Palestine Journal of Mathematics

Vol. 6(2)(2017) , 598–610

A Variant of NTRU with split quaternions algebra

Khushboo Thakur and B.P.Tripathi

Communicated by Ayman Badawi

MSC 2010 Classifications:Primary 94A60; Secondary 20N05, 17A45.

Keywords and phrases:NTRU, split quaternions, noncommutative, Encryption, Decryption

Abstract. In this paper a new multidimensional public key cryptosystem is proposed using split quaternion algebra. The proposed cryptosystem is not fully fit without Circular and Convolutional Modular Lattice. Also in our scheme the decryption failure is reduced due to non-commutative algebraic structure. This system is more resistant to lattice- based attacks and more capable for protocol design.

1 INTRODUCTION

Cryptography is basically a process which relates to data communications, authentication and authorization, integrity and privacy guarantees can be given in addition. We use it in banking or other business sector or even in the railway reservation. Also we are using daily the cryptography is in social work, such as an ATM card to deposit cash into your account and to get cash money.

Modern telecommunication networks especially, the Internet, mobile-phone,have extended the possibilities of communications and information transmissions. which is a cryptographic techniques. focus on being intensive research activities in the study of cryptography.

In mid-1990, a software company, which was one of the few bits of the cryptosystem needs to be based on the system processor and the small numbers. Then three mathematicians, Jeffry Hoffstein, Jill Pipher and Joseph Silverman [4] suggested a new cryptosystem, NTRU (Number Theory Research Unit), which was presented in 1998 completely. NTRU is classified as a lattice based cryptosystem since its security is based on a class of arithmetic operations but it is not based on integer factorization and discrete logarithm problem.It is very efficiently performed with insignificant storage and time complexity [15]. This property made NTRU very suitable choice for a large number of applications, such as mobile phones, portable devices, low-cost smart cards, and RFID devices [5].

After identification of Ntru as a secure and safe core, several researches were carried out on generalization of Ntru algebraic structure to different Euclidean rings from Z including $G_F(2^k)[x]$ and generally Dedekind domain like $Z[i]$, $Z\sqrt{-2}$ and $Z[w]$ [3, 8, 9]. Although generalization of Ntru to $G_F(2^k)[x]$ in [3] never had a desirable result and was broken soon after [9], however, it resulted in a better understanding of the Ntru cryptosystem and suggested the idea of replacing Ntru algebraic structure with other rings, free modules and algebras.

Ntru relies on two fundamental concepts: according to the first concept,this cryptosystem has acquired its inherent security from intractability of the Shortest Vector Problem (SVP) in a certain type of lattice which is assumed to be a NP-Hard problem. From this aspect, Ntru is different from all known cryptosystems like RSA or ECC. According to the second concept that has not been considered in the sense of algebraic generalization, is the possibility of decryption failure, which may lead to the concept of provable security. In Ntru, decryption failure arises from the fact that there is no well-defined and non-trivial homomorphism between two rings Z_p and Z_q as well as the polynomial rings $Z_p[x]$ and $Z_q[x]$.

In this paper, we present our claim about the possibility for replacing Dedekind domains by a broader algebra and generalizing Ntru cryptosystem based on R-Algebra; which is known as sqtru. The main difference between sqtru and those proposed in [9, 11] is that the underlying algebra can be noncommutative. The proposed system is high chance for successful decryption. Also the mathematical base of Ntru in such a way that one can make a similar cryptosystem based on various algebraic structures with the goal of better security against lattice attack and more capability for protocol design.

It is a multi-dimensional public key cryptosystem based on split quaternion algebra, which is broader than Dedekind domain. Its security is depend on underlying algebraic structure, which a non-commutative. Keeping the positive points of NTRU, and making it more resistant to some lattice-based attacks.

The text of this paper is organized in the following way: a brief summarization of the NTRU cryptosystem is presented in Section 2. Some mathematical description of the split quaternion algebra, is discussed in Section 3. In Section 4, the algebraic structure of split quaternion algebra is introduced. The proposed cryptosystem is described in Section 5. The performance analysis is discussed in Section 6, and the conclusions are presented in Section 7.

2 THE NTRU CRYPTOSYSTEM

A simple description of the NTRU cryptosystem is summarized in this section. For more details, the reader is referred to [2, 4, 7, 9, 11, 12] . The NTRU system is principally based on the ring of the convolution polynomials of degree N-1 denoted by $R = Z[x]/(x^N - 1)$. It depends on three integer parameters N, p and q, such that $(p, q) = 1$. Before going through NTRU phases, there are four sets used for choosing NTRU polynomials with small positive integers denoted by L_m, L_f , L_g and $L_r \subseteq R$. It is like any other public key cryptosystem constructed through three phases: key generation, encryption and decryption.

2.1 Key Generation Phase:

To generate the keys, two polynomials f and g are chosen randomly from L_f and L_g respectively. The function f must be invertible. The inverses are denoted by F_p,$F_q \in R$, such that:

$F_p * f = 1$ (mod p) and $F_q * f = 1$ (mod q)

The above parameters are private. The public key h is calculated by,

$$h = pF_q * g(modq) \tag{2.1}$$

Therefore, the public key is $\{h, p, q\}$, and the private key is$\{f, F_p\}$.

2.2 Encryption Phase:

The encryption is done by converting the input message to a polynomial $m \in L_m$ and the coefficient of m is reduced modulo p. A random polynomial r is initially selected by the system, and the cipher text is calculated as follows,

$$e = r * h + m \text{ (mod q)}.$$

2.3 Decryption Phase:

The decryption phase is performed as follows: the private key, f, is multiplied by the cipher text e such that,
a = $f * e$ (mod q).
a = $f*$ ($r * h$ + m) (mod q)
a = $f * h * r + f * m$ (mod q)

a = $p.f * F_q * g * r + f * m$ (mod q)
a = $p.g * r + f * m$ (mod q)

The last polynomial has coefficients most probably within the interval $[-q/2, +q/2]$, which eliminates the need for reduction mod q. This equation is reduced also by mod p to give a term $f * m$ mod p, after diminishing of the first term $p.g * r$. Finally,the message m is extracted after multiplying by ${F_p}^{-1}$, as well as adjusting the resulting coefficients via the interval $[-p/2, p/2)$.

3 A Brief Introduction to Split quaternion Algebra

In 1849, James Cockle introduced the set of split quaternions, also known as coquaternions. The set of split quaternions is four dimensional noncommutative and associative algebra with zero divisors. It has also nilpotent and idempotent elements. The real algebra of coquaternions is denoted by $\hat{H}$ [1, 13].
Some definition and theorem used in proposed cryptosystem:

Definition 3.1. Split Quaternion: The set of split quaternion can be represented as

$$\hat{H} = \{q = q_0 + q_1 i + q_2 j + q_3 k; \qquad q_0, q_1, q_2, q_3 k \in R\}. \tag{3.1}$$

Here the imaginary units $\{i, j, k\}$ satisfy the following relations:

$$\begin{aligned} i^2 = -1, j^2 = k^2 = 1, ijk = 1, \\ ij = k = -ji, \\ jk = -i = -kj, \\ ki = j = -ik. \end{aligned}$$

A split quaternion q is a sum of scalar and vector part. $S_q = q_0$ be the scalar part and $V_q = q_1 i + q_2 j + q_3 k$. be the vector part. Vector part of the split quaternion is very important for multiplication rule.

Let $p, q \in H_s$, where $q = S_q + V_q$ and $p = S_p + V_p$. The addition operator, $+$, is defined then,

$$\begin{aligned} q + p &= (S_q + V_q) + (S_p + V_p) \\ &= (q_0 + p_0) + (q_1 + p_1)i + (q_2 + p_2)j + (q_3 + p_3)k. \end{aligned}$$

The multiplication rule for split quaternions is defined as

$$qp = p_1 q_1 + \langle \bar{V_p}, \bar{V_q} \rangle + p_1 \bar{V_q} + q_1 \bar{V_p} + \bar{V_p} \wedge \bar{V_q}$$

Also, the split quaternion product may be written as

$$X = \begin{bmatrix} p_1 & -p_2 & p_3 & p_4 \\ p_2 & p_1 & p_4 & -p_3 \\ p_3 & p_4 & p_1 & -p_2 \\ p_4 & -p_3 & p_2 & p_1 \end{bmatrix}$$

Split quaternion multiplication is not commutative. It is an associative, nilpotent elements, nontrivial idempotents and non-division ring with four basis element $1, i, j, k$. In this paper i, j and k are defined as i^2 = a, $j^2 = b, k^2 = -ab$ and $ij = -ji = k$, By this definition, a general split quaternion algebraic system is defined. Assuming F is an arbitrary field, the split quaternion algebra A can be defined over F as:

$$A = \{a + bi + cj + dk | a, b, c, d \in F\} \tag{3.2}$$

where,

$$i^2 = a, j^2 = b, k^2 = -ab, ij = -ji = k. \tag{3.3}$$

Clearly, if we assume that $a = -1$, $b = 1$ and F be the field of real numbers R, then, based on the choice of a and b and the nature of the field F, the original definition of split quaternion is obtained.

Definition 3.2. Bar Conjugation in split quaternion algebra: suppose $q = q_0 + q_1 i + q_2 j + q_3 k \in H_s$, we say that q_0, q_1, q_2 and q_3 are the coefficients of q. In particular, q_0 be the real part of q and $q_1 i + q_2 j + q_3 k$ be the imaginary part of q. So the bar conjugate of q is

$$\bar{q} = q_0 - q_1 i - q_2 j - q_3 k. \tag{3.4}$$

Definition 3.3. Norm in split quaternion algebra: The norm of q is defined as

$$N(q) = q \times \bar{q} = \bar{q} \times q = {q_0}^2 + {q_1}^2 - {q_2}^2 - {q_3}^2. \tag{3.5}$$

Definition 3.4. Trace in split quaternion algebra: The trace of q is defined as,

$$T(q) = q + \bar{q} = 2q_0. \tag{3.6}$$

Definition 3.5. Multiplicative inverse in split quaternion algebra: The inverse of the split quaternion q is defined by

$$q^{-1} = \frac{q^*}{N(q)} \qquad if \qquad N(q) \neq 0 \tag{3.7}$$

Definition 3.6. Real Matrix Representation of split quaternion algebra: Let $A = A_1 + A_2 i + A_3 j + A_4 K \in M_{n\times n}(\hat{H})$, where $A_1, A_2, A_3, A_4 \in M_{n\times n}(R)$.The $4n \times 4n$ matrix

$$X = \begin{bmatrix} A_1 & -A_2 & A_3 & A_4 \\ A_2 & A_1 & A_4 & -A_3 \\ A_3 & A_4 & A_1 & -A_2 \\ A_4 & -A_3 & A_2 & A_1 \end{bmatrix}$$

is called the real matrix representation of the split quaternion matrix A and denoted by $\Re_A$.

Theorem 3.7. *Split quaternions satisfy the following properties for the elements p,q and* $r \in H_s$.

(i) $q^*q = qq^*$

(ii) $Jc = \bar{c}J$ *or* $JCJ^* = \bar{c}$ *for any complex number c,*

(iii) $q^2 = |Re\ q|^2 - \|Im\ q\|^2 + 2Re\ q\ Im\ q$,

(iv) $(qp)^* = p^*q^*$,

(v) (pq)r=p(qr),

(vi) $pq \neq qp$ *in general,*

(vii) $q^* = q$ *if and only if q is a real number,*

(viii) $\frac{q^*}{N(q)}$ *is the inverse of q if* ${q_0}^2 + {q_1}^2 \neq {q_2}^2 + {q_3}^2$,

(ix) Every split quaternion q can be uniquely expressed as $q=c_1 + c_2 j$, *where* c_1 *and* c_2 *are complex numbers.*

4 Algebraic Structure of Split quaternions

Consider the convolution polynomial rings $R := Z[x]/(x^N - 1)$, $R_p := Z_p[x]/(x^N - 1)$, and $R_q := Z_q[x]/(x^N - 1)$ that are used in Ntru.AWe define three split quaternion algebras A, A_p and A_q as follows

$$A := \left(\frac{-1, 1}{Z[x]/(x^N - 1)}\right)$$

$$A_p := \left(\frac{-1, 1}{Z_p[x]/(x^N - 1)}\right)$$

$$A_q := \left(\frac{-1, 1}{Z_q[x]/(x^N - 1)}\right)$$

For simplicity, p, q and N are assumed to be prime numbers and $q >> p$. Since $Z_p[x]/(x^N - 1)$ and $Z_q[x]/(x^N - 1)$ are finite rings with characteristics p and q, respectively, one can easily conclude that A_p and A_q are split quaternion algebras. Then,

$$\begin{aligned} A_p : &= \left(\frac{-1, 1}{Z_p[x]/(x^N - 1)}\right) \\ &= \{f_0(x) + f_1(x)i + f_2(x)j + f_3(x)k \\ &\quad | f_0, f_1, f_2, f_3 \in Z_p[x]/(x^N - 1) \\ &\quad i^2 = -1, j^2 = k^2 = 1, ij = -k = ji\} \end{aligned}$$

and

$$\begin{aligned} A_q : &= \left(\frac{-1, 1}{Z_q[x]/(x^N - 1)}\right) \\ &= \{g_0(x) + g_1(x)i + g_2(x)j + g_3(x)k \\ &\quad | g_0, g_1, g_2, g_3 \in Z_q[x]/(x^N - 1) \\ &\quad i^2 = -1, j^2 = k^2 = 1, jk = -i = -kj\} \end{aligned}$$

Now assume that q_1,$q_2 \in A_p$ (or A_q) where,

$$q_1 = y_0(x) + y_1(x)i + y_2(x)j + y_3(x)k$$

and

$$q_2 = z_0(x) + z_1(x)i + z_2(x)j + z_3(x)k.$$

Then, addition, multiplication, norm, trace and multiplicative inverse are defined in the following way

• **Addition:**

$$q_1 + q_2 = (y_0(x) + z_0(x)) + (y_1(x) + z_1(x)).i + (y_2(x) + z_2(x)).j + (y_3(x) + z_3(x)).k$$

• **Multiplication:** of two split quaternions are defined by

$q_1 \circ q_2 = y_0(x)z_0(x) - y_1(x)z_1(x) + y_2(x)z_2(x) + y_3(x)z_3(x)$
$+((y_0(x)z_1(x) + y_1(x)z_0(x) - y_2(x)z_3(x) + y_3(x)z_2(x)).i$
$+((y_0(x)z_2(x) - y_1(x)z_3(x) + y_2(x)z_0(x) + y_3(x)z_1(x)).j$
$+(y_0(x)z_3(x) + y_1(x)z_2(x) - y_2(x)z_1(x) + y_3(x)z_0(x)).k$

where $\circ$ denotes the convolution product and split quaternion multiplication in A_p (or A_q) needs 16 polynomial convolutions and 8 polynomial addition modulo p (q), which together account for $16.N^2$ modular multiplications and $(16N(N-1) + 8N)$ modular additions.

• **Conjugate:**

$q_1{}^* = \bar{q_1} = +y_0(x) - y_1(x)i - y_2(x)j - y_3(x)k$

• **Norm**

$N(q_1)$=$q_1 \times {q_1}^*$= $(y_0(x))^2 + (y_1(x))^2 - (y_2(x))^2 - y_2(x))^2$

• **Multiplicative inverse**
$N(q_1) \neq 0 \rightarrow {q_1}^{-1} = \frac{{q_1}^*}{N(q_1)}$
$=((y_0(x))^2 + (y_1(x))^2 - (y_2(x))^2 - (y_3(x))^2 \circ (y_0(x) - y_1(x).i - y_2(x).j - y_3(x).k$

• **Trace** The trace of q_1 is
$T(q_1)$=q_1+$\bar{q_1}$=$2y_0(x)$.
Thus, the following operations will be needed for calculating the multiplicative inverse of an element in A_p or A_q then we get,

(i) Calculation of $g(x) \leftarrow (y_0(x))^2 + (y_1(x))^2 - (y_2(x))^2 - y_2(x))^2$ over the ground ring $\left(\frac{-1,1}{Z_p[x]/(x^N-1)}\right)$ at the total cost of $4N^2$ multiplications and (3N) additions with the worth case complexity of $O(N^2)$ [**?**].

(ii) Finding the inverse of g(x) over the ring $\left(\frac{-1,1}{Z_p[x]/(x^N-1)}\right)$ with complexity of $O(N^2 log(p^2))$.

(iii) Conjugation of q_1 including $3N$ negations.

(iv) Calculation of $g^{-1}(x).{q_1}^*$ including $4N^2$ multiplication and $4N(N-1)$ addition modulo p or q.

5 Proposed Scheme:

In order to obtain a full understanding of how the proposed cryptosystem works, the algebraic structure for key generation, encryption and decryption, is designed as follows. At the beginning, the parameters N, p, q have the property that N is an integer, p and q are relatively prime, and in all the algorithms, the parameter m represents either p or q depending upon which one is passed into the function.

5.1 Key Generation Phase:

To generate the public key, two small split quaternion F and G are randomly generated, such that

$$F = f_0 + f_1.i + f_2.j + f_3.k, \quad such\ that \quad f_0, f_1, f_2, f_3 \in L_f$$
$$G = g_0 + g_1.i + g_2.j + g_3.k, \quad such\ that \quad g_0, g_1, g_2, g_3 \in L_g$$

The split quaternion F must be invertible over A_p = $\left(\frac{-1,1}{Z_p[x]/(x^N-1)}\right)$ and A_q=$\left(\frac{-1,1}{Z_q[x]/(x^N-1)}\right)$. After generation of F and G then the inverses of F is denoted by F_p and F_q and the inverses of G is denoted by G_p and G_q will be computed in the following way

$$F_q = ({f_0}^2 + {f_1}^2 - {f_2}^2 - {f_3}^2)^{-1} \circ (f_0 - f_1.i - f_2.j - f_3.k) = \alpha_0 + \alpha_1.i + \alpha_2.j + \alpha_3.k$$
$$and$$
$$G_q = ({g_0}^2 + {g_1}^2 - {g_2}^2 - {g_3}^2)^{-1} \circ (g_0 - g_1.i - g_2.j - g_3.k) = \beta_0 + \beta_1.i + \beta_2.j + \beta_3.k$$

Now, the public key is calculated as follows:

$$H = F \circ G_q \ (mod q) \tag{5.1}$$

Here
$F = F_0 + F_1.i + F_2.j + F_3.k$,

$G_q = \beta_0 + \beta_1.i + \beta_2.j + \beta_3.k$
Now

$$\begin{aligned} F \circ G_q &= (F_0 + F_1.i + F_2.j + F_3.k) \circ (\beta_0 + \beta_1.i + \beta_2.j + \beta_3.k) \\ &= (F_0 * \beta_0 - F_1 * \beta_1 + F_2 * \beta_2 + F_3 * \beta_3) \\ &+ (F_0 * \beta_2 - F_1 * \beta_3 + F_2 * \beta_0 + F_3 * \beta_1).j \\ &+ (F_0 * \beta_3 + F_1 * \beta_2 - F_2 * \beta_1 + F_3 * \beta_0).k, \end{aligned}$$

The split quaternions F, G, F_p and G_q will be kept secret in order to be used in the decryption phase. It is obvious that the estimated time to generate a key for the proposed scheme is 16 times slower than that of NTRU, when the same parameters (N, p and q) are selected for both cryptosystems. However, with a lower dimension N, we can achieve the original NTRU speed.

As already described, the new system is a four dimensional vector space over the real field R of real numbers with a basis $\{1, i, j, k\}$. Hence, if one chooses the coefficients of i, j and k to be zeros in the commutative quaternions F and G, then the system will be completely similar to NTRU. Moreover, this choice of zero coefficients for j and k will produce a cryptosystem based on complex numbers. Finally, if one of the coefficients of i, j or k is equal to zero, then we obtain a tridimensional scheme.

5.2 Encryption phase:

At the beginning of the encryption process, the cryptosystem initial generates a random split quaternion which is called the blinding split quaternion. Incoming data must be converted into a split quaternion including four small polynomials with four dimension $\{1, i, j, k\}$. Data conversion into polynomials is performed exactly similar to the NTRU system. The incoming data can be generated from the same or four different sources but transformed into split quaternion based on a simple conversion. After the conversion of the incoming message(s) into split quaternion, the ciphertext will be computed and sent in the following way
Let plaintext message,

$$\begin{aligned} M &= m_0 + m_1.i + m_2.j + m_3.k, \\ where, m_0, m_1, m_2, m_3 &\in L_m. \end{aligned}$$

and blinding quaternion

$$\begin{aligned} \phi &= \phi_0 + \phi_1.i + \phi_2.j + \phi_3.k, \\ where\ \phi_0, \phi_1, \phi_2, \phi_3 &\in L_\phi. \end{aligned}$$

Now create a random split quaternion

$$\begin{aligned} R &= r_0 + r_1.i + r_2.j + r_3.k, \\ where, r_0, r_1, r_2, r_3 &\in L_r. \end{aligned}$$

and

$$\begin{aligned} \psi &= \psi_0 + \psi_1.i + \psi_2.j + \psi_3.k, \\ where, \psi_0, \psi_1, \psi_2, \psi_3 &\in L_\psi. \end{aligned}$$

Hence the encryption function is

$$E = p.\phi \circ \psi \circ H \circ R + M \tag{5.2}$$

Encryption needs split quaternion multiplication including 256 convolution multiplications with $O(N^2)$ complexity, and 4 polynomial additions with $O(N)$ complexity. In the encryption phase, a total of four data vectors are encrypted at once.

5.3 Decryption phase:

After receiving the ciphertext E, the original message is constructed as follows. The private key F and G is used to find B:

$$B = F_q \circ G \circ E(mod\ q) \tag{5.3}$$

The coefficient of B should be reduced mod q into the interval $(-q/2; q/2]$. The next step in the decryption process is to calculate the split quaternion D.

$$D = F \circ G_p \circ B(mod\ p) \tag{5.4}$$

5.4 How Decryption Works:

$$\begin{aligned} B =& F_q \circ G \circ E(mod\ q) \\ &= (F_q \circ G \circ (p.\phi \circ \psi \circ H \circ R + M))mod\ q \\ &= (F_q \circ G \circ p.\phi \circ \psi \circ (F \circ G_q) \circ R + F_q \circ M \circ G)mod\ q \\ &= (F_q \circ F \circ p.\phi \circ \psi \circ G \circ G_q \circ R + F_q \circ M \circ G)mod\ q \\ &= (p.\phi \circ \psi \circ R + F_q \circ M \circ G)mod\ q \end{aligned}$$

Since

$$\begin{aligned} D =& F \circ G_p \circ B(mod\ p) \\ &= F \circ G_p \circ (p.\phi \circ \psi \circ R + F_q \circ M \circ G)(mod\ p) \\ &= F \circ G_p \circ p.\phi \circ \psi \circ R + F \circ F_q \circ G_p \circ G \circ M(mod\ p) \end{aligned}$$

The term $(F \circ G_p \circ p.\phi \circ \psi \circ R)$ will be vanish after reducing mod p, to obtain the term $(F \circ F_q \circ G_p \circ G \circ M)$.

Since $F_q \circ F$ = 1 (mod q) and $G_p \circ G$ = 1(mod p), normalizing the result into the interval $(-p/2 + p/2]$ yields the original message M. Therefore, the decryption speed is half the encryption speed because decryption includes 32 convolutions product. This is clearly analogous to the NTRU cryptosystem.

6 PERFORMANCE ANALYSIS:

After comparing NTRU to other cryptosystems, such as RSA and ECC, which are based on the number theoretic problem (e.g., factorization and discrete logarithm) [10], NTRU was found to have an advantage over them due to its fast and low space storage arithmetic operations. This turned NTRU into a very suitable choice for a large number of applications.

6.1 Computational complexity:

For encryption, one split quaternion multiplication is needed in addition to 256 convolution multiplication and 4 polynomial addition both with O(N) com- plexity. In the encryption phase, any incoming data is converted into polynomial with coefficients between $-p/2$ and $p/2$. In other words, m_0, m_1, m_2 and m_3 are small polynomials mod q.

6.2 Security Attacks:

(a). Brute Force Attack: Compared to NTRU, to improve the privet key f, an attacker has to try using all possible $f \in L_f$ in an attempt to check if $g * h$ mod q has small polynomial coefficients or not. Another way is to try all possible $g \in L_g$ and check if $f * h^{-1}$ mod q has small coefficients. In proposed cryptosystem, the attacker uses the same procedure, where he knows all the public

parameters and constant d_f ,d_g, d_r, p, q and N. The attacker needs to look in the space of large order to be able to look in the spaces L_f and L_g, as follows:

$$|L_f| = \binom{N}{d_f}^4 \qquad \binom{N-d_f+1}{d_f}^4 = (\frac{N!}{(d_f)!^8(N-2d_f)!^4}$$

$$|L_g| = \binom{N}{d_g}^4 \qquad \binom{N-d_g}{d_g}^4 = (\frac{N!}{(d_g)!^8(N-2d_g)!^4}$$

The space of L_f is a bigger than the space of L_g. For this reason, it is easier for the attacker to search in L_g. By using the brute force attack, an attacker can break a message encrypted by proposed cryptosystem. This can be done by searching in the space L_r because $E = HR + M$ (mod q) is known. If the attacker has an ability to find the random split quaternion R then he will be able to find the original message by calculating M=E-HR (mod q). It is obvious that in a brute force attack, the security of any message depends on how hard it is to find R. The order of the space L_r is calculated using the same approach of calculating the order of L_f and L_g,

$$|L_r| = \binom{N}{d_r}^4 \qquad \binom{N-d_r+1}{d_r}^4 = (\frac{N!}{(d_r)!^8(N-2d_r)!^4}$$

This comparison shows that proposed cryptosystem is more robust to this attack than NTRU.
(b). Lattice based attacks: It is known that every split quaternion is isomorphism to a matrix called the fundamental matrix given in below:

$$q = q_0 + q_1 i + q_2 j + q_3 k \equiv \begin{bmatrix} q_0 & -q_1 & q_2 & q_3 \\ q_1 & q_0 & q_3 & -q_2 \\ q_2 & q_3 & q_0 & -q_1 \\ q_3 & -q_2 & q_1 & q_0 \end{bmatrix}$$

The system parameters (d_f, d_g, d_r, p, q, N) are known to the attacker as well as the public key $H = F \circ G_q = h_0 + h_1 i + h_2 j + h_3 k$. When the attacker manages to find one of the split quaternions F or G, the proposed cryptosystem is broken. Note that, h_0, h_1, h_2 and h_3 are polynomials of order N over $Z[x]/(x^N - 1)$. We also represent those polynomials in their isomorphic representation as vectors over Z^N as follows:

$$H = h_0 + h_1 i + h_2 j + h_3 k \cong [h_0\ h_1\ h_2\ h_3]$$

where

$$\begin{aligned} h_0 &= h_{0,0} + h_{0,1}.x + h_{0,2}.x^2 + h_{0,N-2}.x^{N-2} + h_{0,N-1}.x^{N-1}, \\ &\cong [h_{0,0} \quad h_{0,1} \quad h_{0,2} \quad h_{0,N-2} \quad + h_{0,N-1}] \in Z^N \end{aligned}$$

$$\begin{aligned} h_1 &= h_{1,0} + h_{1,1}.x + h_{1,2}.x^2 + h_{1,N-2}.x^{N-2} + h_{1,N-1}.x^{N-1}, \\ &\cong [h_{1,0} \quad h_{1,1} \quad h_{1,2} \quad h_{1,N-2} \quad + h_{1,N-1}] \in Z^N \end{aligned}$$

$$\begin{aligned} h_2 &= h_{2,0} + h_{2,1}.x + h_{2,2}.x^2 + h_{2,N-2}.x^{N-2} + h_{2,N-1}.x^{N-1}, \\ &\cong [h_{2,0} \quad h_{2,1} \quad h_{2,2} \quad h_{2,N-2} \quad + h_{2,N-1}] \in Z^N \end{aligned}$$

$$\begin{aligned} h_3 &= h_{3,0} + h_{3,1}.x + h_{3,2}.x^2 + h_{3,N-2}.x^{N-2} + h_{3,N-1}.x^{N-1}, \\ &\cong [h_{3,0} \quad h_{3,1} \quad h_{3,2} \quad h_{3,N-2} \quad + h_{3,N-1}] \in Z^N \end{aligned}$$

Since the polynomial ring Z is isomorphic to the circulant matrix ring of order N over Z, the polynomials $h_0; h_1; h_2$ and h_3 can be represented in their isomorphic representation for lattice analysis as:

$$h(i)_{N\times N} = \begin{bmatrix} h_{i,0} & .... & h_{i,N-1} \\ h_{i,N-1} & ..... & h_{i,N-2} \\ .... & .... & .... \\ h_{i,2} & ..... & h_{i,1} \\ h_{i,1} & ... & h_{i,0} \end{bmatrix}$$

where i=0,1,2,3.

With respect to the above assumptions, to describe the partial lattice attack first, let the split quaternions F and G be represented by $F = [f_0, f_1, f_2, f_3]$, and $G = [g_0, g_1, g_2, g_3]$ where $f_0, f_1, f_2, f_3, g_0, g_1, g_2, g_3 \in Z[x]\backslash(x^N-1)$. In order to form the lattice, the vectors $[u_0, u_1, u_2, u_3, v_0, v_1, v_2, v_3]$ must belong to Z^{8N}. This lattice is denoted by $L_{partial}$ and defined by:

$\lambda \cdot I_{4N\times 4N}$	$H_{4N\times 4N}$
$0_{4N\times 4N}$	$q \cdot I_{4N\times 4N}$

where, I refers to the identity matrix, 0 is the zero matrix, and H is the fundamental matrix of $hi's$. $L_{partial}$ contains a vector in the form $[u_0, u_1, u_2, u_3, v_0, v_1, v_2, v_3] \in Z^{8N}$, that satisfies $FH = G$. However, there is a major difference between NTRU and SQTRU (split quaternion) lattices, such that all points spanned by the SQTRU lattice simply includes a partial subset of the total set of vectors satisfying $G.H = F$. To see this, let $[u_0, u_1, u_2, u_3, v_0, v_1, v_2, v_3]$ denote the vector satisfying $G.H = F$, then $[-u_1, u_0, -u_3, u_2, -v_1, v_0, -v_3, v_2]$ is the answer. Also, since $iG.H = iF$, therefore, $L_{partial}$ will not necessarily contain such vector. The attacker may manage to use the lattice reduction algorithm [6, 14]to find a short vector satisfying $G.H = F$. However, even with such promising assumption, Lpartial has a dimension that is four times larger than the lattice dimension of NTRU with the same order N

Therefore, for any chosen parameters (N, p, q) to be used in proposed cryptosystem, the system will be four times slower than NTRU with the same parameters. However, the SQTRU security is four times as that offered by NTRU with the same parameters. On the other hand, NTRU with 4N dimensions is sixteen times slower with respect to computational time than NTRU with N dimensions. Therefore, SQTRU has a security advantage over NTRU.

7 Successful Decryption:

Probability of successful decryption in proposed scheme is calculated in the same way as NTRU and under the same assumptions considered in [9] and [12]. Moreover, for successful decryption in proposed scheme , all coefficients of $F_q \circ G \circ E = (p.\phi \circ \psi \circ R + F_q \circ M \circ G) mod q$. Hence, we obtain

$$\begin{aligned} B :&= (p.\phi \circ \psi \circ R + F_q \circ M \circ G)\ mod\ q \\ &= b_0 + b_1.i + b_2.j + b_3.k \end{aligned}$$

where

b_0= p$(\phi_0\psi_0r_0 - \phi_1\psi_1r_0 + \phi_2\psi_2r_0 + \phi_1\psi_3r_0 - \phi_0\psi_1r_1 - \phi_1\psi_0r_1 + \phi_2\psi_3r_1 - \phi_3\psi_2r_1 + \phi_0\psi_2r_2 - \phi_1\psi_3r_2 + \phi_2\psi_0r_2 + \phi_3\psi_1r_2 + \phi_0\psi_3r_3 + \phi_1\psi_2r_3 - \phi_2\psi_1r_3 + \phi_3\psi_0r_3) + fq_0m_0g_0 - fq_1m_1g_0 + fq_2m_2g_0 + fq_1m_3g_0 - fq_0m_1g_1 - fq_1m_0g_1 + fq_2m_3g_1 - fq_3m_2g_1 + fq_0m_2g_2 - fq_1m_3g_2 + fq_2m_0g_2 + fq_3m_1g_2 + fq_0m_3g_3 + fq_1m_2g_3 - fq_2m_3g_1 + fq_3m_0g_3$

b_1= p$(\phi_0\psi_0r_1 - \phi_1\psi_1r_1 + \phi_2\psi_2r_1 + \phi_1\psi_3r_1 + \phi_0\psi_1r_0 + \phi_1\psi_0r_0 - \phi_2\psi_3r_0 + \phi_3\psi_2r_0 - \phi_0\psi_2r_3 + \phi_1\psi_3r_3 - \phi_2\psi_0r_3 - \phi_3\psi_1r_3 + \phi_0\psi_3r_2 + \phi_1\psi_2r_2 - \phi_2\psi_1r_2 + \phi_3\psi_0r_2) + fq_0m_0g_1 - fq_1m_1g_1 + fq_2m_2g_1 + fq_1m_3g_1 + fq_0m_1g_0 + fq_1m_0g_0 - fq_2m_3g_0 + fq_3m_2g_0 - fq_0m_2g_3 + fq_1m_3g_3 -$

$fq_2m_0g_3 - fq_3m_1g_3 + fq_0m_3g_2 + fq_1m_2g_2 - fq_2m_1g_2 + fq_3m_0g_2$

b_2= p$(\phi_0\psi_0r_2 - \phi_1\psi_1r_2 + \phi_2\psi_2r_2 + \phi_1\psi_3r_2 - \phi_0\psi_1r_3 - \phi_1\psi_0r_3 + \phi_2\psi_3r_3 - \phi_3\psi_2r_3 + \phi_0\psi_2r_0 - \phi_1\psi_3r_0 + \phi_2\psi_0r_0 + \phi_3\psi_1r_0 + \phi_0\psi_3r_1 + \phi_1\psi_2r_1 - \phi_2\psi_1r_1 + \phi_3\psi_0r_1) + fq_0m_0g_2 - fq_1m_1g_2 + fq_2m_2g_2 + fq_1m_3g_2 - fq_0m_1g_3 - fq_1m_0g_3 + fq_2m_3g_3 - fq_3m_2g_3 + fq_0m_2g_0 - fq_1m_3g_0 + fq_2m_0g_0 + fq_3m_1g_0 + fq_0m_3g_1 + fq_1m_2g_1 - fq_2m_1g_1 + fq_3m_0g_1$

b_3= p$(\phi_0\psi_0r_3 + \phi_2\psi_2r_3 - \phi_1\psi_1r_3 + \phi_1\psi_3r_3 + \phi_0\psi_1r_2 + \phi_0\psi_1r_2 + \phi_2\psi_3r_2 + \phi_3\psi_2r_3 - \phi_0\psi_2r_1 + \phi_1\psi_3r_1 - \phi_2\psi_0r_1 - \phi_3\psi_1r_1 + \phi_0\psi_3r_0 + \phi_1\psi_2r_0 - \phi_2\psi_1r_0 + \phi_3\psi_0r_0) + fq_0m_0g_0 - fq_1m_1g_3 + fq_2m_2g_3 + fq_1m_3g_3 + fq_0m_1g_2 + fq_0m_1g_2 + fq_2m_3g_2 + fq_3m_2g_3 - fq_0m_2g_1 + fq_1m_3g_1 - fq_2m_0g_1 - fq_3m_1g_1 + fq_0m_3g_0 + fq_1m_2g_0 - fq_2m_1g_0 + fq_3m_0g_0$

Now, we obtain

$$P_r(f_{i,j}=1)=\frac{d_f}{N},\qquad P_r(f_{i,j}=-1)=\frac{d_f-1}{N}\approx\frac{d_f}{N},\qquad P_r(f_{i,j}=0)=\frac{N-2d_f}{N},$$
$$P_r(g_{i,j}=1)=P_r(g_{i,j}=-1)=\frac{d_g}{N},\qquad P_r(g_{i,j}=0)=\frac{N-2d_g}{N},$$
$$P_r(\phi_{i,j}=1)=P_r(\phi_{i,j}=-1)=\frac{d_\phi}{N},\qquad P_r(\phi_{i,j}=0)=\frac{N-2d_\phi}{N},$$
$$P_r(\psi_{i,j}=1)=P_r(\psi_{i,j}=-1)=\frac{d_\psi}{N},\qquad P_r(\psi_{i,j}=0)=\frac{N-2d_\psi}{N},$$
$$P_r(r_{i,j}=1)=P_r(r_{i,j}=-1)=\frac{d_r}{N},\qquad P_r(r_{i,j}=0)=\frac{N-2d_r}{N},$$
$$P_r(m_{i,j}=j)=\frac{1}{p},\qquad i=0,1,2,3\qquad j=\frac{-p+1}{2}.....\frac{+p-1}{2}.$$

where

$$\begin{aligned} f_i &= [f_{i,0}, f_{i,1}, ..., f_{i,N-1}] \qquad i=0,1,2,3 \\ g_i &= [g_{i,0}, g_{i,1}, ..., g_{i,N-1}] \qquad i=0,1,2,3 \\ \phi_i &= [\phi_{i,0}, \phi_{i,1}, ..., \phi_{i,N-1}] \qquad i=0,1,2,3 \\ \psi_i &= [\psi_{i,0}, \psi_{i,1}, ..., \psi_{i,N-1}] \qquad i=0,1,2,3 \\ r_i &= [r_{i,0}, r_{i,1}, ..., r_{i,N-1}] \qquad i=0,1,2,3 \end{aligned} \tag{7.1}$$

Under the above assumptions, we get $E[f_{i,j}] \approx 0$, $E[g_{i,j}] = 0$, $E[h_{ij}] = 0$, and $E[m_{i,j}] = 0$. Therefore, we have
$E[b_{ij}]$ = 0 i= 0,1,2,3 j= 0.....$N-1$.
In order to calculate $Var[b_{i,j}]$, analogous to NTRU, it is sufficient to write

$$Var[\phi_{i,j}.\psi_{k,l}.r_{m,n}] = \frac{8d_\phi.d_\psi.d_r}{N^3} \qquad i,k,m=0,1,2,3. \qquad j,l,n=0,....,N-1,$$
$$Var[f_{qi,k}.m_{j,l}.g_{m,n}] = \frac{d_{fq}.d_g(p+1)}{6.N} \qquad i,j=0,1,2,3 \qquad k,l=0,....,N-1.$$

As a result,

$Var[b_{0,k}]$ = $Var[\sum_{i+j=k}(p(\phi_0\psi_0r_0 - \phi_1\psi_1r_0 + \phi_2\psi_2r_0 + \phi_1\psi_3r_0 - \phi_0\psi_1r_1 - \phi_1\psi_0r_1 + \phi_2\psi_3r_1 - \phi_3\psi_2r_1 + \phi_0\psi_2r_2 - \phi_1\psi_3r_2 + \phi_2\psi_0r_2 + \phi_3\psi_1r_2 + \phi_0\psi_3r_3 + \phi_1\psi_2r_3 - \phi_2\psi_1r_3 + \phi_3\psi_0r_3) + fq_0m_0g_0 - fq_1m_1g_0 + fq_2m_2g_0 + fq_1m_3g_0 - fq_0m_1g_1 - fq_1m_0g_1 + fq_2m_3g_1 - fq_3m_2g_1 + fq_0m_2g_2 - fq_1m_3g_2 + fq_2m_0g_2 + fq_3m_1g_2 + fq_0m_3g_3 + fq_1m_2g_3 - fq_2m_3g_1 + fq_3m_0g_3$

Upon insertion of $Var[\phi_{i,j}.\psi_{k,l}.r_{m,n}]$ and $Var[f_{qi,k}.m_{j,l}.g_{m,n}]$ values, we obtain

$$\begin{aligned} Var[b_{0,k}] &= 64p^2N^2(\frac{8d_\phi d_\psi d_r}{N^3}) + 64N(\frac{d_{fq}d_g(p-1)(p+1)}{6N}) \\ &= \frac{64 \times 8p^2 d_\phi d_\psi d_r}{N}) + \frac{32 d_{fq} d_g (p-1)(p+1)}{3} \\ &= \frac{512p^2 d_\phi d_\psi d_r}{N} + \frac{32 d_{fq} d_g (p-1)(p+1)}{3}. \end{aligned}$$

Similarly, we have

$$\begin{aligned} Var[b_{1,k}] &= Var[b_{2,k}] \\ &= Var[b_{3,k}] \approx \frac{512p^2 d_\phi d_\psi d_r}{N} + \frac{32 d_{fq} d_g (p-1)(p+1)}{3}. \end{aligned}$$

It is desirable to calculate the probability that $a_{i,k}$ lies within $[\frac{-q+1}{2}.....\frac{+q-1}{2}]$, which implies successful decryption. With the assumption that $a_{i,k}$ have normal distribution with zero mean and the variance calculated as above, we have

$$\begin{aligned} P_r &= (|b_{i,k}| \leq \frac{q-1}{2}) \\ &= P_r = (-\frac{q-1}{2} \leq b_{i,k} \leq \frac{q-1}{2}) \\ &= 2\phi(\frac{q-1}{2\sigma}) - 1, \qquad i = 0,1,2,3. \qquad k = 0.....N-1 \end{aligned}$$

where ϕ denotes the distribution of the standard normal variable and $\sigma = \sqrt{\frac{512p^2 d_\phi, d_\psi d_r}{N} + \frac{32 d_f q d_g (p-1)(p+1)}{3}}$

Assuming that $b_{i,k}$'s are independent random variables, the probability for successful decryption in new scheme can be calculated through the following two observations:

• The probability for each of the messages m_0, m_1, m_2,and m_3 to be correctly decrypted is

$$(2\phi(\frac{q-1}{2\sigma}) - 1)^N, \tag{7.2}$$

• The probability for all the messages m_0, m_1, m_2 and m_3 to be correctly decrypted is

$$(2\phi(\frac{q-1}{2\sigma}) - 1)^{4N}, \tag{7.3}$$

8 Conclusion

In this paper the Ntru public key cryptosystem is based on the abstract algebraic concepts and does not limited to Dedekind domain or commutative rings. These concepts can be applied to broader algebras like split quaternions non-commutative algebra in order to create a new Ntru-like cryptosystem.

To prove claims proposed, we have shown that the fundamental concepts behind Ntru could be extended and generalized and then an abstract construction method have been proposed, on the basis of which, a Ntru-like cryptosystem can be correctly implemented with an algebraic structure broader and more complex than the polynomial rings over Dedekind domains.

Our proposed cryptosystem works based on split quaternions algebra and due to its non-commutative nature, it can hardly be attacked by the existing lattice attack algorithms.

References

[1] Y. Alagoz, K. H. Oral, S. Yuce, "Split quaternions matrices, Miskolc Mathematical Notes, 13(2) (2012),223-232.

[2] D. Coppersmith, A. Shamir,“ Lattice attacks on NTRU, in EUROCRYPT, (1997), 52-61.

[3] P. Gaborit, J. Ohler,“ Ctru, a polynomial analogue of ntru, Technical report, INRIA, (2002).

[4] Hoffstein J., Pipher J. and Silverman J.H., “NTRU": A Ring Based Public Key Cryptosystem, In Lecture notes in Computer Science, Springer-Verlag, (1998), 267-288.

[5] J. Hoffstein, J. Silverman,“ Optimizations for ntru, In Public Key Cryptography and Computational Number Theory, (2000), 11-15.

[6] J. Hoffstein, J. H. Silverman, W. Whyte,“ On estimating the lattice security of NTRU, Technical Report 104, Cryptology ePrint Archive, (2005).

[7] J. Hoffstein, J. Pipher, J. H. Silverman, “An Introduction to Mathematical Cryptography, Science Business Media, Springer, (2014).

[8] C. Karimianpour. “Lattice-based cryptosystems, Master’s thesis, Ottawa, Canada, (2007).

[9] R. Kouzmenko. “Generalizations of the NTRU cryptosystem." Master’s thesis, Polytechnique, Montreal, Canada, (2006).

[10] A. J. Menezes, P. C. vanorschot, S. A. Vanstone.“ Handbook of applied cryptography, CRC Press, Boca Raton, Florida, (1996).

[11] M. Nevins, C. Karimianpour, A. Miri,“Ntru over rings beyond Z, Codes and Cryptography, 56(1)(2010), 65-78.

[12] J. Pipher, “Lectures on the NTRU encryption algorithm and digital signa- ture scheme, Brown University, (2002).

[13] R. D. Schafer,“ An Introduction to Nonassociative Alebras, Academic Press, New York, (1996).

[14] J. H. Silverman, “Dimension-reduced lattices, zero-forced lattices and the NTRU public key cryptosystem, Technical Report No. 13 (1999).

[15] N. Smart, F. Vercauteren, J. H. Silverman,“ An algebraic approach to NTRU $(q = 2^n)$ via Witt vectors and overdetermined systems of nonlinear equations, Amalfi, Italy, LNCS vol. 3352, Springer, (2004).

Author information

Khushboo Thakur, Department of Mathematics, Govt. N.P.G. College of Science, Raipur(C.G.), India.
E-mail: khushboo.thakur784@gmail.com

B.P.Tripathi, Department of Mathematics, Govt. N.P.G. College of Science, Raipur(C.G.), India.
E-mail: bhanu.tripathi@gmail.com

Received: June 2, 2016.
Accepted: September 23, 2016.