt{N}$. The Gaussian heuristic expected that the length of the shortest nonzero vector is calculated as $\delta(\mathcal{L}^{h}_{\mathrm{BITRU}}) = \sqrt{\frac{2N}{\pi e}}\sqrt{q} \approx 0.48\sqrt{Nq}$. Also $\frac{\|(\phi_0,\phi_1,f_0,f_1)\|}{\delta} = \frac{1.63\sqrt{N}}{0.48\sqrt{Nq}} \approx \frac{3.39}{\sqrt{q}}$, hence the purpose vectors in $\mathcal{L}^{h}_{\mathrm{BITRU}}$ are shorter than that expected by the Gaussian heuristic, also the dimension of $\mathcal{L}^{h}_{\mathrm{BITRU}}$ is twice the time of the dimension of $\mathcal{L}_{\mathrm{NTRU}}$ when choosing the same value of N. In similar way, the length of the shortest nonzero vector is calculated as $\delta(\mathcal{L}^{k}_{\mathrm{BITRU}}) \approx 0.48\sqrt{Nq}$. Therefore, BITRU is more resistance against lattice attacks than NTRU.

## VII. CONCLUSION

- In NTRU, the computation with small coefficient in the convolution product of polynomials resulted in a fast and low cost system that is superior to other theoretical number cryptosystems (e.g., RSA, ECC, and ElGamal) requiring a series of multiplications. The computation in NRTU also does not require any multi-precision libraries because all the polynomial coefficients are reduced mode q which resulted in 11 bit integers at most.
- In this study, the BITRU cryptosystem based on binary algebra is proposed. It is a multi-dimensional cryptosystem that can encrypt two messages from a single origin or two independent messages from two different origins. This property is important in certain applications such as, cellular phones and electronic voting system. When the coefficient of j is equal to zero.
- BITRU is converted to NTRU, with public key k=1 and g=1.
- The security of BITRU is four times that of NTRU because it contains two public keys h,k with four polynomials private keys $f_0, f_1, g_0$, and $g_1$.
- The proposed BITRU is a promising high-performing system. It exhibits certain robustness against well-known attacks that can threaten the security of the NTRU or NTRU-like cryptosystems.
- By lowering N, the speed of BITRU is faster than that of NTRU with the same parameters.

## REFERENCES

[1] D. Robling, "Cryptography and data security," Addison – Wisely Publishing Company, 1982.

[2] W.Diffie, M. Hellman, "New directions in cryptography," IEEE Transactions On information theory, vol. 22, no.6, pp.644-654, 1976.

[3] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signature and public key cryptosystems, " Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.

[4] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithm, " IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, 1985.

[5] R.Schoof, "Elliptic curve over finite fields and the computation of square roots mod p, " Mathematics of computation, vol.44, no.170, pp. 483-494, 1985.

[6] R. McEliece, "A public key cryptosystem based on algebra coding theory," Pasadena, DSN Progress Reports 42-44, pp. 114-116, 1978.

[7] J. Hoffstein, J. Pipher, and J. Silverman, "NTRU: A ring based public key cryptosystem," Proceeding of ANTS III, LNCS, Springer Verlag, vol.1423, pp. 267-288, 1998.

[8] P. Gaborit J. Ohler, P. Soli, "CTRU, a polynomial analogue of NTRU," INRIA. Rapport de recherche, N. 4621, 2002.

[9] R. Kouzmenko, "Generalizations of the NTRU cryptosystem," Diploma Project, Ecole Polytechnique Federale de Lausanne, 2006.

[10] M. Coglianese and B. Goi, "MaTRU: A new NTRU based cryptosystem," Springer Verlag Berlin Heidelberg, pp. 232-243, 2005.

[11] E. Malecian, 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, vol. 3, no. 1, pp. 29–42, 2011.

[12] E. Malecian, A. Zakerolhsooeini, "OTRU: A non- associative and high speed public key cryptosystem," IEEE Computer Society, pp.83-90, 2010.

[13] N. Vats, NNRU a non-commutative analogue of NTRU, "CoRR, abs/0902.1891, 2009.

[14] N. Zhao and S. Su, "An improvement and a new design of Algorithms for Seeking the Inverse of NTRU polynomial", EEE Computer Society, Washington, 2011.

[15] Y. Pan and Y. Deng, "A General NTRU-Like Framework for Constructing Lattice Based Public Key Cryptosystems ", Springer-Verlag Berlin Heidelberg, p.p. 109–120, 2012.

[16] K. Jarvis and M. Nevins, "ETRU: NTRU over the Eisenstein integers," Springer Science +Business Media New York, 2013.

[17] P. Gauravaram, H. Narumanchi and N. Emmadi, " Analytical study of Implementation issues of NTRU", International Conference on Advances in Computing, Communications and Informatics, IEEE, New Delhi, India, pp. 700-707, 2014.

[18] S. C. Batson, "On the Relationship between Two Embeddings of Ideals into Geometric Space and the Shortest Vector Problem in Principal Ideal Lattices" Ph.D. thesis, North Carolina State University, 2015.

[19] N. Alsaidi, M. Said, A. Sadiq and A. Majeed, "An improved NTRU cryptosystem via commutative quaternions algebra," Int. Conf. Security and Management, SAM'15, pp.198-203, 2015.

[20] N. M. G. AlSaidi, M. Said, A. T. Sadiq, and A.A. Majeed, "An improved NTRU cryptosystem via commutative quaternions algebra," Int. Conf. Security and Management SAM'15, 2015, pp.198-203.

[21] K.Thakur and B.P.Tripathi, "BTRU, A Rational Polynomial Analogue of NTRU Cryptosystem," International Journal of Computer Applications, Foundation of Computer Science (FCS), NY, USA, vol. 145, no.12, 2016.

[22] H.R.Yassein, and N.AlSaidi, "HXDTRU Cryptosystem Based On Hexadecnion Algebra," 5th International Cryptology and Information Security Conference, 2016.