TURKISH JOURNAL OF SCIENCE
VOLUME 9, ISSUE 3, 207–215
ISSN: 2587–0971

https://www.tjoscience.com

A NTRU Type Cryptosystem Based on Circulant Matrices

Mehmet SEVER[a]

[a] *Kilis 7 Aralık University, Department of Mathematics, Faculty of Arts and Sciences, Kilis-Turkey*

Abstract. In this study, NTRU cryptosystem is examined on circulant matrices. These matrix types have been studied due to the rapid selection of matrices that will serve as private keys. Again, using some interesting and important linear algebra properties of circulant matrices, the NTRU cryptosystem has been studied in a different and original ring. Some results obtained place the NTRU cryptosystem on solid foundations in algebraically.

1. Introduction

In 1996, NTRU was first introduced by J. Hoffstein, J. Pipher and J. Silverman in Crypto' 96 [1]. Then NTRU's developers contributed to NTRU which is denoted as a ring-based and a public key encryption method by making parameter optimization [2]. In 2003, they introduced $NTRU_{SIGN}$ [3], i. e., a digital signature version of NTRU. In the same year, they with another team made a presentation which analyzed decryption errors of NTRU [4]. J. H. Silverman published a technical report about invertible polynomials in a ring in 2003 [5]. In 2005, J. H. Silverman ve W. Whyte published a technical report which analyzed error probabilities in NTRU decryption [6]. Also, the founding team which published an article on effects increasing security level of parameter choosing [7] has published related reports in the website www.ntru.com.

NTRU is quietly resistant to quantum computers based attacks as well as its speed. The basic reason of protecting this resistant bases on finding a lattice vector with the least length and powerfulness of problems of finding a lattice point closest to private key into a high dimensional lattice [8]. Unlike the other public key cryptosystems, the sheltering structure of the NTRU cryptosystem against these quantum based attacks moves it more interesting and developing position day by day.

Some examples of quitely full-scale non-destructive attacks to the NTRU cryptosystem were originally made by Coppersmith et al. in 1997 [9]. Then new parameters which does away with effects of this attack were presented by Hoffstein et al. in 2003 [10].

As an another example of attack [11], it has increased importance up till today by presenting to more powerful, current and new parameters and solutions to the NTRU cryptosystem organized an attack of splitting the difference [12].

On behalf of detailed readings, it can be seen to [13–15] for different types of attacks types, and on the contrary, it can be seen to [16–18] for proposed new parameters and new system.

Corresponding author: MS mail address: mhmtsvr.1@gmail.com ORCID: 0000-0003-2967-1943
Received: 14 November 2024; Accepted: 12 December 2024; Published: 31 December 2024.
Keywords. NTRU cryptosystem, NTRUSIGN, cryptology.
2010 *Mathematics Subject Classification*. 11T71, 14G50, 94A60, 94A62.
Cited this article as: Sever, M. (2024). A NTRU Type Cryptosystem Based on Circulant Matrices. Turkish Journal of Science, 9(3), 207–215.

2. Aim and Scope

In this study, which is aimed to carry the NTRU cryptosystem on robust algebraic structures, some interesting properties and results were added to the cryptosystem theoretically. Taking advantage of the fact that matrices are larger and more complex than a vector, more attention has been paid to security, which is the main purpose of cryptology. For this purpose, the newly proposed cryptosystem has been tried to be presented in a more complex and powerful form. But at the same time, since circulant matrices are determined by a vector with a basic rule, the new proposed system is also considered to be practical and useful. In the light of this study, new lattice types will be determined and security analyzes can be made by arranging attacks on the proposed NTRU crypto system.

3. NTRU Parameters

These are parameters using in the encryption and decryption operations of NTRU and in the key generation processes:

- N : it determines a maximum degree of polynomials being used. N is chosen as a prime so that the process is preserved against attacks, and it is chosen big enough so that the process is preserved from lattice attacks.
- q : it is a large module and it is chosen as a positive integer. Its values differ relatedly what we aim in the process.
- p : it is a small module and generally a positive integer. it is rarely chosen as a polynomial with small coefficients.

The parameters N, q and p can be differently chosen according to the preferred security level. The case $(p, q) = 1$ is always preserved so that the ideal (p, q) is equal to the whole ring.

- L_f, L_g : sets of private key, sets in which it is chosen polynomials to be kept confidential chosen for encryption.
- L_m : it is a plain text set. it is stated a set of unencrypted and codable polynomials.
- L_r : it is a set of error polynomials. It is stated a set of arbitrarily chosen error polynomials with small coefficients in the phase of encryption.
- *center* : it is a centralization method. An algorithm guaranteing which *mod* q reductions works in perfect truth in the phase of decryption.

It can be seen [1] for a perscrutation of the NTRU parameter which is introduced above in general for now and can be given its values in the next section.

4. Algebraic background of NTRU

4.1. Definitions and notation

The encryption operations of NTRU is performed in a quotient ring $R = Z[x]/(x^N - 1)$. N is a positive integer and it is generally chosen as a prime. If $f(x)$ is a polynomial in R, then f_k denotes a coefficient of x_k for every $k \in [0, N-1]$ and $f(x)$ denotes a value of f in x for $x \in \mathbb{C}$. A convolution product $h = f \star g$ is given by $h_k = \sum_{i+j \equiv k \ mod \ N} f_i \cdot g_j$ where f and g are two polynomials in R. When NTRU was first introduced, it was chosen p and q as a power of 3 and 2, respectively. The subset L_m : consisted of polynomials with the coefficients $\{-1, 0, 1\}$ called ternary polynomials. The private keys $f \in L_f$ was usually chosen in the form $1 + p \cdot F$. The studies shows that it can be chosen p as a polynomial and parameters can be varied.

4.2. Key generation

1. $f \in L_f$ and $g \in L_g$ is abritrarily chosen such that f is invertible in *mod* p and *mod* q.
2. $F_q = f^{-1}$ *mod* q and $F_p = f^{-1}$ *mod* p.
3. A private key is (p, F_p).
4. A public key is $H = p \cdot g \star F_q$ *mod* q.

It is noted that g cannot be used in the phase of decryption. Thus, it cannot be given as a private key. Since $H \star f = p \cdot g$ *mod* q, $H \star f = 0$ *mod* p which cannot be used when *mod* p is substituted.

4.3. Encryption

If the encryption is represented in an algorithmic language;

Input: a message $m \in L_m$ and a public key H.
Output: a cipher message $e \in \Upsilon(m)$

1. Chose $r \in L_r$ arbitrarily.
2. Return $e = r \star H + m$ *mod* q.

The set $\Upsilon(m)$ denotes plain texts m which can be encrypted.

4.4. Decryption

If a phase of decryption is represented as algorithmic, an algorithm D acts e as below:

Input: a cipher message $e \in \Upsilon(m)$ and a private key (p, F_p).
Output: a plain text $D(e) = m \in L_m$.

1. Calculate a *mod* $q = e \star f$*modq*.
2. Have a polynomial *amodq* with integer coefficients from $a = p \cdot r \star g + f \star m \in R$ by performing centralization operation.
3. m *mod* $p = a \star F_p$ *mod* p
4. a plain text $m = \Psi$ *mod* p

It is noted that Ψ is the mapping $\Psi : m \longmapsto m$ *mod* p. That is, it performs $\Psi : L_m \longrightarrow L_m$ *mod* p. It is important choosing of a convenient parameter in order to work decryption operation impeccably, i.e., $D(e) = m$.

5. Circulant Matrices

In the most general sense, a circulant matrix A is

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix} \tag{1}$$

for certain a_i, $0 \leq i \leq n-1$. Unless otherwise specified, all of the inputs a_i are chosen from Z. The circulant matrices are determined by a characteristic equation

$$A_{j,k} = a_{(k-j) \bmod n}.$$

[19]

Definition 5.1. *[19] If a circulant matrix A has the property $A = A^T$, then A is called a symmetric circulant matrix.*

5.1. Eigenvalues and Eigenvectors

The eigenvalues ψ_k and corresponding eigenvectors y^k of a circulant matrix A are solutions to an equation

$$Ay = \psi y. \tag{2}$$

The values

$$\psi_m = \sum_{k=0}^{n-1} a_k e^{-2\pi imk/n} \tag{3}$$

are different eigenvalues of the circulant matrix A, where $\alpha_m = e^{-2\pi im/n}$ are $n.$ complex roots of the unit for $0 \leq m \leq n-1$. Corresponding eigenvectors are

$$y^m = \frac{1}{\sqrt{n}}(1, e^{-2\pi im/n}, ..., e^{-2\pi im(n-1)/n}). \tag{4}$$

Definition 5.2. *[19] If a row vector forming a first row of a circulant matrix A is chosen in the form $(a_0, a_1, ..., a_{n-1})$, then a polynomial $f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ is called a relevant polynomial of A.*

5.2. Determinant

If a relevant polynomial f of a circulant matrix A, the determinant of A is

$$\det(A) = \prod_{j=0}^{n-1} f(\alpha_j). \tag{5}$$

[19]

Remark 5.3. *Since the determinant of a relevant circulant matrix A cannot be 0 for any polynomial f which does not accept $n.$ complex roots of the unit, A is invertible.*

5.3. Decomposition of circulant matrices

It is possible to write

$$Ay^m = \psi_m y^m, \quad m = 0, 1, ..., n-1$$

for Equation (4.2). If all eigenvectors of A are written in the form

$$U = [y^0|y^1|...|y^{n-1}]$$

such that its columns form a matrix U, respectively, U is called a matrix of eigenvectors of A [19].

Let $D = diag(\psi_m)$ be a matrix where eigenvalues ψ_m are sorted in its diagonal and other inputs are 0. Then it is possible that

$$AU = UD.$$

Thus, a circulant matrix A is split in the form

$$A = UDU^{-1}$$

and it is assimilated to a diagonal matrix. Similarly,

$$D = U^{-1}AU.$$

Theorem 5.4. *[19] Let A and D be two circulant matrices. Then*

(i) $AB = BA$, i.e., the multiplication is commutative,

(ii) $A + B$ is a circulant matrix,

(iii) if $\psi_m \neq 0$, then the matrix A is non-singular and its inverse is

$$A^{-1} = UD^{-1}U^{-1}.$$

Theorem 5.5. *The rank of a circulant matrix A is $n - d$ for* $\deg(\gcd(f(x), x^n - 1)) = d$ *where f is its relevant polynomial.*

Theorem 5.6. *The circulant matrices constitute a commutative ring according to the known matrix addition and multiplication. Also, this ring is denoted by M_C.*

Theorem 5.7. *A relevant circulant matrix is always invertible for a polynomial f such that* $\gcd(f(x), x^n - 1) = 1$.

6. The Proposed Cryptosystem

Let a polynomial f be chosen from a ring $R_q = Z_q[x]/(x^n - 1)$ such that $\gcd(f, x^n - 1) = 1$, and let the relevant circulant matrix of f be denoted by C_f. Define a mapping φ between rings R_q and M_C by

$$\begin{aligned} \varphi \quad &: \quad R_q \longrightarrow M_C \\ &\quad\;\; \varphi(f) = C_f. \end{aligned}$$

If it is shown that φ is an isomorphism, then the operations in the ring R_q are moved to M_C. Thus, a new NTRU-based cryptosystem is constituted by using different algebraic properties.

Theorem 6.1. *The mapping $\varphi(f) = C_f$ is an isomorphism.*

Proof. Since the relevant circulany matrix of a polynomial $f \in R_q$ is single, the mapping is well-defined. If $\varphi(f) = C_f$ and $\varphi(g) = C_g$ for $f, g \in R_q$, then the proof is completed since

(i) $\varphi(f + g) = C_{f+g} = C_f + C_g = \varphi(f) + \varphi(g)$ and

(ii) $\varphi(f \star g) = C_{f\star g} = C_f.C_g = \varphi(f).\varphi(g)$. ⊠

□

Particularly, this isomorphism is important to find invertible elements by utilizing the problem of finding eigenvalues in the ring M_C rather than just using Euclidean algorithm when invertible elements are searched in the ring R_q. Before the proposed system is introduced, the following presupposition are stated.

(i) Unless indicated otherwise, all polynomials $f \in R_q$ and $g \in R_q$ are chosen such that $(f, x^n - 1) = (g, x^n - 1) = 1$.

(ii) The set of polynomials to be sent as messages is as follows:

$$L_m = \{m \in R_q | C_m \ (mod\ p) = C_m\}.$$

(iii) Unless otherwise specified, the parameters (p, q, N) is as in the classical NTRU system.

6.1. How the NTRU system works in the ring M_C?

First, a message polynomial $m \in R_q$ which want to be sent is moved to M_C by the mapping $\varphi(m) = C_m$.Similarly, the operations are continued by moving the polynomials $\{f, g, r\}$ to M_C as follow.

(1) A matrix C_f^{-1} is obtained such that $C_f.C_f^{-1} = I$.

(2) A finite C_h is shared as a public key such that $p.C_f^{-1}.C_g = C_h$.

(3) A text C_e obtained in the form of

$$C_e \equiv p.C_f^{-1}.C_g.C_r + C_m \ (mod\ q)$$

is sent to a receiver as a cipher-text by choosing $C_r \in M_C$. The receiver is decrypted by secret key matrices $\{C_f, C_f^{-1}\}$ as below.

(1) The matrix $C_e.C_f \equiv C_a \ (mod\ q)$ is calculated.

(2) The proper parameters are chosen such that $C_a = C_Q \ (mod\ q)$. Then $C_a.C_f^{-1} \equiv C_b \ (mod\ p)$ is calculated.

(3) The process is finished by controlling $C_m = C_b \ (mod\ p)$.

The above mentioned proposition is to stay loyal to the classical NTRU algorithm. Though, more different systems are proposed in the ring M_C. For example, the following system proposition is an example of a symmetric encryption.

Proposition 6.2. *If a public key (or a secret key) using in the encryption is $C_f.C_g = C_h$ for $C_f, C_g \in M_C$ and $m \in L_m$, then a cipher-text*

$$C_e = p.C_r.C_h + C_h.C_m \ (mod\ q)$$

is only decrypted by a public or secret key.

Proof. If C_h^{-1} and

$$C_e.C_h^{-1} = p.C_r.C_h.C_h^{-1} + C_h.C_m.C_h^{-1} \ (mod\ q)$$

are calculated, then

$$C_e.C_h^{-1} \equiv C_m \ (mod\ p)$$

since M_C is commutative. This case can aim to the speed and effortlessness by decreasing the security. ⊠ □

Now, let the proposed cryptosystem be restated by two public keys and four secret keys as follows.

Proposition 6.3. *If a message $m \in L_m$ is sent by encrypting in the form of*

$$C_e = p.C_h.C_r + C_H.C_m \ (mod\ q)$$

by means of $C_r \in M_C$ where the public keys $h = C_f^{-1}.C_g$ and $H = C_g^{-1}.C_f$ are shared and the matrices $\{C_f, C_g, C_f^{-1}, C_g^{-1}\}$ are kept confidental by means of the matrices C_f^{-1} and C_g^{-1} for $C_f, C_g \in M_C$, then the message is tried to decrypt by sending more safely.

Proof. It follows

$$C_f.C_e.C_g = p.C_g^2.C_r + C_f^2.C_m \ (mod\ q) \tag{6}$$

by means of the statement

$$C_e = p.C_f^{-1}.C_g.C_r + C_g^{-1}.C_f.C_m \ (mod\ q). \tag{7}$$

If $C_f^2 \in M_C$, the matrix C_f^{-1} is multiplied by Equation (6.7) twice and the result is find in *mod p*, then

$$C_f^{-1}.C_e.C_g = C_m \ mod\ p$$

which means that the proof is completed. ⊠ □

Remark 6.4. *As it can be clearly seen from Proposition 6.1 and Proposition 6.2, since a mapping $C_m \xrightarrow{\varphi^{-1}} m$ does not process without knowing the isomorphism φ satisfying $m \in L_m \xrightarrow{\varphi} C_m$, the final step $\varphi^{-1}(C_m) = m$ of the encryption is applied which means that it adds to the set of the secret keys of φ.*

Let a new isomorphism be defined for a different system proposition, and let a ring of diagonal matrices be denoted by M_D.

Theorem 6.5. *It is possible*

$$C_m = UDU^{-1} \text{ and } D = U^{-1}C_mU$$

for a matrix C_m from the decomposition theorem of circulant matrices. By means of this theorem, let a mapping δ be defined by

$$\begin{array}{rcl} \delta & : & M_C \longrightarrow M_D \\ & & \delta(C_m) = D_m \end{array}$$

where D_m denotes an eigenvalue matrix corresponding m. The mapping δ is an isomorphism.

Proof. It is clear from the decomposition theorem of circulant matrices that a circulant matrix C_m is absolutely similar to a diagonal matrix D. Hence, the mapping is well-defined.

Let

(i) $\delta(C_{m_1}) = D_{m_1}$, $\delta(C_{m_2}) = D_{m_2}$ and $\delta(C_{m_1} + C_{m_2}) = \delta(C_{m_1+m_2}) = D_{m_1+m_2} = D_{m_1} + D_{m_2} = \delta(C_{m_1}) + \delta(C_{m_2})$,

(ii) $\delta(C_{m_1}.C_{m_2}) = \delta(C_{m_1 \star m_2}) = D_{m_1 \star m_2} = D_{m_1}.D_{m_2} = \delta(C_{m_1}).\delta(C_{m_2})$, and

(iii) $D_{m_1} = D_{m_2}$
for $C_{m_1} \neq C_{m_2}$. Since the eigenvector matrices U of all circulant matrices are same, it is obvious that

$$D_{m_1} = U^{-1}C_{m_1}U \text{ and } D_{m_2} = U^{-1}C_{m_2}U.$$

If

$$U^{-1}C_{m_1}U = U^{-1}C_{m_2}U,$$

then

$$C_{m_1} = C_{m_2},$$

and so it follows

$$m_1 = m_2$$

which is a contradiction. Thus, the mapping is bijective. ⊠

□

Let an isomorphism δ be added to the NTRU system as follows.

Proposition 6.6. *The encryption*

$$C_e \equiv p.C_h.C_r + C_H.\delta(C_m) \ (mod\ q) \tag{8}$$

processes propoerly for $C_f, C_g \in M_C$ ve $m \in L_m$.

Proof. If Equation (6.8) transforms to

$$C_H^{-1}.C_e = \delta(C_m) \ (mod\ p)$$

and the mapping δ^{-1} is applied in the final step, then

$$\delta^{-1}(C_H^{-1}.C_e) = C_m \ (mod\ p)$$

and

$$\varphi^{-1}\delta^{-1}(C_H^{-1}.C_e) = m$$

after applying φ^{-1}. Thus, the proof is completed. ⊠ □

Now, a new algorithm is presented by using that the eigenvector matrix U of any circulant matrix is single as follows.

Proposition 6.7. *The equation*

$$C_e = p.C_r.C_h.U + U.C_h.\delta(C_m) \ (mod\ q)$$

can be decrypted on condition that $C_f, C_g \in M_C$ and U are as in Proposition 6.3, $C_f.C_g = C_h$ is a public key and U is a secret key.

Proposition 6.8. *A message $m \in L_m$ can be sent in the three steps in encrytion by means of the equation $C_m = UD_mU^{-1}$ as below. $C_m \longrightarrow \{U, D_m, U^{-1}\}$ are taken, respectively. That is,*

$$C_{e_1} \equiv p.C_r.C_h.U + U.C_h.U \ (mod\ q)$$

$$C_{e_2} \equiv p.C_r.C_h.U + U.C_h.D_m \ (mod\ q)$$

$$C_{e_3} \equiv p.C_r.C_h.U + U.C_h.U^{-1} \ (mod\ q)$$

process, respectively, and the product of the found plain texts gives a major plain text after all three decryptions are finished. This suggestion is the effective method against the plain text attacks.

Theorem 6.9. *Let a polynomial $f(x) \in R_q$ be reducible in the ring R_q, i.e. $f(\beta_0) = 0\ (mod\ q)$ be satisfied for some $\beta_0 \in Z_q$. Then there exists a relationship $C_f.C_{\beta^T} = 0$ between the relevant circulant matrix C_f of the polynomial f and C_{β^T} correponding to the transpoze of a vector $\beta = (1, \beta_0, \beta_0^2, ..., \beta_0^{n-1})$.*

Proof. Let $f(x) = \sum_{i=0}^{n-1} \alpha_i x^i$ and $\beta_0 \in Z_q$ için $f(\beta_0) = 0$. Then $\sum \alpha_i \beta_0^i = 0$, and $\langle \alpha, \beta \rangle = 0$ where $\alpha = (\alpha_0, \alpha_1, ..., \alpha_{n-1})$ and $\beta = (1, \beta_0, \beta_0^2, ..., \beta_0^{n-1})$ are in vectorial forms. Similarly, a cyclic translation of α and β is $\langle \overrightarrow{\alpha}\, \overrightarrow{\beta} \rangle = 0$ for $\overrightarrow{\alpha}$ and $\overrightarrow{\beta}$, and since this identity is preserved for all of the $n-1$ translations, it is possible to write

$$C_f.C_{\beta^T} = 0 \ (mod\ q)$$

in the matrix form. ⊠ □

Let Theorem 6.3 be used in the NTRU cryptosystem as follows: let the dual of the relevant circulan matrix of a chosen secret key f add to a message m as an error insertion.

Theorem 6.10. *If a matrix $C_h = C_f^{-1}.C_g$ is chosen as a public key and the dual of a matrix C_f is denoted by C_{β^T} by means of the circulant matrices C_f and C_g, then it is properly obtained a message C_m from the encryption equation*

$$C_e = p.C_h.C_r + (C_m + C_{\beta^T})\ (mod\ q).$$

Proof. It follows that

$$\begin{aligned} C_f.C_e &\equiv p.C_g.C_r + C_f.C_m + C_f.C_{\beta^T}\ (mod\ q) \\ &\equiv p.C_g.C_r + C_f.C_m + 0\ (mod\ q) \\ &\equiv C_f.C_m\ mod\ p \end{aligned} \tag{9}$$

by multiplying

$$C_e \equiv p.C_f^{-1}.C_g.C_r + (C_m + C_{\beta^T})\ (mod\ q)$$

by the private key C_f from the left. Then

$$C_f^{-1}.C_f.C_e \equiv C_m\ mod\ p$$

is obtained by using the private key C_f^{-1}, and so the claim is proved. Thus, the encryption is made safe by hidding the message matrix a bit more by means of an another message. ⊠ □

Traditionally, there exists a uniquely defined solution x_0 of the system of linear equations $Ax = b$ in Z^n as log as A is a matrix with the rank n. Because the circulant matrices satisfy this property, it is presented a different contribution which they add to the NTRU system.

Theorem 6.11. *Let the polynomials $f, g, m \in R_q$ be chosen as in the classical NTRU ring and let C_h, C_H and C_f be chosen as in Proposition 6.2. If a message polynomial m which want to be encrypted is hidden in the form of $C_f.m = y$ and then it is sent in the form of $C_e = p.C_r.C_h + C_H.C_y\ mod\ q$, the decryption processes properly.*

Proof. It is proved from Proposition 6.2 C_y is obtained from the equation $C_e \equiv p.C_r.C_h + C_H.C_y\ mod\ q$. Then it is shown that $C_e \equiv C_y\ mod\ p$. Thus, we have $e \equiv y\ mod\ p$ by the means of the isomorphism φ^{-1} applying in the form of $\varphi^{-1}(C_e) \equiv \varphi^{-1}(C_y)\ mod\ p$, and so it follows from $C_f.m = y \Rightarrow C_f^{-1}.y = m$ that $C_f^{-1}.e = m$ which the claim is proved. □

7. Conclusion and Recommendations

In this study, which aims to carry the NTRU cryptosystem on solid algebraic structures, some interesting features and results are added to the cryptosystem. Taking advantage of the fact that matrices are larger and more complex than a vector, more attention has been paid to security, which is the main purpose of cryptology. But at the same time, since circulant matrices are determined by a vector with a basic rule, the new proposed system is also considered to be practical and useful. In the light of this study, new lattice types can be determined and security analyzes can be made by arranging attacks on the proposed NTRU crypto system.

References

[1] Hoffstein J, Pipher J, Silverman JH. A ring-based public key cryptosystem, ANTS 1998, LNCS, Springer, Vol. 1423, (1998), 267-288.
[2] Hoffstein J and Silverman J. Optimizations for NTRU, in: Public-key cryptography and computational number Theory, Degruyter, (1971).
[3] Hoffstein J, Pipher J, Silverman JH and Whyte W. $NTRU_{SIGN}$: Digital signatures using the NTRU lattice, LNCS, Springer, Vol.2612, (2003).
[4] Silverman JH. Invutibility intruncated polynomial rings. Technical Report, NTRU Cryptosystems, (2003). Available at http://www.ntru.com.
[5] Graham NA, Nguyen PQ, Proos J, Silverman JH, Singer A and Whyte W. The impact of decryption failures on the security of NTRU encryption, Crypto'03, LNCS, Springer-Verlag, Vol. 2729, (2003), 226-246.
[6] Silverman JH and Whyte W. Estimating decryption failure probabilities for NTRU encrypt, Technical Report 18, (2005). Available at http://www.ntru.com. .
[7] Hoffstein J, Pipher J, Silverman JH, Whyte W and Zhang Z. Choosing parameters for NTRU encrypt. NTRU Challenge, (2015). Available at http://www.ntru.com/ntru-challenge.
[8] Abdurrahmane N. The mathematics of the NTRU public key cryptosystem, Mathematical Concepts IGI Global, (2015).
[9] Coppersmith D and Shamir A. Lattice attacks on NTRU, Euro-crypto'97, Lecture Notes in Computer Science, Vol. 1233, Springer, Berlin, (1997).
[10] Hoffstein J, Silverman J and Whyte W. Estimating breaking times for NTRU lattices, Technical Report 12, (2003). Available at http://www.ntru.com.
[11] Graham N, Silverman JH and Whyte W. A meet in the middle attack on a NTRU private key, NTRU Technical Report 04, (2003). Available at http://www.ntru.com.
[12] Graham N, Silverman JH, Singer A and Whyte W. NAEP: provable security in the presence of decryption failures, Cryptology ePrint Archive, Report 2003/172, (2003).
[13] Whyte W, Graham N and Silverman JH. Choosing parameter sets for NTRU encrypt with NAEP and SVES-3, Topics in Cryptology CT-RSA, (2005).
[14] Meskanen T and Renuall A. A wrap error attack against NTRU, University of Turku Technical Report TUCS 507, (2003).
[15] Proos J. Imperfect Decryption and an attack on the NTRU, (2003). Available at http://eprint.iacr.org.
[16] Hong J, Han JW and Han D. Chosen-ciphertext attacks on optimized NTRU, (2002). Available at http://eprint.iacr.org.
[17] Nguyen P and Pointcheval D. Analysis and improvements of NTRU paddings, Crypto 2002, Springer-Verlag, (2002).
[18] Gentry C and Szydlo M. Cryptoanalysis of the revised NTRU signature scheme, Eurocrypt'02, Vol. 2332, Springer-Verlag, (2002).
[19] Roger A. Horn, Charles R. Johnson, Matrix analysis, Cambridge University Press, (1990)