UDC 004.056.55

I.D. GORBENKO, Dr. Sc. (Technology), A.N. ALEKSEYCHUK, Dr. Sc. (Technology),
O.H. KACHKO, Cand. Sc. (Technology), M.V. YESINA, Cand. Sc. (Technology),
V.A. BOBUKH, Cand. Sc. (Technology), S.O. KANDYI, V.A. PONOMAR Cand. Sc. (Technology)

CALCULATION OF GENERAL PARAMETERS FOR NTRU PRIME UKRAINE OF 6-7 LEVELS OF STABILITY

Introduction

Investigations of perspective (including post-quantum) asymmetric cryptanalytic transforms such as asymmetric code (ASC), key encapsulation protocol (KEP) and digital signature (DS) confirm the promising use for constructing post-quantum transformation standards in polynomial rings over finite fields [1 – 4]. The main candidates for constructing the asymmetric cryptographic transforms are NTRUEncrypt ANSI X9.98 [1], NTRU Prime [2] and NTRU Prime Ukraine [3]. Special attention was paid to the ASC and KEP construction in [1], since they provide cryptographic stability up to 256 bits of classical stability and up to 128 bits of quantum stability.

At the same time, the standards of symmetric cryptographic transformations have been constructed and used, which provide cryptographic stability of 512 bits of classical and 256 bits of quantum stability [5, 6]. Therefore, in our opinion, in the long run, the ASC, KEP and DS of 6-7 levels of stability are needed. Moreover, under the 6th level of security it is proposed to understand resistance against 384 bits of classical cryptographic stability and 192 bits of quantum cryptographic stability, respectively, and under the 7th level of security it is proposed to understand resistance against 512 bits of classical cryptographic stability and 256 bits of quantum cryptographic stability, respectively. The implementation of 6-7 levels of stability is associated with the complex problematic task of constructing common parameters and keys for cryptographic transformations in a ring of polynomials over finite fields for recognized and accepted security models [4, 9].

The purpose of this paper is to carry out research and develop an effective practical algorithm for construction and experimental confirmation of the built-in system-wide parameters and keys of cryptographic transformations of the ASC and KEP of 6-7 levels of stability based on transformations in a ring of polynomials over finite fields.

1. Method for calculating general parameters for the algorithm (NTRU Prime Ukraine)

1.1. Basic concepts and notation

Let us consider the general provisions regarding the algorithm of the ASC in the ring of polynomials over a finite field called NTRUPrime [2, 4]. The generation of system-wide parameters is one of the important stages of the ASC mechanism in this algorithm. Let's consider its general provisions regarding the general parameters of NTRUPrime.

Let us denote the ring of residue classes Z_l modulo l for any odd number l. Elements of such a ring are identified with integers belonging to the segment $\left[-1/2\,(l-1), 1/2\,(l-1)\right]$. For any $a \in Z$ the record $a \bmod l$, means the unique integer $a' \in \left[-1/2\,(l-1), 1/2\,(l-1)\right]$ such that $a \equiv a' \bmod l$. Let us fix the general parameters of the algorithm NTRUPrime: a natural number t and different prime numbers n, q such that

$$n \geq \max\{3, 2t\},\ q \geq 48t + 3 \text{ and polynomial } x^n - x - 1, \tag{1}$$

which is irreducible over the field $\mathbf{Z}_q$ [2,4]. Let us also denote the ring of polynomials

$$R = Z[x]/(x^n - x - 1),\ R/q = Z_q[x]/(x^n - x - 1),\ R/3 = Z_3[x]/(x^n - x - 1), \tag{2}$$

where $R/3 \subset R/q \subset R$ as sets.

From the above it follows that in the NTRUPrime the ring of polynomials R/q is a field that consists of q^n polynomials of the form $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1}$, where u_i are integers from the segment

$$\left[-1/2\,(q-1), 1/2\,(q-1)\right],\ i \in \overline{0, n-1}, \tag{3}$$

which are added and multiplied modulo q. At the same time, the multiplication of the polynomials themselves (elements of the field) takes place by the modulus of the polynomial $x^n - x - 1$. Also, for any $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in R$ let us denote polynomial $u \bmod q$

$$(u_0 \bmod q) + (u_1 \bmod q)x + \cdots + (u_{n-1} \bmod q)x^{n-1} \in R/q. \tag{4}$$

A similar meaning has a notation $u \bmod 3$, i.e.

$$(u_0 \bmod 3) + (u_1 \bmod 3)x + \cdots + (u_{n-1} \bmod 3)x^{n-1} \in R/3. \tag{5}$$

Polynomial $u \in R$ of the (2) type is called *small* polynomial, if $u \in R/3$, that is, the coefficients of the polynomial take values (-1, 0, 1). Also, we will call such a polynomial *t*-ternary (*small*) if it has exactly 2*t* nonzero coefficients (-1, 1).

For any $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in R$ we will use such notation

$$\| u \|_\infty = \max_{0 \le i \le n-1} | u_i |,\ \| u \|_1 = \sum_{i=0}^{n-1} | u_i |,\ \| u \|_2 = \left(\sum_{i=0}^{n-1} | u_i |^2 \right)^{1/2}. \tag{6}$$

Next, consider the requirement for *q* defined for $q \ge 48t + 3$. In essence, this condition defines the requirement for an admissible *q* value, which ensures the uniqueness of the encryption and decryption algorithms. Moreover, as shown by the preliminary analysis, there is a need for a reasonable reduction of the value of *q*, first of all for the ASC of 6 and 7 levels of cryptographic stability.

2. Determination of the ASC transformation mechanism

After the construction of system-wide parameters, the next step is the formation (generation) of an asymmetric key pair. Let us consider the problem of forming an asymmetric key pair for an algorithm in the NTRUPrimeUkraine.

2.1. Analysis of algorithm for key generation

To generate the keys, we chose the standard generation scheme, which was proposed in [1].

1. A small polynomial $G \in R/3$ is formed, for which there exists $G^{-1} \bmod q$.
2. A *t*-small polynomial $F \in R/3$ is formed.
3. The polynomial value $f = 3F + 1$ is calculated.
4. The polynomial $h = 3g / f \in R/q$ is calculated.

Polynomials *f* and *h* are the secret and public keys, respectively.

Note that the value h is calculated in the field R/q by multiplying the polynomial $3g$ by the polynomial, which is inverse to f in R/q. This is always possible, since the reverse f^{-1} polynomial exists, because $\| f \|_1 = 2t > 0$.

In [7] the scheme of keys formation is offered, in which the public key is calculated by the formula $h=G/(3F)$ and polynomials F, $G^{-1} \bmod 3$ are stored as the private key. However, such a scheme requires additional multiplication by G^{-1} in the process of decoding. This process also contains two multiplications, substantially different in time from the direct transformation, which requires only one multiplication, the additional multiplication will further increase the asymmetry.

As arguments, the authors suggest the following: a reduction in the length of keys and insignificant increase in time for decryption in the case of using hardware for the implementation of transformations. Indeed, as shown below, the value of *q,* compared with the version applied to NTRUPrime, is increased by 1.5 times. A twofold increase reduces the length of each coefficient by only one bit. An increase by 1.5 times, as a rule, practically does not increase the length of the polynomial element. Indeed, parameters for n=761, t=143, q≥32*143+1=4591 (simple irreducible). In the case of packing 3 numbers, as recommended by authors [7], it requires 37 bits, that is, 5 bytes. When using q≥48*143+1=6869 (simple irreducible). Packing of 3 numbers requires 39 bits, that is, 5 bytes too. At the same time, for the private key you need to store an additional component G^{-1}, which significantly increases the secret key. Below we will show you how to define a limit on q value in the conditions of key generation according to the proposed scheme to provide guaranteed decryption for 6 and 7 levels of stability.

2.2. Pseudo-trapdoor one-way function

Let us consider the requirements and the possibility of reducing q based on the analysis of a pseudo-trapdoor function using cryptographic transformations of the ASC and KEP type in the ring of polynomials over a finite field.

It is known [1 - 3], that for any private key f and the corresponding public key h in the ring of polynomials over a finite field, there are functions of encryption E_h and decryption D_f

$$E_h(m,r) = c = (m + rh) \bmod q\ ,\ m,r \in R/3\ ,\ \| r \|_1 = 2t\ , \tag{7}$$

$$D_f(c) = (cf(\bmod q) \bmod 3\ ,\ c \in R/q\ . \tag{8}$$

Let us determine the conditions under which the uniqueness of encryption (7) and decryption (8) are ensured.

Statement 1 [1, 2]. Encryption (7) and decryption (8) uniqueness is provided for any of the above key data f, g, h, r and message m, that is

$$D_f(E_h(m,r)) = m\ . \tag{9}$$

Proof of property (9) is given in [1], but a polynomial x^n-1 and q=2048 is considered there. Let us consider it, but at the same time let us define the conditions of reduction and the admissible limit of the value of the module q.

Let the cryptogram $c = E_h(m,r)$ be received as a result of encryption, and when decrypting the message $m' = D_f(c)$. Let us prove that $m = m'$ and define the condition of uniqueness. In the proof, we will substitute the value from (7) in (8). As a result, we get

$$(cf) \bmod q = (mf + rhf) \bmod q\ . \tag{10}$$

Next we substitute the value of h in (10), as a result we have

$$(mf + 3rgf\ /\ f) \bmod q = (mf + 3gr) \bmod q\ . \tag{11}$$

Analysis (11) shows that if the moduli of the coefficients of the polynomials mf and $3rg$ of the polynomial $mf + 3rg \in R$ are smaller than $q/2$ and, in general, the condition

$$\| mf + 3rg \|_\infty < q/2\ , \tag{12}$$

is fulfilled, then (10), taking into account (12), can be presented in the following form

$$(cf) \bmod q = (mf + 3rg) \bmod q = mf + 3rg. \tag{13}$$

Taking into account (10) and (12), when decoding *R/3* in the polynomial ring, we have

$$m' = (cf(\bmod q)) \bmod 3 = (mf) \bmod 3 + (3rg) \bmod 3 = (mf) \bmod 3 + 0\ . \tag{14}$$

Finally, we will substitute (7) in (14) and have

$$m' = (m(1+3F) \bmod 3 = m + 0 = m. \quad (15)$$

Thus, to ensure the uniqueness of encryption (7) and decryption (8), that is, $D_f(E_h(m,r)) = m' = m$ it is enough to make sure that inequality (12) is fair. In essence, (12) is necessary, but with certain constraints even sufficient condition.

Next, let us consider the possibility of reducing the value of q and determine to what extent this can be done to ensure unambiguity and no error in decoding. For this we use the lemma from [7].

Lemma. For any $u, v \in R$ following inequalities are fair

$$\| uv \|_\infty \le 2 \| u \|_\infty \| v \|_1, \ \| uv \|_\infty \le 2 \| u \|_2 \| v \|_2.$$

First, let us use the lemma to clarify its proof and the conditions for uniqueness of decryption, and then consider the essence of its proof.

Using formulas (14) and taking into account that in the NTRU Prime Ukraine messages are the polynomial m and key data are the polynomials g and F belong to $R/3$, that is, the polynomial coefficients take values (-1, 0, 1) and taking into account that $\| m \|_\infty = \| g \|_\infty = 1$, $\| F \|_1 = \| r \|_1 = 2t$ we have that the maximum coefficient of polynomial (15) can be determined in this way

$$\begin{aligned} &\| mf + 3rg \|_\infty = \| m(1+3F) + 3rg \|_\infty \le \| m \|_\infty + 3 \| mF + rg \|_\infty \le \\ &\le 1 + 3(2 \| m \|_\infty \| F \|_1 + 2 \| g \|_\infty \| r \|_1) = 1 + 6(\| m \|_\infty \| F \|_1 + \| g \|_\infty \| r \|_1) \le 1 + 24t < q/2. \end{aligned} \quad (16)$$

The last inequality follows from the fact that for our case $q \ge 48t + 3$ .Thus, statement 1 is proved.

Note that if we use the polynomial F instead of the polynomial 1 + 3F in formula (16) we obtain $16t<q/2$, which is equivalent to the requirement $q \ge 32t+1$. It is precisely this expression used to calculate q in [6].

Now let's show that the lemma also holds, that is, that it is true and its use is correct.

It should be noted that in fact the lemma argues that the maximum value of the coefficient [7] is limited

$$\| uv \|_\infty \le 3 \| u \|_\infty \| v \|_1, \ u, v \in R. \quad (17)$$

That is, we can conclude that the decryption of messages in the cryptosystem of the NTRU Prime Ukraine is correct, but subject to condition $q \ge 48t + 3$ [2]. Detailed proof of the lemma. Let $u = \sum_{i=0}^{n-1} u_i x^i$, $v = \sum_{i=0}^{n-1} v_i x^i$; then the product of the polynomials u and v in the ring $Z[x]$ equals $\sum_{i=0}^{2n-2} w_i x^i$, where $w_i = \sum_{j=0}^{i} u_j v_{i-j}$, $i \in \overline{0, 2n-2}$. Consequently, the product of these polynomials in a ring R equals

$$uv = (w_0 + w_n)x^0 + \sum_{i=1}^{n-2} (w_i + w_{i+n} + w_{i+n-1})x^i + (w_{n-1} + w_{2n-2})x^{n-1}.$$

Further, for any $i \in \overline{1, n-2}$ such equalities are fair:

$$w_i + w_{i+n} + w_{i+n-1} = \sum_{j=0}^{i} u_j v_{i-j} + \sum_{j=0}^{i+n} u_j v_{i-j} + \sum_{j=0}^{i+n-1} u_j v_{i-j} =$$

$$= \sum_{j=0}^{i-1} u_j v_{i-j} + u_i (v_0 + v_{n-1}) + \sum_{j=i+1}^{n-1} u_j (v_{i+n-j} + v_{i+n-1-j}) = \quad (18)$$

$$= (u_0 v_i + u_1 v_{i-1} + \cdots + u_i v_0 + u_{i+1} v_{n-1} + u_{i+2} v_{n-2} + \cdots + u_{n-1} v_{i+1}) +$$

$$+ (u_i v_{n-1} + u_{i+1} v_{n-2} + \cdots + u_{n-1} v_i).$$

Hence,

$$| w_i + w_{i+n} + w_{i+n-1} | \le$$

$$\le \max_{0 \le l \le n-1} | u_l | (| v_i | + | v_{i-1} | + \cdots + | v_0 | + | v_{n-1} | + | v_{n-2} | + \cdots + | v_{i+1} |) +$$

$$+ \max_{0 \le l \le n-1} | u_l | (| v_{n-1} | + | v_{n-2} | + \cdots + | v_i |)$$

$$\le 2 \max_{0 \le l \le n-1} | u_l | \sum_{j=0}^{n-1} | v_j | = 2 \| u \|_\infty \| v \|_1 .$$

Similarly, we obtain that

$$| w_0 + w_n | \le 2 \| u \|_\infty \| v \|_1 , \; | w_{n-1} + w_{2n-2} | \le 2 \| u \|_\infty \| v \|_1 ,$$

wherefrom the validity of the formula (14) follows.

Further, based on the formula (18) and Cauchy-Bunyakovskii inequality we find that $| w_i + w_{i+n} + w_{i+n-1} | \le 2 \| u \|_2 \| v \|_2$, $i \in \overline{1, n-2}$; furthermore,

$$| w_0 + w_n | \le 2 \| u \|_2 \| v \|_2 , \; | w_{n-1} + w_{2n-2} | \le 2 \| u \|_2 \| v \|_2 ,$$

Where from the validity of formula (17) follows.

3. Analysis of encryption and decryption algorithms

The padding scheme [NAEP] [10] is used to ensure the stability of the cryptosystem against attacks based on the adaptively selected encrypted messages (IND-CCA2 security). Note that the very padding scheme is used in [1].

Three functions are used in the encryption and decryption algorithms shown below:

$$F : Message \times Random\ bits \to R / 3 ,$$

$$G : Message \times Random\ bits \times Public\ key \to \{ r \in R / 3 : \| r \|_\infty = 2t \} ,$$

$$H : R / q \to R / 3 ,$$

The first function is a reversible mapping, that is, so that each of the functions F and F^{-1} has a fast computation algorithm, and the last two are constructed on the basis of keyless, but stable, hash functions.

Encryption algorithm [1].

Input: natural numbers l_1, l_2; public key h, message $M \in \{0,1\}^{l_1}$.

1: **repeat**

2: generate a random equiprobable vector $b \in \{0,1\}^{l_2}$.

3: calculate $r = G(M, b, h)$, $m = (F(M, b) + H(rh (\mathrm{mod}\, q))) \bmod 3$.

4: **until** each of the number of coefficients of the polynomial m equal to 1, −1 and 0, respectively, is at least t.

5: calculate $E_h(m, r) = (m + rh) \bmod q$.

Output: encrypted message $c = E_h(m, r)$.

Decryption algorithm.

Input: private key (f, g), public key h; encrypted message $c \in R / q$.

1: put $m' = D_f(c) = (cf(\bmod q)) \bmod 3$, $\tilde{r} = (c - m') \bmod q$;

2: calculate $(M', b') = F^{-1}\left((m' - H(\tilde{r})) \bmod 3\right)$, $r' = G(M', b', h)$;

3: **if** $\tilde{r} = (r'h) \bmod q$ and each of the numbers of the polynomial m' coefficients equal to 1, -1 and 0, respectively, are at least no less than t, then $M = M'$;

4: **else** $M = \perp$

5: **end if**

Output: M.

Based on the results of 2.2, the presented encryption scheme ensures that there are no errors in messages decoding.

4. Selection (generation) of parameters

Algorithms for generating parameters for classical NTRU and NTRUPrime are given in [1, 2, 4, 7, 11] and others. In all the papers devoted to the generation of parameters, the parameters are formed for cryptographic stability up to 256 bits inclusive. The feature of this subsection is that it considers the construction of general parameters of the ASC and KEP for cryptographic resistance 2^{512} against classical attacks and 2^{256} against quantum attacks, using the techniques outlined in other works.

According to the cryptographic transformation scheme given in subsections 1 and 2, the following parameters should be selected:

- a prime number *n*, which defines the order of a polynomial;
- parameter *t*, which determines the number of non-zero elements in a small polynomial;
- parameter *q*, which defines a module for polynomial coefficients that specifies an public key. The same module is used for cryptographic transformations of encryption and decryption.

4.1. Selection of a minimum prime *n*

To select a minimum prime number, let us consider the attacks associated with using the sieve. According to [14, 15], the minimum prime number must satisfy inequalities

$$2^k \le (3/2)^n \tag{19}$$

For resistance against classical attacks, *k*=512 we obtain a minimum of *n*=877.

4.2. Selection of the parameter *t*

The task of restoring a private key $(f = (1 + 3F) \bmod q, g)$ under the public key h of a cryptosystem is reduced to solving an equation $(h' + 3Fh') = G$ for unknowns $F, G \in \frac{R}{3}$, where $\| F \| = 2t$ and $h' = (3^{-1} h) \bmod q$. This problem can be formulated as follows.

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

$$\| (h' + 3Fh') \bmod q \|_\infty = 1 \tag{20}$$

The complexity of solving a given task by a complete overview of all polynomials $F \in \Phi$ requires $| \Phi | = 4^t \binom{n}{2t}$ operations.

The given function increases monotonically with the increase in *n*. The value $\log_2|\Phi|=1088$ corresponds to the minimum *n*=883 and *t*=145 (choice of *t* is discussed below), which almost 2 times exceeds the required complexity.

To reduce the complexity you can apply attacks under the general name “meet-in-the-middle attacks”.

Depending on the cryptosystem, there are various estimates of the complexity of this attack. To ensure the stability of the cryptosystem under consideration, with respect to the meet-in-the-middle attacks, the values of n and t are selected for a given security parameter k based on the condition

$$2^k \le 2^{t+1}\binom{n}{2t}^{1/2}. \tag{21}$$

The value t, obtained by formula (21), limits the cryptostability value k above, that is, to provide a guaranteed possibility to achieve a predetermined value of k, taking into account other attacks, it is necessary to set the value k with the stock to calculate the value of t in formula (21). That is, the value $k + \Delta k$ should be used instead of $k = 512$ in formula (21). The value of the parameter $\Delta k = k / 2$ has been experimentally found in the calculation of parameters.

4.3. Selection of *q* parameter

To exclude the decryption error, you must choose a prime number for the given n and t

$$q \ge 48t + 3 \tag{22}$$

such that the polynomial $x^n - x - 1$ is irreducible over the field Z_q.

One set of values (n, t) corresponds to many q values. The performed analysis showed that q value choice may affect the length of the message being encrypted, because the increase in q value increases the number of bits for its internal appearance. As our calculations have shown, it is enough to choose the smallest q, which satisfies formula (22).

4.4. Attack on the lattice

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

$$\begin{pmatrix} 1 & 0_{1\times n} & h' \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}. \tag{23}$$

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

To assess the attack on the lattice (construction of the reduced base B of the lattice the traditional approach is use [8]. It is believed that the base B is constructed using the block algorithm of Korkin-Zolotarev: BKZ 2.0 [13]. 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 us to construct a base of the complete N-dimensional lattice for $C = 2^{E(\beta, m, N)}$ operations reduced according to Korkin-Zolotarev, where

$$E(\beta, m, N) = 0,000784314\ \beta^2 + 0,366078\ \beta + \log(nm) + 0,875. \tag{24}$$

The values of β, m are found using the BKZ 2.0 emulator [13].

4.5. Essence and vulnerability of a combined attack

Previous studies have shown that among the potential analytical attacks the combined (hybrid) attack is the most vulnerable one [9].

The essence of the attack is as follows. First, the base of the lattice (24), which corresponds to the algorithm, is divided into 2 parts. The first part is used to attack the lattice, the "meet-in-the-middle" attack is applied to the second part. To determine the parameters there is such a division option, for which:

- cryptostability for each type of attacks provides the necessary value;
- attacks require about the same time, this time is defined as the cryptostability of the system against a combined attack.

In [9] a formula was got for evaluating the complexity of the "meet-in-the-middle" attack depending on the number of base rows used for this attack. A similar attack is considered in [7], where another formula is provided. Different formulas relate to the fact that methods of analytical calculation of this complexity are not known. We used both methods in our implementation. With regard to the method for determining the complexity for the lattice, in these works and others, the BKZ 2.0 emulator is used.

Table 1 demonstrates the results of determining the parameters for the cryptosecurity of 512 bits.

Table 1

Parameters for cryptosecurity of 512 bits

n	t	q	r	T'_{MITM}	T''_{MITM}	$T_{Lattice}$
1259	210	10103	752	512	469	513
1283	214	10289	797	541	494	513
1289	215	10331	808	548	501	513
1291	215	10331	812	549	503	513
1297	216	10453	823	556	510	512
1301	217	10427	830	562	514	514
1303	217	10429	835	564	517	513
1307	218	10499	842	570	522	513
1319	220	10567	866	584	537	512
1321	220	10597	867	585	537	514
1327	221	10613	881	592	546	512
1361	227	10957	943	630	585	512
1373	229	11057	965	644	599	513
1381	230	11059	981	653	608	513
1399	233	11213	1014	674	629	514
1409	235	11299	1035	689	642	512
1423	237	11383	1059	704	657	514
1427	238	11437	1068	711	663	512
1429	238	11443	1072	712	665	512

Notations in the Table:

n – degree of the polynomial;

t – determines the number of non-zero elements in the secret key (dazzling polynomial);

r – the number of rows of the base for which the "meet-in-the-middle" attack is performed;

T'_{MITM} – the complexity of the attack, according to [9] (Bit);

T''_{MITM} – the complexity of the attack, according to [7] (Bit);

$T_{Lattice}$ – the complexity of the attack on the lattice (Bit).

Gray colors highlighted the values of the parameters for which both methods gave a positive result.

The results of the detailed analysis of the combined (hybrid) attack are given in [9]; it is assumed that, when implemented with protection from it, IND-CCA2 semantic resistance to quantum attack is provided.

Conclusions

1 In the future the cryptographic transformations of the ASC, KEP of 6-7 levels of stability type will be demanded. Under 6 security level, it is suggested to understand resistance against 384 bits of classical cryptographic stability and 192 bits of quantum cryptographic stability, respectively, and under 7 security level l, it is suggested to understand resistance against 512 bits of classical cryptographic stability and 256 bits of quantum cryptographic stability, respectively.

2. The implementation of 6-7 levels of stability is associated with the complex problem task of generating common parameters and keys for cryptographic transformations in the ring of polynomials over the finite fields for recognized and accepted security models.

3. There is a need for a reasonable decrease in the value of q, first of all for ASC 6 and 7 levels of cryptographic stability.

4. Unambiguous encoding (7) and decoding (8) is ensured for any of the above key data f, g, h, r and message m.

5. Following inequalities are fair for any $u, v \in R$

$$\| uv \|_\infty \le 2 \| u \|_\infty \| v \|_1 , \quad \| uv \|_\infty \le 2 \| u \|_2 \| v \|_2 .$$

6. According to the proposed scheme of cryptographic transformations, it is necessary to choose the following parameters:

- prime number n, which determines the order of the polynomial;
- parameter t, which determines the number of non-zero elements in a small polynomial;
- parameter q, which defines a module for polynomial coefficients that specifies a public key.

7. The results of determining the parameters for the cryptosecurity of 512 bits are shown in Table. 1 of this paper. It is believed that a combined attack is the most vulnerable to the ASC, IND-CCA2 semantic resistance to quantum attack is provided, while protecting against it.

References:

1. American National Standard X 9.98-2010. Lattice-Based Polynomial Public Key Encryption Algorithm Part 1: Key Establishment: Part 2: Data Encryption, 2010.

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

3. I. Gorbenko, O. Kachko, K. Pogrebnyak. Features of parameters calculation for NTRU algorithm // Прикладная радиоэлектроника. – 2015. – V. 14. – № 3. – P. 272-277.

4. Gorbenko I.D. General Provisions and Analysis of NTRU Prime IIT Ukraine Directional Encryption Algorithm / I.D. Gorbenko, E.G. Kachko, M.V. Yesina // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – Kharkiv : KNURE. – 2018. – № 193. – P. 5-16.

5. DSTU 7624: 2014. Information Technology. Cryptographic protection of information. The algorithm of symmetric block transformation. [On-line]. Internet: http://shop.uas.org.ua/ua/informacijni-tehnologii-kriptografichnij-zahist-informacii-algoritm-simetrichnogo-blokovogo-peretvorennja.html.

6. Gorbenko I., Kuznetsov A., Lutsenko M. and Ivanenko D. The research of modern stream ciphers // 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). – Kharkov, 2017. – P. 207-210.

7. Bernstein D.J. NTRU Prime / Bernstein D.J., Chuengsatiansup Ch., Lange T., van Vredendaal Ch. // [Electronic resource]. – Access mode: http://eprint.iacr.org/2016/461.

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

9. Wunderer Th. Revising the hibrid attack: improved analysis and refined security estimates // http://eprint.iacr.org/2016/733.

10. Howgrave-Graham N. NAEP: provable security in the presence of decryption failures / Howgrave-Graham N., Silverman J.H., Singer A., Whyte W. // [Electronic resource]. – Access mode: http://eprint.iacr.org/2003/172.

11. Choosing Parameters for NTRUEncrypt Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman , William Whyte, and Zhenfei Zhang// [Electronic resource]. – Access mode: https://eprint.iacr.org/2015/708.pdf.

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

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

14. Becker A., Ducas L., Gama N., Laarhoven Th. New directions in nearest neighbor searching with application to lattice sieving // SODA 2016. – Proccedings. SIAM, 2016. – P. 10 – 24.

15. Laarhoven Th. Sieving voe closest lattice vectors (with preprocessing). [Electronic resource]. – Access mode: https://arxiv.org/pdf/1607.04789.pdf.

JSC "Institute of Information Technologies", Kharkiv;
Institute for Special Communications and Information Protection
of the National Technical University of Ukraine "Igor Sikorsky
Kyiv Polytechnic Institute";
V.N. Karazin Kharkiv National University;
Kharkiv National University of Radio Electronics

Received 02.10.2018