International Journal of Maps in Mathematics

*Volume **4**, Issue **1**, 2021, Pages:**53-66***

ISSN: 2636-7467 (Online)

www.journalmim.com

A GENERALIZATION OF NTRU CRYPTOSYSTEM AND A NEW DIGITAL SIGNATURE VERSION

MEHMET SEVER AND AHMET ŞÜKRÜ ÖZDEMİR *

Abstract. In this study, it is made new generalizations by adding a security parameter "n" to NTRU cryptosystem. These generalizations are analyzed in three categories. The first category clarifies summative generalization, the second category explains a multiplicative generalization and the latest category expresses a dimension generalization, and the system is researched with greater sets and many choosings of parameters. As a result of all these evidences, it is stated that these generalization outputs creates a new NTRUSIGN.

Keywords: NTRU, NTRU cryptosystem, NTRUSIGN, cryptology, (digital) signature

2010 Mathematics Subject Classification: 11T71, 14G50, 94A60, 94A62.

1. Introduction

In 1996, NTRU was first introduced by J. Hoffstein, J. Pipher ve J. Silverman in Crypto' 96 [5]. Then NTRU's developers contributed to NTRU which is denoted as a ring-based and a public key encryption method by making parameter optimization [4]. In 2003, they introduced $NTRU_{SIGN}$ [9], i. e., a digital signature version of NTRU. In the same year, they with another team made a presentation which analyzed description errors of NTRU [21]. J. H. Silverman published a technical report about invertible polynomials in a ring in 2003 [13]. In 2005, J. H. Silverman and W. Whyte published a technical report which analyzed error probabilities in NTRU decryption [22]. Also, the founding team which published an article

Received:2020.05.22 *Revised:2020.09.24* *Accepted:2020.10.07*

* Corresponding author

Mehmet Sever; msever@agri.edu.tr; https://orcid.org/0000-0003-2967-1943

Ahmet Şükrü Özdemir; ahmet.ozdemir@marmara.edu.tr; https://orcid.org/0000-0002-0597-3093

.

on effects increasing security level of parameter choosing [11] has published related reports in the website www.ntru.com.

NTRU is quite 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 [20]. 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 quitely full-scale non-destructive attacks to the NTRU cryptosystem were originally made by Coppersmith et al. in 1997 [1]. Then new parameters which does away with effects of this attack were presented by Hoffstein et al. in 2003 [8].

As an another example of attack [14], 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 [15].

On behalf of detailed readings, it can be seen to [16, 17, 24] for different types of attacks types, and on the contrary, it can be seen to [12, 19, 3] for proposed new parameters and new system.

2. Motivation and Method

Hoffstein et al. introduced the first NTRU based digital signature in 2001 [18]. Then they gave a verification method for the NTRU cryptosystem in the same year [6]. The basic aim of these studies which present a digital signature and a verification method is to guarantee which there is no leakage into the system.

Even decoding a cryptological message falls short to state that you are an approved user of the system. Hence, solving a verification code or a reposted different text in the same way can co-opt you. It is clear in this age which the development of mobile payment methods and all business and government works are solved on the network that the discipline of digital signature is open for improvement. In this sense, the basic motivation of this study studies proposed in [7] and [23], and also the articles in [2, 25, 10] can be helpful on behalf of extra readings.

3. Aim and Scope

This study aims primarily to generalize the NTRU cryptosystem. This study which can be summarize as sending the sum, product or enhancing dimension of composed encoded texts by hiding a message with multi public keys and error polynomials purposes specially to avoid an attack on the plain text. It is obtained that the message is divided into parts with this method and also can be sent partially by showing that several two message can be sent in the generalization of enhancing dimension simultaneously.

Besides, this article explains the conditions that all these generalization offers can be used as a digital signature. If a new encoded text composed in the form of generalizations is sent just after previously partial encoded texts, the recipient is interpreted as a correct system user since s/he reads and obtains the message, and it can transform to a digital signature.

The most important output of this study is to enlarge still the NTRU cryptosystem against the developing quantum computers attacks and render to sheltering case.

4. NTRU Parameters

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

- N : it is 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 guaranteeing which *mod* q reductions works in perfect truth in the phase of decryption.

It can be seen [5] 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.

5. Algebraic background of NTRU

5.1. **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 $h_k = \sum_{i+j \equiv k \ mod \ N} f_i \cdot g_i$ 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.

5.2. **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.

5.3. **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.

5.4. **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 $a \ mod \ q = e \star f mod q$.
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., $D(e) = m$.

6. Choosing Parameters of the New System

The proposed generalized system has used some parameters literally. That is, the choosings of the prime number p and q, the number N, the polynomials f, g, r etc. is the same as in the classical NTRU system. The only difference is that different polynomials f, g and r can be chosen for different public keys generation.

7. Using Notations in the New System

The same representations can be used under the same conditions and the same choosings by holding to all classical NTRU notations. It is only useful to introduce three notations $f^*_{(n)}$, $f^*_{(n,j)}$ and $f^{-1}_{(n)}$. $f^*_{(n)}$ consists of a convolution product of n chosen all secret keys where $f^*_{(n)} = f_1 \star f_2 \star ... \star f_n$. $f^*_{(n,j)} = f_1 \star f_2 \star ... \star f_{j-1} \star f_{j+1} \star ... \star f_n$ consists of a convolution product of all except the j. secret key. Let $f^{-1}_{(n)}$ denote an inverse of product of n unitary secret keys f on $mod \ p$.

8. How does the summative generalization system work?

This generalized system pre-encrypts differently a message by choosing n different public keys and n different error polynomials. The sum of these composed pre-encrypted texts is sent as a recent encrypted message. The number n is relatively prime p and q, respectively. However, there exist two different cases where the number n is greater and less than the

numbers p and q being modules. Thus, it leads to add a new parameter in the old classical system NTRU since it works as a security parameter of this system. Now, we show how the system works in the case $n < p$, $n < q$ and $(n, p) = 1$, $(n, q) = 1$. We consider initially this system in the classical NTRU rings as $Z_p[x]/(x^N - 1)$ and $Z_q[x]/(x^N - 1)$. Then it is reconsidered by taking a field instead of a ring.

Lemma 8.1. *A message polynomial m is encrypted n times by choosings of a public key $h_i = f_{iq}^{-1} \star g_i$ and an error polynomial r_i, $1 \leq i \leq n$ according to the classical method of the NTRU cryptosystem and then the plain text m can be achieved in the case which the sum of composed encrypted texts e_i $1 \leq i \leq n$ is sent.*

Proof. Let the encrypted forms of messages m be written and summed obviously and one under the other. We have

$$\begin{array}{rcl} e_1 & = & ph_1 \star r_1 + m \ (mod\ q) \\ e_2 & = & ph_2 \star r_2 + m \ (mod\ q) \\ : & & : \\ +\quad e_n & = & ph_n \star r_n + m \ (mod\ q) \\ \hline e_1 + e_2 + ... + e_n & = & p[(h_1 \star r_1) + (h_2 \star r_2) + ... + (h_n \star r_n)] + nm \ (mod\ q). \end{array} \tag{8.1}$$

Now, we obtain

$$\begin{array}{rcl} f_{(n)}^*(e_1 + e_2 + ... + e_n) & = & p[(f_{(n,1)}^* \star g_1 \star r_1) + (f_{(n,2)}^* \star g_2 \star r_2) + ... \\ & & +(f_{(n,n)}^* \star g_n \star r_n)] + f_{(n)}^* \star nm \ (mod\ q) \end{array} \tag{8.2}$$

by applying the product of each unitary polynomial f_i, $1 \leq i \leq n$ to Equation (8.1). Since $f_{(n)}^*$ consists of the product of the invertible secret keys f and this product is invertible in the statement (8.2), both sides of the equation is multiplied by $f_{(n)}^{-1}$ and then the message nm should not impressed by these values if we consider the equation in *mod p* instead of *mod q*. So,

$$e_1 + e_2 + ... + e_n = nm \ (mod\ p).$$

Since an user knows the security parameter n into the system, he knows that taken message is m or the message nm being its $n-$fold by the notion in the form

$$e_1 + e_2 + ... + e_n = \underbrace{m + m + ... + m}_{n} \ (mod\ p).$$

This case goes into the probabilistic cryptology. That is, it is based on the assumption that an user of the system can exit the intricate situation. Now, let us give a certain decryption method by means of fields.

Lemma 8.2. *Let p and q be prime numbers, and let M and S be two $N-$order irreducible polynomials in $F_p[x]$ and $F_q[x]$. Then the system proposal given in Lemma 8.1 works in the fields $F_p[x]/(M)$ and $F_q[x]/(S)$ non-probabilistically.*

Proof. Let us remind that the polynomials f, g, r and m can be only chosen in $F_p[x]/(M)$ or $F_q[x]/(S)$ such that all conditions in Lemma 8.1 remain the same. Similarly, let the polynomial m be encrypted by n different public keys h and n different error polynomials r, and whole encrypted text be divided by n and be sent. Let the statement (8.1) in Lemma 8.1 be divided by n, and let

$$\begin{aligned} a &= \frac{e_1 + e_2 + ... + e_n}{n} \\ &= p.\frac{1}{n}[(h_1 \star r_1) + (h_2 \star r_2) + ... + (h_n \star r_n)] + m \ (mod\ q) \end{aligned}$$

be sent as a encrypted text. If the polynomial a is first multiplied by $f^*_{(n)}$ and then $f^{-1}_{(n)}$, and the current statement calculate in *mod* p, the system works non-probabilistically as

$$\frac{e_1 + e_2 + ... + e_n}{n} = m \ (mod\ p).$$

Now, we state how the system works in the case $q > n > p$ and $(p, n) = 1$.

Lemma 8.3. *All conditions in Lemma 8.1 remain the same, and the system works with small probability part in the case $q > n > p$ and $(p, n) = 1$.*

Proof. To avoid writing repetition, we skip the steps of decryption in Lemma 8.1 and consider the last step as follows:

$$e_1 + e_2 + ... + e_n = nm \ (mod\ p). \tag{8.3}$$

When $n < q$, we reach to *mod* p without changing. But, there exist $k, l \in Z$ such that $n = kp + l$ when $n > p$. Then Equation (8.3) becomes

$$e_1 + e_2 + ... + e_n = lm \ (mod\ p).$$

When $l < n$ in the last situation, a probabilistic decryption should be done. That is, taken message can be only m, lm or nm. Since the user of the system knows parameters n, p, q, he chooses an appropriate text from the set $\{m, lm, nm\}$.

Proposition 8.1. *The system works with the probability 4 since there is a possibility of multiplying by a as a result of b mod p from $n = aq + b$ in addition to the operations in Lemma 8.3 in the case $n > q > p$.*

9. Multiplicative Generalization

We clarify a method that a message encrypts n times and then the product of recent composed encrypted polynomials is sent as an encrypted text. The choosings and operations of summative generalization told in the first chapter remain the same, and let's encrypt a message m in n different forms. Let all pre-encrypted texts m be written and multiplied one under the other. We specify that it is helpful choosing the prime p large enough so that the residue classes does not constitute a complex situation.

9.1. **How does the system work?**

$$\begin{array}{lcl} e_1 & = & ph_1 \star r_1 + m \ (mod\ q) \\ e_2 & = & ph_2 \star r_2 + m \ (mod\ q) \\ : & & : \\ \star \quad e_n & = & ph_n \star r_n + m \ (mod\ q) \\ \hline e_1 \star e_2 \star ... \star e_n & = & p^n(h_1 \star h_2 \star ... \star h_n) \star (r_1 \star r_2 \star ... \star r_n) \star p[H \star R] \star m \\ & & +m^n \ (mod\ q) \end{array} \tag{9.4}$$

where $H \star R$ is a short result of the convolution product of h_i and r_i. In the decryption phase, a symbolic result is only written since its inverse need not to be calculated and is zeroized in mod p. If Equation (9.4) is multiplied by $f^*_{(n)}$ and $f^{-1}_{(n)}$ as in Lemma 8.1, respectively, and the result is calculated in *mod p*, then we have an equation

$$e_1 \star e_2 \star ... \star e_n = m^n \ (mod\ p).$$

If m^n $(mod\ p)$ is chosen in the form that need not to be the reduction, then

$$e_1 \star e_2 \star ... \star e_n = m^n \tag{9.5}$$

is possible. Equation (9.5) reached in the latest phase proposes us a two probability decryption:

(1) The message is only m. That is, m becomes known by means of the security parameter n in a polynomial m^n.
(2) Or the message is already m^n.

Now, we give the nonprobability working situation of the system.

Lemma 9.1. *If all conditions and choosings are done as in the previous chapter, we consider Equation (9.4). The system works non probabilistically in the case that* $[e_1 \star e_2 \star ... \star e_n]^n$ *is sent as a encrypted text by exponentiating* $n-th$ *power of the polynomial* $e_1 \star e_2 \star ... \star e_n$ *instead of* $e_1 \star e_2 \star ... \star e_n$.

Proof. When the $n-$th power of the encrypted text is exponentiated in the statement (9.4) and is sent in the form

$$[e_1 \star e_2 \star ... \star e_n]^n,$$

if all decryption steps are done appropriately then an equation

$$(e_1 \star e_2 \star ... \star e_n)^n = m^n \ mod \ p$$

consists of instead of the statement (9.5) so that the message becomes directly known in the form

$$e_1 \star e_2 \star ... \star e_n = m$$

when p is chosen as a sufficiently large parameter.

10. Coordinate Generalization and Enhancing dimension

When a NTRU cryptographic operation is made in a ring $R = Z[x]/(x^N - 1)$, a different public key h_2 can be generated by choosing an error polynomial $r_2 \in R$ from a generated public key h_1. The first cryptographic operation is made in the form which $e_1 = h_1 \star r_1 + m \ (mod \ q)$ if $h_1 = pf_q^{-1} \star g$ for $f, g \in R$. The same message (it can be different) can be hidden in the form $e_2 = h_2 \star r_2 + m$ by means of an another public key produced by $h_2 = h_1 \star r_1 + r_2$ for an arbitrarily chosen $r_2 \in R$. In the latest case, (h_1, h_2) is a public key, (e_1, e_2) is a encrypted text and (f, g) is a secret key where the choosings of f and g is as in the classical NTRU operations. The message that wishes sent can be (m, m) or (m_1, m_2). It is worth noting that all polynomials are the same degree. If they are not, an appropriate monomial with 0 coefficient must be added. To explain the algebraic structure on which this new proposed system is constructed, it is clear that a mapping

$$\theta : R = Z[x]/(x^N - 1) \longrightarrow Z^N$$

defined by

$$\theta(a) = (a_0, a_1, ..., a_{N-1})$$

is a homeomorphism for $a(x) = a_0 + a_1x + ... + a_{N-1}x^{N-1} \in R$. We define a mapping μ by means of the mapping θ.

$$\mu : R \times R \longrightarrow Z^N \times Z^N, \qquad \mu((a,b)) = (\theta(a), \theta(b))$$

under the operations $(a,b) \oplus (c,d) = (a+c, b+d)$, $(a,b) \odot (c,d) = (a \star c, b \star d)$ for a, b, c and $d \in R$, i.e., we define by

$$\mu((a,b)) = ((a_0, a_1, ..., a_{N-1}), (b_0, b_1, ..., b_{N-1})).$$

It can be seen easily that the operations $\oplus$ and $\odot$ are well-defined. μ is a homeomorphism since

$$\begin{aligned} \mu((a,b) \oplus (c,d)) &= \mu((a+c, b+d)) \\ &= (\theta(a+c), \theta(b+d)) \\ &= (\theta(a) + \theta(c), \theta(b) + \theta(d)) \\ &= (\theta(a), \theta(b)) + (\theta(c), \theta(d)) \\ &= \mu((a,b)) + \mu((c,d)) \end{aligned}$$

and

$$\begin{aligned} \mu((a,b) \odot (c,d)) &= \mu((a \star c, b \star d)) \\ &= (\theta(a \star c), \theta(b \star d)) \\ &= (\theta(a) \star \theta(c), \theta(b) \star \theta(d)) \\ &= (\theta(a), \theta(b)) \star (\theta(c), \theta(d)) \\ &= \mu((a,b)) \star \mu((c,d)) \end{aligned}$$

so that it is shown that μ is a homeomorphism. More clearly, it is written by the laws

$$\begin{aligned} (f,g) \oplus (f',g') &= (f+f', g+g') \\ (f,g) \odot (f',g') &= (f \star f', g \star g') \end{aligned}$$

in $R \times R$ for the operations $f, f', g, g' \in R$. Since the ring R can be embedding into $R \times R$ by $f \mapsto (1,f), (1,f) \in R \times R$ is used for all $f \in R$. Then it is possible that the element $(1,f)$ is invertible since $f \in R$ is invertible. That is, if $f \star f' \equiv 1 \ mod\ p$ for $f \in R$ then $(1,f) \odot (1,f') = (1,1)$ so that $(1,1)$ is a unit element of $R \times R$.

After all these details and explanations, we present a NTRU on this structure. Let $f, g, r_i \in R$ be determined according to the classical NTRU methodology. Let a message (m_1, m_2) be sent for the message polynomials $m_1, m_2 \in R$. A vector $(e_1, e_2) \in R \times R \cong Z^{2N}$ constituted by the polynomials e_1 and e_2 which are determined by the pre-encryptions

$$e_1 = pf_q^{-1} \star g \star r_1 + m_1 \ (mod\ q)$$

$$e_2 = ph_2 + m_2 \ (mod\ q)$$

is sent where $h_1 = pf_q^{-1} \star g$ and $h_2 = ph_1 \star r_1 + r_2 \ (mod\ q)$ are two public keys. (f, f) and (f_p, f_p) represent secret keys and (r_1, r_2) represents error vectors of the new proposed system where (h_1, h_2) is a public key and f_p is an inverse of f in $mod\ p$. Since the arbitrarily choosings of g generate many secret keys, it is stated that the keys (f, f) and (f_p, f_p) is only sufficient for the system.

10.1. **How does the system work?** The receiver opens the vector (e_1, e_2) by means of secret keys (f, f) and (f_p, f_p) as follow.

$$\begin{aligned} (e_1, e_2) \odot (f, f) &= (e_1 \star f, e_2 \star f) \ (mod\ q) \\ &= (p \star g \star r_1 + f \star m_1, p^2 \star g \star r_1 + pr_2 \star f + f \star m_2) \ (mod\ q) \\ &= (f \star m_1, f \star m_2) \ (mod\ p). \end{aligned} \tag{10.6}$$

If the statement (10.6) is multiplied by (f_p, f_p), then $(f_p, f_p) \odot (e_1, e_2) \odot (f, f) = (m_1, m_2)\ mod\, p$ and the decryption result becomes directly known the message.

10.2. **Advantages of the system.**

- The receiver uses two public keys such as h_1 and h_2. Hence, even if a key is obtained, the other is not obtained easily.
- A larger message such as (m_1, m_2) is sent in a lump instead of a message m.
- On the constituted system is on $Z^{2N} \cong Z^N \times Z^N$, NTRU is more sheltering according to the ring $Z^N \cong R = Z[x]/(x^N - 1)$.
- If $f \in R$ is a private key, then $(f, f) \in R \times R$ is a private key so that no extra search operation and time are needed.

10.3. **Disadvantage of the system.** Although involving multiple operations and producing multiple secret keys tighten the security, it leads to a regression in time and effort capacity.

11. NTRU Digital Signatures

It is understood that if the messages e_i, $1 \leq i \leq n$ are sent to the receiver and are correctly read by the receiver, then there is not infiltration into the system and this receiver is the right person in summative generalization method given in the first chapter as follow:

If you decode the codes $e_1, e_2, ..., e_n$, you must also decode the code $e_1 + e_2 + ... + e_n$, thus you prove that you are a confidential user! If the receiver also decodes this summative code, then he digitally signs. Similarly, the multiplicative generalization method is also used

as a digital signature and finally sending related codes (e_1, e_2) in an upper dimension, i.e., working in $R \times R$ instead of R can be used as a new digital signature method. e_1 and e_2 are sent in this method and it is expected that the receiver decodes finally the text (e_1, e_2). Its another decipherment acts as a digital signature. Enlarging dimension can remove to the set

$$R^N = \underbrace{R \times R \times ... \times R}_{N}$$

easily. Thus, it is understood that the receiver is the right user when the code $(e_1, e_2, ..., e_n)$ is read.

It is shown that the conducted system generalizations can be worked as a digital signature and a verification method. If a generalization parameter "n" is chosen as $n = p_1 q_1$ for a multiplicative generalization, then the top step of the decryption phase of the system is reduced to solve the RSA problem. It is shown how the proposed generalization systems are based on a strong foundation. That is, the reached final phase is

$$e \equiv m^{p_1 q_1} \qquad (mod\ q)$$

when NTRU decryption steps are applied properly.

A digital signature

$$D^n_{NTRUSIGN} : m \longmapsto (m, \sum e_i), \qquad 1 \leq i \leq n$$

is defined by means of a mapping

$$D^i_{NTRUEncrypt} : (m, r_i, h_i) \longmapsto e_i, \qquad 1 \leq i \leq n$$

where all of the parameters are chosen as introduced in the classical NTRU cryptosystem, and a verification of this signature is defined by

$$D_{verification} : \sum e_i \longmapsto (m, n, n\ mod\ q), \qquad 1 \leq i \leq n$$

and a new NTRU based digital signature is obtained.

12. Conclusion and Recommendations

The basic output of this study is to make a production of NTRU on more comprehensive structure. In this sense, the obtained datas enlarged the system and proposed to constitute the system on large sets for choosings of extra public keys, error polynomials. However, this proposals supporting security, effectiveness and sheltering necessitate the devices which contain a larger processor and more comprehensive memory as a result of many operations

and choosings of key from a larger set. It is obvious that the speed is affected negatively but effectiveness increases by enhancing an usage area and intended use effectiveness increase under existing conditions. These proposals which can be used as a new digital signature method can be affirmed practically. The Cryptoanalysis of a new NTRU generalized system can be done by trying attacks and analyzing new lattice structures corresponding to all these generalizations. Since the main sending message which is constituted in the form of a sum or product of encrypted messages consisting of during the sending of the same message can mean n messages, it can be developed as a probabilistically encryption method. In addition to this, sending different messages in the same time according to this method means sending a huge message in different parts by choosing a larger parameter p so that it is important to preserve the plain text.

References

[1] D. Coppersmith and A. Shamir, Lattice attacks on NTRU, Euro-crypto'97, Lecture Notes in Computer Science, Vol. 1233, Springer, Berlin, (1997).

[2] Elbasheer, M. O., Mohammed, T. (2015, April). Signing and verifying certificates by NTRU and RSA algorithms. In 2015 International Conference on Cloud Computing (ICCC) (pp. 1-4). IEEE.

[3] Gentry, C., Szydlo, M. (2002, April). Cryptanalysis of the revised NTRU signature scheme. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 299-320). Springer, Berlin, Heidelberg.

[4] Hoffstein, J., Silverman, J. (1971). Optimizations for NTRU. Public-Key Cryptography and Computational Number Theory, De Gruyter Proceedings in Mathematics, 77-88.

[5] Hoffstein, J., Pipher, J., Silverman, J. H. (1998, June). NTRU: A ring-based public key cryptosystem. In International Algorithmic Number Theory Symposium (pp. 267-288). Springer, Berlin, Heidelberg.

[6] Hoffstein, J., Pipher, J., Silverman, J. H. (2001, May). NSS: An NTRU lattice-based signature scheme. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 211-228). Springer, Berlin, Heidelberg.

[7] Hoffstein, J., Pipher, J., Silverman, J. H. (2001). Enhanced encoding and verification methods for the NTRU signature scheme. Previously posted on http://www. ntru. com/technology/tech. technical. htm.

[8] Hoffstein, J.,Silverman, J. H. and Whyte, W.(2003). Estimating breaking times for NTRU lattices, Technical Report 12. Available at http://www.ntru.com.

[9] Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J. H., Whyte, W. (2003, April). NTRUSIGN: Digital signatures using the NTRU lattice. In Cryptographers' track at the RSA conference (pp. 122-140). Springer, Berlin, Heidelberg.

[10] Hoffstein, J., Pipher, J., Schanck, J. M., Silverman, J. H., Whyte, W. (2014, October). Transcript secure signatures based on modular lattices. In International Workshop on Post-Quantum Cryptography (pp. 142-159). Springer, Cham.

[11] Hoffstein, J., Pipher, J., Schanck, J. M., Silverman, J. H., Whyte, W., Zhang, Z. (2015). Choosing parameters for NTRU encrypt. NTRU Challenge . Available at http://www.ntru.com/ntru-challenge.

[12] Hong, J., Han, J. W., Kwon, D., Han, D. (2002). Chosen-Ciphertext Attacks on Optimized NTRU. http.

[13] Howgrave-Graham, N., Nguyen, P. Q., Pointcheval, D., Proos, J., Silverman, J. H., Singer, A., Whyte, W. (2003, August). The impact of decryption failures on the security of NTRU encryption. In Annual International Cryptology Conference (pp. 226-246). Springer, Berlin, Heidelberg.

[14] Howgrave-Graham, N., Silverman, J. H., Whyte, W. (2003). A Meet-in-the-Middle Attack on an NTRU Private key (Vol. 4). Technical report, NTRU Cryptosystems, June 2003. Report. Available at http://www.ntru.com.

[15] Howgrave-Graham, N., Silverman, J. H., Singer, A., Whyte, W., Cryptosystems, N. T. R. U. (2003). NAEP: Provable Security in the Presence of Decryption Failures. IACR Cryptol. ePrint Arch., 2003, 172.

[16] Howgrave-Graham, N., Silverman, J. H., Whyte, W. (2005, February). Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3. In Cryptographers' Track at the RSA Conference (pp. 118-135). Springer, Berlin, Heidelberg.

[17] Meskanen, T., Renvall, A. (2003). A Wrap Error Attack against NTRUEncrypt. Turku Centre for Computer Science.

[18] Näslund, M., Shparlinski, I. E., Whyte, W. (2003, January). On the bit security of NTRUEncrypt. In International Workshop on Public Key Cryptography (pp. 62-70). Springer, Berlin, Heidelberg.

[19] Nguyen, P. Q., Pointcheval, D. (2002, August). Analysis and improvements of NTRU encryption paddings. In Annual International Cryptology Conference (pp. 210-225). Springer, Berlin, Heidelberg.

[20] Nitaj, A. (2015). The Mathematics of the NTRU Public Key Cryptosystem. Mathematical Concepts IGI Global.

[21] Silverman, J. H.(2003). Invisibility truncated polynomial rings. Technical Report . NTRU Cryptosystems, Available at http://www.ntru.com.

[22] Silverman, J. H., Whyte, W. (2005). Estimating decryption failure probabilities for NTRU encrypt, Technical Report 18 . Available at http://www.ntru.com.

[23] Park, S. W., Lee, I. Y. (2013). Anonymous authentication scheme based on NTRU for the protection of payment information in NFC mobile environment. Journal of Information Processing Systems, 9(3), 461-476.

[24] Proos, J. (2003). Imperfect decryption and an attack on the NTRU encryption scheme. Faculty of Mathematics, University of Waterloo.

[25] Yu-Pu, H. U. (2008). A novel NTRU-class digital signature scheme [J]. Chinese Journal of Computers, 31(9), 1661-1666.

Department of Mathematics, Faculty of Arts and Sciences, Ağri İbrahim Çeçen University, Ağri-Turkey

Department of Mathematics and Science Education, Ataturk Faculty of Education, Marmara University, Istanbul-Turkey