Post-Quantum Network Security: McEliece and Niederreiter Cryptosystems Analysis and Education Issues

ALEKSEI VAMBOL[1], VYACHESLAV KHARCHENKO[1], OLEXANDR POTII[1], NIKOS BARDIS[2]
[1] Department of Computer Systems and Networks
National Aerospace University «KhAI»,
Kharkiv, Ukraine
[2] Department of Mathematics and Engineering Sciences
Hellenic Army Academy
Athens, 19400, Greece

o.vambol@csn.khai.edu; v.kharchenko@csn.khai.edu; a.potiiv@csn.khai.edu; bardis@ieee.org

***Abstract*—**The paper is aimed at analyzing of the classical McEliece and Niederreiter cryptosystems as well as the Quasi-Cyclic MDPC McEliece cipher in a context of the post-quantum network security. Theoretical foundations of the aforesaid cryptographic schemes are considered. The characteristics of the given cryptosystems and other asymmetric encryption schemes are analyzed. The cipher metrics, which are considered in the paper, include cryptographic strength, performance, public key size and length of ciphertext. The binary Goppa codes are described in the context of their role for the cryptanalytic resistance of the classic McEliece and Niederreiter schemes. The crucial advantages and drawbacks of the aforementioned cryptosystems are analyzed. The prospects for application of these ciphers to the network security protocols are outlined. The investigations, which are aimed at finding ways to reduce the public key sizes and improve the energy efficiency of the given ciphers, are briefly described. A new educational module "Introduction to Post-Quantum Cryptography" is presented.

Keywords—McEliece cryptosystem, Niederreiter cryptosystem, Quasi-Cyclic MDPC McEliece cryptosystem, . post-quantum cryptography

Received: May 5, 2020. Revised: October 12, 2020. Accepted: October 30, 2020. Published: November 15, 2020.

1. Introduction

Public key cryptographic algorithms are one of the fundamental tools for providing secure data storage and communication for users and systems. Their principal advantage arises from their ability to provide a solution to the problem of sharing symmetric keys between distant users communicating over insecure channels.

The current technological advances in the field of quantum computers make quantum cryptanalysis feasible. This fact in turn, renders most contemporary Public Key Cryptosystems such as the RSA and El-Gamal algorithms susceptible to quantum cryptanalysis attacks.

Post-quantum cryptography therefore, requires the development for a variety of innovative cryptographic algorithms that are resilient to attacks using quantum computers [1, 2].

Code based cryptography is a class of Public Key Cryptosystems that are viewed by many researchers as suitable for achieving good results in the post – quantum era. Representative schemes of this class are the McEliece and Niederreiter cryptographic algorithms that are developed based on the binary Goppa codes. The further development of the McEliece and Niederreiter algorithms is therefore highly relevant in the context of the advancement of post – quantum cryptography [1, 2].

The aim of this paper is to present an analysis of the McEliece and Niederreiter schemes focusing on the underlying theory, foundations and a comparative study between these two and other asymmetric cryptographic algorithms. The comparison is based on suitable metrics of cipher quality such as cryptographic strength, computational complexity, public key size and ciphertext length.

The given work analyzes both the classical versions of the aforementioned code-based cryptosystems and the Quasi-Cyclic MDPC McEliece cipher developed in order to reduce public key sizes. The analysis focuses especially on the operation of the binary Goppa codes and their contribution

towards the cryptanalytic resilience of the classical McEliece and Niederreiter schemes [2]. Besides, an educational module "Introduction to Post-Quantum Cryptography", which has been developed by authors of paper, is briefly discussed.

The paper is organized as folows. The features of the classical McEliece and Niederreiter schemes are analyzed in Sections II and III. In Section IV an analysis of the binary Goppa codes. The comparison between the features of these two cryptographic algorithms is given in Section V. An analysis of the the Quasi-Cyclic MDPC McEliece cipher is presented in Section VI. The aforementioned educational module is presented in Section VII. Section VIII includes a summary of the advantages and weaknesses of the investigated cryptographic algorithms, as well as principles for the utilization of these cryptosystems in network security protocols. Additionally, a description is given of current research efforts aiming at finding ways to reduce the public key sizes and improve the energy efficiency of these cryptographic schemes.

2 Features of Cryptosystems

2.1 The McEliece cipher

The first probabilistic cipher was developed by Robert McEliece in 1978 [3]. The algorithm is based on binary linear codes and linear algebra over GF(2).

The key pair generation includes the following actions [3]:

1) A binary linear *(n, k)*-code C with $k \times n$ generator matrix G is chosen at random. The code should be suitable for correcting at least t errors and the corresponding decoder should be efficient.

2) An $n \times n$ random permutation matrix P and a nonsingular $k \times k$ matrix S are also randomly generated.

3) The matrix $E = S \bullet G \bullet P$ of size $k \times n$ is also generated.

4) The tuples *(E, t)* and *(S, G, P),* corresponding to the public and private respectively are hence created.

Consequently, the encryption algorithm is completed as follows [4]:

1) The message is represented as a k-dimensional vector m.

2) The vector $v = m \bullet E$ is calculated.

3) A random vector z of weight t and dimension n is chosen at random.

4) The ciphertext c is calculated as $c=v+z$.

The corresponding decryption algorithm consists of the following steps [4]:

1) The vector $u = c \bullet P^{-1}$ of lentgh n is first computed.

2) The vector d which is the result of decoding the vector u with the code C is hence obtained.

3) The vector $m' = d \bullet S^{-1}$ of the decrypted message is formulated.

The proof of the correctness of this cipher is given below:

1) The value of the vector u is calculated as $u = c \bullet P^{-1} = (m \bullet E + z) \bullet P^{-1} = m \bullet S \bullet G + z \bullet P^{-1}$. Given that G is a generator matrix of the linear code C, the vector $m \bullet S \bullet G$ is a valid word of the code C. Because of the fact that P is a permutation matrix, it follows that $z \bullet P^{-1}$ is of weight t. It may therefore be deduced that the vector u, that is the result of the encoding of the message $m \bullet S$, is a is essence a distortion of t symbols in a word of code C,

2) Accordingly, d, the decoded version of the vector u with the code C, is equal to $m \bullet S$ because of the fact that code C is capable of correcting at least t errors.

3) The decryption process $d \bullet S^{-1} = m \bullet S \bullet S^{-1} = m$ hence recovers the decrypted message vector m′.

2.2 The Niederreiter cipher

Contrary to the McEliece algorithm, the cryptographic algorithm proposed by Harald Niederreiter is deterministic, with the corresponding encryption process being faster. The algorithm is suitable for digital signature applications [5], but the computational effort required for signature generation is larger compared to other quantum safe algorithms [1]. Similarly to the McEliece cipher, this cipher also employs linear algebra over *GF(2)* and binary linear codes.

The key pairs are obtained using the following algorithm [4]:

1) A binary linear *(n, k)*-code C is randomly chosen, together with a parity check matrix H of size $(n - k) \times n$. The code should be such that it has an efficient decoding algorithm and should be capable of correcting at least t errors.

2) A random nonsingular $(n – k) \times (n – k)$ matrix S and a random $n \times n$ permutation matrix P are also generated.

3) The $(n – k) \times n$ matrix $E = S \bullet H \bullet P$ is hence calculated.

4) The public and respective private keys are hence obtained as (E, t) and (S, H, P).

For encryption of a message, the algorithm has as follows [4]:

1) The initial message is represented as an n-dimensional vector m with a maximum weight of t.

2) The ciphertext is obtained using the equation

$c = E \bullet m^T$.

The corresponding decryption algorithm has as follows [3]:

1) The $(n – k)$-dimensional vector u is calculated:

$u = S^{-1} \bullet c$.

2) The variable d is obtained as the transpose of the error vector corresponding to the syndrome u by applying the error correction of the code C.

3) The message vector is recovered by equation

$m' = (P^{-1} \bullet d)^T$.

The proof of correctness of the cipher is hence derived:

1. Vector u is equal to:

$S^{-1} \bullet c = S^{-1} \bullet E \bullet m^T = H \bullet P \bullet m^T$.

Given that P is a permutation matrix, the column vector $P \bullet m^T$ has a weight less than or equal to t. It is shown that u is the syndrome of the error vector $(P \bullet m^T)^T$ with maximum weight t, given that H is a parity check matrix of the linear code C

2) Since the code C is capable of correcting at least t errors, then vector d, the transposed error vector corresponding to the syndrome u in the error correction procedure of the code C, is equal to $P \bullet m^T$.

3) The recovered message m' is derived using equation:

$(P^{-1} \bullet d)^T = (P^{-1} \bullet P \bullet m^T)^T = m$.

2.3 Binary Goppa codes

Valery Goppa proposed a class of linear block error correction codes in 1969. Each code is specified by a separable polynomial $g(x)$ of degree t over $GF(2^m)$ and a sequence L of n distinct elements of this field, which are not the roots of $g(x)$. Properties of the codes include [5]:

- Length of codeword $n \leq 2^m$.
- Distance of code $d \geq 2t + 1$.
- $k \geq n – mt$ information symbols.

Vector representation over $GF(2)$ is used for the codewords:

$$c = (c_1, \ldots, c_n)$$

satisfying the condition [6]:

$$\sum_{i=1}^{n} \frac{c_i}{x - L_i} \equiv 0 \bmod g(x)$$

Binary Goppa codes possess a series of properties rendering them particularly relevant in the context of error correcting coding:

- The decoding algorithms corresponding to these codes are efficient with complexity $O(n^2)$ [7].
- Members of this class of codes possess properties considered highly advantageous compared to other linear codes [8].
- The class of codes is a generalized version of the BCH codes [4].

Binary Goppa codes provide an important element in strengthening the cryptographic resilience of the McEliece and Niederreiter ciphers.

Cryptanalysis of the above ciphers involves decoding an arbitrary public linear code obtained by a random transformation of a rapidly decodable private one, a problem which is shown to be an NP-complete problem [4].

There do not exist efficient algorithms allowing a distinction between binary Goppa codes and binary random codes [9]. The number of non – equivalent binary Goppa codes increases exponentially as their length and dimension becomes larger [10].

Consequently, it can be deduced that the recovery of a hidden code and a reduction of the subsequent stage in the cryptanalysis of the McEliece and Niederreiter ciphers for effective decoding of the restored code cannot be achieved in polynomial time [4].

2.4 Comparison between the McEliece and Niederreiter cryptographic algorithms

The ciphers under study possess the following properties:

- Quantum resistance, a feature that does not exist in widely used asymmetric algorithms, such as RSA and ElGamal schemes [1, 2].
- Smaller encryption and decryption computational complexity compared with RSA. The quantum safe schemes under study

have a computational complexity of $O(n^2)$, while RSA has correspondingly $O(n^3)$ [3].

- The computational complexity of the key generation for the quantum safe, code-based ciphers under study is $O(n^3)$ [11]. The corresponding complexity for the generation of the RSA key pair is of $O(n^4)$ [12].
- Increases in the size of the cryptographic scheme result in significantly smaller increases in the computational complexity in comparison with RSA. The complexity for n-bit encryption and decryption schemes are of orders $O(n^2)$ for the considered quantum safe ciphers and $O(n^6)$ for RSA [1].
- The key size required to achieve n-bit cryptographic strength is $O(n^2 \log^2 n)$ for the quantum-resistant ciphers and $O(n^3 / \log^2 n)$ for RSA [13].

The McEliece and Niederreiter cryptographic algorithms have the following disadvantages:

- The public keys of the McEliece and Niederreiter ciphers must be of sizes of 429.5 KB and 69.2 KB respectively, so as to be equally secure to the RSA-2048 with 0.5 KB public keys [14].
- The RSA present no ciphertext expansion. The ciphertext produced is on average expanded by 1.6 times longer compared to the plain text for the McEliece scheme [3]. For the case of the Niederreiter cipher, this figure is different than in case of the McEliece cryptosystem, depending on the parameters of the underlying code, but still greater than one [14].

3 The Quasi-Cyclic MDPC McEliece cryptosystem

The problem of large public keys is the most significant one for code-based cryptographic schemes. Several proposals have been made to overcome this drawback, among which the most notable one is the McEliece cryptosystem based on the quasi-cyclic moderate-density parity-check codes [15]. This encryption scheme was proposed in [16].

According to the most widespread definition, the code is quasi-cyclic if there is such integer s that a cyclic shift of any codeword by s positions produces another word of this code. A generator matrix of this code can be represented as array of circulants, which has been multiplied from the right by a suitable column permutation matrix [17].

However, another definition of quasi-cyclic codes was given, where they were described as codes, whose words consist of s successive blocks of the same length in a way that application of simultaneous circular shift to each of this blocks results in another codeword. The codes, which are used in the aforementioned cryptosystem, are quasi-cyclic according to this definition [18]. In the rest of this paper the term "quasi-cyclic codes" is used in this sense.

There are several advantages of quasi-cyclic codes which determine their usage in the given cryptographic scheme. Both generator and parity-check matrices of these codes can be represented as arrays of circulants, and a circulant can be completely described by its first row. The given properties make possible a storage of the aforementioned matrices in a compact representation. There is an isomorphism between the ring of polynomials modulo $x^n - 1$ and the ring of n × n circulants over $GF(2)$, in which every element of the first algebraic structure corresponds to the circulant, whose first row is represented by a sequence of coefficients of the preimage polynomial. These circumstances make possible efficient computations, where polynomials are used in operations instead of matrices [16].

Low-density parity-check (LDPC) codes are the class of linear block codes, whose rows have constant small Hamming weight, which is usually less than 10. These codes have been proposed by Robert Gallager in [19]. Moderate-density parity-check (MDPC) codes differ from LDPC ones only in a larger weight of rows, which is $O(n^{0.5} \log^{0.5} n)$, where n is length of a codeword [16].

The procedure of construction of a binary quasi-cyclic $(n, n - r)$-MDPC code, where rows of a parity-check matrix H have weight w and $n = rc$, consists of the following steps [16]:

1) Random generation of n-dimensional binary vector h of weight w. This vector defines H and can be represented as the sequence of r-dimensional binary vectors $d_0, d_1, ..., d_{c-1}$ of weights $w_0, w_1, ..., w_{c-1}$.

2) Forming of H as $[H_0|H_1|... |H_{c-1}]$, where H_i is r × r circulant, whose first row is equal to d_i. Each circulant H_i has row weight w_i and j-th row of H is a sequence of j-th rows of circulants $H_0, H_1, ..., H_{c-1}$, thus all rows of H are of weight w.

3) Assuming H_{c-1} is non-singular, a generator matrix G in row reduced echelon form is obtained as $[I|Q]$, where I is $(n - r) \times (n - r)$ identity matrix and Q is a column of $r \times r$ matrices $Q_0, Q_1,..., Q_{c-2}$, where $Q_i=((H_{c-1})^{-1} \bullet H_i)^T$.

The results of inversion, product and transposition of circulants are also circulants [19]. Thus, Q is a column vector of circulants, and G can be compactly stored in memory, being represented by array of c - 2 binary vectors, which are used for description of corresponding circulants in Q.

Encoding of $(n - r)$-dimensional binary vector can be implemented as its multiplication from the right by G, and the result of this operation is n-dimensional binary vector, whose first $n - r$ elements constitute an input sequence. These properties are determined by G, which is a generator matrix of a systematic linear block code [16].

Decoding of MDPC codes can be performed with a variant of Gallager's bit flipping algorithm, which is proposed in [16]. Initial version of Gallager's algorithm, which was intended for decoding of LDPC codes, can be described in the following way [19]:

1. Computation of a syndrome column vector $y = H \bullet m^T$, were H is a parity-check matrix of the given $(n, n - r)$-LDPC code and m is a binary vector of received message.

2. If each element of y is equal to 0, algorithm has succeeded and the plaintext vector, which consists of the first $n - r$ elements of m, is returned as a result.

3. If maximum permissible number of iteration is reached, algorithm has failed to decode m and error notification is returned.

4. Forming of an integer vector e, whose every element e_i is equal to amount of such integers $j \in [0, r - 1]$ that j-th row of y and i-th element of j-th row of H and are nonzero.

5. Inversion of elements of m, for which the element of e with the same index is greater than some constant b, and return to the first step.

The number of nonzero elements in rows of parity-check matrix for LDPC codes is small. Therefore, in a case of moderate number of errors in a received message most of syndrome elements will be either 1 due to impact of only one erroneous digit or 0 owing to absence of corrupted digits influence. Thus, if for most rows of parity-check matrix with nonzero i-th element the same row of syndrome is 1, it is likely, that i-th digit of received message is corrupted [19].

Specificity of the aforementioned MDPC-oriented variant of this algorithm lies in the approach for choice of b, where this parameter is recomputed at each iteration between forming of e and bits inverting in m. A new value of b is defined as the largest element of e decreased by a small integer δ. In case of decoding unsuccess, a value of δ is decremented by 1. If updated δ is non-negative, another attempt is made, otherwise, failure notification is returned. The purpose of the given approach for definition of a parameter b is to achieve maximum error-correcting ability for Gallager's bit flipping algorithm, while trying to retain a performance as good as possible [16].

Estimation of the error-correction capability of this MDPC-oriented Gallager's algorithm can be performed using Gallager's analysis proposed in [19], which has been developed to calculate a threshold for the amount of errors, that LDPC codes are able to correct. Although the given analysis is less precise for MDPC codes, it makes possible to compute an upper bound for their error-correction capability. Decoding failure rate of MDPC codes can be estimated by means of simulation [16].

Quasi-Cyclic MDPC McEliece cryptosystem can be described as follows. The key pair generation is the aforementioned construction procedure of quasi-cyclic $(n, n - r)$-MDPC code. The public key is represented by a pair of systematic generator matrix G and error-correction capability t. The private key is parity-check matrix H. Thus, both of these keys can by compactly stored in memory. Encryption of binary message vector m lies in its encoding with error injection in the obtained codeword. The ciphertext is obtained by the formula $u = m \bullet G + z$, where z is a random error vector of weight up to t. Decryption of u is its decoding by the aforesaid MDPC-oriented bit flipping algorithm [16].

The given cryptosystem has to be used in conjunction with CCA-2 security-conversion, for example, with the one proposed in [21]. In this case, systematicity of generator matrix does not introduce any security-flaw [16].

Encryption into a ciphertext, which cannot be decrypted in a way mentioned above, is not impossible due to nonzero probability of a decoding failure of the aforementioned MDPC-oriented bit flipping algorithm. The given case has to be treated, and several solutions has been proposed for this. Straightforward approach lies in generation of a

random error vector of such weight that is sufficiently small to provide a negligible decoding failure rate, which is less than machine failure rate. On-the-fly solution consists in attempt to decode a ciphertext by means of another algorithms with better error-correction capability, but significantly lower performance. Resend approach implies a request for a new encryption [16].

Permutation and scrambling matrices, which play an important role in the classical McEliece cipher, are not used in Quasi-Cyclic MDPC McEliece cryptosystem, because its public key does not contain any information helpful for decoding of the underlying code [16].

The characteristics of the public keys for the given cryptosystem are given in Table 1, which was compiled using data from [16]. Public keys for this cipher are from 96 to 234 times smaller than for the classical McEliece scheme with the same security level [16].

Table 1. Public key sizes in bits for the Quasi-Cyclic MDPC McEliece cryptosystem.

		Security level		
		80 bits	128 bits	256 bits
Ciphertext expansion	2 times	4801	9857	32771
	1.5 times	7186	14866	45062
	1⅓ times	9237	20409	61449

Despite the advantages of the aforementioned cipher, recent researches have led to discovery of an efficient attack on the given cryptosystem. This cryptanalytic approach allows to recover a private key by means of sending a large amount of random ciphertexts and analyzing the probability of decoding failure for different types of error vectors. The given reaction attack has been proposed in [22]. Nevertheless, it is not considered to be devastating enough to make the Quasi-Cyclic MDPC McEliece cryptosystem useless, and this cipher has a prospect of being used securely after slight improvements [23].

4 Case study in education: Introduction to post-quantum cryptography”

Within the framework of TEMPUS SEREIN project an educational module for MSc and PhD students, which is called “Introduction to Post Quantum Cryptography”, has been developed by authors of the paper. Its structure, which is given in Table 2, includes both lecture and practical classes with 30 hours total workload. In particular, it contains the sections dedicated to the McEliece and Niederreiter cryptosystems.

Table 2. Structure of the module “Introduction to Post-Quantum Cryptography”.

Themes	Contact work				Individual work
	Lectures	Seminars	Practicums	Total	
1. Introduction to post-quantum cryptography. 1.1. Quantum computers and their impact on cryptography. 1.2. Post-quantum cryptography concept. 1.3. Comparison of post-quantum and classical cryptosystems.	2	4		6	2
2. Code-base cryptography. 1.1. The McEliece cryptosystem. 1.2. The Niederreiter cryptosystem.	2		4	6	4
3. Multivariate cryptography.	2		4	6	3
4. Application of post-quantum cryptography in network security protocols.	2			2	1
Total	8	4	8	20	10

The given module requires the following prerequisites:

- Applied Cryptology.
- Linear algebra.
- Theory of Finite Fields.
- Basics of Computer Networks.
- Basics of Number Theory.

5 Conclusion

The McEliece and Niederreiter schemes based on the binary Goppa codes are among the most promising candidates for inclusion into the post-quantum standards of asymmetric cryptosystems.

Their main advantages besides the quantum resistance are high performance and cryptographic strength. The biggest drawback of these ciphers is large key sizes which are the reason of the less prevalence of the given cryptosystems in comparison with RSA and ElGamal schemes.

The aforementioned code-based ciphers can be employed in the asymmetric encryption components of the majority of network security protocols as quantum safe alternative to the currently used cryptosystems. These protocols, in particular, include TLS, S/MIME and SSH [1].

The scientific community is looking for ways to eliminate the drawbacks of the given ciphers. A variant of the McEliece scheme with the public keys, which are from 96 to 234 times smaller than ones for the classical version of this cryptosystem, has been presented in [16]. In the given approach the McEliece cipher is constructed on the basis of quasi-cyclic moderate density parity-check codes. Although this variant of the McEliece cryptosystem is vulnerable to recently discovered new reaction attack on it, there is a prospect of secure use of this cipher after slight improvements.

Elliptic shortened codes are used in McEliece cryptosystem [24] for increasing encryption and decryption procedures by reducing of the key length.

ACKNOWLEDGMENT

The authors thank for advising Associate Professor I. N. Shulga. Besides, we thanks to TEMPUS-SEREIN project (http://serein.eu.org/) team and colleagues from the Computer Systems and Networks Department of National Aerospace University KhAI and other participants of CriCTechS seminar for discussion of the presented results.

References

[1] ETSI White Paper No. 8. “Quantum Safe Cryptography and Security”, European Telecommunications Standards Institute”, 2015, 49 p.

[2] Vambol, Aleksei, et al. "McEliece and Niederreiter Cryptosystems Analysis in the Context of Post-Quantum Network Security." 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI). IEEE, 2017.

[3] S. Y. Yan, “Quantum Attacks on Public-Key Cryptosystems”, Springer, 2013, 214 p.

[4] E. Jochemsz, “Goppa Codes & the McEliece Cryptosystem”, Vrije Universiteit Amsterdam, 2002, 63 p.

[5] R. Lu, X. Lin, X. Liang, X. Shen, “An efficient and provably secure public key encryption scheme based on coding theory”, Security and Communication Networks, 2011, vol. 4, iss. 12, pp. 1440-1447.

[6] V. D. Goppa, “A New Class of Linear Correcting Codes”. Problems of Information Transmission, 1970, vol. 6, iss. 3, pp. 207-212.

[7] C. Löndahl, T. Johansson, “A New Version of McEliece PKC Based on Convolutional Codes”, Lecture Notes in Computer Science, 2012, vol. 7618, pp. 461-470.

[8] M. Loeloeian, J. Conan, “A [55,16,19] binary Goppa code”, IEEE Transactions on Information Theory, 1984, vol. 30, iss. 5, p. 773.

[9] T. P. Berger, P.-L. Cayrel, P. Gaborit, A. Otmani, “Reducing Key Length of the McEliece Cryptosystem”, Lecture Notes in Computer Science, 2009, vol. 5580, pp. 77-97.

[10] P. Fitzpatrick, J. A. Ryan, “Enumeration of inequivalent irreducible Goppa codes”, Discrete Applied Mathematics, 2006, vol. 154, iss. 2, pp. 399-412.

[11] M. Kratochvíl, “Implementation of cryptosystem based on error-correcting code”, Charles University in Prague, 2013, 60 p.

[12] P. Fahn, “Answers to Frequently Asked Questions about Today's Cryptography”, RSA Laboratories, 1996, 204 p.

[13] D. J. Bernstein, J. Buchmann, E. Dahmen, “Post-Quantum Cryptography”, Springer, 2009, 246 p.

[14] I. Woungang, S. Misra, S. C. Misra, “Selected Topics in Information and Coding Theory”, World Scientific, 2010, 724 p.

[15] “ETSI GR QSC 001: Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework”, European Telecommunications Standards Institute, 2016, 42 p.

[16] R. Misoczki, J.-P. Tillich, N. Sendrier, P. S. L. M. Barreto, “MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes”, IEEE International Symposium on

Information Theory (ISIT-2013), 2013, pp. 2069-2073.

[17] R. Daskalov, P. Hristov, "New one-generator quasi-cyclic codes over GF(7)", Problems of Information Transmission, 2002, vol. 38, iss. 1, pp. 50-54.

[18] C. Aguilar, O. Blazy, J.-C. Deneuville, P. Gaborit, G. Zemor, "Efficient Encryption from Random Quasi-Cyclic Codes", CoRR abs/1612.05572, 2016, 28 p.

[19] R. G. Gallager, "Low-Density Parity-Check Codes", M.I.T. Press, 1963, 90 p.

[20] H. Crapo, D. Senato, "Algebraic Combinatorics and Computer Science: A Tribute to Gian-Carlo Rota", Springer Science & Business Media, 2001, 546 p.

[21] K. Kobara, H. Imai, "Semantically secure McEliece public-key cryptosystems - conversions for McEliece PKC", PKC 2001: Public Key Cryptography, 2001, vol. 1992, pp. 19-35.

[22] Q. Guo, T. Johansson, P. Stankovski, "A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors", Lecture Notes in Computer Science, 2016, vol. 10031, pp. 789-815.

[23] M. Kindberg, "A usability study of post-quantum algorithms", Lunds universitet, 2017, 68 p.

[24] S. Yevseiev, K. Rzayev, O. Korol, Z. Imanova, "Development of McEliece modified asymmetric crypto-code system on elliptic truncated codes", Eastern-European Journal of Enterprise Technologies, 2016, vol. 4, iss. 9 (82), pp. 18-26.