Prospective Areas of Research in the Development of Post-Quantum Cryptography

Vasyl Sheketa[a], Svitlana Chupakhina[b], Mariya Leshchenko[c], Larysa Tymchuk[d], and Kostiantyn Chub[e]

[a] *National Technical University of Oil and Gas, 15 Karpatska str., Ivano-Frankivsk, 76068, Ukraine*
[b] *Vasyl Stefanyk Precarpathian National University, 57 Shevchenko str., Ivano-Frankivsk, 76000, Ukraine*
[c] *Institute of Information Technologies and Learning, 9 M. Berlynskoho str., Kyiv, 04060, Ukraine*
[d] *Center Ivan Chernyakhovsky National University of Defense, 28 Povitroflotskiy ave., Kyiv, 03049, Ukraine*
[e] *Poltava V. G. Korolenko National Pedagogical University, 2 Ostrogradskogo str., Poltava, 36000, Ukraine*

Abstract

Critical questions about the need to prepare both international and domestic information infrastructure for the emergence of post-quantum mechanisms of cryptanalysis of critical information on the corresponding computing systems are considered. This requires taking into account the experience of the international community in developing and testing a series of post-quantum standards in the field of cryptographic protection of key information. At the same time, it is very important to take into account the following aspects that the Ukrainian standardized system insists on the use of time-tested encryption mechanisms: when the long-term studies of connectivity will not be detected in this mechanism. Except for the NTRU scheme based on McAlice's theory and other encoding schemes, post-quantum cryptography has a history of up to 5 years. To some extent, NIST has been rushing to implement post-quantum encryption technology (for example, a memorandum issued by the U.S. National Security Agency in 2015 provided U.S. developers with encryption to protect important information that has not yet been included in its products. Introduction of information encryption technology. Algorithms based on elliptical curve operations avoid the implementation of these algorithms to save resources with the proposed transition to post-quantum algorithms), which forces us to carefully test new standards developed in the procedures of the organization to avoid using standards for the generation of pseudo-random numbers. Many researchers objected, but pointed to obvious loopholes, so the standard needs to be revoked. Proceeding from this it is obvious that the moment of transition to post-quantum cryptography will require fundamental reorganization of the whole basic infrastructure of information protection, all methods of information protection using asymmetric cryptographic algorithms, especially the infrastructure of an authentication center. Taking into account the cost of these events, one should make a cautious decision about the transition to post-quantum cryptography based on accurate forecasts of the development of post-quantum computing system functions. Based on the above-mentioned research, we can confidently say that the global IT community is actively preparing for significant changes with the advent of the post-quantum era.

Keywords

Algorithms, cryptography, post-quantum computing system, encoding schemes, critical data, software applications.

1. Introduction

In the era of rapid information development, active global research in the field of post-quantum computing systems and computation is being carried out all over the world. Thus, the creation of a supercomputing system that will use the post-quantum model in the processing of computational

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine

EMAIL: vasylsheketa@gmail.com (A.1); cvitlana2706@gmail.com (B.2); darlyngpetra18@gmail.com (C.3); lucky.clio2017@gmail.com (D.4); kchub2017@gmail.com (E.5)
ORCID: 0000-0002-1318-4895 (A.1); 0000-0002-3058-6650 (B.2); 0000-0003-4121-565X (C.3); 0000-0003-4678-2362 (D.4); 0000-0001-6325-6466 (E.5)

algorithms (post-quantum computing system), which in turn can create negative consequences for the decryption of a number of cryptographic mechanisms of systems for the protection of important information data. In the modern understanding of post-quantum computing technology, it is assumed to create and manage complex post-quantum computing systems, which are created from a significant volume of objects, at the level of separately created components such as individual atoms, ions, photons, electrons, molecules, etc., which will be used for the protection of important data. This scientific approach makes it possible to use such unusual phenomena as post-quantum superposition, which is the ability of post-quantum computing systems to be in all possible known states at once. And such post-quantum multi-coordination of objects is manifested by strong interrelationships between different parameters of specially designed post-quantum computing systems. Therefore, the modern period of information development of post-quantum technologies is often called the "second quantum revolution." In particular, on the created post-quantum computing system there will be an opportunity to implement algorithms of factorization and discrete logarithmize in arbitrary groups with polynomial complexity (Shore method), and the essence of his studies and the proposed hypothesis (which made a lot of noise in the world), that it is the solution of the algorithmically complex problem of number factorization is based on numerous modern algorithms and cryptography systems. The algorithm found by Peter Shore in 1994 allows to solve this problem in polynomial time (polynomial number of gates) and on polynomial number of qubits, while classical algorithms solve it in super polynomial (sub-exponential) time. This means that once a post-quantum computer with a sufficient number of qubits is created, all modern cryptography will be compromised. It will be compromised immediately since any information hidden using this approach can be obtained by anyone who has access to such a post-quantum computer [1, 3, 4, 5, 7].

The algorithm, discovered by Peter Shore in 1994, solves this problem in polynomial time (hence, the number of valves is polynomial) and on polynomial qubits, while the classical algorithm solves it in hyper polynomial time (sub-exponential). This means that once a post-quantum computing system with sufficient qubits is created, all modern encryption technologies will be at risk. These cyber defense systems will be tied up since any information hidden by these methods can be obtained by any user who has the right to use this post-quantum computer [2, 6, 8, 10, 11].

The stability of the algorithm is based on the assumption of the complexity of solving the above problems, including RSA (Rivest-Shamir-Adleman) Diffie-Hellman scheme, ECDSA (Elliptic Curve Digital Signature Algorithm) the digital signature, and various standards. At the same time, the currently known post-quantum algorithms for the analysis of hash functions and block cipher (the F. Ambainis collision search method and the original M. Grover image search method) still have exponential complexity, although their complexity is less than classical Fig. 1.

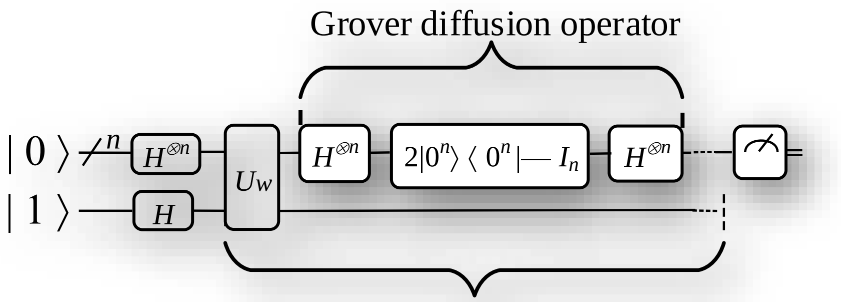

Figure 1: Grover Algorithm presentation

The meaning of the Grover algorithm is to "increase the target state amplitude" by reducing the amplitude of all other classes. Geometrically speaking, the Grover algorithm consists of a precise rotation of the current state vector of a post-quantum computer in the direction of the target state (movement along the shortest path ensures optimality of the Grover algorithm) [9, 12, 15, 16].

Each iteration step gives a rotation of 2α, where the angle between $I_{\tilde{o}}$ and I_{xtar} is defined as $\pi/2 - \alpha$. Further prolongation of iterative calculations of operator G will give a continuation of circumvention of the circle in the real plane generated by these vectors.

The stability of the algorithm processing is based in the proposed cases on the assumption of the complexity of solving the above problems, including RSA, Diffie-Hellman scheme, digital signature

ECDSA, and various other approaches and standards. At the same time, since the currently known post-quantum algorithms for the analysis of hash functions and block cipher (the Amboina's collision search method and the original Grover image search method) still have a significant exponential complexity, although their complexity is less than the classical approaches [13, 17, 18].

At the same time, experts assess differently the prospects of creating a working sample of post-quantum computing systems with capabilities sufficient to solve practical problems of cryptanalysis. The estimated time for the creation of such a post-quantum computer is from 7 to 25 years. Some especially pessimistic scientists believe that physical obstacles to the creation of post-quantum computing systems cannot be overcome, where the main feature of the functioning of post-quantum computing systems is based on the number of qubit-base blocks in it [14, 20, 21, 24].

The main feature of the post-quantum computing system functions is the number of qubit-base blocks. Thus, the condition of the cryptanalysis task is set as the initial state of the qubit system, from which the post-quantum computing system is built, to perform a number of transformations defined by the post-quantum algorithm. As a result of the final measurement of the qubit system state, an optimal solution to the cryptanalysis problem can be found. However, in this case, in the process of calculating and accurately measuring the state of qubits, it is necessary to overcome the physical degradation of qubits, so there are great engineering and physical difficulties [22, 27, 28, 30].

For a successful solution of the cryptographic analysis task, it is necessary to perform factorization of number N, which is the secret key of the RSA cryptographic system, using the Shore method it is necessary to use approximately 4/3logN cubits and a polynomial number of computational operations. At present, the cryptographic protection standards used in business models, which regulate the application of RSA software and data protection system, recommend the use of a numerical sequence with a length of at least 2048 bits, so to perform a successful cryptographic analysis of such a sequence will require a post-quantum computing system with a power of more than 2736 cubits [19, 23, 26].

2. Prospective Development of Crypto Mechanisms on Post-Quantum Computing Systems

At the moment there are several commercial prototypes of post-quantum computing systems, including those developed by such companies as IBM and D-Wave. These post-quantum computing systems are designed to solve global optimization problems and are not suitable for detailed sequence cryptanalysis. At the same time, it should be noted that at the beginning of this year one of the firms (IBM) which is actively engaged in the development of post-quantum computing systems presented to the IT community a "personal" 20-cubit post-quantum computer. It was mounted in a case with a total volume of about 9m3. D-Wave post-quantum computing systems, which are used, including by Google and NASA, have, according to the manufacturer, a productive capacity of up to 1,152 cubic meters. These post-quantum computing systems are grouped into several clusters, but the nature of their internal topological relationships allows us to assert with some certainty that they have significant limitations that these devices are built for post-quantum computing models [25, 28, 29].

The areas of synthesis of cryptographic computational schemes resistant to cryptanalysis using both classical approaches and post-quantum computing have received the general name "post-quantum cryptography." The first international conference dedicated to the problems of PQCrypto cryptanalysis was held in 2006 and has since become an annual conference.

In today's realities, research conducted by the international cryptographic community in the field of improvement and synthesis of post-quantum cryptographic algorithms has intensified thanks to the efforts of the National Institute of Standards and Technology (NIST), which organized a forum for submitting proposals for standardization and discussion of post-quantum cryptographic computational schemes. (It should also be noted that this event is not a contest of ideas, as it does not involve the nomination and awarding of the winner, but only the identification of a set of optimal synthesis solutions for further practical research with the prospect of standardization.

During this forum, more than 179 descriptions of cryptographic mechanisms were offered, which were developed by different teams of authors from different countries, including Ukraine. These proposals were the basis for symposia, where the analysis of these cryptographic mechanisms was summarized. Thus, the cryptographic mechanisms submitted for analysis and discussion have the following implementation: encryption, digital signature, key encapsulation, and shared key generation. And taking into account the experience of NIST's previous studies on the creation of block cipher (AES) and hash functions (SHA-3), a set of research works on cryptanalysis of the proposed mechanisms and creation of new standards and proposals based on them may take from 4 to 7 years.

Thus, among the developments of complex cybersecurity systems, NIST systems are used by thousands of commercial and non-profit organizations around the world to minimize cybersecurity risks for critical infrastructure. Where there were formalized requirements for computing system endurance, both formal (strictly proved based on the assumption of the complexity of solutions to a certain task) and practical.

2.1. Asymmetric Encryption Systems for Infrastructure Critical Data

For asymmetric encryption systems with infrastructure critical data (listed from minor requirements to strong ones):

- Resistance of cryptanalysis to the threat of text cipher definition against cyberattack based on selected open text (Indistinguishability Against Chosen Plaintext Attack, IND-CPA).
- Cryptanalysis resistance to the threat of ciphertext determination against cyberattack and based on selected ciphertext (Indistinguishability Against Chosen Plaintext Attack, IND-CCA).
- Cryptanalysis resistance to the threat of ciphertext determination against cyberattack based on (non-adaptive) selected plaintext (Indistinguishability Against (non-adaptive) Chosen Plaintext Attack, IND-CPA1).
- Resistance of cryptanalysis to the threat of text cipher determination against cyberattack based on (incorrectly) selected ciphertext (Indistinguishability Against (non-adaptive) Chosen Plaintext Attack, IND-CCA1).
- Resistance of cryptanalysis to the threat of distinguishing text ciphers from an attack based on adaptively chosen plaintext (Indistinguishability Against Adaptive Chosen Plaintext Attack, IND-CPA2).
- Cryptanalysis vulnerability to text cipher differentiation against an adaptively matched plaintext attack (Indistinguishability Against Adaptive Chosen Plaintext Attack, IND-CCA2).

2.2. Features of using Electronic Signature Mechanisms

To select effective electronic signature schemes, developers of computer systems for processing critical information should pay special attention to the following levels of cybersecurity in order from weak to strongest:

- Strong resistance of cryptographic protection to active attacks based on selected messages SUF-CMA (Strong Enforceability under Chosen Message Attacks).
- Strongest of cryptographic protection against active based on existential forgery using selected messages EUF-CMA (Eventually Enforceability under Chosen Message Attacks).

2.3. Practical Resistance of Cryptographic Signature Crypto-Mechanisms to Cryptanalysis

Determining the practical resistance of crypto-mechanisms of digital signature to the specified conditions from the company NIST one of the developers of the world crypto standards provides five different levels of resistance Table 1.

Table 1.

Five levels of crypto mechanism resistance

Level	Practical crypto mechanism
I	Equivalent to finding a 128-bit block cipher key
II	Equivalent search for 256-bit hash function collisions
III	Equivalent to finding a 256-bit block cipher key
IV	Equivalent search for 384-bit hash function collisions
V	Equivalent to finding a 384-bit block cipher key

Thus, for each proposal, it was necessary to provide formal and practical proof of the firmness of cryptographic mechanisms of digital signatures against cryptanalysis, as well as to propose certain sets of parameters for different levels of cryptographic firmness of the proposed schemes.

To solve this rather complicated and at the same time practical task, 69 proposals were submitted, 27 of which were unacceptable because their crypto-mechanisms were weak to cryptanalysis.

At the same time, the practical analysis of cryptographic mechanisms of the submitted proposals did not do without curiosities, for example, the proposal submitted by D. Berstein with the co-authors, namely, for the organization of the fifth cryptographic level of critical data protection, they proposed to use RSA cryptographic mechanism with the exponential size of keys larger than 1 Gbyte.

Let's give an example of the basic synthesis of solutions for cryptographic protection of critical data, which apply to compete to NIST groups of developers of crypto-mechanisms:

- Using integer lattice theory for crypto-mechanisms.
- Using error correction codes for crypto-mechanisms.
- Using for crypto-mechanisms multi-members from many variables.
- Use of cryptographic hash functions for crypto-mechanisms.
- Use of curves on super-singular elliptical curves for crypto-mechanisms; use of hash functions for crypto-mechanisms.
- Highly specialized tasks for crypto-mechanisms (Search Problem or Braid Group operation, A. Keli octonion algebra, P. Chebyshev polynomials, etc.).

Ring learning with errors (RLWE) is a computational problem-solving solution underlying new cryptographic algorithms such as NewHope to prevent quantum computing systems from performing cryptanalysis and provide a foundation for strong homomorphic encryption. Thus, cryptographic mechanisms with public keys are based on the construction of mathematical tasks. If there is a sufficiently large quantum computing system, it can successfully solve some of these crypto analysis problems, which are now used in cryptography, so that crypto researchers will protect critical information and need to look for persistent problems. The use of homomorphic encryption is a form of encryption that provides mathematical computations with encrypted critical text, for example, we can use arithmetic operations with certain values stored in an encrypted data warehouse.

RLWE is more appropriate to be called ring error training, it's just a big Learning With Errors (LWE) problem, which specializes in multi-member rings over end fields. Because of the complexity of solving RLWE problems even on quantum computers, RLWE-based encryption technology may become the basis of public-key cryptography in the future, as well as problems of integer factorization and discrete logarithm have become public secrets since the early 1980s. The basis of key cryptography is the same. An important feature of cryptography with cyclic error learning is that the RLWE solution can be used to solve the Problem of Shortest Vectors (SVP) of NP-hard lattice.

Crypto-mechanisms based on lattice theory (see an example of the corresponding mechanisms for generating a common key in Fig. 1) is based on a number of complex problems, including the NP problem of searching for the shortest vector (SVP) and searching for the nearest vector (SNP); the problem of error learning (LWE; RLWE) and the problem of searching for the smallest integer solution of the system of linear algebraic equations (SIS).

Example 1 of a generalized crypto mechanism Ring learning with errors (**RLWE**)

- $R_q = Z_q[X]/(X^n + 1)$
- ξ is error distribution (usually Gaussian)
- sequence crypto secret key $s \in R_q$

- public-key cryptographic sequence $as + e, a \in_R R_q, e$ errors
- Diffie-Hellman cryptographic algorithm: $as + e, b\acute{s} + \acute{a}$ the common key of the $v = as\acute{s} + \acute{e}s \approx bs\acute{s} + e\acute{s}; s, \acute{s}, e, \acute{e} -$ is small relative to some norm

Among the developers of crypto-mechanisms for digital signatures, which were preliminary analyzed and positively evaluated by NIST, according to their initial requirements, which were based on lattice theory: Compact LWE; CRYSTALS-KYBER; Ding Key Exchange; EMBLEM and R.EMBLEM; FrodoKEM; HILA$_5$; KINDI; LAS; LIMA; Lizard; LOTUS; NewHORE; qTESLA.

For example, since the late 1970s, the problem of coding theory has been considered in cryptography. Although the McAlice scheme has been cracked by cryptographers in many individual cases, it may remain stable as long as the Goppa code is used.

Example 2 of the R. McEliece cryptography mechanism

- G is generating a double linear (n, k) matrix—code that corrects k errors
- $S \in_R GL(k, 2)$ is random matrix
- P is supplied $n \times n$ matrix
- $G' = SGP$; (G', t) is a public key, (S, G, P) is a secret key
- Encoded: $c = E(m) = mG' + e, e$ is random weight vector t
- Decryption: $c' = c * P^{-1}; m'$ is code decoding result $G; m = m' * S^{-1}$

Participants who accepted NIST's proposal include the development and analysis of crypto mechanics, which are based on coding theory: BIG QUAKE, BIKE, Classic McEliece, Edon-K, HQC, LAKE, LEDApkc, Lepton, LOCKER, McNie, NTS-KEM, QC-MDPC KEM, Ramstake, RLCE-KEM, RQC, RaCoSS, RankSign.

Since the mid-1980s, from the point of view of synthetic cryptography, the following idea has been studied: the use of NP-complete tasks for solving polynomial systems. (Example 3). At the same time, various practical and effective methods to solve this problem have been developed (method XL, F4, F5, etc.), and many encryption schemes based on this task have been successful.

Example 3. Pure crypto mechanism scheme

- In the final field K is chosen easily reversible square display $F\colon K^n \to K^n, m \geq n,$ and reversible linear display (linear endomorphism) $S\colon K^m \to K^m, T\colon K^n \to K^n$;
- sequence crypto secret key—presentation of S, F, T;
- public-key cryptographic sequence—presentation of $P = S \bullet F \bullet T$;
- Encoded: $m \in K^n, c = E(m) = P(m)$;
- Decryption: $x = S^{-1}(c), y =; F^{-1}(x), y = C^{-1}(y)$.

Competing groups of developers, which are based on this paradigm of the question on the development and improvement of existing crypto mechanisms with NIST, are as follows: CFPKM, Giophantus, DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow, SRTPI, DME.

And the hash-based signature scheme, developed back in the late 1970s for the one-time signature of Lamport and Winternitz, makes it suitable for the construction of multiple signature schemes based on the tree structure of a special type of hash value. In this way, the companies SPHINCS+ and GravitySPHINCS which used this idea in one form or another are direct competitors of NIST.

3. Practical Use of Crypto Mechanisms for Critical Data

It should be noted that the NIST experts have not voiced an unambiguous preference for cryptographic mechanisms when choosing a basic integrated solution, but only excluded the most peculiar vulnerable solutions (which accounted for the majority of cyber-attacks).

The next step is to fix and improve the cryptographic plan, which has entered the second phase, and the deadline for this process is late 2020. Also important is the validity of the proposed NIST competition plan. It should be noted that all cryptographic schemes, without exception, have the size of parameters, key length and, as a rule, the length of an encrypted text message (signature, shared key) is greater than that of a traditional cryptographic computer scheme with the same security level as the traditional calculator as RSA, ECDH, ECDSA. In practice, it usually requires significantly more computing resources, such as the performance of the cryptographic system, the use of processor time, and available memory.

Consequently, the transition to inverse post-quantum cryptography will require a significant increase in computing resources dedicated to the cryptographic conversion of critical data streams to reliably support the functions of a secure network for processing critical information [31, 32].

The International Organization for Standardization/International Electrotechnical Commission also covers the field of post-quantum standardization of cryptography. Therefore, the professional technical committee responsible for the standardization of information protection mechanisms has started to create a configuration file that will reflect the main direction of the post-quantum cryptographic scheme after its creation.

Thus, summing up our review it is possible to assert with certainty that today only a small number of proposed crypto mechanisms from the following groups working in this direction deserve the close attention of developers of software systems with the maintenance of critical information.

For public-key encryption and key encapsulation: BIKE, Classic McEliece, CRYSTALS-KYBER, FrodoKEM, HQC, LAC, LEDAcrypt (derivative scheme from LEDAkem/LEDApkc), NewHope, NTRU (from NTRUEncrypt/NEMTRU-HRSS-KYBER NTRU Prime, NTS-KEM, ROLLO (derivative scheme from LAKE/LOCKER/Ouroboros-R), Round5 (derivative scheme from Hila5/Round2), RQC, SABER, SIKE, Three Bears.

For digital signature schemes: CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow, SPHINCS+.

4. Conclusions

It is also necessary to prepare the domestic information infrastructure for the emergence of post-quantum cryptanalysis and corresponding computing systems. Of course, it is necessary to take into account the experience of the international community for developing and testing a series of post-quantum standards in the field of cryptographic protection of key information. However, the following aspects should be taken into account.

Usually, the Ukrainian standardized system insists on using time-tested encryption mechanisms: no loopholes will be detected in this mechanism during long-term research. Except for the NTRU scheme based on McAlice’s theory and other encoding schemes, post-quantum cryptography has a history of up to 5 years.

To some extent, NIST has been hasty in taking steps to implement post-quantum encryption technology (for example, a memorandum issued by the U.S. National Security Agency in 2015 provided U.S. developers with encryption to protect important information that has not yet been included in its products. Introduction of encrypted information. Algorithms based on elliptical curve operations, avoid the implementation of these algorithms to save resources for the proposed transition to post-quantum algorithms), forcing us to carefully test new standards developed in the procedures of the organization to avoid using standards for the generation of pseudo-random numbers. The repetition of the scandalous Dual_EC_DRBG history has been standardized. Many researchers objected, but pointed to obvious loopholes, so the standard needs to be revoked.

Proceeding from this it is obvious that the moment of transition to post-quantum cryptography will require fundamental reorganization of the entire basic infrastructure of information security, all methods of information protection using asymmetric cryptographic algorithms, especially the infrastructure of the authentication center. Taking into account the cost of these events, we should make a cautious decision on the transition to post-quantum cryptography based on accurate forecasts of the development of post-quantum computing system functions.

The moment of transition to post-quantum cryptography will require fundamental reorganization of all basic infrastructure of information security, all methods of information protection using asymmetric cryptographic algorithms, especially the infrastructure of the authentication center. Taking into account the cost of these events, it is necessary to make a cautious decision on the transition to post-quantum cryptography using accurate data of forecasts of the development of post-quantum computing system functions.

Based on the above scientific research, we can confidently say that the international IT community is actively preparing for significant changes with the advent of the post-quantum era.

5. References

[1] A. Aguado, V. López, J. P. Brito, A. Pastor, D. R. López, V. Martin, Enabling Quantum Key Distribution Networks via Software-Defined Networking, in: 2020 International Conference on Optical Network Design and Modeling (ONDM), 2020, pp. 1–5. doi:10.23919/ONDM48393.2020.9133024.

[2] A. Alkhulaifi, E. M. El-Alfy, Exploring Lattice-based Post-Quantum Signature for JWT Authentication: Review and Case Study, in: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 2020, pp. 1–5. doi:10.1109/VTC2020-Spring48590.2020.9129505.

[3] A. Facon, S. Guilley, M. Lec'Hvien, A. Schaub, Y. Souissi, Detecting Cache-Timing Vulnerabilities in Post-Quantum Cryptography Algorithms, in: 2018 IEEE 3rd International Verification and Security Workshop (IVSW), Costa Brava, 2018, pp. 7–12. doi:10.1109/IVSW.2018.8494855.

[4] A. Kuznetsov, M. Lutsenko, N. Kiian, T. Makushenko, T. Kuznetsova, Code-based key encapsulation mechanisms for post-quantum standardization, in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, 2018, pp. 276–281. doi:10.1109/DESSERT.2018.8409144.

[5] D. Ageyev, A. Mohsin, T. Radivilova, L. Kirichenko, Infocommunication Networks Design with Self-Similar Traffic, in: IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), Polyana, Ukraine, 2019, pp. 24–27. doi:10.1109/CADSM.2019.8779314.

[6] D. Suyitno, H. O. Asmar, R. W. Wardhani, M. Syahral, D. Ogi, D. S. C. Putranto, Analysis of Secure Bit Rate for Quantum Key Distribution based on EDU-QCRY1, in: 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), Surabaya, Indonesia, 2019, pp. 244–247. doi:10.1109/ISITIA.2019.8937140.

[7] F. Borges, P. R. Reis, D. Pereira, A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography, IEEE Access 8 (2020) 142413–142422. doi:10.1109/ACCESS.2020.3013250.

[8] F. Farahmand, D. T. Nguyen, V. B. Dang, A. Ferozpuri, K. Gaj, Software/Hardware Codesign of the Post Quantum Cryptography Algorithm NTRUEncrypt Using High-Level Synthesis and Register-Transfer Level Design Methodologies, in: 2019 29th International Conference on Field Programmable Logic and Applications (FPL), Barcelona, Spain, 2019, pp. 225–231. doi:10.1109/FPL.2019.00042.

[9] I. Dronyuk, O. Fedevych, N. Kryvinska, High Quality Video Traffic Ateb-Forecasting and Fuzzy Logic Management, in: 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, 2019, pp. 308–311. doi:10.1109/FiCloud.2019.00051.

[10] I. Dronyuk, Y. Klishch, S. Chupakhina, Developing Fuzzy Traffic Management for Telecommunication Network Services, in: 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), Polyana, Ukraine, 2019, pp. 1–4. doi:10.1109/CADSM.2019.8779323.

[11] J. Xie, K. Basu, K. Gaj, U. Guin, Special Session: The Recent Advance in Hardware Implementation of Post-Quantum Cryptography, in: 2020 IEEE 38th VLSI Test Symposium (VTS), San Diego, CA, USA, 2020, pp. 1–10. doi:10.1109/VTS48691.2020.9107585.

[12] L. Chen, Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?, IEEE Security & Privacy 15 (2017) 51–57. doi:10.1109/MSP.2017.3151339

[13] M. -J. O. Saarinen, Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards, in: 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, GB, 2020, pp. 23–30. doi:10.1109/MobileCloud48802.2020.00012.

[14] M. Pasyeka, V. Sheketa, N. Pasieka, S. Chupakhina, I. Dronyuk, System Analysis of Caching Requests on Network Computing Nodes, in: 2019 3rd International Conference on Advanced

Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 216–222. doi:10.1109/AIACT.2019.8847909.

[15] M. X. Lyons, K. Gaj, Sampling from Discrete Distributions in Combinational Hardware with Application to Post-Quantum Cryptography, in: 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 2020, pp. 610–613. doi:10.23919/DATE48585.2020.9116434.

[16] M. Medykovskyy, M. Pasyeka, N. Pasyeka, O. Turchyn, Scientific research of life cycle perfomance of information technology, in: 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 1 (2017) 425–428.

[17] M. Nazarkevych, A. Marchuk, L. Vysochan, Y. Voznyi, H. Nazarkevych, A. Kuza, Ateb-Gabor Filtering Simulation for Biometric Protection systems, CPITS 1 (2020) 14–22. doi:10.1109/STC-CSIT.2017.809882

[18] M. Nazarkevych, N. Lotoshynska, V. Brytkovskyi, S. Dmytruk, V. Dordiak, I. Pikh, Biometric identification system with ateb-gabor filtering, in: 2019 11th International Scientific and Practical Conference on Electronics and Information Technologies, ELIT 2019 - Proceedings, 2019, pp. 15–18. doi:10.1109/ELIT.2019.8892282

[19] M. Nazarkevych, N. Lotoshynska, I. Klyujnyk, Y. Voznyi, S. Forostyna, I. Maslanych, Complexity Evaluation of the Ateb-Gabor Filtration Algorithm in Biometric Security Systems, in: 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2019, pp. 961–964.

[20] P. Ravi, V. K. Sundar, A. Chattopadhyay, S. Bhasin, A. Easwaran, Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography, in: 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Sevilla, 2020, pp. 1–5. doi:10.1109/ISCAS45731.2020.9180847.

[21] N. Pasieka, V. Sheketa, Y. Romanyshyn, M. Pasieka, U. Domska, A. Struk, Models, methods and algorithms of web system architecture optimization, in: 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, Kyiv, Ukraine, 2019, pp. 147–152. doi:10.1109/PICST47496.2019.9061539.

[22] M. Pasyeka, V. Sheketa, N. Pasieka, S. Chupakhina, I. Dronyuk, System analysis of caching requests on network computing nodes, in: 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings, 2019, pp. 216–222. doi:10.1109/AIACT.2019.8847909.

[23] R. Alléaume et al., Worldwide standardization activity for quantum key distribution, Globecom Workshops (GC Wkshps) (2014) 656–661.

[24] R. Tkachenko, I. Izonin, N. Kryvinska, I. Dronyuk, K. Zub, An Approach towards Increasing Prediction Accuracy for the Recovery of Missing IoT Data based on the GRNN-SGTM Ensemble, Sensors 20 (2020). doi:10.3390/s20092625.

[25] R.Tkachenko, I. Izonin, P.Vitynskyi, N. Lotoshynska, O. Pavlyuk, Development of the Non-Iterative Supervised Learning Predictor Based on the Ito Decomposition and SGTM Neural-Like Structure for Managing Medical Insurance Costs, Data 3(4) (2018). doi:10.3390/data3040046.

[26] U. Banerjee, A. Pathak, A. P. Chandrakasan, 2.3 An Energy-Efficient Configurable Lattice Cryptography Processor for the Quantum-Secure Internet of Things, in: 2019 IEEE International Solid-State Circuits Conference - (ISSCC), San Francisco, CA, USA, 2019, pp. 46–48. doi:10.1109/ISSCC.2019.8662528.

[27] V. B. Dang, F. Farahmand, M. Andrzejczak, K. Gaj, Implementing and Benchmarking Three Lattice-Based Post-Quantum Cryptography Algorithms Using Software/Hardware Codesign, in: 2019 International Conference on Field-Programmable Technology (ICFPT), Tianjin, China, 2019, pp. 206–214. doi:10.1109/ICFPT47387.2019.00032.

[28] V. Drăgoi, T. Richmond, D. Bucerzan, A. Legay, Survey on cryptanalysis of code-based cryptography: From theoretical to physical attacks, in: 2018 7th International Conference on Computers Communications and Control (ICCCC), Oradea, 2018, pp. 215–223. doi:10.1109/ICCCC.2018.8390461.

[29] V. Sheketa, L. Poteriailo, Y. Romanyshyn, V. Pikh, M. Pasyeka, M. Chesanovskyy, Case-Based Notations for Technological Problems Solving in the Knowledge-Based Environment, in: 2019

IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2019, pp. 10–14. doi:10.1109/STC-CSIT.2019.8929784.

[30] V. Sheketa, M. Pasyeka, N. Lysenko, O. Lysenko, N. Pasieka, Y. Romanyshyn, Neural Networks in Intelligent Analysis Medical Data for Decision Support, IDDM (2020) 252–264.

[31] A. Bessalov, V. Sokolov, P. Skladannyi, Modeling of 3- and 5-isogenies of supersingular Edwards curves, in: Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science, June 2–3, 2020, no. I, vol. 2631, pp. 30–39.

[32] A. Bessalov, et al., Analysis of 2-isogeny properties of generalized form Edwards curves, in: Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems, July 7, 2020, vol. 2746, pp. 1–13.