UDC 004.056.55

NTRU PRIME IIT UKRAINE ENCRYPTION ALGORITHM WITH CONSIDERATION KNOWN ATTACKS ANALYSIS

Ivan Gorbenko[1], Olena Kachko[2], Maryna Yesina[1]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, rinayes20@gmail.com
[2] JSC «Institute of Information Technologies», Kharkiv, Kharkiv National University of Radio Electronics, Nauka Ave., 14, Kharkov, 61022, Ukraine
kachko@iit.com.ua, iit@iit.kharkov.ua

Reviewer: Roman Oliynikov, Doctor of Sciences (Engineering), Full Professor, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
roliynykov@gmail.com

Received on November 2017

Abstract: *The paper deals with the modern cryptographic transformations of the asymmetric end-to-end encryption type, namely – NTRU-like cryptographic systems. A new cryptographic system NTRU Prime IIT Ukraine was created based on existing cryptographic transformations of this type (cryptographic algorithms NTRU (ANSI X9.98-2010) and NTRU Prime). A brief description of this cryptographic system is given and an analysis of its resistance to known attacks is made. At the end of the work, conclusions are made and recommendations on the features, advantages and possibilities of using the new cryptographic asymmetric algorithm of end-to-end encryption NTRU Prime IIT Ukraine are given.*

Keywords: *NTRU Prime, Attack, Ring, End-to-End Encryption, Field, Quotient Ring.*

1 Introduction

In 2016-2017 there were the series of important events, that have significantly affected to the intensive development of post-quantum cryptography. To them should be referred the statement on the Internet – Alfred J. Menezes and Neal Koblitz article [2], organization and conduction by NSA and NIST USA VII international conference on post quantum cryptography [5, 6]. An extremely important event was the publication in the USA report «Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT)» [3], in which fully confirmed the possibility of electronic signature (ES) asymmetric cryptographic primitives successful quantum cryptanalysis and the main problems and opportunities, and stages of their decision are identified.

NIST USA announced a competition to develop the standards of post-quantum asymmetric cryptographic primitives [5], understanding the need to find new electronic signature and asymmetric encryption type cryptographic transformation, which will be relevant and can be applied in post-quantum period. The specified one due to two factors. First, there is significant progress in the development of quantum computers, including experimental demonstration of physical qubits realization are carried out, which can be scaled up to larger systems. A confirmation of this is the successive announcement of IBM 20, 50 and 53 qubits quantum computers [26,27].

Second, likely transition to post-quantum cryptography will not be easy, because it is unlikely to be a simple replacement of the current asymmetric cryptographic primitives standards. Significant efforts will be needed to develop, standardize and implement a new post-quantum cryptosystems. Therefore, should be a significant transition stage, when as current and post-quantum cryptographic primitives are used.

Applications were received by NIST until November 30, 2017. They relate to: asymmetric encryption algorithms and ES. Subsequently, their detailed analysis and comparison is expected, with a period of up to 3 years. This indicates the significant complexity of the problem to be solved.

The European Union has also started the preparation of a new post-quantum standards. A new direction "Quantum-Safe Cryptography" are formed by European Organization for Standardization

ETSI in the cluster "Security" [1,4,7]. According to the results of these studies are predicted the groups standards for post-quantum period adoption. ETSI has published a group report "Quantum-Safe Cryptography. Quantum-Secure infrastructure" [1], in which fixed bases of perspective infrastructure, provided algorithms, described primitives types, that will be used. Separately requirements are nominated and estimation criteria are formed for future candidates.

With the participation of the authors of this article for the NIST USA competition, a cryptographic algorithm for NTRU Prime IIT Ukraine [10], developed using NTRU [8] and NTRU Prime [9], was presented. The objective of this paper is a general overview and description of the proposed cryptographic transformation, implementation specificity, estimation and comparison of the main characteristics and indicators from [8-10] according to cryptographic stability criteria from existing and potentially possible attacks.

2 Problem formulation

On the basis of the analysis of a number of sources [8, 9] concerning the existing encryption algorithms, their features, advantages and disadvantages, as well as resistance to attacks, it was determined that on their basis it is possible to create a new encryption algorithm, which will combine the main advantages of existing ones and will not have certain disadvantages. As a result of extensive research, the essence of the candidate was substantiated, its implementations, wich has the advantages of relatively well-known were developed, made tests and estimations of the main characteristics. In November 2017 a full set of project descriptions and program implementations were sent and received by NIST USA [5]. It is considered necessary to consider the article as the first stage of the preliminary study of our proposal and to familiarize the general public with the problem of creating a post-quantum standard of asymmetric encryption. Thus, the objective of this paper is to justify and outline the main ideas for constructing a post-quantum standard of asymmetric encryption, to analyze the state of work in the indicated direction, to indicate the essence of the difference between the «NTRU Prime IIT Ukraine» proposal and known ones, and to discuss the results of the estimation and testing in relation to requirements imposed by NIST USA.

An analysis of the requirements for post-quantum cryptographic transformations of asymmetric encryption allows us to conclude that the main, and unconditional requirement for «NTRU Prime IIT Ukraine», is the requirement of cryptographic stability regarding known and potentially possible attacks. The specified attacks can be implemented using both classical attacks based on the use of classical computer systems and classical mathematical methods, as well as on the basis of quantum computers and corresponding mathematical and software methods.

Obviously, that cryptographic asymmetric transformations should provide protection from both classical and quantum cryptanalysis methods. The above should be taken into account, if possible, during the construction and analysis of post-quantum cryptographic transformations in general, and the adoption of post-quantum standards of asymmetric cryptographic transformations on their basis.

3 Description and analysis of general parameters of modern NTRU-like encryption algorithms

Let's consider the existing today encryption algorithms and created on their basis a new encryption algorithm «NTRU Prime IIT Ukraine» [8-10].

Analysis of NTRU encryption algorithm. NTRU – the first public key cryptosystem not based on factorization or discrete logarithmic problem. NTRU is based on the shortest vector problem in a lattice. Operations are based on objects in a truncated polynomial ring $R = \mathbf{Z}[x]/(x^n - 1)$, polynomial degree at most $n-1$.

NTRU parameters are as follows: n – the polynomials in the ring R have degree $n-1$ (non-secret); q – the large modulus to which each coefficient is reduced (non-secret); p – the small modulus to which each coefficient is reduced (non-secret); f – a polynomial that is the private key; g – a polynomial that is used to generate the public key h from f (secret but discarded after ini-

tial use); h – the public key, also a polynomial; r – the random "blinding" polynomial (secret but discarded after initial use); d – coefficient.

The encryption of message m is carried out according to the formula $c = rh + m$.

Decryption is performed as follows: using a private polynomial f it is calculated polynomial $a = f \cdot e (\mathrm{mod}\, q)$. Then the polynomial $b = a \bmod p$ is calculated. Another private polynomial f_p is used to compute $c = f_p \cdot b (\mathrm{mod}\, p)$, where c is an output message m.

More details about the NTRU algorithm is described in [8].

4 Analysis of NTRU Prime encryption algorithm

The NTRU Prime cryptosystem is proposed as one of the alternative variants of the asymmetric NTRU method in order to get rid of the weaknesses inherent in NTRU, which are associated with undesirable structural properties of the ring $\mathbf{Z}_q[x]/(x^n - 1)$: in many cases, a ring of this type has a subrings and a factor-rings of a high order. Unlike NTRU, NTRU Prime uses a ring $\mathbf{Z}_q[x]/(x^n - x - 1)$, which provided that the proper selection of numbers q and n, is a field, that does not contain its own subfields. In addition, the Galois group of polynomial $x^n - x - 1$ over the field Q is a symmetric group S_n, which excludes the possibility of attacking a certain type on the cryptosystem.

In NTRU Prime, the public key is calculated by the formula $h = g/3f$ that it matters to create an effective secret key transfer protocol. However, to construct an asymmetric encryption system, it is desirable to use the traditional formula $h = 3g/f$.

The decryption of messages in the cryptosystem NTRU Prime occurs correctly on condition $q > 48t$.

Details about the NTRU Prime algorithm is described in [9].

5 Analysis of NTRU Prime IIT Ukraine encryption algorithm

The given asymmetric encryption scheme is a modification of the NTRU scheme, and differs from the latter only in two aspects:

1. Instead of the ring $\mathbf{Z}_q[x]/(x^n - 1)$ used in NTRU, a field $\mathbf{Z}_q[x]/(x^n - x - 1)$ is used, as in the NTRU Prime cryptosystem [9]. According to [9], this prevents cryptosystem attacks of some kind and precludes the use of (at least potentially) weaknesses of the standard NTRU cryptosystem that are associated with the existence of non-trivial subrings or truncated rings of ring $\mathbf{Z}_q[x]/(x^n - 1)$.

2. In the proposed scheme, polynomials F and r are arbitrary t-small, that is, they have $2t$ non-zero coefficients equal to ± 1, whereas in [8] each of these polynomials has exactly t nonzero coefficients equal to 1 and -1 correspondingly. A similar remark is also valid for a polynomial g, which is an arbitrary small polynomial in a modified cryptosystem and has the same number of non-zero coefficients, which are equal 1 and -1 in NTRU. This difference is not significant, however, it provides the opportunity to expand the amount of key space in comparison with NTRU without losing the effectiveness of algorithms implementation for key generation and messages encryption-decryption.

In this algorithm, the secret key is any pair of polynomials (f, g), where $f = (1 + 3F) \bmod q$, $F, g \in R/3$, $\| F \|_1 = 2t$, and the corresponding public key is a polynomial $h = 3g/f \in R/q$.

Encryption of the message m is carried out according to the formula $c = m + rh$, where r – the random equal probability t-small polynomial, h – public key, and the addition and multiplication are carried out in the field R/q.

To retrieve a message m by message c using a secret key (f,g), we must calculate $m' = (cf \pmod q) \bmod 3$ and put $m'' = (m' f^*) \bmod 3$. That is, only polynomials f and f^* are used to decrypt messages, where f^* there is an inverse to an element $f \bmod 3$ in the ring $R/3$.

In «NTRU Prime IIT Ukraine» using the appropriate estimates as specified in the description of the algorithm, can (it is allowed) to significantly weaken the condition for decryption of messages in comparison with NTRU Prime, namely, to replace it with a condition $q > 32t$. This, in turn, allows you to reduce the value q compared to NTRU Prime, while maintaining the decryption correct. More details about the «NTRU Prime IIT Ukraine» algorithm is described in [10].

6 Analysis of algorithm taking into account known attacks on «NTRU Prime IIT Ukraine»

Let's analyze the stability of the encryption algorithm «NTRU Prime IIT Ukraine» [10] for known attacks.

Meet-in-the-middle

It should be noted that this attack is currently being implemented on ordinary computers, but without language, it is possible to implement it on quantum computers.

The task of recovery the secret key $(f = (1+3F) \bmod q, g)$ by the public key h of the cryptosystem is reduced to solving the equation $(h' + Fh') \bmod q = g$ for unknown $F, g \in R/3$, where $\| f \|_1 = 2t$ and $h' = (3^{-1} h) \bmod q$. This problem can be formulated in such way.

Let $\Phi = \{F \in R : \| F \|_\infty = 1, \| F \|_1 = 2t\}$. We must find a polynomial $F \in \Phi$ such that

$$\| (h' + h'F) \bmod q \|_\infty = 1. \quad (1)$$

The complexity of solving the task by enumeration of all polynomials $F \in \Phi$ requires $|\Phi| = 4^t \binom{n}{2t}$ operations. To reduce the complexity you can apply attacks under the general name «meet in the middle». We describe the general scheme of conducting such attacks, based on the ideas of works [11,13,14].

We assign sets $\Phi_1, \Phi_2 \subseteq \mathbf{Z}^n$ such that each vector $F \in \Phi$ has a single representation in the form $F = F_1 + F_2$, where $F_1 \in \Phi_1$, $F_2 \in \Phi_2$, and a certain mapping $D : Z_q{}^n \to \{0,1\}^r$, where $r \le n$.

The algorithm for solving the equation (1) relative to the unknown $F \in \Phi$ consists of two stages, on the first of which the table is built, which consists of all pairs $(h'F_1 (\bmod q), D(h'F_1 (\bmod q)))$, located by non-growing integers corresponding to binary vectors $D(h'F_1 (\bmod q))$, where $F_1 \in \Phi_1$. Then, on the second stage, for each $F_2 \in \Phi_2$, the vector $D(-h' - h'F_2 (\bmod q))$ is searched for among the other pairs components that are in constructed table. The algorithm completes successfully in case of finding vectors $F_1 \in \Phi_1$, $F_2 \in \Phi_2$ such that $D(h'F_1 (\bmod q)) = D(-h' - h'F_2 (\bmod q))$ and $\| (h' + h'(F_1 + F_2)) \bmod q \|_\infty = 1$.

Note that in [9,11,13,14], for various variants of the NTRU cryptosystem, heuristic complexity estimates of meet in the middle attacks are presented based on explicit or implicit assumptions regarding the mapping D and distribution of vectors in a table, that is constructed on the first stage. Along with that, regardless of mapping D choice, the maximum complexity of the described algorithm is limited below by the value $|\Phi_1| + |\Phi_2| \ge 2\sqrt{|\Phi_1||\Phi_2|}$, which, in its turn, is at leas

$$\text{t } 2\sqrt{|\Phi|} = 2^{t+1} \binom{n}{2t}^{1/2}.$$

Thus, in order to ensure the resistance of cryptosystem «NTRU Prime IIT Ukraine», according to the meet-in-the-middle attacks, values n and t are selected for the given security parameter k, based on the condition

$$2^k \le 2^{t+1}\binom{n}{2t}^{1/2}. \quad (2)$$

Let's consider later the attacks in terms of their stability in the application of quantum algorithms [8, 20-24], and first consider the attack “meet-in-the-middle”.

Let B – the set of Boolean polynomials of degree N. Also let $B(d)$ – B subset, whose polynomial has d coefficients 1, and $N-d$ coefficients 0. $T(d+,d-)$ – the set of polynomials, where the number of coefficients 1 equals $d+$, and the number of coefficients –1 is equal $d-$, and the others are 0.

The “meeting-in-the-middle” attack allows cryptanalyst under certain conditions to calculate the user private key that is selected from space of 2^N elements in time $O\left(2^{N/2}\right)$. The proposed attack is implemented as follows [9]. The private keys space ($f=(1+pF) mod\ q$) f is divided into two large parts $f_1 \| f_2$, where f_1 and f_2 have a length $N/2$ of $d/2$ units each, whereby the same number of units is achieved by cyclic shift f when dividing into two parts. Under this condition, based on ($h = p(f_q^{-1} * g)\ mod\ q$), when $p = 2$, the condition is fulfilled:

$$f \cdot h = g (\mathrm{mod}\, q). \quad (3)$$

Substituting instead of f its representation in the form $f_1 \| f_2$ we have that

$$(f_1 \| f_2) \cdot h = g (\mathrm{mod}\, q). \quad (4)$$

Comparison (4) can be presented in the form

$$f_1 \cdot h = g - f_2 \cdot h (\mathrm{mod}\, q). \quad (5)$$

Finally, (5) can be presented in the form

$$(f_1 \cdot h)_i = \{1,0\} - (f_2 \cdot h)_i (\mathrm{mod}\, q) \forall i. \quad (6)$$

In fact for f the condition that half of the units fall into the first $N/2$ records can not be fulfilled. As shown in [23], there is at least one torsion f that will satisfy this property, and as a private key there will be any torsion f.

Under these conditions, the attack consists of the following steps.

1. A number k is determined that satisfies the condition

$$2^k \ge \binom{N/2}{d/2}. \quad (7)$$

Next, the memory is allocated to 2^k baskets for storing polynomials. Then the larger k will be chosen, than the faster the algorithm will run, but more memory will be required.

2. $N/2$ zeros are added to the polynomial f_1 and their selection is carried out. Browsing will take $\binom{N/2}{d/2}$ steps. Each value f_1 is written to the basket in such way that the number of the basket to which the polynomial will be placed is equal to the most significant bits of the first k coeffi-

cients $f \cdot h = g(\mathrm{mod}\, q)$. We will mark each basket as $label\_f_1$. In this case, in some baskets there will be several values of the polynomials.

3. Then the polynomials f_2 are sorted in the same way and the baskets $label\_f_2$ are formed, but zero bits are added to the beginning. The formed polynomial is placed in baskets whose number is formed as follows – the most significant bits for the first k polynomial coefficients $-f_2 * h(\mathrm{mod}\, q)$, as well as the most significant bits for the first k polynomial coefficients $-f_2 * h(\mathrm{mod}\, q)$ to each coefficient of which is added 1.

4. In the case if in the record f_2 a polynomial f_1 contains in the basket, it is considered a good candidate for recovery f. The cryptanalyst calculates $(f_1 \| f_2) \cdot h = g(\mathrm{mod}\, q)$. If it consists of $\{0,1\}$, then the private key is found.

Thus, in an attack with the use of the method "meet-in-the-middle" type it is established that this algorithm can always return the result, which is most likely a private key f, or a cyclic shift f.

According to [25], the temporal and spatial complexity of the "meet-in-the-middle" attack can be estimated as

$$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}}). \tag{8}$$

In general, (8) allows you to estimate the complexity of temporal and spatial attack on the algorithm NTRU. The above ratio can be used to compare the complexity of the "full disclosure" attack with attacks based on quantum algorithms.

Attack on the lattices

We note that this type of attack is implemented on ordinary computers, but in the future it can be implemented on quantum computers.

For any $h \in R/q$ we denote $L(h)$ the lattice in the vector space R^{2n+1} generated by the rows of the matrix

$$\begin{pmatrix} 1 & 0_{1\times n} & h' \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}, \tag{9}$$

where I_n – the unit matrix of order n, H – $n\times n$ matrix, whose i-th row is equal to the vector of polynomial coefficients $(x^i h) \bmod (x^n - x - 1)$, $i \in \overline{0, n-1}$, $h' = (3^{-1} h) \bmod q$, 3^{-1} – the of ring R/q element, reversed to 3:

$$3^{-1} = (5+q)/6, \text{ if } q \equiv 1 \bmod 3; \quad 3^{-1} = (5-q)/6, \text{ if } q \equiv -1 \bmod 3.$$

The following statement refines on (for the case of considered cryptosystem) the main result of work [15].

Statement 1. If the vector $(f = (1+3F) \bmod q, g)$ is the cryptosystem secret key, which corresponds to the public key h, then

$$(1, F, g) \in L(h) \tag{10}$$

and

$$\| (F, g) \|_2 = \left(\sum_{i=0}^{n-1} |F_i|^2 + \sum_{i=0}^{n-1} |g_i|^2 \right)^{1/2} \le \sqrt{n+2t}. \tag{11}$$

On the other hand, if the vector (F, g) satisfies (10) and has a length

$$\| (F,g) \|_2 < \frac{q-2}{12(\sqrt{n}+\sqrt{2t})}, \quad (12)$$

then with the help of the vector $f = (1+3F) \bmod q$ you can recovery any input message m by cryptogram $c = E_h(m,r)$, supposing that $m = (cf \,(\bmod q)) \bmod 3$.

Proof. The first part of the statement follows directly from the above definitions.

To prove the second part we consider the cryptogram $c = (m+rh) \bmod q$ received as a result of converting an input message $m \in R/3$ using the public key h and t-small polynomial r.

Based on condition (10), the equality $(3g) \bmod q = (fh) \bmod q$ is valid. Note that $f \neq 0$, because otherwise $F = 3^{-1}$, $g = 0$ $\| (F,g) \|_2 \geq \frac{q-5}{6} > \frac{q-2}{12(\sqrt{n}+\sqrt{2t})}$, because $q > 48$, which contradicts the condition (12).

Using the estimate ($\| uv \|_\infty \leq 2 \| u \|_\infty \| v \|_1$) and formula (12), we obtain that

$$\| mf + 3rg \|_\infty \leq \| m \|_\infty + 3(\| mF \|_\infty + \| rg \|_\infty) \leq 1 + 6(\| m \|_2 \| F \|_2 + \| g \|_2 \| r \|_2) \leq$$

$$\leq 1 + 6(\| m \|_2 + \| r \|_2) \| (F,g) \|_2 \leq 1 + 6(\sqrt{n}+\sqrt{2t}) \| (F,g) \|_2 < q/2.$$

It follows that $(cf) \bmod q = (mf + 3rg) \bmod q = mf + 3rg$, and therefore,

$$(cf \,(\bmod q)) \bmod 3 = (mf + 3rg) \bmod 3 = (m(1+3F)) \bmod 3 = m.$$

The statement is proven.

Thus, the task of recovery the cryptosystem secret key by its public key h is reduced to find a sufficiently short vector (with the first coordinate equal to one) in the lattice $L(h)$. Taking the usual heuristic assumption that the desired vector is the shortest non-zero vector of the lattice $L(h)$, we conclude that the secret key recovery is equivalent to solving the problem of the shortest vector problem (SVP) for this lattice. Note that the latter problem is equivalent to finding vector which is closest to the vector $(0_{1\times n}, h')$ in the lattice generated by the rows of the matrix $\begin{pmatrix} I_n & H \\ 0_{n\times 1} & qI_n \end{pmatrix}$ (closest vector problem (CVP)).

The inverse of a function E_h task or, equivalently, the recovery of the input message $m \in R/3$ by the output cryptogram $c = (m+rh) \bmod q$, where $r \in R/3$, $\| r \|_1 = 2t$, also reduces to the search for the shortest (or short enough) vector of the lattice $L(h,c)$ generated by the rows of the matrix

$$\begin{pmatrix} 1 & 0_{1\times n} & c \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}.$$

Both lattices $L(h)$, $L(h,c)$ have the same form and belong to the class of modular lattices.

Hybrid attack

It should be noted that this attack is now implemented on ordinary computers, but it is also possible to implement it in the future and on quantum ones.

A hybrid attack on the classic NTRU cryptosystem was proposed in [13] and was subsequently researched in many publications. A certain result of these studies is the work [16], which shows that the complexity estimates of the hybrid attack received earlier for different cryptosystems are very inaccurate due to false assumptions and questionable heuristic considerations, that are used to obtain these estimates.

Note that certain heuristic assumptions are also used in [16], so the question of well-grounded estimates of the hybrid attack complexity is the subject of further researches.

In relation to the cryptosystem under consideration, a hybrid attack is carried out in this way [16].

Consider the lattice $L(h)$ generated by the rows of the matrix (9), fix the number $r \in \overline{1, n-1}$ and write the matrix H in the form $H = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}$, where H_1 and H_2 are integer matrixes of size $r \times n$ and $(n-r) \times n$, respectively. An arbitrary vector $F \in Z^n$ will be written in the form $F = (F_1, F_2)$, where $F_1 \in Z^r$, $F_2 \in Z^{n-r}$.

Note that the vector $(1, F, g)$ belongs to the lattice $L(h)$ if and only if there is a vector $x \in Z^n$ such that

$$F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1) = -(1, F_2, x)\begin{pmatrix} 1 & 0_{1\times(n-r)} & h' \\ 0_{(n-r)\times 1} & I_{n-r} & H_2 \\ 0_{n\times 1} & 0_{n\times(n-r)} & qI_n \end{pmatrix} + (1, F_2, g). \quad (13)$$

The last equality is equivalent to the vector $F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1) - (1, F_2, g)$ that belongs to a lattice $L_r(h)$ generated by the rows of the matrix

$$\begin{pmatrix} 1 & 0_{1\times(n-r)} & h' \\ 0_{(n-r)\times 1} & I_{n-r} & H_2 \\ 0_{n\times 1} & 0_{n\times(n-r)} & qI_n \end{pmatrix}.$$

According to [16], a hybrid attack depends on the parameters r, l, c_{-1}, c_1 and is aimed to finding a vector $(1, F_1, F_2, g) \in L(h)$ that satisfies the following conditions:

(a) F_1 is a small vector that has precisely $2c_{-1}$ coordinates equal to -1, and $2c_1$ coordinates, that equal to 1;

(b) (F_2, g) is a small vector, that has an Euclidean norm l.

The attack consists of two stages, on the first – a reduced lattice $L_r(h)$ basis B constructed in one way or another. Next, on the second stage, vectors of F_1, that satisfy the condition (a), by which vectors $(\nu, F_2, g) = \mathrm{NP}_B(\hat{F}_1)$ are calculated, where $\nu \in Z$ and $\mathrm{NP}_B(\hat{F}_1)$ is a result of Babai algorithm application to the vector $\hat{F}_1 = F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1)$ and basis B of the lattice $L_r(h)$. Mentioned algorithm finds a "sufficiently short" vector $e = \mathrm{NP}_B(\hat{F}_1)$ for which $\hat{F}_1 - e \in L$, provided that the basis B is "sufficiently well" reduced [17].

From equation (13) and condition (b) it follows that the vector $\hat{F}_1$ is close to the lattice $L_r(h)$, so it is natural to look for the nearest to it vector of this lattice in the form $\hat{F}_1 - \mathrm{NP}_B(\hat{F}_1)$. In addition, on the basis of equality (13), for any $F_1 \in Z^r$ vector $(1, F_1, F_2, g)$ belongs to lattice $L(g)$, if $\mathrm{NP}_B(\hat{F}_1) = (1, F_2, g)$. Therefore, all that remains to be checked for a vector $\mathrm{NP}_B(\hat{F}_1)$ on the second stage of an attack is equality $\nu = 1$ and condition (b).

In order to speed up the search for vectors in the second stage, the method of meet in the middle is used: instead of the vectors F_1 satisfying condition (a), small vectors f_1 of length r, each of which have exactly c_{-1} coordinates, that are equal to -1, and c_1 the coordinates, that are equal to 1, are sorted. Each vector f_1 is stored in a hash table with addresses of a certain set $A(f_1)$, which de-

pends only on the vector $\mathrm{NP}_B(\hat{f}_1)$, where $\hat{f}_1 = f_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1)$, and consists of some binary vectors of length $2n-r+1$. The set of addresses is constructed so, that $A(f_1') \cap A(f_1'') \neq \varnothing$ if the difference between vectors $\mathrm{NP}_B(\hat{f}_1')$ and $\mathrm{NP}_B(\hat{f}_1'')$ is a small vector.

Each time when in the search process it is performed repeatedly to the table at the same address, that is, for some vectors f_1', f_1'' that are enumerated, the condition $A(f_1') \cap A(f_1'') \neq \varnothing$ is fulfilled, the vector (F_1, F_2, g) is calculated, where $F_1 = f_1' + f_1''$, $(\nu, F_2, g) = \mathrm{NP}_B(\hat{f}_1') + \mathrm{NP}_B(\hat{f}_1'')$ for which the conditions (a) and (b) and equality $\nu = 1$ are verified. Therefore, the attack ends successfully, if there is a pair of small vectors f_1', f_1'' satisfying the following conditions:

(a′) each of the vectors f_1', f_1'' has exactly c_{-1} coordinates equal to -1, and c_1 coordinates that are equal to 1;

(b′) the vector $F_1 = f_1' + f_1''$ satisfies the condition (a);

(c′) vector $\mathrm{NP}_B(\hat{F}_1)$ equals to $\mathrm{NP}_B(\hat{f}_1') + \mathrm{NP}_B(\hat{f}_1'')$, has the first coordinate $\nu = 1$ and satisfies the condition (b).

In [16] using heuristic considerations, the formula for the described second stage attack complexity is obtained:

$$T_2(\delta, r) = \frac{2^{15} r!}{c_{-1}! c_1! (r - c_{-1} - c_1)!} \left(\binom{2c_{-1}}{c_{-1}} \binom{2c_1}{c_1} p\,|S| \right)^{-1/2} \frac{1}{\tilde{p}}, \tag{14}$$

where

$$p = \prod_{i=1}^{2n-r+1} \left(1 - \frac{1}{r_i B\left(\frac{2n-r}{2}, \frac{1}{2}\right)} \int_{-r_i-1}^{-r_i} \int_{\max\{-1, z-r_i\}}^{z+r_i} (1-t^2)^{\frac{2n-r-2}{2}} dt dz \right), \tag{15}$$

$$|S| = 2 + 2(n-t-1) p_S, \tag{16}$$

$$p_S = \frac{p_{\mathrm{NP}} 2^{-4c_1} r!}{(2c_{-1})!(2c_1)!(r - 2c_{-1} - 2c_1)!} \binom{n-r}{4t-4c_1} \binom{n}{2t}^{-1}, \tag{17}$$

$$p_{\mathrm{NP}} = \prod_{i=1}^{2n-r+1} \left(1 - \frac{2}{r_i B\left(\frac{2n-r}{2}, \frac{1}{2}\right)} \int_{-1}^{\max\{-r_i, -1\}} (1-t^2)^{\frac{2n-r-2}{2}} dt \right), \tag{18}$$

$$\tilde{p} = 1 - (1 - p_S)^{n-t}. \tag{19}$$

In formulas (15), (18) $B(\cdot,\cdot)$ denotes the Euler beta-function, and the numbers r_i are determined by the formulas

$$r_i = \frac{R_i(\delta)}{2l},\ i \in \overline{1, 2n-r+1}, \tag{20}$$

where

$$R_i(\delta) = q, \text{ if } 1 \le i \le 2n - r + 1 - \mu;$$

$$R_i(\delta) = q^{-2(i-(2n-r+1-\mu)-1)+\mu} q^{\frac{\mu-(n-r)}{\mu}}, \text{ if } 2n-r+1-\mu < i \le 2n-r+1,$$

$$\mu = \min\left\{2n-r+1, \left\lfloor \sqrt{\frac{n-r}{\log_q \delta}} \right\rfloor\right\},\ \delta > 1.$$

It is recommended to use the following parameter values:

$$|c_{-1}| = |c_1| = \left\lceil \frac{rt}{2n} \right\rceil,\ l = \sqrt{\frac{2n}{3} + \frac{2t(n-r)}{n}}. \tag{21}$$

To estimate the first stage of a hybrid attack (the construction of a reduced basis B of lattice L), a traditional approach is used [18]. It is believed that the basis B is constructed using the Korkin-Zolotarev block algorithm: BKZ 2.0 [19] (which is considered to be one of the best algorithms for solving similar problems nowadays). The BKZ 2.0 algorithm depends on the natural parameters β and m, which denote the so-called *block length* and the *number of iterations* respectively, and allows to build the reduced Korkin-Zolotarev basis of a complete lattice of dimension $2n-r+1$ by $2^{E(\beta,m,2n-r+1)}$ operations, where

$$E(\beta, m, 2n-r+1) = 0{,}000784314\beta^2 + 0{,}366078\beta + \log((2n-r+1)m) + 0{,}875 \tag{22}$$

(note that formula (22) is an empirical estimate based on the results of computational experiments [18]).

The degree of the reduced basis quality, which is built using the algorithm, is the so-called root Hermite factor: the number $\delta > 1$ determined by the formula

$$\| b_1 \|_2 = \delta^{2n-r+1} \left(\det L(H_2, h)\right)^{\frac{1}{2n-r+1}} = \delta^{2n-r+1} q^{\frac{n}{2n-r+1}},$$

where b_1 is the shortest vector in the built basis. [19] describes the BKZ 2.0 algorithm simulator, which allows to calculate such values β and m by the input parameter $\delta > 1$, that application of the BKZ 2.0 with these parameters to any input basis of the full lattice of the dimension $2n-r+1$ leads to its reduced basis with the root factor of Hermite δ.

The complexity $T_1(\delta, r)$ calculation of the hybrid attack first stage is carried out as follows:

1) using BKZ 2.0 algorithm simulator [19], find β and m by the input data $2n-r+1$ and δ;
2) put

$$T_1(\delta, r) = 2^{E(\beta,m,2n-r+1)}, \tag{23}$$

where $E(\beta, m, 2n-r+1)$ is determined by the formula (22).

The total complexity of the hybrid attack is calculated by the formula

$$T(\delta, r) = T_1(\delta, r) + T_2(\delta, r); \tag{24}$$

with this estimation of the cryptosystem stability in relation to this attack is the number $T_{\min} = \min\{T(\delta, r) : \delta > 1, r \in \overline{1, n-1}\}$.

According to [16], to calculate the value $T_{\min}$, $\delta_r > 1$ should be found for each $r \in \overline{1, n-1}$ so that $T(\delta_r, r) = \min\{T(\delta, r) : \delta > 1\}$ and set $T_{\min} = \min\{T(\delta_r, r) : r \in \overline{1, n-1}\}$. To find δ_r it can be applied an iterative algorithm (dichotomy) as $T_1(\delta, r)$ is decreasing, and $T_2(\delta, r)$ − an increasing function

of the parameter $\delta > 1$: the desired value δ_r is approximately equal to the equation root $T_1(\delta, r) = T_2(\delta, r)$.

Thus, using the formulas (14), (23), (24), we can estimate the resistance of the considered cryptosystem in relation to the hybrid attack. To ensure resistance at the k-th level it is sufficient to fulfill the condition

$$2^k \le T_{\min}. \tag{25}$$

Sieving methods

Such attacks today are realized on ordinary computers, but in the future they may be implemented on quantum computers.

In recent years, a number of algorithms for solving SVP and CVP problems with sieving methods have been proposed. The most effective of known algorithms have heuristic complexity $(3/2)^{N/2+o(1)}$ with $N \to \infty$, where N – the dimension of the lattice, with the residual term $o(1)$ that is positive [20, 21]. Since in our case $N = 2n+1$, to ensure the resistance of the cryptosystem relative to the attacks based on the sieving methods, it is sufficient to fulfill the condition

$$2^k \le (3/2)^n. \tag{26}$$

7 Conclusions

1. An analysis of the requirements for post-quantum cryptographic transformations of asymmetric encryption allows us to conclude that the basic, and unconditional requirement for cryptographic transformation «NTRU Prime IIT Ukraine», is the requirement of cryptographic stability regarding known and potentially possible attacks. These attacks can be implemented using classical attacks based on the use of classical computer systems and classical mathematical methods, as well as on the basis of quantum computers and corresponding mathematical and programmatic methods.
2. Obviously, cryptographic asymmetric transformations should provide protection from both classical and quantum methods of cryptanalysis. The above should be taken into account, if possible, in the construction and analysis of general-type post-quantum transformations, and the adoption of their post-quantum standards of asymmetric cryptographic transformations.
3. In the cryptosystem «NTRU Prime IIT Ukraine» as the main cryptographic transformation, as in NTRU Prime, unlike NTRU, the transformation is used in the finite field. The above makes it impossible to conduct a series of potential attacks regarding the cryptographic system «NTRU Prime IIT Ukraine» and eliminates the potential weaknesses present in the NTRU cryptosystem. They are mainly related to the existence of non-trivial subfields or factor rings of the factor (truncated) polynomials ring.
4. In the cryptosystem «NTRU Prime IIT Ukraine» polynomials F and r are arbitrary t-small, they have $2t$ non-zero coefficients (+1, −1), whereas in NTRU, each of these polynomials has exactly t nonzero coefficients equal to 1 and −1 respectively. The same is true for the polynomial g used in the cryptosystem «NTRU Prime IIT Ukraine», which is an arbitrary small polynomial with $2t$ nonzero coefficients (+1, −1). Specified allows to expand the size of the key space in comparison with NTRU without losing the efficiency of algorithms implementation for the keys formation and implementation of encryption and decryption algorithms.
5. To ensure the stability of the cryptosystem relative to the attack with a known open message, which is based on the overview of the vectors $b \in \{0,1\}^{l_2}$, the value l_2 (taking into account the quantum algorithms of overview) should be at least $2k$, where k – the security parameter. In this case, the length of the initial state of the gamma generator used to obtain the vector b must be at least $2k + 64$ bits.

6. For the «NTRU Prime IIT Ukraine» cryptosystem, the most effective of known potential attacks, it is necessary to justify the choice of parameters n, t,and q depending on the security parameter k. It is necessary to ensure that the following conditions are met:
   a) choose a simple number n in such a way that it satisfies the inequality (26);
   b) for a given n choice, if it exists, a natural t, that satisfies the inequalities (2);
   c) for the given n and t choose a prime $q \geq 48t+3$ such, that the polynomial $x^n - x - 1$ was irreducible over the field $\mathbf{Z}_q$, and the condition (25) was fulfilled.
7. An adequate condition for the cryptographic stability of the «NTRU Prime IIT Ukraine» cryptographic transformation with the given three parameters (n,t,q) is the unconditional fulfillment of the condition (25).

References

[1] ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. [Electronic resource]. – Access mode: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id =46690.

[2] Koblitz Neal A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes // – Access mode: https://eprint.iacr.org/2015/1018.pdf.

[3] Lily Chen Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone // – Access mode: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

[4] Mosca M. "Setting the Scene for the ETSI Quantum-safe Cryptography Workshop" / M. Mosca // E-proceedings of "1st Quantum-Safe-Crypto Workshop", Sophia Antipolis, Sep 26-27, 2013. – Access mode: http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/eproceedings_Crypto_2013.pdf.

[5] Post-quantum crypto project. [Electronic resource]. – Access mode: http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html.

[6] Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. [Electronic resource]. – Access mode: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-draft-aug-2016.pdf.

[7] Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges Access mode: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

[8] American National Standard for Financial Services – Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry – ANSI X9.98–2010, 2010. – 284 p.

[9] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal: NTRU Prime. – Access mode: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf.

[10] Kachko O. G. The optimization of NTRU-like algorithm for asymmetric encryption with "inconvenient parameters" / O. G. Kachko, L. V Makutonina, O. S. Akolzina //. Mathematical and computer modeling. Series: Engineering, 15 (2017), 79–85. (in Ukrainian)

[11] Hoffstein J. NTRU: a ring based public key cryptosystem / J. Hoffstein, J. Pipher, J. H. Silverman // Algorithmic Number Theory, Third International Symposium, Portland, Oregon, USA, June 21 – 25, 1998. – Proceedings. – Springer, 1998. – P. 267–288.

[12] Campbell P., Groves M., Shepherd D. SOLYLOQUI: a cautionary tale, 2014. – Access mode: http:docbox.etsi.org /Workshop/2014/201410_CRYPTO/S07_Systams_and_Ayyacks/S07_Groves_Annex.pdf.

[13] Howgrave-Graham N. A hibrid lattice-reduction and the meet-in-the-midle attack against NTRU / N. Howgrave-Graham // Advances in Cryptology – CRYPTO 2007. – Proceedings. – Springer-Verlag. – 2007. – P. 150–169.

[14] Howgrave-Graham N. A meet-in-the-midle attack on an NTRU private key / N. Howgrave-Graham, J. H. Silverman, W. Whyte // Technical report, NTRUCryptosystems, June 2003. Report, 2003.

[15] Coppersmith D. Lattice attack on NTRU / D. Coppersmith, A. Shamir // Advances in Cryptology – EUROCRYPT'97. – Proceedings. – Springer-Verlag. – 1997. – P. 52–61.

[16] Wunderer Th. Revising the hibrid attack: improved analysis and refined security estimates. – Access mode: http://eprint.iacr.org /2016/733.

[17] Babai L. On Lova′sz' lattice reduction and the nearest lattice point problem / L. Babai // Combinatorica. – 1986. – Vol. 5. – № 6(11). – P. 1–13.

[18] Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Z. Choosing parameters for NTRUEncrypt. – Access mode: http://eprint.iacr.org/2015/708.

[19] Chen Y. BKZ 2.0: better lattice security estimates / Y. Chen, P.Q. Nguyen // Advances in Cryptology – ASIACRYPT 2011. – Proceedings. – Springer-Verlag. – 2011. – P. 1–20.

[20] Gorbenko Yu. I. Special'na tema / Yu. I. Gorbenko, R. S. Ganzja // Zbirnyk naukovyh prac', vyp.2(22) Special'ni telekomunikacijni systemy ta zahyst informacii', prym.№59 DSSZZI Ukrai'ny. – S. 17–26.

[21] Gorbenko Yu. I. Analiz stijkosti populjarnyh kryptosystem proty kvantovogo kryptoanalizu na osnovi algorytmu Grovera / Yu. I. Gorbenko, R. S. Ganzja // Zahyst informacii': Naukovo-praktychnyj zhurnal, 2014. – Tom 16, №2. – S. 106–112.

[22] Gorbenko Yu. I. Analiz shljahiv rozvytku kryptografii' pislja pojavy kvantovyh komp'juteriv / Ju. I. Gorbenko, R. S. Ganzja // Visnyk Nacional'nogo universytetu «L'vivs'ka Politehnika». Serija «Komp'juterni systemy ta merezhi», 2014. – № 806. – S. 40–49.

[23] J. Silverman and A. Odlyzko, NTRU Report 004, Version 2, A Meet-The Middle Attack on an NTRU Private Key, Technical Report, NTRU Cryptosysytems, (2003).

[24] A Chosen-Ciphertext Attack against NTRU. [Electronic resource]. – Access mode: http://www.iacr.org/archive/crypto2000/18800021/18800021.pdf.
[25] Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms : ISO/IEC 9796-2:2010. – 54 p.
[26] IBM Raises the Bar with a 50-Qubit Quantum Computer. [Electronic resource]. – Access mode: https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/?utm_campaign=add_this&utm_source=twitter&utm_medium=post.
[27] Sozdan pervyi kvantovyi komp'yuter na 53 kubitakh. [Electronic resource]. – Access mode: https://hightech.fm/2017/11/30/53-qubit.

Рецензент: Роман Олійников, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна. E-mail: roliynykov@gmail.com.

Надійшло: Листопад 2017.

Автори:

Іван Дмитрович Горбенко, доктор технічних наук, професор, лауреат Державної премії України, професор кафедри безпеки інформаційних систем і технологій, ХНУ імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: gorbenkoi@iit.kharkov.ua.

Качко Олена Григорівна, кандидат технічний наук, начальник відділу програмування АТ «Інститут інформаційних технологій», професор кафедри програмної інженерії, Харьковский національний университет радіоелектроніки, проспект Науки 14, м. Харків, 61022, Україна.
E-mail: iit@iit.kharkov.ua.

Марина Віталіївна Єсіна, кандидат технічний наук, старший викладач кафедри безпеки інформаційних систем і технологій, ХНУ імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: rinayes20@gmail.com.

Аналіз алгоритму направленого шифрування NTRU Prime IIT Ukraine з урахуванням відомих атак.

Анотація. У роботі розглянуто сучасні криптографічні перетворення типу асиметричне направлене шифрування, а саме – NTRU-подібні криптографічні системи. На основі існуючих криптографічних перетворень цього типу (криптографічні алгоритми NTRU (ANSI X9.98-2010) та NTRU Prime) створено нову криптографічну систему NTRU Prime IIT Ukraine. Наведено короткий опис цієї криптографічної системи та проведено аналіз її стійкості до відомих атак. В кінці роботи зроблено висновки та наведено рекомендації щодо особливостей, переваг та можливості застосування нового криптографічного асиметричного алгоритму направленого шифрування NTRU Prime IIT Ukraine.

Ключові слова: атака, кільце, направлене шифрування, поле, фактор-кільце.

Рецензент: Роман Олейников, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, г. Харьков, Украина. E-mail: roliynykov@gmail.com.

Поступила: Ноябрь 2017.

Авторы:

Иван Дмитриевич Горбенко, доктор технических наук, профессор, лауреат Государственной премии Украины, профессор кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: gorbenkoi@iit.kharkov.ua.

Качко Елена Григорьевна, кандидат технических наук, начальник отдела программирования АТ «Институт информационных технологий», профессор кафедры программной инженерии, Харьковский национальный университет радиоэлектроники, проспект Науки 14, г. Харьков, 61022, Украина.
E-mail: iit@iit.kharkov.ua.

Марина Витальевна Есина, кандидат технических наук, старший преподаватель кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: rinayes20@gmail.com.

Анализ алгоритма направленного шифрования NTRU Prime IIT Ukraine с учетом известных атак.

Аннотация. В работе рассмотрены современные криптографические преобразования типа ассиметричное направленное шифрование, а именно – NTRU-подобные криптографические системы. На основе существующих криптографических преобразований этого типа (криптографические алгоритмы NTRU (ANSI X9.98-2010) и NTRU Prime) создана новая криптографическая система NTRU Prime IIT Ukraine. Приведено краткое описание этой криптографической системы и проведен анализ ее устойчивости к известным атакам. В конце работы сделаны выводы и приведены рекомендации касательно особенностей, преимуществ та возможности применения нового криптографического ассиметричного алгоритма направленного шифрования NTRU Prime IIT Ukraine.

Ключевые слова: атака, кольцо, направленное шифрование, поле, фактор-кольцо.