УДК 004.056

THE STATE OF STANDARDIZATION OF POST-QUANTUM CRYPTO-ALGORITHMS AT THE GLOBAL LEVEL

Oleksandra Tsentseria[1], Kateryna Hleha, Aleksandra Matiyko[2], Igor Samoilov[3]

[1]Institute of Special Communication and Information Protection, [2,3]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (Kyiv, Ukraine)
ORCID: [3] https://orcid.org/0000-0002-6963-1877, [2] https://orcid.org/0000-0002-6963-1877
E-mail: [3]samoilov1966igor@gmail.com, [2]alexm1710@ukr.net, [1]zenzera1809@gmail.com, akafelix54@gmail.com

DOI: 10.15673/atbp.v15i2.2527

Abstract. *In the digital age, cryptography is widely used in various important systems such as financial, military and government ones, medical records etc.*

The life of modern people is closely connected with the cryptography. We send messages via instant messengers without even considering in which way the security of communications and data is ensured. We buy things both online and transfer money with confidence in transaction security. The level of digitization of our society is constantly increasing, and the digital data needs a reliable protection, which makes cryptography a current topic.

Cryptographic systems ensure our security and the basic properties of information, such as privacy, integrity, availability.

However, with the beginning of the development of quantum computers, the field of cryptography has developed in a new direction. Quantum cryptography is a science that studies the methods of communication systems protection. It is based on the idea that patterns of quantum physics (physical properties described by the laws of quantum optics, quantum electrodynamics, or quantum field theory) are inviolable. The current state of development and usage of powerful quantum computers, as well as their mathematical and software, is strictly confidential and securely protected. Only clear-cut information about quantum computers and their usage in cryptography is provided.

NIST has announced an open competition to select quantum-resistant public-key cryptographic algorithms. After the third round, CRYSTALS-KYBER, CRYSTALS Dilithium, FALCON, and SPHINCS+ were proposed to be standardized. NIST has already recommended moving from the sizes of keys and algorithms that provide 80 security bits to the sizes of keys and algorithms that provide 112 or 128 security bits in order to protect against classic attacks.

Post-quantum cryptography, which with its complexities still requires a more detailed study, challenge science once more. However, it is unknown when the changes will occur and when the quantum era will begin, as well as what consequences they will have. It is only possible to predict how many advantages will have quantum calculations compared to usual, and how different the new quantum models will be from classic ones.

Keywords: cryptography, post-quantum cryptography, data security, standart, quantum computers, post-quantum algorithms.

I. Introduction

Currently, the one, who owns the information, owns the world. Therefore, its protection is an important component of the security of a person, organization, or state. The science that studies and analyzes mathematical methods which ensure safety, confidentiality, integrity, and availability of data is called cryptography. Its main tools are symmetric-key encryption, public key algorithms and hash functions.

Most of the communication protocols, which play a significant role in providing communications, usually rely on three main cryptographic functionalities, namely: public key encryption, digital signatures and key exchange. Presently, key exchange is mainly implemented using the Diffie-Hellman key exchange protocol, and both RSA (Rivest–Shamir–Adleman) and elliptic-curve cryptosystems are used for public key encryption and creating digital signatures. The safety of these protocols and cryptosystems depends on the complexity of several theoretic problems such as integer factorization or the discrete logarithm problem over different groups [1].

Furthermore, when studying cryptography, special attention should be paid to the execution of cryptographic algorithms and administration of cryptographic keys, their appliance, users, and goals of usage.

A significant threat to modern cryptographic algorithms is the so-called "quantum computers" — extremely powerful machines that, unlike classic computers, use quantum bits (qubits), which can be in the state of superposition. Quantum

cryptography is the science that studies the methods of communication systems and is based on the inviolability of the patterns of quantum physics. It supposed to create new and improve already existing post-quantum algorithms that will help counteract quantum computers in the future.

The concept of quantum computing was presented by Feynman in 1982. Its novelty consisted in representing data in quantum bits instead of classic bits. While bits can take only two values — 0 and 1 — qubits can be in the state of 0, 1 and also in both at the same time. This feature made it possible for quantum computers to execute a number of difficult operations a lot faster than classical computers, which means that they are dangerous for algorithms based on these operations [2].

The efficiency of quantum computers was clearly demonstrated in 1994 by Peter Shore, when he had shown how fast they can solve both the integer factorization problem and the discrete logarithm problem over different groups. That was the significant proof of insecurity of a public-key cryptosystems based on these presumptions [1].

Thus, many modern communications, such as key exchange or digital authentication, may be at risk if a sufficiently powerful quantum computer appears.

If the issue of quantum computers will not be solved in the nearest future, many systems that use communications and cryptographic algorithms will be in danger. Financial systems will not be able to conduct financial transactions, emailing and messaging will not be safe anymore and electronic commerce along with military and government systems will not be able to function properly.

It is obvious that cryptography is widely used in various spheres of modern society, including the most important ones, to ensure the necessary data security. That is why it is essential to study and implement new post-quantum cryptographic algorithms, which will be able to protect valuable information from quantum computers.

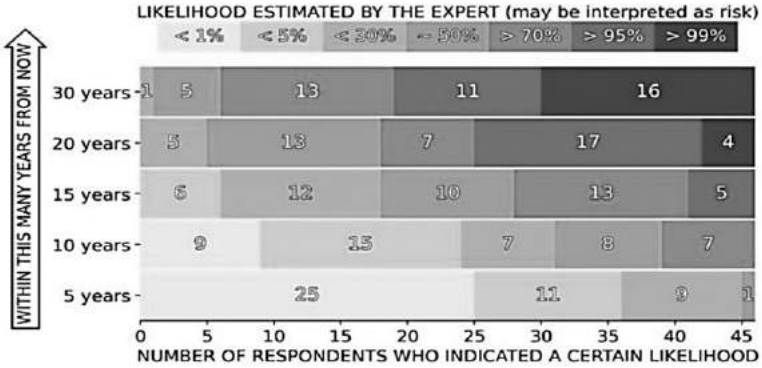

Fig. 1 — Assessment of the probability that quantum computer will be able to break RSA-2048 quickly [3]

As shown in the figure, after 20 years, the probability of breaking the RSA-2048 by quantum computer becomes quite high.

Unfortunately, the exact date and consequences of the advent of the "quantum era" are not known, but the changes promise to be unexpected and rapid. However, it can be predicted how many more advantages quantum computing will have and how much quantum algorithms and models will differ from classical ones [2].

For this purpose, it is necessary to conduct a large amount of research, try out different approaches and methods, and definitely investigate the possibility of developing post-quantum algorithms that could claim the role of standards in the future and solve the problems of post-quantum cryptography.

II. Literature analysis and problem statement

The selected literature allows you to explore the current state of quantum stable cryptography. At the same time, various cryptographic algorithms were analyzed along with their type, purpose, and an influence of quantum computers on them [4].

Table 1 — Predicted Impact of Quantum Computers on NIST's Common Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	-----	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

The algorithms and approaches indicated in the table are well implemented for classical computers, but if they are used for quantum ones, the above result will be obtained.

According to the literature [5], applying AES, SHA-2, SHA-3, PSA, ECDSA, ECDH, DSA without upgrading is dangerous for data security.

Due to the need for stronger cryptography, there has been huge progress in both classical and quantum computing technologies. To increase the security of systems against classical attacks, NIST has already recommended moving from key sizes and algorithms that provide 80 bits of security to key sizes and algorithms that provide 112 or 128 bits of security. Such actions by NIST should lighten the more arduous transition to new post-quantum cryptosystems that will ensure security against quantum attacks [6].

The problem is that known algorithms cannot be used to the fullest as existing ones because quantum algorithms, although developed, have not yet been fully studied and improved.

III. Research aim and objectives

The purpose of the research is to study the possibilities of already existing cryptographic algorithms and post-quantum ones, which are candidates for standards, as one of the ways to ensure data security during the implementation of quantum computers.

In this research the standards CRYSTALS-KYBER, CRYSTALS Dilithium, FALCON and SPHINCS+, which NIST proposed to standardize after an open competition for choosing quantum-resistant cryptographic algorithms with an open key, will be analyzed.

IV. Object, subject, and methods of research

The subject of the work is post-quantum crypto-algorithms.

The object of the work is the basics of quantum cryptography, related to the preparation of secure systems before the advent of quantum computers. The results of the research should enable understanding at what stage science currently is in preparing algorithms for the quantum transition and what further actions required to be implemented so that the information security system works properly.

This study aims to answer the following research question: post-quantum algorithms that are contenders for standards, their implementation capabilities, and their ability to provide security against the computational capabilities of quantum computers.

This study is conducted according to the PRISMA model.

The links and research content below were obtained from Google Scholar and Research Gate [2].

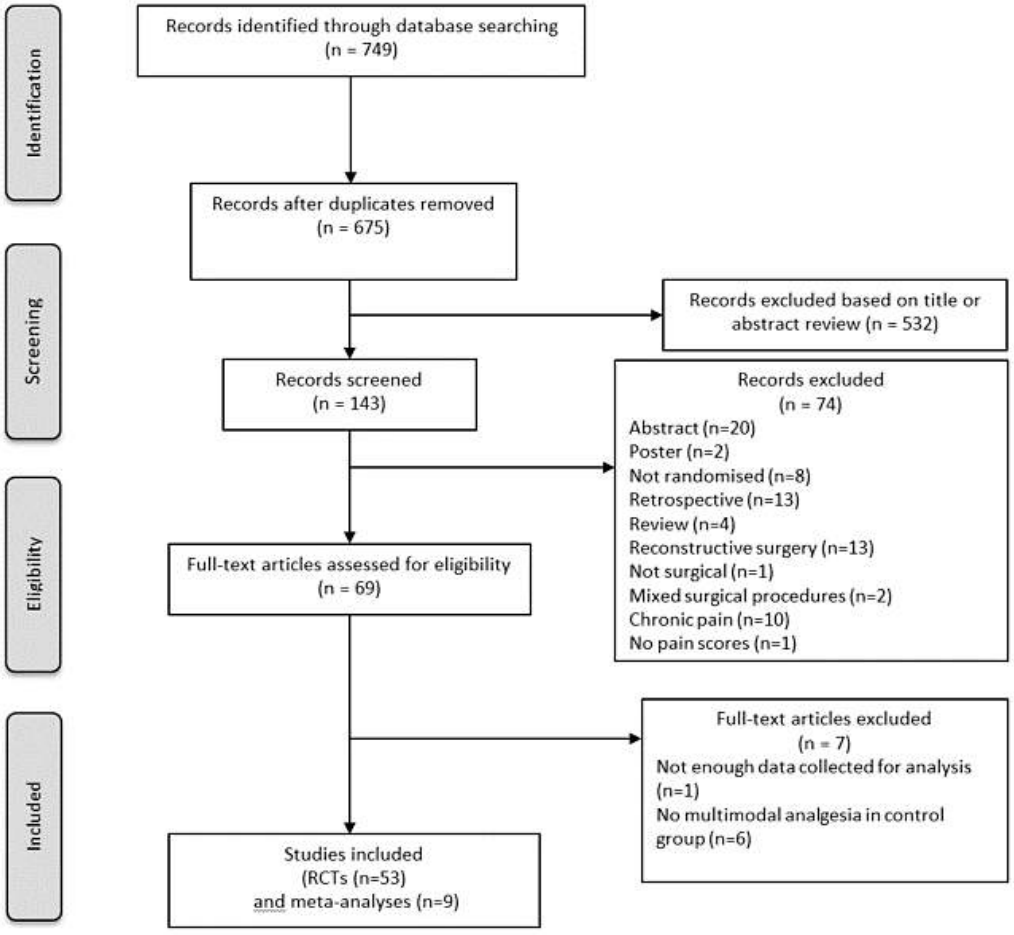

Fig. 2 — PRISMA's record selection flow [2]

Figure 2 shows PRISMA's record selection flow.

Many scientific articles were analyzed, they were selected according to the topic and purpose of the research and according to modern scientific challenges. Some information was excluded as outdated, and the latest scientific researches and results were described in more details. No prohibited sources were used.

V. Results

The factors of further development determine the unreliability of the prospects of traditional cryptography and force us to look for alternative methods of ensuring the security of information resources. Due to the current trends in the development of cryptography, such alternatives can be methods of quantum cryptography. Successes in this area prove the ability of such methods to solve a number of traditional cryptographic problems, in particular, the distribution of encryption keys [7].

The discovery of cryptographic vulnerabilities and limitations, as well as progress in cryptanalysis, force the replacement of outdated cryptographic algorithms.

When Shor's algorithm can be put into practice, then additional security measures will have to be taken. For example, protecting stored keys and data would require their re-encrypting using a quantum-resistant algorithm and deleting or physically protecting “old” copies, such as backups. The integrity and sources of information will be considered untrustworthy unless they are processed or encapsulated by a mechanism that is not vulnerable to quantum computing-based attacks. This is, for example, a re-sign or a timestamp. However, if the encrypted material was previously stored by the attacker, nothing can be done to protect its confidentiality [8].

The National Institute of Standards and Technology (NIST), along with other international institutions, is engaged in the standardization of quantum algorithms. To solve this problem, NIST announced an open competition to select quantum-resistant public-key cryptographic algorithms. After the 3rd evaluation round, it was proposed to standardize the Public Key Encapsulation Mechanism (KEM) called CRYSTALS-KYBER. Regarding algorithms for the protection of digital signatures, CRYSTALS Dilithium, FALCON and SPHINCS+ have been proposed [6]. In practice, it takes from 5 to 15 or even more years from the moment of publication to finalize the implementation of accepted cryptographic standards [9].

Therefore, using quantum cryptography in comparison with classical cryptography, it is possible to ensure the necessary data security, even in opposition to quantum computers.

5.1. CRYSTALS-Kyber

KYBER is a module learning with errors (MLWE) based key encapsulation mechanism. The effective implementation of the polynomial operation is crucial for high-performance CRYSTALS-KYBER programs. This means that the processor performs optimized ring polynomial arithmetic, which reduces modular multiplication or addition times by more than 20%/50% compared to straightforward implementations. Alternating parameters allow MLWE to obtain a more flexible compromise between security and performance than Ring-LWE [10].

Regarding security — many results remain conjectural, but are consistent with modern lattice cryptanalysis. Another advantage of KYBER over other algorithms of its type is the size of the public key and encrypted text. It is about a thousand bytes, which should be acceptable for most applications [6].

Table 2 — Key and ciphertext sizes (in bytes) for Kyber, according to source [6]

Candidate	Claimed Security	Public Key	Private Key	Ciphertext
KYBER512	Level 1	800	1632	768
KYBER768	Level 3	1184	2400	1088
KYBER1024	Level 5	1568	3168	1568

In comparison to other KEM candidates, Kyber has excellent performance in both software and hardware [11].

5.2. CRYSTALS–Dilithium

Dilithium is a lattice-based digital signature algorithm based on the Fiat-Shamir paradigm and built on top of MLWE.

The main novelty of the Crystal-Dilithium algorithm is that by increasing the signature by approximately 150 bytes, the size of the public key is reduced by 2.5 times. In addition, the size of the public key can be reduced in another way — with the help of algorithms that extract the bits of the “high” and “low” order elements into Zp.

The security of the Dilithium digital signature scheme is based on the difficulty of finding short vectors in lattices. The design of the algorithm itself is based on the “Fiat-Shamir with interrupts” method, which uses deviation sampling to make lattice-based Fiat-Shamir circuits compact and secure [12].

Dilithium's security establishment is based on the Module-LWE decision assumption, which suffices to demonstrate that the public key does not leak any information about the private key. As for the strong binding property, it can be used for non-repudiation as the unique public key and message identify a specific Dilithium signature. This algorithm is considered efficient and simple to implement, and also has a strong theoretical basis [6].

5.3. FALCON

FALCON (Fast Fourier Lattice-based Compact Signatures over NTRU) is a lattice-based signature scheme using a “hash-and-sign” paradigm.

FALCON does not offer certain desirable properties other than unforgeable security ones, although it is possible to achieve them through modifications with little performance cost [2].

True Gaussian sampling is used internally. This guarantees little leakage of information about the secret key to an almost infinite number of signatures (more than 264). The main novelty is a very fast recursive Gaussian sampling algorithm using a tree data structure ("falcon tree") [12].

FALCON has two big advantages. The first one is the lowest bandwidth among the NIST candidates. The second one is a fast signature verification. Both of these characteristics may make this algorithm well suited for some applications [13].

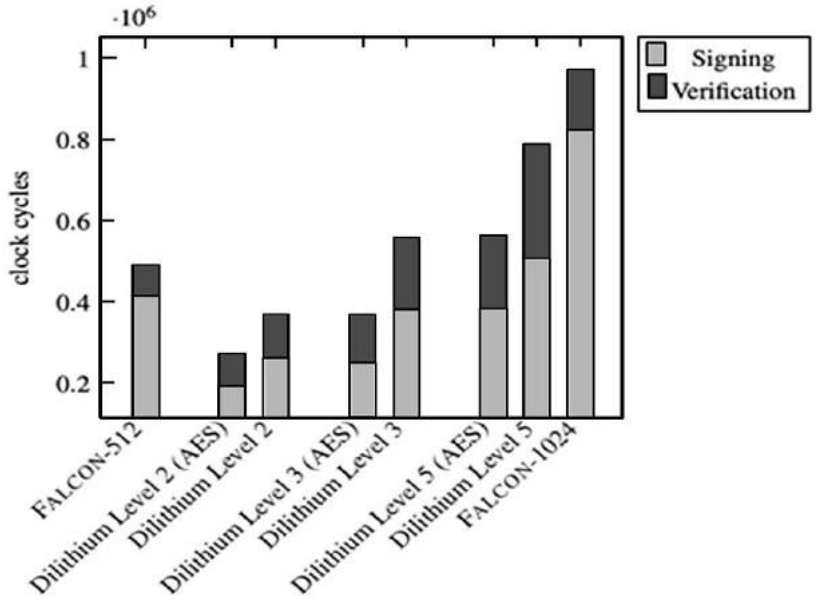

Fig. 3 — Signature tests on an x86-64 processor with AVX2 extensions [6]

The most famous attacks against FALCON are based on truncation of the lattice base, without making significant use of the special NTRU lattice structure. In order for the signature algorithm to be protected against side-channel attacks, it needs to be refined [12].

5.4. SPHINCS+

SPHINCS+ is a stateless hash-based signature scheme. It combines the use of one-time signatures, multiple signatures, Merkle trees, and hypertrees to create a digital signature scheme which is suitable for general use [14].

Since the scheme is stateless, there is no need for the user to store state in signatures, which is an advantage. After all, if the state is stored incorrectly, it can lead to catastrophic consequences.

Since the scheme is stateless, there is no need for the user to store state in signatures, which is an advantage. After all, if the state is stored incorrectly, it can lead to catastrophic consequences.

The complexity of this signature makes it difficult to implement and evaluate security. At the same time, it relies on basic hash functions, thus providing a loophole for cryptanalyst attacks [6].

Table 3 — Key and signature sizes (in bytes) for signature finalists, according to source [6]

Candidate	Claimed Security	Public key	Private Key	Ciphertext
Dilithium	Level 2	1 312	2 528	2 420
	Level 3	1 952	4 000	3 293
	Level 5	2 592	4 864	4 595
FALCON-512	Level 1	897	7 553	666
FALCON-1024	Level 5	1 793	13 953	1 280
SPHINCS+-128s	Level 1	32	64	7 856
SPHINCS+-128f	Level 1	32	64	17 088
SPHINCS+-192s	Level 3	48	96	16 224
SPHINCS+-192f	Level 3	48	96	35 664
SPHINCS+-256s	Level 5	64	128	29 792
SPHINCS+-256f	Level 5	64	128	49 856

For this signature scheme, both key generation and verification are much faster than signing itself. At the same time, very short open keys contrasting with rather long signatures are characteristic. Since SPHINCS+ is based on a different

mathematical foundation than Dilithium and FALCON, it was reckoned as a good candidate on account of variousness.

VI. Results discussion

The search for new cryptographic approaches for a post-quantum world shows that organizations for standardization are aware of the dangers of quantum computers. If a quantum computer becomes available for illicit use, many things which are considered safe will no longer be so.

New studies, their results and timing prompt organizations such as NIST to publish a final list of candidates for standardization in 2023. Of course, the definition of standards is not the final stage yet and there is still a lot of work to be done. Moreover, before standardization, it is necessary to thoroughly research the field of quantum algorithms, compare them, and improve them according to the criteria. Time and effort must be invested to prepare for the challenge of the post-quantum world.

When evaluating candidates, NIST was paying attention to the performance of the new algorithms, the time needed to generate keys, the size of these keys, and the time required to verify signatures [2].

There are still many unanswered questions, including variants of each algorithm, different approaches to each implementation, and how each algorithm can be improved and made more resilient to different attacks [15].

VII. Conclusions

Unfortunately, the underlying systems lack of cryptographic flexibility, that is, the ability to quickly adapt to new cryptographic algorithms without the need for significant changes to the system itself.

The results of the conducted research showed that existing and new algorithms will have different mathematical bases and requirements, so it is necessary to ensure compatibility for new algorithms or new protocols that will be compatible to some extent with existing algorithms.

Considering the disadvantages and advantages of new quantum algorithms, it is already possible to develop the next stages of standardization actions. If this action plan is implemented successfully, the desired level of protection will be achieved along with new systems that will be more flexible, reliable and promising.

Currently, none of the known quantum algorithms can fully replace the existing ones, since, although they have already been developed, they have not yet been fully studied and improved.

VIII. References

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

[2.] Pinto, J. (2022). Post-quantum cryptography challenges, 13.

[3.] Mavroeidis, V., Vishi, K., Zych, M. D., Jøsang A. (2018). The Impact of Quantum Computing on Present Cryptography, 25.

[4.] Christopher, P. (2019). Identifying research challenges in post quantum cryptography migration and cryptographic agility, 30.

[5.] Barker, W., Consulting, D., Polk, W. (2021). Getting ready for post-quantum
Cryptography: exploring challenges associated with adopting and using post-quantum cryptographic algorithms, 10.

[6.] Moody, D. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, National Institute of Standards and Technology, Gaithersburg, 35.

[7.] Корченко, О.Г., Луцький, М.Г., Гнатюк, С.О. (2011). Сучасні комерційні системи квантової криптографії, Мир, 115.

[8.] Chen, L., Jordan, S., Liu, Y-K, Moody, D., Peralta, R., Perlner, R., Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR), 23.

[9.] Chen, L. (2017). Cryptography Standards in Quantum Time: New Wine in an Old Wineskin? IEEE Security & Privacy, 15(4), 51-57.

[10.] Zhaohui, C., Yuan, M., Tianyu, C., Jingqiang, L., Jiwu, J. (2020). High-performance area-efficient polynomial ring processor for CRYSTALS-Kyber on FPGAs, 25-35.

[11.] Duarte, N., Coelho, N., Guarda, T. (2021). Social Engineering: The Art of Attacks. In: Guarda, T., Portela, F., Santos, M.F. (eds) Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS. Communications in Computer and Information Science, vol 1485. Springer, Cham, 127.

[12.] Перший міжнародний науково-практичний форум «Global Cyber Security Forum». Зб. матеріалів форуму. – Харків: ХНУРЕ. 2019. – 115 с. https://openarchive.nure.ua/server/api/core/bitstreams/ed01c8c4-0251-43f7-9851-ad5797f1de8e/content#page=59

[13.] Limniotis, K. (2021). Cryptography as the Means to Protect Fundamental Human Rights, Cryptography, vol. 5, 34.

[14.] Chen, L. (2016). Report on Post-Quantum Cryptography, National Institute of Standards and Technology, NIST IR 8105, 23-45.

[15.] Hoffstein, J., Pipher J., Silverman J. H. NTRU: A ring-based public key cryptosystem, in Algorithmic Number Theory, vol. 1423, J. P. Buhler, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 267–288.

Отримана в редакції 24.04.2023. Прийнята до друку 22.05.2023. Received 24 April 2023. Approved 22 May 2023. Available in Internet 19 June 2023.