Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 5 (2017), pp. 1447–1464

http://www.ripublication.com/gjpam.htm

STRU: A Non Alternative and Multidimensional Public Key Cryptosystem

Khushboo Thakur

Department of Mathematics,
Govt. N.P.G. College of Science,
Raipur (C.G.), India.

B.P. Tripathi

Department of Mathematics,
Govt. N.P.G. College of Science,
Raipur (C.G.), India.

Abstract

In this paper, we propose STRU by using sedenion algebra which is a non alternative and multi-dimensional public key cryptosystem based on the NTRU. Our scheme STRU encrypts sixteen data vectors in each encryption procedure. The underlying algebraic structure of STRU is a non associative and non alternative but power-associative 16 dimensional algebra with a quadratic form and whose element are constructed from real number R by iterations of the Cayley–Dickson Process. Moreover, it is neither a composition algebra nor a division algebra because it has zero divisors. Further, we provide the details of the key generation, encryption and decryption algorithms and discuss the object about key security, message security, and probability of successful decryption.

AMS subject classification: 94A60, 20N05, 17A45.
Keywords: NTRU, STRU, sedenion algebra, zero divisors, Cayley-Dickson Process, Encryption, Decryption.

1. Introduction

NTRU is a probabilistic public key cryptosystem that was first proposed by Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman in the rump session of Crypto' 96 and the first official paper was published in 1998 [15]. Compared to more well-known systems such as RSA or ECC, the greatest advantage of NTRU is that it is based on a class of basic arithmetic operations whose inherent complexity is rather low, amounting to $O(N^2)$ in worst-case. Computational efficiency along with low cost of implementation have turned NTRU into a very suitable choice for a large number of applications such as embedded systems, mobile phones, portable devices and resource constrained devices [1].

As a rough comparison, NTRU is hundreds of times faster than RSA and has a much faster key generation algorithm. However, there is an obvious drawback in using NTRU in that sometimes the decryption process fails to give the plaintext back with a very small probability (e.g., smaller than 2^{-80}) [3].

NTRU is classified as a lattice-based cryptosystem since its security is based on difficulty of hard-problems in certain types of lattices, contrary to RSA and ECC. On the other hand, NTRU is also classified as a probabilistic cryptosystem as each encryption involves a random vector (ephemeral key) and, hence, messages do not have unique encryptions.

During the past ten years, NTRU has been strictly analyzed by researchers and its main core is still assumed to be safe. Most sophisticated attacks against NTRU are based on lattice reduction techniques. Two famous lattice problems, Shortest Vector Problem (SVP) and Closest Vector Problem (CVP), have shown to be among NP-hard problems [12, 5, 7, 4]. However, the lattice problem arising in NTRU is classified as a Convolution Modular Lattice (CML) and it is not determined, yet, whether or not the cyclic structure of CML is going to help reducing the complexity of CVP or SVP. This issue has been considered in new versions of NTRU [8, 9].

In this paper by introducing a non-alternative and multidimensional public key cryptosystem. We will prove that a lattice based public key cryptosystem based on non-alternative algebra is not sufficient but also possibly more secure then Ntru, because its lattice does not completely fit within Circular and Convolutional Modular Lattice.

In completely even circumstances, i.e., choosing the same parameters for both NTRU and STRU, STRU works sixteen times slower than NTRU and the data are encrypted simultaneously as sixteen vectors. Other than changing the underlying algebra, no other change has been made. In particular, STRU keeps the probabilistic properties of NTRU. Hence the main advantages of the proposed cryptosystem would be higher security and the increase of parallelism levels. Since sixteen vectors of data are encrypted simultaneously in each system call, STRU can be considered as a multidimensional cryptosystem. As a result of high complexity of the STRU lattice, the dimension can be reduced. Hence, the imposed speed reduction caused by sedenionic processing, can be compensated.

This paper is organized as follows: Section 2 summarizes the NTRU cryptosystem. Then, Section 3 includes a brief introduction to sedenion algebras. We dedicate Section 4 to introducing the algebraic structure of STRU. Then, Sections 5 and 6 are devoted to the description of STRU and general analysis of the scheme.

2. The NTRU Cryptosystem

The basic operations in NTRU take place in the ring $Z[x]/(x^N - 1)$, which is known as the ring of convolution polynomial of rank N, where N is a prime [16]. Let define the following three rings: $\Re = Z[x]/(x^N - 1)$, $\Re_p = (Z/pZ)[x]/(x^N - 1)$, and $\Re_q = (Z/qZ)[x]/(x^N - 1)$. An element f of the rings $\Re$, $\Re_p$, $\Re_q$ can be written as a polynomial or a vector of coefficients: $\mathrm{f} = \Sigma_{i=0}^{N-1} f_i.x_i \triangleq [f_0, f_1, \ldots, f_{N-1}]$. In the convolution rings, addition corresponds to the ordinary polynomials addition, i.e., element-wise vector addition. But multiplication, is denoted by $*$ is explicitly defined as follows,

$$f(x) := \sum_{i=0}^{N-1} f_i.x^i = [f_0, f_1, \ldots, f_{N-1}]_{1\times N}, f_i \in Z.$$

$$g(x) := \sum_{i=0}^{N-1} g_i.x^i = [g_0, g_1, \ldots, g_{N-1}]_{1\times N}, g_i \in Z.$$

$$h(x) := \sum_{i=0}^{N-1} h_i.x^i = [h_0, h_1, \ldots, h_{N-1}]_{1\times N}, h_i \in Z.$$

$$h_k := \sum_{i=0}^{k} f_i.g_{k-i} + \sum_{i=k+1}^{N-1} f_i.g_{N+k-i} = \sum_{i+j=k} f_i.g_j.$$

Clearly, addition and multiplication in $\Re_p$ or $\Re_q$ are equivalent to performing the same operations in $\Re$ and ultimately reducing the resulting coefficients mod p or mod q.

Let d_f, d_g, d_ϕ, and d_m be constant integers less than N. These are the public parameters of the cryptosystem and determine the distribution of the coefficients of the polynomials. Based on these constants, we shall define the subsets $L_f, L_m, L_{\acute{A}}, L_g \subset \Re$ according to the criteria presented in Table 1. With this notations and definitions, the Ntru public key cryptosystem can now be described as follows.

Public Parameters: The public parameters (N, p, q, d) in NTRU are assumed to be fixed and must be agreed upon by both the sender and the receiver. N and p are prime numbers such that $gcd(p, q) = gcd(N, q) = 1$ and $q >> p$. Usual value include $N = 167$ for moderate security, $N = 251$ for high security, and $N = 503$ for very high security along with p=3 and $d \approx \frac{N}{3}$.

Key Generation: To create an NTRU key, first two small polynomials $g \in L_g$ and $f \in L_f$ are randomly generated. The polynomial f must be invertible in R_p and R_q. When f is randomly selected from the subset L_f, the probability for this polynomial to be invertible in R_p and R_q is very high. However, in rare event that f is not invertible, a new polynomial f can be easily generated.

The inverse of f over R_p and R_q are computed using the extended Euclidian algorithm. We call those two inverses f_p^{-1} and f_q^{-1}, respectively. Hence, we have $f* f_p^{-1} \equiv$

Table 1: Definition of public parameters of NTRU

Notation	Definition	Typical Value for N=167, p=3, q=128
L_f	$\{f \in \Re \mid f$ has d_f coefficients equal to $+1$, $(d_f - 1)$ equal to -1, the rest $0\}$	$d_f = 61$
L_g	$\{g \in \Re \mid g$ has d_f coefficients equal to $+1$, $(d_g - 1)$ equal to -1, the rest $0\}$	$d_g = 61$
L_ϕ	$\{\phi \in \Re \mid \phi$ has d_f coefficients equal to $+1$, $(d_\phi - 1)$ equal to -1, the rest $0\}$	$d_\phi = 61$
L_m	$\{m \in \Re \mid$ coefficients of m are chosen modulo p, between $-p/2$ and $p/2\}$	

$1(modp)$ and $f * f_q^{-1} \equiv 1(modq)$. While f, g, f_p^{-1} and f_q^{-1} are kept private, the public key h is computed in the following manner

$$h = f_q^{-1} * g(modq).$$

Encryption: The system initially selects a random polynomial $\phi \in L_\phi$, called the ephemeral key, and cipher the input message to a polynomial $m \in L_m$. The ciphertext is computed as follows:

$$e = p.h * \phi + m(modq).$$

Note that p is a constant parameter and we can pre-compute the polynomial p.h. Hence, disregarding the time required for generating the ephemeral key and transforming the incoming message into the polynomial m, the encryption process demands N^2 multiplication and N addition mod q.

Decryption: The first step of the decryption process starts by multiplying (convolving) the received polynomial e by the private key f

$$\begin{aligned}
a &= f * e(modq).\\
a &= f * (p.h * \phi + m)(modq)\\
a &= p.f * h * \phi + f * m(modq)\\
a &= p.f * f_q^{-1} * g * \phi + f * m(modq)\\
a &= p.g * \phi + f * m(modq)
\end{aligned}$$

In the second step, the coefficients of $a \in \Re_q$ are identified with the equivalent representatives in the interval $[-q/2, +q/2]$. Assuming that the public parameters have been chosen properly, the resulting polynomial is exactly equal to $p.g * \phi + f * m(modq)$ in $\Re$. With this assumption, when we reduce the coefficients of a mod p, the term $p.g * \phi$ vanishes and $f * m(modp)$ remains. In order to extract the message m, it is enough to

multiply $f * m(modp)$ by f_p^{-1}.

Decryption Failure: If the public parameters (N, p, q, d) are chosen to satisfy $q > (6d+1)p$ then decryption process will never fail. However, to have a better performance and also to reduce the size of the public key, smaller value of q may be chosen for q such that the probability of decryption failure be very small of order 2^{-80} [3]. Successful decryption depends on whether or not $|p.g * \phi + f * m|_\infty < q$. Through a few simple probabilistic calculations [17], the approximate bound for successful decryption probability can be calculated as follows

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

where ϕ denotes the distribution of the standard normal variable and

$$\sigma \approx \sqrt{\frac{36d_f.d_g}{N} + \frac{8d_f}{6}}.$$

3. A Brief Introduction to Sedenion Algebra

The algebras C (complex numbers), H (quaternions), and O (octonions) are real division algebras obtained from the real numbers R by a doubling procedure called the Cayley-Dickson Process. By doubling R (dim 1), we obtain C (dim 2), then C produces H (dim 4), and H yields O (dim 8), The next doubling process applied to O then yields an algebra S (dim 16) called the sedenions. The world sedenion is derived from sexdecim, meaning sixteen.The real sedenion or hexadecanions is denoted by S. The sedenion is a non-commutative, non-associative, non-alternative, but power-associative 16 dimensional algebra with a quadratic form and whose elements are constructed from real numbers R by iterations of the Cayley-Dickson Process [10, 11]. Moreover, it is neither a composition algebra nor a division algebra because it has zero divisors. This means that there exist sedenions $a, b \neq 0$ such that $ab = 0$. The sedenions have multiplicative identity element and multiplicative inverse.

Notation: Let $2^4 = 16$ basis elements of the sedenion algebra S be represented by the set $S_E = \{e_0, e_1, e_2, \ldots, e_{15}\}$, where e_0 is the identity element and $e_1, \ldots, e_{15}$ are called imaginaries. Then every sedenion is a linear combination of the unit sedenions $e_0, e_1, e_2, \ldots, e_{15}$, which form a basis of the vector space of sedenions. Every sedenion can be represented in the form,

$$S = x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3 + \cdots + x_{14}e_{14} + x_{15}e_{15}$$

$$S = \{x_0 + \sum_{i=1}^{15} x_ie_i | x_0, \ldots, x_{15} \in \Re\}$$

where $x_i \in \Re$. Here x_0 is called the real part of S while $\sum_{i=1}^{15} x_i e_i$ is called its imaginary part.

The addition of two sedenion is performed by adding corresponding coefficients (i.e., element-wise) but multiplication is defined by bilinearity and the multiplication rule of the base elements. Thus, if $x, y \in S$, we have:

$$xy = \left(\sum_{i=0}^{15} x_i e_i\right)\left(\sum_{i=0}^{15} y_j e_i\right) = \sum_{i,j=0}^{15} x_i y_j (e_i e_j) \sum_{i,j,k=1}^{15} f_{ij}\gamma_{ij}^{k} e_k$$

where $e_i, e_j, e_k \in E_{16}$, $f_{ij} = x_i y_j \in \Re$, and the quantities $\gamma_{ij}^{k} \in \Re$ are called structure constants. The multiplication rule of the sedenion base elements is given by

$$e_i e_j = \sum_{k=0}^{15} \gamma_{ij}^{k} e_k$$

and is summarized in Table 2 [13]

Table 2: The multiplication Table Of The Sedenion element

×	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}
e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}
e_1	e_1	$-e_0$	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6	e_9	$-e_8$	$-e_{11}$	e_{10}	$-e_{13}$	e_{12}	e_{15}	$-e_{14}$
e_2	e_2	$-e_3$	$-e_0$	e_1	e_6	e_7	$-e_4$	$-e_5$	e_{10}	e_{11}	$-e_8$	$-e_9$	$-e_{14}$	$-e_{15}$	e_{12}	e_{13}
e_3	e_3	e_2	$-e_1$	$-e_0$	e_7	$-e_6$	e_5	$-e_4$	e_{11}	$-e_{10}$	e_9	$-e_8$	$-e_{15}$	e_{14}	$-e_{13}$	e_{12}
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	$-e_0$	e_1	e_2	e_3	e_{12}	e_{13}	e_{14}	e_{15}	$-e_8$	$-e_9$	$-e_{10}$	e_{11}
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	$-e_0$	$-e_3$	e_2	e_{13}	$-e_{12}$	e_{15}	$-e_{14}$	e_9	$-e_8$	e_{11}	$-e_{10}$
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	$-e_0$	$-e_1$	e_{14}	$-e_{15}$	$-e_{12}$	e_{13}	e_{10}	$-e_{11}$	$-e_8$	e_9
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	$-e_0$	e_{15}	e_{14}	$-e_{13}$	$-e_{12}$	e_{11}	e_{10}	$-e_9$	e_8
e_8	e_8	$-e_9$	$-e_{10}$	$-e_{11}$	$-e_{12}$	$-e_{13}$	$-e_{14}$	$-e_{15}$	$-e_0$	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_9	e_9	e_8	$-e_{11}$	e_{10}	$-e_{13}$	e_{12}	e_{15}	$-e_{14}$	$-e_1$	$-e_0$	$-e_3$	e_2	$-e_5$	e_4	e_7	$-e_6$
e_{10}	e_{10}	e_{11}	e_8	$-e_9$	$-e_{14}$	$-e_{15}$	e_{12}	e_{13}	$-e_2$	e_3	$-e_0$	$-e_1$	$-e_6$	$-e_7$	e_4	e_5
e_{11}	e_{11}	$-e_{10}$	e_9	e_8	$-e_{15}$	e_{14}	$-e_{13}$	e_{12}	$-e_3$	$-e_2$	e_1	$-e_0$	$-e_7$	e_6	$-e_5$	e_4
e_{12}	e_{12}	e_{13}	e_{14}	e_{15}	e_8	$-e_9$	$-e_{10}$	$-e_{11}$	$-e_4$	e_5	e_6	e_7	$-e_0$	$-e_1$	$-e_2$	$-e_3$
e_{13}	e_{13}	$-e_{12}$	e_{15}	$-e_{14}$	e_9	e_8	e_{11}	$-e_{10}$	$-e_5$	$-e_4$	e_7	$-e_6$	e_1	$-e_0$	e_3	$-e_2$
e_{14}	e_{14}	$-e_{15}$	$-e_{12}$	e_{13}	e_{10}	$-e_{11}$	e_8	e_9	$-e_6$	$-e_7$	$-e_4$	e_5	e_2	$-e_3$	$-e_0$	e_1
e_{15}	e_{15}	e_{14}	$-e_{13}$	$-e_{12}$	e_{11}	e_{10}	$-e_9$	e_8	$-e_7$	e_6	$-e_5$	$-e_4$	e_3	e_2	$-e_1$	$-e_0$

Multiplication is neither commutative nor associative but is power-associative and have zero divisors. The conjugate and square norm of an sedenion $x = x_0 + \sum_{i=1}^{15} x_i e_i$ are given by [18] $x^* = x_0 - \sum_{i=1}^{15} x_i e_i$ and $N(x) = x.x^* = x^*.x = \sum_{i=0}^{15} x_i^2$ respectively. Every non-zero element in S has a unique multiplicative inverse which is given by $x^{-1} = N(x)^{-1}.x^*$.

Now, suppose that $\Re$ is an arbitrary finite ring of odd characteristic. We can define the sedenion algebra A over $\Re$ as follows

$$A = \{x_0 + \sum_{i=1}^{15} x_i e_i | x_0, \ldots, x_{15} \in \Re\} \tag{3.1}$$

with the same multiplication defined for the real sedenion. The algebra A is a non-associative algebra with a norm and multiplicative inverse that has much the same properties as the real sedenion algebra S.

Note that the sedenion algebra is non-associative and consequently does not have any matrix representation because ordinary matrix multiplication is always associative.

4. Algebraic Structure of STRU

Consider the convolution polynomial rings $\Re := Z[x]/(x^N-1)$, $\Re_p := Z_p[x]/(x^N-1)$, and $\Re_q := Z_q[x]/(x^N-1)$ that are used in Ntru. 'We define three sedenion algebras A, A_p and A_q as follows

$$A := \{a_0(x) + \sum_{i=1}^{15} a_i(x).e_i | a_0(x), \ldots, a_{15}(x) \in \Re\} \tag{4.1}$$

$$A_p := \{a_0(x) + \sum_{i=1}^{15} a_i(x).e_i | a_0(x), \ldots, a_{15}(x) \in \Re_p\} \tag{4.2}$$

$$A_q := \{a_0(x) + \sum_{i=1}^{15} a_i(x).e_i | a_0(x), \ldots, a_{15}(x) \in \Re_q\} \tag{4.3}$$

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 sedenionic nonassociative split algebras similar to S. Let us detailed more on algebras A_p and A_q.

$$\begin{aligned} A_p :&= \{a_0(x) + \sum_{i=1}^{15} a_i(x).e_i | a_0(x), \ldots, a_{15}(x) \in \Re_p\} \\ &= \{f_0 + f_1.e_1 + \cdots + f_{15}.e_{15} | f_0 \ldots\ldots\ldots f_{15} \subset A_p\} \end{aligned}$$

$$\begin{aligned} A_q :&= \{a_0(x) + \sum_{i=1}^{15} a_i(x).e_i | a_0(x), \ldots, a_{15}(x) \in \Re_q\} \\ &= \{g_0 + g_1.e_1 + \cdots + g_{15}.e_{15} | g_0 \ldots\ldots\ldots g_{15} \subset A_q\} \end{aligned}$$

Now assume that $s_1, s_2 \in A_p$ (or A_q) where,

$$\begin{aligned} s_1 &= f_0(x) + f_1(x).e_1 + \cdots + f_{15}(x).e_{15}, \\ s_2 &= g_0(x) + g_1(x).e_1 + \cdots + g_{15}(x).e_{15}. \end{aligned}$$

Then, the Addition, Multiplication, Norm, Trace and Multiplicative Inverse are defined in the below:

- **Addition:** The addition of two sedenions corresponds to the usual addition of sixteen polynomials including 16N modular addition mod p (mod q), i.e.,

$$\begin{aligned} s_1 + s_2 = {} & (f_0(x) + g_0(x)) + (f_1(x) + g_1(x)).e_1 + (f_2(x) + g_2(x)).e_2 + (f_3(x) \\ & + g_3(x)).e_3 + (f_4(x) + g_4(x)).e_4 + (f_5(x) + g_5(x)).e_5 + (f_6(x) \\ & + g_6(x)).e_6 + (f_7(x) + g_7(x)).e_7 + (f_8(x) + g_8(x)).e_8 \\ & + (f_9(x) + g_9(x)).e_9 + (f_{10}(x) + g_{10}(x)).e_{10} + (f_{11}(x) + g_{11}(x)).e_{11} \\ & + (f_{12}(x) + g_{12}(x)).e_{12} + (f_{13}(x) + g_{13}(x)).e_{13} + (f_{14}(x) + g_{14}(x)).e_{14} \\ & + (f_{15}(x) + g_{15}(x)).e_{15}. \end{aligned}$$

- **Multiplication:** The multiplication of two sedenions is defined by

$s_1 \star s_2$=$(f_0g_0 - f_1g_1 - f_2g_2 - f_3g_3 - f_4g_4 - f_5g_5 - f_6g_6 - f_7g_7 - f_8g_8 - f_9g_9 - f_{10}g_{10} - f_{11}g_{11} - f_{12}g_{12} - f_{13}g_{13} - f_{14}g_{14} - f_{15}g_{15})$
$+(f_0g_1 + f_1g_0 + f_2g_3 - f_3g_2 + f_4g_5 - f_5g_4 - f_6g_7 + f_7g_6 + f_8g_9 - f_9g_8 - f_{10}g_{11} + f_{11}g_{10} - f_{12}g_{13} + f_{13}g_{12} + f_{14}g_{15} - f_{15}g_{14}).e_1$
$+(f_0g_2 - f_1g_3 + f_2g_0 + f_3g_1 + f_4g_6 + f_5g_7 - f_6g_4 - f_7g_5 + f_8g_{10} + f_9g_{11} - f_{10}g_8 - f_{11}g_9 - f_{12}g_{14} - f_{13}g_{15} + f_{14}g_{12} + f_{15}g_{13}).e_2$
$+(f_0g_3 + f_1g_2 - f_2g_1 + f_3g_0 + f_4g_7 - f_5g_6 + f_6g_5 - f_7g_4 + f_8g_{11} - f_9g_{10} + f_{10}g_9 - f_{11}g_8 - f_{12}g_{15} + f_{13}g_{14} - f_{14}g_{13} + f_{15}g_{12}).e_3$
$+(f_0g_4 - f_1g_5 - f_2g_6 - f_3g_7 + f_4g_0 + f_5g_1 + f_6g_2 + f_7g_3 + f_8g_{12} + f_9g_{13} + f_{10}g_{14} + f_{11}g_{15} - f_{12}g_8 - f_{13}g_9 - f_{14}g_{10} - f_{15}g_{11}).e_4$
$+(f_0g_5 + f_1g_4 - f_2g_7 + f_3g_6 - f_4g_1 + f_5g_0 - f_6g_3 + f_7g_2 + f_8g_{13} - f_9g_{12} + f_{10}g_{15} - f_{11}g_{14} + f_{12}g_9 - f_{13}g_8 + f_{14}g_{11} - f_{15}g_{10}).e_5$
$+(f_0g_6 + f_1g_7 + f_2g_4 - f_3g_5 - f_4g_2 + f_5g_3 + f_6g_0 - f_7g_1 + f_8g_{14} - f_9g_{15} - f_{10}g_{12} + f_{11}g_{13} + f_{12}g_{10} - f_{13}g_{11} - f_{14}g_8 + f_{15}g_9).e_6$
$+(f_0g_7 - f_1g_6 + f_2g_5 + f_3g_4 - f_4g_3 - f_5g_2 + f_6g_1 + f_7g_0 + f_8g_{15} + f_9g_{14} - f_{10}g_{13} - f_{11}g_{12} + f_{12}g_{11} + f_{13}g_{10} - f_{14}g_9 - f_{15}g_8).e_7$
$+(f_0g_8 - f_1g_9 - f_2g_{10} - f_3g_{11} - f_4g_{12} - f_5g_{13} - f_6g_{14} - f_7g_{15} + f_8g_0 + f_9g_1 + f_{10}g_2 + f_{11}g_3 + f_{12}g_4 + f_{13}g_5 + f_{14}g_6 + f_{15}g_7).e_8$
$+(f_0g_9 + f_1g_8 - f_2g_{11} + f_3g_{10} - f_4g_{13} + f_5g_{12} + f_6g_{15} - f_7g_{14} - f_8g_1 + f_9g_0 - f_{10}g_3 + f_{11}g_2 - f_{12}g_5 + f_{13}g_4 + f_{14}g_7 - f_{15}g_6).e_9$
$+(f_0g_{10} + f_1g_{11} + f_2g_8 - f_3g_9 - f_4g_{14} - f_5g_{15} + f_6g_{12} + f_7g_{13} - f_8g_2 + f_9g_3 + f_{10}g_0 - f_{11}g_1 - f_{12}g_6 - f_{13}g_7 + f_{14}g_4 + f_{15}g_5).e_{10}$
$+(f_0g_{11} - f_1g_{10} + f_2g_9 + f_3g_8 - f_4g_{15} + f_5g_{14} - f_6g_{13} + f_7g_{12} - f_8g_3 - f_9g_2 + f_{10}g_1 + f_{11}g_0 - f_{12}g_7 + f_{13}g_6 - f_{14}g_5 + f_{15}g_4).e_{11}$
$+(f_0g_{12} + f_1g_{13} + f_2g_{14} + f_3g_{15} + f_4g_8 - f_5g_9 - f_6g_{10} - f_7g_{11} - f_8g_4 + f_9g_5 + f_{10}g_6 + f_{11}g_7 + f_{12}g_0 - f_{13}g_1 - f_{14}g_2 - f_{15}g_3).e_{12}$
$+(f_0g_{13} - f_1g_{12} + f_2g_{15} - f_3g_{14} + f_4g_9 + f_5g_8 + f_6g_{11} - f_7g_{10} - f_8g_5 - f_9g_4 + f_{10}g_7 - f_{11}g_6 + f_{12}g_1 + f_{13}g_0 + f_{14}g_3 - f_{15}g_2).e_{13}$
$+(f_0g_{14} - f_1g_{15} - f_2g_{12} + f_3g_{13} + f_4g_{10} - f_5g_{11} + f_6g_8 + f_7g_9 - f_8g_6 - f_9g_7 - f_{10}g_4 + f_{11}g_5 + f_{12}g_2 - f_{13}g_3 + f_{14}g_0 + f_{15}g_1).e_{14}$
$+(f_0g_{15} + f_1g_{14} - f_2g_{13} - f_3g_{12} + f_4g_{11} + f_5g_{10} - f_6g_9 + f_7g_8 - f_8g_7 + f_9g_6 -$

$f_{10}g_5 - f_{11}g_4 - f_{12}g_3 + f_{13}g_2 - f_{14}g_1 + f_{15}g_0).e_{15},$

Here $\star$ denotes the convolution product. sedenion multiplication in A_p (or A_q) needs 256 polynomial convolutions and 240 polynomial addition modulo $p(q)$, which together account for $256.N^2$ modular multiplications and (256N(N-1)+240N) modular additions.

- **Conjugate:** The conjugate of sedenions which is defined as below needs 15N negations mod p or q.

$$s^* = +f_0(x) - f_1(x)e_1 - f_2(x)e_2 - f_3(x)e_3 - \cdots - f_{15}(x)e_{15}$$

- **Norm:** we define the norm of a sedenion S, defined as follows

$$N(s_1) = s_1 \times {s_1}^* = {s_1}^* \times s_1 = (f_0(x))^2 + (f_1(x))^2 + (f_2(x))^2 + (f_0(x))^2 + \cdots + (f_{15}(x))^2$$

Totally, $16N^2$ multiplications and (16N(N-1)+15N) additions are required for calculating the squared norm of an sedenions.

- **Multiplicative inverse:**

$$N(s_1) \neq 0 \rightarrow s^{-1} = \frac{{s_1}^*}{N(s_1)} = ((f_0(x))^2 + (f_1(x))^2 + (f_2(x))^2 + (f_0(x))^2 + \cdots + (f_{15}(x))^2)^{-1}.(f_0(x) - f_1(x).e_1 - f_2(x).e_2 - f_3(x).e_3 - \cdots - f_{15}(x).e_{15})$$

Thus, the following operations will be needed for calculating the multiplicative inverse of an element in A_p or A_q

1. Calculation of $g(x) \leftarrow N(s)$ over the ground ring $(Z/pZ)[x]/(x^N - 1)$ and $(Z/qZ)[x]/(x^N - 1)$ at the total cost of $16N^2$ multiplications and (16N(N-1)+15N) additions.
2. Finding the inverse of $g(x)$ over the ground ring using the extended Euclid algorithm with a running time of $O(N^2)$ [14].
3. Conjugation of s including $15N$ negations.
4. Calculation of $g^{-1}(x).s^*$ including $16N^2$ multiplication and $16N(N-1)$ addition modulo p or q.

After setting up the required notation and algebras A, A_p and A_q, we describe STRU.

5. Proposed Scheme: STRU

In the STRU cryptosystem, encryption and decryption are taken place in a multi-dimensional vector space and similar to Ntru, the security of the cryptosystem depends on three parameters (N, p, q) and four subsets $L_f, L_m, L_f, L_g \subset A$ as defined in Table I. N, p and q, d_f, d_g, d_f are constant parameters which play a similar role as in Ntru except that for simplicity these constants are supposed to be all prime numbers. Now proposed scheme is divided into three parts: Key Generation, Encryption and Decryption as follows,

a) Key Generation: In order to generate a pair of public and private keys, initially, two small sedenion F and G are randomly generated.

$$F := f_0 + f_1.e_1 + f_2.e_2 + \cdots + f_{15}.e_{15} \in A \qquad f_0.....f_{15} \in L_f \subset A$$

$$G := g_0 + g_1.e_1 + g_2.e_2 + \cdots + g_{15}.e_{15} \in A \qquad g_0.....g_{15} \in L_g \subset A$$

The sedenion F must be invertible over A_p and A_q. If such an inverse does not exist i.e., when $\sum_{i=0}^{15} f_i^2(x)$ is not invertible in $Z_p[x]/(x^N - 1)$, and $Z_q[x]/(x^N - 1)$, a new sedenion F will be generated. The inverses of F over the algebras A_p and A_q are denoted by ${F_p}^{-1}$ and ${F_q}^{-1}$ The public key, which is an sedenion, is computed as follows

$$H = F_q \star G \tag{5.1}$$

The sedenions F, F_p and F_q are kept secret in order to be used in the decryption phase. One can estimate that the key generation of STRU is 256 times slower than that of Ntru, when the same parameters (N, p, q) are used in both cryptosystems. However, in STRU, we can definitely work with a lower dimension N, without reducing the system security.

b) Encryption: In the encryption process, the cryptosystem initially generates a random sedenion, called the blinding sedenion. Incoming data must be converted into a sedenion including sixteen polynomial in L_ϕ based on a simple conversion. The ciphertext E is then calculated as follows

$$E = p.H \star \phi + M \in A_q \tag{5.2}$$

c) Decryption: The received encryption E is first multiplied by the private key F

$$\begin{aligned} F \star E &= (F \star (p.H \star \phi + M))modq \\ &= (F \star p.H \star \phi + F \star M)modq \\ &= (p.F \star F_q \star G \star \phi + F \star M)modq \\ &= (p.G \star \phi + F \star M). \end{aligned}$$

The coefficients of the sixteen polynomials in the resulting sedenion must be reduced mod q into the interval $(-q/2, +q/2]$. Upon suitable selection of the cryptosystem

constant parameters, the coefficients of the sixteen polynomial in $(p.G \star \phi + F \star M)$ will most probably be within $(-q/2, +q/2]$ and the last reduction mod q will not be required. With such an assumption, when the result of $(p.G \star \phi + F \star M)$ is reduced mod p, the term $p.G \star \phi$ vanishes and the $F \star M$ (modp) remains. In order to extract the original message M it will be sufficient to multiply $F \star M$ mod p by F_p and adjust the resulting coefficients within the interval $[-p/2, +p/2]$.

One can estimate that the encryption and decryption algorithms in STRU with the same dimension N are about 16 and 32 times slower than that of Ntru, however, in STRU we can work with a lower dimension N, without reducing the cryptosystem security. Also, similar to Ntru, STRU can be optimized for efficiency based on the various optimization methods proposed in [6]. In addition, there are multiple parallelism levels in the proposed scheme that can be exploited to improve encryption and decryption speed.

6. Analyzing of STRU cryptosystem

In this section, we analyze STRU and discuss the probability of successful decryption, key security, message security, and the message expansion rate.

Successful Decryption: Probability of successful decryption in STRU is calculated in the same way as NTRU and under the same assumptions considered in [16] and [17]. Moreover, for successful decryption in STRU, all sedenion coefficients of $F \star E = (p.G \star \phi + F \star M)$ must lie in the interval $[-q + 1/2, +q - 1/2]$. Hence, we obtain

$$\begin{aligned} A := F \star E &= (p.G \star \phi + F \star M) \\ &= a_0 + a_1.e_1 + a_2.e_2 + a_3.e_3 + a_4.e_4 + a_5.e_5 \\ &+ a_6.e_6 + a_7.e_7 + a_8.e_8 + a_9.e_9 + a_{10}.e_{10} \\ &+ a_{11}.e_{11} + a_{12}.e_{12} + a_{13}.e_{13} + a_{14}.e_{14} + a_{15}.e_{15} \end{aligned}$$

where

$$\begin{aligned} a_0 = p(&g_0\phi_0 - g_1\phi_1 - g_2\phi_2 - g_3\phi_3 - g_4\phi_4 - g_5\phi_5 - g_6\phi_6 - g_7\phi_7 - g_8\phi_8 \\ &- g_9\phi_9 - g_{10}\phi_{10} - g_{11}\phi_{11} - g_{12}\phi_{12} - g_{13}\phi_{13} - g_{14}\phi_{14} - g_{15}\phi_{15} \\ &+ f_0m_0 - f_1m_1 - f_2m_2 - f_3m_3 - f_4m_4 - f_5m_5 - f_6m_6 - f_7m_7 - f_8m_8 \\ &- f_9m_9 - f_{10}m_{10} - f_{11}m_{11} - f_{12}m_{12} - f_{13}m_{13} - f_{14}m_{14} - f_{15}m_{15}) \end{aligned}$$

$$
\begin{aligned}
a_1 &= p(g_0\phi_1 + g_1\phi_0 + g_2\phi_3 - g_3\phi_2 + g_4\phi_5 - g_5\phi_4 - g_6\phi_7 + g_7\phi_6 + g_8\phi_9 \\
&\quad - g_9\phi_8 - g_{10}\phi_{11} + g_{11}\phi_{10} - g_{12}\phi_{13} + g_{13}\phi_{12} + g_{14}\phi_{15} - g_{15}\phi_{14} \\
&\quad + f_0m_1 + f_1m_0 + f_2m_3 - f_3m_2 + f_4m_5 - f_5m_4 - f_6m_7 + f_7m_6 + f_8m_9 \\
&\quad - f_9m_8 - f_{10}m_{11} + f_{11}m_{10} - f_{12}m_{13} + f_{13}m_{12} + f_{14}m_{15} - f_{15}m_{14}) \\
a_2 &= p(g_0\phi_2 - g_1\phi_3 + g_2\phi_0 + g_3\phi_1 + g_4\phi_6 + g_5\phi_7 - g_6\phi_4 - g_7\phi_5 + g_8\phi_{10} \\
&\quad + g_9\phi_{11} - g_{10}\phi_8 - g_{11}\phi_9 - g_{12}\phi_{14} - g_{13}\phi_{15} + g_{14}\phi_{12} + g_{15}\phi_{13} \\
&\quad + f_0g_m - f_1m_3 + f_2m_0 + f_3m_1 + f_4m_6 + f_5m_7 - f_6m_4 - f_7m_5 + f_8m_{10} \\
&\quad + f_9m_{11} - f_{10}m_8 - f_{11}m_9 - f_{12}m_{14} - f_{13}m_{15} + f_{14}m_{12} + f_{15}m_{13}) \\
a_3 &= p(g_0\phi_3 + g_1\phi_2 - g_2\phi_1 + g_3\phi_0 + g_4\phi_7 - g_5\phi_6 + g_6\phi_5 - g_7\phi_4 + g_8\phi_{11} \\
&\quad - g_9\phi_{10} + g_{10}\phi_9 - g_{11}\phi_8 - g_{12}\phi_{15} + g_{13}\phi_{14} - g_{14}\phi_{13} + g_{15}\phi_{12} \\
&\quad + f_0m_3 + f_1m_2 - f_2m_1 + f_3m_0 + f_4m_7 - f_5m_6 + f_6m_5 - f_7m_4 + f_8m_{11} \\
&\quad - f_9m_{10} + f_{10}m_9 - f_{11}m_8 - f_{12}m_{15} + f_{13}m_{14} - f_{14}m_{13} + f_{15}m_{12}) \\
a_4 &= p(g_0\phi_4 - g_1\phi_5 - g_2\phi_6 - g_3\phi_7 + g_4\phi_0 + g_5\phi_1 + g_6\phi_2 + g_7\phi_3 + g_8\phi_{12} \\
&\quad + g_9\phi_{13} + g_{10}\phi_{14} + g_{11}\phi_{15} - g_{12}\phi_8 - g_{13}\phi_9 - g_{14}\phi_{10} - g_{15}\phi_{11} \\
&\quad + f_0m_4 - f_1m_5 - f_2m_6 - f_3m_7 + f_4m_0 + f_5m_1 + f_6m_2 + f_7m_3 + f_8m_{12} \\
&\quad + f_9m_{13} + f_{10}m_{14} + f_{11}m_{15} - f_{12}m_8 - f_{13}m_9 - f_{14}m_{10} - f_{15}m_{11}) \\
a_5 &= p(g_0\phi_5 + g_1\phi_4 - g_2\phi_7 + g_3\phi_6 - g_4\phi_1 + g_5\phi_0 - g_6\phi_3 + g_7\phi_2 + g_8\phi_{13} \\
&\quad - g_9\phi_{12} + g_{10}\phi_{15} - g_{11}\phi_{14} + g_{12}\phi_9 - g_{13}\phi_8 + g_{14}\phi_{11} - g_{15}\phi_{10} \\
&\quad + f_0m_5 + f_1m_4 - f_2m_7 + f_3m_6 - f_4m_1 + f_5m_0 - f_6m_3 + f_7m_2 + f_8m_{13} \\
&\quad - f_9m_{12} + f_{10}m_{15} - f_{11}m_{14} + f_{12}m_9 - f_{13}m_8 + f_{14}m_{11} - f_{15}m_{10}) \\
a_6 &= p(g_0\phi_6 + g_1\phi_7 + g_2\phi_4 - g_3\phi_5 - g_4\phi_2 + g_5\phi_3 + g_6\phi_0 - g_7\phi_1 + g_8\phi_{14} \\
&\quad - g_9\phi_{15} - g_{10}\phi_{12} + g_{11}\phi_{13} + g_{12}\phi_{10} - g_{13}\phi_{11} - g_{14}\phi_8 + g_{15}\phi_9 \\
&\quad + f_0m_6 + f_1m_7 + f_2m_4 - f_3m_5 - f_4m_2 + f_5m_3 + f_6m_0 - f_7m_1 + f_8m_{14} \\
&\quad - f_9m_{15} - f_{10}m_{12} + f_{11}m_{13} + f_{12}m_{10} - f_{13}m_{11} - f_{14}m_8 + f_{15}m_9) \\
a_7 &= p(g_0\phi_7 - g_1\phi_6 + g_2\phi_5 + g_3\phi_4 - g_4\phi_3 - g_5\phi_2 + g_6\phi_1 + g_7\phi_0 + g_8\phi_{15} \\
&\quad + g_9\phi_{14} - g_{10}\phi_{13} - g_{11}\phi_{12} + g_{12}\phi_{11} + g_{13}\phi_{10} - g_{14}\phi_9 - g_{15}\phi_8 \\
&\quad + f_0m_7 - f_1m_6 + f_2m_5 + f_3m_4 - f_4m_3 - f_5m_2 + f_6m_1 + f_7m_0 + f_8m_{15} + f_9m_{14} \\
&\quad - f_{10}m_{13} - f_{11}m_{12} + f_{12}m_{11} + f_{13}m_{10} - f_{14}m_9 - f_{15}m_8) \\
a_8 &= p(g_0\phi_8 - g_1\phi_9 - g_2\phi_{10} - g_3\phi_{11} - g_4\phi_{12} - g_5\phi_{13} - g_6\phi_{14} - g_7\phi_{15} \\
&\quad + g_8\phi_0 + g_9\phi_1 + g_{10}\phi_2 + g_{11}\phi_3 + g_{12}\phi_4 + g_{13}\phi_5 + g_{14}\phi_6 + g_{15}\phi_7 \\
&\quad + f_0m_8 - f_1m_9 - f_2m_{10} - f_3m_{11} - f_4m_{12} - f_5m_{13} - f_6m_{14} - f_7m_{15} + f_8m_0 \\
&\quad + f_9m_1 + f_{10}m_2 + f_{11}m_3 + f_{12}m_4 + f_{13}m_5 + f_{14}m_6 + f_{15}m_7)
\end{aligned}
$$

$$
\begin{aligned}
a_9 &= p(g_0\phi_{10} + g_1\phi_{11} + g_2\phi_8 - g_3\phi_9 - g_4\phi_{14} - g_5\phi_{15} + g_6\phi_{12} + g_7\phi_{13} \\
&\quad - g_8\phi_2 + g_9\phi_3 + g_{10}\phi_0 - g_{11}\phi_1 - g_{12}\phi_6 - g_{13}\phi_7 + g_{14}\phi_4 + g_{15}\phi_5 \\
&\quad + f_0m_{10} + f_1m_{11} + f_2m_8 - f_3m_9 - f_4m_{14} - f_5m_{15} + f_6m_{12} + f_7m_{13} - f_8m_2 \\
&\quad + f_9m_3 + f_{10}m_0 - f_{11}m_1 - f_{12}m_6 - f_{13}m_7 + f_{14}m_4 + f_{15}m_5) \\
a_{10} &= p(g_0\phi_{10} + g_1\phi_{11} + g_2\phi_8 - g_3\phi_9 - g_4\phi_{14} - g_5\phi_{15} + g_6\phi_{12} + g_7\phi_{13} - g_8\phi_2 \\
&\quad + g_9\phi_3 + g_{10}\phi_0 - g_{11}\phi_1 - g_{12}\phi_6 - g_{13}\phi_7 + g_{14}\phi_4 + g_{15}\phi_5 \\
&\quad + f_0\phi_{10} + f_1\phi_{11} + f_2m_8 - f_3m_9 - f_4m_{14} - f_5m_{15} + f_6m_{12} + f_7m_{13} - f_8m_2 \\
&\quad + f_9m_3 + f_{10}m_0 - f_{11}m_1 - f_{12}m_6 - f_{13}m_7 + f_{14}m_4 + f_{15}m_5) \\
a_{11} &= p(f_0\phi_{11} - f_1\phi_{10} + f_2\phi_9 + f_3\phi_8 - f_4\phi_{15} + f_5\phi_{14} - f_6\phi_{13} \\
&\quad + f_7\phi_{12} - f_8\phi_3 - f_9\phi_2 + f_{10}\phi_1 + f_{11}\phi_0 - f_{12}\phi_7 \\
&\quad + f_{13}\phi_6 - f_{14}\phi_5 + f_{15}\phi_4 \\
&\quad + (f_0m_{11} - f_1m_{10} + f_2m_9 + f_3m_8 - f_4m_{15} + f_5m_{14} - f_6m_{13} + f_7m_{12} - f_8m_3 \\
&\quad - f_9m_2 + f_{10}m_1 + f_{11}m_0 - f_{12}m_7 + f_{13}m_6 - f_{14}m_5 + f_{15}m_4) \\
a_{12} &= p(g_0\phi_{12} + g_1\phi_{13} + g_2\phi_{14} + g_3\phi_{15} + g_4\phi_8 - g_5\phi_9 - g_6\phi_{10} \\
&\quad - g_7\phi_{11} - g_8\phi_4 + g_9\phi_5 + g_{10}\phi_6 + g_{11}\phi_7 + g_{12}\phi_0 - g_{13}\phi_1 - g_{14}\phi_2 - g_{15}\phi_3 \\
&\quad + f_0m_{12} + f_1m_{13} + f_2m_{14} + f_3m_{15} - f_4m_8 - f_5m_9 - f_6m_{10} - f_7m_{11} - f_8m_4 \\
&\quad + f_9m_5 + f_{10}m_6 + f_{11}m_7 + f_{12}m_0 - f_{13}m_1 - f_{14}m_2 - f_{15}m_3) \\
a_{13} &= p(g_0\phi_{13} - g_1\phi_{12} + g_2\phi_{15} - g_3\phi_{14} + g_4\phi_9 + g_5\phi_8 + g_6\phi_{11} - g_7\phi_{10} - g_8\phi_5 \\
&\quad - g_9\phi_4 + g_{10}\phi_7 - g_{11}\phi_6 + g_{12}\phi_1 + g_{13}\phi_0 + g_{14}\phi_3 - g_{15}\phi_2 + f_0m_{13} - f_1m_{12} \\
&\quad + f_2m_{15} - f_3m_{14} + f_4m_9 + f_5m_8 + f_6m_{11} \\
&\quad - f_7m_{10} - f_8m_5 - f_9m_4 + f_{10}m_7 - f_{11}m_6 + f_{12}m_1 + f_{13}m_0 + f_{14}m_3 - f_{15}m_2) \\
a_{14} &= p(g_0\phi_{14} - g_1\phi_{15} - g_2\phi_{12} + g_3\phi_{13} + g_4\phi_{10} - g_5\phi_{11} + g_6\phi_8 + g_7\phi_9 - g_8\phi_6 \\
&\quad - g_9\phi_7 - g_{10}\phi_4 + g_{11}\phi_5 + g_{12}\phi_2 - g_{13}\phi_3 + g_{14}\phi_0 + g_{15}\phi_1 \\
&\quad + f_0m_{14} - f_1m_{15} - f_2m_{12} + f_3m_{13} + f_4m_{10} - f_5m_{11} + f_6m_8 + f_7m_9 - f_8m_6 \\
&\quad - f_9m_7 - f_{10}m_4 + f_{11}m_5 + f_{12}m_2 - f_{13}m_3 + f_{14}m_0 + f_{15}m_1) \\
a_{15} &= (g_0\phi_{15} + g_1\phi_{14} - g_2\phi_{13} - g_3\phi_{12} + g_4\phi_{11} + g_5\phi_{10} - g_6\phi_9 + g_7\phi_8 - g_8\phi_7 \\
&\quad + g_9\phi_6 - g_{10}\phi_5 - g_{11}\phi_4 - g_{12}\phi_3 + g_{13}\phi_2 - g_{14}\phi_1 + g_{15}\phi_0 \\
&\quad + f_0m_{15} + f_1m_{14} - f_2m_{13} - f_3m_{12} + f_4m_{11} + f_5m_{10} - f_6m_9 + f_7m_8 - f_8m_7 \\
&\quad + f_9m_6 - f_{10}m_5 - f_{11}m_4 - f_{12}m_3 + f_{13}m_2 - f_{14}m_1 + f_{15}m_0)
\end{aligned}
$$

Now, according to the definition of the subsets L_f, L_g, L_ϕ and L_m from Table 1, we obtain

$$P_r(f_{i,j}=1)=\frac{d_f}{N},\qquad P_r(f_{i,j}=-1)=\frac{d_f-1}{N}\approx\frac{d_f}{N},\qquad P_r(f_{i,j}=0)=\frac{N-2d_f}{N},$$
$$P_r(g_{i,j}=1)=P_r(g_{i,j}=-1)=\frac{d_g}{N},\qquad P_r(g_{i,j}=0)=\frac{N-2d_g}{N},$$
$$P_r(\phi_{i,j}=1)=P_r(\phi_{i,j}=-1)=\frac{d_\phi}{N},\qquad P_r(\phi_{i,j}=0)=\frac{N-2d_\phi}{N},$$
$$P_r(m_{i,j}=j)=\frac{1}{p},\qquad i=0.....15\qquad j=\frac{-p+1}{2}.....\frac{+p-1}{2}.$$

where

$$\begin{aligned} f_i&=[f_{i,0},f_{i,1},\ldots,f_{i,N-1}] \qquad i=0,.....15\\ g_i&=[g_{i,0},g_{i,1},\ldots,g_{i,N-1}] \qquad i=0,.....15\\ \phi_i&=[\phi_{i,0},\phi_{i,1},\ldots,\phi_{i,N-1}] \qquad i=0,.....15 \end{aligned} \tag{6.1}$$

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

$$E[a_{ij}]=0\qquad i=0.....15\qquad j=0.....N-1.$$

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

$$Var[\phi_{i,k}.g_{j,l}]=\frac{4d_\phi.d_g}{N^2}\qquad i,j=0,1,.....,15\qquad k,l=0,....,N-1,$$
$$Var[f_{i,k}.m_{j,l}]=\frac{d_f(p-1).(p+1)}{6.N}\qquad i,j=0,1,.....,15\qquad k,l=0,....,N-1.$$

As a result,

$$\begin{aligned} Var[a_{0,k}]=Var\Bigg[\sum_{i+j=k}(&p(g_0\phi_0-g_1\phi_1-g_2\phi_2-g_3\phi_3-g_4\phi_4-g_5\phi_5-g_6\phi_6\\ &-g_7\phi_7-g_8\phi_8-g_9\phi_9-g_{10}\phi_{10}-g_{11}\phi_{11}-g_{12}\phi_{12}-g_{13}\phi_{13}\\ &-g_{14}\phi_{14}-g_{15}\phi_{15}+f_0m_0-f_1m_1-f_2m_2-f_3m_3-f_4m_4\\ &-f_5m_5-f_6m_6-f_7m_7-f_8m_8\\ &-f_9m_9-f_{10}m_{10}-f_{11}m_{11}-f_{12}m_{12}-f_{13}m_{13}-f_{14}m_{14}-f_{15}m_{15}))\Bigg]. \end{aligned}$$

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

$$\begin{aligned} Var[a_{0,k}] &= 256p^2N\left(\frac{4d_fd_g}{N^2}\right) + 256N\left(\frac{d_f(p-1)(p+1)}{6N}\right) \\ &= \left(\frac{256\times 4p^2d_fd_g}{N}\right) + \frac{128d_f(p-1)(p+1)}{3} \\ &= \frac{1024p^2d_fd_g}{N} + \frac{128d_f(p-1)(p+1)}{3}. \end{aligned}$$

Similarly, we have

$$\begin{aligned} Var[a_{1,k}] &= Var[a_{2,k}]..... \\ &= Var[a_{15,k}] \approx \frac{1024p^2d_fd_g}{N} + \frac{128d_f(p-1)(p+1)}{3}. \end{aligned}$$

It is desirable to calculate the probability that $a_{i,k}$ lies within $\left[\frac{-q+1}{2}.....\frac{+q-1}{2}\right]$, 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

$$\begin{aligned} P_r &= \left(|a_{i,k}| \le \frac{q-1}{2}\right) \\ &= P_r = \left(-\frac{q-1}{2} \le a_{i,k} \le \frac{q-1}{2}\right) \\ &= 2\phi\left(\frac{q-1}{2\sigma}\right) - 1, \qquad i = 0, ..., 15, \qquad k = 0.....N-1 \end{aligned}$$

where ϕ denotes the distribution of the standard normal variable and

$$\sigma = \sqrt{\frac{1024p^2d_fd_g}{N} + \frac{128d_f(p-1)(p+1)}{3}}.$$

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

- The probability for each of the messages m_0, m_1, $m_2, \ldots, m_{16}$ to be correctly decrypted is

$$\left(2\phi\left(\frac{q-1}{2\sigma}\right) - 1\right)^N, \tag{6.2}$$

- The probability for all the messages $m_0, m_1, m_2, \ldots, m_{16}$ to be correctly decrypted is

$$\left(2\phi\left(\frac{q-1}{2\sigma}\right) - 1\right)^{16N}, \tag{6.3}$$

Brute Force Attack: In STRU, an attacker knows the constant and public parameters,namely $d\phi$, d_g, d_f, q, p and N, as well as, the public key $H = F_q \star G{=}h_0 + h_1 + \cdots + h_{15}$. If the attacker finds one of the sedenions $G \in L_g$ or $F \in L_f$, the private key can be easily computed. In order to find G or F using a brute force attack, the attacker can try all possible values and check to see if $F \star H$ $(G \star H^{-1})$ turns into a sedenion with small coefficients or not. The total state space for the two subsets L_f and L_g is calculated as follows

$$|L_f| = \binom{N}{d_f+1}^{16} \quad \binom{N-d_f-1}{d_f}^{16} = \left(\frac{N!}{(d_f+1)!d_f!(N-2d_f-1)}\right)^{16}$$

$$|L_g| = \binom{N}{d_f}^{16} \quad \binom{N-d_f+1}{d_g}^{16} = \frac{N!^{16}}{(d_g)!^{32}(N-2d_g)!^{16}}$$

Since d_g is generally considered to be smaller than d_f , L_g is smaller than L_f and by trying all possible values of $G \in L_g$ in $G \star H^{-1}$, the attacker can find the private key through searching a space of order $|L_g|$. Using a Meet-In-The-Middle attack approach, the order of the search space can be reduced through searching a space of order $\sqrt{|L_g|} = \dfrac{N!^4}{(d_g)!^{16}(N-2d_g)!^4}$ [2].Similarly, in order to find the original message from the corresponding ciphertext, the attacker must search in L_ϕ. On average, the search must be done in a space of order $\sqrt{|L_\phi|} = \dfrac{N!^4}{(d_\phi)!^{16}(N-2d_\phi)!^4}$. However, with the typical values for d_ϕ, d_g and N, finding the private key or plaintext using brute force attack is computationally infeasible.

Message Expansion: Analogous to Ntru, the length of the encrypted message in STRU is more than the original message and that is part of the price one has to pay for gaining more encryption speed in both cryptosystems. The expansion ratio can be easily calculated as $\dfrac{log|C|}{log|P|}{=}\dfrac{logq^{16N}}{logp^{16N}}{=}\dfrac{logq}{logp}$, where C and P are ciphertext space and plaintext space, respectively. For both Ntru and STRU, it seems that this ratio depends merely on p and q, however, we have to choose q in such a way that the probability of decryption failure be very small (e.g., smaller than 2^{-80}). Thus, the maximum expansion ratio in STRU is at most about 17.

Advantages of STRU: The advantages of using the non-associative algebra in the proposed public key cryptosystem can be summarized as follows:

- The encryption process in STRU compared with Ntru (with an equal dimension) is almost sixteen times slower than Ntru and its decryption process runs almost 32 times slower. On the other hand, considering that the complexity of the convolution multiplication is $O(N^2)$, the reduction of N with the power of two affects the speed

of the calculations. Therefore, the Ntru cryptosystem with a dimension of $16.N$ is almost 256 times slower than Ntru with a dimension of N and is also naturally much slower than the STRU. Hence, we claim that with the reduction of N within a reasonable range, one can compensate for the decrease of the speed of STRU in such a way that a higher security is achieved. One can also compensate for the fact that the length of the parameter q in the STRU is larger and also that it is not prime, with an insignificant cost.

- The STRU lattice is not completely convolutional and the open problems and doubts which exist with respect to the cyclic structure of the Ntru lattice are not there in the case. The open problem is whether the cyclic structure of the convolutional lattices can possibly contribute to the improvement of lattice reduction algorithms and finding the shortest vector in polynomial time.

- The STRU is an operational instance of a public key cryptosystem with a non-associative algebra which relies for its security on the intractability of finding shortest vector problem in a lattice. On the other hand, its core (or in other words, basic operations in the underlying algebraic structure) is fast, efficient and cost effective, just like the Ntru public key cryptosystem.

7. Conclusion

In this paper, we have introduced sedenion algebra, analogue of NTRU, which is called STRU. It is non-associative, non-alternative, non division algebra and non-composition algebra. The sedenion algebra do not have any matrix isomorphic representation because it is a non-associative and this feature causes for its cryptanalysis with the help of the system of linear equations, also if the sedenion algebra is represented in the form of lattice then the dimension of the lattice increases to 32N. To achieve such a level of security in the Ntru,the parameter N shall be considered sixteen times larger, something that will cause the decrease of the speed of the cryptosystem at a rate of about 256. Therefore, even though STRU, with a dimension (N) equal to Ntru, is slower than Ntru, this decrease of speed can be compensated by the reduction of N Instead. The increase of parameter q in STRU will lead to the increase of the message expansion ratio and the reduction of the speed of the modular operations. The complexity of encryption and decryption is the same in both the cryptosystem (STRU, NTRU) for the same parameter N.

References

[1] D. V. Bailey, D. Coffin, A. Elbirt, J. H. Silverman, and A. D. Woodbury, "NTRU in constrained devices". In CHES '01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems. London, UK: Springer-Verlag, 2001, pp. 262–272.

[2] N. H. Graham, J. H. Silverman, and W. Whyte. "A meet-in-the-middle attack on an NTRU private key." 2002.

[3] J. Hffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem." In Lecture Notes in Computer Science Springer-Verlag, 1998, pp. 267–288.

[4] D. Micciancio and S. Goldwasser, "Complexity of Lattice Problems". A cryptographic perspective, volume 671 of The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, Boston, Massachusetts, 2002.

[5] D. Micciancio. "The hardness of the closest vector problem with preprocessing". IEEE Transactions on Information Theory, 2001, pp. 1212–1215.

[6] J. Hoffstein and J. Silverman, "Optimizations for ntru." In In Public Key Cryptography and Computational Number Theory, 2000, pp. 11–15.

[7] D. Micciancio. "The shortest vector problem is NP-hard to approximate to within some constant". SIAM Journal on Computing, 2001, pp. 2008–2035.

[8] A. May and J. H. Silverman. "Dimension reduction methods for convolution modular lattices." In CaLC '01: Revised Papers from the Internationa Conference on Cryptography and Lattices, London, UK: Springer-Verlag, 2001, pp. 110–125.

[9] N H.Graham, J. Hoffstein, J. Pipher, W. Whyte, and Ntru Cryptosystems, "On estimating the lattice security of NTRU," 2005.

[10] R.D. Schafer, "An Introduction to Nonassociative Algebras," Academic Press, New York, 1966.

[11] L.E. Dickson, J. de Math. "Pures et Appliq." 2 (1923) 281.

[12] M. Ajtai. "The shortest vector problem in l2 is np-hard for randomized reductions." In STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing, New York, NY: USA, 1998, pp. 10–19.

[13] R.E. Cawagas, "On the structure and zero divisors of the cayley-dickson sedenion algebra." Discussiones Mathematicae General Algebra and Applications, 2004, pp. 251–265.

[14] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of applied cryptography." Boca Raton, Florida: CRC Press, 1996.

[15] Hoffstein J., Pipher J. and Silverman J.H., "NTRU": A Ring Based Public Key Cryptosystem, Lecture notes in Computer Science, Springer-Verlag, Berlin 1433, pp. 267–288, 1998.

[16] J. Pipher and Ntru Cryptosystems. "Lectures on the NTRU encryption algorithm and digital signature scheme", 2005.

[17] R. Kouzmenko. "Generalizations of the NTRU cryptosystem." Master's thesis, Polytechnique, Montreal, Canada, 2006.

[18] K. Imaeda and M. Imaeda, "Sedenions: algebra and analysis". Appl. Math. Comput. 115 (2000), pp. 77–88.