OTRU: A Non-Associative and High Speed Public Key Cryptosystem

Ehsan Malekian, Ali Zakerolhosseini
Faculty of Electrical and Computer Engineering, Shahid Beheshti University, Evin, Tehran, Iran
malekian@sbu.ac.ir, a-zaker@sbu.ac.ir

***Abstract*— In this paper, we propose OTRU, a high speed probabilistic multi-dimensional public key cryptosystem that encrypts eight data vectors in each encryption round. The underlying algebraic structure of the proposed scheme is the power-associative and alternative octonions algebra which can be defined over any Dedekind domain such as convolution polynomial ring.**

The proposed public key cryptosystem relies for its inherent security on the difficulty of the shortest vector problem (SVP) in a non-circular modular lattice.

After a brief introduction to Ntrū, we describe the algebraic structure used in the proposed cryptosystem. Further, we provide the details of the key generation, encryption and decryption algorithms and discuss the issues regarding key security, message security, and probability of successful decryption.

OTRU has been designed based on the Ntrū core and exhibits high levels of parallelism with full operand length. By reducing the dimension of the underlying convolution polynomial ring (N) and using parallelism techniques we can increase the OTRU encryption/decryption speed to a level even higher than Ntrū.

I. Introduction

Ntrū 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 [1]. Compared to number theoretic-based cryptosystems such as RSA or ECC, the greatest advantage of Ntrū is that it is based on a class of arithmetic operations that can be performed very efficiently with a low area and time complexity. Computational efficiency along with low cost of implementation have turned Ntrū into a very suitable choice for a large number of applications such as embedded systems, mobile phones, portable devices and resource constrained devices [2].

Ntrū is classified as a lattice-based cryptosystem since its security is based on intractability of solving SVP/CVP (Shortest/Closest Vector Problem) in a particular type of lattice called *Convolutional Modular Lattice*. As a result, most sophisticated attacks against Ntrū are based on lattice reduction techniques that was suggested in [3]. Ntrū has been sufficiently analyzed during the past decade and after eliminating some minor flaws and applying some methods for optimizing the performance and speed of the cryptosystem [4], it has now been fully standardized within IEEE P1363.1.

In [5], [6], [7], extensive efforts have been made to generalize Ntrū over Dedekind domains beyond $\mathbb{Z}$ (including $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\zeta_3]$, $\mathbb{Z}[\zeta_5]$ and the non-commutative ring of $k \times k$ matrices of polynomials in $\mathbb{Z}[x]/(x^N-1)$) and the generalized versions seem to be secure as well.

As we have demonstrated in [8], we believe that the basic concept on which the Ntrū cryptosystem pivots is totally abstract and can be extended to a broader algebra than Dedekind domains. This concept can be summarized as follows:

Let $\mathscr{D}$ be a Dedekind Domain and let $\mathscr{R} = \mathscr{D}[x]/(x^N-1)$ be the convolution polynomial ring defined over $\mathscr{D}$. Assume that $< p >$ and $< q >$ are ideals generated by p and q in $\mathscr{D}$ such that $< p > \cap < q >= 1$. Obviously, we have: $\mathscr{R}/ < p > \simeq (\mathscr{D}/ < p >)[x]/(x^N-1)$ and $\mathscr{R}/ < q > \simeq (\mathscr{D}/ < q >)[x]/(x^N-1)$. Let denote the set of all coset representatives for each equivalence class modulo $< q >$ by $\mathscr{S} \subset \mathscr{R}$. If certain restrictions are imposed on the coefficients of $f(x)$, $g(x)$, $\phi(x)$ and $m(x)$ such that the result of $p.g(x).\phi(x)+m(x).f(x)$ lies exactly in $\mathscr{S}$ (i.e., $p.g(x).\phi(x)+m(x).f(x) \bmod < q >$ is exactly equal to $(p.g(x).\phi(x)+m(x).f(x) \in \mathscr{R}$), then one can easily switch from $\mathscr{R}/ < q >$ to $\mathscr{R}/ < p >$ and follow the rest of the calculations in the new ring. This abstract concept can clearly be extended to other algebraic structures such as modules and sub-modules, algebras and sub-algebras as well.

In this paper by introducing a non-associative cryptosystem we will prove that a lattice-based public key cryptosystem based on non-associative algebra is not only feasible but also arguably more secure than Ntrū, because its lattice does not fully fit within Circular and Convolutional Modular Lattice. We have considered the proposed scheme (let us call it OTRU thereafter) exactly identical to Ntrū in order to be able to cite the extensive researches carried out regarding security aspects of the cryptosystems in the past ten years. The main advantages of the proposed cryptosystem would be higher security and the increase of parallelism levels.

The rest of this paper is structured as follows. The Ntrū public key cryptosystem is described in Section II. In Section III we introduce the algebraic structure used in OTRU. Section IV describes the proposed scheme in detail and in Section V we analyze the security of the proposed scheme against lattice attacks.

II. The Ntrū Cryptosystem

The basic operations in Ntrū take place in the ring $\mathbb{Z}[x]/(x^N-1)$, which is known as the ring of convolution polynomials of rank N, where N is a prime [9, p. 392]. Let define the following three rings: $\mathscr{R} = \mathbb{Z}[x]/(x^N-1)$, $\mathscr{R}_p = (\mathbb{Z}/p\mathbb{Z})[x]/(x^N-1)$, and $\mathscr{R}_q = (\mathbb{Z}/q\mathbb{Z})[x]/(x^N-1)$. An element f of the rings $\mathscr{R}$, $\mathscr{R}_p$, and $\mathscr{R}_q$, can be denoted interchangeably by a polynomial or its vector of coefficients:

978-1-4244-6269-8/10/$26.00 ©2010 IEEE

$f = \sum_{i=0}^{N-1} f_i.x_i \triangleq [f_0, f_1, ..., f_{N-1}]$. In the convolution rings, addition corresponds to the ordinary polynomials addition, i.e., element-wise, but multiplication, denoted by the symbol $\star$, is explicitly defined as follows

$$\begin{aligned} f(x) &:= \sum_{i=0}^{N-1} f_i x^i = [f_0, f_1, \ldots, f_{N-1}]_{1\times N},\ f_i \in \mathbb{Z} \\ g(x) &:= \sum_{i=0}^{N-1} g_i x^i = [g_0, g_1, \ldots, g_{N-1}]_{1\times N},\ g_i \in \mathbb{Z} \\ h(x) &:= \sum_{i=0}^{N-1} h_i x^i = [h_0, h_1, \ldots, h_{N-1}]_{1\times N},\ h_i \in \mathbb{Z} \\ h_k &:= \sum_{i=0}^{k} f_i.g_{k-i} + \sum_{i=k+1}^{N-1} f_i.g_{N+k-i} = \sum_{i+j \overset{N}{\equiv} k} f_i.g_j. \end{aligned} \tag{1}$$

Let d_f, d_g, d_ϕ, and d_m be constant integers less than N (typically $d_f = d_g = d_\phi = d_m = \mathbf{d} \approx N/3$) and let $\mathscr{L}_f$, $\mathscr{L}_m$, $\mathscr{L}_\phi$, $\mathscr{L}_g \subset \mathscr{R}$ be the subsets of *small polynomials* as defined in Table I. With these notations and definitions, the Ntrū public key cryptosystem can now be described as follows.

Public parameters: The public parameters (N, p, q, d) in Ntrū are assumed to be fixed and must be agreed upon by both the sender and the receiver. N and p are prime numbers providing that $\gcd(p,q) = \gcd(N,q) = 1$ and $q \gg p$. Typical values include $N = 167$ for moderate security, $N = 251$ for high security, and $N = 503$ for very high security along with $p = 3$ and $d \approx N/3$.

Key Generation: To create a pair of public and private keys, first two small polynomials $g \in \mathscr{L}_g$ and $f \in \mathscr{L}_f$ are randomly generated. The polynomial f must be invertible in $\mathscr{R}_p$ and $\mathscr{R}_q$. The probability that a randomly chosen polynomial is invertible in $\mathscr{R}_q$ will be greater than $(1 - p^{-n})^{(N-1)}/n$, where n is the smallest integer which satisfies $p^n = 1 \bmod N$ [10]. However, in a rare event that f is not invertible, a new polynomial f can be easily generated. Let f_p^{-1} and f_q^{-1} denote the two inverses, in $\mathscr{R}_p$ and $\mathscr{R}_q$, respectively. While f, g, f_p^{-1}, and f_q^{-1} are kept secret, the public key h is computed and published as follows

$$h = f_q^{-1} \star g \,(\bmod\ q). \tag{2}$$

Encryption: The cryptosystem initially selects a random polynomial $\phi \in \mathscr{L}_\phi$, called the ephemeral key, and encodes the input message into a polynomial $m \in \mathscr{L}_m$. The ciphertext is computed as follows:

$$e = p.h \star \phi + m \,(mod\ q). \tag{3}$$

Neglecting the time required for ephemeral key generation and conversion time of the incoming message into the polynomial $m \in \mathscr{L}_m$, and by pre-computing and storing $p.h$, Ntrū encryption takes $\mathscr{O}(N^2)$ steps.

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

$$\begin{aligned} a &:= f \star e \,(\bmod\ q) = f \star (p.h \star \phi + m) \,(\bmod\ q) \\ &= p.f \star h \star \phi + f \star m \ \ (\bmod\ q) \\ &= p.f \star f_q^{-1} \star g \star \phi + f \star m \ \ (\bmod\ q) \\ &= p.g \star \phi + f \star m \ \ (\bmod\ q). \end{aligned} \tag{4}$$

In the second step, the coefficients of $a \in \mathscr{R}_q$ are identified with the equivalent representatives in $\mathscr{S} := \{-q/2+1, ..., +q/2\}$. Assuming that the public parameters have been chosen properly, the resulting polynomial is exactly equal to $p.g \star \phi + f \star m$ in $\mathscr{R}$. With this assumption, when we reduce the coefficients of a modulo p, the term $p.g \star \phi$ vanishes and $f \star m \,(\bmod\ p)$ remains. In order to extract the message m, it is enough to multiply $f \star m \,(\bmod\ p)$ by f_p^{-1}.

Decryption Failure: If the public parameters (N, p, q, d) are chosen to satisfy $q > (6d+1).p$ (where $d := d_f = d_g = d_\phi$, as defined earlier), then decryption process will never fail. However, to have a better performance and also to reduce the size of the public key, the public parameter q can be chosen in such a way that the probability of decryption failure is very small (e.g., 2^{-80}) [9, p. 395]. Successful decryption depends on whether $|p.g \star \phi + f \star m|_\infty < q$ or not. With a few simple assumptions and probabilistic calculations [6, pp. 16], the upper-bound for the probability of successful decryption can be approximated as follows

$$\Pr(\textit{successful decryption}) = \left(2\Phi(\frac{q-1}{2\sigma}) - 1\right)^N, \tag{5}$$

where $\Phi(\cdot)$ denotes the standard normal distribution function and $\sigma \approx \sqrt{\frac{36 d_f . d_g}{N} + \frac{8 d_f}{6}}$.

III. Algebraic Structure of OTRU

In this section, we briefly review some basic definitions and properties in octonions algebra and introduce the algebraic structure used in our proposed cryptosystem. It is presumed that the reader is familiar with the concepts of nonassociative algebras as well as octonions. Otherwise, references [11] and [12], [13] are recommended for comprehensive introduction to nonassociative algebra and octonions, respectively. Throughout this paper by $\mathscr{R}$-Algebra ($\mathbb{K}$-Algebra) we mean a finite dimensional $\mathscr{R}$-module (vector space) equipped by a bilinear map, called multiplication. An algebra $\mathbb{A}$ is called division algebra providing for every $a, b \in \mathbb{A}$, $a.b = 0$ implies $a = 0$ or $b = 0$. In other words, division algebra does not have any zero divisors. Normed division algebra is a division algebra equipped with a multiplicative norm function (denoted by $\|\cdot\|$). A normed division algebra is not necessarily associative. An algebra is *power-associative* if the subalgebra generated by a single element is associative (i.e., for computing x^n, the order of multiplication does not matter) and it is *alternative* if the subalgebra generated by any two elements is associative, i.e., for all x and y in the alternative algebra we have $x(xy) = (xx)y$ and $(yx)x = y(xx)$. Every alternative algebra satisfies the following three identities: (I) $y((xz)x) = ((yx)z)x$, (II) $(xy)(zx) = (x(yz))x$ and (III) $(x(yx))z = x(y(xz))$, which are known as *Moufang*

TABLE I

DEFINITION OF PUBLIC PARAMETERS OF NTRŪ

Notation	Definition	Typical Value for $N=167,\ p=3,\ q=128$
$\mathscr{L}_f$	$\{f \in \mathscr{R} \mid f$ has d_f coefficients equal to +1, (d_f-1) equal to -1, the rest 0$\}$	d_f =61
$\mathscr{L}_g$	$\{g \in \mathscr{R} \mid g$ has d_g coefficients equal to +1, d_g equal to -1, the rest 0$\}$	d_g =20
$\mathscr{L}_\phi$	$\{\phi \in \mathscr{R} \mid \phi$ has d_ϕ coefficients equal to +1, d_ϕ equal to -1, the rest 0$\}$	d_ϕ =18
$\mathscr{L}_m$	$\{m \in \mathscr{R} \mid$ coefficients of m are chosen modulo p, between $-p/2$ and $p/2\}$	-

Identities. The real octonions (denoted by $\mathbb{O}$) can be thought of as a vector space of dimension 8 over $\mathbb{R}$ defined as follows

$$\mathbb{O} := \{x_0 + \sum_{i=1}^{7} x_i.e_i \mid x_0, \cdots, x_7 \in \mathbb{R}\} \tag{6}$$

where $\{1,\ e_1,\ e_2,\ e_3,\ e_4,\ e_5,\ e_6,\ e_7\}$ form the basis of the algebra and x_i's are scalars in $\mathbb{R}$. Addition of two octonions is performed by adding corresponding coefficients (i.e., element-wise) but multiplication can be determined using the following rules

$$\begin{aligned} &e_i^2=-1,\ i=1,\cdots,7 \qquad e_i.e_j=-e_j.e_i \quad i\neq j,\ i,j=1,\cdots,7 \\ &e_i.e_j=e_k \rightarrow e_{i+1}.e_{j+1}=e_{k+1}, \quad e_i.e_j=e_k \rightarrow e_{2i}.e_{2j}=e_{2k}, \quad i\neq j,\ i,j=1,\cdots,7 \end{aligned} \tag{7}$$

where indices greater than 7 should be reduced mod 7.

Multiplication is neither commutative nor associative but is alternative and (consequently) power-associative. The conjugate and square norm of an octonion $\underset{\sim}{x} = x_0 + \sum_{i=1}^{7} x_i.e_i$ are given by $\underset{\sim}{x}^* = x_0 - \sum_{i=1}^{7} x_i.e_i$ and $N(\underset{\sim}{x}) = \underset{\sim}{x}.\underset{\sim}{x}^* = \underset{\sim}{x}^*.\underset{\sim}{x} = \sum_{i=0}^{7} x_i^2$, respectively. Every non-zero element in $\mathbb{O}$ has a unique multiplicative inverse which is given by $\underset{\sim}{x}^{-1} = N(\underset{\sim}{x})^{-1}.\underset{\sim}{x}^*$.

Now, suppose that $\mathscr{R}$ is an arbitrary finite ring of odd characteristic. We can define the octonion algebra $\mathbb{A}$ over $\mathscr{R}$ as follows

$$\mathbb{A} := \{x_0 + \sum_{i=1}^{7} x_i.e_i \mid x_0, \cdots, x_7 \in \mathscr{R}\} \tag{8}$$

with the same multiplication defined for the real octonions. The algebra $\mathbb{A}$ is a non-associative algebra with a norm and multiplicative inverse that has much the same properties as the real octonion algebra $\mathbb{O}$.

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

Now, let us describe the algebraic structure of OTRU. Consider the convolution polynomial rings $\mathscr{R} := \mathbb{Z}[x]/(x^N-1)$, $\mathscr{R}_p := \mathbb{Z}_p[x]/(x^N-1)$ and $\mathscr{R}_q := \mathbb{Z}_q[x]/(x^N-1)$ that are used in Ntrū. We define three octonionic algebras $\mathbb{A}$, $\mathbb{A}_p$ and $\mathbb{A}_q$ as follows

$$\mathbb{A} := \{a_0(x) + \sum_{i=1}^{7} a_i(x).e_i \mid a_0(x), \cdots, a_7(x) \in \mathscr{R}\} \tag{9}$$

$$\mathbb{A}_p := \{a_0(x) + \sum_{i=1}^{7} a_i(x).e_i \mid a_0(x), \cdots, a_7(x) \in \mathscr{R}_p\} \tag{10}$$

$$\mathbb{A}_q := \{a_0(x) + \sum_{i=1}^{7} a_i(x).e_i \mid a_0(x), \cdots, a_7(x) \in \mathscr{R}_q\} \tag{11}$$

For simplicity, p, q and N are assumed to be prime numbers and $q \gg p$. Since $\mathbb{Z}_p[x]/(x^N-1)$ and $\mathbb{Z}_q[x]/(x^N-1)$ are finite rings with characteristics p and q, respectively, one can easily conclude that $\mathbb{A}_p$ and $\mathbb{A}_q$ are octonionic nonassociative split algebras similar to $\mathbb{O}$, except that they contain some nonzero elements whose norm is zero and naturally such elements do not have a multiplicative inverse.

Evidently, the concept of homomorphism do not involve associativity of multiplication and there exists a well defined and non-trivial homomorphism which sends every elements of $\mathbb{A}$ to $\mathbb{A}_p$ (or $\mathbb{A}_q$). Thus, every element in the finite split algebras $\mathbb{A}_p$ ($\mathbb{A}_q$) can be represented by a coset representative in $\mathbb{A}$. Let us concentrate more on algebras $\mathbb{A}_p$ and $\mathbb{A}_q$. Let $\varrho_1 = f_0(x) + f_1(x)e_1 + \cdots + f_7(x)e_7$ and $\varrho_2 = g_0(x) + g_1(x)e_1 + \cdots + g_7(x)e_7$ be two elements in $\mathbb{A}_p$ (or $\mathbb{A}_q$) where $f_i(x)$ and $g_i(x)$ are polynomials in $\mathscr{R}_p$ ($\mathscr{R}_q$). Then, the addition and multiplication of two octonions, norm and multiplicative inverse are defined in the following way

Addition of octonions corresponds to the usual addition of eight polynomials including $8N$ modular addition mod p (mod q), i.e.,

$$\varrho_1 + \varrho_2 = (f_0(x)+g_0(x)) + (f_1(x)+g_1(x))e_1 + \cdots + (f_7(x)+g_7(x))e_7. \tag{12}$$

Multiplication of two octonions is defined by

$$\begin{aligned} \varrho_1 \circ \varrho_2 = &(f_0 \star g_0 - f_1 \star g_1 - f_2 \star g_2 - f_3 \star g_3 - f_4 \star g_4 - f_5 \star g_5 - f_6 \star g_6 - f_7 \star g_7) \\ &+ (f_0 \star g_1 + f_1 \star g_0 + f_2 \star g_4 + f_3 \star g_7 - f_4 \star g_2 + f_5 \star g_6 - f_6 \star g_5 - f_7 \star g_3).e_1 \\ &+ (f_0 \star g_2 - f_1 \star g_4 + f_2 \star g_0 + f_3 \star g_5 + f_4 \star g_1 - f_5 \star g_3 + f_6 \star g_7 - f_7 \star g_6).e_2 \\ &+ (f_0 \star g_3 - f_1 \star g_7 - f_2 \star g_5 + f_3 \star g_0 + f_4 \star g_6 + f_5 \star g_2 - f_6 \star g_4 + f_7 \star g_1).e_3 \\ &+ (f_0 \star g_4 + f_1 \star g_2 - f_2 \star g_1 - f_3 \star g_6 + f_4 \star g_0 + f_5 \star g_7 + f_6 \star g_3 - f_7 \star g_5).e_4 \\ &+ (f_0 \star g_5 - f_1 \star g_6 + f_2 \star g_3 - f_3 \star g_2 - f_4 \star g_7 + f_5 \star g_0 + f_6 \star g_1 + f_7 \star g_4).e_5 \\ &+ (f_0 \star g_6 + f_1 \star g_5 - f_2 \star g_7 + f_3 \star g_4 - f_4 \star g_3 - f_5 \star g_1 + f_6 \star g_0 + f_7 \star g_2).e_6 \\ &+ (f_0 \star g_7 + f_1 \star g_3 + f_2 \star g_6 - f_3 \star g_1 + f_4 \star g_5 - f_5 \star g_4 - f_6 \star g_2 + f_7 \star g_0).e_7 \end{aligned} \tag{13}$$

where $\star$ denotes the convolution product. Octonionic multiplication in $\mathbb{A}_p$ (or $\mathbb{A}_q$) needs 64 polynomial convolutions and 56 polynomial addition modulo p (q), which together account for $64.N^2$ modular multiplications and $(64N(N-1)+56N)$ modular additions.

Conjugate of an octonion which is defined as below needs $7N$ negations modulo p or q.

$$\varrho^* = +f_0(x) - f_1(x)e_1 - f_2(x)e_2 - \cdots - f_7(x)e_7. \tag{14}$$

Squared Norm By a slight abuse of the word norm, we define the squared norm of an octonion as

$$N(\underset{\sim}{o}) = (f_0(x))^2 + (f_1(x))^2 \cdots + (f_7(x))^2 \tag{15}$$

Totally, $8N^2$ multiplications and $(8N(N-1)+7N)$ additions are required for calculating the squared norm of an octonions.

Multiplicative inverse Providing $N(\underset{\sim}{o}) \neq 0$, the multiplicative inverse of $\underset{\sim}{o}$ is computed by $N(\underset{\sim}{o}) \neq 0 \rightarrow \underset{\sim}{o}^{-1} = \frac{\underset{\sim}{o}^*}{N(\underset{\sim}{o})}$. Thus, the following operations will be needed for calculating the multiplicative inverse of an element in $\mathbb{A}_p$ (or $\mathbb{A}_q$)

I Calculation of $g(x) \leftarrow N(\underset{\sim}{o})$ over the ground ring $\mathbb{Z}_p[x]/(x^N-1)$ ($\mathbb{Z}_q[x]/(x^N-1)$) at the total cost of $8N^2$ multiplications and $(8N(N-1)+7N)$ additions.

II Finding the inverse of $g(x)$ over the ground ring using the extended Euclid algorithm with a running time of $\mathcal{O}(N^2)$. ([14, p. 82])

III Conjugation of $\underset{\sim}{o}$ including $7N$ negations.

IV Calculation of $g^{-1}(x).\underset{\sim}{o}^*$ including $8N^2$ multiplication and $8N(N-1)$ addition modulo p (q).

After setting up the required notation and algebras $\mathbb{A}$, $\mathbb{A}_p$ and $\mathbb{A}_q$, we describe OTRU.

IV. Proposed Scheme: OTRU

In the OTRU cryptosystem, encryption and decryption are taken place in a multi-dimensional vector space and similar to Ntrū, the security of the cryptosystem depends on three parameters (N,p,q) and four subsets $\mathscr{L}_f$, $\mathscr{L}_m$, $\mathscr{L}_\phi$, $\mathscr{L}_g \subset \mathbb{A}$ as defined in Table II. N, p and q, d_f, d_g, d_ϕ are constant parameters which play a similar role as in Ntrū except that for simplicity these constants are supposed to be all prime numbers. OTRU operates as described below.

a) Key Generation: In order to generate a pair of public and private keys, initially, two small octonions $\underset{\sim}{F} \in \mathscr{L}_f$ and $\underset{\sim}{G} \in \mathscr{L}_g$ are randomly generated.

$$\underset{\sim}{F} := f_0 + f_1.e_1 + \cdots + f_7.e_7 \in \mathbb{A}, \qquad f_0, \cdots, f_7 \in \mathscr{L}_f \subset \mathbb{A}$$

$$\underset{\sim}{G} := g_0 + g_1.e_1 + \cdots + g_7.e_7 \in \mathbb{A}, \qquad g_0, \cdots, g_7 \in \mathscr{L}_g \subset \mathbb{A}$$

The octonion $\underset{\sim}{F}$ must be invertible over $\mathbb{A}_p$ and $\mathbb{A}_q$. If such an inverse does not exist (i.e., when $\sum_{i=0}^{7} f_i^2(x)$ is not invertible in $\mathbb{Z}_p[x]/(x^N-1)$ or $\mathbb{Z}_q[x]/(x^N-1)$), a new octonion $\underset{\sim}{F}$ will be generated. The inverses of $\underset{\sim}{F}$ over the algebras $\mathbb{A}_p$ and $\mathbb{A}_q$ are denoted by $\underset{\sim}{F}_p^{-1}$ and $\underset{\sim}{F}_q^{-1}$. The public key, which is an octonion, is computed as follows

$$\underset{\sim}{H} = \underset{\sim}{F}_q^{-1} \circ \underset{\sim}{G} \in \mathbb{A}_q. \tag{16}$$

The octonions $\underset{\sim}{F}$, $\underset{\sim}{F}_p$ and $\underset{\sim}{F}_q$ are kept secret in order to be used in the decryption phase. One can estimate that the key generation of OTRU is 64 times slower than that of Ntrū, when the same parameters (N,p,q) are used in both cryptosystems. However, in OTRU, we can definitely work with a smaller dimension N, without reducing the system security.

b) Encryption: Initially, a random octonion $\underset{\sim}{\Phi}$ is generated. The incoming data must be converted into an octonion including eight polynomial in $\mathscr{L}_\phi$ based on a simple conversion. The ciphertext $\underset{\sim}{E}$ is then calculated as follows

$$\underset{\sim}{E} = p.\underset{\sim}{H} \circ \underset{\sim}{\Phi} + \underset{\sim}{M} \in \mathbb{A}_q. \tag{17}$$

c) Decryption: Since the octonions algebra is non-associative, not only the terms of $(\underset{\sim}{F}_q^{-1} \circ \underset{\sim}{G}) \circ \underset{\sim}{\Phi}$ do not commute, but also the parentheses order can not be changed, and this will reveal some problem during decryption, because one cannot simply remove the term $\underset{\sim}{F}_q^{-1}$ from $((\underset{\sim}{F}_q^{-1} \circ \underset{\sim}{G}) \circ \underset{\sim}{\Phi})$ by multiplying $\underset{\sim}{F}$ on the left. Thus, in order to decrypt, first of all, the received octonion $\underset{\sim}{E}$ is multiplied on the left by the private key $\underset{\sim}{F}$ and then on the right as follows

$$\begin{aligned}
\underset{\sim}{B} :&= ((\underset{\sim}{F} \circ \underset{\sim}{E}) \circ \underset{\sim}{F}) = p.(\underset{\sim}{F} \circ (\underset{\sim}{H} \circ \underset{\sim}{\Phi})) \circ \underset{\sim}{F} + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_q \\
&= p.\underbrace{(\underset{\sim}{F} \circ \underset{\sim}{H}) \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F})}_{\text{Moufang identities}} + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_q \\
&= p.(\underset{\sim}{F} \circ (\underset{\sim}{F}_q^{-1} \circ \underset{\sim}{G})) \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F}) + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_q \\
&= p.\underset{\sim}{G} \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F}) + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_q.
\end{aligned} \tag{18}$$

Upon suitable selection of the cryptosystem constant parameters, the coefficients of the eight polynomial in $p.\underset{\sim}{G} \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F}) + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F}$ will most probably lie within the interval $(-q/2, +q/2]$ and the last reduction mod q will be superfluous. Thus, in the second step, $\underset{\sim}{B} \in \mathbb{A}_q$ should be identified with its equivalent representative in $\Omega = (-q/2, +q/2]$ and all the coefficients in the eight polynomials should be reduced mod p. Thus we have $(\underset{\sim}{B} \bmod p) = (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} \in \mathbb{A}_p$. In order to extract the original message $\underset{\sim}{M}$, simply multiply $\underset{\sim}{B}$ on the right by $\underset{\sim}{F}_p^{-1}$ and then repeat the same operation on the left and adjust the resulting coefficients in $[-p/2, +p/2]$.

One can estimate that the encryption and decryption algorithms in OTRU with the same dimension N are about 8 and 16 times slower than that of Ntrū, however, in OTRU we can work with a lower dimension N, without reducing the cryptosystem security. Also, similar to Ntrū, OTRU can be optimized for efficiency based on the various optimization methods proposed in [4]. In addition, there are multiple parallelism levels in the proposed scheme that can be exploited to improve encryption and decryption speed.

d) Successful Decryption: Probability of successful decryption in OTRU is calculated in the same way as Ntrū and under the same assumptions made in the standard version [10], [6]. Successful decryption in OTRU, depends on whether all octonion coefficients of $p.\underset{\sim}{G} \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F}) + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F}$ lie in the interval $\left[\frac{-q+1}{2}, \frac{+q-1}{2}\right]$ or not. In the first step of decryption process we have

$$\underset{\sim}{B} := p.\underset{\sim}{G} \circ (\underset{\sim}{\Phi} \circ \underset{\sim}{F}) + (\underset{\sim}{F} \circ \underset{\sim}{M}) \circ \underset{\sim}{F} := b_0(x) + \sum_{i=1}^{7} b_i(x).e_i$$

TABLE II

SUBSETS DEFINITIONS IN OTRU

Notation	Definition $(\mathscr{R} := \mathbb{Z}/(x^N-1))$
$\mathscr{L}_f$	$\{f_0(x)+f_1(x)e_1+...+f_7(x)e_7 \in \mathbb{A} \mid f_i(x) \in \mathscr{R}$ has d_f coefficients equal to +1, (d_f-1) equal to -1, the rest 0$\}$
$\mathscr{L}_g$	$\{g_0(x)+g_1(x)e_1+...+g_7(x)e_7 \in \mathbb{A} \mid g_i(x) \in \mathscr{R}$ has d_g coefficients equal to +1, d_g equal to -1, the rest 0$\}$
$\mathscr{L}_\phi$	$\{\phi_0(x)+\phi_1(x)e_1+...+\phi_7(x)e_7 \in \mathbb{A} \mid \phi_i(x) \in \mathscr{R}$ has d_ϕ coefficients equal to +1, d_ϕ equal to -1, the rest 0$\}$
$\mathscr{L}_g$	$\{m_0(x)+m_1(x)e_1+...+m_7(x)e_7 \in \mathbb{A} \mid$ coefficients of $m_i(x) \in \mathscr{R}$ is chosen modulo p, between $-p/2$ and $p/2$ $\}$

In the above expression, for instance, b_0 which is a polynomial of degree N is calculated as

$$
\begin{aligned}
&b_0 := \\
&p.(+g_6\phi_5f_1+g_4\phi_7f_5-g_5\phi_0f_5+g_5\phi_1f_6-g_5\phi_2f_3+g_5\phi_3f_2+g_5\phi_4f_7-g_3\phi_5f_2 \\
&+g_3\phi_6f_4-g_3\phi_7f_1-g_4\phi_0f_4-g_4\phi_1f_2+g_4\phi_2f_1+g_4\phi_3f_6-g_4\phi_4f_0-g_4\phi_5f_7 \\
&-g_4\phi_6f_3-g_3\phi_3f_0-g_3\phi_4f_6+g_1\phi_6f_5+g_3\phi_1f_7+g_3\phi_2f_5+g_6\phi_4f_3-g_6\phi_3f_4 \\
&-g_5\phi_7f_4-g_5\phi_6f_1+g_2\phi_7f_6+g_6\phi_2f_7-g_2\phi_3f_5-g_2\phi_4f_1-g_6\phi_1f_5+g_1\phi_7f_3 \\
&-g_1\phi_5f_6-g_0\phi_1f_1+g_0\phi_0f_0-g_0\phi_3f_3-g_0\phi_2f_2+g_7\phi_6f_2-g_0\phi_5f_5-g_0\phi_4f_4 \\
&-g_0\phi_6f_6-g_1\phi_3f_7-g_1\phi_2f_4-g_1\phi_1f_0-g_2\phi_6f_7-g_1\phi_0f_1-g_0\phi_7f_7-g_7\phi_7f_0 \\
&+g_1\phi_4f_2+g_7\phi_5f_4-g_7\phi_4f_5+g_2\phi_5f_3-g_6\phi_0f_6-g_7\phi_0f_7-g_5\phi_5f_0-g_6\phi_7f_2 \\
&-g_6\phi_6f_0+g_2\phi_1f_4-g_2\phi_0f_2-g_2\phi_2f_0+g_7\phi_3f_1-g_3\phi_0f_3-g_7\phi_2f_6-g_7\phi_1f_3) \\
&+(f_6{}^2m_1+f_5{}^2m_1+f_3{}^2m_1-2f_1f_4m_4+f_7{}^2m_1+f_2{}^2m_1-2f_1f_5m_5-2f_1f_6m_6 \\
&-2f_1f_3m_3-2f_1f_2m_2+2f_1f_0m_0+f_4{}^2m_1-2f_1f_7m_7+f_0{}^2m_1-f_1{}^2m_1) \\
&:= [b_{0,0}, b_{0,2}\cdots b_{0,N-1}]
\end{aligned}
\tag{19}
$$

All of the polynomials b_1, b_2, ..., b_7 in $\underset{\sim}{B}$ would have the same form as above expression except that some indices of $g_i.\phi_j.f_k$, $f_i.f_j.m_k$ and $f_i^2.m_k$ are permuted.

According to the definition of $\mathscr{L}_f$, $\mathscr{L}_g$, $\mathscr{L}_\phi$ and $\mathscr{L}_m$ we can easily assume

$$
\begin{aligned}
&\Pr(f_{i,j}=1)=\tfrac{d_f}{N}, \quad \Pr(f_{i,j}=-1)=\tfrac{d_f-1}{N}\approx\tfrac{d_f}{N}, \quad \Pr(f_{i,j}=0)=\tfrac{N-2d_f}{N}, \\
&\Pr(g_{i,j}=1)=\Pr(g_{i,j}=-1)=\tfrac{d_g}{N}, \qquad \Pr(g_{i,j}=0)=\tfrac{N-2d_g}{N}, \\
&\Pr(\phi_{i,j}=1)=\Pr(\phi_{i,j}=-1)=\tfrac{d_\phi}{N}, \qquad \Pr(\phi_{i,j}=0)=\tfrac{N-2d_\phi}{N}, \\
&\Pr(m_{i,j}=\lambda)=\tfrac{1}{p}, \quad i=0,\cdots 7 \qquad \lambda=-\tfrac{+p-1}{2}\ \ldots\ \tfrac{+p-1}{2}.
\end{aligned}
\tag{20}
$$

where

$$
\begin{aligned}
f_i &= [f_{i,0}, f_{i,1}, ..., f_{i,N-1}] \qquad i=0,\cdots 7, \\
g_i &= [g_{i,0}, g_{i,1}, ..., g_{i,N-1}] \qquad i=0,\cdots 7, \\
\phi_i &= [\phi_{i,0}, \phi_{i,1}, ..., \phi_{i,N-1}] \qquad i=0,\cdots 7.
\end{aligned}
\tag{21}
$$

We can simply assume that $f_{i,s}$, $g_{j,t}$ and $\phi_{k,u}$ are all pairwise independent random variables. Thus, for all $i,j,k = 0,...,7$ and $s,t,u = 0,...,N-1$ and $\lambda = -\frac{+p-1}{2},...,\frac{+p-1}{2}$ we have

$$
\begin{aligned}
&\Pr(f_{i,s}.g_{j,t}.\phi_{k,u}=\pm 1)=\tfrac{4d_fd_gd_\phi}{N^3} \\
&\Pr(f_{i,s}.g_{j,t}.\phi_{k,u}=0)=\tfrac{N^3-8d_fd_gd_\phi}{N^3} \\
&\Pr(f_{i,s}.f_{j,t}.m_{k,u}=\lambda)=\tfrac{4d_f{}^2}{p.N^2}, \quad (i\neq j \vee s\neq t)\wedge(\lambda\neq 0) \\
&\Pr(f_{i,s}.f_{i,t}.m_{k,u}=\lambda)=\tfrac{2d_f(d_f-1)+2d_f{}^2}{pN(N-1)}, (s\neq t)\wedge(\lambda\neq 0) \\
&\Pr(f_{i,s}{}^2.m_{k,u}=\lambda)=\tfrac{2d_f}{p.N}.
\end{aligned}
\tag{22}
$$

From the above distributions we can deduce that

$$
\begin{aligned}
&E(f_{i,s}.g_{j,t}.\phi_{k,u})=0, \quad E(f_{i,s}.f_{j,t}.m_{k,u})=0 \\
&Var(f_{i,s}.g_{j,t}.\phi_{k,u})=\tfrac{8d_fd_gd_\phi}{N^3} \\
&Var(f_{i,s}.f_{j,t}.m_{k,u})=\tfrac{2(4d_f{}^2)}{p.N^2}\sum_{i=1}^{\frac{p-1}{2}} i^2=\tfrac{d_f{}^2(p-1)(p+1)}{3N^2} \\
&Var(f_{i,s}{}^2.m_{k,u})=\tfrac{2(2d_f)}{p.N}\sum_{i=1}^{\frac{p-1}{2}} i^2=\tfrac{d_f(p-1)(p+1)}{6N}
\end{aligned}
\tag{23}
$$

With this simplifying assumptions that the covariance of $f_{i,s}$ and $f_{i,t}$ is negligible we obtain (although it is not generally true but this assumption underestimates the final result)

$$
\begin{aligned}
Var\left((f_i.g_j.\phi_k)_l\right) &= Var\left(\sum_{s+t+u\equiv l(\bmod N)}\sum f_{i,s}.g_{j,t}.\phi_{k,u}\right) \\
&= \frac{8d_fd_gd_\phi}{N} \\
Var\left((f_i.f_j.m_k)_l\right) &= Var\left(\sum_{s+t+u\equiv l(\bmod N)}\sum f_{i,s}.f_{j,t}.m_{k,u}\right) \\
&= \frac{d_f{}^2(p-1)(p+1)}{3} \\
Var\left((f_i{}^2.m_k)_l\right) &= Var\left(\sum_{s+t+u\equiv l(\bmod N)}\sum f_{i,s}.f_{i,t}.m_{k,u}\right)
\end{aligned}
$$

$$
\approx \frac{d_f{}^2(N-1)(p-1)(p+1)}{3N} + \frac{d_f(p-1)(p+1)}{6}. \tag{24}
$$

Upon insertion of $Var\left((f_i.g_j.\phi_k)_l\right)$, $Var\left((f_i.f_j.m_k)_l\right)$ and $Var\left((f_i{}^2.m_k)_l\right)$, we obtain

$$
\begin{aligned}
Var[b_{0,k}] \approx{}& \frac{512p^2d_fd_gd_\phi}{N} + \frac{28d_f{}^2(p-1)(p+1)}{3} \\
&+ \frac{8d_f{}^2(N-1)(p-1)(p+1)}{3N} + \frac{4d_f(p-1)(p+1)}{3}.
\end{aligned}
$$

In a similar way, we have

$$
\begin{aligned}
&Var[b_{1,k}] = Var[b_{2,k}] = \cdots = Var[b_{7,k}] \approx \\
&\tfrac{512p^2d_fd_gd_\phi}{N} + \tfrac{28d_f{}^2(p-1)(p+1)}{3} + \tfrac{8d_f{}^2(N-1)(p-1)(p+1)}{3N} + \tfrac{4d_f(p-1)(p+1)}{3}.
\end{aligned}
\tag{25}
$$

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

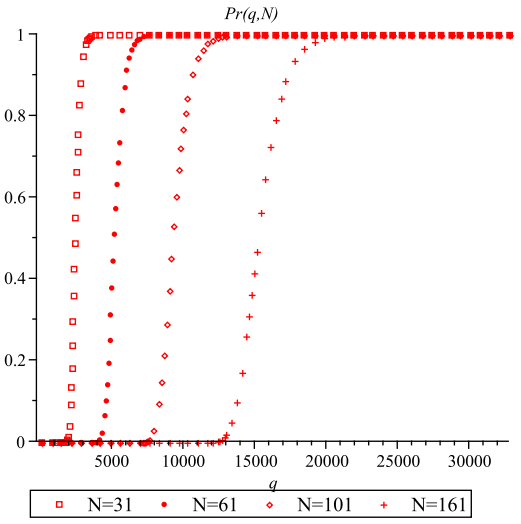

Fig. 1. Probability of successful decryption for some typical values of N

$$\Pr\left(|b_{i,k}| \le \frac{q-1}{2}\right) = \Pr\left(-\frac{q-1}{2} \le b_{i,k} \le \frac{q-1}{2}\right) = 2\Phi\left(\frac{q-1}{2\sigma}\right) - 1, \quad i = 0,\dots,7,\ k = 0,\dots,N-1 \tag{26}$$

where Φ denotes the distribution of the standard normal variable and

$$\sigma = \sqrt{\frac{512p^2 d_f d_g d_\phi}{N} + \frac{28{d_f}^2(p-1)(p+1)}{3} + \frac{8{d_f}^2(N-1)(p-1)(p+1)}{3N} + \frac{4d_f(p-1)(p+1)}{3}}. \tag{27}$$

Based on above calculations, the probability of successful decryption in OTRU can be calculated through the following two observations

- The probability for each of the messages m_0, m_1, m_2, …, m_8 to be correctly decrypted is
$$\left(2\Phi(\frac{q-1}{2\sigma}) - 1\right)^N. \tag{28}$$
- The probability for all the messages m_0, m_1, m_2, …, m_8 to be correctly decrypted is
$$\left(2\Phi(\frac{q-1}{2\sigma}) - 1\right)^{8.N}. \tag{29}$$

Figure 1 shows the probability of successful decryption for $N = 31$, $N = 61$, $N = 101$ and $N = 161$ versus q.

e) Brute Force Attack: For conducting a brute force attack, an attacker who knows the public parameters including the public key $\underset{\sim}{H} = \underset{\sim}{F}_q^{-1} \circ \underset{\sim}{G}$, must try each possible octonion in $\mathscr{L}_f$ (by multiplying on the left) until s/he finds a short key for decryption. The size of the subset $\mathscr{L}_f$ is calculated as follows

$$\#\mathscr{L}_f = \begin{pmatrix} N \\ d_f+1 \end{pmatrix}^8 \begin{pmatrix} N-d_f-1 \\ d_f \end{pmatrix}^8 = \left(\frac{N!}{(d_f+1)!d_f!(N-2d_f-1)}\right)^8$$

Note that just like Ntrū, $\underset{\sim}{F}$ and all of its scalar rotations $(x^i.\underset{\sim}{F})$ can be served as decryption key. Thus, the total state space an attacker has to search for an encryption key is about $\#\mathscr{L}_f/N$. If enough memory is provided, the search time could be reduced to $\sqrt{\#\mathscr{L}_f/N}$ using Meet-In-The-Middle attack [15].

Similarly, in order to find the original message using brute force attack, the attacker must search in $\mathscr{L}_\phi$. Thus, the message security is $\#\mathscr{L}_\phi/N$ for brute force and $\sqrt{\#\mathscr{L}_\phi/N}$ for Meet-In-The-Middle attack, where

$$\#\mathscr{L}_\phi = \begin{pmatrix} N \\ d_\phi \end{pmatrix}^8 \begin{pmatrix} N-d_\phi \\ d_\phi \end{pmatrix}^8 = \left(\frac{N!}{{d_\phi!}^2(N-2d_\phi)}\right)^8 \tag{30}$$

f) Message Expansion: Analogous to Ntrū, the length of the encrypted message in OTRU 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 $\frac{\log|C|}{\log|P|} = \frac{\log q^{8N}}{\log p^{8N}} = \frac{\log q}{\log p}$, where C and P are ciphertext space and plaintext space, respectively. For both Ntrū and OTRU, 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, based on above calculation, choosing suitable q depends on all public constants such as d_f, d_g, d_ϕ and N. Based on Figure 1 one can deduce that $q = 2^{14}$ is sufficient for all security needs. Thus, the maximum expansion ratio in OTRU is at most about 9.

V. The OTRU Lattice

In this section we prove that similar to Ntrū, the security of the proposed cryptosystems relies on the intractability of SVP in a certain type of lattice. Lattice basis reduction algorithms (such as *LLL* and its variants) are able to solve SVP to within a factor of 2^N and, consequently, in order to ensure that the cryptosystem is secure, the lattice dimension (which is determined by parameter N in both Ntrū and OTRU) must be large enough to provide a reasonable security level. In this section, we turn to the security of the proposed cryptosystem against the attacks based on lattice reduction.

As pointed out in Section III, the octonions do not have a matrix isomorphic representation and consequently, for finding a small norm octonion satisfying $\underset{\sim}{F}.\underset{\sim}{H} = \underset{\sim}{G} \pmod q$, one cannot form an octonionic lattice by building a matrix with octonionic entries and use a lattice reduction algorithm to find an octonions with any desired norm. The only way which remains for attacking the OTRU cryptosystem and finding a suitable key for decryption is to expand $\underset{\sim}{F}.\underset{\sim}{H} = \underset{\sim}{G} \pmod q$ as follows

$$\begin{cases} f_0\star h_0 - f_1\star h_1 - f_2\star h_2 - f_3\star h_3 - f_4\star h_4 - f_5\star h_5 - f_6\star h_6 - f_7\star h_7 = g_0 + qu_0 \\ f_0\star h_1 + f_1\star h_0 + f_2\star h_4 + f_3\star h_7 - f_4\star h_2 + f_5\star h_6 - f_6\star h_5 - f_7\star h_3 = g_1 + qu_1 \\ \vdots \\ f_0\star h_7 + f_1\star h_3 + f_2\star h_6 - f_3\star h_1 + f_4\star h_5 - f_5\star h_4 - f_6\star h_2 + f_7\star h_0 = g_7 + qu_7 \end{cases} \tag{31}$$

Let represent the polynomials $h_0, h_1, ..., h_7$ in their matrix isomorphic representation as follows

$$(\mathscr{H}_i)_{N\times N} := \begin{bmatrix} h_{i,0} & h_{i,1} & h_{i,2} & \cdots & h_{i,N-1} \\ h_{i,N-1} & h_{i,0} & h_{i,1} & & h_{i,N-2} \\ h_{i,N-2} & h_{i,N-1} & h_{i,0} & & h_{i,N-3} \\ \vdots & & & \ddots & \vdots \\ h_{i,2} & h_{i,3} & & & \\ h_{i,1} & h_{i,2} & & \cdots & h_{i,0} \end{bmatrix}$$

Based upon the above notations, we can set up the OTRU lattice of dimension $16N$ spanned by the rows of the matrix $\mathscr{M}$ defined in Table III.

From the system of linear equations (31), it is clear that the vector $\langle f_0, f_1, \cdots, f_7, g_0, g_1, \cdots, g_7 \rangle_{1\times 16.N}$ is in the OTRU lattice (denoted by $\mathscr{L}_{OTRU}$). Finding a short vector in this lattice may be used as the decryption key. Similar to the Ntrū lattice [9, p. 400–403], for the OTRU lattice we have:

(I) $Det(\mathscr{L}_{OTRU}) = q^{8.N}$.

(II) $\|\langle f_0, f_1, \cdots, f_7, g_0, g_1, \cdots, g_7 \rangle\| \approx \sqrt{32.d} \approx 3.27\sqrt{N}$ (assuming $d_f = d_g = d_\phi = d \approx N/3$).

(III) Based on the Gaussian heuristic we can predict that the expected length of the shortest nonzero vector in the $\mathscr{L}_{OTRU}$ is about $\lambda_0 \approx \sqrt{\frac{n}{2\pi e}}.Det(\mathscr{L})^{1/n} = \sqrt{\frac{8N}{\pi e}}.\sqrt{q} \approx 0.968.\sqrt{N.q}$. (IV) $\frac{\|<f_0,f_1,\cdots,f_7,g_0,g_1,\cdots,g_7>\|}{\lambda_0} = \frac{3.27\sqrt{N}}{0.968\sqrt{Nq}} \approx \frac{3.38}{\sqrt{q}}$. This means that the target vectors in $\mathscr{L}_{OTRU}$ are about $\mathscr{O}(\sqrt{q})$ shorter than predicted by the Gaussian heuristic.

Clearly, the OTRU lattice is similar to the Ntrū lattice with the differences that *it is not fully circular* and under equal circumstances (i.e. choosing the same value for N in both OTRU and Ntrū), the dimension of $\mathscr{L}_{OTRU}$ is eight times of Ntrū. Therefore, all of the analyses done with respect to the Ntrū lattice also apply to the OTRU lattice. Thus, based upon the analytical and experimental results presented in [16], [17] the expected running time needed to find a suitable vector (spurious decryption key) in $\mathscr{L}_{OTRU}$ is exponential in N. For example, the expected running time for $N_{Ntru} = 251$ is estimated as 1.37×10^{13} MIPS-Years. Taking the fact that $q_{OTRU} \gg q_{NTRU}$ into account, we claim that this level of security could be achieved through OTRU with $N_{OTRU} = 61$.

At first glance, it may seem that using non-associative algebra has no advantage over the standard Ntrū and one can set aside the complexities and implementation cost of OTRU and use Ntrū with a dimension of $8.N$ and achieve the same level of security, whereas this is not true. The advantages of using the non-associative algebra in the proposed public key cryptosystem can be summarized as follows:

- The encryption process in OTRU compared with Ntrū (with an equal dimension) is almost eight times slower than Ntrū and its decryption process runs almost 16 times slower. On the other hand, considering that the complexity of the convolution multiplication is $\mathscr{O}(N^2)$, the reduction of N with the power of two affects the speed of the calculations. Therefore, the Ntrū cryptosystem with a dimension of $8.N$ is almost 64 times slower than Ntrū with a dimension of N and is also naturally much slower than the OTRU. Hence, we claim that with the reduction of N within a reasonable range, one can compensate for the decrease of the speed of OTRU 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 OTRU is larger and also that it is not prime, with an insignificant cost.
- One of the positive features of OTRU is that there are multiple levels of parallelism in it and its speed can be brought up to a level almost equal to the speed of Ntrū with an equal N by bearing the higher costs of implementation. Now if we reduce the dimension of OTRU to a reasonable level (for example 61), we can increase the processing speed to a level even higher than Ntrū using parallelism techniques. In this way, we can achieve one of the fastest of existing cryptosystems without decreasing the cryptosystem security. Let us not forget that the public key cryptosystems have always suffered from low speed, and also, that in many of the existing methods, the parallelism levels are limited.
- The OTRU lattice is not completely convolutional and the open problems and doubts which exist with respect to the cyclic structure of the Ntrū 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.

In the closing of this section, we would like to emphasize that the OTRU 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 Ntrū public key cryptosystem.

VI. Conclusion

In this paper, we introduced OTRU, a public key cryptosystem based on the octonions non-associative algebra the core of which is precisely similar to the Ntrū. The underlying algebraic structure for the proposed scheme is the octonions algebra which is a non-associative and non-commutative algebra. The octonions do not have a matrix isomorphic representation and this feature causes that for its cryptanalysis with the help of the linear equations system, the dimension of the lattice increases to $16N$. To achieve such a level of security in the Ntrū, the parameter N shall be considered eight times larger, something that will cause the decrease of the speed of the cryptosystem at a rate of about 64. Therefore, even though OTRU, with a dimension (N) equal to Ntrū, is slower than Ntrū, this decrease of speed can be compensated by the reduction of N Instead, the increase of parameter q in OTRU (by a bit-length about two times of this very amount in the Ntrū) will lead to the increase of the message expansion ratio and the reduction of the speed of the modular operations modulo q. The second problem can

TABLE III

THE OTRU LATTICE GENERATED BY THE ROWS OF $\mathscr{M}$

$$\mathscr{M}_{16N\times 16N} := \left[\begin{array}{c|cccccccc} & +\mathscr{H}_0 & +\mathscr{H}_1 & +\mathscr{H}_2 & +\mathscr{H}_3 & +\mathscr{H}_4 & +\mathscr{H}_5 & +\mathscr{H}_6 & +\mathscr{H}_7 \\ & -\mathscr{H}_1 & +\mathscr{H}_0 & -\mathscr{H}_4 & -\mathscr{H}_7 & +\mathscr{H}_2 & -\mathscr{H}_6 & +\mathscr{H}_5 & +\mathscr{H}_3 \\ & -\mathscr{H}_2 & +\mathscr{H}_4 & +\mathscr{H}_0 & -\mathscr{H}_5 & -\mathscr{H}_1 & +\mathscr{H}_3 & -\mathscr{H}_7 & +\mathscr{H}_6 \\ & -\mathscr{H}_3 & +\mathscr{H}_7 & +\mathscr{H}_5 & +\mathscr{H}_0 & -\mathscr{H}_6 & -\mathscr{H}_2 & +\mathscr{H}_4 & -\mathscr{H}_1 \\ I_{8N\times 8N} & -\mathscr{H}_4 & -\mathscr{H}_2 & +\mathscr{H}_1 & +\mathscr{H}_6 & +\mathscr{H}_0 & -\mathscr{H}_7 & -\mathscr{H}_3 & +\mathscr{H}_5 \\ & -\mathscr{H}_5 & +\mathscr{H}_6 & -\mathscr{H}_3 & +\mathscr{H}_2 & +\mathscr{H}_7 & +\mathscr{H}_0 & -\mathscr{H}_1 & -\mathscr{H}_4 \\ & -\mathscr{H}_6 & -\mathscr{H}_5 & +\mathscr{H}_7 & -\mathscr{H}_4 & +\mathscr{H}_3 & +\mathscr{H}_1 & +\mathscr{H}_0 & -\mathscr{H}_2 \\ & -\mathscr{H}_7 & -\mathscr{H}_3 & -\mathscr{H}_6 & +\mathscr{H}_1 & -\mathscr{H}_5 & +\mathscr{H}_4 & +\mathscr{H}_2 & +\mathscr{H}_0 \\ \hline 0_{8N\times 8N} & \multicolumn{8}{c}{I_{8N\times 8N}} \end{array}\right]$$

be eliminated easily by bearing some more implementation cost.

We claim that the proposed cryptosystem is the first functional cryptosystem with a non-associative algebra. Other features of this cryptosystem include the following

- The OTRU has been designed based on the Ntrū core and is fully compatible with it. (By considering the values of $h_1, h_2, \cdots h_7$, $m_1, m_2, \cdots m_7$ and $\phi_1, \phi_2, \cdots \phi_7$, the OTRU cryptosystem will be completely converted to Ntrū.) All of the proposed optimization methods for Ntrū (for example all of the methods proposed in [4]) can be exploited in OTRU.
- The parallelism levels in OTRU are much more than Ntrū and by bearing some more cost OTRU can be designed and implemented in such a way that its speed becomes even much higher than Ntrū while having a dimension much lower than the Ntrū. Furthermore, considering the existing and optimized hardware and software implementation of the Ntrū cryptosystem, the design and implementation of OTRU will be very easy, fast, reliable and cost effective. Any future optimizations in Ntrū core are applicable and usable in OTRU too.
- The OTRU is a multi-dimensional probabilistic public key cryptosystem which encrypts eight data vectors in parallel. These data may possibly be generated from a single source or from multiple independent sources. This feature may be useful in protocol design or such applications as electronic voting or financial transactions.

The details of the proposed cryptosystem and comprehensive analysis of the security and efficiency aspects are beyond the scope of this paper and will be published soon [18]. In the end, we would like to point out that OTRU is the first step in the design of the public key cryptosystems with a non-associative algebra. The idea which was put forward in this paper can serve as a starting point for the design of other non-associative cryptosystems with a different algebraic structure and better features.

ACKNOWLEDGMENT

The authors of this paper would like to thank ITRC (IRAN Telecommunications Research Center) for their support of this project. The authors would also wish to express their cordial thanks to Professor Hossein Hajiabolhassan, Faculty of Mathematics at Shahid Beheshti University.

REFERENCES

[1] J. Hoffstein, 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.

[2] 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.

[3] D. Coppersmith and A. Shamir, "Lattice attacks on NTRU," in *EUROCRYPT*, 1997, pp. 52–61.

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

[5] M. Nevins, C. Karimianpour, and A. Miri, "Ntru over rings beyond z," *accepted to Designs, Codes and Cryptography*, May 2009.

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

[7] M. Coglianese and B.-M. Goi, "MaTRU: A new NTRU-based cryptosystem," in *INDOCRYPT*, 2005, pp. 232–243.

[8] E. Malekian and A. Zakerolhosseini, "A non-associative lattice-based public key cryptosystem," *Submitted to Security Communication Networks*, 2010.

[9] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*, ser. Science+Business Media, LLC. Springer, 2008.

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

[11] R. D. Schafer, *An introduction to non-associative algebras*. New York: Dover Publications Inc., 1996, corrected reprint of the 1966 original.

[12] J. C. Baez, "The octonions," *Bulletin of the American Mathematical Society*, vol. 39, no. 2, pp. 145–205, 2002.

[13] J. H. Conway and D. A. Smith, *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*. A. K. Peters, Ltd., 2003.

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

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

[16] J. Hoffstein, J. H. Silverman, and W. Whyte, "On estimating the lattice security of NTRU," 2005.

[17] J. H. Silverman, "Dimension-reduced lattices, zero-forced lattices, and the NTRU public key cryptosystem," 1999.

[18] E. Malekian and A. Zakerolhosseini, "Ntru-like public key cryptosystems beyond dedekind domain up to alternative algebra," Cryptology ePrint Archive, Report 2009/446, Submitted to Springer Transaction on Computational Science, 2009, http://eprint.iacr.org/2009/446.pdf.