UDC 004 056 55

PROPOSALS OF COMPARATIVE ANALYSIS AND DECISION MAKING DURING THE COMPETITION REGARDING THE CERTAIN BENEFITS OF ASYMMETRIC POST QUANTUM CRYPTOGRAPHIC PRIMITIVES

I. Gorbenko, Yu. Gorbenko, M. Yesina, V. Ponomar

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

Reviewer: Roman Oliynikov, Dr., Full Professor, V.N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
roliynykov@gmail.com

Received on February 2017

Abstract. *The paper considers proposals on the implementation of cryptographic primitives comparative analysis and substantiation, development and experimental confirmation of methodical bases application possibilities of system unconditional and conditional criteria selection and application, and methods and technique of comparative analysis and making the decision on asymmetric post quantum cryptographic primitives type directional encryption, and keys encapsulation and electronic signatures mechanisms. Some criteria and indicators that can be used for comparative analysis of properties of the candidates for the post quantum cryptographic primitives are presented. Comparative analysis of the existing mechanisms of perspective electronic signatures in accordance with ISO/IEC 14888-3:2016 standard and some cryptographic primitives that are considered possible to use in the post quantum period is carried out. The results of the cryptographic primitives conducted estimation are presented. Conclusions and recommendations on the use of certain cryptographic primitives estimation methods are made.*

Keywords*: electronic signature mechanisms analysis, weight indices, electronic signature, electronic signature estimation criterion, electronic signature comparison analysis methods.*

1 Introduction

In 2016 there were the series of important events, that have significantly affected to the intensive development of post quantum cryptography. To them should be referred the statement on the Internet – Alfred J. Menezes and Neal Koblitz articles [7], organization and conduction by NSA and NIST USA VII international conference on post quantum cryptography, which took place in February 2016 in Japan [12,14]. An extremely important event was the publication in the USA report «Report on Post – Quantum Cryptography. NISTIR 8105 (DRAFT)» [9], in which fully confirmed the possibility of electronic signatures (ES) asymmetric cryptographic systems successful quantum and the main cryptanalysis, problems and opportunities, and stages of their decision are identified.

NIST USA announced a competition to develop the standards of post quantum asymmetric cryptographic primitives [12], understanding the need to find new electronic signature asymmetric cryptographic primitives and asymmetric end-to-end encryption, which will be relevant and can be applied in post quantum period. The specified one due to two factors. First, there is significant progress in the development of quantum computers, including experimental demonstration of physical qubits realization are carried out, which can be scaled up to larger systems.

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

Proposals must be received by NIST to November 30, 2017. Filed proposals received before September 30, 2017 will be considered in terms of fulfillment of requirements completeness, and then pass through the stages of open civil research and standardization according to the announced requirements [12,14]. They shall apply to: directional encryption (E2EE) asymmetric mechanisms, keys encapsulation (KE) and electronic signature (ES). But a preliminary analysis of a creation

condition of a quantum computer and its capabilities in the future also confirms the previous list and essence of requirements announced by NIST.

The specified one, in our view, requires special attention to the selection estimation and comparing crypto primitives criteria and indicators, that would allow to take into account all the announced requirements and, if necessary, extend or narrow them.

The European Union has also started the preparation of a new post quantum standards. A new direction "Quantum-Safe Cryptography" are formed by European Organization for Standardization ETSI in the cluster "Security" [3,10,15]. According to the results of these studies are predicted the groups standards for post quantum period adoption. ETSI has published a group report "Quantum-Safe Cryptography. Quantum-Secure infrastructure" [3], in which fixed bases of perspective infrastructure, provided mechanisms, described primitives types, that will be used. Separately requirements are nominated and estimation criteria are formed for future candidates.

ES and E2EE, and their application mechanisms are allocated among the set of asymmetric cryptographic primitives. The specified one is explained by their wide application in a significant number of applications and potential large losses in case of discrediting ES and E2EE, that are used at present [4-6, 8].

Our experience obtained during the conducting research on projects AES and NESSIE [1,11], and in national standards for hash function DSTU 7564:2014 developing and adopting, and block symmetric encryption algorithm DSTU 7624:2014 [4,8] etc., allows to conclude, that the extremely important problem is substantiation of the estimation criteria system choice and comparison of each cryptographic primitives with other, and development and application the scientifically based techniques of them analysis and comparison in accordance with the nominated requirements. These methods and developed on their basis technique or techniques should take into account all requirements, that are nominated for asymmetric cryptographic primitives and allow to help make the decision about winners based on use the unconditional and conditional criteria system, as partial and integral.

The objective of these proposals are the substantiation, development and experimental confirmation of methodical bases application possibilities of system unconditional and conditional criteria selection and application, and methods and technique of comparative analysis and making the decision on asymmetric post quantum cryptographic primitives type directional encryption, and keys encapsulation and electronic signatures mechanisms.

2 The state of cryptographic primitives comparative analysis techniques development and application

After analysis, it was determined that the first time techniques of estimation and comparative analysis of cryptographic primitives type block symmetric cipher (BSC), streaming symmetric cipher (SSC), electronic signature (ES) and cryptographic protocol were proposed in [22,25], and detailed in [24]. They are based on the use of unconditional and conditional partial and integral criteria system, and indicators, that allow to assess the degree of nominated to the candidate requirements fulfillment. In our opinion the main task of these techniques are the formalization of decision-making processes regarding fulfillment of nominated to them requirements, taking into account the strengths and weaknesses of cryptographic primitives, that are candidates for the post quantum standard, reduce the influence of subjective factors in decision-making,. For example, following techniques can be applied to estimate and compare the ES, E2EE and KE mechanisms, which are the candidates for the post quantum standard in our case.

At the formal level such estimation and comparison techniques ES, E2EE and KE mechanisms can be summarized. But, since to these crypto primitives are nominated different requirements, then for each of the primitives they may be supplemented or simplified and display the entire spectrum of nominated requirements. Also, these techniques can ensure transparency of decision-making, experts independent, and help substantiate making appropriate decisions and confidence in them. Further in research technique we'll mean a fixed set of methods, methods of practice, tested and studied for the expedient implementation of specified work, that leads to a predetermined outcome [24].

In research in the broad sense we'll mean the search of new knowledge or a systematic investigation in order to establish the facts. In a narrow sense this is the scientific method (process) of study anything.

3 Criteria and indexes of cryptographic primitives ES and E2EE estimation

In criterion we'll mean the sign based on which estimate, determination or classification of anything are carried out [24], that is, in fact, we'll mean a measure of estimate. Our previous researchers have allowed to conclude, that cryptographic primitives comparison can be done using two criteria sets: unconditional and conditional [24]. This approach allows to make an estimate and compare the crypto transformations, that are candidates, in 2 stages. This approach is based, in particular, and on taking into consideration or use expert estimates.

At the first stage, at first checked the crypto transform conformity for the partial unconditional criteria system, and then unconditional integral criterion is calculated for each crypto primitive based on partial criteria. At the second stage appropriate estimates are obtained using at first partial conditional criteria system, and then integral conditional criterion is calculated on their base.

This two-step approach allows to reject crypto transformations, that do not meet the unconditional requirements, i.e. requirements, that must be fulfilled unconditionally. Moreover integral unconditional criterion allows to accept the decision regarding each of crypto primitives.

The partial conditional criteria using, and then integral conditional criterion using on their base, allow to estimate the crypto primitive quality in a broad sense, as the quality in average, and then compare crypto primitives, that are candidates for the post quantum algorithm, using the value of the integral criterion for each of crypto primitives. Estimation indexes of ES and E2EE asymmetric crypto transformations by unconditional criteria, that are recommended for use, is given further.

3.1 Unconditional estimation criteria of cryptographic transformations

To unconditional criteria will refer those criteria, which fulfillment is mandatory for cryptographic primitive, that is unconditional. Moreover, in our view, for asymmetric crypto transformations type ES and E2EE you can select the same unconditional criteria system. But this does not preclude the consideration possibilities of requirements features and according to the choice in the analysis and estimation of cryptographic primitives additional partial unconditional criteria. Let's consider and choose at first the partial unconditional criteria system, based on the NIST requirements [12,14].

Requirements analysis, that are nominated by NIST for asymmetric cryptographic transformation type ES and E2EE partial unconditional criteria, our experience in the development and estimation of crypto transformations type ES, BSC, SSC etc. properties [24], achieved results in the practical solution of cryptanalysis problems, including based on quantum cryptanalysis algorithms implementations [24], allow to choose unconditional estimation criteria ES and E2EE at least, listed in Table 1.

As the listed partial criteria are unconditional, then the selection criterion is a logical variable yes/no (1/0), so the unconditional criterion can be written as:

$$(W_1,\ W_2,\ W_3,\ W_4,\ W_5,\ W_6,\ W_7,\ W_8) \in (1,0). \quad (1)$$

In view of described above partial unconditional criteria W1–W8 and condition (1), the crypto transformation compliance function to requirements, that are set out above, written as integral unconditional criterion:

$$fi() = W_1 \wedge W_2\,(W_3) \wedge W_4 \wedge W_5 \wedge W_6 \wedge W_7 \wedge W_8 = W_\delta, \quad (2)$$

where the symbol «∧» indicates the Boolean variables conjunction operation according to (1). It should be noted that in (2) W_3 is taken in parenthesis, that should be used either W_2 or W_3.

Table 1 – Unconditional estimation criteria of ES and E2EE

№	Unconditional criteria	Denotation
1	Reliability, simplicity and transparency of mathematical base (mathematical transformations) used in the implementation of post quantum cryptographic transformations ES and E2EE.	W1
2	Practical security of E2EE type cryptographic transformations in the mechanism "semantically secure encryption" implementation against known attacks using a quantum computer and cryptanalyst access to the 264 selected ciphertexts for security model IND–CCF2.	W2
3	Practical security of ES type cryptographic transformations against known attacks using a quantum computer and cryptanalyst access to the 264 selected ciphertexts for security model EUF–CMA.	W3
4	The validity of real security (stability) ES or E2EE cryptographic transformations against all known and potential cryptanalytic attacks of post quantum period based on the use of common parameters and keys with the necessary size and properties (128-bit keys and more classical stability (safety)).	W4
5	Theoretical security of ES or E2EE type cryptographic transformations in post quantum period against existing force, analytical and special attacks for existing threats models (at least for the model EUF-CMA for ES and IND-CCF2 for E2EE).	W5
6	The possibility of replacing existing standardized cryptographic primitives to the post quantum ones and application in the existing cryptographic systems and protocols in certain conditions and restrictions.	W6
7	Computational efficiency – complexity of direct I_{dir} and reverse I_{rev} cryptographic transformations ES and E2EE, and generating asymmetric key pairs I_{key} is not above polynomial, providing the necessary complexity (performance) values I_{dir}, I_{rev}, I_{key} in practical use in applications with their hardware and software, and program implementation.	W7
8	The performance of limitations for minimum and maximum lengths of private and public key, sizes and unprofitability of ciphertext and ES, the absence of weak private keys for post quantum period security models.	W8

That is, the post quantum cryptographic transformation ES and E2EE quality can be estimated using the integral unconditional criterion – compliance function as integral unconditional criterion

$$f_i() = 1, \tag{3}$$

if cryptographic transformation ES and E2EE corresponds to demanded requirements and

$$f_i() = 0, \tag{4}$$

if cryptographic transformation ES and E2EE does not correspond to demanded requirements.

Thus, according to (1–4) can formalize the decision according to the candidate conformity for post quantum type ES and E2EE cryptographic transformation to nominated for it demands. Thus, if the condition (3) is carried out, the crypto primitive is corresponding to the unconditional requirements, otherwise, that is when we get (4), then the corresponding crypto primitive does not meet the requirements and it is rejected from the further consideration.

3.2 Conditional estimation criteria of cryptographic transformations ES and E2EE

Qualitative and quantitative comparison of type EP and E2EE cryptographic transformations can be carried out using preferences partial conditional and generalized conditional criterion [22, 24, 25]. Table 2 provides a list and designations of estimating partial conditional criteria of type ES and E2EE cryptographic transformations, whose requirements are nominated by NIST [12,14].

Table 2 – Conditional estimation criteria of ES and E2EE

№	Conditional criteria	Denotation
1	Additional security features: - perfect forward secrecy; - resistance to side-channel attack; - resistance to multi-key attacks; - resistance to failures.	K1
2	Stability requirements 1) classic security 128-bit / 64-bit quantum protection (stability reserve AES-128); 2) classic security 128-bit / 80-bit quantum protection (stability reserve SHA-256/ SHA3-256); 3) classic security 192-bit / 96-bit quantum protection (stability reserve AES-192); 4) classic security 192-bit / 128-bit quantum protection (stability reserve SHA-384/ SHA3-384); 5) classic security 256-bit / 128-bit quantum protection (stability reserve SHA2-512, SHA3-512);	K2
3	Additional requirements to stability 6) classic security 512-bit / 256-bit quantum protection (stability reserve SHA-512/ SHA3-512, DSTU 7564: 2014 – 512 bit); 7) classic security 512-bit / from 128-bit to 256-bit quantum protection (stability reserve DSTU 7624:2014 (Kalyna – 512)); 8) classic security 512-bit / quantum protection (stability reserve DSTU 7624:2014 (Kalyna – 512)).	K3
4	Encryption errors. The low percentage of encryption errors.	K4
5	The possibility of multiple E2EE or ES.	K5
6	Flexibility: 1) additional scheme options (optimization, implicit keys exchange etc.); 2) cross-platform; 3) the possibility of parallelization.	K6
7	Correctness verification. Checking the correctness of basic and optimized implementations.	K7

Continuation of Table 2

№	Conditional criteria	Denotation
8	Effectiveness verification: Calculation of time needed for key generation, encryption, decryption, digital signature, signature verification or keys establishing (testing is carried out on optimized versions).	K8
9	Test conditions The main platforms: 1) NIST PQC Reference Platform; 2) Intel x64; 3) Windows or Linux, the GCC compiler; 4) Additional testing of other conditions (8-bit processors, digital signal processors, dedicated CMOS etc.)	K9
10	Possibility and conditions of free distribution post quantum crypto transformations ES or E2EE.	K10
11	Confidence level to the post quantum crypto transformations ES or E2EE at different levels of use.	K11
12	Perspective and justification the use of post quantum crypto transformations ES or E2EE.	K12

As basic components of the generalized preferences criterion proposed to use such partial conditional criteria as shown in Table 2.

4 The partial unconditional criteria and integral unconditional criterion calculation

At the first stage the estimation and verification of post quantum crypto primitives ES and E2EE mechanisms is carried out by partial unconditional criteria and integral unconditional criterion. Partial unconditional criteria are defined by the data, given in Table 1. Estimates are made using the criteria given in Table 1, using the expert estimates methods. Unconditional criteria values are received as a result of expert estimates

$$(W_1, W_2(W_3), W_4, W_5, W_6, W_7, W_8), \quad (5)$$

that take the binary values 1 or 0 (yes/no). Integral unconditional criterion is determined based on these values according to (2)

$$f(W_1, W_2(W_3), W_4, W_5, W_6, W_7, W_8) \quad (6)$$

In the integral unconditional criterion $f() = 1$ post quantum cryptographic primitive passes the test and verification, otherwise, in the integral unconditional criterion $f() = 0$, it is rejected and is not considered further.

Introduced so integral criterion allows to establish, whether the considered type ES or E2EE crypto transformation is responded to nominated unconditional requirements. In case of positive estimation ES or E2EE by integral unconditional criterion, their subsequent comparison and estimation can be made on the basis of partial conditional criteria and as a result, integral conditional criteria [20]. It should be noted that in (5) and (6) W_3 is taken in parenthesis, that should be used either W_2 or W_3.

5 Expert estimation methods

In expert estimates understand the search method and the result of applying the method, that obtained based on the use of personal expert opinion or collective expert group opinion, and a set of logical and mathematical procedures aimed at obtaining information from specialists, its analysis and generalization in order to prepare and making rational decisions [19, 20].

5.1 The expert estimations method application

Application of the expert estimates method generally associated with the implementation of the experts selection procedures, the experts selection and establishment the expert opinion consistency degree.

Expert estimation methods used in situations, when the choice, substantiation and estimation of decisions cannot be made based on accurate calculations [19].

The expert estimates results statistical processing similar to measurement results statistical processing. On the expertise reliability significantly influenced such factors as the expert group size, the experts competence level, the questions composition, offered to experts, etc. [19].

Individual expert estimates also bear the stamp of chance; mood, health, environment, and knowledge and expert experience.

5.2 The experts selection procedure

Expert – a competent person to produce the estimate, that has special experience in a particular area and participating in the research as sources of information [19].

Among the a priori estimation methods of experts quality are the widespread self-concept methods as the most simple in mathematical terms. In this methods group, each expert evaluates himself on any scale – point or verbal-numerical. One of the main problematic tasks by this estimation is the problematic task of same understanding the scales grading by experts.

A variety of self-assessment is a differential method, which usually the estimate is given by the two criteria groups, that characterize expert acquaintance with expertise objects and by criteria, and expert introduce with the main information sources in this area.

It is possible to determine the level of expert competence in mutual estimation. In a simpler case, each expert from the given experts group indicates the list of experts, whom he considers as competent in this area. Coefficient expert competence is defined as the ratio of the lists number, in which is given expert, to the total lists number. This method allows to receive the increased experts estimates.

Another approach consists in the mutual estimating by experts of each other: q_{ij} – estimate in points of the i-th expert. The combination of these estimates forms the definitely orderly matrix. The consistent application of the same procedure to this matrix and interim values vector of competence estimates, obtained in the previous step, gives the finite values vector of experts competency estimates in the result [19]. Another approach based on the fact, that the expert competence must be estimated by how its assessment coordinated with estimates of most.

An effective means of experts estimating is the test method. It is important the following testing moments [19]:

1 - test should be designed for specific expertise objects;

2 - it is necessary the scale, that allows to determine the expert estimates accuracy degree;

3 - the probability of random guessing the true estimate by expert in text experiment should be sufficiently small.

In the case of test method can achieve the simplification, if it is enough data about results of specialist participation in similar expertise. In this case, about the expert competence can be judged on relative to the number of "accurate" estimates are made by him, to the total number of estimates are rendered by him.

Thus, there are several possible experts choice variants. Variant choice depends on how accurate should be estimate and on the complexity of the estimation procedure.

5.3 The experts selection

Depending on the problem task scale, that is solved, the expertise organization is carried out by a person, who makes the decision or management group is designed by him. The selection of quantitative and qualitative experts composition is carried out based on the analysis of problem task breadth, required estimates reliability, experts characteristics and resource costs [19].

The latitude of solved problematic task determines the need for involvement in expertise specialists from different fields. However, the minimum number of experts is determined by quantity of various aspects and directions, that need to be taken into account when deciding the problematic task.

The reliability of experts group estimates depends on the knowledge of individual experts and the number of experts in the group.

The spending resources on the expertise is proportional to the number of experts. Usually to the estimation are attached 5–12 experts [19]. Characteristics of the experts group are determined by the individual experts characteristics: competence, creativity, relevance to the expertise, conformity, thinking constructive, collectivism, self-criticism [19].

Competence – the degree of expert qualification in a particular field of knowledge.

Conformity – propensity to authorities influence.

Relevance to the expertise – negative or passive specialist attitude to solve the problematic task, high employment and other factors significantly effect to the experts functions performance.

Thinking constructive – pragmatic aspect of thinking.

Collectivism – should be taken into consideration during the open discussions.

Self-criticism –it is manifested in the self-concept degree of own competence and taking into account other experts opinions and decision making of this problematic task.

5.4 The expert opinions coherence degree establishing

In case of participation in the survey several experts, discrepancies in their estimates are inevitable, but the value of this difference is important. Group estimate can be considered sufficiently reliable only on condition of good coordination the individual professionals responses.

For analysis of estimates scatter and coherence used statistical characteristics – the measures of scatter or statistical variation [19,21].

5.5 The algorithms ES and E2EE estimation by conditional criteria

In case of a positive estimate of cryptographic transformation ES or E2EE by integral unconditional criterion, further comparison and estimation can be made based on determination the conditional criteria (Table 2) and their comparison by integral conditional criterion.

The main method of calculating the integral conditional criterion value is the partial conditional criteria clotting in integral conditional criterion. As the main methods of partial conditional criteria clotting can choose the analytic hierarchy process based on pairwise comparisons or method of determining the weight indices [20].

6 The analytic hierarchy process based on pairwise comparisons and features of its application for estimation ES and E2EE

For application the analytic hierarchy process must choose conditional criteria and indicators system for getting the values according to conditional criteria. With this set of indicators, means the use of conditional criteria can calculate the integral conditional criteria value and, as a result, make the ES or E2EE comparison by conditional integral criterion.

The method pairwise comparison essence consists in the following [2,20]. The set of pairwise comparisons matrices is constructed. Pairwise comparisons are carried out in terms of the dominance one element over another. Obtained opinions are expressed in integers, taking into account the scale, for example, the used nine.

6.1 The essence and conditions of use the pairwise comparisons method in cryptography

In pairwise comparison the expert compares researched objects of their importance in pairs, sets the most important object in each pair. All possible objects pairs expert represents in a record of each combination (object 1–object 2, object 2–object 3, etc.) or in the matrix form [18,20].

The method of pairwise comparisons is very simple and it allows to explore a large number of objects (compared, for example, by ranking method) and with greater accuracy [20].

Let $E_1,E_2,...,E_n$ – plenty of n elements (alternatives) and $v_1,v_2,...,v_n$ – according to their weight or intensity. Let's compare pairwise weight or intensity of each element with weight or intensity of any other element of the set relative to the total for them property or goal (relative to the element–"father").

When constructing a pairwise comparisons matrix for all criteria is necessary to determine the coherence ratio [20] for each criteria as follows.

The estimate of the eigenvector component calculated by the formula:

$$q_i = (W_{yi} \times W_{yi+1} \times \ldots \times W_{yn})^{\frac{1}{n}}. \quad (7)$$

Normalized estimate of priority vector calculated by the formula:

$$r_i = q_i \div z, \quad (8)$$

where z – matrix coherence ratio, calculated by the formula:

$$z = \sum_{i=1}^{n} q_i \ . \quad (9)$$

Matrix coherence ratio value is in the range $[0, \sum_{i=1}^{n} q_{i\max}]$, where $q_{i\max}$ – the maximum possible eigenvector component estimate value for selected case.

Let's further consider the results of cryptographic primitives estimation by this estimation method on the ES ISO/IEC 14888-3:2016 algorithms example.

7 Method and suggestions of the estimation and ES comparative analysis based on the weight indices

7.1 General formulation of the comparative analysis problem

The other class of clotting partial conditional criteria in the integral conditional criterion methods are formalized methods based on defined weight indices. Preliminary analysis is shown that most of them can be applied essentially to clotting the private conditional indicators [13,16,20,21]. Let's consider them on an example ES algorithms ISO/IEC 14888-3:2016 similarly as in section 6 (it is clear for what reasons cannot be considered post quantum crypto primitives ES and E2EE, because they do not exist in the approved form).

Let need to estimate the ES set according to the specified standard [4,5], which consists of:

1) k ES algorithms, which is necessary to estimate;
2) m indicators, by which each of ES alternatives are estimated;
3) n experts, which conducts ES estimation.

As partial indicators can be used indicators similar to partial conditional criteria specified above.

We can distinguish the following methods of weight indices:

- weight indices and ES estimation using the Fishburn scale;
- weight indices and ES estimation based on the ranking method;
- weight indices and ES estimation based on the points attribution method;
- weight indices and ES estimation based on the numerical method.

Let's consider and compare the mentioned methods by an integral conditional criteria ultimately.

7.2 The method of determining weight indices and ES estimation using the Fishburn scale

In the method of weight indices and ES estimation using the Fishburn scale the following steps are carried out.

1. Every indicator x_i, $i=1,...,m$ is assigned an estimation of its importance. Then the system of weights is constructed so that [20,21]

$$\begin{cases} \sum_{i=1}^{m} a_i = 1, \\ a_i \geq 0, i = 1,....,m \end{cases}, \quad (10)$$

where a_i – i-th indicator weights, i – indicator number, m – indicators quantity.

2. Indicators are ranked by the importance decreasing of each, so that:

$$x_1 \succ x_2 \succ x_3 \succ ... \succ x_i \succ ... \succ x_m .$$

3. Weight indices using the Fishburn scale are determined:

$$a_i = \frac{2 \cdot (m - i + 1)}{m \cdot (m+1)}. \quad (11)$$

4. The weight indices value and their average value are entered in Table 3, where $\overline{a_i}$ – weight indices arithmetic average for the i-th indicator, and $w_i = \overline{a_i}$ – weight indices values.

Table 3 – The weight indices value 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

7.3 The method of determining weight indices and ES estimation based on the ranking method

In the method of weight indices and ES estimation based on the ranking method the following steps are carried out.

1. The most important indicator corresponds to rank (estimate) m, the following – (m-1) and etc., the rank equals to 1, is the least important indicator. Then, the weight indices are determined by the formula [16,20]:

$$w_j = \frac{r_j}{\sum_{j=1}^{m} r_j}, \quad j = 1,...,m, \quad (12)$$

x_m – m-th indicator, r_j – j-th rank (estimate), n – experts quantity, m – indicators quantity.

2. Results of the experts survey are written in Table 4. In the penultimate string of this table ranks sum (estimates) is written, that have been exposed by experts, and in the last string of table indicators weight indices values are recorded. According to the estimation rules in accordance with specified method, we build the table for indicators and tables for all ES algorithms.

Table 4 – The weight indices value

Experts \ Indicators	x_1	x_2	…	x_m
1	r_{11}	r_{12}	…	r_{1m}
2	r_{21}	r_{22}	…	r_{2m}
…	…	…	…	…
n	r_{n1}	r_{n2}	…	r_{nm}
$r_j = \sum_{i=1}^{n} r_{ij}$	r_1	r_2	…	r_m
w_j	w_1	w_2	….	w_m

7.4 The method of determining weight indices and ES estimation based on the points attribution method

1. In method of determining weight indices and ES estimation based on the points attribution method first experts, depending on the importance indicator, give grades from 0 to 10, whereby it is permitted to estimate the indicator importance by fractional values, as well as the various indicators can attribute the same points [13,16,20].

2. It is determined the each indicator weight, calculated by each expert [20]:

$$r_{ij} = \frac{h_{ij}}{\sum_{j=1}^{m} h_{ij}}, \tag{13}$$

where r_{ij} – j-th indicator weight, defined by i-th expert, h_{ij} – i-th expert point, exhibited j-th indicator, n – experts quantity, m – indicators quantity.

3. The final indicators weight indices are determined by the formula [20]:

$$w_j = \frac{\sum_{i=1}^{n} r_{ij}}{\sum_{j=1}^{m}\sum_{i=1}^{n} r_{ij}}. \tag{14}$$

All obtained values are entered to the table (Table 5).

7.5 The method of determining weight indices and ES estimation based on the numerical method

The method of weight indices and ES estimation based on numerical method is implemented so.

1. For each indicator is calculated the relative scatter ratio by the formula [20]:

$$\delta_i = \frac{x_{i\max} - x_{i\min}}{x_{i\max}}, \tag{15}$$

where $x_{i\max}$, $x_{i\min}$ - in accordance with the max and min i-th indicator value, m - indicators quantity.

Table 5 – The weight indices value

Indicators / Experts	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	$w_1=\frac{r_1}{\sum_{j=1}^{m} r_j}$	$w_2=\frac{r_2}{\sum_{j=1}^{m} r_j}$		$w_m=\frac{r_m}{\sum_{j=1}^{m} r_j}$

2. The indicators value is determined by any of the above methods.

3. The weight indices get the most important value for those indicators, those relative scatter is more significant. All obtained data are entered to the table (Table 6).

Table 6 – The weight indices value

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

4. The indicators values are found by any one of the above methods.

$$w_i = \frac{\delta_i}{\sum_{i=1}^{m} \delta_i}. \qquad (16)$$

7.6 The ES mechanisms research results analysis according to the conditional integral criteria

The listed above results were obtained by selected ES algorithms estimation methods. The comparison of ES algorithms was made based on expert estimates. After that calculations were made by aforementioned methods.

It is believed that the results of ES algorithms estimation by various methods of weight indices were obtained almost identical – almost the same ES algorithms order from the best to the worst.

Numeric scatter of weight indices values for one algorithm is negligible, only numeric values for ES algorithms IBS-1,2 in the analytic hierarchy process based on pairwise comparisons different from weight indices values for these ES algorithms by other estimation methods. This is conditioned by more strong influence of subjective expert opinion on estimates result in a certain method. Table 7 shows the results of ES algorithms estimation by all estimation methods. Figure 1 shows graphically the results of ES algorithms estimation by various methods.

Table 7 – The results of ES algorithms estimation

Pairwise comparisons method	Methods of determining weight indices			
	using the Fishburn scale	based on the ranking method	based on the points attribution method	based on the numerical method
IBS-1 – 0,256 IBS-2 – 0,256 EC-KCDSA – 0,144 EC-GDSA – 0,125 EC-DSA – 0,099 EC-SDSA – 0,048 EC-FSDSA – 0,048 EC-RDSA – 0,025	IBS-1 – 0,159 IBS-2 – 0,159 EC-DSA – 0,15 EC-GDSA – 0,147 EC-KCDSA – 0,142 EC-FSDSA – 0,118 EC-SDSA – 0,117 EC-RDSA – 0,106	IBS-1 – 0,147 IBS-2 – 0,147 EC-KCDSA – 0,143 EC-GDSA – 0,142 EC-DSA – 0,139 EC-FSDSA – 0,115 EC-SDSA – 0,111 EC-RDSA – 0,103	IBS-1 – 0,137 IBS-2 – 0,137 EC-RDSA – 0,132 EC-FSDSA – 0,128 EC-DSA – 0,127 EC-SDSA – 0,127 EC-GDSA – 0,126 EC-KCDSA – 0,124	IBS-1 – 0,15 IBS-2 – 0,15 EC-DSA – 0,144 EC-GDSA – 0,141 EC-KCDSA – 0,138 EC-FSDSA – 0,126 EC-SDSA – 0,123 EC-RDSA – 0,109

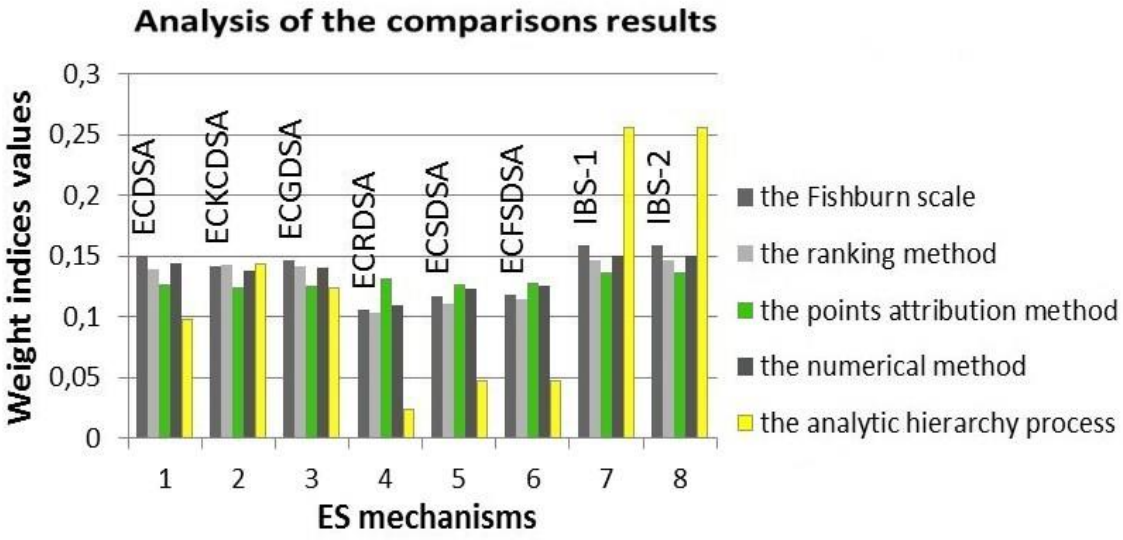

Fig. 1 – The results of ES algorithms estimation by different methods

Table 8 shows the averaged results of ES algorithms estimation by all estimation methods. Figure 2 shows graphically the averaged results of ES algorithms estimation by various methods.

Table 8 – The averaged results of ES algorithms estimation

Algorithm	Averaged estimate	Algorithm	Averaged estimate
EC-DSA	0,1318	EC-SDSA	0,1052
EC-KCDSA	0,1382	EC-FSDSA	0,107
EC-GDSA	0,1362	IBS-1	0,1698
EC-RDSA	0,095	IBS-2	0,1698

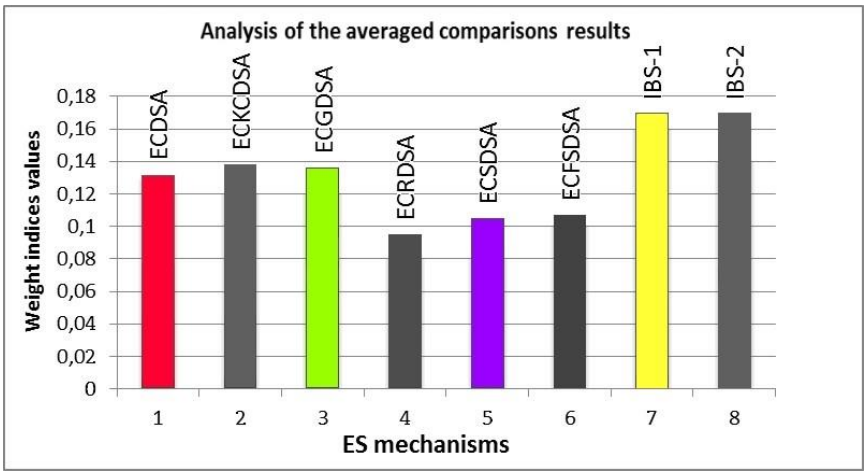

Fig. 2 – The averaged results of ES algorithms estimation by different methods

8 Features and requirements for cryptographic primitives in post quantum period

8.1 Intruder and threats models in the post quantum period

The analysis are showed, that a quantum computer can be considered as the basic intruder model, and methods and algorithms, that implemented on quantum computers – as threats models.

In our opinion the second problem task is successfully solved. So today there are quantum methods and developed based on these algorithms that allow to carry out attacks on asymmetric cryptosystem RSA, DSA, ECC and NTRU [24]. These include, first of all, should be referred quantum algorithms such as [24]: Grover quantum algorithm; Shor factorization algorithm; Shor algorithm for discrete logarithm; Wang algorithms etc.

Given the haste, with which USA and EU have started to build post quantum computers, and advances in this direction, it'll appear immediately in an explicit form after some time. So in the "1000-qubits" computer qubits actually are organized in clusters of 8 qubits each.

8.2 Preliminary analysis of asymmetric post quantum crypto transformations

In the Table 9 are shown general characteristics of mathematical apparatus, on which ES mechanisms are based, using which can be developed quantum-protected ES algorithms [3,12,14,23,24].

Shown in the table 10 ES mechanisms are proposed by ETSI for further study and research as possible candidates for quantum-protected ES circuits. Analysis of the data, that is given in the Tabl. 9,10, allows to conclude about advantages and disadvantages of some crypto transformations.

Table 9 – Directions of quantum-protected asymmetric algorithms

Cryptography scheme	Signature	Encryption	Key size	Data type	Core Ops.	Cryptographic Maturity
Hash-Based	Yes	No	≈ 20	Hash out.	Hashing	High
Multivariate Quadratic	Yes	No	≈ 10k	GF(2m)	Matrix LSE	Low, medium schemes
L-B: NTRU General lattice	Maybe Maybe	Yes Yes	< 0.1k ≈ 100k	Zq GF(2m)	Matrix mult. Medium	Medium Medium
Code-Based	Expensive	Yes	≈ 100k	GF(2m)	Matrix mult.	High, with prec. to impl.

Table 10 – Comparison of key lengths and signatures for quantum-protected ES algorithms

Type	Scheme	Security *(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
MQ	Quartz	80	72 237	16
	UOV	128	413 145	135
	Cyclic-UOV	128	60 840	135
	Rainbow	128	139 363	79
	Cyclic-Rainbow	128	48 411	79
Code	Parallel-CFS	120	503 316 480	108
	Cayrel et al	128	10 920	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

8.3 Substantiation parameters and keys in comparing

The preliminary results of available post quantum algorithms comparison have been obtained during the study. Restrictions were used due to lack of complete information. Table 11 presents some comparison parameters and properties.

Table 11 – Indexes and properties of post quantum crypto primitives

Parameters/ Algorithms	Crypto-graphy stability	The public key length	The private key length	The signature length	Direct conversion speed	Reverse conversion speed
	1	*2*	*3*	*4*	*5*	*6*
1. NTRU	128	988	256	988-	0,5	0,02
2. BLISS	128	896	256	640	0,02	0,02
3. Quartz	80	72237	3000	16	2	0,05
4. XMSS	128	1700	280	2083	2	0,2
5.SPHINCS	128	1056	1088	41000	2	0,2
6.RankSign	130	7200	21600	1080	0,02	0,02
7. Jao-Souk	128	768	768	1280*	5	5

Note: *Cryptography strong is given in bits, data size – in bytes, and the transformations speed – as a coefficient relative to speed of corresponding RSA algorithm transformation with a key length of 4096 bits.*

8.4 Comparative estimation of the using cryptographic algorithms

Table 12 is given the result of determining the weighting indexes according to expert estimates for the electronic signature mechanisms for standard automated systems cryptography *(number from Table 11)*.

Table 12 – The weights indices of standard signature mechanisms

Criteria	1	2	3	4	5	6
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	0,153	0,089	0,058	0,274	0,153	0,274
W	0,178	0,202	0,075	0,134	0,138	0,273

The level of estimates consistency is 0,3, which satisfies the requirements. BLISS algorithm has a level 0,763, XMSS – 0,237 after conducting estimates.

In the table 13 is given the result of determining weight indices of encryption mechanisms in cloud environment.

Table 13 – The encryption weights indices for cryptography in the cloud

Criteria	1	2	3	4	5	6
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	0,243	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

The level of estimates consistency is 0,3, which satisfies the requirements. NTRU algorithm has a level 0,685, Jao-Sukharev – 0,315 after conducting estimates.

9 Conclusions

1. In comparing post quantum algorithms it is proposed to use the system of unconditional and conditional partial and integral criteria. To unconditional criteria will refer those criteria, which fulfillment is mandatory for cryptographic primitive, that is unconditional. Conditional is called criteria, which performance for any ES is carried out by only defined condition.
2. The researches results are showed, that as the main criterion for integral estimation can be recommended to use the integral unconditional criterion, that is derived based on partial unconditional criteria. If at least one partial criterion does not meet conditions, then this ES is rejected.
3. To determine the integral conditional criterion regarding ES standard is possible to use several methods, such as: analytic hierarchy process based on pairwise comparisons and method of determining weight indices.
4. Conducted analysis and studies allowed to compare the properties of selected estimation methods, and to identify the advantages and disadvantages of each method. To obtain the final

result by this method, it is necessary to multiply the level 1 priorities vector and acquired values level 1 matrix, and ranging obtained numerical values from the highest to the lowest.

5. In post quantum period as the basic model infringer can be considered a quantum computer, and as the basic model of threats – methods and algorithms of quantum cryptanalysis.
6. Table 9 shows general characteristics of mathematical apparatus, on which ES mechanisms are based. Tables 12 and 13 are shown the results of weight indices determination according to expert estimates for post quantum crypto primitives that are presented in Table 11.
7. In general, according to the results of the comparative analysis we can conclude, that the best choice among all candidates is the choice of algorithms that use lattices. The disadvantage of these algorithms is that according to recent studies, these algorithms have reduced complexity for quantum attack "meeting in the middle", but this complexity is satisfactory for minimal requirements. So these algorithms are the best choice for the transitional period, which will give the time with sustainable algorithms to search the further improve decisions of these algorithms, or search of other options.

References

[1] AES: the Advanced Encryption Standard [Electronic Resource]. – Way of access: https://competitions.cr.yp.to/aes.html. – Title from the screen.

[2] Analytic hierarchy process [Electronic Resource]. – Way of access: https:// en.wikipedia.org/wiki/ Analytic_hierarchy_ process. – Title from the screen.

[3] ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework [Electronic Resource]. – Way of access: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=46690. – Title from the screen.

[4] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms: ISO/IEC 14888-3 (Edition 2 (2006-11-15)): 2006. – 68 p.

[5] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms: ISO/IEC 14888-3 (Edition 3): 2016. – 130 p.

[6] Kalyna [Electronic Resource]. – Way of access: http://www.slideshare.net/oliynykov/kalyna. – Title from the screen.

[7] 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.

[8] Kupyna [Electronic Resource]. – Way of access: https://ru.wikipedia.org/wiki/Kupyna. – Title from the screen.

[9] Chen L. Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu et al. [Electronic Resource]. – Way of access: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf. – Title from the screen.

[10] 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.

[11] NESSIE: New European Schemes for Signatures, Integrity, and Encryption [Electronic Resource]. – Way of access : https://competitions.cr.yp.to/nessie.html. – Title from the screen.

[12] Post-quantum crypto project [Electronic Resource]. – Way of access: http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html. – Title from the screen.

[13] Procedures for Determining the Weights of Selection Factors in the Weighted-Matrix Delivery Decision [Electronic Resource]. – Way of access: http://www.tcrponline.org/PDFDocuments/tcrp_rpt_131AppF.pdf. – Title from the screen.

[14] Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process [Electronic Resource]. – Way of access: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-draft-aug-2016.pdf. – Title from the screen.

[15] Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges // ETSI White Paper. – 2015. – No. 8 [Electronic Resource]. – Way of access: http://www.etsi.org/images/files/ETSI White Papers / Quantum Safe Whitepaper.pdf. – Title from the screen.

[16] Roszkowska E. Rank ordering criteria weighting methods – a comparative overview / Ewa Roszkowska // Optimum. Studia ekonomiczne. – 2013. – № 5 (65). – P. 14–33 [Electronic Resource]. – Way of access: http:// repozytorium. uwb.edu.pl /jspui/bitstream/ 11320/2189/1/02_Ewa%20ROSZKOWSKA.pdf. – Title from the screen.

[17] Saaty T. L. Decision making with the analytic hierarchy process / Thomas L. Saaty // Int. J. Services Sciences. – 2008. – Vol. 1. – №1. – P. 83 – 98 [Electronic Resource]. – Way of access: http://www.colorado.edu/geography/leyk/geog_5113/ readings/saaty_2008.pdf. – Title from the screen.

[18] Saaty T. L. The Analytic Hierarchy Process / T. L. Saaty. – New York: McGraw Hill, 1980. – 278 p.

[19] The methods of expert estimations [Electronic Resource]. – Way of access: http://books forstudy.com/19650323/ ekonomika/metodi ekspertnih otsinok.htm. – Title from the screen.

[20] 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.

[21] Zhukova O. V. Fishburne's method and the classical method of pharmacoeconomic analysis in the evaluation of antibiotic treatment of acute and recurrent bronchitis in children / Olga V. Zhukova, Tatjana M. Konyshkina, Svetlana V. Kononova // Int. J. Pharm. Science. – 2015. – Vol. 7. – Issue 11. – P. 185–190 [Electronic Resource]. – Way of access: http://innovareacademics.in/journals/index.php/ijpps/article/view/7770/5973. – Title from the screen.
[22] Andreichikov A. V. Analiz, sintez, planirovanie reshenii v ekonomike / A. V. Andreichikov, O. N. Andreichikova. – Moskva: Finansy i statistika, 2002. – 359 s.
[23] Gorbenko I. D. Postkvantova kryptografija ta mehanizmy i'i' realizacii' / I.D. Gorbenko, O.O. Kuznecov, O.V. Potij ta in. // Radiotehnika. – 2016. – Vyp. 186. – S. 32–52.
[24] Gorbenko Ju. I. Metody pobuduvannja ta analizu kryptografichnyh system: monografija. / Ju. I. Gorbenko. – Kharkiv: Fort, 2015. – 959 s.
[25] Orlovskii S. A. Problemy prinyatiya reshenii pri nechetkoi iskhodnoi informatsii / S. A. Orlovskii. – Moskva: Nauka, 1981. – 208 s.

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

Надійшло: Лютий 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
Юрій Горбенко, к.т.н., ХНУ імені В.Н. Каразіна, Харків, Україна. E-mail: gorbenkou@iit.kharkov.ua
Марина Єсіна, аспірантка, ХНУ імені В.Н. Каразіна, Харків, Україна. E-mail: rinayes20@gmail.com
Володимир Пономар, аспірант, ХНУ імені В.Н. Каразіна, Харків, Україна. E-mail: laedaa@gmail.com

Пропозиції з виконання порівняльного аналізу та прийняття в процесі конкурсу рішень щодо переваг певних асиметричних пост квантових криптографічних примітивів.

Анотація. У роботі розглянуто пропозиції із виконання порівняльного аналізу криптографічних примітивів та обґрунтування, розроблення та експериментальне підтвердження можливостей застосування методичних основ вибору та застосування системи безумовних та умовних критеріїв, а також методів та методики порівняльного аналізу та прийняття рішень щодо асиметричних пост квантових криптографічних примітивів типу направлений шифр, а також алгоритмів інкапсуляції ключів та електронних підписів. Наведено певні критерії та показники, що можуть бути використані при порівняльному аналізі властивостей кандидатів у пост квантові криптографічні примітиви. Проведено порівняльний аналіз існуючих перспективних механізмів електронних підписів згідно стандарту ISO/IEC 14888-3:2016 та деяких криптографічних примітивів, що вважаються можливими до застосування у пост квантовий період. Наведено результати оцінювання криптографічних примітивів. Зроблено висновки та надано рекомендації із застосування методів оцінки визначених криптографічних примітивів.

Ключові слова: аналіз алгоритмів ЕП, вагові коефіцієнти, електронний підпис, критерій оцінки ЕП, методи порівняльного аналізу ЕП.

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

Поступила: Февраль 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
Юрий Горбенко, к.т.н., ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: gorbenkou@iit.kharkov.ua
Марина Есина, аспирантка, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: rinayes20@gmail.com
Владимир Пономарь, аспирант, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: Laedaa@gmail.com

Предложения по выполнению сравнительного анализа и принятия в процессе конкурса решений относительно преимуществ определенных асимметрических пост квантовых криптографических примитивов.

Аннотация. В работе рассмотрены предложения по выполнению сравнительного анализа криптографических примитивов и обоснование, разработка и экспериментальное подтверждение возможностей применения методических основ выбора и применения системы безусловных и условных критериев, а также методов и методики сравнительного анализа и принятия решений относительно асимметричных пост квантовых криптографических примитивов типа направленный шифр, а также алгоритмов инкапсуляции ключей и электронных подписей. Приведены определенные критерии и показатели, которые могут быть использованы при сравнительном анализе свойств кандидатов в пост квантовые криптографические примитивы. Проведен сравнительный анализ существующих перспективных механизмов электронных подписей согласно стандарту ISO/IEC 14888-3: 2016 и некоторых криптографических примитивов, которые считаются возможными к применению в пост квантовый период. Приведены результаты оценивания криптографических примитивов. Сделаны выводы и даны рекомендации по применению методов оценки определенных криптографических примитивов.

Ключевые слова: анализ алгоритмов ЭП, весовые коэффициенты, электронная подпись, критерий оценки ЭП, методы сравнительного анализа ЭП.