УДК 004.056.55 **DOI:10.30837/rt.2021.2.205.06**

V.A. KULIBABA, PhD student

PROCESSES AND METHODS FOR SELECTING SYSTEM-WIDE PARAMETERS AND ANALYSIS OF RESISTANCE AGAINST THIRD-PARTY CHANNEL ATTACKS FOR THE KEY ENCAPSULATION MECHANISM DSTU 8961:2019

Introduction

In recent years, there has been significant progress in the creation of quantum computers. If scalable quantum computers are implemented, it will jeopardize the security of most widely used public key cryptosystems. The most vulnerable are key schemes, i.e. digital signatures, based on factorization, discrete logarithms and elliptic curve cryptography. The main task now is to develop, evaluate, research and standardize asymmetric crypto transformations at the international level, including key encapsulation mechanisms (KEM), resistant to attacks by violators of the post-quantum period. Another important task is to further study the already adopted national standards of ACS and PIC on resistance to attacks by third-party channels, in particular to assess the dependence of the conversion time using the private key on the structure of the key bits.

The main efforts of the international cryptographic community to develop standardize and implement new post-quantum crypto transformations are centered around the NIST US competition – NIST PQC Standardization Process, which began in December 2016 [1].

Of the 82 submitted candidates, 69 were admitted to the 1st round of the competition. In January 2019, based on open discussion and feedback from the cryptographic community, NIST selected 26 algorithms for the second round [2], including 17 asymmetric encryption and/or KEM.

The state of development and standardization of key encapsulation protocols at the international level and in Ukraine

Of the NIST evaluation criteria, the most important is the algorithm security criterion. For the KEM algorithms, NIST in the program statement of the competition put forward requirements for "semantic security" of algorithms in terms of resistance to attacks with adaptively selected ciphertext, which is equivalent to the security model IND-CCA2. Given that meeting the more stringent requirements of the IND-CCA2 model for some algorithms may affect performance [3], NIST has also adopted algorithms that provide protection against attacks with selected ciphertext in the IND-CPA.

In July 2020, the 2nd stage of the competition ended and the start of the 3rd round was announced [3]. Fifteen candidates advanced to Round 3, of which 7 were selected as finalists and 8 as alternative candidates. In particular, the following KEM algorithms were selected as finalists: Classic McEliece, SABER, CRYSTALS-KYBER, NTRU. Alternative candidates were: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE. Of the 4 main finalists, NTRU, CRYSTALS-KYBER, SABER are based on algebraic lattices, which provided a basis for the assumption of including at least one of them in the standard.

In the report [3] the second most important requirement is speed, and for the candidates of the 3rd round will be considered as the speed of key generation, forward and reverse transformations, and the spatial complexity of public keys, digital signatures and ciphertexts computation. For KEM algorithms, the key generation time is considered to be on a par with the forward and reverse conversion times because a large number of applications use a new key pair for each session to provide perfect forward security. As a result, safety and performance requirements are currently the main ones considered for NIST's decision in the 3rd round of the PQC competition.

In [4], NIST recommended that developers focus on developing parameters for the stability levels 1–5 defined in [5], i.e. for the stability level of 128 bits of quantum and 256 bits of classical security. Despite this, at the national level it was substantiated [6] and set the task to develop an al-

gorithm for asymmetric transformation of the KEM type and parameter sets that would provide 7 levels of stability, i.e. 256 bits of quantum and 512 bits of classical security. In [7], the main algorithms for generating system-wide parameters, encryption and decryption for the advanced NTRU Prime IIT Ukraine KEM algorithm was substantiated.

Further issues of constructing system-wide parameters for the 7th level of stability, proving the correctness of the algorithm, as well as cryptographic stability are considered in detail in [7-9]. Subsequently, based on studies conducted in [6-10], the national standard DSTU 8961:2019 [11] was adopted.

The main parameters of DSTU 8961:2019 and the method of generation parameters for 7th stability level

The main parameters of the algorithm presented in Table 1 and Table 2. The whole set of parameters can be found in [8,10].

Table 1

General parameters

Definition	Description
$(Z/q)[x]$	Ring of polynomials. All the coefficients reduced by module *q*
$N \geq \max(3, 2t)$	Order of polynomial. Should be a prime number for which the polynomial $x^n - x - 1$ is irreversible. The order determines the number of its coefficients
$P = x^n - x - 1 \in (Z/q)[x]$	Monic polynomial of N degree, irreducible over the field $(Z/q)[x]$, by which polynomials are reduced – elements from R/q
$Z[x]/(x^n - x - 1)$	Ring of polynomials $Z[x]$ with a module $x^n - x - 1$
$(Z/3)[x]/(x^n - x - 1)$	Ring of polynomials $(Z/3)[x]$ with a module $x^n - x - 1$
$(Z/q)[x]/(x^n - x - 1)$	Ring of polynomials $(Z/q)[x]$ with a module $x^n - x - 1$
$p = 3$	Smaller module, all the coefficients reduced by this module in the *R/3* polynomial
$q \geq 48t + 3$	Larger module, all the coefficients reduced by this module in the *R/q* polynomial
$t \geq 1$	A natural number, the number of nonzero elements of a polynomial depends on this parameter.
$\lambda \in \{256, 384, 512\}$	The level of crypto strength of classical security
$m \in R/3$	Private message. The number of 0, 1, -1 greater or equal *t*.
$e \in R/q$	Encrypted message.
$G \in R/3$	Random *t*-small element (polynomial), reversible in *R/3* field. The number of 1 and -1 are not necessarily equal. The secret parameter used to calculate the public key
$f \in R/q; f = (1+3F) \bmod q$	A small polynomial, irreducible in *R/q*, is a secret key.
$F \in R/3$	A random polynomial that identifies a private key.
$dF = 2t/3$	Number of 1 and -1 in polynomial F
$df = 2t; df = dr$	Number of 1 and -1 in secret key, not necessarily equal.
$dg = \begin{cases} dg_1 = n/3+1 \\ dg_{-1} = n/3 \end{cases}$	Number of 1 and -1 in polynomial *G*

Table 2

Additional parameters

Definition	Description
$qBits = \lceil \log_2 q \rceil$	Number of bits in *q*
$r \in R/3$	Blinding polynomial, random t-*small*
$dr = n/3$	The number of 1 and -1 in Blinding polynomial
b	Random component (salt), to add to the message.
db=256	Length of the random component (bits).
$bLen = db/8$	Length of the random component (octets).
$\max MLen = \frac{\frac{3(N-1)}{2} - db}{8} - 1$	Maximum length of message for encrypt(bytes).
$Hlen = \begin{cases} 256, \lambda = 256 \\ 512, \lambda = 384 \| 512 \end{cases}$	Hash value length (bits)

The comprehensive algorithm description of calculation general parameters presented in [7, 8, 13]. A simplified sequence of steps can be represented as follows:

Step 1. Select prime number N.

As a prime number, prime N are chosen for which the order is N-1 or (N-1) / 2.

$$2^{\lambda} < (3/2^{N}) \tag{1}$$

Step 2. Formation of key space for private keys

To specify the key space, it is necessary to determine the number of nonzero N / 3 (1 and -1) elements in the polynomial *F = F1 * F2 + F3* and the keys G.

Then the maximum number of nonzero elements in the key defined[8] by the polynomial F = F1 * F2 + F3 taking into account the number (1) and (-1) is equal to

$$2d_1 * 2d_2 + 2d_3 = 4d_1d_2 + 2d_3 \tag{2}$$

In order to find the keys on the polynomials F1, F2, F3 was approximately the same complexity we choose

$$d_1 \approx d_2 \approx d_3$$

In [13] it is proposed to calculate the value according to formulas (3,4):

$$d_1 = \left\lceil \frac{-1 + \sqrt{1 + \frac{8N}{3}}}{4} \right\rceil, d_2 = \left\lceil \frac{\left\lceil \frac{N}{3} \right\rceil - d_1}{2d_1} \right\rceil, d_3 = \max\left(\left\lceil \frac{d_1 + 1}{2} \right\rceil, \left\lceil \frac{N}{3} - 2d_1d_2 \right\rceil \right) \tag{3}$$

$$d_g = \frac{N}{3} \tag{4}$$

Step 3. Calculation of security parameter taking into account key space and attack meeting in the middle (upper security boundaries)

To calculate the security parameter taking into account the key space and the attack of the meeting in the middle[8], the number of keys is determined taking into account their form of representation and the attack of the meet-in-the middle[14].

To determine the minimum prime number that provides the desired stability λ, the next inequality(5) is used [13]

$$2^{\lambda} \le \sqrt{\frac{\binom{N}{d_1 \quad d_1} * \binom{N}{d_2 \quad d_2} * \binom{N}{d_3 \quad d_3}}{N}} \tag{5}$$

If $\lambda <$ *required,* then choose greater prime N, and go to step 2.

Step 4. Calculate the maximum number of non-zero elements in the message (d_m)

During encryption of the data of encoded message, converted into a form of small polynomial, it should contain a number of non-zero elements, defined by general parameter d_m to prevent attacks. However, in case of the number of such non-zero elements is larger than some threshold, then the probability of reselecting a mask and multiplying by a blinding polynomial will be high[8]. Therefore, this parameter significantly affects the performance of the encryption algorithm.

The following condition(6) is a sufficient to eliminate the decryption error:

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

Step 5. Calculate q. It should be prime and satisfy conditions from [13]

The analysis showed that the value of the modulus q affects the probability of decryption error and is used in assessing the security of the lattice.

To calculate the value of q, which provides the maximum probability of error, which is determined by stability, the inequality(7) can be used:

$$q \ge 24(2d_1d_2 + d_3) + 3 \tag{7}$$

Step 6. Calculate T_{mintm}. Calculate minimum value $0 < r \le N$, which satisfy conditions(8):

$$T_{MITM}(N, r, d_g) > \lambda \text{ and } T_{MITM}(N, r, d_m) > \lambda \tag{8}$$

If at least one of the conditions fails, select greater prime N and go to step 2.

Step 7. Calculate the size of the lattice:

$$S = 2N - r \tag{9}$$

Step 8. Calculate $T_{lattice}$ - the number of operations for the construction of Korkin-Zolotarev-reduced basis[13] of a complete lattice of dimension S by formula(10):

$$T_{Lattice} = 2^{E(S,m,\beta)}, \tag{10}$$

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

This value should be greater the value that corresponds to the securely level λ. If, $T_{Lattice} < \lambda$, select greater prime N, and go to step 2. Else, while $T_{Lattice} > T_{MITM}$, increment *r*, and go to step 6.

Calculated values of parameters N, t, q are present in Table 3. They can be applicable for key encapsulation and direct encryption. Highlighted rows are used in standard DSTU 8961:2019[10].

Table 3

Calculated values of parameters for different stability levels of standard DSTU 8961:2019

	N	t	q
SKELYA 256/128	881	159	7673
	883	168	8089
	907	160	7727
	907	183	8807
	953	132	6343
	953	171	8237
	967	171	8243
	971	101	4871
	971	198	9551
	977	120	5783
	977	162	7817
	991	194	9349
	997	112	5393
	1013	149	7177
	1019	139	6691
	1021	112	5393
	1021	183	8819
SKELYA 384/192	1201	192	9221
SKELYA 512/256	1259	210	10103
	1283	214	10289
	1289	215	10331
	1291	215	10331
	1297	216	10453
	1301	217	10427
	1303	217	10429
	1307	218	10499
	1319	220	10567
	1321	220	10597
	1327	221	10613
	1361	227	10957
	1373	229	11057
	1381	230	11059
	1399	233	11213
	1409	235	11299
	1423	237	11383
	1471	255	12251

Comparative analysis of sets of parameters $\lambda \in (256, 384, 512)$ of the standard DSTU 8961 on criteria of stability and complexity

Table 4

Performance metrics for different stability levels

Stability level λ	Encryption	Decryption
256	89224	102982
384	138237	146128
512	163658	188235

There is a direct relationship between the level of stability and the time of direct and inverse transformation. The Fig. 1 shows a graph of this dependence. It is obvious that with increasing stability level, the complexity of transformations increases, so it is important to choose a sufficient level of stability based on available computing power.

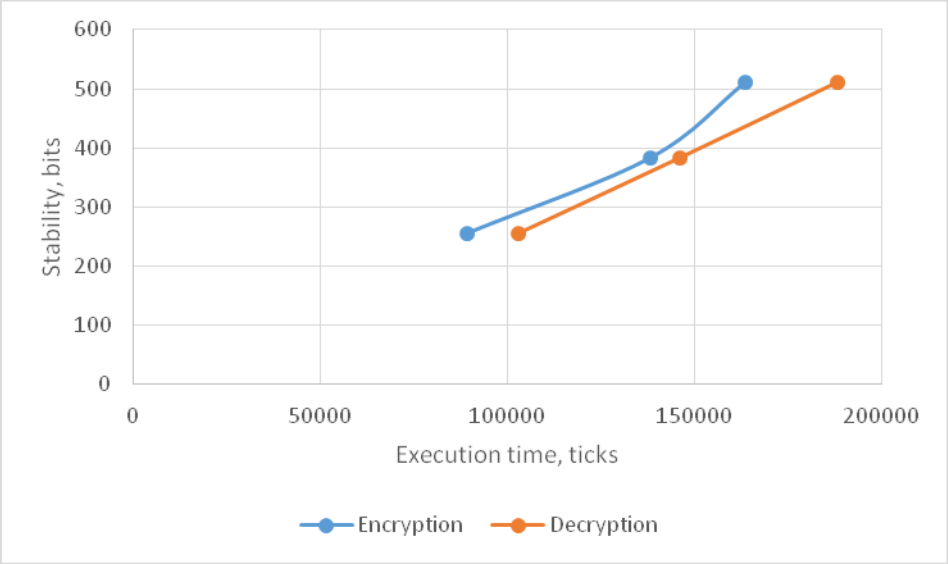

Fig. 1. Encryption and decryption time

Analysis of the stability of the standard DSTU 8961:2019 against side-channel attacks

An important issue is the stability of the national standard DSTU 8961:2019 against side-channel attacks, as well as against attacks on implementation. This paper considers the analysis of the dependence of the time of direct and inverse transformations (encapsulation/decapsulation of keys) on the structure of the long-term key, namely on the number of units in the long-term key.

The hash function defined in the national standard DSTU 7564:2014 was used as a hash function. The algorithm defined in DSTU 8845:2019 is used as an algorithm of symmetric streaming transformation.

For the experiment, 10,000 keys were generated and sorted by increasing number of ones. For each key, 100 calls were made to each of the tested functions and the average value of the execution time in CPU clocks for such a key was calculated. In Fig. 2-3 shows graphs of the number of CPU cycles from the key number. Random deviations can be caused by other processes in the operating system and do not depend on the number of units in the key. However, some optimizations of the implementation still possible and the number of cycles may depend on implementation.

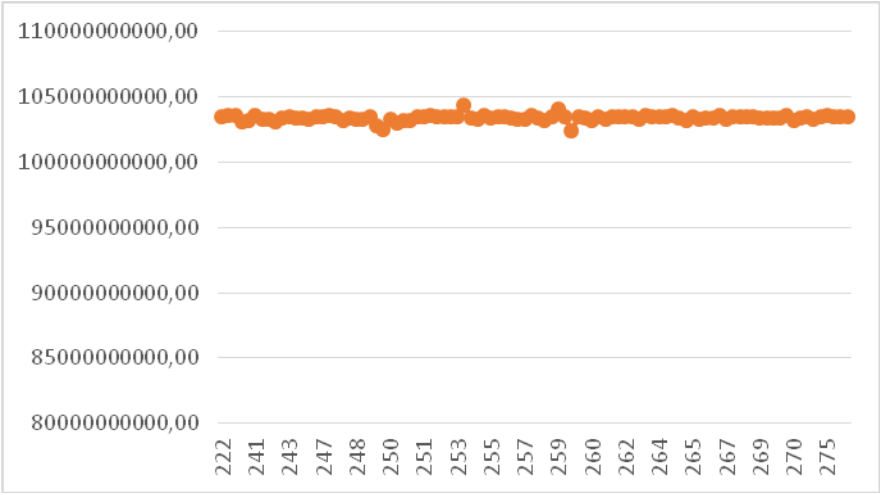

Fig. 2. Fragment of the graph of the dependence of the encapsulation execution time on the number of units in the key for the standard DSTU 8961:2019

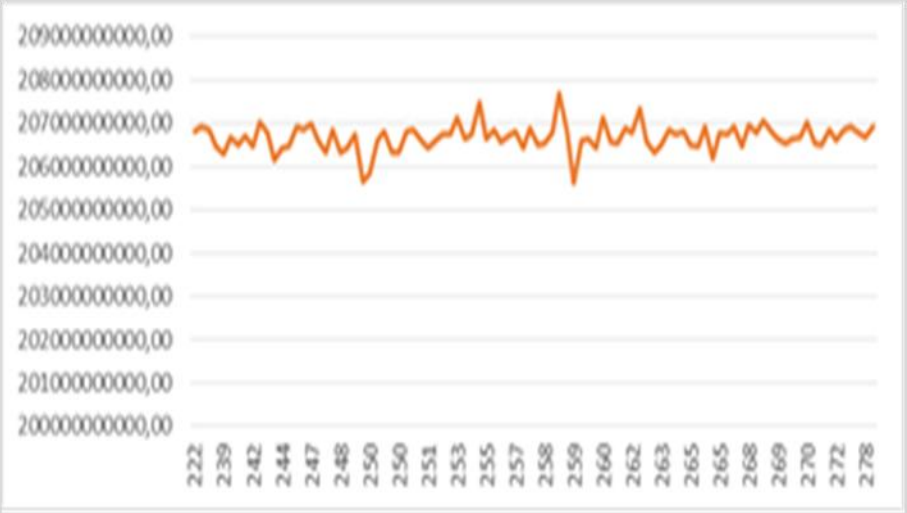

Fig. 3. Fragment of the graph of the dependence of the time of decapsulation on the number of units in the key for the standard DSTU 8961:2019

Table 5

The values of the correlation coefficients between the execution time for the functions of encapsulation / decapsulation of keys and the number of units in the key for the standard DSTU 8961:2019

	KeyNumber	CodeKem	DecodeKem
KeyNumber	1.000000	0.106736	0.153254
CodeKem	0.106736	1.000000	0.768122
DecodeKem	0.153254	0.768122	1.000000

The correlation coefficients between the execution time for the functions of encapsulation / decapsulation of keys and the number of units in the key for the standard DSTU 8961: 2019 are in the range [0.106 ... 0.153], which indicates the practical independence of execution time converted from the number of units in the key.

Conclusions

The main problems with asymmetric cryptography are the development of stable asymmetric crypto transformations such as KEM against both classical and quantum attacks, as well as the construction of system-wide parameters of 5-7 levels of stability [7,8].

Of particular relevance is the provision of cryptographic resistance to attacks by third-party channels, which requires a fundamentally new approach to the implementation of testing of cryptographic solutions of constant time, as well as analysis of existing standards on vulnerability to this class of attacks and countermeasures.

The study of the national standard DSTU 8961:2019 on resistance to attacks by third-party channels was performed. The KEM algorithms set out in DSTU 8961:2019 are protected from attacks by third-party channels in case of correct and accurate implementation, which has been confirmed experimentally.

The stability level has direct impact on the performance, so it is important to choose a sufficient level of stability based on device, e.g. for smart cards and tokens it might be reasonable to choose lower level of stability. The article presents the dependency between performance and stability level.

The simultaneous usage of keys encapsulation end encryption allows to setup symmetric encryption keys such as AES keys to increase speed of secure data transfer across communication channels.

References:

1. Post-Quantum Cryptography – Project Overview (2016) // Electronic resource. Access mode: https://csrc.nist.gov/projects/post-quantum-cryptography.
2. Gorjan Alagic Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8240 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, Yi-Kai Liu // Electronic resource. Access mode: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf.
3. Gorjan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, Yi-Kai Liu // Electronic resource. Access mode: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf.
4. National Institute of Standards and Technology Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. // Electronic resource. Access mode: https://csrc.nist.gov/CSRC/media/Projects/Post-QuantumCryptography/documents/call-for-proposals-final-dec-2016.pdf.
5. Gorbenko I.D., Kachko O.G, Alekseychuk A.N., Kuznetsov O.O., Gorbenko Yu.I., Onoprienko V.V., Yesina M.V., Candiy S.O. Algorithms of asymmetric encryptation and encapsulation of keys of post-quantum period of 5-7 levels of stability and their applications // Radiotekhnika. 2019. Is. 198. P. 5-18. DOI:10.30837/rt.2019.3.198.01.
6. Gorbenko I.D., Kachko O.G., Esina M.V. General statements and analysis of the end-to-end encryption algorithm NTRU Prime IIT Ukraine // Radiotekhnika. Kharkov : KNURE, 2018. Is. 193. P. 5-16.
7. Gorbenko I. D., Alekseychuk A.N., Kachko O.G., Yesina M.V., Stelnik I.V., Kandy S.O., Bobukh V. A., Ponomar V.A. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability // Telecommunications and Radio Engineering. 2019. Vol. 78, Is. 4. P.327-340. DOI: 10.1615/TelecomRadEng.v78.i4.40.
8. Gorbenko I.D., Kachko O.G., Gorbenko Yu.I., Stelnik I.V., Kandyi S.O., Yesina M.V. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th–7th levels of stability. Product form // Telecommunications and Radio Engineering. 2019. Vol. 78, Is. 7 P. 579-594. DOI: 10.1615/TelecomRadEng.v78.i7.30.98.
9. Kachko O.G, Gorbenko Yu.I., Yesina M.V, Akolzina O. Asymmetric encryption algorithm optimization based on using NTRU Prime mathematics // Radiotekhnika. 2017. Issue 191. P. 5-10.
10. DSTU 8961:2019 Information Technology. Cryptographic information protection. Asymmetric encryption and key encapsulation algorithms.
11. DSTU 7564:2014 Information Technology. Cryptographic information protection. Hashing function.
12. DSTU 8845:2019 Information Technology. Cryptographic information protection. Symmetric flow transformation algorithm.
13. Choosing Parameters for NTRUEncrypt. J. Horstein, J.Pipher, J.Schanck, J.Silverman, W. Whyte, Z. Zhang, https://eprint.iacr.org/2015/708.pdf
14. Nick Howgrave Graham NTRU Cryptosystems Technical Report. Report #4, Version 2. A Meet-In-TheMiddle Attack on an NTRU Private key / Nick Howgrave Graham, Joseph H. Silverman, William Whyte [Electronic resource]. Access mode.

Надійшла до редколегії 09.03.2021

Відомості про автора:

Кулібаба Владислав Андрійович – Харківський національний університет імені В.Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультету комп'ютерних наук, Україна, E-mail: vlad.kulibaba1994@gmail.com