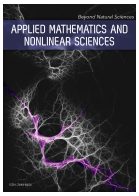
sciendo Applied Mathematics and Nonlinear Sciences 6(1) (2021) 499–506



Applied Mathematics and Nonlinear Sciences

https://www.sciendo.com

NTRU Over Galois Rings

Mehmet Sever[1], Ahmet Şükrü Özdemir[2]

[1]Ağrı Ibrahim Çeçen University, Faculty of Science and Arts, Department of Mathematics, 04100, Ağrı, Turkey, E-mail: mhmtsvr.1@gmail.com

[2]Marmara University, Atatürk Faculty of Education, Department of Mathematics Education, 34712, Istanbul, Turkey, E-mail: aso23@hotmail.com

Submission Info

Communicated by Ahmet Ocak Akdemir
Received July 26th 2019
Accepted September 19th 2019
Available online October 30th 2020

Abstract

As a cryptosystem, Nth Truncated Polynomial Ring (NTRU) is established on the fast and easy calculation. Improving the security is aimed by enlarging a ring where the processes execute and enhancing the number of a private key and a public key. In this study, NTRU takes over the Galois rings and is analysed by adding a new private key.

Keywords: Vector field, complete lift, diagonal lift, pull-back bundle, cross-section, semi-cotangent bundle
AMS 2010 codes: 11R33

1 Introduction

Nth Truncated Polynomial Ring (NTRU) was first introduced by J. H. Silverman, J. Hoffstein and J. Piper as a public key system data encryption in 1996 [1]. In the later years, it has been consistently developed by the same team. Reports and articles have been published on titles such as fast key generation and organizing attacks to the secret key [**?**]. NTRU, which is a ring-based system, is an asymmetric encryption method.

Some researchers have analysed the system cryptologically. Some interesting results can be found in [2–4]. Variants of the system have been suggested in the advancing years. Generalized NTRU schemes from the first suggestions is a study that proposes using two pieces instead of one public key [5]. Another suggestion is on the necessity of building on a finite field of the system by publishing under the name of CTRU [6] in 2002. The study named as MATRU [7] was analysed in the case where the ring is matrices. NNRU is a suggestion on the necessity that the ring should not be commutative in 2009. Also, the systems QTRU (2009) on quaternions and OTRU (2010) on octonions were purposed. Finally, the study, so-called ETRU, was propounded by replacing the ring with the Eisenstein integers [8].

This article is organized as follows: in Section 2, we provide some basic information about NTRU. In Section 3, we provide some notations used in the article. In Section 4, we describe the NTRU cryptosystem. In Section

ISSN 2444-8656 doi:10.2478/AMNS.2020.2.00041

5, we introduce the Galois rings. In Section 6, we examine the NTRU system on the Galois rings; accordingly, we propose a new cryptosystem. In the next section, we proved how the system works on the Galois rings. Finally, we discuss the advantages of this system.

2 NTRU cryptosystem

NTRU is established on the polynomial convolution ring $R = \frac{Z[x]}{x^N-1}$. A polynomial in the ring R has integer coefficients and is at most $N-1$ order. A convolution product of any two polynomials $f, g \in R$ is performed according to the following rule.

$$f = \sum_{i=0}^{N-1} f_i x^i = (f_0, f_1, \ldots, f_{N-1})$$

$$g = \sum_{j=0}^{N-1} g_j x^j = (g_0, g_1, \ldots, g_{N-1})$$

If $f * g = h$, then $h_k = \sum_{i+j \equiv k(modN)} f_i g_j$.

Before beginning, we inform about parameters of the system.

N – size parameter
Large modulo q
Small modulo p
A polynomial f indicates that the inverses according to $mod p$ and $mod q$ are available
A polynomial g indicates that it does not need to be invertible
Error polynomial r
Message polynomial m
df: a distribution of coefficients of the polynomial f
dg: a distribution of coefficients of the polynomial g
dr: the number of 1 s and -1 s in coefficients of the specified polynomial
L_f: polynomials in $\mathbb{Z}[x]/(x^N-1)$ whose coefficients provide df
L_g: polynomials in $\mathbb{Z}[x]/(x^N-1)$ whose coefficients provide dg
L_r: polynomials in $Z[x]/(x^N-1)$ whose coefficients provide dr.

In the following section, we provide some notations used in the whole article.

3 Using Notations

f is a polynomial in $Z[x]/(x^N-1)$,
f_p is a reduced form of f by *mod p* (secret key) in $Z[x]/(p, x^N-1)$,
f_q is a polynomial whose coefficients reduced by *mod q* in $Z[x]/(q, x^N-1)$,
g is a polynomial in $Z[x]/(q, x^N-1)$ (it constitutes the public key with f_q),
$f_p{}^{-1}$ is the inverse of f_p in the ring ,
$f_q{}^{-1}$ is the inverse of in the ring $Z[x]/(q, x^N-1)$, and
an encoded message e is a polynomial in $Z[x]/(p, x^N-1)$.

4 Key Generation

To generate a NTRU key, we choose randomly $f \in L_f$ and $g \in L_g$. In addition, the polynomial f is an invertible by *mod p* and *mod q*. If suitable parameters are chosen, then f will be quite likely invertible [9].

That is

$$f_q^{-1} \star f \equiv 1 \ (mod\ q) \text{ and } f_p^{-1} \star f \equiv 1 \ (mod\ p)\,. \tag{1}$$

Encryption

$$h \equiv p f_q^{-1} \star g \ (mod\ q) \tag{2}$$

is the public key.
The message m is encoded with the secret keys such as f, f_p^{-1} and the public key h by computing

$$e \equiv r \star h + m \ (mod\ q)\,. \tag{3}$$

Decryption

The cipher message is decoded in the following form

$$a \equiv f \star e \ (mod\ q) \tag{4}$$

by using the secret key. At this stage, it is checked whether the coefficients of a are in an interval $\left(-\frac{q}{2}, \frac{q}{2}\right]$. The process is finished by computing

$$c = f_p^{-1} \star a \ (mod\ p)\,. \tag{5}$$

To work decoding correctly, the absolute values of coefficients of a polynomial $prg + fm$ should not exceed $\frac{q}{2}$. Also, it may be supposed that a reduction cannot be done by *mod q* since large coefficients are chosen [10].

Why the decryption works?

Mathematically, since

$$a = f \star e \ (mod\ q) = f \star (r \star h + m) \ (mod q) = f \star r \star h + f \star m \ (mod\ q) \tag{6}$$

$$h \equiv p f_q^{-1} \star g, \tag{7}$$

$$a = \left[\left(f \star r \star \left(p f_q^{-1} \star g\right)\right) + (f \star m)\right] mod\ q \tag{8}$$

and

$$a = [(pr \star g) + (f \star m)] \ mod\ q \tag{9}$$

because

$$f_q^{-1} \star f \equiv 1 \ (mod\ q)\,.$$

$c = f_p^{-1} \star a \ (mod\ p) = p\left(f_q^{-1} \star r \star g\right) + \left(f_p^{-1} \star f \star m\right) \ (mod\ p) = 0 + (1 \star m) = m \ (mod\ p)$ so that the message m is found correctly.

As can be seen, the coefficients of these polynomials are chosen small because a convolution product of two n-order polynomials, namely f and g in the ring NTRU, necessitates n^2 processes. In previous studies, choosing an invertible polynomial f is done in the form of $f = 1 + pF$ where F is an arbitrary polynomial because $f\ mod\ p \equiv 1$ and its inverse are easily computable. The statement in Equation (8) is properly chosen in terms

of *mod q*. Thus, we say that NTRU grounds on speed and processing easily. It also gives the security flaws inherently. NTRU processes are executed in $Z_p[x]$ ve $Z_q[x]$ [11]. Moving the system into a larger set contributes to the system. It is clear that $Z_{p^k}[x]$ is a larger set. Also, it is a special type of Galois rings. Proposed new parameters and private keys are selected from this ring.

NTRU over Galois rings

Algebraic structure of Galois rings

Galois rings are obtained from Galois extensions of a ring, and they are denoted by $GR(p^n, r)$ where p is a prime number, n and r are positive integers. Some explicit examples are as follows:

If $n = 1$, then we find an extension r of the field $Z_p \cong F_p$.

$$GR(p, r) = GF(p^r) = F_{p^r}$$

If $r = 1$, then $GR(p^n, 1) = Z_{p^n}$

The Galois rings $GR(p^n, 1)$ are isomorphic to the quotient ring $Z_{p^n}[x]/(f(x))$. $f(x) \in Z_{p^n}[x]$ is a monic, basic irreducible polynomial. Equally, if $f(x) \in Z[x]$ is chosen a r th-order monic, irreducible by *mod p*, then $GR(p^n, r) \cong Z[x]/(p^n, f(x))$. This ring is local, and its single maximal ideal is $pGR(p^n, r)$.

Moreover, all the ideals of this ring are principal ideals, and it is in the following form:

$(p^i) = p^i GR(p^n, r)$ $0 \le i \le n$ [11].

Lemma 1 [12] $Z_m \cong Z_{p_1{}^{e_i}} \times Z_{p_2{}^{e_i}} \times \ldots \times Z_{p_n{}^{e_i}}$

where $m = \prod p_i{}^{e_i}$, $e_i \ge 1$, p_i are distinct prime numbers. The mapping gives isomorphism in the form of

$\varphi : i \to (a^1, a^2, \ldots, a^s)$, $i \in Z_m$ and $i \equiv a^j \ (mod\ p_j{}^{e_j})$, $j = 1, 2, \ldots, s$.

When $m \neq p^n$, Z_m is not a local ring or a chain ring, but it is a semi-local ring because it is written in the form of a direct product of local rings. Note that all the non-unitary elements of Z_{p^n} are nilpotent, and so it belongs to the class of Artin rings. Z_m does not have such a structure for $m \neq p^n$.

Proposition 1 [12] Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial in $Z_{p^k}[x]$. The following conditions are equivalent:

f is a unitary.

$\mu(f)$ is a unitary in $Z_p[x]$.

$a_0 \in Z_{p^k}$ is a unitary, and $a_1, \ldots, a_n$ are nilpotent.

Proposition 2 [12] Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial in $Z_{p^k}[x]$. The following conditions are equivalent:

f is nilpotent.

$$\mu(f) = 0.$$

$a_0, a_1, \ldots, a_n$ are nilpotent elements.

f is a zero-divisor.

The canonical homomorphism μ transforms a polynomial to $Z_p[x]$ by reducing the coefficients of a polynomial in $Z_{p^k}[x]$ in terms of *mod p*.

5 The Proposed Cryptosystem

If an integer $p^k$is replaced with modulo p in the classical NTRU processes, then we again obtain $(p^k, q) = 1$. If modulo is p^k, for prime number p and $k \ge 2$ are chosen, the processes can be executed in the Galois ring as a result of choosing suitable parameters. Because the representation is uniform so that $m = p_1{}^{\alpha_1} p_2{}^{\alpha_2} \ldots p_r{}^{\alpha_r}$ for $m \in Z$ if $p_1{}^{\alpha_1} \to p^k$ and $p_1{}^{\alpha_1} p_2{}^{\alpha_2} \ldots p_r{}^{\alpha_r} \to q$ are substituted, $Z_m[x] \cong Z_{p^k}[x] \times Z_q[x]$ so that it can be processed in an algebraic structure of the ring $Z_{p^k}[x]$ due to $(p_1{}^{\alpha_1}, p_2{}^{\alpha_2} \ldots p_r{}^{\alpha_r}) = 1$.

Again, let the message polynomial $m \in {Z_p[x]}/{(x^n-1)}$ in the classical NTRU protocol be changed to $m \in {Z_{p^k}[x]}/{(x^n-1)}$, and let the public key $h \equiv pf_q^{-1} \star g \ (mod\ q)$ be transformed to $h \equiv p^k f_q^{-1} \star g \ (mod\ q)$. The statement $e \equiv r \star h + m \ (mod\ q)$ becomes $e \equiv r \star p^k f_q^{-1} \star g + m \ (mod\ q)$. $e \star f \equiv r \star p^k f_q^{-1} \star f \star g + f \star m \ (mod\ q)$ and $e \star f \equiv r \star p^k \star g + f \star m \ (mod\ q)$. Because $p^k \to \infty$ if $k \to \infty$, it is preserved as

$$e \star f \equiv f \star m \ \left(mod\ p^k\right)$$

$$e \star f \star f_{p^k}^{-1} \equiv m \ \left(mod\ p^k\right)$$

$$e = m$$

if the number k is chosen as large as desired and the statement $f \star m \ (mod\ q)$ becomes $f \star m \ \left(mod\ p^k\right)$, it indicates that the coefficients of polynomial $f \star m$ are not reduced by $mod\ p^k$.
Since $\left(p^k, q\right) = 1$ for each p, q that provides the condition $(p, q) = 1$ being the parameter of system, it can transform the classical parameter in the case $k = 1$. In response to the chosen number k, f^k is substituted instead of the polynomial f being a secret key. If $\left(f^k\right)^{-1} = \left(f^{-1}\right)^k$, then the system becomes
$h \equiv (pf_q^{-1})^k \star g \ (mod\ q)$ where $h \equiv p^k (f_q^{-1})^k \star g \ (mod\ q)$. The statement $e \equiv r \star h + m \ (mod\ q)$ becomes

$$e \equiv r \star p^k (f_q^{-1})^k \star g \ + m \ (mod\ q)$$

$$e \star f^k \ \equiv r \star p^k \star g \ + m \star f^k \ (mod\ q)$$

$$e \star f^k \star (f_{p^k}^{-1})^k \ \equiv r \star p^k \star g \star (f_{p^k}^{-1})^k \ + m \ \left(mod\ p^k\right)$$

$$\equiv 0 \ + m \ \left(mod\ p^k\right)$$

$$e \equiv m \ \left(mod\ p^k\right)$$

$e = m$, and if the order of secret key in the multiplicative group is chosen large, it can present a different encryption protocol. The polynomial f may be chosen as a generator polynomial.
An another choosing of key could be getting new keys in the form of $f \star x^i$ for $1 \leq i \leq n-1$ by applying rotations to a secret key f.
Since $f \star x^n = f \star 1 = f$, this rotation should be finished in $n-1$ steps. Then, the polynomial $h \equiv pf_q^{-1} \star g \ (mod\ q)$, that is a public key, becomes $h \equiv p^k (f_q^{-1})^k \star g \star x^{n-i} \ (mod\ q)$.

$$e \equiv r \star h + m \ (mod\ q)$$

$$\equiv r \star p^k (f_q^{-1})^k \star g \star x^{n-i} + m \ (mod\ q)$$

$$\vdots$$

$$e \star f^k \star x^i \ \equiv r \star p^k \star g \ + f^k \star m \star x^i \ (mod\ q)$$

$$\equiv f^k \star m \star x^i \ \left(mod\ p^k\right)$$

$$e \star f^k \star (f_{p^k}^{-1})^k \star x^i \star x^{n-i} \ \equiv m \ \left(mod\ p^k\right)$$

$$e \equiv m \ \left(mod\ p^k\right)$$

$$e = m$$

so that the ith rotation of secret key acts also as a secret key.

Consequently, the numbers p ve q do not choose too small so that $(p,\ q)=1$ in the classical key protocol, they may be enlarged as desired, and it is predicted that the calculations can make in the larger rings. Since every power of a polynomial f is also invertible when it is an invertible, it is foreseen that the invertible generator polynomials contribute to NTRU. Because the statement $f\star g\equiv h\ (mod\ q)$ holds, that is, the statement $f\star g\star x^i\equiv h\star x^i\ (mod\ q)$ holds for each $0\leq i\leq n$, it is predicted that regarding a wide range of rotations of the private key has also a securty-building effect.

$$Z_{p^k}[x]/(x^n-1)\cong Z_{p^k}[x]/(x-1)\times Z_{p^k}[x]/\left(x^{n-1}+x^{n-2}+\ldots+1\right) \tag{10}$$

where $(n,\ p)=1$. If a prime number q is chosen so that $(p,\ q)=1$ is substituted instead of n, the cyclotomic polynomial $\Phi_q(x)=x^{q-1}+x^{q-2}+\ldots+x+1$ of qth order is obtained. This polynomial is irreducible in Z but all its roots are discrete in a suitably chosen ring Z_{p^k}. If the polynomial $\Phi_q(x)$ is irreducible in Z_p, then it is also irreducible in Z_{p^k}. Then $Z_{p^k}[x]/\left(x^{q-1}+x^{q-2}+\ldots+x+1\right)$ becomes a Galois ring. By $Z_{p^k}[x]/(x-1)\cong Z_{p^k}$ and the fact that Z_{p^k} is also a Galois ring, the ring $Z_{p^k}[x]/(x^n-1)$ is written as a direct product of Galois rings in the case that n is the prime q and $(q,\ p)=1$. At this stage, a homomorphism φ can be found by defining in the following form

$$\varphi: Z_{p^k}[x]/(x^n-1)\to Z_{p^k}[x]/(x-1)\times Z_{p^k}[x]/(\Phi_q(x))$$
$$\varphi(f)\to(f(1),\ f\ mod\ \Phi_q(x)).$$

When we look for an invertible f for NTRU, the conditions $f(1)\neq 0$ and $f\ mod\ \Phi_q(x)=0$ should be provided. An another case is to construct the ring Z_{p^k} containing all roots of the polynomial $\Phi_q(x)=x^{q-1}+x^{q-2}+\ldots+x+1$. For $p^k\in Z$ satisfying these conditions, it can be written

$$\Phi_q(1)=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_{q-1})$$

where $\alpha_i\in Z_{p^k}$, $1\leq i\leq q-1$.Since $\alpha_i\neq\alpha_j,\ 1\leq i,\ j\leq q-1$, $(x-\alpha_i,\ x-\alpha_j)=1$ and

$$Z_{p^k}[x]/(\Phi_q(x))\cong Z_{p^k}[x]/(x-\alpha_1)\times Z_{p^k}[x]/(x-\alpha_2)\times\ldots\times Z_{p^k}[x]/(x-\alpha_{q-1}). \tag{11}$$

Then

$$Z_{p^k}[x]/(x^n-1)\cong Z_{p^k}[x]/(x-1)\times Z_{p^k}[x]/(x-\alpha_1)\times\ldots\times Z_{p^k}[x]/(x-\alpha_{q-1}) \tag{12}$$

and a homomorphism φ may be defined as

$$\varphi: Z_{p^k}[x]/(x^n-1)\to Z_{p^k}[x]/(x-1)\times Z_{p^k}[x]/(x-\alpha_1)\times\ldots\times Z_{p^k}[x]/(x-\alpha_{q-1})$$
$$\varphi(f)\to(f(1),\ f(\alpha_1),\ f(\alpha_2),\ \ldots,\ f(\alpha_{q-1})).$$

If the polynomials $\varphi(f)$ compute by $mod\ p^k$, that is, the images under canonical homomorphism $\bar{\varphi}(f)\to(f(1),\ f(\alpha_1),\ f(\alpha_2),\ \ldots,\ f(\alpha_{q-1}))\ mod\ p^k$ are taken, it can be treated as $\bar{\varphi}(f)\in Z_{p^k}[x]$.
An invertible polynomial $f\in Z_{p^k}[x]/(x^n-1)$ is in the form of $f=\beta+ps(x)$, $s(x)\in Z_{p^k}[x]/(x^n-1)$ and $\left(\beta,\ p^k\right)=1$. $\varphi(f)$, which is an isomorphic image of chosen polynomial f in this form, is invertible. If we write a number $m\in Z^+$ as $m=\underset{p^k}{p_1^{s_1}}\ \underset{q}{p_2^{s_2}}\ldots p_i^{s_i}$ in a canonical form,

$$Z_m[x]/(x^n-1)\cong Z_{p^k}[x]/(x^n-1)\times Z_q[x]/(x^n-1)$$

and because $m\to\infty$ for $p^k\to\infty$ and $q\to\infty$, to examine an algebraic structure of the ring NTRU coverging to infinite as a direct product of Galois rings is beneficial.

As a result of all these evidences, we can add an isomorphism φ to a NTRU process as a secret key. Let $h = f_q^{-1} \star g \ (mod\ q)$ be a public key where $f \in {Z_{p^k}[x]}/{(x^n-1)}$ and $g \in {Z_q[x]}/{(x^n-1)}$. Let $m \in {Z_{p^k}[x]}/{(x^n-1)}$ and an error polynomial $r(x)$ be arbitrarily chosen. Let the message be hidden as $e \equiv p^k r \star f_q^{-1} \star g + \varphi(m) \ (mod\ q)$.

$$e \star f \equiv p^k r \star g + f \star \varphi(m) (mod\ q) \equiv f \star \varphi(m) \left(mod\ p^k\right)$$

(let a suitable parameter k be chosen).

$$e \star f \star {f_{p^k}}^{-1} \equiv \varphi(m) \left(mod\ p^k\right)$$

$$e \equiv \varphi(m) \left(mod\ p^k\right)$$

$$\left(e \in {Z_{p^k}[x]}/{(x^n-1)}\right)$$

$$\varphi^{-1}(e) \equiv m \left(mod\ p^k\right).$$

6 The Choosing of Private Key Polynomial F

Now we provide a lemma that specifies the choosing of private key polynomial f for the NTRU system moving into Galois rings.

Lemma 2 Let $p \geq 3$ be a prime number and $n \in$. If $(f(x),\ p) = 1$, then $f^p(x) \equiv 1 \left(mod\ p^{n+1}\right)$ if and only if $f(x) \equiv 1 \ (mod\ p^n)$.

Proof. ($\Leftarrow$) Let $f(x) \equiv 1 \ (mod\ p^n)$. Then $p^n \mid f(x) - 1$, in fact $p \mid f(x) - 1$ and it means that $f(x) \equiv 1 \ (mod\ p)$. Thus,

$$f^{p-1}(x) + f^{p-2}(x) + \ldots + f(x) + 1 \equiv 1 + 1 + \ldots + 1 \equiv p \equiv 0 \ (mod\ p),$$

i.e., $p \mid f^{p-1}(x) + f^{p-2}(x) + \ldots + f(x) + 1$. Hence

$$p^{n+1} \mid (f(x) - 1)\left(f^{p-1}(x) + f^{p-2}(x) + \ldots + f(x) + 1\right) = f^p(x) - 1 \Rightarrow f^p(x) \equiv 1 \left(mod\ p^{n+1}\right).$$

($\Rightarrow$) Let's prove it by mathematical induction over n. Assume that $f^p(x) \equiv 1 \left(mod\ p^2\right)$ for $n = 1$. Then

$$f^p(x) = f(x).f^{p-1}(x) = f(x).(1 + kp)\,1 + lp^2 \Rightarrow f(x) \equiv 1 \ (mod\ p)$$

and the claim is verified. Now, let the assumption be verified for $n \in$. Suppose that $f(x) \equiv 1 \left(mod\ p^{n+2}\right)$. We obtain from the hypothesis that $f^p(x) \equiv 1 \left(mod\ p^{n+1}\right) \Leftrightarrow f(x) \equiv 1 \ (mod\ p^n)$. Since

$$f^p(x) = (1 + kp^n)^p = 1 + pkp^n + \sum_{j=2}^{p} \binom{p}{j} k^j p^{nj}$$

$$= 1 + pkp^n + lp^{2n+1} + k^p p^{np},$$

$p \mid \binom{p}{j}$ and $2n + 1 \geq n + 2$, $np \geq n + 2 \ \ (p \geq 3)$ by writing $f(x) = 1 + kp^n$, we obtain

$$1 \equiv f^p(x) \equiv 1 + kp^{n+1} \ \left(mod\ p^{n+2}\right)$$

$$p^{n+2} \mid \left(1 + kp^{n+1}\right) - 1 = kp^{n+1} \Rightarrow p \mid k.$$

Because $f(x) = 1 + kp^n$, it follows $f(x) \equiv 1 \left(mod\ p^{n+1}\right)$ and the proof given by mathematical induction.

Table 1 The proposed NTRU scheme

Old		New	
public key	Secret key	public key	Secret key
$p,\ q,\ h,\ N$	$f,\ f_p^{-1},\ g$	$p^k,\ q^t,\ h,\ N$	$f,\ f_{p^k}^{-1}$
$p=3$	$f=1+pF$	$p=3^{37}$	g, x^k, φ^{-1}
$q=59$		$q=59^{23}$	$f=88+pF$
$N=11$		$N=113$	$g \to g^k$
$h=f_q^{-1}\star g$		$h=f_{q^t}^{-1}\star g^k$	

7 Discussion and Conclusion

By transforming the set of chosen invertible polynomial f to ${Z_{p^k}[x]}/{(x^n-1)}$, a greater number of private key generation is aimed to be given. Also, by exponentiating the specified kth power of private key polynomials g and f in the statement $f\star h=g$, the public key h is made slightly more complex. By substituting $h\star x^k=f_q^{-1}\star g\star x^k$ instead of $h=f_q^{-1}\star g$, an appropriate kth rotation of public key is chosen. Since $Z_m\cong Z_{p^\alpha}\times Z_{q^\beta}$ for $m\in Z$ so that $m=p^\alpha q^\beta$, $(p,\ q)=1$, a homomorphism φ is defined by

$$\varphi : Z_m \to Z_{p^\alpha}\times Z_{q^\beta}$$

$$\varphi(f)=\left(f\ \ mod\ p^\alpha,\ f\ \ mod\ q^\beta\right)$$

and it is applied to the chosen message polynomial. The inverse of isomorphism φ is added to the secret key set. By taking the message polynomials m from the ring ${Z_{p^k}[x]}/{(x^n-1)}$ instead of ${Z_p[x]}/{(x^n-1)}$, the further sets of concealable polynomial are obtained. It is suggested that the processes executing in the fields Z_p ve Z_q of classical NTRU system perform in the Galois rings Z_{p^k} ve Z_{q^r}. Because $p^\alpha\to\infty$ for $\alpha\to\infty$ and $m\to\infty$, it is predicted that the modulos p ve q can be chosen as large as desired from the public keys.

References

[1] Hoffstein, J., Pipher, J. and Silverman, J. H. (1996). NTRU: A new high speed public key cryptosystem. *Crypto 96,* preprint. Available at http://www.ntru.com/articles
[2] Jaulmes, É. and Joux, A. (2000). A chosen-ciphertext attack against NTRU. *Advances in Cryptology Conference-Crypto 2000.*
[3] Gentry, C. Cryptoanalysis of the revised NTRU signature scheme.
[4] Gentry, C. (2001). Key recoverge and message attcaks on NTRU-Composite. Springer Verlag.
[5] Banks, W. D. (2002). A variant of NTRU with non invertible polynomials. Springer Verlag.
[6] Gaborit, P. and Sole, P. (2002). CTRU, a polynomial analogue of NTRU. Inria.
[7] Coglianese, M. and Goi, B. M. (2005). MaTRU: A new of NTRU based cryptosystem. Springer Verlag.
[8] Jarvis, K. and Nevins, M. (2015). ETRU: NTRU over the Eisenstein integers. Springer.
[9] Hoffstein, J., Pipher, J. and Silverman, J. H. (2009). Choosing parameters for NTRUEncrypt. Springer Verlag.
[10] Hoffstein, J., Pipher, J., Shanck, J. M. and Whyte, W. (2015). Choosing parameters for NTRU. Springer Verlag.
[11] Wan, Z. X. (2011). Finite fields and Galois rings. World Scientific Publishing Company.
[12] McDonald, B. R. (1973). Finite rings with identity. University of Oklahama Publishing.