ПЕРСПЕКТИВНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ И ПРОТОКОЛЫ

UDC 519.2:519.7

I.D. GORBENKO, Dr. Sc.,(Tecnology), O.G. KACHKO, Cand. Sc. (Tecnology),
Yu.I. GORBENKO, Cand. Sc. (Tecnology), I.V. STELNIK, S.O. KANDYI,
M.V. ESINA, Cand. Sc. (*Tecnology*)

METHODS OF BUILDING GENERAL PARAMETERS AND KEYS FOR NTRU Prime Ukraine OF 5th – 7th LEVELS OF STABILITY. PRODUCT FORM

Introduction

There is now a reasonable suspicion that in the post-quantum period, existing standards for asymmetric cryptographic transformations are likely to be broken up by a third-level crypt analyst with polynomial or sub-exponential complexity using quantum cryptanalysis systems [1 – 5]. An important feature of the post-quantum period is the significant uncertainty regarding the source data for cryptanalysis and counteraction – basically, in our opinion, in terms of the capabilities of quantum computers, their mathematical and software resources, as well as applications for cryptanalysis and the implementation of potentially possible attacks [1, 4 – 5]. Therefore, in the future, in the post-quantum period, cryptographic transformations and cryptographic protocols that will be stable both against classical and possible quantum crypto analytic systems should be applied. The indicated problem of creating and standardizing asymmetric cryptographic transformations that will be stable, both against classical and against quantum attacks, is extremely important and should be solved before the post-quantum period. Previous studies have shown that significant prospects for constructing asymmetric cryptographic transforms such as asymmetric cipher (ASC), key encapsulation protocol (KEP), and digital signature (DS) have cryptographic transformations based on the use of quantum polynomials over finite fields [6 – 8]. Due to the fact that algebraic lattices are among the effective attacks on the indicated transformations, the asymmetric transformations of the ASC, KEP and DS are also called as those ones based on “algebraic lattices”

The following cryptographic transformations: NTRUEncrypt ANSI X9.9 8 [9, 14]; NTRU prime [6, 16] and NTRU Prime Ukraine [10] are historically important achievements in the application of the “algebraic lattices”. The construction of the ASC and KEP projects with cryptographic stability of 1st -5th levels of stability is the maximum achievement in the first two directions. At the same time they require ASC, KEP and DS of the 6th – 7th levels, rather, for the post-quantum period, taking into account possible new achievements in the construction of quantum computers and their mathematical support and software. Moreover, under the 6th level of security, we will understand the resistance against 384 bits of classical cryptographic stability and 192 bits of quantum cryptographic stability, respectively, and under the 7th level of security we will understand the resistance against 512 bits of classical cryptographic stability and 256 bits of quantum cryptographic stability, respectively. The need for such levels of stability can also be explained by the standards of symmetric crypt-transforms [17], which provide 256 bits of quantum stability and a consistent application of both symmetric and asymmetric cryptographic transformations.

The results of the analysis showed that when constructing the ASC and KEP of the 6th – 7th levels it is necessary to solve the following problematic tasks:

- justification of methods for investigation and construction with their use of general parameters of cryptographic transformations;
- justification of methods and generation of asymmetric key pairs;
- justification of the method and implementation of direct and inverse cryptographic transformations of encryption and decryption;
- comparative analysis and decision-making on the choice of mechanisms of the ASC of the 6th-7th levels of cryptographic stability.

The purpose of this paper is to propose solutions to the first and second tasks, that is, methodological considerations and construction with their use of general-system parameters and keys of crypto-transformations of the ASC and the KEP of the 6th – 7th levels of stability, as well as experimental confirmation by means of software modeling in the case of using PRODUCT FORM [14] for private keys and blinding polynomial.

1. List and essence of general-system parameters and keys

Below is the essence and list of general-system parameters of the cryptographic transformations of the ASC and KEP of the 6th – to 7th levels of stability in the ring of polynomials over the finite field. When considering, we will focus on standard references and consider, respectively: NTRUEncrypt ANSI X9.98 [9, 14], NTRU Prime [6, 16] and NTRU Prime Ukraine [10].

The NTRU Prime Ukraine NSRU mechanism is a NTRU-like cryptosystem that is promising for use in the post-quantum period. The NTRU cryptosystem was chosen for several reasons. It is fully compliant with IEEE P1363 standards according to lattice-based public key cryptography specifications (IEEE P1363.1). The NTRUEncrypt cryptosystem provides high-speed and low-resource memory usage, and can be used in applications such as mobile devices and start-up cards. In April 2011, NTRUEncrypt was accepted as the ANSI X9.98 standard for use in financial services, currently it's tested by time. Taking into account known possible attacks, NTRU Prime Ukraine uses new parameters, such as those proposed in [6,16]. In addition, some reduction in the computational complexity of the ASC has been achieved. Algorithmic optimization and capabilities of modern computer systems (AVX-operations, parallelization, etc.) were used for optimization.

General-system parameters and keys, destination and formulas for their calculations are given in Tables 1, 2 [6 – 10].

Table 1

General-system parameters of ASC NTRU Prime

Notation	Use	Formula
$(Z/q)[x]$	Ring of polynomials Each element Z/q is usually encoded in $\lceil \log_2 q \rceil$ bit. Reduction is allowed due to the packaging of several elements in one	
n (N)	Polynomial order. Determines the number of its coefficients. A prime number for which the polynomial $x^n - x - 1$ is irreversible	$n \geq \max\{3, 2t\}$
P	Monic polynomial of n degree, irreducible over the field $(Z/q)[x]$, by which polynomials are reduced – elements of R/q field	$x^n - x - 1$
R	Ring of polynomials $Z[x]$ over a finite field with a module $x^n - x - 1$	$Z[x]/(x^n - x - 1)$
$R/3$	Ring of polynomials $(Z/3)[x]$ over a finite field with a module $x^n - x - 1$	$(Z/3)[x]/(x^n - x - 1)$
R/q	Ring of polynomials $(Z/q)[x]$ over a finite field with a module $x^n - x - 1$	$(Z/q)[x]/(x^n - x - 1)$
p	Smaller module, which reduces all the coefficients of the R / 3 polynomial	$p = 3$
t	The natural number, the number of nonzero elements of T polynomial depends on this parameter.	$t \geq 1$, T = 2t
q	Larger module, the prime number, by which all the coefficients of the polynomial R/q are reduced	$q \geq 48t + 3$
k	Level of cryptostability	256, 384, 512

It should be noted that $R/3 \subset R/q \subset R$ as plurals.

A small element is also *t*-small if it has exactly 2*t* nonzero coefficients.

The number of non-zero elements in the private key and in the blinding polynomial is determined by *n* and the cryptostability *k*, which must be ensured. For all parameters they are identical and equal to T.

Table 2

Parameters and keys required for generating keys

Notation	Use	Formula
G	Random small polynomial, reversible in $R/3$. The number 1 and -1 is not necessarily equal. The secret parameter used to calculate the public key.	G € R/3 T=2n/3+1
F	Random t-small polynomial that defines a private key	$F \in R/3$ *T=2t*
f	A small polynomial, irreducible in R/q, is a private (personal) key.	$f = (1+3F) \bmod q \;\; f \in R/q$
h	The sender's public key.	$h = 3g / f \in R/q$
$\underline{h}$	h encoded in a row	The length $\underline{h}$ is equal to $n\lceil \log_2 q \rceil$

2. Presentation of elements of polynomials ring over a finite field

For any odd number l we denote the ring Z_l of classes of residues by the module l. Further, the elements of this ring are identified with the integers belonging to the segment $\left[-1/2(l-1), 1/2(l-1)\right]$. In particular, for any $a \in Z$ the record $a \bmod l$ denotes a single integer $a' \in \left[-1/2(l-1), 1/2(l-1)\right]$ such that $a \equiv a' \bmod l$.

Let us fix a natural number t and different prime numbers n, q such that $n \geq \max\{3, 2t\}$, $q \geq 48t+3$ and the polynomial $x^n - x - 1$ is irreducible over the field Z_q. Let's also mark

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

Let's consider that $R/3 \subset R/q \subset R$ as plurals.

From the above conditions, it follows that the ring R/q is a ring of polynomials over a finite field, which consists of q^n polynomials of the form $u = u_0 + u_1 x + \cdots + u_{p-1} x^{n-1}$, where u_i there are integers of the interval $\left[-1/2(q-1), 1/2(q-1)\right]$, $i \in \overline{0, n-1}$ which are added and multiplied by the modulum q. In this case, the addition and multiplication of the polynomials themselves (elements of the field R/q) takes place by the modulus of the polynomial $x^n - x - 1$.

For any polynomial $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in R$ denote $u \bmod q$ by the polynomial $(u_0 \bmod q) + (u_1 \bmod q)x + \cdots + (u_{n-1} \bmod q)x^{n-1} \in R/q$. $u \bmod 3$ notation has also a similar meaning.

Let us assume that $u \in R$ is called *small* if $u \in R/3$. A small polynomial will be called t-*small* one if it has exactly $2t$ nonzero coefficients.

Also, for any polynomial $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in R$ we denote in the form

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

In the future, we will use similar notation for an arbitrary vector $u = (u_0, u_1, ..., u_{n-1}) \in R^n$.

In this work, as is customary in similar works, the notations are used:

$$\binom{a}{b} = \frac{a!}{b!*(a-b)!};\ \binom{a}{b \quad c} = \binom{a}{b} * \binom{a-b}{c} \tag{2}$$

3. Method for calculation of general-system parameters and keys OF 6th AND 7th stability levels in F1 * F2 + F3 form (product form)

The performed analysis showed that, when using the special form of the task of the secret (private) key [11, 14], there is a possibility to reduce significantly the complexity (time) of such a key generation and the main operations associated with the generation of the public key, and performance of asymmetric encryption and decryption with stability of 128, 192 and 256 bits versus quantum attacks (256, 384, and 512 bits of classical attacks, respectively).

3.1. General statements

An algorithm for generating parameters is proposed in [11]. It is proposed for generating parameters with a maximum cryptostability of 256 bits for classical attacks (128 against quantum attacks) for a classical NTRU algorithm with a polynomial X^n-1 and a value $q = 2^m$, where the product form is used for the private key F and the polynomial r. The algorithm for formation of parameters for a polynomial x^n-x-1 is given in [6, 16]. It uses the standard polynomial format as an array of 1, -1, 0 with a limitation of cryptostability to K = 300 for classical attacks. In addition, the algorithms NTRUPrime [6, 16] and NTRUPrime Ukraine, considered in this work, use different algorithms for the formation of keys and cryptographic transformations, therefore there is a need for studying algorithms for generating parameters. In [15] the algorithm is presented and parameters for the 5th – 7th levels of stability for the usual polynomial problem are calculated. This paper is devoted to the algorithmic analysis of parameters generation for the 5th – 7th levels of stability in the case of using the product form that meets the requirements for a post-quantum ASC to provide 384 and 512 bits of cryptostability with respect to classical attacks and, respectively, 192 and 256 for quantum attacks.

The generation parameters, to provide 384 (192) and 512 (256) bits for the specified data, can be given in the following sequence [11 – 16]:

- choice of a prime number of n – degree polynomial;
- formation of key space for private keys;
- calculation of the maximum number of non-zero elements in the message;
- computing the security parameter based on the key space and the meet-in-the-middle attack (upper security boundary);
- calculation of the larger module *q;*
- calculation of the complexity (time) of a hybrid attack.

3.2. Choice of the degree of the polynomial *N*

A prime number is used as a polynomial degree. To select a minimum number, let us consider the attacks associated with the use of the sieve. According to [12], the minimum prime number must satisfy inequality:

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

For stability against classical attacks, k = 384, we obtain a prime number N = 659, and for a critical stability 512 we obtain a prime – N = 877. But, in accordance with [11], the minimum value of n for reciving cryptostability, which is not less than 256, is 743, exactly this value will be used as the minimum N.

3.3. Formation of key space for private keys

The transition to the cryptostability of the 6th and 7th levels requires an increase in the order of the polynomials N. This, in turn, leads to an increase in the computational complexity of the multiplication operations for these polynomials. In order to reduce this effect, for the representation of small polynomials, instead of the usual one, a special form of the polynomial (product) [11] is used: $F=F_1*F_2+F_3$, for specification of which 3 polynomials are used: F_1, F_2, F_3. Each of them is a small polynomial, with an equal number of units and minus units, this number is, respectively, equal to d_1, d_2, d_3. By analogy with t-small ones, these are d_1, d_2, d_3 small polynomials. But the number of units and minus units in them are the same. To obtain a polynomial F, we perform the multiplication operation of the polynomials F_1, F_2 followed by the modulation of the X^n-X-1 and the addition of the polynomial F_3.

The maximum number of nonzero elements for polynomial F: $2d_1 * 2d_2 + 2d_3$. The value of nonzero coefficients of a polynomial F may differ from the values of nonzero coefficients of the t-small polynomial, which extends the key space of the polynomial F with the appropriate choice of d_1, d_2, d_3.

To select d_1, d_2, d_3 authors [11] recommend the use of the following algorithm:

Let the values d_1, d_2, d_3 be respectively chosen for the polynomials F_1, F_2, F_3.

In order the search for keys, using the polynomials F_1, F_2, F, was approximately of the same complexity, we choose $d_1 \approx d_2 \approx d_3$.

To balance the number of zeros and nonzero elements d_1, d_2 and d_3, the condition $2d_1 * d_2 + d_3 \approx$ N/3 must be satisfied, i.e., the value d_i is the positive root of the equation: $2d^2+d-N/3=0$, whose solution for a positive value d:

$$d_1 = \left\lceil \frac{-1+\sqrt{1+\frac{8N}{3}}}{4} \right\rceil;$$

$$d_2 = \left\lceil \frac{\frac{N}{3}-d_1}{2d_1} \right\rceil \qquad (4)$$

$$d_3 = \max \left\lceil \begin{matrix} \frac{d_1+1}{2} \\ \frac{N}{3}-2d_1d_2 \end{matrix} \right\rceil$$

But for practical purposes, the authors [11] used formulas (4) to find d_1, d_2. And values of d_3 were chosen more than d_1, d_2. Thus, for N = 743 from formulas 4 we get d_1, d_2=11, d_3=6, and according to Table 3 [11] for N = 743 the values d_1, d_2 = 11, d_3 = 15. This is probably due to the need to increase the key space to provide the required cryptostability against the MITM attack.

In the future, we use the following formula for calculation:

$$d_1 = d_2 = \left\lceil \frac{-1+\sqrt{1+\frac{8N}{3}}}{4} \right\rceil; \qquad (5)$$

The value of d_3 is determined so that at N close to N, obtained for the usual form of setting keys, to provide the necessary cryptostability, when using the Product Form [15].

For N = 743 the values of d_1, d_2 =11, d_3 = 15 [11].

Regarding the key G, the usual method of setting 1 and -1 elements is used for its setting. To provide the maximum key space for this key, the number of units is N/3 +1, the number of minus items is N/3. When calculating N/3, it may be a rejection of a fractional part or a rounding. For example, rounding is used in [11], while the fractional part is thrown away in EESS # 1 [14].

In the course of the research, both methods were considered and it was discovered experimentally that the choice of the method did not actually affect other parameters.

3.4. Calculation of the maximum number of nonzero elements in the message

When encrypting the data the disguised message, converted into a small polynomial, should contain a sufficient number of non-zero elements, defined by d_m parameter to protect against attacks. On the other hand, if the number of non-zero elements is large, then the probability of re-selecting a mask and multiplying by a blinding polynomial will be high. This factor greatly affects the computational complexity of encryption.

To select the maximum possible value of d_m, where the probability of repeated execution of the multiplication operation does not exceed 2^{-10}, the formula [11] is used:

$$2^{-10} \geq 1 - \frac{\sum_{i=d_m}^{N-2d_m-1}\left(\sum_{j=d_m}^{N-d_m-i}\left(\binom{N}{i}\binom{N-i}{j}\right)\right)}{3^N} \tag{6}$$

For N=739, we get d_m=205, which coincides with [11].

3.5. Calculation of the security parameter based on the key space and the meet-in-the middle attack (upper security boundary)

To calculate the security parameter, taking into account the key space and meet-in- the middle attack, the number of keys, taking into account their form of representation and the meet-in-the middle attack, is determined.

For this purpose, the square root of this quantity is calculated, that is, [11]

$$O\left(\sqrt{\frac{\left({}_{d_1}{}^{N}{}_{d_1}\right)*\left({}_{d_2}{}^{N}{}_{d_2}\right)*\left({}_{d_3}{}^{N}{}_{d_3}\right)}{N}}\right); \tag{7}$$

where $\left({}_{d}{}^{N}{}_{d}\right)$ – is the number of keys, taking into account the number of (1) and (-1), that is

$$\left({}_{d}{}^{N}{}_{d}\right) = \binom{N}{d} * \binom{N-d}{d} \tag{8}$$

In (7) the division into N takes into account the possibility of cyclic transformation (automorphism) of the key.

Inequality [11] is used to determine the minimum prime number that provides the required cryopresistance *k*.

$$2^k \leq \sqrt{\frac{\left({}_{d_1}{}^{N}{}_{d_1}\right)*\left({}_{d_2}{}^{N}{}_{d_2}\right)*\left({}_{d_3}{}^{N}{}_{d_3}\right)}{N}} \tag{9}$$

This formula is used to calculate d_3 for N. If $d_3 > 3d_1$, then the next N is chosen. The latter condition is related to the efficiency of multiplying the polynomials given in the product form..

As the calculations show the condition (9) is much stronger than the condition (3), which we used previously to determine the minimum prime number. The results of the determination of N and the values of d_1, d_2, d_3 for cryptostabilities 256, 384 and 512 are given in Table 3 after the definition of q.

3.6. Ensuring no errors in decoding. Formation of q

In [11], the mechanism of the ASC of the transformation is determined, which basically coincides with the ASC transformation for NTRUPrime Ukraine, with the exception of using the algorithm of the field $R/q = Z_q[x]/(x^n - x - 1)$ in the last instead of the ring (Z / qZ) [X] (XN-1) and simple q instead of q = 2^m.

When encrypting/decrypting, the following operations are performed:

$$E_h(m,r) = c = (m + rh) \bmod q\,,\ m, r \in R/3, \text{h €R/q} \tag{10}$$

$$D_f(c) = (cf (\bmod q) \bmod 3,\ c \in R/q \tag{11}$$

Sufficient conditions for error-free decryption are also defined, which set restrictions for the module q

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

Consider the condition (7) for the case of using the product form for the keys F and *r*.

Let $r = r_1 * r_2 + r_3$, $F = F_1 * F_2 + F_3$ where $r_1, r_2, r_3, F_1, F_2, F_3$ d – are small polynomials. In this case $\|\mathrm{r}\|_1 \leq \|r_1\| * \|r_2\| + \|r_3\| = 4d_1 * d_2 + 2d_3$; $\|\mathrm{F}\|_1 \leq \|F_1\| * \|F_2\| + \|F_3\| = 4d_1 * d_2 + 2d_3$, where d_1, d_2, d_3 – are the number of 1 (-1) in the plynomials. Then the condition (7) $\| mf + 3rg \|_\infty < q/2$ taking into accounta $\| m \|_\infty = \| g \|_\infty = 1$, f = 3F + 1, and values $\|\mathrm{r}\|_1, \|\mathrm{F}\|_1$, can be presented in the form of:

3(8d$_1$d$_2$+4d$_3$) <q/2 – 1. From here

$$q \geq 24(2d_1d_2+d_3) + 3. \qquad (13)$$

Thus, if a product form is used, the value q is determined by the values d$_1$, d$_2$, d$_3$. The minimum value of q is determined from the inequality (8). In addition, the value q must be prime and such that the polynomial $x^n - x - 1$ is irreducible over the field $\mathbf{Z}_q$.

Table 3 lists the parameters that provide the required cryptographic stability and the absence of decryption errors without taking into account the combined attack.

Table 3

Values of parameters that provide
the required cryptostability and lack of decryption errors

K	N	d$_1$	d$_2$	d$_3$	d$_m$	q
256	743	11	11	15	205	6263
384	1019	13	13	31	290	8867
512	1409	16	16	43	411	13327

3.7. Calculation of complexity (time) of hybrid attack execution

The calculation of complexity (time) is performed in the following way. Matrix-base is divided into 2 parts. One part of the length of the r lines is used to search the key part with the help of “meet-in-the middle” attack, the other, using the length 2N-r, is processed as part of the lattice. Finding the optimal r, in which the “meet- in-the middle” attack and attack on the lattice gives roughly the same time, that exceeds the needed one, taking into account the required cryptosecurity.

3.7.1. Meet- in-the middle attack

As a search object, you can select F key, for which the product form is used and G key, for setting of which the regular polynomial F/3 is used with a number of N/3 + 1 units and -1 N/3. Next $d_G = \frac{N}{3}$. If key G is found, then it is easy to find G^{-1}, and then F.

Next, let’s consider the use of G key for search. The number of rows of the base, for which *r* search is performed, and the number of -1 in key G (d_G) are used as search parameters. The method from [11] is used to determine the time complexity of a hybrid attack.

To prevent the message from being reproduced, a combined attack is also considered with respect to a polynomial having d$_m$ units (minus units).

The method of using a combined attack for key G and message M is the same, so it is further described for key G. The minimum time, required for both attacks, is taken as the final result.

First, the key space is defined, that is, the total number of keys G

$$Total = \binom{N}{d_G + 1 \quad d_G}$$

To determine the probability of the presence of *a* units and b -1 in the selected base area, the following formula is used:

$$P(v(a,b)) = \frac{\binom{N-r}{d_G+1-a \quad d_G-b}}{Total}$$

The probability $P(v(a,b))$ is used to calculate the number of H (p) versions, that should be considered:

$$H(P) = -\sum_{\substack{0 \le a \le d_G+1, \\ 0 \le b \le d_G}} \binom{r}{a \quad b} P(v(a,b)) log_2 P(v(a,b))$$

Taking into account the specifics of the “meeting-in-the middle” attack and the possibility of cyclic keys permutations, the general formula for calculating the time for the “meeting-in-the middle” attack is:

$$T_{MITM}(N, r,\ d_G) \ge 0.5(H(P) - \ log_2 N); \qquad (14)$$

$T_{MITM}(N, r,\ d_m)$ is determined similarly.

Table 4 shows the calculation results of $T_{MITM}(N, r,\ d_G)$ for cryptostability of the 6th and 7th levels for d_G and d_m

Table 4

Combined attack. MITM (6th and 7th levels of cryptostability)

K	N	d_G	$T_{MITM}(N, r, d_G)$	r(d_G)	d_m	$T_{MITM}(N, r, d_m)$	r(d_m)
256	743	247	256	329	205	256	338
384	1019	339	384	491	290	384	501
512	1409	469	512	653	411	512	661

The value r (d_m) is used for the next attack, it exceeds r (d_G) for all K values..

3.7.2. Attack on the lattice

Let the size of the lattice, for which the attack is performed, be S = 2N – r.

1. First, the Hermite constant is determined using the formula:

$$h = e^{\frac{\ln\sqrt{\pi eq/2}}{S}} \qquad (15)$$

2. The size of the block β and the iteration number m are sought for the lattice, for which the Hermite constant value is selected. The initial size of the block is 60, the final size is S. The BKZ-2 emulator [18] is used for searching.

3. The value of the attack on the lattice is determined, that is, the number of operations for the construction of Korkin-Zolotarev-reduced basis of a complete lattice of dimension S:

$$T_{Lattice} = 2^{E(\beta, m, S)}, \qquad (16)$$

where $E(\beta, m, S) = 0{,}000784314\beta^2 + 0{,}366098\beta + \log_2(Sm) + 0{,}875$

This time should not be less than the value that corresponds to the cryptostability K.

Table 5 shows the experimental results of calculation of $T_{Lattice}$, agreed with T_{MITM} for cryptostability of the 6th and 7th levels for $r = \max(\mathrm{r}(d_G),\ \mathrm{r}(d_m))$.

Table 5

Combined attack. Attack on the lattice
(Cryptostability of the 6th and 7th levels)

K	N	r	T_{MITM}	β	m	$T_{Lattice}$
256	743	338	256	342	18	232
384	1019	501	384	499	16	393
512	1409	661	512	758	17	744

As can be seen from Table 5 for K = 256 $T_{Lattice} < 256$, i.e., to achieve the cryptostability of 256 it is necessary to increase the value of N. For K = 384 and 512 values of $T_{Lattice} > K$, to determine the most effective attacks, it is necessary to agree the value of *r*.

According to the calculations, to ensure the cryptostability of K = 256 in case of using not only the MITM and attack on the lattice, it is necessary to choose the parameters

N= 787, d_1 =12, d_2 =12, d_3 =15, d_m =219, d_G =262

The first row of Table 5 shows these parameters:

K	N	r	T_{MITM}	β	m	$T_{Lattice}$
256	787	337	256	374	17	262

These are parameters used later for K = 256.

3.7.3. Calculation of time for hybrid attack

You can choose different ways to calculate the time for a hybrid attack.

1. By formula 12, find the minimum value of *r*, at which $T_{MITM}(N,r,\ d_G) \geq K,\ T_{MITM}(N,r,\ d_m) \geq K$. For *r*, determine the size of the lattice (S = 2N – r). Determine the time required for cryptanalysis in accordance with 3.7.2 for a lattice of a given size. If for the given S the $T_{Lattice} \geq K$ parameters are found, matching parameters for finding r is being performed, in which both times exceed K, and the difference between $T_{Lattice}$ and T_{MITM} is minimal.

2. Start calculations to determine the minimum size of the lattice S for which $T_{Lattice} \geq K$. For r = 2N-S determine $T_{MITM}(N,r,\ d_G),\ T_{MITM}(N,r,\ d_m)$ for the MITM attack. If the parameters $T_{MITM}(N,r,\ d_G) \geq K,\ T_{MITM}(N,r,\ d_m) \geq K$ are found. matching of the parameters is carried out as in the previous case.

3. Use an iterative algorithm, in which simultaneously execute the values $T_{MITM}(N,r,\ d_G),\ T_{MITM}(N,r,\ d_m)$, for the selected *r*. In this case, r is determined, in which all three values satisfy the condition of the cryptostability K and are the closest to each other. Such a method is used in [11, 6].

In the case of solution of the problem for cryptostability more than 256, the time for the solution of each task is essentially significant. We use the first way, as the most effective on the part of computational complexity.

The results for the hybrid attack after matching are given in Table 6.

Table 6

Hybrid attack

K	N	r	T_{MITM}	β	m	$T_{Lattice}$
256	787	343	260.69	371	18	259
384	1019	508	390.16	496	15	390
512	1409	817	633.39	684	16	633

4. Algorithm of calculation of general system parameters

The above justification allowed us to construct a set of general-system parameters for the post-quantum asymmetric cryptographic transformations of the ASC and KEP type experimentally by means of software simulation. The algorithm given below is intended for generating general-system parameters and a suite of parameters for the ASC on an algebraic lattice with resistance 2^{512} to classical attacks and 2^{256} against attacks based on a quantum attack. The algorithm is implemented taking into account the data given in [9]. Thus, the generation of parameters is proposed to be performed in such a sequence.

Input data: K Security Level

Output data: **N, $\mathbf{d_1, d_2, d_3}$, $\mathbf{d_G}$, $\mathbf{d_m}$, q**

1. Choose a prime number N (n) (Formula 3)
2. Calculate values d_1, d_2, d_3 (Formula 5)
3. Calculate a value $d_G = \frac{N}{3}$
4. Determine the cryptostability k (Formula 9), which is provided by the selected N, d_1, d_2, d_3. If k <K, then choose the next prime number N and proceed to step 2 of the algorithm
5. Calculate the value of d_m (Formula 6)
6. Calculate the value of q, which must satisfy the condition (Formula 8), be prime and such that the polynomial $x^n - x - 1$ is irreducible over the field $\mathbf{Z}_q$
7. Calculate the minimum value 0 <r ≤ N, at which $T_{MITM}(N, r,\ d_G) > K,\ T_{MITM}(N, r,\ d_m) > K$ are simultaneously executed (Formula 14). If there is no such value, then choose the next prime number and go to step 2
8. Calculate the size of the lattice S = 2N – r
9. Calculate $T_{Lattice}$ (Formula 16)
10. If $T_{Lattice} < K$, choose the next prime number and go to step 2
11. If $T_{Lattice} < K$, choose the next prime number and go to step 2 2
12. While $T_{Lattice} > T_{MITM}$
    a. r:=r + 1;
    b. Calculate $T_{MITM}(N, r,\ d_m)$ (Formula 12)
    c. Calculate $T_{Lattice}$ (Formula 14)

Table 7 provides a complete set of parameters for PRODUCT FORM representing the private key F and dazzling polynomial r (Cryptostability of the 6th and 7th levels).

Table 7

Parameters for NTRUPrime Ukraine
(Cryptostability of 6th and 7th levels).
PRODUCT FORM

K	N	d_1	d_2	d_3	dm	q
256	787	12	12	15	219	7307
384	1019	13	13	31	290	8867
512	1409	16	16	43	411	13327

Conclusion

1. In the future, in the post-quantum period, cryptographic transformations and cryptographic protocols that will be resistant to classical and possible quantum cryptographic analytical systems should be applied. The problem of creating and standardizing asymmetric cryptographic transformations that will be stable, both against classical and against quantum attacks, is pointed out, and it is extremely important and should be solved before the post-quantum period.

2. Previous studies have shown significant prospects for constructing asymmetrical cryptographic transforms such as asymmetric code (ASC), key encapsulated protocol (KEP) and digital signature (DS) have cryptographic transformations based on the use of rings of polynomials over finite fields.

3. Historically important advances in the application of "algebraic lattices" are the following cryptographic transformations as: NTRUEncrypt ANSI X9.9 8; NTRU prime and NTRU Prime Ukraine.

4. When using the special form F1 * F2 + F3 the private (personal key) task the possibility appears to reduce significantly the complexity (time) of generating such a key and the basic operations related to generating a public key, as well as performing asymmetric encryption and decryption with a resistance of 128, 192 and 256 bits against quantum attacks (256, 384 and 512 bits of classical attacks, respectively).

5. The substantiated and implemented algorithm for generating general-system parameters has allowed to construct a suite of parameters for the ASC on the algebraic lattice with a resistance of 2^{384},.. 2^{512} against classical attacks and 2^{192}, 2^{256} against attacks based on a quantum attack.

6. The performed simulation has allowed to obtain experimentally a set of general-system parameters for k = 384 and $k = 512$ for the post-quantum ASC.

References:

1. Neal Koblitz and Alfred J. Menezes A Riddle wrapped in an Enigma. Department of Mathematics, Box 353.350, University of Washington, Seattle, WA 98195 U.S.A. – Access mode: https://eprint.iacr.org/2015/1018.pdf.

2. 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.

3. 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.

4. 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.

5. Gorbenko Yu. I. Methods of construction and analysis, standardization and application of cryptographic systems: monograph / Yuri I. Gorbenko. – Kharkov : Fort, 2016. – 959 p. (In Ukr.)

6. 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.

7. NTRU Open Source Project [Electronic resource]. – Access mode: https://github.com/NTRU OpenSource Project/ntru-crypto.

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

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

10. Gorbenko I.D. General Provisions and Analysis of NTRU Prime IIT Ukraine Directional Encryption Algorithm / I.D Gorbenko, O.G. Kachko MV Yesina // Radiotechnika. – 2018. – № 193. – P. 5-16. (In Russ.)

11. Horstein J. Choosing Parameters for NTRUEncrypt / J.Horstein, J.Pipher, J.Schanck, J.Silverman, W. Whyte, Z. Zhang [Electronic resource]. – Access mode: https://eprint.iacr.org/2015/708.pdf.

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

13. Nick Howgrave Graham NTRU Cryptosystems Technical Report. Report #4, Version 2. A Meet-In-The-Middle Attack on an NTRU Private key / Nick Howgrave Graham, Joseph H. Silverman, William Whyte [Electronic resource]. – Access mode.

14. Efficient Embedded Security Standards (EESS) [Electronic resource]. – Access mode: https://github.com /NTRUOpenSourceProject/ntru-crypto/blob/e5655c2a10b74b5a0256ca849dbe85e4860f2eb5/doc/EESS1-2015v3.0.pdf.

15. Gorbenko I.D. Improved method for generating system-wide parameters for NTRU Prime Ukraine / I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, M.V. Yesina // Radiotechnika. – 2018. – № 195. – P. 5 – 16.

16. Daniel J. Bernstein. Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal NTRU Prime: reducing attack surface at low cost. [Electronic resource]. – Access mode: https://eprint.iacr.org/2016/461.pdf

17. 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.

18 Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better Lattice Security Estimates. [Electronic resource]. – Access mode https://www.iacr.org/archive/asiacrypt2011/70730001/70730001.pdf

JSC «Institute of Information Technologies»;
Kharkiv National V.N. Karazin University;
Kharkiv NationalUniversity of Radio Electronics

Received 06.11.2018