IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 37, No. 3, June, 2023, pp. 655-664
Journal homepage: http://iieta.org/journals/ria

Analysis of Existing Approaches and Algorithms of Post-Quantum Cryptography

Aigerim Kerimbayeva

Department of Cyber Security, Information Processing and Storage, Satbayev University, 22A Satpaev Str. 050013, Almaty, Republic of Kazakhstan

Corresponding Author Email: kerimbayevaaigerim0@gmail.com

https://doi.org/10.18280/ria.370314

Received: 1 May 2023
Accepted: 31 May 2023

Keywords:
encryption, information security, data protection, key exchange protocols, electronic digital signature, post-quantum cryptography

ABSTRACT

The rapidly evolving field of post-quantum cryptography necessitates a comprehensive analysis of existing technologies to determine their efficiency and reliability. This study aims to identify the strengths and weaknesses of contemporary approaches and algorithms in post-quantum cryptography, ultimately pinpointing the most effective solutions. To achieve this objective, an analytical comparison of practical post-quantum cryptography systems was conducted, considering key metrics such as security against quantum attacks, computational efficiency, compatibility with existing systems, resistance to various cyber threats, ease of implementation, potential for standardization, and compliance with regulatory requirements. The findings reveal that while numerous approaches and algorithms exist in post-quantum cryptography, the NTRU and SIKE algorithms demonstrate superior efficacy. Additionally, WOTS+, Dilithium, and SABER exhibit promising potential, each possessing unique advantages and disadvantages concerning key size, computation speed, attack resistance, and implementation feasibility. This study offers practical value by providing guidance in the selection and adoption of post-quantum cryptography technologies, thereby contributing to the field's advancement and ensuring robust security in a post-quantum era.

1. INTRODUCTION

The pressing need to safeguard confidentiality, authentication, and data integrity has led to the development of post-quantum cryptography approaches and algorithms designed to thwart attacks by quantum computers. Various interpretations of this term exist within the literature. Renowned American-German mathematician, cryptographer, and programmer Bernstein [1] defines post-quantum cryptography (also referred to as quantum-proof, quantum-safe, or quantum-resistant) as encompassing cryptographic algorithms (primarily public key algorithms) that remain secure against cryptanalytic attacks by quantum computers. From this perspective, this aspect of cryptography retains its relevance in the face of quantum computers and quantum attacks.

Conversely, German cryptographer and number theory expert Lange [2] posits that "post-quantum cryptography is the study of cryptosystems that can run on a classical computer but remain secure even if the adversary has a quantum computer". This alternative definition emphasizes the importance of maintaining security in cryptosystems that operate on classical computers while recognizing the potential threat posed by adversaries with access to quantum computing capabilities.

Both definitions recognize the need to address the security implications of quantum computers. They agree that post-quantum cryptography involves developing cryptographic systems that can withstand attacks from quantum computers. Bernstein's definition [1] specifically highlights the importance of protecting against cryptanalytic attacks of a quantum computer using post-quantum cryptographic algorithms, particularly public key algorithms. Lange's definition [2] focuses on the study of cryptosystems that are secure against quantum attacks, even if executed on classical computers. The key difference between the two definitions lies in the emphasis placed on the nature of the cryptographic algorithms used (protected from cryptanalytic attacks of a quantum computer in Bernstein's definition [1]) and the execution environment (classical computer but safe against a quantum computer in Lange's definition).

The main disadvantage of current algorithms is that their security relies on one of three mathematically challenging problems: the integer factorization problem, the discrete logarithm problem, or the discrete elliptic curve logarithm problem. All of these problems can be efficiently solved by powerful quantum computers using algorithms such as Deutsch's algorithm, Deutsch-Jozsa algorithm, Shor's algorithm, or Grover's algorithm. In contrast, classical computers are significantly slower in solving these problems using pre-quantum algorithms. As a result, cryptographic systems based on integer factorization or discrete logarithm problems can become vulnerable to attacks by quantum computers. Recognizing this vulnerability, cryptographers have been actively developing algorithms that are resistant to quantum attacks [3].

The relevance and role of algorithms like Deutsch's algorithm, Deutsch-Jozsa algorithm, Shor's algorithm, and Grover's algorithm lie in their potential threat to classical cryptographic systems posed by quantum computers. Deutsch's algorithm and Deutsch-Jozsa algorithm: While these algorithms themselves do not pose a direct threat to classical

cryptographic systems. They showcase the computational advantage of quantum computers in solving certain types of problems. This highlights the need for developing new cryptographic algorithms that can resist quantum attacks and maintain security in the face of quantum computing power. Shor's algorithm is a significant concern for classical cryptographic systems, particularly those based on the hardness of factoring large integers or solving discrete logarithm problems. By efficiently factoring large numbers, Shor's algorithm can break widely used asymmetric encryption schemes like RSA and Diffie-Hellman.

This emphasizes the urgency of adopting post-quantum cryptographic algorithms that are resistant to Shor's algorithm and can provide secure encryption in the quantum era. Grover's algorithm poses a threat to symmetric key cryptographic algorithms by significantly reducing the effective key size. It allows for a quadratic speedup in searching an unsorted database, which can undermine the security of symmetric encryption algorithms like AES. As with the other algorithms, the emergence of Grover's algorithm underscores the need for post-quantum cryptographic solutions that can resist quantum search algorithms and maintain the confidentiality and integrity of data.

There have been numerous studies focusing on improving the security of post-quantum cryptography algorithms, with the goal of ensuring their resistance to attacks from quantum computers. The National Institute of Standards and Technology (NIST) initiated a competition to standardize quantum-resistant public-key algorithms, which has spurred extensive research in this field. Researchers such as Basu et al. [4, 5] have conducted hardware comparisons of candidate algorithms for the NIST competition, identifying weaknesses and proposing enhancements to their security.

Dutch specialists have provided an overview of the ongoing standardization process for post-quantum cryptography, covering algorithm families, encryption schemes, and signatures, along with recommendations for protecting confidential data using hybrid schemes of quantum and post-quantum cryptography [6]. The transition to post-quantum cryptography and its implications have been explored by Barker et al. [7], who examine the NIST standardization processes, testing, resistance to attacks, and conditions for ensuring algorithm security.

Additionally, Nguyen et al. [8] propose the use of number-theoretic transformations to expedite hardware and software implementation of post-quantum cryptography algorithms, presenting an improved hardware architecture and confirming its efficiency through experimental validation. Kumar [9], an Indian cryptographer, emphasizes the vulnerability of all cryptography algorithms to hacker attacks, advocating for the adoption of post-quantum cryptographic algorithms to achieve the required level of security. Kumar provides insights into the design, development, and standardization processes of secure quantum algorithms and proposes ways to facilitate the rapid and efficient implementation of this technology. While many recent studies have focused on NIST standardization and a limited set of algorithms, this article delves deeper into the possibilities and capabilities of post-quantum cryptography technologies.

The purpose of the work is to analyse and compare existing algorithms in this science area, their advantages and disadvantages. The study considers both established systems and participants/finalists of the NIST competition for post-quantum cryptographic algorithms. The stages cover different categories of algorithms, including approaches based on Merkle signatures, hash functions, error correction codes (McEliece system), NTRU encryption, braid groups, supersingular isogeny, lattice-based encryption, public-key encryption (CRYSTALS-KYBER, Dilithium, SABER), and digital signature algorithms (Dilithium, Falcon, Rainbow, SPHINCS+, among others). Each stage provides detailed explanations, comparisons, and evaluations of the algorithms, highlighting their strengths, weaknesses, and security levels. The study concludes with a comparison of the obtained results with existing publications, identifying areas for further research, and outlining future directions in the field of post-quantum cryptography.

2. MATERIALS AND METHODS

The methodological approach of this study involves an analysis of the functioning features of various cryptosystems, comparing their efficiency and stability. The analysis considers not only the models that participated in the NIST competition for post-quantum cryptography algorithms but also systems that have been used for a long time. Including non-NIST algorithms allows for a broader exploration of the cryptographic landscape beyond the competition. These alternative algorithms may offer unique features, novel approaches, or different trade-offs in terms of efficiency, security, or practical implementation. Evaluating their performance and comparing them to NIST competition algorithms provides a more comprehensive understanding of the available options for post-quantum cryptography. Including non-NIST algorithms in the study enables a more holistic assessment of the cryptographic systems landscape, ensuring that the evaluation considers established systems alongside the latest competition participants. This approach helps identify the most effective technologies and provides insights into potential directions for future research and development in the field of post-quantum cryptography.

The study is conducted in six stages, each focusing on a specific aspect of post-quantum cryptography. These stages include exploring approaches and Merkle signatures, examining NTRU encryption and the advantages of multidimensional quadratic systems, studying cryptographic encryption with supersingular isogeny and the SIKE model, analyzing public-key encryption and key establishment algorithms with CRYSTALS-KYBER and SABER, investigating digital signature algorithms such as Dilithium, Falcon, and alternative approaches, and concluding with a comparative analysis, identifying strengths and weaknesses, and outlining future directions in post-quantum cryptography. The study employs detailed descriptions, explanations, and comparisons to assess the effectiveness and security of different algorithms, providing valuable insights for the field of post-quantum cryptography.

Exploring approaches and Merkle signatures in post-quantum cryptography. At the first stage, it was indicated which approaches of post-quantum cryptography exclude the attacks possibility. A detailed description of the Merkle signature was provided. The disadvantages of algorithms based on hash functions were described. An explanation of the essence of cryptography based on error correction codes was provided on the example of the McEliece system, the history of its occurrence was presented.

NTRU encryption and the advantages of multidimensional

quadratic systems. At the second stage, the Nth-degree TRUncated polynomial ring (NTRU) encryption system was presented, its main differences from the McEliece system were indicated. It was noted what actions should be taken to obtain an NTRU security guarantee. The cryptography advantages on multidimensional quadratic systems and the mathematical model of the braid group were revealed. The principle of the cryptosystem functioning of the hidden field's equation was indicated. The process of developing a braid group, the conditions under which this model works effectively, as well as the advantages and disadvantages of the algorithm were described.

Cryptographic encryption with supersingular isogeny and the SIKE model. At the third stage, cryptographic encryption algorithms using supersingular isogeny were considered. The definition of the "isogeny" notion was provided. The features of the SIKE model, which reached the final of the third round of the NIST competition, were revealed. A protocol for generating a common key was described, which is based on the isogenies operation of supersingular elliptic curves. Emphasis was made on what tasks should be solved in this area.

Public-key encryption and key establishment algorithms with CRYSTALS-KYBER and SABER. The fourth stage considers public-key encryption and key establishment algorithms, which also made it to the third round of NIST. The features of an algebraic cryptographic suite based on the CRYSTALS-KYBER lattice and modular lattices were described. What operations are required for KyBER and Dilithium cryptographic primitives were indicated. An explanation was provided for the difference in algebraic structure between the lattices used in KyBER and Dilithium from Ring-LWE. The features of the KyBER mechanism and its design were studied, the existing modifications of this model were listed. The features of SABER, which is a secure mechanism for encapsulating IND-CCA2 keys, were considered. Three security levels of the SABER-suite were compared to standard counterparts.

Study of digital signature algorithms, including dilithium, falcon, and alternatives. At the fifth stage, a study of digital signature algorithms was conducted. A description of the operation principle of Dilithium was provided. The advantages and disadvantages of Falcon and Rainbow were briefly described. In addition, alternative algorithms that did not reach the NIST finals were provided at this stage. These include: SPHINCS+, Picnic, GeMSS, Haraka, SHAKE-256, Winternitz, etc. Similarities and differences between GeMSS and Rainbow were indicated. The process of keys generation in the Winternitz algorithm was described, one-time signature scheme was provided. A comparative table of characteristics of the SPHINCS+, Dilithium, Rainbox and Falcon algorithms was provided. A description of the SPHINCS+ digital signature modification was provided.

Comparative analysis, strengths, and future directions in post-quantum cryptography. At the final stage, the obtained results were compared with existing publications regarding this topic. It was revealed what information was missed or insufficiently disclosed. The strengths and shortcomings of the article were identified, conclusions about the most effective technologies were made, and ways for future studies were outlined.

3. RESULTS

In post-quantum cryptography, there are six approaches that exclude the possibility of quantum attacks. These include cryptography based on hash functions, error correction codes, lattices, multidimensional quadratic systems and braid groups [10]. Supersingular isogeny encryption is also used. The first four approaches are described in the scientific article by Bernstein and Lange [11]. According to the authors, the Merkle signature is a classic example of cryptography based on hash functions. This reusable digital signature algorithm is based on the use of the Merkle tree and an arbitrary one-time signature based on a cryptosecure hash function. The algorithm consists of three steps. First of all, the arrays of secret keys X and public keys Y are generated. The pair (Xi, Yi) is used as a "public-private" key pair for a one-time signature. Then, the Merkle tree generates Y: for each Yi, using the cryptosecure hash function H, (Xi, Yi) is calculated, the zero layer of the tree a0. Each further layer is calculated as H (ai, 2n} || ai, 2n+1) (where || – concatenation) until there is one key left in the layer, which is public and is designated as pub_key. Signature generation is as follows. A pair of keys (Xi, Yi), a one-time signature b for message d, a path from Yi to the tree root are determined. The Yi value in this case is the verification key. Parameters Yi, b, the path to the tree root is included in the signature. Signature verification occurs in two steps: first, the recipient determines whether signature b corresponds to message d. In case of a successful check, the path. (Yi) is built up to the tree root. The match of the obtained tree root with pub_key is a successful verification of the signature. The disadvantage of algorithms based on hash functions is the limitation of the signatures number used once for each message. This is the main obstacle to the mass use of this approach.

Numerous studies should be conducted to gain confidence in the security of lattice-based cryptography [11, 12]. It should also be noted that there is no exact method for evaluating the algorithms complexity on lattices for the existing types of attacks. The quantum-resistance of cryptography on multidimensional quadratic systems is built on the complexity of solving a system of multidimensional quadratic polynomials over a finite field. This is an NP-complete task. These systems are characterised by good speeds and require large computing resources, but the length of the public keys is quite large. The best-known example is the Hidden Field Equation (HFE) cryptosystem, which is based on hidden field equations and was released in 1996. It was suggested by Bernstein [1].

Braid groups have been cryptanalyzed many times and improved due to the results of the attacks. The conjugation search algorithm has also been upgraded. However, from the point of view of modern technologies and theory, the conjugation problem of these systems is still difficult. This means that there is no method for solving it in polynomial time. Thus, n is a strong security parameter. The advantages include a higher computational complexity of the algorithm (in contrast to RSA-1024). Keys are generated a hundred times faster, and it takes less time to encrypt and decrypt messages. The latest versions of electronic digital signature schemes are of high value in practice. The disadvantages include the high computational complexity of encryption [13].

Cryptographic encryption algorithms using supersingular isogeny have rather low speeds, but also contain short public keys and ciphertexts [3]. This is similar to the Diffie-Hellman protocol, which is based on walking in a supersingular isogenic graph and allows other parties to obtain a shared secret key using an insecure communication channel. An

isogeny is a rational mapping between two elliptic curves, known as a "homomorphism". Supersingular elliptic curves were initially considered ineffective in pre-quantum cryptography. However, it was discovered that the l-isogeny graph possesses qualities that ensure high cryptographic strength. Building upon this, cryptographers developed the SIKE algorithm based on SIDH, which became an alternative finalist in the third round of the NIST competition. Compared to other algorithms, SIKE offers the advantage of smaller sizes for public keys and ciphertexts. Additionally, Grebnev et al. [12] developed the "forsythia" protocol, which generates a common key using the apparatus of supersingular elliptic curves isogenies. The authors opted against compressing public keys to ensure fast protocol operation. Currently, challenges remain in creating effective schemes for authenticated generation of a common key and digital signature based on the isogenic apparatus of supersingular elliptic curves, and efforts are needed to improve their productivity.

Moving forward, the next stage of the study involves reviewing the algorithms for public key encryption and key derivation that advanced to the third round of the NIST competition. The CRYSTALS-KYBER suite is a lattice-based algebraic cryptographic suite that includes two cryptographic primitives: KyBER, an IND-CCA2 secure key encapsulation mechanism (KEM), and Dilithium, a highly secure EUF-CMA digital signature algorithm. Both algorithms are built upon complex modular lattice problems designed to resist attacks from large quantum computers, and they were introduced as part of the NIST Post-Quantum Cryptography Project [9]. Modular lattices can be considered as the lattices lying between the lattices used in the Learning with Errors (LWE) problem definitions and the lattices used for the Ring-LWE problem. If the base ring of modules has a sufficiently high degree (for example, 256), then these lattices inherit all the efficiency used in the Ring-LWE problem, and also have the following advantages when used in cryptographic algorithms.

The only operations necessary for KyBER and Dilithium for all security levels are the Keccak variants, adding/multiplying in Zq for fixed q, and theoretical number transformation (NTT) for the Zq[X]/(X256+1) ring. This means that updating or downgrading security level requires little or no re-implementation of the schemes in software or hardware. The lattices used in KyBER and Dilithium differ in algebraic structure from Ring-LWE, and are more similar to the unstructured lattices used in LWE. Therefore, they may be less effective against the KyBER and Dilithium schemes if algebraic attacks on the Ring-LWE occur [14].

The six approaches to post-quantum cryptography discussed in the study encompass cryptography based on hash functions, lattice-based cryptography, multidimensional quadratic systems, error correction code-based cryptography, braid groups, and cryptographic encryption with supersingular isogeny. These approaches vary in their underlying mathematical foundations and cryptographic techniques. For example, hash function-based cryptography relies on Merkle signatures but faces limitations in the number of signatures used per message. Lattice-based cryptography offers advantages such as smaller key sizes, while error correction code-based cryptography utilizes generator matrices for encryption. Braid groups provide high computational complexity, and supersingular isogeny encryption offers small-sized public keys and ciphertexts.

KyBER is a secure IND-CCA2 key encapsulation mechanism (KEM) whose security depends on the difficulty of solving the learning with error (LWE) problem over modular lattices. The design of this mechanism is based on the original Regev encryption scheme based on LWE. Since Regev's first work, the practical efficiency of LWE encryption schemes has been improved, because the secret in LWE can come from the same distribution as the noise, and LWE type schemes can be created using a square (not rectangular) matrix as the public key. Another modernisation was to implement the idea originally used in the NTRU cryptosystem for the description of the Ring-LWE and Module-LWE problems using polynomial rings rather than integers. CCA-secure KEM Khyber is built on a CPA-secure cryptosystem based on the Module-LWE security. However, NIST also reminds that the LWE module is a relatively understudied problem and requires more detailed cryptanalysis. Table 1 shows the performance characteristics of different KyBER versions.

Table 1. Characteristics of the KyBER work

KyBER512					
Sizes (in bites)		Haswell	Cycles (ref)	Haswell cycles	(AVX2)
sk:	1632	gen:	141872	gen:	55160
pk:	736	enc:	205468	enc:	75680
ct:	800	dec:	246040	dec:	74428
KyBER768					
Sizes (in bites)		Haswell	Cycles (ref)	Haswell cycles	(AVX2)
sk:	2400	gen:	243004	gen:	85472
pk:	1088	enc:	332616	enc:	112660
ct:	1152	dec:	394424	dec:	108904
KyBER1024					
Sizes (in bites)		Haswell	Cycles (ref)	Haswell cycles	(AVX2)
sk:	3168	gen:	368564	gen:	121056
pk:	1440	enc:	481042	enc:	157964
ct:	1504	dec:	558740	dec:	154952

Source: [15]

Table 2. SABER parameters

LightSABER					
Sizes (in bites)		Haswell cycles (ref) [x1000]		Haswell cycles (AVX2) [x1000]	
sk:	1568 (992)	gen:	98	gen:	45
pk:	672	enc:	139	enc:	61
ct:	736	dec:	151	dec:	63
SABER					
Sizes (in bites)		Haswell cycles (ref) [x1000]		Haswell cycles (AVX2) [x1000]	
sk:	2304 (1440)	gen:	200	gen:	82
pk:	992	enc:	260	enc:	105
ct:	1088	dec:	271	dec:	108
FireSABER					
Sizes (in bites)		Haswell cycles (ref) [x1000]		Haswell cycles (AVX2) [x1000]	
sk:	3040 (1760)	gen:	336	gen:	131
pk:	1312	enc:	402	enc:	159
ct:	1472	dec:	422	dec:	165

Source: [16]

NTRU refers to lattice cryptography. It is based on the NTRUEncrypt scheme suggested over 20 years ago. Unlike the LWE module (and other modifications), the NTRU

problem is very well studied, which is a very important factor. SABER is a secure IND-CCA2 key encapsulation mechanism (KEM) that is based on the module learning with rounding (MLWR), provides security and remains secure even from quantum computers. SABER is one of the contenders for participation in the second round of NIST standardisation of post-quantum cryptography. SABER-suite provides three levels of security. The first one is the LightSABER, a post-quantum security similar to the AES-128. The second one is SABER, post-quantum security similar to AES-192. The third one is FireSABER, post-quantum security similar to AES-256. SABER parameters are described in Table 2.

Then, let's consider digital signature algorithms. Dilithium is a highly secure digital signature scheme that provides protection against single message attacks by leveraging the complexity of lattice problems over modular lattices. The security concept ensures that an adversary with access to the signature oracle cannot forge a signature for an unseen message or create a different signature for a message that was previously considered signed. Dilithium is among the candidate algorithms submitted to the NIST Post-Quantum Cryptography Project. Its design is based on the Fiat-Shamir method, incorporating Lukaszewski interruption methods to create compact and secure Fiat-Shamir network circuits. The smallest signature size scheme using this approach is the Duke, Durmus, LePoint, and Lubashevsky scheme, which relies on the NTRU assumption and employs Gaussian sampling for signature generation. To address the challenges associated with safe and efficient Gaussian sampling, a uniform distribution is used instead. Dilithium further enhances the scheme by combining uniform distribution and introducing a novel technique that reduces the public key size by more than 2 times. Table 3 presents the performance data for Dilithium, including all the updates made to the parameter sets for round 3 of the NIST PQC project.

All tests were conducted by the authors of the study on a single core of the Intel Core i7-6600U processor (Skylake). Two different implementations were tested: A reference implementation and an optimized implementation utilizing AVX2 vector instructions. Falcon is classified under the lattice cryptography family. Its main disadvantage lies in its complex hardware and software implementation. The scheme involves computations with floating-point numbers, which not only makes it challenging to analyze its resistance against third-party channel attacks but also complicates implementation on resource-constrained devices. When using the reference implementation on a typical desktop computer (Intel Core i5-8259U, clock frequency of 2.3 GHz with TurboBoost disabled), Falcon demonstrates the performance results shown in Table 4.

Table 3. Dilithium performance

Dilithium2					
Sizes (in bites)		Skylake cycles (ref)		Skylake cycles (AVX2)	
		gen:	300751	gen:	124031
pk:	1312	signature:	1355434	signature:	333013
signature:	2420	Verification:	327362	Verification:	118412
Dilithium3					
Sizes (in bites)		Skylake cycles (ref)		Skylake cycles (AVX2)	
		gen:	544232	gen:	256403
pk:	1952	signature:	2348703	signature:	529106
signature:	3293	Verification:	522267	Verification:	179424
Dilithium5					
Sizes (in bites)		Skylake cycles (ref)		Skylake cycles (AVX2)	
		gen:	819475	gen:	298050
pk	2592	signature:	2856803	signature:	642192
signature:	4595	Verification:	871609	Verification:	279936

Source: [17]

Table 4. Falcon performance

Version	Keygen (ms)	Keygen (RAM)	Signing Speed	Signature Verification Speed	Key Size	Signature Size
Falcon-512	8.64	14336	5948.1	27933	897	666
Falcon-1024	27.45	28672	2913	13650	1793	1280

Source: [18]

Table 5. Standard rainbow key and signature sizes

Level	Parameters	Public Key Size (kB)	Private Key Size (kB)	Signature Size (bit)
I	(GF(16), 36,32,32)	157.8	101.2	528
III	(GF(256),68,32,48)	861.4	611.3	1.312
V	(GF(256),96,36,64)	1.885.4	1375.7	1.632

Source: [19]

Table 6. Cyclis rainbow key and signature sizes

Level	Parameters	Public Key Size (kB)	Private Key Size (kB)	Signature Size (bit)
I	(GF(16), 36,32,32)	58.8	101.2 (99)	528
III	(GF(256),68,32,48)	258.4	611.3 (603)	1.312
V	(GF(256),96,36,64)	523.5	1375.7 (1.361.8)	1.696

Source: [19]

Rainbow is a multidimensional cryptography based on the UOV scheme. The main advantage is the size of the digital signature. However, due to the large key size, it is recommended to use this scheme only for certain tasks where the key size is not critical. Rainbow performance parameters are shown in Tables 5-6.

Additionally, eight alternative schemes were selected by NIST that did not advance to the final round but show promise. Among the digital signature schemes are SPHINCS+ and Picnic, which are based on symmetric cryptographic primitives. The security analysis of SPHINCS+ focuses on the security of hash functions, non-interactive zero-knowledge proofs (NIZK), and block ciphers. These schemes are relatively new and still require further study. However, their main drawback lies in their large signature size, which makes them unsuitable for many applications. GeMSS, on the other hand, is similar to Rainbow but is based on hidden field equations (HFE) instead of unbalanced oil and vinegar (UOV). GeMSS has a larger key size and slower signing process compared to Rainbow, and it serves as an alternative option in the event of vulnerabilities being discovered in Rainbow. Although these schemes did not make it to the final three contenders for the NIST Post-Quantum Cryptography winner, they still provide an alternative approach to digital signatures. Most hash-based methods require the private keys used for signing previous messages to be stored. SPHINCS, proposed by Bernstein [1], is a stateless hash-based signature scheme. For instance, the public key size of 128-bit SPHINCS+ 256 is 32 bytes, the private key is 64 bytes, and the signature size is 17 kilobytes. On a 3.5GHz 4-core processor, it can achieve hundreds of hashes per second. Other methods mentioned are Haraka and SHAKE-256 in 128-bit, 192-bit, and 256-bit versions [20].

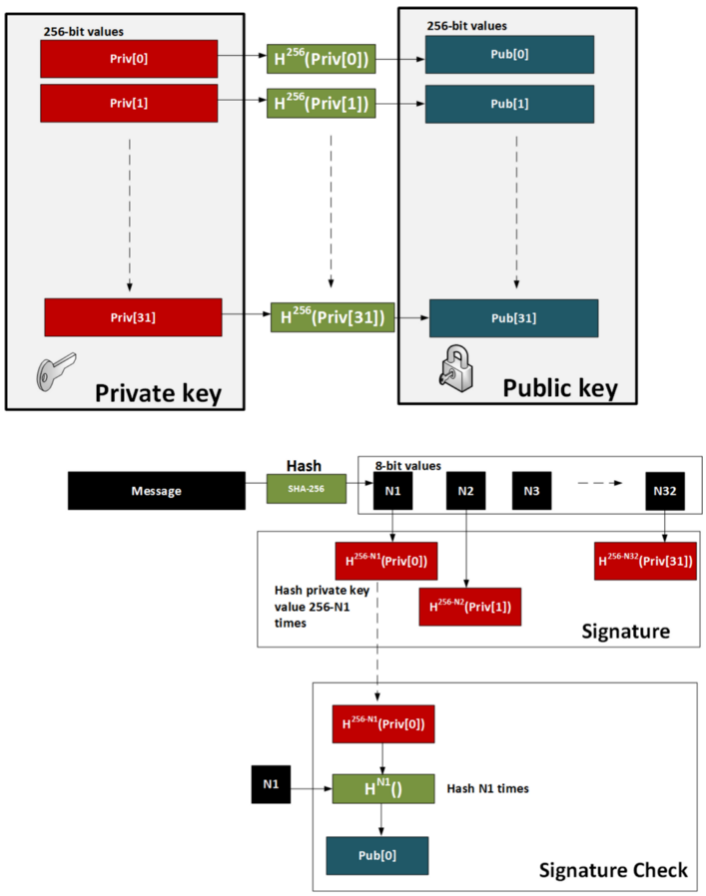

Figure 1. Winternitz One Time Signature Scheme (WOTS)
Source: [21]

Method	Public key size	Private key size	Signature size	Security level
Crystals Dilithium 2 (Lattice)	1,312	2,528	2,420	1 (128-bit)
Crystals Dilithium 3	1,952	4,000	3,293	3 (192-bit)
Crystals Dilithium 5	2,592	4,864	4,595	5 (256-bit)
Rainbow Level Ia (Oil-and-Vineger)	161,600	103,648	66	1 (128-bit)
Rainbow Level IIIa	861,400	611,300	164	3 (192-bit)
Rainbow Level Vc	1,885,400	1,375,700	204	5 (256-bit)
FALCON 512 (Lattice)	897	1,281	690	
FALCON 1024	1,793	2,305	1,330	
SPHINCS+ SHA-256 128-bit	32	64	17,088	1 (128-bit)
SPHINCS+ SHA-256 192-bit	48	96	35,664	3 (192-bit)
SPHINCS+ SHA-256 256-bit	64	128	49,856	5 (256-bit)
RSA-2048	256	256	256	
ECC 256-bit	64	32	256	

Figure 2. SPHINCS+ Dilithium, rainbow and falcon characteristics

WOTS uses small key and signature sizes. It is considered quantum-resistant. 32x256 bits of random private keys are generated. This is then repeated several times, depending on the parameter (w). If w=8, private keys up to (2w) are hashed. This creates 32x256-bit public keys. Signature creation occurs by taking eight bits at a time, then subtracting the 8-bit binary number int(n) from 256, and hashing the private key 256-n times. The signature consists of 32 hashes obtained from random private keys. Signature verification occurs as follows: the recipient analyses the signature hash (using 8 bits at a time and extracting an 8-bit integer n). The signature is then deduced from the signature. This method is as follows.

Initially, 32 256-bit random numbers are generated. These 32 values are the private key. Each of these values is then hashed 256 times. These 32 values will be the public key. The message is then taken and hashed using SHA-256. The result is 32 8-bit values (N1, N2...N32). The signature takes each 8-bit value in the message hash and then hashes it 256-N times (where N is the value of the 8-bit value). To verify the signature, the message is taken and hashed using SHA-256, then each 8-bit value is taken. Then it is hashed into the 8-bit signature value as many times as specified in the hash value of the message (N1, N2...). The result of each operation should be equal to the public key value. This circuit is shown below in Figure 1.

According to Buchanan, SPHINCS+ did not make it to the finals of the NIST competition due to the fact that, despite the short public and private keys, it has a longer signature than Dilithium, Rainbox, and Falcon [21]. As evidence, they cite a table that shows the comparative characteristics of SPHINCS +, Dilithium, Rainbow and Falcon, this table is shown in Figure 2.

With the same security level, SPHINCS+ has a signature size of 49 kilobytes compared to 4 kilobytes for Dilithium and 1 kilobyte for Falcon.

4. DISCUSSION

Following the emergence of powerful quantum computers, many researchers in the cryptography area spoke about the need to revise information security algorithms. Post-quantum cryptographic algorithms were analysed by Kravchenko and Cherkesova [14]. In their work, the authors explained the “quantum superiority” concept and, as an example, described the condition under which a quantum computer is able to hack the RSA algorithm, which is a modern standard.

The current research provides additional details and insights compared to previous studies in the field of post-quantum cryptography. Specifically, the current study offers a more detailed analysis of the properties and cryptographic strength of various systems. For example, the study highlights that with an adequate key length, the symmetric AES encryption algorithm becomes more resistant to attacks, emphasizing the importance of its architecture. The advantages and disadvantages of different systems are explored, such as the limited number of signatures in hash functions, the practical difficulties with the McEliece code addressed by the McEliece-Niederreiter system and the subsequent NTRU encryption system, and the trade-offs in computational speed and key length in multidimensional quadratic systems and braid groups. The study also analyzes the encryption algorithms that made it to the finals of the NIST competition, comparing their resistance to quantum attacks and highlighting the strengths and weaknesses of each. The most promising algorithms identified in the study include WOTS+, Dilithium, and SABER. The research concludes by emphasizing the need for further development, testing, and thorough stability assessment of new algorithms in the field of post-quantum cryptography.

Key management complexity and suitability of elliptic curve systems: exploring vulnerabilities, benefits, and performance. Key management is quite complex; the algorithm is vulnerable to attacks through third-party channels [22, 23]. With regard to elliptic curves, the researchers [24] believe that these systems are suitable for public key encryption and key exchange. Benefits were identified for blind signature and undeniable signature schemes. The algorithm also has a small key size. However, the system is slow and unsuitable for devices with limited resources. This system arose relatively recently and is therefore little studied.

Examining cryptographic systems: exploring advantages, disadvantages, and development trends. The advantages of error correction codes include high speed of encryption and decryption, the information protection degree increases significantly with increasing key length [25]. The main disadvantage is the fact that in order to increase the algorithm security, it is necessary to increase the public key size many times over. Cryptography on lattices, as noted by the authors, has an acceptable performance. The features of the hash functions application are described and an overview of the development trend of post-quantum algorithms is provided. Unlike the work of the researchers, this article covers existing cryptographic systems in more detail.

In the work of Fedorov, more attention is paid to the classical system of McEliece, SABER, KyBER and NTRU, which reached the final of the second round of NIST [26]. The mechanisms of the algorithms action are described in more detail and the degree of their reliability is evaluated. Improved algorithms based on the McEliece system, for example, a double public key encryption system, are considered. Such system is more efficient and safer. The proof of the algorithm stability to ROM and QROM attacks is provided. The KyBER structure description is provided, however, not as detailed as in this article. The author points out that the SABER system was designed to be easy and flexible to use. To do this, the same key components are used in the module structure at different security levels [27]. SABER was also compared with NTRU and LWE schemes.

Exploring multidimensional public key cryptography: assessing security, performance, and advantages over discrete logarithms and integer factorization. The features analysis of multidimensional public key cryptography is conducted by Zakharova and Makarova [28]. The study noted that the security of these algorithms is based on the hypothesis that solving systems of quadratic polynomials is an NP-complete problem. The disadvantages of public-key cryptosystems based on discrete logarithms and integer factorisation are considered by the authors to be low calculation speed and unreliability [29]. As an alternative, multidimensional quadratic cryptosystems are suggested. Despite the requirement for a big length of public keys, the speed of these systems is much higher. As an example, researchers provide a cryptosystem based on hidden field equations (HFE) and substantiate their security.

The concept of cryptographic strength and the essence of algorithms based on learning with errors are extensively discussed in the study by Zakharova and Makhotin [30]. The

authors provide a definition of stable algorithms and highlight that establishing absolute resistance to attacks is often impractical, but it is possible to calculate the probability of hacking. These algorithms are categorized into three types based on their level of resistance: computational, information-theoretic, and provable stability. The study also presents methods for solving cryptosystems based on learning with errors.

In the research conducted by Razumov et al. [31], an in-depth study of the NTRUEncrypt cryptosystem and its modification is presented. Unlike the current article, this study includes an analysis of the algorithmic complexity of NTRUEncrypt and its optimized version. The researchers developed software to implement both systems and demonstrated that the modified version performs faster than the standard version while optimizing the use of internal memory. The cryptographic strength of the system was confirmed, and performance comparisons with RSA showed significant speed improvements. The standard NTRUEncrypt outperformed RSA by 80% in message encryption speed, and the modified version performed even better with an 84% improvement. In decryption, both NTRUEncrypt systems achieved a 99% higher information processing speed than RSA, with the modified version being 17% faster than the standard one.

Bhattacharyya and Chakrabarti [32] emphasize the importance of consistency and simplicity in the encryption and decryption algorithms of an effective cryptosystem. They review the historical development of cryptography, discuss classical systems and their drawbacks, and focus on signature schemes based on hashing. The authors [33] also delve into the differences between quantum and post-quantum cryptography. Ott and Peikert explore the challenge of replacing widely used systems like RSA, ECDSA, ECDH, and DSA with alternative post-quantum cryptography. They point out that NIST's efforts alone are insufficient to ensure a smooth transition to post-quantum cryptography, given the diverse range of computer systems in existence. The work presents an action plan for disseminating new NIST standards and highlights the greater memory and computational requirements of post-quantum cryptography systems due to their larger key sizes and increased algorithmic complexity. The authors [34-36] analyze various factors influencing the transition process and propose solutions to expedite it, including conducting studies to evaluate algorithm replacements in different conditions, addressing political and social aspects of the transition, and exploring the application of these processes to new branches of cryptography, such as confidential computing protocols, blockchain, and homomorphic encryption.

Another review conducted by Di Chiano et al. [37] focuses on the NIST third-round finalists and alternative candidates for digital signatures. The study compares algorithms such as CRYSTALS-DILITHIUM, SPHINCS+, Picnic, Falcon, Rainbow, and GeMSS. Similarly, the work by W. Beullens provides a simplified description of the unbalanced UOV scheme and its Rainbow modification [38]. The authors experimentally investigate two types of attacks: rectangular MinRank attack and intersection attack, which are shown to be more powerful than existing attacks [39]. The findings indicate that UOV and Rainbow are not NIST compliant, as the new attacks significantly reduce the cost of key recovery. It is worth noting that this work lacks experimental evaluations of post-quantum cryptography algorithms and does not cover the functioning of cryptosystems such as NTRUEncrypt and AES. Nevertheless, the article offers a comprehensive overview of the various technologies in the emerging field of post-quantum cryptography. The analysis of various cryptographic systems in the current study provides valuable insights that can inform the development of new post-quantum cryptographic algorithms or the refinement of existing ones. The study offers a detailed understanding of the advantages and disadvantages of different systems, allowing researchers to identify areas for improvement and optimization. For example, the study highlights the limitations of traditional public-key cryptosystems based on discrete logarithms and integer factorization, such as low calculation speed and unreliability.

In contrast, multidimensional quadratic cryptosystems are suggested as an alternative with higher speed and security, despite the requirement for larger key sizes [40, 41]. This insight can guide researchers in the development of new algorithms that leverage the strengths of multidimensional quadratic systems while addressing their limitations, such as exploring methods to reduce key size without compromising security. Furthermore, the study provides a comprehensive analysis of the encryption algorithms that made it to the finals of the NIST competition, comparing their resistance to quantum attacks and highlighting their strengths and weaknesses. This analysis can inform researchers in the refinement and optimization of these algorithms to enhance their security and efficiency.

To further advance the field of post-quantum cryptography, several potential areas for future research and challenges need to be addressed. Continued cryptanalysis and security evaluation of post-quantum cryptographic algorithms are essential to ensure their resilience against both classical and quantum attacks. Researchers should explore novel attack techniques and evaluate the resistance of algorithms in various scenarios. Additionally, further research is needed to develop efficient and reliable methods for assessing the security of post-quantum cryptographic schemes, including formal security proofs and analysis tools.

Also, many post-quantum cryptographic algorithms have larger key sizes and higher computational requirements compared to traditional schemes. Future research should focus on improving the scalability and efficiency of these algorithms to make them more practical for real-world applications. This includes exploring optimization techniques, hardware acceleration, and parallelization strategies to enhance the performance of post-quantum cryptographic operations, enabling their seamless integration into existing systems and networks.

5. CONCLUSIONS

The analysis conducted in this study yielded several key insights and advances in the field of post-quantum cryptography. First, the study identified the main disadvantages of different cryptographic approaches, such as the limited number of signatures in hash functions and the large key size in the McEliece code. This led to the development of improved systems like the "McEliece-Niederreiter system" and the NTRU encryption system, which addressed these limitations and reduced the number of keys required.

The study also compared and evaluated encryption algorithms that reached the finals of the NIST competition. It identified KyBER and Dilithium schemes as more resistant to

quantum attacks compared to modular lattices. The SABER algorithm was recognized for its high reliability and provision of three levels of security. Dilithium stood out among the algorithms for having the smallest key size. The study also highlighted the limitations of certain systems, such as the complex implementation requirements of the Falcon lattice cryptography algorithm and the large digital signature size of the Rainbow system.

Based on the analysis, the study identified the most promising algorithms for further exploration and advancement in post-quantum cryptography, including WOTS+, Dilithium, and SABER.In the future, the development and testing of new algorithms for post-quantum cryptography will continue. In future studies, it is necessary to continue the study of new systems, conducting thorough tests of their stability.

The practical implications of the findings in the context of post-quantum cryptography are significant. The study highlights various cryptographic systems and algorithms that show promise in resisting quantum attacks, which is crucial as quantum computers become more powerful and pose a threat to traditional cryptographic schemes. By identifying the advantages and disadvantages of these systems, the study provides valuable insights for practitioners and researchers in choosing appropriate post-quantum cryptographic algorithms for real-world applications.

One practical implication is the identification of specific algorithms that exhibit strong resistance to quantum attacks, such as KyBER, Dilithium, and SABER. These algorithms can be considered as potential replacements for existing cryptographic systems vulnerable to quantum attacks, such as RSA or ECC. The findings provide guidance for organizations and individuals seeking to adopt more secure post-quantum cryptographic solutions.

The study also highlights the need for further research and development in post-quantum cryptography. The identified areas of improvement, such as optimizing key sizes, reducing computational complexity, and addressing practical implementation challenges, provide directions for future studies. Continued research efforts in these areas will contribute to the advancement and practical application of post-quantum cryptographic algorithms.

REFERENCES

[1] Bernstein, D.J., Buchmann, J., Dahmen, E. (2009). Post-Quantum Cryptography. Springer, Heidelberg.

[2] Lange, T. (2008). Post-quantum Cryptography. Eindhoven University of Technology, Eindhoven.

[3] Zhatkin, A.V. (2013). Application of quadratic equations systems of many variables in asymmetric cryptography. Information Technology Security, 20(1): 98-99.

[4] Basu, K., Soni, D., Nabeel, M., Karri, R. (2019). NIST post-quantum cryptography – A hardware evaluation study. Cryptology ePrint Archive, 47: 1-16.

[5] Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms. (2016). https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms, accessed on Mar. 15, 2023.

[6] Post-quantum cryptography: Current state and quantum mitigation. (2021). https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation, accessed on Mar. 15, 2023.

[7] Barker, W., Polk, W., Souppaya, M. (2021). Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms. NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.04282021

[8] Nguyen, D.T., Dang, V.B., Gaj, K. (2019). A high-level synthesis approach to the software/hardware codesign of NTT-based post-quantum cryptography algorithms. In: 2019 International Conference on Field-Programmable Technology (ICFPT), Tianjin, China, pp. 371-374. https://doi.org/10.1109/ICFPT47387.2019.00070

[9] Kumar, M. (2022). Post-quantum cryptography algorithms standardization and performance analysis. Array, 15: 100242. https://doi.org/10.1016/j.array.2022.100242

[10] Shor, P.W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Review, 41(2): 303-332. https://doi.org/10.1137/S0036144598347011

[11] Bernstein, D.J., Lange, T. (2017). Post-quantum cryptography – Dealing with the fallout of physics success. Cryptology ePrint Archive, 314: 1-20.

[12] Grebnev, S., Klyucharov, P., Koreneva, A., Koshelev, D., Taraskin, O., Tulebayev, A. (2021). A protocol for deriving a shared key based on the isogeny apparatus of supersingular elliptic curves. Moscow, RusCrypto'2021, pp. 99-104. https://test.ruscrypto.ru/accociation/archive/rc2021.html

[13] You, W., Chen, X. (2018). Provably secure integration cryptosystem on non-commutative group. Cryptology ePrint Archive, 512: 1-12.

[14] Kravchenko, V.O., Cherkesova, L.V. (2019). Review of post-quantum cryptographic algorithms. Alley of Science, 3(1): 966-974. https://alley-science.ru/domains_data/files/10January2019/OBZOR%20POSTKVANTOVYH%20KRIPTOGRAFIChESKIH%20ALGORITMOV.pdf

[15] Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T. (2021). CRYSTALS-Kyber algorithm specifications and supporting documentation. https://pq-crystals.org/kyber/data/kyber-specification.pdf, accessed on Mar. 16, 2023

[16] SABER: LWR-based KEM. (2019). https://www.esat.kuleuven.be/cosic/pqcrypto/SABER/performance.html, accessed on Mar. 16, 2023.

[17] CRYSTALS cryptographic suite for algebraic lattices. (2021). https://pq-crystals.org/dilithium/index.shtml, accessed on Mar. 16, 2023.

[18] Falcon: Fast-Fourier Lattice-based compact signatures over NTRU. (2022). https://falcon-sign.info, accessed on Mar. 16, 2023.

[19] Rainbow signature. One of the three NIST Post-Quantum signature finalists. (2022). https://www.pqcrainbow.org, accessed on Mar. 20, 2023.

[20] Supersingular isogeny-based cryptography. (2022). https://qapp.tech/help/supersingular-isogeny-based, accessed on Mar. 20, 2023.

[21] Buchanan, B. (2021). SPHINCS+: A hash-based quantum robust method. https://medium.com/asecuritysite-when-bob-met-alice/sphincs-a-hash-based-quantum-robust-method-bbe8495efb6d.

[22] Aizstrauta, D., Ginters, E. (2015). Integrated acceptance and sustainability assessment model transformations into executable system dynamics model. Procedia Computer Science, 77: 92-97. https://doi.org/10.1016/j.procs.2015.12.364
[23] Ginters, E., Barkane, Z., Vincent, H. (2010). System dynamics use for technologies assessment. In: 22th European Modeling and Simulation Symposium, EMSS 2010, pp. 357-361.
[24] Dey, K., Debnath, S.K., Stănică, P., Srivastava, V. (2022). A post-quantum signcryption scheme using isogeny-based cryptography. Journal of Information Security and Applications, 69: 103280. https://doi.org/10.1016/j.jisa.2022.103280
[25] Aviv, I., Gafni, R., Sherman, S., Aviv, B., Sterkin, A., Bega, E. (2023). Infrastructure from code: The next generation of cloud lifecycle automation. IEEE Software, 40(1): 42-49. https://doi.org/10.1109/MS.2022.3209958
[26] Fedorov, S.K. (2021). Analysis of post-quantum cryptographic algorithms. Alley of Science, 1(6): 28-32.
[27] Nussibaliyeva, A., Carbone, G., Mussina, A., Balbayev, G. (2019). Study of artificial vision on the adaptive filter basis for implementation in robotic systems. Mechanisms and Machine Science, 73: 2319-2328. https://doi.org/10.1007/978-3-030-20131-9_229
[28] Zakharova, Y.F., Makarova, S.E. (2020). Features of cryptographic algorithms based on multidimensional quadratic systems. In: Proceedings of the Fourteenth International Conference MCM-2020, Penza: PSU Publishing House, pp. 193-198. https://dep_vipm.pnzgu.ru/files/dep_vipm.pnzgu.ru/konference/mkm_2021.pdf
[29] Shebanin, V., Atamanyuk, I., Kondratenko, Y., Volosyuk, Y. (2017). Canonical mathematical model and information technology for cardio-vascular diseases diagnostics. In: 2017 14th International Conference the Experience of Designing and Application of CAD Systems in Microelectronics, CADSM 2017 – Proceedings, Lviv - Polyana: Institute of Electrical and Electronics Engineers, pp. 438-440. https://doi.org/10.1109/CADSM.2017.7916170
[30] Zakharova, Y.F., Makhotin, A.N. (2020). Analysis of the cryptographic strength of an algorithm based on learning with errors. In: Proceedings of the Fourteenth International Conference MCM-2020, Penza: PSU Publishing House, pp. 176-179. https://dep_vipm.pnzgu.ru/files/dep_vipm.pnzgu.ru/konference/mkm_2020.pdf
[31] Razumov, P.V., Smirnov, I.A., Pilipenko, I.A., Seleva, A.V., Cherkesova, L.V. (2019). Comparative analysis of the modified post-quantum cryptographic system NTRUENcrypt and the generally accepted cryptosystem RSA. Advanced Engineering Research, 19(2): 185-194. http://dx.doi.org/10.23947/1992-5980-2019-19-2-185-194
[32] Bhattacharyya, S., Chakrabarti, A. (2022). Post-quantum cryptography: A brief survey of classical cryptosystems, their fallacy and the advent of post-quantum cryptography with the deep insight into hashed based signature scheme. In: Sharma, N., Chakrabarti, A., Balas, V.E., Bruckstein, A.M. (eds) Data Management, Analytics and Innovation. Lecture Notes on Data Engineering and Communications Technologies, vol 71. Springer, Singapore. https://doi.org/10.1007/978-981-16-2937-2_24
[33] Ott, D., Peikert, C. (2019). Identifying research challenges in post quantum cryptography migration and cryptographic agility. Washington, Computing Community Consortium. arXiv preprint arXiv:1909.07353. https://doi.org/10.48550/arXiv.1909.07353
[34] Rika, H., Aviv, I., Weitzfeld, R. (2022). Unleashing the Potentials of quantum probability theory for customer experience analytics. Big Data and Cognitive Computing, 6(4): 135. https://doi.org/10.3390/bdcc6040135
[35] Mukasheva, A., Iliev, T., Balbayev, G. (2020). Development of the information system based on bigdata technology to support endocrinologist-doctors. In: 2020 7th International Conference on Energy Efficiency and Agricultural Engineering, EE and AE 2020 – Proceedings, Ruse: Institute of Electrical and Electronics Engineers, article number 9278971. https://doi.org/10.1109/EEAE49144.2020.9278971
[36] Ginters, E. (2020). New trends towards digital technology sustainability assessment. In: Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020, London: Institute of Electrical and Electronics Engineers, pp. 184-189.
[37] Di Chiano, N., Longo, R., Meneghetti, A., Santilli, G. (2021). A survey on NIST PQ signatures. ArXiv, https://doi.org/10.48550/arXiv.2107.11082
[38] Beullens, W. (2021). Improved cryptanalysis of UOV and rainbow. In: Canteaut, A., Standaert, FX. (eds) Advances in Cryptology – EUROCRYPT 2021. EUROCRYPT 2021. Lecture Notes in Computer Science, vol 12696. Springer, Cham. https://doi.org/10.1007/978-3-030-77870-5_13
[39] Mussina, A., Ceccarelli, M., Balbayev, G. (2018). Neurorobotic investigation into the control of artificial eye movements. Mechanisms and Machine Science, 57: 211-221.
[40] Barlybayev, A., Sabyrov, T., Sharipbay, A., Omarbekova, A. (2017). Data base processing programs with using extended base semantic hypergraph. Advances in Intelligent Systems and Computing, 569: 28-37. https://doi.org/10.1007/978-3-319-56535-4_3
[41] Aviv, I. (2022). The Distributed Ledger Technology as Development Platform for Distributed Information Systems. In: Sharma, H., Vyas, V.K., Pandey, R.K., Prasad, M. (eds) Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021). ICIVC 2021. Proceedings in Adaptation, Learning and Optimization, vol 15, Springer, Cham. https://doi.org/10.1007/978-3-030-97196-0_28