TURKISH JOURNAL OF SCIENCE https://www.tjoscience.com
VOLUME 9, ISSUE 2, 147–156
ISSN: 2587–0971

A NTRU Type Cryptosystem and a Construction of Digital Signature Version over Companion Matrices

Mehmet SEVER[a]

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

Abstract. In this study, the NTRU cryptosystem is examined on companion 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 companion matrices, the NTRU cryptosystem has been studied in a different and specific ring. Some results obtained place the NTRU crypto system on solid foundations in algebraically. NTRU cryptosystem was found to be stronger than Knapsack method. And a new type of digital signature has been obtained over companion matrices.

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 quitely 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 cryptosystems against these quantum based attacks moves it more interesting and developing position day by day.

Some examples of quietly full-scale non-destructive attacks to the NTRU cryptosystem were originally made by Coppersmith et al.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 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: 2 June 2024; Accepted: 10 August 2024; Published: 30 September 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 and a Construction of Digital Signature Version over Companion Matrices. Turkish Journal of Science, 9(2), 147–156.

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 companion 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 cryptosystem.

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 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 coeffients $\{-1, 0, 1\}$ 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 arbitrarily 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. Companion Matrices

Because of having the interesting algebraic properties, some preliminaries are given before the companion matrices' contribution to the NTRU system is mentioned.

Remark 5.1. *Unless otherwise specified, the polynomials whose constant terms are not "0" are used.*

Definition 5.2. *[19] A companion matrix of a monic polynomial $P(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} + x^n$ on a field K is a square matrix defined by as follows:*

$$C_P = \begin{bmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -c_{n-1} \end{bmatrix}.$$

In consideration of Definition 4.1, a base $v_1, v_2, ..., v_n$ of a vector space V on the field K is translated in the form of

$$Cv_i = C^i v_1 = v_{i+1}, \quad i < n$$

by means of a matrix C.

Remark 5.3. *It is moved to the NTRU system interesting algebraic properties such as the characteristic and minimal polynomials of a companion matrix C_f of a monic and irreducible polynomial $f \in K[x]$ chosen from a ring $K[x]$ of polynomials of a variable x on a field K are same and the roots of this polynomial are eigenvalues of C_f.*

Remark 5.4. *An arbitrarily irreducible polynomial f is chosen in this study when operating in a module $x^n - 1 = 0$ in the classical NTRU system, and the matrix C_f operates $g \longmapsto x.g$ for $g \in R_q$ in the ring.*

Remark 5.5. *Calculating inverses of a private key f is long in the NTRU ring but calculating the inverse of C_f is easy for irreducible f whose leading coefficient is not 0 in this study. The constant term of f is found by $\det C_f = a_0$ and $C_f^{-1} = \dfrac{Adj\ C_f}{\det C_f}$ for $a_0 \neq 0$.*

Remark 5.6. *Even though the inverse of $f \in R$ in mod p is known, it is also necessary to calculate its inverse in mod q. In fact, the forms $C_f^{-1} + pU$ and $C_f^{-1} + qU$, $U \in M_{n\times n}$ of a matrix C_f^{-1} found in the form of $C_f.C_f^{-1} = I$ are the inverses of C_f in mod p and mod q, respectively.*

5.1. Characterization

A characteristic and minimal polynomials of a matrix C_P are same and it equals to P. Moreover, the following statements are equivalent

- A is similar to a companion matrix on the field K,
- a characteristic and minimal polynomials of A are same and its degree is n,
- there exists a vector $v \in V$ in the space $V = K^n$ such that $\{v, Av, A^2v, ..., A^{n-1}v\}$ is a new base of V,

where A is a $n \times n$ matrix on the field K (See [19]).

Remark 5.7. *Every square matrix is not similar to a companion matrix. However, it can be assimilated to a block matrix whose blocks are companion matrices.*

5.2. Diagonalisation

If all roots of a chosen polynomial $P(x)$ are discrete, then the corresponding companion matrix C_P can be diagonalized by

$$vC_Pv^{-1} = diag(\tau_1, \tau_2, ..., \tau_n)$$

where $\tau_1, \tau_2, ..., \tau_n$ are different roots of P (See [19]).

5.3. Determinant

The determinant of the corresponding companion matrix is non-zero as long as the constant term of the relevant polynomial $P(x)$ of a companion matrix is not zero.

6. The Construction of The NTRU based Cryptographic Application On The Companion Matrices

Choosing parameters is generally as in the classical NTRU choices and different choices are applied in some special cases. For example, the choices p, q and N remain the same in general. But a private key is mostly chosen by a irreducible polynomial whose constant term is non-zero. Now, let the system be stated mathematically. First, a polynomial $m \in R_q$ be mapped to a companion matrix by means of a mapping φ defined by

$$\varphi : R_q \longrightarrow M_C$$

$$\varphi(m) = \begin{bmatrix} 0 & 0 & \dots & 0 & -m_0 \\ 1 & 0 & \dots & 0 & -m_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -m_{n-1} \end{bmatrix}$$

where M_C is a set of companion matrices. It is clear that φ is well-defined and one-to-one. Also, the mapping φ^{-1} maps a matrix C_m to $m \in R_q$ which determines single C_m. Let polynomials $f, g, r \in R_q$ be chosen arbitrarily such that their constant terms are non-zero. The relevant companion matrices C_f, C_g and C_r are constituted and a message $m \in R_q$ is sent by calculating in the form of

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

where $C_f^{-1}.C_g = C_h$ is a public key. It is indicated that C_e does not need to be a companion matrix. C_e is only chosen for the notation rapport. Besides, the addition and multiplication of companion matrices from the set M_C are the ordinary matrix addition and multiplication, respectively.

Proposition 6.1. *The classical NTRU encryption algorithm runs properly over the companion matrices.*

Proof. If the constant term of f is not sero, then $\det C_f \neq 0$ and there exists C_f^{-1}. If the equation

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

is multiplied by C_f, then it is obtained

$$C_f.C_e \equiv p.C_r.C_g + C_f.C_m \ (mod\ q)$$

, and so an equation

$$C_f.C_e \equiv C_f.C_m \ (mod\ p)$$

is reached in *mod p* under choosing of the proper parameters. If the latest equation is multiplied by C_f^{-1}, then it follows that

$$C_e \equiv C_m \ mod\ p$$

which $C_e = C_m\ mod\ p$ for $\mathbf{m} \in R_q$ chosen under the condition $C_{\mathbf{m}} = C_m\ (mod\ p)$ and $\varphi^{-1}(C_e) = \varphi^{-1}(C_m) = \mathbf{m}$ in the final step, i.e., the claim is proved. ⊠ □

Theorem 6.2. *If q is chosen as a prime number, f is chosen as an irreducible polynomial and $\deg f = n$, then $R_q = Z_q[x]/\langle f(x)\rangle$ is a field and is a n-dimensional vector space on the field Z_q. If j times rotations of $\mathbf{m}$ to the right is denoted by $\mathbf{m}^j$ for $\mathbf{m} = (m_0, m_1, ..., m_{n-1})$ and $e_j = (0, 0, ..., x^j, ..., 0)$, where C_p is a companion matrix of $p \in R_q$ and $m \in R_q$ is chosen an arbitrary polynomial according to the classical base $\{1, x, x^2, ..., x^{n-1}\}$, then the statement*

$$e_j. \sum_{i=0}^{n} m_i C_p^i = \mathbf{m}^j$$

is verified.

Proof. It is sufficient to prove the theorem for the base vector $e_1 = (1, 0, ..., 0)$. It follows that

$$\begin{array}{rcl} e_1.\sum_{i=0}^{n} m_i C_p^i & = & e_1.[m_0 I + m_1 C_p + m_2 C_p^2 + ... + m_{n-1} C_p^{n-1}] \\ & = & m_0 e_1 + m_1 e_2 + ... + m_{n-1} e_n \quad (C_p e_i = e_{i+1}) \\ & = & (m_0, m_1, ..., m_{n-1}) \\ & = & \mathbf{m}. \end{array}$$

If it is multiplied from left by e_2 instead of e_1, then the result is the second rotation of **m**, and if it is multiplied from left by e_n instead of e_1,, then the result is the n-th rotation of **m**. Thus, the claim is proved. ⊠ □

Let theorem 6.1 be added to the NTRU system.

Theorem 6.3. *In addition to the conditions in Proposition 6.1, a matrix C_t is chosen for extra $t \in R_q$, a message $m \in R_q$ is sent by encrypting in the form of*

$$C_e = p.C_r.C_h + \sum m_i C_t^i \ (mod\ q),$$

and it is properly decrypted by adding an extra base e_1 to the set of private keys.

Proof. If the final step of Proposition 6.1 is reached without repeating similar steps, then it follows that

$$e_1.C_e = e_1 \sum m_i C_t^i = \mathbf{m}$$

when

$$C_e = \sum m_i C_t^i \ mod\ p \tag{1}$$

is multiplied by the base vector e_1. Hence, the proof is completed. ⊠ □

Remark 6.4. *An arbitrary base e_j can be chosen as a private key instead of the base e_1. Since it follows the j. rotation of the message, the message can be reached by the inverse rotation.*

Theorem 6.5. *Let a polynomial $t \in R_q$ be determined such that it does not have a multiple zero. Then $(t, t') = 1$ where t' is the derivative of the polynomial t. There exists $s \in R_q$ satisfying the statement*

$$t'.C_t.[s].\alpha^T = 1$$

for a vector

$$\alpha^T = \begin{bmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{bmatrix}$$

where α is a root of t.

Proof. Since t does not have a multiple zero, $t' \neq 0$ and C_t is an invertible matrix. Under these conditions, there exists at least one solution to the n equation system with n variables so that this solution can be chosen as $[s]$. ⊠ □

Theorem 6.3 is used in the NTRU system as follows.

Theorem 6.6. *After the encryption algorithm stated in Proposition 6.1 is calculated in the form of*

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

if the encrypted form

$$t'.C_t.[s].e_c = e_c'$$

is sent, then the message m is properly reached.

Proof. Since $t'.C_t.[s].[\alpha^T] = 1$ from Theorem 6.3, the first code $e'_c.[\alpha^T] = e_c$ is reached and the later steps are as in Proposition 6.1. Hence, the vector α^T can be added to the set of secret keys by means of a root of a chosen polynomial t. ⊠ □

Theorem 6.7. *If A_1, A_2, A_3 and A_4 are companion matrices on R_q, then a message $m \in R_q \times R_q$ can be sent double lengt by means of a matrix $\mathcal{A}$ by*

$$\mathcal{A} = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}.$$

Proof. The companion matrices A_i are invertible for $1 \leq i \leq 4$. Since $\det \mathcal{A} = \det A_1.A_4 - \det A_2.A_3$, the matrix $\mathcal{A}$ is invertible under the condition $\det A_1.A_4 \neq \det A_2.A_3$ and so the message m is properly decrypted if $\mathcal{A}$ is chosen as a secret key and is added to the system in the form of

$$c_e \equiv p.\begin{bmatrix} C_r & C_r \\ C_r & C_r \end{bmatrix}.\begin{bmatrix} C_h & C_h \\ C_h & C_h \end{bmatrix} + \mathcal{A}.\begin{bmatrix} C_m & C_m \\ C_m & C_m \end{bmatrix} \, mod\ q. \quad ⊠$$

□

7. A New Multiplication Type of Companion Matrices

A new multiplication of companion matrices defined on Z is introduced.

Let the multiplication of the relevant companion matrices C_x and C_y of vectors $x = (x_0, x_1, ..., x_{n-1})$ and $y = (y_0, y_1, ..., y_{n-1})$ be definde by

$$\theta : M_C \times M_C \longrightarrow M_C$$

$$\theta(C_x, C_y) = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & \langle x, y\rangle \\ 1 & 0 & 0 & \dots & 0 & \langle x, y\rangle \\ 0 & 1 & 0 & \dots & 0 & \langle x, y\rangle \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & \langle x, y\rangle \end{bmatrix},$$

respectively. It is obvious that θ is a binary operation on M_C. That is, it is well-defined and closed. However, there exists no unit element according to this operation, and so there exists no invertible elements. When the vectors x and y are arbitrarily chosen, the operation θ can generate an output

$$\left[\begin{array}{c|c} \frac{0}{I} & \alpha \end{array}\right]$$

for any $\alpha \in Z$. A linear equation

$$a_1x_1 + a_2x_2 + ... + a_nx_n + b = 0$$

has also infinite solutions in Z^n. If the set $\{x_1, x_2, ..., x_{j-1}, x_{j+1}, ..., x_n\}$ is known or x_i are chosen for $x_i \neq x_j$ under the choice of all $a_i \neq 0$, then x_j is known from the formulae

$$x_j = -\frac{b}{a_j} - \sum_{i \neq j} \frac{a_i}{a_j} x_i.$$

Therefore, there exists a vector (x_i) which can give the output b for a chosen vector (a_i). Exactly q of these solutions are in Z_q. Now, let the addition be defined in M_C by

$$\oplus : M_C \times M_C \longrightarrow M_C$$

$$\oplus(C_x, C_y) = \left[\begin{array}{c|c} \frac{0}{I} & x + y \end{array}\right].$$

$\oplus$ is a well-defined and closed operation on M_C. A zero of this operation is an element

$$\oplus(C_x, C_y) = \left[\begin{array}{c|c} 0 & \\ \hline I & \end{array} 0\right].$$

The following proposition can be given without proof.

Proposition 7.1. *There exists at least one C_y such that $\theta(C_x, C_y) = 0_{M_C}$, when C_x is known for $x, y \in Z^n$ whose componenets are non-zero.*

Proposition 7.1 can be added to the NTRU based cryptosystem as below.

C_f is obtained and is hidden such that $\theta(C_g, C_f) = 0$ for an arbitrarily chosen $g \in R_q$. Also, C_r is obtained and $\theta(C_r, C_g) = C_h$ is shared as a public key for an arbitrarily chosen $r \in R_q$. When a message C_m is encrypted, C_e calculated as

$$C_e \quad \equiv \quad p.\theta(C_r, C_g) \oplus (C_g \oplus C_m) \; mod \; q \tag{2}$$

is sent to the receiver by paying attention that $\theta(C_f, C_m) \neq 0$. C_h is hold as a public key, C_f and the matrices $C_m.\theta(C_f, C_m)$ are hold as secret keys.

Theorem 7.2. *The encrypted message m can be properly obtained from Equation (7.2).*

Proof. If Equation (7.2) is multiplied by C_f, then

$$\theta(C_f, C_e) \equiv p.\theta(C_f, \theta(C_r, C_g)) \oplus \theta(C_g, C_f) \oplus \theta(C_f, C_m) \; mod \; q.$$

Since θ is commutative and associative,

$$\theta(C_f, C_e) \equiv p.\theta(C_r, \theta(C_f, C_g)) \oplus \theta(C_f, C_g) \oplus \theta(C_f, C_m) \; mod \; q$$

and if $\theta(C_f, C_g) = 0$ is substituted, then the final form of the equation is

$$\theta(C_f, C_m) \; mod \; q. \tag{3}$$

If $\langle f, m \rangle = t \; mod \; q$ then

$$\theta(C_f, C_m) = \left[\begin{array}{cc} 0 & t \\ & t \\ \hline & \vdots \\ I & t \end{array}\right],$$

and so it follows from Equation (7.3) that the matrix C_m if it is added by the matrix $C_{\mathbf{m}} - \theta(C_f, C_m)$. Thus, the proof is completed. ⊠ □

Remark 7.3. *As the value $\theta(C_f, C_m)$ is chosen great, so the security of the system is high.*

Remark 7.4. *If the sets $\{x_i\}$ and $\{y_i\}$ are chosen as super increasing sequences, then the vectors x and y transform to a knapsack problem to find the matrix $\theta(C_f, C_m)$. Even though the secret key C_f is obtained, the algebraic power of the system is quitely high since it implies that the value $\theta(C_f, C_m)$ is researched by the knapsack method.*

Remark 7.5. *Since the product of two polynomials implies N^2 operations in the NTRU rings and the operation θ multiplies only N times on M_C, the proposed system is also superior as speed.*

Remark 7.6. *Since there exist infinite solutions to line equations in R^n and q of these solutions which are integers are in Z_q, the private key numbers C_f increase for $q \longrightarrow \infty$.*

A different NTRU encryption algorithm and digital signature are introduced by means of the following theorem.

Theorem 7.7. *The matrices S and S^{-1} can be found such that the sum of the matrices C_f and C_g assimilates to a companion matrix for the polynomials $f, g \in R_q$. That is, there exists a companion matrix $C \in Z_{n\times n}$ such that $C_f + C_g = SCS^{-1}$.*

Since Theorem 7.2 can be proved by the basic linear algebra information, its proof is not included here. The theorem is added to the NTRU system as follows.

Since the relevant companion matrices of the polynomials $m_1, m_2 \in R_p$ can be written as $C_{m_1} + C_{m_2} = S.C.S^{-1}$, C_f, C_g and C_r are constituted for $f, g, r \in R_q$, and it is packaged and sent by a public key $C_f^{-1}.C_g$ and a secret key C_f by encrypting as

$$e \equiv p.C_f^{-1}.C_g.C_r + C_f^{-1}.(S.C.S^{-1})\ mod\ q.$$

Theorem 7.8. *The messages m_1 and m_2 are probabilistically decrypted from an equation*

$$e \quad \equiv \quad p.C_f^{-1}.C_g.C_r + C_f^{-1}.(S.C.S^{-1})\ mod\ q \tag{4}$$

such that C_f is invertible for two polynomials m_1 and m_2 in the ring R_p.

Proof. If Equation (7.4) is multiplied from left by C_f, then it follows that

$$C_f.e \equiv p.C_g.C_r + (S.C.S^{-1})\ mod\ q.$$

Hence,

$$C_f.e \equiv S.C.S^{-1}\ mod\ p$$

is obtained if it is calculated in *mod p*. Since $S.C.S^{-1} = C_{t_1} + C_{t_2}$ is written for $t_1, t_2 \in Z_p$, the receiver can obtain that the correct probability is $C_{m_1} + C_{m_2}$. ⊠ □

Now, an another variation of Theorem 7.3 is presented as a digital signature.

Theorem 7.9. *Let $f \in R_q$ and C_f be chosen such that it is commutative with $S.C.S^{-1}$. A public key $S^{-1}.C_f = C_h$ and a encryption method*

$$e \equiv p.C_r + S.C_f^{-1}.S.C\ mod\ q$$

can be applied as a digital signature.

Proof. Let it be stated the existence of many f which are commutative with $S.C.S^{-1}$. Since

$$A.f(A) = f(a).A$$

where f is any polynomial for an arbitrary matrix $A \in Z_{n\times n\times}$, the existence of many f is exact.

If the result e is multiplied from right by $h = S^{-1}.C_f$, then

$$e.h \equiv p.C_r.S^{-1}.C_f + [S.C_f^{-1}.S.C].S^{-1}.C_f\ mod\ q$$

is obtained. Since the matrix multiplication is associative and C_f is commutative with $S.C.S^{-1}$,

$$e.h \equiv p.C_r.S^{-1}.C_f + S.(C_f.C_f^{-1}).(S.C.S^{-1})\ mod\ q$$

is reached. If it is calculated in *mod p*, then it follows

$$e.h \equiv S.(C_{m_1} + C_{m_2})\ mod\ p.$$

Thus, S is the message in the case that it is used as a secret key, and S can be used as a signature in the case that the message is known. ⊠ □

8. 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 companion 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 new 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)