UDC 004 056 55

RESEARCH OF USAGE POSSIBILITY AND POST-QUANTUM ALGORITHMS ADVANTAGES DEPEND ON APPLICATION CONDITIONS

Ivan Gorbenko, Vladimir Ponomar, Marina Yesina

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, laedaa@gmail.com, rinayes20@gmail.com

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 June 2017

Abstract: *We established the need for comparative analysis and evaluation of the possibility to use asymmetric post-quantum cryptographic mechanisms. In order to compare, a procedure for evaluation was selected based on integral assessments of unconditional and conditional criteria. An analysis was conducted among the algorithms that fulfilled general unconditional criteria. As conditional criteria, we chose numerical characteristics of algorithms. In addition, additional unconditional criteria were put forward that differed depending on the conditions of use. The relevance of present research is associated with the emergence of a quantum computer. Previous studies have already proved that the existing cryptographic algorithms are vulnerable to the methods of quantum cryptanalysis. That is why, at present, leading organizations in the standardization of crypto algorithms conduct research and comparisons for selecting the post-quantum standard of cryptography. As a result of present research, we found a lack of a universal post-quantum cryptographic algorithm. It is proposed to separate three variants in the application of post-quantum algorithms: for lightweight cryptography, for the use by standard automated systems and use in a cloud-based environment. For all conditions of use, a separate evaluation of benefits in the cryptographic algorithms was carried out. Deficiencies in the leading candidate were detected. That is why the recommendations were given to employ these algorithms as the basic ones in the transition period. And, if the suspicion is confirmed, then we proposed alternatives. Results of present research allow us to understand current state in the development of post-quantum crypto algorithms and to predict their possible further development. The practical value of the research consists in obtaining the evaluation for post-quantum algorithms, depending on the conditions of their application.*

Keywords: *post-quantum cryptographic algorithms, comparative assessment of crypto algorithms, comparison criteria of crypto algorithms.*

1 Introduction

Due to the development of technologies for quantum computing and the introduction of quantum computer, there is a threat to the current state of protection of cryptographic systems with a public key [1]. With an advent of quantum computer that would have the volume of register required for the methods of quantum cryptanalysis, the stability of existing crypto algorithms will significantly degrade [2, 3]. This necessitates the creation of algorithms resistant to the methods of quantum cryptanalysis. The European project "New European Schemes for Signatures, Integrity, and Encryptions " (NESSIE) and the National Institute of Standards and Technologies (NIST) of the USA announced a start of recruiting the applicants for the contest of post-quantum algorithms whose standards are planned to be adopted over 2020–2022 [4,5].

A peculiarity of this task is that the contest will accept the algorithms whose cryptographic transformations are based on the latest information or insufficiently tested mathematical methods that will require considerable time to prove their stability in terms of quantum cryptanalysis. That is why the choice of the new standard will affect not only the algorithm that will be employed but also further development of the post-quantum cryptography.

Another feature is that the universal algorithms are lacking that can be used both for electronic signature (ES) and the encryption. Therefore, it is necessary for each of the security services to select its particular algorithm. A possible exception is the use of isogenies by the Jao-Soukharev algorithm, but a special feature of the ES mechanism by this algorithm is that it requires interactivity and full trust from a third party [6].

A relevant task is the comparative analysis and evaluation of a possibility to use the post-quantum mechanisms, which are represented by the algorithms that already exist, depending on the

conditions of applying them. At present, only the possibility of using the appropriate crypto transformations over a post-quantum period is being examined, but the analysis of advantages of one over another has not been run yet. In addition, it is necessary to evaluate the very possibility to use such algorithms taking into account those constraints that are imposed by the existing information systems.

2 Literature review and problem statement

As a confirmation of necessity to develop the post-quantum algorithms, article [1] should be brought here. It notes that in August 2015, the National Security Agency (NSA) of the US Government came up with a broad statement about the need for devising the standards for post-quantum cryptography. This article analyzed the risk of applying quantum computers for modern crypto algorithms and proposed the mechanisms for crypto transformations that are resistant to the cryptanalysis of different types (Table 1).

Table 1 – Types of crypto transformations that are resistant to quantum cryptanalysis

Lattice-based primitives	Cryptographic resistance (protection) depends on the complexity of solving the equation on algebraic grids
Multivariate primitives	Cryptographic resistance (protection) depends on the complexity of solving a system of multivariate polynomial equations
Code-based primitives	Cryptographic resistance (protection) depends on the complexity of fulfilling the task on decoding a linear code
Hash-based primitives	Cryptographic resistance (protection) depends on the complexity of finding collisions or prototypes in the cryptographic hash-functions
Isogeny-based key primitives	Cryptographic resistance (protection) depends on the complexity of finding an unknown isogeny between a pair of supersingular elliptic curves

The algorithms given in Table 2 were proposed by the task force of the European Telecommunications Standards Institute (ETSI) [5] for further research and study as possible candidates for quantum-protected algorithms.

Table 2 – List of post-quantum algorithms and their characteristics, proposed by ETSI

Type	**Scheme**	**Resistance** [bits]	**Public key** [bytes]	**Signature** [bytes]
Lattice	Lyubashevsky	–	1 664	2 560
	NTRU-MLS	128	988	988
	Aguilar et al	128	1 082	1 894
	Guneysu te al	80	1 472	1 120
	BLISS	128	896	640
	Ducas et al	80	320	320
	HIMMO	128	32	-----
MQ	Quartz	80	72 237	16
	Ding	123	142 576	21
	UOV	128	413 145	135
	Cyclic-UOV	128	60 840	135
	Rainbow	128	139 363	79
	Cyclic-Rainbow	128	48 411	79

Each of the quantum-resistant types of cryptographic transformations is under examination and there are already algorithms for ES and directed encryption (DE or E2EE) that are based on these transformations [5-7]. There are preliminary results of comparing these algorithms to the existing standardized ones [7].

Continuation of Table 2

Type	Scheme	Resistance [bits]	Public key [bytes]	Signature [bytes]
Code	Parallel-CFS	120	503 316 480	108
	Cayrel et al	128	10 920	47 248
	Cyclic-Cayrel et al	128	208	47 248
	RankSign	130	7 200	1 080
	Cyclic RankSign	130	3 538	1 080
Hash	Merkle	128	32	1 731
	Leighton-Micali	128	20	668
	XMSS	256	64	8 392
	SPHINCS	256	1 056	41 000
Isogeny	Jao-Soukharev	128	768	1 280
	Sun-Tian-Wang	128	768	16

An analysis of scientific literature [1, 4-7] revealed that comparisons between potentially possible post-quantum mechanisms are still lacking, as well as information about the possibilities of their use depending on the conditions and the environment. At the same time, it is the choice of the most promising cryptographic transformations for the post quantum application, which is extremely important, as it defines future direction in the development of cryptography – asymmetric cryptography.

At [5-7] note that post-quantum algorithms, compared with others, in addition to the resistance to quantum cryptanalysis, demonstrate other advantages, as well as shortcomings. Thus, the algorithms based on multivariate transformations have a very small size of the signature. However, in contrast, for the required stability they demand key data of such large size that it makes their widespread use and application problematic. The algorithms based on the use of algebraic codes display a similar flaw, but their benefit is high performance speed.

The disadvantage of algorithms based on hashes is the large size of the crypto transformation result. In addition, to reduce the threat of attack of the "replay" type, additional information must be stored together with a private key.

The disadvantage of using algorithms based on elliptic curves isogenies is the high complexity in crypto transformations.

However [5-7] do not focus on these shortcomings. There is no analysis for a possibility to employ algorithms with such properties into existing systems. And there is no analysis of their advantages and shortcomings in comparison to other post-quantum algorithms. Nevertheless, this very analysis is particularly important. Since the need for a standard post-quantum asymmetric algorithm has been already defined [1, 4-5], it is necessary to choose the most suitable one to the requirements of the existing information systems.

3 The aim and tasks of the research

The aim of present research is to evaluate and to conduct comparative analysis of the existing methods for post-quantum crypto transformations of algorithms depending on the requirements put forward and conditions for their application. This will allow us, first, to select the algorithms that are most likely to become future post-quantum standards, second, to predict the future direction in the development of asymmetric cryptography.

To achieve the set aim, we solved the following tasks in the course of research:

– to select a technique, which will enable conducting an assessment and comparative analysis of post-quantum algorithms depending on the requirements put forward and conditions of application;

– to choose and analyze methods and algorithms that are based on different mathematical methods but meet unconditional (basic) requirements put forward to the candidates for post-quantum

standards (proved correctness and resistance, tested protection, exact assessment of parameters and complexity of implementation);

– to make up proposals and recommendations regarding the use of the examined algorithms when adopting the post-quantum standards of asymmetric crypto transformations.

4 Materials and methods for examining a possibility and advantages of using post-quantum algorithms depending on conditions

4.1 Substantiation of the choice of technique for comparing the cryptographic algorithms

One of the most important issues in the process of holding a contest is the application of objective methods and technique for the evaluation and comparative analysis of cryptographic primitives. Paper [8] described methods and techniques for comparative analysis of symmetric and asymmetric crypto primitives. They are based on the system of unconditional and conditional partial and integral criteria, as well as indicators that allow assessment of the degree of satisfying the requirements put forward to a candidate. The main task of such techniques is [8-10]:

– formalization of decision-making processes regarding the execution of requirements put forward to them;

– consideration of advantages and shortcomings in the cryptographic primitives that are candidates for the post-quantum standard;

– reducing the impact of subjective factors on decision making.

Under the criterion we shall understand an attribute, based on which the assessment is made, or determining or categorization of anything, that is, in essence, we shall understand it as an evaluation measure.

Previous studies [7,10] allowed drawing a conclusion that the comparison of cryptographic primitives can be carried out using two clusters of criteria: unconditional and conditional. This approach makes it possible to assess and compare those crypto transformations that are the candidates in 2 stages. This approach is based as well on accounting for or utilizing the expert evaluations.

At the first stage, they verify the appropriateness of crypto transformation for the system of partial unconditional criteria, and then for each crypto primitive, based on the partial ones, an unconditional integral criterion is computed.

At the second stage they receive appropriate assessments using first the system of partial conditional criteria, and then, based on them, an integral conditional criterion is calculated. The application of partial conditional criteria, and then, based on them, of integral conditional criterion, allow obtaining a more accurate estimate. Such assessment is obtained from the normalization of overall estimates of characteristics of crypto transformations and makes it possible to compare crypto primitives, which are the candidates for a post-quantum algorithm.

4.2 Examining the mechanisms of cryptographic transformations by the totality of unconditional criteria

It is by using the unconditional and conditional criteria that it becomes possible to compare different cryptographic transformations by the integral conditional and general criteria.

Further, by the conformity of one or another mechanism to the unconditional criteria we shall understand that expert assessments by the unconditional criteria are positive, in other words, they are satisfied unequivocally. We shall assign to the unconditional criteria those criteria whose fulfillment for cryptographic transformations is compulsory, that is, unconditional.

Thus, under condition of positive assessment by the integral unconditional criterion, further comparison and evaluation can be carried out based on determining and comparing the conditional criteria and an integral conditional criterion.

The general unconditional criteria are:

$W_{\delta 1}$ – reliability of mathematical base that is used in the cryptographic transformations;

$W_{\delta 2}$ – practical protection of cryptographic transformations from known quantum attacks;

$W_{\delta 3}$ – real protection from all known and potentially possible cryptanalytic attacks;

$W_{\delta 4}$ – statistical safety of cryptographic transformation;

$W_{\delta 5}$ – theoretical protection of cryptographic transformation;

$W_{\delta 6}$ – absence of weak private keys for cryptographic transformation or the existence of a proven mechanism to identify/verify such keys;

$W_{\delta 7}$ – complexity of direct and inverse cryptographic transformations regarding ES does not exceed a polynomial character.

1. Under the reliability of mathematical base, we shall understand practical absence of intruder's capabilities to carry out attacks of the "universal disclosure" type due to the imperfection of mathematical apparatus that is used, or weaknesses that can be predetermined by the specific properties of general parameters and keys. In this case, the criterion for estimating the reliability of mathematical base is the fact that the complexity of the attack "universal disclosure" is exponential in nature, and the criterion of unreliability is the subexponential or polynomial complexity.

2. Under the practical protection of crypto transformations, we shall understand protection from power and analytic attacks, which is achieved by selecting the size of general parameters and keys, as well as the means for their generation. In other words, the criterion of practical protection of crypto transformations is determined by a dependence of the complexity of attack on the size of general parameters and keys. There must exist such parameters, for which complexity of the attack considerably (*by the required number of orders*) exceeds the existing capacity of cryptanalytic systems in the technologically advanced states (*third level offender*). Including those that take into account a forecast for increase in the capacity of cryptanalytic systems due to the development of mathematical provision and software, as well as hardware and software means. In the present study, we considered future application of the means based on quantum computing. Since the emergence of such means necessitates introduction of new cryptographic algorithms.

3. Real protection from all known and potentially possible cryptanalytic attacks. Such protection refers to the fact that all known cryptanalytic attacks of the "full disclosure" type have exponential complexity. And the criterion of vulnerability – subexponential and lower character of complexity of the attack "full disclosure".

4. Statistical safety of cryptographic transformation, which we shall understand as a statistical independence of the result of cryptographic transformation from the input block that is encrypted (EP-signed), and a private key that is used.

5. Theoretical protection of cryptographic transformation. A crypto transformation is estimated when using general parameters with the appropriate properties and lengths. There should not exist (*unidentified*) theoretical analytical attacks whose complexity is lower than the complexity of attack of the "full disclosure" type.

6. Absence of weak key pairs, including private keys. Weak keys are the keys with which complexity of cryptanalytic attacks of the "full disclosure" and "universal disclosure" types is lower than the complexity of attack "full disclosure" for other (*not weak*) private keys. It is allowed to accept a mechanism, which has weak key pairs, but the probability of their generation is low and there is a proven algorithm for the validation of key pair on weakness of (*if all such key pairs have been already discovered*).

7. A complexity of the direct and inverse cryptographic transformations, as well as the generation or deployment of keys, has a polynomial character and does not exceed permissible magnitudes.

When using the given unconditional criteria, we chose the following algorithms (Table 3) under condition of applying the following parameters (*minimum values*) [7,8,10]:

1) $I_{res.}$ – cryptographic resistance;

2) $l_{pub.k.}$ – length of the public key;

3) $l_{pr.k.}$ – length of private key;

4) $l_{t.res.}$ – length of the result of cryptotransformation;

5) $T_{dir.}$ – speed of direct crypto transformation;

6) $T_{inv.}$ – speed of inverse crypto transformation.

Characteristics of algorithms from this Table. Among these algorithms, Jao-Soukharev is

highlighted because it can be used both for the encryption and for ES, but a signature requires interactivity.

Table 3 – Comparison of characteristics of post-quantum algorithms

Algorithms	$\mathbf{I_{res.}}$	$\mathbf{l_{pub.k.}}$	$\mathbf{l_{pr.k.}}$	$\mathbf{l_{t.res.}}$	$\mathbf{T_{dir.}}$	$\mathbf{T_{inv..}}$
NTRU	128	988	256	988	0,5	0,02
BLISS	128	896	256	640	0,02	0,01
Quartz	80	72237	3000	16	2	0,05
XMSS	128	1700	280	2048	2	0,2
SPHINCS	128	1024	1024	41000	0,5	0,02
RankSign	130	7200	21600	1080	0,02	0,02
Jao-Soukharev	128	768	768	1280	5	5

Note: Cryptographic resistance is given in bits, data size in bytes, and the speed of transformations in the form of coefficient relative to the speed of the corresponding transformation of the RSA algorithm with a key length of 4096 bits.

Among the indicated algorithms, we used a comparison by the unconditional criteria for various areas of application. The criteria are:

W_{s1} – $l_{pub.k.}$ – length of the public key;

W_{s2} – $l_{pr.k.}$ – length of private key;

W_{s3} – $l_{t.res.}$ – length of the result of crypto transformation;

W_{s4} – interactivity of algorithm.

These criteria are different for the following cases:

1) Lightweight cryptography is due to the use of smart cards, hardware electronic keys. A peculiarity of lightweight cryptography is:

– limited amount of internal storage;

– low computing capacities for satisfying which it is possible to reduce resistance;

– the use in combination with an extensive system of another type (such as an object of multifactor authentication in the internal network).

The criteria are:

W_{s1} – $l_{pub.k.}$ <=2048;

W_{s2} – $l_{pr.k.}$<=768;

W_{s3} – $l_{t.res.}$<=2048;

W_{s4} – interactivity is prohibited.

2) Cryptography in the standard automated systems (AS). Compared to the lightweight cryptography, the requirements to the size of the key data are reduced while requirements for resistance are increased. However, at the same time, such AS can be employed as servers. This predetermines a large amount of concurrent operations and storing, accordingly, a large volume of public-key certificates *(that includes a public key and its signature by the key of the certificate authority (CA))*. The criteria are:

W_{s1} – $l_{pub.k.}$ <=8192;

W_{s2} – $l_{pr.k.}$<=2048;

W_{s3} – $l_{t.res.}$<=8192;

W_{s4} – interactivity is prohibited.

3) Cryptography in a cloud-based environment:

Special conditional criteria are absent, that is, all algorithms from Table 3 can be applied.

Evaluation of the potential to use crypto transformation W_s under these conditions can be represented in the form:

$$W_s = W_{s1} \wedge W_{s2} \wedge W_{s3} \wedge W_{s4}. \quad (1)$$

Tables 4 and 5 give the results of comparing the crypto algorithms by formula (1) for the conditions of applying in lightweight cryptography and standard AS, respectively.

Table 4 – Conformity of algorithms to the unconditional criteria of light cryptography

Criterion / Algorithm	W_{s1}	W_{s2}	W_{s3}	W_{s4}	W_s
NTRU	1	1	1	1	1
BLISS	1	1	1	1	1
Quartz	0	0	1	1	0
XMSS	1	1	1	1	1
SPHINCS	1	0	0	1	0
RankSign	0	0	1	1	0
Jao-Soukharev DH	1	1	1	1	1
Jao-Soukharev Sign	1	1	1	0	0

Table 5 – Conformity of algorithms to the unconditional criteria of cryptography for standard AS

Criterion / Algorithm	W_{s1}	W_{s2}	W_{s3}	W_{s4}	W_s
NTRU	1	1	1	1	1
BLISS	1	1	1	1	1
Quartz	0	0	1	1	0
XMSS	1	1	1	1	1
SPHINCS	1	1	0	1	0
RankSign	1	0	1	1	0
Jao-Soukharev DH	1	1	1	1	1
Jao-Soukharev Sign	1	1	1	0	0

That is, for the conditions of light cryptography and cryptography of standard AS, we shall compare algorithms for ES BLISS and XMSS and the encryption algorithms NTRU and the Diffie-Hellman scheme for the Jao-Soukharev algorithm.

4.3 Examining the mechanisms of cryptographic transformations by the totality of conditional criteria

Studies have demonstrated that qualitative and quantitative comparison of cryptographic transformations can be conducted using a generalized conditional benefit criterion or an integral conditional criterion [10,11].

As the basic partial conditional criteria, it is proposed to use numerical characteristics of the algorithms that are listed in Table 3.

When applying the chosen partial conditional criteria, it is important to select a method for the convolution of partial conditional criteria into a conditional integral criterion.

Conducted analysis, as well as practical study, has demonstrated that as the methods for the convolution of partial conditional criteria, it is possible to choose the hierarchy analysis method based on pairwise comparisons and the ranking method.

When using the hierarchy analysis method based on pairwise comparisons, the obtained judgments are expressed by integers. These numbers *(ratings)* are selected by a 9-point scale *(Table 6, in the explanation column: interpretation of the score in our comparison is recorded)*. The validity of this scale is proved theoretically when compared to many other scales. When using the specified relation scale, comparing two objects in the sense of achieving the goal, which is located at the highest level of hierarchy. It is necessary to match this comparison with a number in the interval between 1 and 9, or the inverse value of numbers.

Table 6 – Scale of expert estimations of the pairwise comparison method

Degree of significance	Definition	Explanation
1	Equal significance	Two characteristics have the same significance.
3	Some advantage of one action over another (weak significance)	Characteristic in the numerical value is 2 times better, has some advantage qualitatively
5	Essential or strong significance	Characteristic in the numerical value is 4 times better, has a distinct advantage qualitatively
7	Obvious or very strong significance	Characteristic in the numerical value is 32 times better, has a considerable advantage qualitatively
9	Absolute significance	Characteristic in the numerical value is more than 32 times better, the other characteristic can be neglected qualitatively
2, 4, 6, 8	Intermediate values between two adjacent judgments	The situation needs a compromise solution
Inverse magnitudes of the non-zero magnitudes shown above	If action i when compared to j is assigned with one of the non-zero numbers defined above, then action j when compared to action is assigned with the inverse value	If the coherence was postulated when obtaining N numeric values for the formation of matrix

Thus, a comparison of cryptographic transformations can be carried out by using a generalized conditional benefit criteria or a conditional integral criterion. In this case, as the methods for the convolution of partial conditional criteria, one may choose the hierarchy analysis method based on pairwise comparisons and the ranking method.

Since the algorithms are compared by the determined numeric characteristics, then it is possible by the scale from Table 6 to receive their accurate assessment. However, determining the significance of each characteristic for the selected conditions cannot be performed with the same accuracy as determining the weight coefficients has a qualitative character. Therefore, in order to determine them, it is necessary to apply the method of expert evaluations [12].

4.4 Methods of expert evaluation

The expert evaluations are understood as a complex of logical and mathematical procedures aimed at obtaining information from specialists, its analysis and generalization in order to prepare and develop rational decisions [12].

Methods of expert evaluations are the methods for organizing work with specialists-experts and processing of expert opinions.

The essence of methods of expert evaluations – underlying the decision made, or forecast, or opinion, is the specialist's opinion or of a team of experts, based on their knowledge and practical professional experience.

Stages of expert evaluation [12]:

1) statement of purpose of the research;
2) selection of form of research, defining the budget of project;
3) preparation of information materials, forms, moderator of the procedure;
4) selection of experts;
5) conducting the survey;
6) analysis of results *(processing expert assessments)*;

7) preparation of the report with results of the expert evaluation.

There are the following methods of expert evaluations *(ways to work out both collective and individual expert assessments)*:

− method of association: based on studying the object similar in properties with another object;

− method of pairwise comparisons: based on the comparison by an expert of alternative choices among which the most significant is to be chosen;

− method of benefit vectors: an expert analyses the whole set of alternatives, chooses the most significant;

− method of focal objects: based on assigning the attributes of randomly selected analogues to the examined object;

− individual expert survey: a survey in the form of an interview in the form of analysis of expert assessments;

− the midpoint method: two alternative variants of solution are stated, one of which has a lower benefit. After that, the expert has to select a third alternative variant whose estimate is between the values of the first and second alternatives;

− method of simple ranking: each expert should position the attributes in order of benefits;

− method for assigning the weighting coefficients: all attributes are assigned with certain weighting coefficients;

− method of sequential comparisons (all the attributes are arranged by the decrease in their significance; the first attribute is assigned with value 1, others are assigned with weighting coefficients in fractions of a unity; the value of the first attribute is compared to the sum of all of the subsequent ones);

− method of assigning the points: experts, depending on the significance of the indicator *(attribute)* assign points (0–10), and are permitted to evaluate the significance of the indicator in decimal values, as well as different indicators can be assigned with equal points.

Common opinion displays a larger accuracy than the individual opinions of each of the experts. This method is used to obtain quantitative estimates of qualitative characteristics and properties.

Thus, there are collective and individual expert assessments. As far as each of the groups of scores is concerned, there are appropriate methods for defining such estimates. The given methods are selected according to the conditions of evaluation, degree of complexity and the required accuracy of assessment, etc. Each of the methods has also its own advantages and shortcomings.

In the case when all characteristics of the cryptographic algorithms have a precise numeric value, the role of experts is to determine the weighting coefficients of the significance of characteristics. These coefficients vary depending on the area of application. That is why the chosen experts were specialists in their relevant fields.

4.5 Establishing a degree of coherence among expert opinions

If several experts participate in a survey, then the differences in their assessments are unavoidable, however, the magnitude of such discrepancy is important. Group evaluation can be considered sufficiently reliable only under condition of a good degree of coherence among the responses from individual experts [12].

For the analysis of variability and coherence in the assessments, they apply statistical characteristics – a measure of spread or statistical variance.

The means of computing a measure of spread:

1) Variance spread:

$$R = x_{\max} - x_{\min},$$

where x_{max}, x_{min} are the maximal and minimal value of indicator (attribute), respectively.

2) Mean linear deviation:

$$a = \frac{1}{n}\sum_{i=1}^{n}\left|x_i - \bar{x}\right|,$$

where n is the number of expert estimates of characteristic *(number of experts)*, x_i is the estimate of the *i*-th expert, i=1,..., n, $\bar{x}$ is the mean value of estimate of characteristic.

3) The root mean square deviation:

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2}.$$

4) Dispersion:

$$\sigma^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2.$$

As a reliability measure of the degree of reliability of a given survey, the method of pairwise comparisons employs the values of variation in the estimates of a characteristic:

$$\beta_j = \frac{\sigma_j}{\bar{x}_j},$$

where σ_j is the root mean square deviation of the *j*-th characteristic, $\overline{x_j}$ is the mean value of assessment of the *j*-th characteristic. The closer a variance coefficient to zero, the more coherent experts' estimates are. If the value of variance is larger than 0,33, the opinion of experts is considered to be unsatisfactorily coherent, 0,17 - 0,33 – satisfactorily coherent, 0,17 – coherent enough. The total variance (that is, coherence among the assessments of all characteristics) can be selected by the maximax criterion – maximum value of the variance. Another variant is to perform the evaluation for the variance of variance, that is, to repeat calculations, but, instead of the values of estimates, to apply the values of variance.

For the method of pairwise comparisons, the mean value of a characteristic's estimate will become a weight coefficient for this characteristic.

For the ranking method, they use a different method to evaluate coherence among the opinions of experts – a method for determining the coefficient of concordance:

1) d experts estimate n attributes by the ranking method, r_{ij} is the estimate of the *i*-th attribute by the *j*-th expert.

2) the sum of ranks of the attribute is determined:

$$r_{is} = \sum_{j=1}^{d} r_{ij}, \quad i = \overline{1,n.}$$

3) the average sum of the ranks is determined:

$$\bar{r}_s = \frac{1}{n}\sum_{i=1}^{n} r_{is}.$$

4) the coefficient of deviation is determined:

$$S = \sum_{i=1}^{n}(r_{is} - \bar{r}_s)^2.$$

5) the coefficient of concordance is determined:

$$W = \frac{12}{d^2(n^3 - n)}S.$$

The closer coefficient of concordance to 1, the more coherent is the opinion of experts. It is believed that at W > 0,5, the coherence of opinions is satisfactory.

4.6 The hierarchy analysis method based on pairwise comparisons and the peculiarities of its application for the evaluation of algorithms

In order to apply the hierarchy analysis method, it is necessary to select a system of conditional criteria. By using such a set of indicators, by applying the conditional criteria, it is possible to calculate the values of integral conditional criterion and, as a consequence, to compare cryptographic algorithms by the conditional integral criterion [8,10,12].

The method for pairwise comparison of elements can be described in the following way. We construct a set of matrices of paired comparisons. Paired comparisons are represented in terms of dominance of one element over another. At pairwise comparison, expert compares examined objects by their significance in pairs, establishing the most important in each pair of objects. All possible pairs of objects are represented by an expert in the form of record of each of the combinations (object 1 – object 2, object 2 – object 3, etc.) or in the form of a matrix. The method of pairwise comparisons is very simple and allows examining a larger number of objects (in comparison, for example, with the ranking method) and with a better accuracy.

Assume E_1, E_2,... ,E_n is the multitude of n elements (*alternatives*) and v_1 ,v_2,..., v_n are, respectively, their weight or intensity. Let us compare in pairs the weight, or intensity, of each element to the weight, or intensity, of any other element in the set relative to a property or goal common to them (*relative to the element "father"*). In this case, the matrix of pairwise comparisons [E] takes the form of Table 7.

Table 7 – Representation of matrix of pairwise comparisons

Criteria	**E_1**	**E_2**	**…**	**E_n**
E_1	ν_1 / ν_1	ν_1 / ν_2	…	ν_1 / ν_n
E_2	ν_2 / ν_1	ν_2 / ν_2	…	ν_2 / ν_n
…	…	…	…	…
E_n	ν_n / ν_1	ν_n / ν_2	…	ν_n / ν_n

The matrix of pairwise comparisons has a property of inverse symmetry, that is, $a_{ij}=1/a_{ji}$, where $a_{ij}=v_i/v_j$. When conducting the pairwise comparisons, one should answer the following questions: which of the two compared elements is more important or exerts a larger influence, which is more probable and which has a larger benefit. When comparing the criteria, they usually ask which of the criteria is more important; when comparing the alternatives relative to the criteria – which of the alternatives has a larger benefit, or is more likely. When constructing a matrix of pairwise comparisons for all criteria, it is necessary to determine a relation of coherence for each of the criteria in the following way. The estimate of component of the natural vector will be calculated by formula (2):

$$q_i = (W_{yi} \times W_{yi+1} \times \ldots \times W_{yn})^{\frac{1}{n}}. \quad (2)$$

The normalized estimate of the priority vector will be calculated by formula (3):

$$r_i = q_i \div z, \quad (3)$$

where z is the ratio of consistency of the matrix, which is calculated by expression (4):

$$z = \sum_{i=1}^{n} q_i. \quad (4)$$

The value of relation in the consistency of the matrix is in the range of $[0, \sum_{i=1}^{n} q_{i\max}]$, where $q_{i\max}$ is the maximal possible value of the estimate of component of the natural vector for the chosen case. Therefore, the hierarchy analysis method based on the pairwise comparisons demonstrates both advantages and disadvantages. The main shortcoming is a sufficiently strong influence of the subjective opinion of an expert on the outcome of the assessment. One of the benefits is a simple mathematical apparatus used.

4.7 Methods for determining the weight coefficients

In the case, when get information about parameters comparable systems importance using informal methods is not possible, necessary to use formalized methods. Among them are methods based on determining the weight indices. Let us consider the general problem formulation for cryptographic primitives evaluation technique based on the determining the weight indices method. Let there are:

1) *k* systems *(cryptoprimitives)*, which is necessary to evaluate;
2) *m* indicators, according to which systems are evaluated;
3) *n* experts, that carry out the evaluation.

For the evaluation, you can use the following weight indices determining methods: using the Fishburn scale; based on the ranking method; based on the points attribution method; based on the numerical method. Let us consider these methods more detail hereafter. The cryptographic primitives estimation in this article are done only with using method for determining the weight coefficients based on the ranking method and hierarchy analysis method based on pairwise comparisons.

4.7.1 Method for determining the weight coefficients using the Fishburn scale

Let we have *m* indicators and *n* experts, that estimate the importance of these indicators for some system. To each indicator x_i, $i = 1,...,m$ the estimate of their importance is put on accordance. After that the weight system are built by the next way

$$\begin{cases} \sum_{i=1}^{m} a_i = 1, \\ a_i \geq 0, i = 1,....,m \end{cases}, \quad (5)$$

where a_i – i-th indicator weight; i – indicator number; m – indicators amount. Indicators are ranging by the significance increasing: $x_1 \succ x_2 \succ x_3 \succ ... \succ x_i \succ ... \succ x_m$.

Let we define weight indices by using the Fishburn scale:

$$a_i = \frac{2 \cdot (m - i + 1)}{m \cdot (m + 1)}. \quad (6)$$

Values of weight indices and their average value are brought under the table (Table 8).

$\overline{a_i}$ – average value of weight indices for i-th indicator; $w_i = \overline{a_i}$ – weight indices values.

Table 8 – Weight indices values and their average value

Indicators / Experts	x_1	x_2	...	x_m
1	a_{11}	a_{12}	...	a_{1m}
2	a_{21}	a_{22}	...	a_{2m}
...	...	...	...	...
n	a_{n1}	a_{n2}	...	a_{nm}
w_i	w_1	w_2	....	w_m

4.7.2 Method for determining the weight coefficients based on the ranking method

The ranking method – one builds a matrix of evaluations of the attributes by experts, where each expert assigns a rank to each attribute. Assume there is n of partial indicators and group of d experts who assess the significance of these indicators for a certain system. The most important indicator is matched by rank (*score*) n, the next one – by (n–1), etc.; the rank equal to 1 is the least important. Then, the weighting coefficients are determined by formula (7) [8-10]:

$$w_j = \frac{r_j}{\sum_{j=1}^{n} r_j}, \quad j = 1,...,n. \tag{7}$$

Table 9 – Table of expert estimates by the ranking method

Indicators / Experts	x_1	x_2	…	x_n
1	r_{11}	r_{12}	…	r_{1n}
2	r_{21}	r_{22}	…	r_{2n}
…	…	…	…	…
d	r_{d1}	r_{d2}	…	r_{dn}
$r_j = \sum_{i=1}^{n} r_{ij}$	r_1	r_2	…	r_n
w_j	w_1	w_2	….	w_n

Notes: x_n is the n-th indicator, r_j is the j-th rank (estimate), d is the number of experts, n is the number of indicators.

Results of a survey of experts are compiled in a table (Table 9). The penultimate line of this table contains a record of the sum of the ranks (*estimates*) that were assigned by the experts, and the last line of the table contains a record of values of weighting coefficients of the indicators.

4.7.3 Method for determining the weight coefficients based on the points attribution method

Let we have *m* indicators and *n* experts, that estimate the importance of these indicators for some system. Experts according to indicator significance put points from 0 to 10, herewith it's allow to estimate the importance of indicator by the fractional values, and also to the different indicators we can charge off similar points. After that it's defined weights of each indicator that is calculated by each expert:

$$r_{ij} = \frac{h_{ij}}{\sum_{j=1}^{m} h_{ij}}; \ \sum_{j=1}^{m} r_{ij} = 1, \tag{8}$$

where r_{ij} – weights of j-th indicator, that are defined by i-th expert; h_{ij} – point of i-th expert, that are put to the j-th indicator; *n* – amount of experts; *m* – amount of indicators.

All received data are brought under the table (Table 10). The finale weight indices of indicators are defined by the formula:

$$w_j = \frac{\sum_{i=1}^{n} r_{ij}}{\sum_{j=1}^{m}\sum_{i=1}^{n} r_{ij}}; \ \sum_{j=1}^{n} w_j = 1. \tag{9}$$

Besides experts estimates for define weight indices we can use some formal methods, which take into the consideration values of indicators itself.

Table 10 – Weight indices values

Indicators (j) / Experts (i)	x_1	x_2	…	x_m	$\sum_{j=1}^{m} h_{ij}$	Indicators weights			
						r_{i1}	r_{i2}	…	r_{im}
1	h_{11}	h_{12}	…	h_{1m}	$\sum_{j=1}^{m} h_{1j}$	$r_{11}=\frac{h_{11}}{\sum_{j=1}^{m} h_{1j}}$	$r_{12}=\frac{h_{12}}{\sum_{j=1}^{m} h_{1j}}$	…	$r_{1m}=\frac{h_{1m}}{\sum_{j=1}^{m} h_{1j}}$
2	h_{21}	h_{22}	…	h_{2m}	$\sum_{j=1}^{m} h_{2j}$	$r_{21}=\frac{h_{21}}{\sum_{j=1}^{m} h_{2j}}$	$r_{22}=\frac{h_{22}}{\sum_{j=1}^{m} h_{2j}}$	…	$r_{2m}=\frac{h_{2m}}{\sum_{j=1}^{m} h_{2j}}$
…	…	…	…	…	…	…	…	…	…
n	h_{n1}	h_{n2}	…	h_{nm}	$\sum_{j=1}^{m} h_{nj}$	$r_{n1}=\frac{h_{n1}}{\sum_{j=1}^{m} h_{nj}}$	$r_{n2}=\frac{h_{n2}}{\sum_{j=1}^{m} h_{nj}}$	…	$r_{nm}=\frac{h_{nm}}{\sum_{j=1}^{m} h_{nj}}$
					$\sum_{i=1}^{n} r_{ij}$	$r_1=\sum_{i=1}^{n} r_{i1}$	$r_2=\sum_{i=1}^{n} r_{i2}$	…	$r_m=\sum_{i=1}^{n} r_{im}$
					w_j	$w_1=\frac{r_1}{\sum_{j=1}^{m} r_j}$	$w_2=\frac{r_2}{\sum_{j=1}^{m} r_j}$	…	$w_m=\frac{r_m}{\sum_{j=1}^{m} r_j}$

4.7.4 Method for determining the weight coefficients based on the numerical method

For each indicator the coefficient of relative spreading is calculated by the formula:

$$\delta_i = \frac{x_{i\max} - x_{i\min}}{x_{i\max}}, \tag{10}$$

where $x_{i\max}$, $x_{i\min}$ – maximum and minimum values of i-th indicator accordingly, m – indicators amount.

Values of indicators itself can find by the any above mentioned methods. Weight indices take the greatest value for that indicators, which relative spreading are the most significant

$$w_i = \frac{\delta_i}{\sum_{i=1}^{m} \delta_i}. \tag{11}$$

All received data are brought under the table (Table 11).

Table 11 – Weight indices values

Indicators / Estimation	x_1	x_2	…	x_m
$x_{i\min}$	$x_{1\min}$	$x_{2\min}$	….	$x_{m\min}$
$x_{i\max}$	$x_{1\max}$	$x_{2\max}$	….	$x_{m\max}$
δ_i	δ_1	δ_2	….	δ_m
w_i	w_1	w_2	….	w_m

5 Results of examining the comparative evaluation of the application of post-quantum cryptographic algorithms

Table 12 gives the result of determining the weight coefficients by expert estimates for the mechanisms of ES for lightweight cryptography.

The level of consistency in the assessments is 0,156 that meets the requirements. After conducting evaluations of characteristics for the algorithms (Table 3) that were selected by unconditional criteria (Table 4), by the scale of Table 6, the BLISS algorithm has the level of 0,709, XMSS – 0,291.

Table 12 – Weight coefficients of the ES mechanisms criteria by expert estimates for lightweight cryptography by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,235	0,124	0,235	0,124	0,235	0,045
2	0,218	0,096	0,286	0,129	0,218	0,053
3	0,242	0,084	0,242	0,135	0,242	0,056
4	0,264	0,098	0,264	0,137	0,186	0,050
5	0,275	0,092	0,275	0,155	0,155	0,047
W	0,247	0,099	0,260	0,136	0,207	0,050

Table 13 gives the result of determining the weight coefficients by expert estimates for the encryption mechanisms for lightweight cryptography.

The level of consistency in the assessments is 0,108 that meets the requirements. After conducting evaluations of characteristics for the algorithms (Table 3) that were selected by unconditional criteria (Table 4), by the scale of Table 6, the NTRU algorithm has the level of 0,704, Jao-Soukharev – 0,296.

Table 13 – Weight coefficients of the encryption mechanisms criteria by expert estimates for lightweight cryptography by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,079	0,137	0,079	0,187	0,259	0,259
2	0,087	0,114	0,076	0,241	0,241	0,241
3	0,082	0,133	0,064	0,240	0,240	0,240
4	0,089	0,123	0,089	0,233	0,233	0,233
5	0,071	0,119	0,071	0,199	0,269	0,269
W	0,081	0,125	0,076	0,220	0,249	0,249

Table 14 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for the cryptography of standard AS. The level of consistency in the assessments is 0,310 that meets the requirements. After conducting evaluations of characteristics for the algorithms (Table 3) that were selected by unconditional criteria (Table 5), by the scale of Table 6, the BLISS algorithm has the level of 0,763, XMSS - 0,237.

Table 15 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for the cryptography of standard AS.

The level of consistency in the assessments is 0,176 that meets the requirements. After conducting evaluations of characteristics for the algorithms (Table 3) that were selected by unconditional criteria (Table 5), by the scale of Table 6, the NTRU algorithm has the level of 0,705, Jao-Soukharev – 0,295.

Table 14 – Weight coefficients of the ES mechanisms criteria by expert estimates for the standard AS by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,263	0,181	0,123	0,072	0,181	0,181
2	0,203	0,281	0,065	0,105	0,143	0,203
3	0,138	0,232	0,054	0,083	0,138	0,354
4	0,134	0,229	0,075	0,134	0,075	0,353
5	0,198	0,142	0,068	0,153	0,175	0,264
W	0,187	0,213	0,077	0,109	0,142	0,271

Table 15 – Weight coefficients of the encryption mechanisms criteria by expert estimates for the standard AS by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,100	0,077	0,060	0,254	0,254	0,254
2	0,096	0,096	0,059	0,203	0,273	0,273
3	0,110	0,067	0,067	0,302	0,226	0,226
4	0,123	0,078	0,052	0,335	0,206	0,206
5	0,107	0,107	0,064	0,329	0,196	0,196
W	0,107	0,085	0,061	0,285	0,231	0,231

Table 16 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for the cryptography in a cloud-based environment.

The level of consistency in the assessments is 0,199 that meets the requirements. After conducting evaluation of characteristics for the algorithms (Table 3), by the scale of Table 6, the BLISS algorithm has the level of 0,267, RankSign – 0,218, Quartz – 0,158, SPHINKS – 0,154, XMSS – 0,123, Jao-Soukharev – 0,11.

Table 16 – Weight coefficients of the ES mechanisms criteria by expert estimates for clouds by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,305	0,068	0,068	0,168	0,168	0,222
2	0,233	0,055	0,082	0,164	0,233	0,233
3	0,329	0,064	0,107	0,107	0,196	0,196
4	0,274	0,058	0,089	0,153	0,153	0,274
5	0,246	0,062	0,062	0,140	0,246	0,246
W	0,277	0,061	0,082	0,147	0,199	0,234

Table 17 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for the cryptography in a cloud-based environment.

The level of consistency in the assessments is 0,197 that meets the requirements. After conducting evaluation of characteristics for the algorithms (Table 3), by the scale of Table 6, the NTRU algorithm has the level of 0,685, Jao-Soukharev – 0,315.

Table 17 – Weight coefficients of the encryption mechanisms criteria by expert estimates for clouds by the method of pairwise comparisons

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	0,319	0,068	0,068	0,182	0,182	0,182
2	0,233	0,055	0,082	0,164	0,233	0,233
3	0,329	0,064	0,107	0,107	0,196	0,196
4	0,242	0,056	0,084	0,135	0,242	0,242
5	0,246	0,062	0,062	0,140	0,246	0,246
W	0,274	0,061	0,081	0,146	0,220	0,220

As in determining the weight coefficients, some attributes were assigned equal estimates, then to define a more accurate estimate we also used the ranking method, in which during expert assessment it was prohibited to assign features with the same rank, and when evaluating the very cryptographic algorithms, the equal rank was assigned only at complete matching of attributes. In Table 3, such matching is only for the resistance and speed of transformations, but in the case of speed of the transformations, we analysed not only the relative performance speed but comparative as well, which allowed us to obtain a more accurate ration for some pairs of algorithms.

Table 18 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for lightweight cryptography.

The coefficient of concordance is equal to 0,904 that satisfies the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), BLISS has the levels of 0,618, XMSS – 0,382.

An analysis of Tables 12 and 18 reveals that, regardless of the applied methods, the values of weighting coefficients are almost identical. However, XMSS has a higher rating due to the fact that in the ranking method they do not take into account the difference in characteristics, and rank is assigned only. This leads to a decrease in the level of estimates in the case when a small number of objects are estimated. This property is one of the largest differences between these two methods: if, for the method of pairwise comparisons, a larger influence is exerted by the difference in characteristics (*given the weighting coefficients*), then for the ranking method, a larger impact is exerted by the number of characteristics according to which the object has an advantage (*also taking into account the weighting coefficients*).

Table 18 – Weight coefficients of the ES mechanisms criteria by expert estimates for lightweight cryptography by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	4	2	5	3	6	1
2	4	2	6	3	5	1
3	5	2	6	3	4	1
4	6	2	5	3	4	1
5	6	2	5	3	4	1
W	0,238	0,095	0,257	0,143	0,219	0,048

Table 19 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for lightweight cryptography. The coefficient of concordance equals 0,872, which meets the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the NTRU algorithm has the level of 0,606, Jao-Soukharev – 0,394.

Table 19 – Weight coefficients of the encryption mechanisms criteria by expert estimates for lightweight cryptography by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	1	3	2	4	6	5
2	2	3	1	4	6	5
3	2	3	1	6	5	4
4	1	3	2	6	5	4
5	1	3	2	4	5	6
W	0,067	0,143	0,076	0,229	0,257	0,229

Table 20 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for the cryptography in standard AS. The coefficient of concordance is equal to 0,762, which satisfies the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the BLISS algorithm has the level of 0,619, XMSS – 0,381.

Table 20 – Weight coefficients of the ES mechanisms criteria by expert estimates for standard AS by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	6	4	2	1	3	5
2	5	6	1	2	3	4
3	4	5	1	2	3	6
4	4	5	1	3	2	6
5	5	2	1	3	4	6
W	0,229	0,210	0,057	0,105	0,143	0,257

Table 21 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for the cryptography of standard AS.

The coefficient of concordance equals 0,872, which meets the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the NTRU algorithm has the level of 0,605, Jao-Soukharev – 0,395.

Table 21 – Weight coefficients of the encryption mechanisms criteria by expert estimates for standard AS by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	3	2	1	4	5	6
2	2	3	1	4	5	6
3	3	2	1	6	4	5
4	3	2	1	6	5	4
5	3	2	1	6	5	4
W	0,133	0,105	0,048	0,248	0,229	0,238

Table 22 gives the result of determining the weight coefficients by expert estimates of the ES mechanisms for cryptography in clouds.

The coefficient of concordance is equal to 0,954, which satisfies the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the BLISS algorithm has the level of 0,244, RankSign – 0,203, SPHINKS – 0,168, XMSS – 0,149, Jao-Soukharev – 0,132, Quartz – 0,105.

Table 22 – Weight coefficients of the ES mechanisms criteria by expert estimates for clouds by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	6	2	1	3	4	5
2	6	1	2	3	5	4
3	6	1	2	3	4	5
4	6	1	2	3	4	5
5	6	2	1	3	4	5
W	0,286	0,067	0,076	0,143	0,200	0,229

Table 23 gives the result of determining the weight coefficients by expert estimates of the encryption mechanisms for cryptography in clouds.

Table 23 – Weight coefficients of the encryption mechanisms criteria by expert estimates for clouds by the ranking method

Indicators / Experts	$I_{res.}$	$l_{pub.k.}$	$l_{pr.k.}$	$l_{t.res.}$	$T_{dir.}$	$T_{inv..}$
1	6	2	1	3	5	4
2	6	1	2	3	5	4
3	6	1	2	3	5	4
4	6	1	2	3	4	5
5	6	2	1	3	4	5
W	0,286	0,067	0,076	0,143	0,219	0,210

The coefficient of concordance equals 0,945, which meets the requirements. After conducting evaluation of characteristics of the algorithms (Table 3), the NTRU algorithm has the level of 0,588, Jao-Soukharev – 0,412.

6 Discussion of results of examining the possibility of using and benefits of post-quantum algorithms depending on conditions

Weight coefficients for the conditions of lightweight cryptography (Tables 12,13,18,19) are determined from the fact that for ES, a complexity of the ES verification is almost non-essential, because the main verification of ES is performed outside the system, not in the smart card. The hardware means conducts the ES verification while performing the following procedures:

– update (*firmware renewal by developer*);

– change in the system critical data (*downloading a new CA or developer's certificate, formatting the card*);

– the process of authentication (*electronic passport, etc.*).

Also important is the size of a private key as the memory capacity is limited. For the encryption, complexity of direct and inverse transformations have the same impact. The size of the result has a big impact since it has to be transferred with every operation, and for encrypting, a public key as well.

For the standard systems (Tables 14,15,20,21), more important is the crypto transformation speed and resistance. In addition, the importance of complex validation of ES is higher than the complexity of ES procedure itself. This is due to the fact that in the public key infrastructure (PKI), the ES validation (*that is, additional check on certificate*) takes place significantly more often than the ES procedure itself.

In the cloud-based environment (Tables 16,17,22,23), the most important is the mechanism re-

sistance and speed of crypto transformations. This is so because resistance characterizes reliability of the systems, and the use of crypto-equipment in the clouds is fee-based. At the same time, storing the public keys is predetermined by the structure of clouds, and storage of private keys is included in the service when using the crypto-equipment in clouds. The size of the result of crypto transformations is more important than the size of the keys, because the result, first, may be stored not in the clouds but in the system, and, second, these messages are transmitted by communications that increase the load on the system.

When applying the methods of pairwise comparisons and ranking, the crypto algorithms estimates do not change significantly and the advantage of these over the others is maintained. But there is an exception in the evaluation of ES algorithms under conditions of cloud environment (*the case in our study, in which we simultaneously compared the largest number of algorithms*). When using the ranking method (Table 22), algorithm Quartz took the last position in contrast to the method of pairwise comparison (Table 16), where this algorithm takes a third place. This was due to the fact that the ranking method does not account for the difference between the values of characteristics, and the main benefit of the Quartz algorithm is a very small size of ES. Therefore, since the ranking method takes into account the existence of a benefit rather than its size, the Quartz algorithm gets a low benefit rank.

The comparative analysis revealed that the best choice for all systems and cases is the choice of lattice-based algorithms (BLISS and NTRU). A shortcoming of these algorithms is that according to the latest research, these algorithms have a reduced complexity for quantum attack of the "meeting in the middle" type [13,14], however, such complexity is satisfactory for minimum requirements. Hence, it follows that these algorithms are the best choice for the transition period, which will permit, by stable algorithms, finding further solutions to improve these algorithms, or searching for other variants.

Among the post-quantum mechanisms for ES, one of the most promising is the hash-based algorithm. These algorithms have a proven resistance to all known methods of quantum cryptanalysis (*in contrast to lattice-based mechanisms*). Their advantage is in that they can be used in all environments and even in the cloud-based environment they are competitive. For the use in clouds, good results were demonstrated by the RankSign algorithm, which is based on the application of mathematical codes. Other algorithms have close estimates and it is recommended to choose an algorithm depending on the structure of the appropriate cloud (*in case the state of optimization and research into protection of these algorithms will not change*).

As far as the encryption algorithms are concerned, then in the case the NTRU vulnerability [13,14] is confirmed, the choice will be limited by the mechanisms that employ isogenies.

7 Conclusions

1. In view of the specific requirements to the post-quantum crypto transformations, it is expediently to use two classes of criteria: conditional and unconditional. Conditional criteria are the criteria whose fulfilment for the examined crypto transformations is compulsory, that is, unconditioned. Conditional criteria are the criteria whose fulfilment for the examined crypto transformations must be carried out only under specified conditions. In a comparative analysis, for the purpose of conducting targeted evaluation, it is necessary to apply precise numerical values for the attributes of characteristic candidates in the post-quantum cryptographic transformations, as well as the defined scale of evaluation. To conduct evaluation of post-quantum algorithms relative to the environment, it is necessary to conduct expert assessment of weighting coefficients of attributes, or their standardization.

2. Results of comparative analysis revealed that in some cases it is possible to employ crypto transformations whose resistance is based on the transformations in the rings of abridged polynomials and lattice-based. The disadvantage of these algorithms (BLISS and NTRU) is in that, according to the latest research, these algorithms have a reduced complexity regarding the quantum attack *"meeting in the middle"*, but this complexity is satisfactory for minimal requirements. The aforementioned allows us to conclude that the crypto transformations whose resistance is based on the

transformations in the rings of abridged polynomials, and lattice-based, can be applied in the transition and the initial post-quantum periods. In the future, it is necessary to continue studies and search for or improve those adopted. Probably, an important alternative is the use of algorithms based on the hash trees of ES and algorithms with the use of isogenies of elliptic curves for encryption. When using the post-quantum crypto transformations in a cloud-based environment, it is possible to apply several candidates that have close evaluation results, which requires further research and substantiation of the choice depending on the type and use of cloud environment by the clients.

3. Depending on the application, the system of criteria may and be refined or changed, for example depending on the environment. Among the selected post-quantum cryptographic mechanisms, all the requirements are satisfied only by the lattice-based algorithms, as well as signature based on hash functions and the encryption using isogenies. Other algorithms meet only the requirements of cloud-based environment.

References

[1] Koblitz N. A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes [Electronic Resource]. – Way of access: https://eprint.iacr.org/2015/1018.pdf. – Title from the screen.

[2] Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor // SIAM J. Comput. – 1997. – Issue 26 (5). – P. 1484 – 1509.

[3] Grover L. K. A fast quantum mechanics algorithm for database search / L. K. Grover [Electronic Resource]. – Way of access: http://cds.cern.ch/record/304210/files/9605043.pdf. – Title from the screen.

[4] Moody D. Post-Quntum Cryptography: NIST's Plan for the Future / D. Moody // The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016 [Electronic Resource]. – Way of access: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf. – Title from the screen.

[5] 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 [Electronic Resource]. – Way of access: http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/eproceedings_Crypto_2013.pdf. – Title from the screen.

[6] Jao D. Isogeny-Based Quantum-Resistant Undeniable Signatures / D. Jao, V. Soukharev // PQCrypto 2014. – P. 160–179.

[7] Postkvantova kryptografija ta mehanizmy i'i' realizacii' / I.D. Gorbenko, O.O.Kuznjecov, O.V.Potij ta in. // Radiotehnika. – 2016. – Vyp. 186. – S. 32–52.

[8] Gorbenko Ju.I. Metody pobuduvannja ta analizu, standartyzacija ta zastosuvannja kryptografichnyh system / Ju. I. Gorbenko: monografija; za zag. red. I. D. Gorbenko. – Harkiv: Fort, 2015. – 959 s.

[9] Lenstra H. W. Analysis and comparison of some integer factoring algorithms, in Computational Methods in Number Theory / H. W. Lenstra, Jr. Tijdeman , R. Tijdeman // Math. Centre Tract 154. – 1982. – P. 89–141.

[10] Yesina M. Methods of cryptographic primitives comparative analysis / Maryna Yesina, Yurij Gorbenko // Inżynier XXI wieku ("Engineer of XXI Century"): the VI Inter University Conference of Students, PhD Students and Young Scientists; University of Bielsko-Biala, Poland, December 02, 2016. – Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016. – P. 451–462.

[11] Nogin V. D. Uproshchennyi variant metoda analiza ierarkhii na osnove nelineinoi svertki kriteriev / V. D. Nogin [Elektronnyi resurs]. – Rezhim dostupa: http://www.apmath.spbu.ru/ru/staff/nogin/nogin_p11.pdf. – Zagl. s ekrana.

[12] Ekspertnye otsenki pri razrabotke reshenii [Elektronnyi resurs]. – Rezhim dostupa: http://books.ifmo.ru/file/pdf/817.pdf – 20.05.2016. – Zagl. s ekrana.

[13] Wang H. An efficient quantum meet-in-the-middle attack against NTRU-2005 / H. Wang, M. Zhi, M. ChuanGui // Chinese Science Bulletin. – 2013. – Vol. 58. – № 28–29. – P. 3514–3518.

[14] An Improved MITM Attack Against NTRU / Zhijian Xiong, Jinshuang Wang, Yanbo Wang et al. // International Journal of Security and Its Applications. – 2012. – Vol. 6. – № 2. – P. 269–274.

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

Надійшло: Червень 2017.

Автори:
Іван Горбенко, д.т.н., проф., лауреат Державної премії України, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: gorbenkoi@iit.kharkov.ua

Володимир Пономар, аспірант, ХНУ імені В.Н. Каразіна, Харків, Україна.
E-mail: laedaa@gmail.com

Марина Єсіна, аспірантка, ХНУ імені В.Н. Каразіна, Харків, Україна.
E-mail: rinayes20@gmail.com

Дослідження можливості використання та переваг постквантових алгоритмів залежно від умов застосування.

Анотація. Встановлена необхідність проведення порівняльного аналізу та оцінки можливості використання асиметричних постквантових криптографічних механізмів. Для порівняння обрано методику оцінювання на основі інтегральних оцінок безумовних і умовних критеріїв. Аналіз проведено серед алгоритмів, що задовольнили загальні безумовні критерії. В якості умовних критеріїв обрано чисельні характеристики алгоритмів. Крім того, висувалися додаткові безумовні критерії, що відрізнялися залежно від умов застосування. Актуальність досліджень пов'язана з прогнозом появи квантового комп'ютера. А в існуючих дослідженнях вже доведено, що поточні криптографічні алгоритми мають вразливості до методів квантового криптоаналізу. Тому вже зараз лідируючі інститути стандартизації криптоалгоритмів проводять дослідження та порівняння для вибору постквантового стандарту криптографії. У результаті досліджень було встановлено відсутність універсального постквантового криптографічного алгоритму. Запропоновано відокремити три варіанти використання постквантових алгоритмів: для легкої криптографії, використання стандартними автоматизованими системами і використання в хмарному середовищі. Для кожних умов застосування проведено окреме оцінювання переваг криптографічних алгоритмів. Виявлені недоліки лідируючого кандидата. Надані рекомендації використовувати ці алгоритми в якості основного на час перехідного періоду. А, якщо підозра підтвердиться, запропоновано альтернативи. Результати досліджень дозволяють зрозуміти поточний стан розвитку постквантових криптоалгоритмів і спрогнозувати можливий їх подальший розвиток. Практичне значення дослідження полягає в отриманні оцінки постквантових алгоритмів в залежності від умов застосування.

Ключові слова: постквантові криптографічні алгоритми, порівняльна оцінка криптоалгоритмів, критерії порівняння криптоалгоритмів.

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

Поступила: Июнь 2017.

Авторы:
Иван Горбенко, д.т.н., проф., лауреат Государственной премии Украины, Харьковский национальный университет имени В. Н. Каразина, Украина.
E-mail: gorbenkoi@iit.kharkov.ua

Владимир Пономарь, аспирант, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: Laedaa@gmail.com

Марина Есина, аспирантка, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: rinayes20@gmail.com

Исследование возможности использования и преимуществ постквантовых алгоритмов в зависимости от условий применения.

Аннотация. Была установлена необходимость проведения сравнительного анализа и оценки возможности использования асимметрических постквантових криптографических механизмов. Для сравнения выбрано методику оценивания на основе интегральных оценок безусловных и условных критериев. Анализ проводился среди алгоритмов, которые удовлетворили общие безусловные критерии. В качестве условных критериев выбрано численные характеристики алгоритмов. Кроме того, выдвигались дополнительные безусловные критерии, которые отличались в зависимости от условий использования. Актуальность данных исследований связана з прогнозом появления квантового компьютера. А в существующих исследованиях уже доказано, что текущие криптографические алгоритмы имеют уязвимости к методам квантового криптоанализа. Поэтому уже сейчас лидирующие институты стандартизации криптоалгоритмов проводят исследования и сравнения для выбора постквантового стандарта криптографии. В результате исследований было установлено отсутствие универсального постквантового криптографического алгоритма. Предложено выделить три варианта использования постквантовых алгоритмов: для легкой криптографии, использование стандартными автоматизированными системами и использование в облачной среде. Для каждых условий применения проведено отдельное оценивание преимуществ криптографических алгоритмов. Выявлены недостатки лидирующего кандидата. Даны рекомендации использовать эти алгоритмы в качестве основного на время переходного периода. А, если угроза подтвердится, предложены альтернативы. Результаты исследований дают понять текущее состояние развития постквантовых криптоалгоритмов и спрогнозировать возможное их дальнейшее развитие. Практическое значение исследования заключается в получении оценки постквантовых алгоритмов в зависимости от условий применения.

Ключевые слова: постквантовые криптографические алгоритмы, сравнительная оценка криптоалгоритмов, критерии сравнения криптоалгоритмов.