ISSN 0974 - 9373

Vol. 19 No.1 (2015) Journal of International Academy of Physical Sciences pp. 51-63

CSTRU: A NTRU-Like Public Key Cryptosystem Over Conic Sedenion Algebra

Khushboo Thakur and B. P. Tripathi

Department of Mathematics
Govt. N. P. G. College of Science, Raipur (C. G.), India
Email: khushboo.thakur784@gmail.com, bhanu.tripathi@gmail.com

Swati Verma

Department of Mathematics
Gurukul Mahila Mahavidyalaya, Raipur(C. G.), India
Email: swativerma15@gmail.com

(Received January 08, 2015)

Abstract: Conic sedenion from "C. Muses" hypernumbers are capable to express the Dirac equation in physics via their hyperbolic subalgebra, with electromagnetic eld and a counterpart on circular geometry proposed for quantum gravity. In this paper, we propose CSTRU by using conic sedenion algebra which is high speed probabilistic multi-dimensional public key cryptosystem that encrypt sixteen data vectors in each encryption and decryption process. The underlying algebraic structure of the proposed scheme is the non-commutative,non-associative, multiplicative modulus and multiplicative alternative conic sedenion algebra which can be de ned over any Dedekind domain such as convolution polynomial ring.

Keywords: NTRU, Conic Sedenion, Hyper number, Encryption, Decryption.

2010 Mathematics Classification No.: 94A60.

1. Inroduction

The NTRU public key cryptosystem was proposed by J. Hoffstein, J. Pipher and J. H. Silverman in 1996. It has since been standardized and implemented both for commercial applications[1] and open-source models[2]. Comparison with RSA cryptosystem and ECC cryptosystem, NTRU is faster and has signicantly smaller keys. Its security is conjectured to rely on the hardness of certain lattice problems, which are not known to be susceptible to quantum attack, NTRU is viewed as a quantum-resistant cryptosystem. One weakness of NTRU is the possibility of decryption failure.

In this paper, a new NTRU public key cryptosystem is proposed using conic sedenion algebra. Conic sedenions contains octonionsubalgebras with

hyperbolic (Minkowski) and circular (Euclidean) geometries[3, 4]. They form a 16 dimensional arithmetic which has a multiplicative modulus, but is non-commutative and nonassociative. They cannot be obtained through matrix-extension of traditional complex numbers or Cayley-Dickson constructs such as traditional quaternions, octonions, and further 2^n dimensional number systems on 1 real and (2^n-1) imaginary bases. Conic sedenions, instead, are built on 1 real basis, 7 imaginary bases i_n, 7 counterimaginary bases ε_n and 1 compound basis i_0 [5].CSTRU has been designed based on the Ntru core and exhibit high levels of similarity with full operand length. By using parallelism techniques we can increase the CSTRU encryption and decryption speed to a level even higher than NTRU.

2. NTRU Cryptosystem

A simple description of the NTRU cryptosystem is summarized in this section. For more details, the reader is referred to[6-11]. 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

$$F_p * f = 1(\text{mod } p) \text{ and } F_q * f = 1(\text{mod } q).$$

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

$$h = pF_q * g \,(\text{mod } q). \tag{1}$$

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 coecient of m is reduced modulo p. A random polynomial r is initially selected by the system, and the cipher text is calculated as follows,

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

2.3. Decryption Phase:

The decryption phase is performed as follows: the private key f is multiplied by the cipher text e such that,

$$a = f * e (\mathrm{mod}\, q)$$
$$a = f * (r * h + m) (\mathrm{mod}\, q)$$
$$a = f * h * r + f * m (\mathrm{mod}\, q)$$
$$a = pf * F_q * g * r + f * m (\mathrm{mod}\, q)$$
$$a = pg * r + f * m (\mathrm{mod}\, q).$$

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

3. Algebraic Structure of Conic Sedenion

In a sixteen dimension vector space, a conic sedenions set is denoted by S_c and denoted as:

$$S_c = a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3 + a_4 i_4 + a_5 i_5 + a_6 i_6 + a_7 i_7 + A_0 i_0 + A_1 \varepsilon_1 + A_2 \varepsilon_2 + A_2 \varepsilon_2 + A_3 \varepsilon_3 + A_4 \varepsilon_4 + A_5 \varepsilon_5 + A_6 \varepsilon_6 + A_7 \varepsilon_7$$

where $a_0 .... a_7, A_0 .... A_7 \in R$.

$$S_c = a_0 + \sum_{m=1}^{7} a_m i_m + A_0 i_0 + \sum_{n=1}^{7} A_n \varepsilon_n$$

where $1, a_0 ..... a_7$ and $A_0 ..... A_7$ are real number and $i_1, i_2, i_3, ... i_7$ are

imaginary bases, i_0 be the com-pound basis, $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7$ be the counterimaginary bases.

Now the imaginary bases, counterimaginary bases and compound bases are de ned as follows:

$$i_n^2 = -1 \text{ for } n = 1, 2, ..., 7 ,$$

$$\varepsilon_n^2 = 1 \text{ for } n = 1, 2, ..., 7$$

and

$$i_1\varepsilon_1 = i_2\varepsilon_2 = i_3\varepsilon_3 .....i_7\varepsilon_7 = i_0 .$$

Now above equation summarized by the following Table 1.

Table 1: Multiplication of bases of conic sedenion

X	1	i_1	i_2	i_3	i_4	i_5	i_6	i_7	i_0	ε_1	ε_2	ε_3	ε_4	ε_5	ε_6	ε_7
1	1	i_1	i_2	i_3	i_4	i_5	i_6	i_7	i_0	ε_1	ε_2	ε_3	ε_4	ε_5	ε_6	ε_7
i_1	i_1	-1	i_3	$-i_2$	i_5	$-i_4$	$-i_7$	i_6	$-\varepsilon_1$	i_0	ε_3	$-\varepsilon_2$	ε_5	$-\varepsilon_4$	$-\varepsilon_7$	ε_6
i_2	i_2	$-i_3$	-1	i_1	i_6	i_7	$-i_4$	$-i_5$	$-\varepsilon_2$	$-\varepsilon_3$	i_0	ε_1	ε_6	ε_7	$-\varepsilon_4$	$-\varepsilon_5$
i_3	i_3	i_2	$-i_1$	-1	i_7	$-i_6$	i_5	$-i_4$	ε_3	ε_2	$-\varepsilon_1$	i_0	ε_7	$-\varepsilon_6$	ε_5	$-\varepsilon_4$
i_4	i_4	$-i_5$	$-i_6$	$-i_7$	-1	i_1	i_2	i_3	$-\varepsilon_4$	$-\varepsilon_5$	$-\varepsilon_6$	$-\varepsilon_7$	i_0	ε_1	ε_2	ε_3
i_5	i_5	i_4	$-i_7$	i_6	$-i_1$	-1	$-i_3$	i_2	$-\varepsilon_5$	ε_4	$-\varepsilon_7$	ε_6	$-\varepsilon_1$	i_0	$-\varepsilon_3$	ε_2
i_6	i_6	i_7	i_4	$-i_5$	$-i_2$	i_3	-1	$-i_1$	$-\varepsilon_6$	ε_7	ε_4	$-\varepsilon_5$	$-\varepsilon_2$	ε_3	i_0	$-\varepsilon_1$
i_7	i_7	$-i_6$	i_5	i_4	$-i_3$	$-i_2$	i_1	-1	$-\varepsilon_7$	$-\varepsilon_6$	ε_5	ε_4	$-\varepsilon_3$	$-\varepsilon_2$	ε_1	i_0
i_0	i_0	$-\varepsilon_1$	$-\varepsilon_2$	$-\varepsilon_3$	$-\varepsilon_4$	$-\varepsilon_5$	$-\varepsilon_6$	$-\varepsilon_7$	-1	i_1	i_2	i_3	i_4	i_5	i_6	i_7
ε_1	ε_1	i_0	ε_3	$-\varepsilon_2$	ε_5	$-\varepsilon_4$	$-\varepsilon_7$	ε_6	i_1	1	$-i_3$	i_2	$-i_5$	i_4	i_7	i_6
ε_2	ε_2	$-\varepsilon_3$	i_0	ε_1	ε_6	ε_7	$-\varepsilon_4$	$-\varepsilon_5$	$-i_2$	i_3	1	$-i_1$	$-i_6$	$-i_7$	i_4	i_5
ε_3	ε_3	ε_2	$-\varepsilon_1$	i_0	ε_7	$-\varepsilon_6$	ε_5	$-\varepsilon_4$	i_3	$-i_2$	i_1	1	$-i_7$	i_6	$-i_5$	i_4
ε_4	ε_4	$-\varepsilon_5$	ε_6	$-\varepsilon_7$	i_0	ε_1	ε_2	ε_3	i_4	i_5	i_6	i_7	1	$-i_1$	$-i_2$	$-i_3$

ε_5	ε_5	ε_4	$-\varepsilon_7$	ε_6	$-\varepsilon_1$	i_0	$-\varepsilon_3$	ε_2	i_5	$-i_4$	i_7	$-i_6$	i_1	1	i_3	$-i_2$
ε_6	ε_6	ε_7	ε_4	$-\varepsilon_5$	$-\varepsilon_2$	ε_3	i_0	$-\varepsilon_1$	i_6	$-i_7$	$-i_4$	i_5	i_2	$-i_3$	1	i_1
ε_7	ε_7	$-\varepsilon_6$	ε_5	ε_4	$-\varepsilon_3$	$-\varepsilon_2$	ε_1	i_0	i_7	i_6	$-i_5$	$-i_4$	i_3	i_2	$-i_1$	1

Assuming F is an arbitrary Field. The conic sedenion algebra A can be defined over F as

$$A=b_0+b_1i_1+b_2i_2+b_3i_3+b_4i_4+b_5i_5+b_6i_6+b_7i_7+B_0i_0 + B_1\varepsilon_1+B_2\varepsilon_2+B_3\varepsilon_3+B_4\varepsilon_4+B_5\varepsilon_5+B_6\varepsilon_6+B_7\varepsilon_7,$$

where $b_0....b_7, B_0....B_7 \in R$.

Let A_0 and A_1 be two conic sedenion algebra such that:

$$A_0 = f_0+f_1i_1+f_2i_2+f_3i_3+f_4i_4+f_5i_5+f_6i_6+f_7i_7+F_0i_0 + F_1\varepsilon_1+F_2\varepsilon_2+F_3\varepsilon_3+F_4\varepsilon_4+F_5\varepsilon_5+F_6\varepsilon_6+F_7\varepsilon_7,$$

where $f_0....f_7, F_0....F_7 \in R_p$,

and

$$A_1=g_0+g_1i_1+g_2i_2+g_3i_3+g_4i_4+g_5i_5+g_6i_6+g_7i_7+G_0i_0 + G_1\varepsilon_1+G_2\varepsilon_2+G_3\varepsilon_3+G_4\varepsilon_4+G_5\varepsilon_5+G_6\varepsilon_6+G_7\varepsilon_7$$

where $g_0....g_7, G_0....G_7 \in R_q$.

Assume that $a_0,\ a_1 \in A_0$ (or A_1), such that

$$a_0=u_0+u_1i_1+u_2i_2+u_3i_3+u_4i_4+u_5i_5+u_6i_6+u_7i_7+U_0i_0 + U_1\varepsilon_1+U_2\varepsilon_2+U_3\varepsilon_3+U_4\varepsilon_4+U_5\varepsilon_5+U_6\varepsilon_6+U_7\varepsilon_7$$

and

$$a_1=v_0+v_1i_1+v_2i_2+v_3i_3+v_4i_4+v_5i_5+v_6i_6+v_7i_7+V_0i_0 + V_1\varepsilon_1+V_2\varepsilon_2+V_3\varepsilon_3+V_4\varepsilon_4+V_5\varepsilon_5+V_6\varepsilon_6+V_7\varepsilon_7\ .$$

Then, the Addition, Multiplication, Norm, Trace and Multiplicative Inverse are de ned as follows:

Addition: The addition of two conic sedenions corresponds to the usual addition of sixteen polyno-mials including $16N$ modular addition mod p or (mod q), i.e.,

$$\begin{aligned}a_0+a_1=&(u_0+v_0)+(u_1+v_1)i_1+(u_2+v_2)i_2+(u_3+v_3)i_3\\&+(u_4+v_4)i_4+(u_5+v_5)i_5+(u_6+v_6)i_6+(U_0+V_0)i_0\\&+(U_1+V_1)\varepsilon_1+(U_2+V_2)\varepsilon_2+(U_3+V_3)\varepsilon_3+(U_4+V_4)\varepsilon_4\\&+(U_5+V_5)\varepsilon_5+(U_6+V_6)\varepsilon_6+(U_7+V_7)\varepsilon_7.\end{aligned}$$

Multiplication: The multiplication of two conic sedenions is defined as

$$\begin{aligned}a_0*a_1=&(u_0V_0-u_1V_1-u_2V_2-u_3V_3-u_4V_4-u_5V_5-u_6V_6-u_7V_7-U_0v_0+U_1v_1+U_2v_2+U_3v_3\\&+U_4v_4+U_5v_5+U_6v_6+U_7v_7)+(u_0V_1+u_1V_0-u_2V_3+u_3V_2-u_4V_5+u_5V_4+u_6V_7\\&-u_7V_6+U_0v_1+U_1v_0+U_2v_3-U_3v_2+U_4v_5-U_5v_4-U_6v_7+U_7v_6)i_1+(u_0V_2+u_1V_3\\&+u_2V_0-u_3V_1-u_4V_6-u_5V_7+u_6V_4+u_7V_5+U_0v_2-U_1v_3+U_2v_0+U_3v_1+U_4v_6+U_5v_7\\&-U_6v_4-U_7v_5)i_2+(u_0V_3-u_1V_2+u_2V_1+u_3V_0-u_4V_7+u_5V_6-u_6V_5+u_7V_4+U_0v_3\\&+U_1v_2-U_2v_1+U_3v_0+U_4v_7-U_5v_6+U_6v_5-U_7v_4)i_3+(u_0V_4+u_1V_5+u_2V_6+u_3V_7\\&+u_4V_0-u_5V_1-u_6V_2-u_7V_3+U_0v_4-U_1v_5-U_2v_6-U_3v_7+U_4v_0+U_5v_1+U_6v_2\\&+U_7v_3)i_4+(u_0V_5-u_1V_4+u_2V_7-u_3V_6+u_4V_1+u_5V_0+u_6V_3-u_7V_2+U_0v_5+U_1v_4\\&-U_2v_7+U_3v_6-U_4v_1+U_5v_0-U_6v_3+U_7v_2)i_5+(u_0V_6-u_1V_7-u_2V_4+u_3V_5+u_4V_2\\&-u_5V_3+u_6V_0+u_7V_1+U_0v_6+U_1v_7+U_2v_4-U_3v_5-U_4v_2+U_5v_3+U_6v_0-U_7v_1)i_6\\&+(u_0V_7+u_1V_6-u_2V_5-u_3V_4+u_4V_3+u_5V_2-u_6V_1+u_7V_0+U_0v_7-U_1v_6+U_2v_5+U_3v_4\\&-U_4v_3-U_5v_2+U_6v_1+U_7v_0)i_7+(u_0V_0+u_1V_1+u_2V_2+u_3V_3+u_4V_4+u_5V_5+u_6V_6\\&+u_7V_7+U_0v_0+U_1v_1+U_2v_2+U_3v_3+U_4v_4+U_5v_5+U_6v_6+U_7v_7)i_0+(u_0V_1-u_1V_0\\&-u_2V_3+u_3V_2-u_4V_5+u_5V_4+u_6V_7-u_7V_6-U_0v_1+U_1v_0-U_2v_3+U_3v_2-U_4v_5+U_5v_4\\&+U_6v_7-U_7v_6)\varepsilon_1+(u_0V_2+u_1V_3-u_2V_0-u_3V_1-u_4V_6-u_5V_7+u_6V_4+u_7V_5-U_0v_2\\&+U_1v_3+U_2v_0-U_3v_1-U_4v_6-U_5v_7+U_6v_4+U_7v_5)\varepsilon_2+(u_0V_3-u_1V_2+u_2V_1-u_3V_0\\&-u_4V_7+u_5V_6-u_6V_5+u_7V_4-U_0v_3-U_1v_2+U_2v_1+U_3v_0-U_4v_7+U_5v_6-U_6v_5\\&+U_7v_4)\varepsilon_3+(u_0V_4+u_1V_5+u_2V_6+u_3V_7-u_4V_0-u_5V_1-u_6V_2-u_7V_3-U_0v_4+U_1v_5\\&+U_2v_6+U_3v_7+U_4v_0-U_5v_1-U_6v_2-U_7v_3)\varepsilon_4+(u_0V_5-u_1V_4+u_2V_7-u_3V_6+u_4V_1\\&-u_5V_0+u_6V_3-u_7V_2-U_0v_5-U_1v_4+U_2v_7-U_3v_6+U_4v_1+U_5v_0+U_6v_3-U_7v_2)\varepsilon_5\\&+(u_0V_6-u_1V_7-u_2V_4+u_3V_5+u_4V_2-u_5V_3-u_6V_0+u_7V_1-U_0v_6-U_1v_7-U_2v_4\\&+U_3v_5+U_4v_2-U_5v_3+U_6v_0+U_7v_1)\varepsilon_6+(u_0V_7+u_1V_6-u_2V_5-u_3V_4+u_4V_3+u_5V_2\\&-u_6V_1-u_7V_0-U_0v_7+U_1v_6-U_2v_5-U_3v_4+U_4v_3+U_5v_2-U_6v_1+U_7v_0)\varepsilon_7.\end{aligned}$$

Conjugate: The conjugate of sedenions algebra is defined as below

$$a_0^* = u_0(x) - u_1(x)i_1 - u_2(x)i_2 - u_3(x)i_3 - u_4(x)i_4 - u_5(x)i_5 - u_6(x)i_6 - u_7(x)i_7 - U_0(x)i_0 + U_1(X)\varepsilon_1 + U_2(X)\varepsilon_2 + U_3(X)\varepsilon_3 + U_4(X)\varepsilon_4 + U_5(X)\varepsilon_5 + U_6(X)\varepsilon_6 + U_7(X)\varepsilon_7.$$

Norm: We define the norm of a conic sedenion is defined as follows

$$\begin{aligned} N(a_0) = a_0 \times a_0^* = a_0^* \times a_0 = {} & (u_0(x))^2 + (u_1(x))^2 + (u_2(x))^2 + (u_3(x))^2 + (u_4(x))^2 \\ & + (u_5(x))^2 + (u_6(x))^2 + (u_7(x))^2 + (U_0(x))^2 \\ & + (U_1(x))^2 + (U_2(x))^2 + (U_3(x))^2 + (U_4(x))^2 \\ & + (U_5(x))^2 + (U_6(x))^2 + (U_7(x))^2. \end{aligned}$$

Multiplicative inverse:

$$\begin{aligned} N(a_0) \neq 0 \to a_0^{-1} = \frac{a_0^*}{N(a_0)} = {} & \big((u_0(x))^2 + (u_1(x))^2 + (u_2(x))^2 + (u_3(x))^2 + (u_4(x))^2 \\ & + (u_5(x))^2 + (u_6(x))^2 + (u_7(x))^2 + (U_0(x))^2 + (\varepsilon_1(x))^2 \\ & + (\varepsilon_2(x))^2 - (\varepsilon_3(x))^2 + (\varepsilon_4(x))^2 + (\varepsilon_5(x))^2 + (\varepsilon_6(x))^2 \\ & + (\varepsilon_7(x))^2\big)\big(u_0(x) - u_1(x)i_1 - u_2(x)i_2 - u_3(x)i_3 - u_4(x)i_4 \\ & - u_5(x)i_5 - u_6(x)i_6 - u_7(x)i_7 - U_0(x)i_0 + U_1(X)\varepsilon_1 + U_2(X)\varepsilon_2 \\ & + U_3(X)\varepsilon_3 + U_4(X)\varepsilon_4 + U_5(X)\varepsilon_5 + U_6(X)\varepsilon_6 + U_7(X)\varepsilon_7\big). \end{aligned}$$

4. Proposed Algorithm

The proposed cryptosystem is divided into three parts: Key generation, Encryption and Decryption.

4.1 Key Generation:

Step 1: Bob create a pair of public and private keys. He first randomly chooses two small conic sedenion F and G,
where

$$F = f_0 + f_1 i_1 + f_2 i_2 + f_3 i_3 + f_4 i_4 + f_5 i_5 + f_6 i_6 + f_7 i_7 + F_0 i_0 + F_1 \varepsilon_1 + F_2 \varepsilon_2 + F_3 \varepsilon_3 + F_4 \varepsilon_4 + F_5 \varepsilon_5 + F_6 \varepsilon_6 + F_7 \varepsilon_7, \quad f_0 \ldots\ldots f_7, F_0 \ldots\ldots F_7 \in L_f \subset A.$$

$$G = g_0 + g_1 i_1 + g_2 i_2 + g_3 i_3 + g_4 i_4 + g_5 i_5 + g_6 i_6 + g_7 i_7 + G_0 i_0 + G_1 \varepsilon_1 + G_2 \varepsilon_2 + G_3 \varepsilon_3 + G_4 \varepsilon_4 + G_5 \varepsilon_5 + G_6 \varepsilon_6 + G_7 \varepsilon_7, \quad g_0 \ldots\ldots g_7, G_0 \ldots\ldots G_7 \in L_g \subset A.$$

Step 2: Bob's next step is to compute the inverse of $F \bmod p$, $C \bmod p$, $W \bmod p$ and $G \bmod p$. Thus he computes F_p, G_p, C_p and W_p which satisfies

$$F * F_p = 1 (\bmod p) \; and \; F * F_q = 1 (\bmod q),$$

$$G * G_p = 1 (\bmod p) \; and \; G * G_q = 1 (\bmod q),$$

$$C * C_p = 1 (\bmod p) \; and \; C * C_q = 1 (\bmod q),$$

and

$$W * W_p = 1 (\bmod p) \; and \; W * W_q = 1 (\bmod q).$$

Step 3: Now the public key is calculated as follows

$$h = G * F_q (\bmod q), \text{ and } H = F_q (\bmod q).$$

Bob's private key is the pair of conic sedenion F and G and his public key is h and H.

4.2 Encryption:

Step 1: Suppose Alice (the encrypter) wants to send a message M to Bob (the decrypte).

Step 2: Next Alice randomly choose a conic sedenion $R \in L_R$ and use Bob's public key (h, H) to computes(the ciphertext e)

$$e = pR * h + H * M (\bmod q).$$

Step 3: The encrypted message E is send to Bob.

4.3 Decryption:

Step 1: To decrypt the ciphertext, Bob first compute,

$$A = f * E (\bmod q).$$

Step 2: Bob next computes the conic sedenions B

$$B = A (\bmod p).$$

Here we obtained B is the decrypted ciphertext which should be equal to original message M.

4.4 Correctness of Algorithm:

$$A = f * E (\text{mod}\, q)$$

$$A = f * (pR * h + H * M) (\text{mod}\, q)$$

$$A = (f * pR * G * F_q + f * F_q * M) (\text{mod}\, q)$$

$$A = pR * G + M (\text{mod} q)$$

Since

$$B = A (\text{mod}\, p)$$

$$B = pR * G + M (\text{mod}\, p)$$

$$B = pR * G (\text{mod}\, p) + M (\text{mod}\, p)$$

$$B = 0 + M (\text{mod}\, p)$$

$$B = M (\text{mod}\, p).$$

5. Analysis of Proposed Cryptosystem

In this section, we analyze the probability of successful decryption of proposed algorithm.

Successful Decryption: probability of successful decryption for proposed algorithm is calculated in the same way as NTRU and under the same assumptions considered in[9] and[10]. Moreover, for successful decryption in CSTRU, all hyper complex number coefficients of $f * E = (p * R * G + M)$ must lie in the interval $[-q + 1/2, +q - 1/2]$. Hence, we obtain

$$\begin{aligned} A &:= f * E = (pR * G + M) \\ &= a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3 + a_4 i_4 + a_5 i_5 + a_6 i_6 + a_7 i_7 + A_0 i_0 \\ &\quad + A_1 \varepsilon_1 + A_2 \varepsilon_2 + A_3 \varepsilon_3 + A_4 \varepsilon_4 + A_5 \varepsilon_5 + A_6 \varepsilon_6 + A_7 \varepsilon_7 \end{aligned}$$

where

$$\begin{aligned} d_0 &= p(r_0 G_0 - r_1 G_1 - r_2 G_2 - r_3 G_3 - r_4 G_4 - r_5 G_5 - r_6 G_6 - r_7 G_7 - R_0 g_0 \\ &\quad + R_1 g_1 + R_2 g_2 + R_3 g_3 + R_4 g_4 + R_5 g_5 + R_6 g_6 + R_7 g_7 + m_0) \end{aligned}$$

$$\begin{aligned} d_1 &= p(r_0 G_1 + r_1 G_0 - r_2 G_3 + r_3 G_2 - r_4 G_5 + r_5 G_4 + r_6 G_7 - r_7 G_6 + R_0 g_1 \\ &\quad + R_1 g_0 + R_2 g_3 - R_3 g_2 + R_4 g_5 - R_5 g_4 - R_6 g_7 + R_7 g_6 + m_1) \end{aligned}$$

$$\begin{aligned} d_2 &= p(r_0 G_2 + r_1 G_3 + r_2 G_0 - r_3 G_1 - r_4 G_6 - r_5 G_7 + r_6 G_4 + r_7 G_5 + R_0 g_2 \\ &\quad - R_1 g_3 + R_2 g_0 + R_3 g_1 + R_4 g_6 + R_5 g_7 - R_6 g_4 - R_7 g_5 + m - 2) \end{aligned}$$

$$d_3 = p(r_0G_3 - r_1G_2 + r_2G_1 + r_3G_0 - r_4G_7 + r_5G_6 - r_6G_5 + r_7G_4 + R_0g_3 + R_1g_2 - R_2g_1 + R_3g_0 + R_4g_7 - R_5g_6 + R_6g_5 - R_7g_4 + m_3)$$

$$d_4 = p(r_0G_4 + r_1G_5 + r_2G_6 + r_3G_7 + r_4G_0 - r_5G_1 - r_6G_2 - r_7G_3 + R_0g_4 - R_1g_5 - R_2g_6 - R_3g_7 + R_4g_0 + R_5g_1 + R_6g_2 + R_7g_3 + m_4)$$

$$d_5 = p(r_0G_5 - r_1G_4 + r_2G_7 - r_3G_6 + r_4G_1 + r_5G_0 + r_6G_3 - r_7G_2 + R_0g_5 + R_1g_4 - R_2g_7 + R_3g_6 - R_4g_1 + R_5g_0 - R_6g_3 + R_7g_2 + m_5)$$

$$d_6 = p(r_0G_6 - r_1G_7 - r_2G_4 + r_3G_5 + r_4G_2 - r_5G_3 + r_6G_0 + r_7G_1 + R_0g_6 + R_1g_7 + R_2g_4 - R_3g_5 - R_4g_2 + R_5g_3 + R_6g_0 - R_7g_1 + m_6)$$

$$d_7 = p(r_0G_7 + r_1G_6 - r_2G_5 - r_3G_4 + r_4G_3 + r_5G_2 - r_6G_1 + r_7G_0 + R_0g_7 - R_1g_6 + R_2g_5 + R_3g_4 - R_4g_3 - R_5g_2 + R_6g_1 + R_7g_0 + m_7)$$

$$D_0 = p(r_0G_0 + r_1G_1 + r_2G_2 + r_3G_3 + r_4G_4 + r_5G_5 + r_6G_6 + r_7G_7 + R_0g_0 + R_1g_1 + R_2g_2 + R_3g_3 + R_4g_4 + R_5g_5 + R_6g_6 + R_7g_7 + M_0)$$

$$D_1 = p(r_0G_1 - r_1G_0 - r_2G_3 + r_3G_2 - r_4G_5 + r_5G_4 + r_6G_7 - u_7G_6 - R_0g_1 + R_1g_0 - R_2g_3 + R_3g_2 - R_4g_5 + R_5g_4 + R_6g_7 - R_7g_6 + M_1)$$

$$D_2 = p(r_0G_2 + r_1G_3 - r_2G_0 - r_3G_1 - r_4G_6 - r_5G_7 + r_6G_4 + u_7G_5 - R_0g_2 + R_1g_3 + R_2g_0 - R_3g_1 - R_4g_6 - R_5g_7 + R_6g_4 + R_7g_5 + M_2)$$

$$D_3 = p(r_0G_3 - r_1G_2 + r_2G_1 - r_3G_0 - r_4G_7 + r_5G_6 - r_6G_5 + u_7G_4 - R_0g_3 - R_1g_2 + R_2g_1 + R_3g_0 - R_4g_7 + R_5g_6 - R_6g_5 + R_7g_4 + M_3)$$

$$D_4 = p(r_0G_4 + r_1G_5 + r_2G_6 + r_3G_7 - r_4G_0 - r_5G_1 - r_6G_2 - u_7G_3 - R_0g_4 + R_1g_5 + R_2g_6 + R_3g_7 + R_4g_0 - R_5g_1 - R_6g_2 - R_7g_3 + M_4)$$

$$D_5 = p(r_0G_5 - r_1G_4 + r_2G_7 - r_3G_6 + r_4G_1 - r_5G_0 + r_6G_3 - u_7G_2 - R_0g_5 - R_1g_4 + R_2g_7 - R_3g_6 + R_4g_1 + R_5g_0 + R_6g_3 - R_7g_2 + M_5)$$

$$D_6 = p(r_0G_6 - r_1G_7 - r_2G_4 + r_3G_5 + r_4G_2 - r_5G_3 - r_6G_0 + u_7G_1 - R_0g_6 - R_1g_7 - R_2g_4 + R_3g_5 + R_4g_2 - R_5g_3 + R_6g_0 + R_7g_1 + M_6)$$

$$D_7 = p(r_0G_7 + r_1G_6 - r_2G_5 - r_3G_4 + r_4G_3 + r_5G_2 - r_6G_1 - r_7G_0 - R_0g_7 + R_1g_6 - R_2g_5 - R_3g_4 + R_4g_3 + R_5g_2 - R_6g_1 + R_7g_0 + M_7)$$

Now, we obtain

$$P_r(R_{i,j}=1)=\frac{d_R}{N},\ P_r(R_{i,j}=-1)=\frac{d_R-1}{N}\approx\frac{d_R}{N},\ P_r(R_{i,j}=0)=\frac{N-2d_R}{N},$$

$$P_r(G_{i,j}=1)=P_r(G_{i,j}=-1)=\frac{d_G}{N},\quad P_r(G_{i,j}=0)=\frac{N-2d_G}{N},$$

$$P_r(m_{i,j}=j)=\frac{1}{p},\quad i=0,1,....7\quad j=\frac{-p+1}{2}.....\frac{+p-1}{2}.$$

where

$$R_i=[R_{i,0},R_{i,1},.....R_{i,N-1}],\quad i=0,.....7$$
$$G_i=[G_{i,0},G_{i,1},.....G_{i,N-1}],\quad i=0,.....7 \tag{3}$$

Under the above assumptions, we get $E[R_{i,j}]\approx 0$, $E[G_{i,j}]=0$ and $E[m_{i,j}]=0$. Therefore, we have

$$E[d_{i,j}]=0,\quad i=0,.....7\ \&\ \ j=0...N-1.$$

In order to calculate $Var[d_{i,j}]$, analogous to NTRU, it is sufficient to write

$$Var[R_{i,k}G_{j,l}]=\frac{4d_Rd_G}{N^2}\quad i,j=0,1,.....7\quad k,l=0.....N-1.$$

$$Var[m_{j,k}]=\frac{(p-1)(p+1)}{6}\quad j=0,1,.....7\quad k=0.....N-1.$$

As a result,

$$Var[d_{0,k}]=Var\left[\sum_{i+j=k}\begin{pmatrix}p(r_0G_0-r_1G_1-r_2G_2-r_3G_3-r_4G_4-r_5G_5-r_6G_6-r_7G_7-R_0g_0\\+R_1g_1+R_2g_2+R_3g_3+R_4g_4+R_5g_5+R_6g_6+R_7g_7+m_0)\end{pmatrix}\right]$$

Upon insertion of the values of $Var[R_{i,k}G_{j,l}]$ and $Var[m_{j,k}]$, we obtain

$$Var[d_{0,k}]=256p^2N\left(\frac{4d_Rd_G}{N^2}\right)+16N\left(\frac{(p-1)(p+1)}{6}\right)$$
$$=\frac{256\times 4p^2d_Rd_G}{N}+\frac{8N(p-1)(p+1)}{3}$$
$$=\frac{1024p^2d_Rd_G}{N}+\frac{8N(p-1)(p+1)}{3}$$

Similarly, we have

$$Var[d_{1,k}] = Var[d_{2,k}].....$$
$$= Var[D_{7,k}] \approx \frac{1024 p^2 d_R d_G}{N} + \frac{8N(p-1)(p+1)}{3} .$$

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

$$P_r = \left(|d_{i,k}| \le \frac{q-1}{2}\right)$$
$$= \left(-\frac{q-1}{2} \le a_{i,k} \le \frac{q-1}{2}\right)$$
$$= 2\phi\left(\frac{q-1}{2\sigma}\right) - 1, \quad i = 0,.....7, \quad k = 0.....N-1 ,$$

where ϕ denotes the distribution of the standard normal variable and $\sigma = \sqrt{= \frac{1024 p^2 d_R d_{CP}}{N} + \frac{8N(p-1)(p+1)}{3}}$.

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

- The probability for each of the messages $m_0,.....m_7$, $M_0,.....M_7$ to be correctly decrypted is

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

- The probability for all messages $m_0,.....m_7$, $M_0,.....M_7$ to be correctly decrypted is

$$\left(2\phi\left(\frac{q-1}{2\sigma}\right) - 1\right)^{16N} .$$

6. Remark

By changing the underlying ring of NTRU, the NTRU cryptosystem has been improved through the introduction of a new NTRU public key cryptosystem. This is constructed by replacing the base ring of NTRU with a conic sedenion algebra that resulted in the appearance of CSTRU cryptosystem. The conic sedenion algebra do not have a matrix representation and this feature causes that for its cryptanalysis with the help of the linear equation system[12].

References

1. Security Innovation, The Application Security Company, SSL Encryption Library, http://www.securityinnovation.com, 2012.

2. T. Buktu, The NTRU Project, http://ntru.sf.net/

3. Hyperbolic octonions are computationally identical to spilt-octonions. In addition, conic sedenions contain conic octonion subalgebras which exhibita mixed geometry.

4. J. Koplinger, Gravity and electromagnetism on conic sedenions. *Applied Mathematics and Computation*, **188** (2007) 948-953.

5. K. Carmody, Circular and Hyperbolic Quaternions, Octonions and Sedenions, *Appl. Math. Comput.* **28** (1988) 47-72, prepint http://www.kevincarmody.com/math/hypernumbers.html.

6. D. Coppersmith and A. Shamir, Lattice attacks on NTRU, in EUROCRYPT, (1997), 52-61.

7. J. Hoffstein, J. Pipher and J. H. Silverman, *NTRU: A ring-based public key cryptosystem*. In Lecture Notes in Computer Science Springer-Verlag, **1423** (1998) 267-288.

8. J. Hoffstein, J. Pipher and J. H. Silverman, *An Introduction to Mathematical Cryptography*, *Science Bussiness Media*, Springer, (2008).

9. J. Pipher, *Lectures on the NTRU encryption algorithm and digital signature scheme*, Brown University, 2002.

10. R. Kouzmenko, Generalizations of the NTRU cryptosystem. Master's thesis, Polytechnique, Montreal, Canada, 2006.

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

12. J. Koplinger, Signature of gravity in conic sedenions. *Applied Mathematics and Computation*, **188** (2007) 942-947.