УДК 004.056.5

A.A. KUZNETSOV, Doctor of Sciences, Yu.I. GORBENKO, Ph.D.,
M.S. LUTSENKO, D.I. PROKOPOVYCH-TKACHENKO, Ph.D., M.V. PASTUKHOV, Ph.D.

NIST PQC: CODE-BASED CRYPTOSYSTEMS

1. Introduction

The National Institute of Standards and Technology (NIST) addressed to the public and announced the launch of a Post-Quantum Cryptography (PQC) bidder competition, which is scheduled for adoption in 2020–2022 [1, 2], In particular, on post-quantum electronic digital signature schemes (EDS), public key encryption schemes and key encapsulation mechanisms. Among the promising areas of research, code-based public-key cryptosystems (Code-Based Public-Key Cryptosystems) occupy a special place, allowing to effectively implement all three groups of algorithms.

The feature of the contest announced by NIST is that algorithms based on mathematical methods that are not sufficiently tested can be submitted. Therefore, study of such algorithms regarding their resistance to quantum cryptographic analysis requires significant time expenses. The aforementioned fact determines relevance of the comprehensive study of the submitted projects, their comparative analysis, as well as the assessment of their security [1, 2]. Within this work, we limit ourselves to research of algorithms of code-based cryptosystems, we will conduct their primary analysis and systematization.

For the primary evaluation of cryptographic properties, an analysis was made of the correspondence of the presented algorithms to modern requirements for public-key cryptosystems, namely, ensuring the properties of indistinguishability [3]. The property of indistinguishability of ciphertext determines the cryptostability of the algorithm to chosen plaintext attack. Providing such an indistinguishability under chosen plaintext attack (IND-CPA) is considered a basic requirement for most provably protected public-key cryptosystems [3], although some schemes also provide cryptographic resistance against chosen ciphertext attacks and adaptive chosen ciphertext attacks. Such indistinguishability properties are designated as IND-CCA1 and IND-CCA2, respectively [3].

2. Characteristics of EDS algorithms

Authors presented 3 different code-based schemes for EDS generation and verification: pqsigRM, RaCoSS, RankSign.

2.1. pqsigRM scheme

The pqsigRM was developed by a group of researchers from Korea [4]. It is based on the Reed-Mueller code (RM), improving the scheme based on Goppa codes, developed by Courtois, Finiasz and Sendrier (CFS). The benefit of this algorithm is controlled time of signing. Compared to CFS, signature time does not depend on the ability to fix *t* errors. Also, signature time and security level is controlled by changing parameters.

2.2. RacoSS scheme

Name of this algorithm stands for a Random Code-based Signature Scheme. RaCoSS is proved to be strong existentially unforgeable under chosen message attack (SEUF-CMA). The signature size is small in respect of other code-based signature schemes apart from CFS signature scheme with 81 bits security. However, the key sizes of CFS signature scheme are much higher than RaCoss. The key generation, signature generation and signature verification processes can easily be speeded up by parallel computation.

2.3. RankSign scheme

RankSign cryptosystem was introduced in 2014 [5]. This signature scheme is based on a code in the rank metric. The general idea is to use the LRPC code (which is equivalent to the MDPC in the Hamming metric or NTRU in the Euclidean metric) as a loophole for calculating the error associated with the message. The signature scheme has small parameters and is relatively fast. Since we need to pick a large value for *q*, all known combinatorial attacks are ineffective to violate the RankSign's security. Thus, the best attacks against it are based on the calculations of Griubner.

3. Comparative analysis of the EDS

A comparative analysis of the presented algorithms of EDS will be useful in terms of their performance and length parameters. Fig. 1 shows the values of the length of signatures for different versions of algorithms with different security levels. In order to demonstrate the values more clearly the length is given in bytes, on a logarithmic scale.

Analyzing the obtained data, it can be noted that for versions of RacoSS algorithm, the length of the public and private keys is the smallest, while the length of the ciphertext for this scheme also takes one of the smallest values. It was not possible to investigate length of a private key of the RankSign scheme because it does not require the use of a private key. The largest length of the ciphertext corresponds to the RankSign and in case the provided security level is increased, length of ciphertext increases as well as the length of the public key.

Fig. 2 shows the parameters of the speed of the key generation, the generation and verification of the signature, as well as indicates computing platform, which was used in the testing. Speed, given in milliseconds, is converted to the number of cycles, taking into account the specifications of a particular computing platform.

In terms of performance it is obvious that the most efficient algorithm will be the one with higher indicators. Analyzing the histograms, it's obvious that the Optimized RacoSS is faster than all the presented algorithms. While the signature scheme pqsigRM for its various versions showed comparable performance, which is an order of magnitude less than the speed of RankSign and RacoSS.

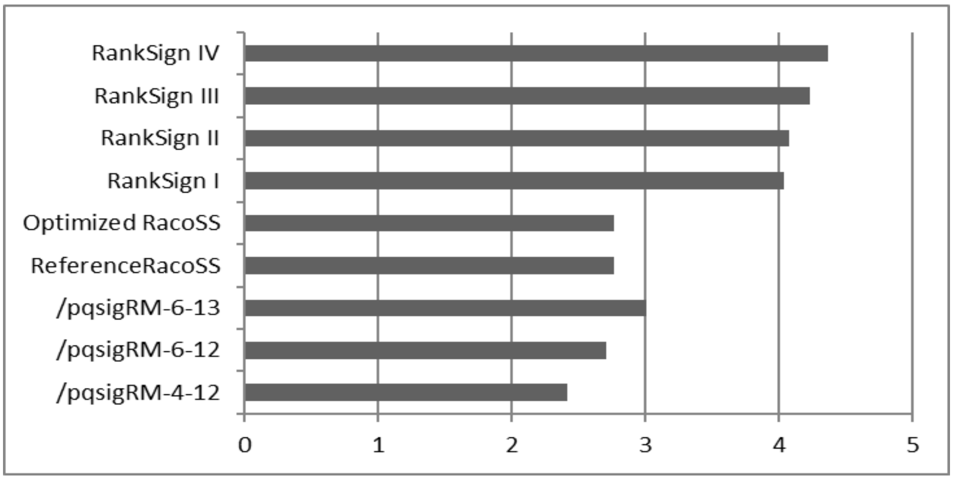

Fig. 1. Comparison of generated signatures (in bytes, logarithmic scale) of different EDS schemes

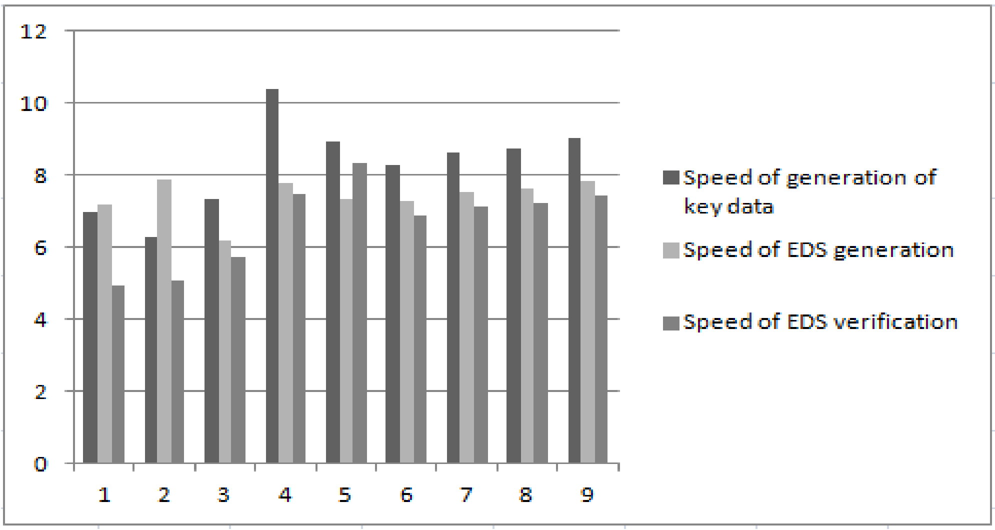

Fig. 2. Speed parameters at all stages of the algorithms

4. Characteristics of public-key cryptosystems

After analyzing the projects submitted to the contest, five code-based public-key cryptosystems were allocated: BIG QUAKE [6], HQC [7], LEDApkc [8], LOCKER [5] та McNie [5].

4.1. BIG QUAKE scheme

Within the framework of the project, an public-key cryptosystems is proposed, which turns into a key encapsulation mechanism. The authors of the project assume the use of Goppa binary codes in this scheme. BIQ QUAKE is built like the Niderraiter scheme. Compared to the original Niederreiter scheme, proposal avoids the computation of a bijection between words of fixed length and constant weight words. This provides a light scheme more suitable for embedded system with restricted computing resources.

4.2.HQC scheme

The HQC name is the abbreviation Hamming Quasi-cyclic, which implies the use of the quasi-cyclic Hamming code HQC is a code-based public key cryptosystem with several desirable properties. It is proved IND-CPA assuming the hardness of (a decisional version of) the Syndrome Decoding on structured codes. By design, HQC perfectly fits the recent KEMDEM transformation, and allows to get a hybrid encryption scheme with strong security guarantees (IND-CCA2).

4.3. LEDApkc scheme

This project was presented by a group of Italian researchers. LEDApkc is a public-key cryptosystem built from the McEliece cryptosystem based on linear error-correcting codes. In particular, LEDApkc exploits the advantages of relying on quasicyclic low-density parity-check (QC-LDPC) codes providing high decoding speeds and compact keypairs. Among the advantages of the LEDApkc scheme are the following. Built on an NP-complete problem under reasonable assumptions. Exploits improved BF decoders which are faster than classical BF decoders.

4.4. LOCKER scheme

The proposal is based on variations of the LRPC approach. The scheme is effective in terms of the size of the parameters and the computational complexity, which uses the properties of the rank metric. The LOCKER has the probability of failure, but this probability is justified and can be very low from 2 $^{-64}$ to 2^{-128}. Also, the positive point is that the choice of parameters is universal.

4.5. McNie scheme.

The authors of the hybrid scheme that unites elements of the McElice and Niderreiter cryptosystems are Korean scientists. McNie provides smaller key sizes employing quasi-cyclicity of matrices for 128-bit, 192-bit and 256-bit securities compared to those of RSA.

McNie can use various kinds of known block codes as inputs even though McEliece cryptosystem based on those codes were broken. The reason is that a random code is used in the encryption so that McNie is secure against structural and information set decoding attacks.

5. Comparative analysis of public-key cryptosystems

Fig. 3 shows the lengths of the ciphertext for different versions of encryption schemes which provide different levels of security. Analyzing the obtained results, it should be noted that the length of the public key and ciphertext for the Big Quake algorithm are the largest. McNie, on the other hand, shows the lowest values of all parameters, while it is able to provide fifth security level as well as other schemes.

The obtained comparison results for speed indicators are shown in Fig. 4. The data given in milliseconds was reduced to the number of cycles that require the execution of the algorithm, taking into account the features of the used computing platform.

The analysis shows that the Big Quake algorithm provides the greatest speed of key generation. The McNie and LEDApkc algorithms are relatively comparable, while the versions of HQC algorithm provide the lowest performance of all the schemes.

Analyzing data, it's obvious that the encryption speed is fairly high in all encryption schemes, but LEDApkc - 5.3 provides the best performance. The decryption rate is comparable to the McNie, Big Quake and HQC algorithms, while LEDApkc performance is the best.

So, in terms of performance, the most effective of the schemes presented is the LEDApkc scheme in all its variants, and HQC, in turn, showed the worst results.

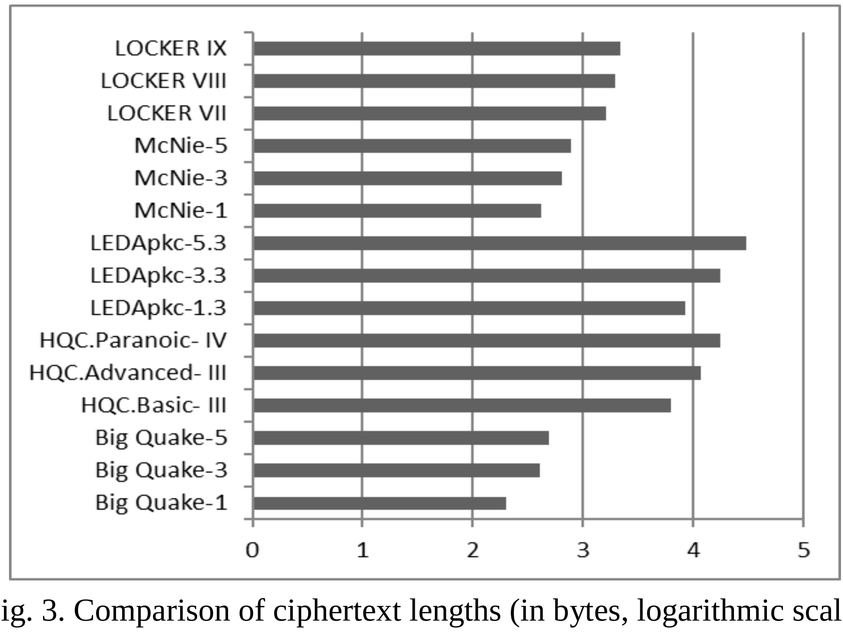

Fig. 3. Comparison of ciphertext lengths (in bytes, logarithmic scale) of different encryption schemes

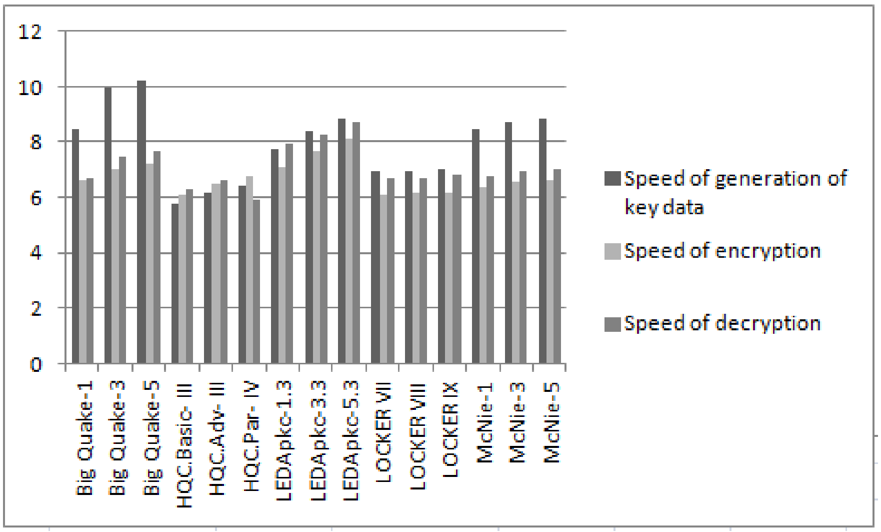

Fig. 4. Histogram of values of the speed of encryption schemes (logarithmic scale)

6. Characteristics of key encapsulation mechanisms

All 12 key encapsulation algorithms presented for the contest are analyzed: BIKE [9], Classic McElice [10], DAGS [11], Edon-K [12], LAKE [13], LedaKem [14], Lepton [15], NTS-KEM [16], Ouroboros-R [17], QC–MDPC KEM [18], RLCE-KEM [19], RQC [20].

6.1. BIKE

In BIKE (BIt Flipping Key Encapsulation is used Quasi-cyclic codes with parity check (QC-MDPC) with moderate density, that can be decoded using the technique of bit flipping. The algorithm has an IND-CPA cryptographic stability, due to the use of the technique of bit flipping is expected and the provision of IND-CCA resistance. The BIKE-1 scheme is based on the variation of the McElice algorithm. In BIKE-1, accelerated key generation is provided. The public key has a double length, compared to BIKE-2. The basis of the BIKE-2 algorithm is the Niederreiter cryptosystem with the parity check matrix.

6.2. Classic McElice

Classic McElice is a scheme proposed by a group of researchers from the USA, Japan, the Netherlands, Germany, France. There is variation of the McElice algorithm, based on the binary Goppa code. This key encapsulation algorithm is designed to ensure the security of IND-CCA2 at a very high level of cryptographic stability. The authors suggest that the algorithm can find an effective application even in systems with limited computing capabilities and resources, while maintaining effective cryptographic stability.

6.3. DAGS

DAGS (Key Encapsulation from DyAdic GS Codes) is an algorithm for key encapsulation submitted by researchers from the universities of the Netherlands, United States, Senegal, France, Brazil. The DAGSa Key Encapsulation Mechanism based on Quasi-Dyadic (QD) Generalized Srivastava codes. The authors claim that this is the first algorithm based on structured algebraic codes that provide not only IND-CPA cryptostability, but also IND-CCA. Presumably the algorithm can find application in applications for the Internet of things.

6.4. Edon-K

Edon-K presented by Norwegian scientists. This algorithm is based on the McElice scheme, but uses a different family of codes. These codes are defined over another field and are not based on the Hamming metric. This approach allows to significantly reduce the length of public keys. In the construction of EDON-K authors use one related class of matrices that they call quasi-binary quasi-orthogonal matrices. EDON-K is designed to offer CCA2 security without a need of some extra CPA-to-CCA transformation.

6.5. LAKE

LAKE (Low rAnk parity check codes Key Exchange) is another algorithm presented by a group of scientists from France. The algorithm is based on the Ideal-LRPC parity codes and the IND-CPA key encapsulation mechanism (KEM). The scheme has some probability of error during decapsulation. The proposed scheme is very effective, both from the point of view of the chosen sizes of basic parameters (keys and ciphertext) and computational complexity.

6.6. LedaKem

LedaKem (Low dEnsity coDe-bAsed key encapsulation mechanism) is based on the Niederreiter cryptosystem with linear error correction. LEDAkem takes advantage of the use of low-density quasi-cyclic codes (QC-LDPC) that provide high decoding rates and small key lengths. It should be noted the extremely short length of the obtained ciphertext – 64 bytes, even at a category 5 of cryptographic stability. The scheme possesses IND-CCA cryptostability.

6.7. Lepton

Lepton (LEarning PariTy with Noise) is Chinese encapsulation algorithm. This algorithm is based on the variation of Learning Parity with Noise (LPN). The Lepton.CPA is aimed at achieving CPA-security, and is based on Ring-CLPN (Compact Learning Parity with Noise). The Lepton.CCA is a KEM scheme for achieving CCA security, which is obtained by applying the Fujisaki-Okamoto transformation over Lepton.CPA.

6.8. NTS-KEM

NTS-KEM scheme submitted by researchers from the United Kingdom. NTS-KEM can be considered as a variant of the McElice public-key cryptography scheme. In this mechanism, binary linear Goppa codes are used in the Niederreiter cryptosystem. NTS-KEM provides the security of IND-CCA (like as KEM) in a Random Oracle model using a transformation similar to the Fujisaki-Okamoto or Dent transformations.

6.9. Ouroboros-R

Ouroboros-R presented by the researchers from France. The quasi-cyclic code used allows the decoding process to be accelerated. The algorithm has some similarities with NTRU-like circuits. Ouroboros-R also has the probability of failure, due to the decoding algorithm used. Ouroboros-R possesses the crypto-resistance of IND-CPA in accordance with the assumptions of 2-QCRSD and 3-QCRSD.

6.10. QC-MDPC KEM

QC-MDPC KEM was developed by researchers from Canada. The algorithm is based on the McElice cryptosystem. QC-MDPC KEM uses a quasi-cyclic parity check with a moderate density. The authors state that the algorithm may not be fast enough compared to other algorithms. The algorithm provides IND-CPA cryptographic stability.

6.11. RLCE-KEM

RLCE-KEM is a scheme for key encapsulating of researcher from the United States. The algorithm uses the McElice cipher scheme based on a random linear code. The advantage of the RLCE scheme is that its security does not depend on any particular structure of underlying linear codes. It is believed that the security in RLCE depends on the NP-hardness of decoding random linear codes.

6.12. RQC

RQC (Rank Quasi-Cyclic) is formed by a group of French scientists. The RQC scheme is based on a quasi-cyclic code. The approach used to key encapsulating the makes it possible to guarantee IND-CCA2 cryptographic stability and provides high performance indicators. The authors indicate that the algorithm has a zero probability of decoding failure.

7. Comparative analysis of key encapsulation mechanisms

According to the data submitted by authors, the smallest length of a private key is in scheme Edon-K, for both variations. The largest private keys of the algorithms DAGS-5 and RLCE-KEM, It should be noted that for all algorithms the length of ciphertext is relatively small and ranges from 32 to 9032.75 bytes. The smallest length – variations of the LedaKem and RLCE-KEM ID = 6 scheme. Some authors intentionally tried to minimize the length of the ciphertext as shown on Fig. 5.

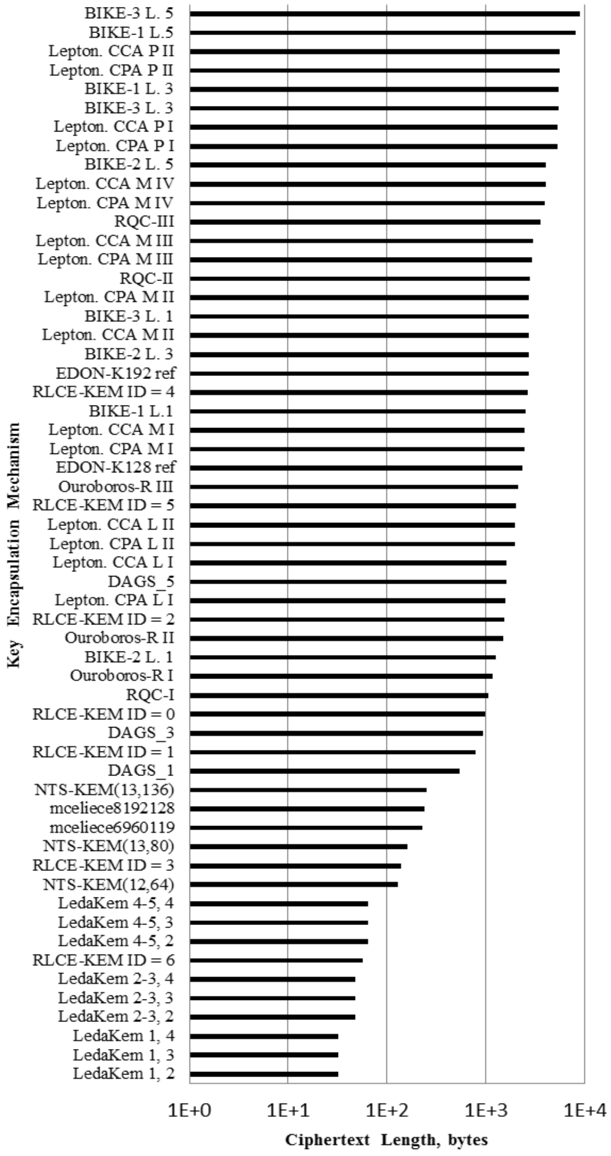

Fig. 5. Ciphertext lengths (in bytes, logarithmic scale) of key encapsulation algorithms

Evaluation of the performance in the format of the number of processor cycles spent on the execution of the main operation is shown in Fig. 6. In Fig. 6 shown the data for various variants of algorithms providing the highest level of cryptographic stability.

Analysis of the results of the comparison shows that the comparable speed of all operations have algorithms Lepton.CCA and Lepton.CPA, Ouroboros-R, LAKE, LedaKem. The EDON-K, Classic McElic, RLCE-KEM, DAGS_5 schemes have a fairly large performance gap between key generation and encapsulation.

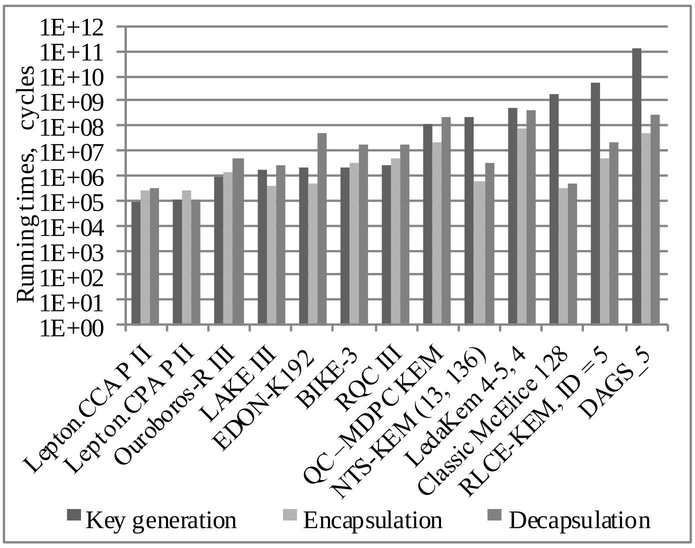

Fig. 6. Performance (in cycles, logarithmic scale) of key encapsulation algorithms

The Lepton algorithm has rather small lengths of both public and private keys, and due to the algorithm used, public and private keys, and due to the algorithm used, the speed of generating key data for this scheme is greatest. The lowest speed of key generation in DAGS_5. The Lepton algorithm also has the fastest rate of key encapsulation, the slowest rate is LedaKem scheme.

Conclusions

The National Institute of Standards and Technology of the United States announced the launch of a contest for the selection of applicants for the standards of post-quantum algorithms, which decisions are scheduled for adoption in 2020–2022. Since NIST intends to standardize post-quantum alternatives to its existing standards for key establishment (SP 800-56A, SP 800-56B). And these standards are used in a wide variety of Internet protocols, such as TLS (Transport Layer Security), SSH (Secure Shell), IKE (Internet Key Exchange), IPsec (IP Security), and DNSSEC (Domain Name System Security Extensions). So, presented schemes will be evaluated by the security they provide in these applications.

Code-based cryptography is now considered one of the most promising areas [21 – 24]. This is confirmed by the fact that out of the 82 projects submitted for the contest, 20 are based on codes. Among them there are 3 electronic digital signature generation and verification schemes, 5 encryption schemes and 12 mechanisms of key encapsulation. Having examined their general characteristics and having conducted a preliminary comparative analysis of their effectiveness, we can conclude that the best indicators, in terms of performance, and the length of signatures, secret and public keys have been demonstrated by the RacoSЫб LEDApkc scheme and Lepton.

References:

1. D. Bernstein, J. Buchmann and E. Dahmen. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009. – 245 p.

2. D. Moody. Post-Quntum Cryptography: NIST's Plan for the Future" The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. Internet: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf [March 8, 2016].

3. J. Katz, Y. Lindell. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall / CRC Press, 2007. 553 p.

4. Lee, Young-Sik Kim, Yong-Woo Lee, Jong-Seon No. A modified RM code-based post-quantum digital signature algorithm [On-line]. Internet: https://sites.google.com/view/pqsigrm/home

5. Post-Quantum Cryptography, Round 1 Submissions, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

6. Alain Couvreur, Magali Bardet, Elise Barelli, Olivier Blazy, Rodolfo Canto-Torres, Philippe Gaborit, Ayoub Otmani, Nicolas Sendrier, Jean-Pierre Tillich. Binary Goppa QUAsi-cyclic Key Encsapulation [On-line] Internet: https://bigquake.inria.fr/

7. Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor. Hamming Quasi-Cyclic [On-line]. Interner: http://pqc-hqc.org/

8. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, Paolo Santini. LEDApkc Public Key Cryptosystem [On-line]. Internet: https://www.ledacrypt.org/LEDApkc/

9. Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zemor. BIKE – Bit Flipping Key Encapsulation. NIST Submission, 2017. [On-line]. Internet: http://bikesuite.org/#spec.

10. Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer. Classic McEliece. NIST Submission, 2017. [On-line]. Internet: https://classic.mceliece.org/index.html.

11. Gustavo Banegas, Paolo S.L M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiecoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen. DAGS: Key Encapsulation using Dyadic GS Codes. NIST Submission, 2017. [On-line]. Internet: https://www.dags-project.org/#files.

12. Danilo Gligoroski, Kristian Gjøsteen. Post-quantum Key Encapsulation Mechanism EDON-K. NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

13. Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zémor. LAKE – Low rAnk parity check codes Key Exchange. NIST Submission, 2017. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

14. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, Paolo Santini. LEDAkem (Low dEnsity coDe-bAsed key encapsulation mechanism). NIST Submission, 2017. [On-line]. Internet: https://www.ledacrypt.org/LEDAkem/

15. Y. Yu, J. Zhang. Lepton: Key Encapsulation Mechanisms from a variant of Learning Parity with Noise. NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

16. M. Albrecht, C. Cid, K. G. Paterson, C. J. Tjhai, M. Tomlinson. NTS-KEM. NIST Submission, 2017. [On-line]. Internet: https://nts-kem.io/.

17. C. A. Melchor, J.-C. Deneuville, N. Aragon, P. Gaborit, S. Bettaieb, A. Hauteville, L. Bidoux, G. Zémor. Ouroboros-R. NIST Submission, 2017. [On-line]. Internet: http://pqc-ouroborosr.org/.

18. A. Yamada, E. Eaton, K. Kalach, P. Lafrance, A. Parent. QC-MDPC KEM: A Key Encapsulation Mechanism Based on the QC-MDPC McEliece Encryption Scheme, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

19. Y. Wang. RLCEKeyEncapsulation Mechanism (RLCE-KEM) Specifcation. NIST Submission, 2017. [On-line]. Internet: http://quantumca.org/.

20. C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, G. Zemor. Rank Quasi-Cyclic (RQC). NIST Submission, 2017. [On-line]. Internet: http://pqc-rqc.org/.

21. Yu.V.Stasev, A.A.Kuznetsov. Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes // Cybernetics and Systems Analysis. – Vol. 41, Issue 3. – P. 354-363, May 2005.

22. A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov. Code-based public-key cryptosystems for the post-quantum period // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017. – P. 125-130.

23. A. Kuznetsov, R. Serhiienko and D. Prokopovych-Tkachenko.Construction of cascade codes in the frequency domain // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017. – P. 131-136.

24. Yu.V. Stasev, A.A. Kuznetsov. Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes // *Kibernetika i Sistemnyi Analiz*/. – No. 3. – P. 47-57, May-June 2005.

V.N. Karazin Kharkiv National University;
JSC "Institute of Information Technologies", Kharkiv;
University of Customs and Finance, Dnipro

Received 02.11.2018