Journal of Theoretical and Applied Information Technology
15th August 2024. Vol.102. No. 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE IMPACT OF QUANTUM COMPUTING (ALGORITHMS) ON CONTEMPORARY SECURITY SYSTEMS AND FUTURE

AKKU KUBIGENOVA [1], ALIMBUBI AKTAYEVA [2,*], GALIYA YESMAGAMBETOVA [3], ALTYNBEK SHARIPBAY [4], VLADIMIR SUKHOMLIN [5] , NAZERKE AUSSILOVA [6]

[1] Department of Information Systems, S.Seifullin Kazakh Agrotechnical Research University, Kazakhstan
[2, 6] Department of Information Systems and Informatics, Abay Myrzakhmetov Kokshetau University, Kazakhstan
[3] Department of Information and Communication Technologies, Sh.Ualikhanov Kokshetau University, Kazakhstan
[4] Department of Artificial Intelligence Technologies, L.Gumilyov Eurasian National University, Kazakhstan
[5] Department of Information Security, Lomonosov Moscow State University, Russian Federation

E-mail:[1] akkukubigenova@gmail.com, [2] aakhtaewa@gmail.com, [3]gal.esm@mail.ru, [4]sharalt@mail.ru, [5]sukhomlin@mail.ru, [6]nazerke-m1995@mail.ru

* Corresponding authors: *aakhtaewa@gmail.com*

ABSTRACT

In the course of technological evolution, a new scientific point of view arose, reviving interest in the theoretical foundations of quantum mechanics and many new issues combining physics, computer science, and information theory. There is a growing understanding that quantum computation may be a more natural model of computation than the classical model and that fundamental information security issues may be more readily revealed through the concepts of quantum computation. This research aims to contribute to these advancements in these areas: the quantum computer based on the theory of ternary logic is an efficient general-purpose computing device capable of simulating any computing process, increasing the computation time by a polynomial factor only. Quantum computation has the potential to significantly enhance our understanding of security issues, making our work more important than ever. The authors suggest ways to develop optimally using the theoretical principles of the functioning of a quantum computer based on three-digit logic and how to implement structural elements' security using ternary technology.
Keywords: *Three - digit logic, Quantum computing, Quantum theory, Qubits; Cybersecurity.*

1. INTRODUCTION

The process of globalization presented around the world introduces both new capabilities and new challenges, and inclusion has positive and negative effects on contemporary life and society. For example, the number of people employed in ICT fields is steadily rising; IT applications are highly valued in many scientific fields, such as education and industry. All these developments are occurring alongside radical shifts in conventional perceptions of media, television, and radio communications. As a consequence of globalization, the necessary conditions for forming a global information environment came forward, such as the internet, which is undoubtedly the foundation for developing a global information space in the market economy.

On an international scale, the technological progress of globalization has considerably reduced the price of information accumulation, processing, and transfers, which cannot but impact rates of economic growth and has increased the sharing and flow of information and knowledge, access to ideas, and cultural exchange among people of different countries.

In general, the uniting of computer capabilities with telecommunication networks "compresses" time and space, reduces the significance of state borders, and gives individuals the feeling of communicating with and being a part of a global community. Of course, globalization would not be

possible without the tremendous technological growth, most of all in the spheres of ICT, electronics, communication, transport, etc. The rapid development of microprocessor technologies, digital technologies, and means of communication should be especially emphasized.

According to historical analyses by some researchers, the development of information technology is exponential. Particular emphasis should be placed on the rapid development of microprocessor, digital, and media technologies. Historical analyses by some researchers suggest that the development process of information technology is exponential [1, 2].

Figure 1 demonstrates the interrelation of the number of transistors per microprocessor. For example, at the IEEE International Electron Devices Meeting (IEDM) 2022, a new and upcoming process node technology was demonstrated, stating that Intel is currently developing its 10^{+++} optimizations as well as the 7 nm processor family. Intel is currently in "*path-finding*" and "*research*" modes. To date, Intel is considering new materials, new transistor designs, and so on. Over the past century, the scientific community has experimented with a variety of computation theories and techniques to harness the power of nature and create computers that would allow us to process massive amounts of data (big data) in a matter of seconds, fundamentally changing our environment in the span of a few decades.

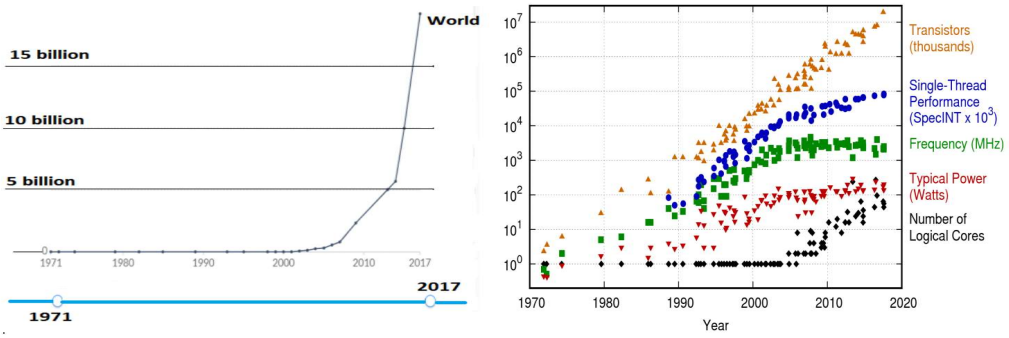

Figure 1: Moore's Law for Quantum Computers [3]

The development of modern civilization from the second half of the 20th century to the present has been fueled by the central role that information technology (IT) has played in the modern era. The new digital technologies have become available in our daily lives, bringing a perplexing mix of benefits and problems. The empirical finding that component transistor density on a computer chip doubled every two years was the basis for the original Moore's Law, which was published in 1965 and has currently become a benchmark for technological advancements in ICT. However, the longevity of these technological predictions under this law points to more profound phenomena [2].

Currently, Moore's Law has become a benchmark for technological progress in computing, and the exponential law states that an increase in data processing speed, an expansion in storage capacity, a reduction in the critical dimension of the technology, and a reduction in the cost of an ICT product per individual transistor then depend on the properties of the semiconductor component. The aforementioned trends also involve supercomputing, parallel computing, and quantum computations to a large extent, with Moore's law generally having a positive influence.

The model described by Moore's Law suggests that current trends in information technology will continue until approximately 2030, when existing technologies will be replaced by innovative technologies such as optics, molecules, and quantum computing technologies [2]. For example, multicore processor architectures arose when problems with thermal amplification did not allow for increased processor speed. The use of graphics processors with hundreds of processor cores has become the standard for some computers. The number of semiconductor devices has already grown exponentially in quantum computing experiments, unlike Moore's Law for conventional computers [2].

If a property is proven to have a logarithmic qubit scale, this case clearly corresponds to an exponential increase, similar to Moore's law for classical computers, and fits the data, indicating a doubling of the number of qubits every 5.7 ± 0.4 years. Then, for the first time, the power of quantum computing doubles approximately every six years, with quantum computing for real-world applications occurring between nine and twelve years if this trend continues (see Fig. 2).

The miniaturization of transistors is limited by the size of their atoms, which is invariably present in all cases. However, major difficulties because of

uncontrolled quantum tunnelling are expected much earlier (the first being a technology smaller than approximately 15 nanometers for transistors of 5 nanometers or less).

The primary barrier facing supercomputing might be the correlation between the exponential growth of computing and the corresponding exponential growth in the amount of electricity used by the supercomputer. The most advanced supercomputers still use megawatts of electricity today. A gigawatt of electricity will be required for an exascale supercomputer, according to a straightforward extrapolation.

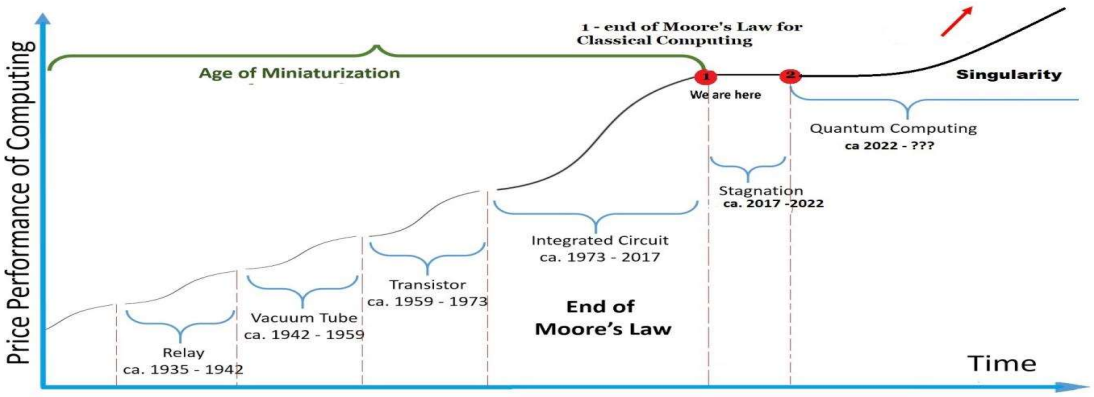

Figure 2: Moore's Law for Quantum Computers [3]

However, in the current era, conventional computers are reaching a point where significant improvements in efficiency will not be possible due to the physical limitations of transistors. The National Institute of Standards and Technology (NIST) is currently standardizing algorithms accordingly, and the first postquantum cryptography standards are expected in 2023–2025 [4].

This development has given researchers a new incentive to revive previous research of new types of classical computation. Quantum computation is unquestionably the most promising of all the ideas put forth as a potential replacement for classical computing. First, quantum computation with three-digit logic enables the exploitation of the most fundamental properties of physics; it is founded on applying the properties of quantum mechanics; second, it thus makes use of the basic laws of nature to achieve information security.

Quantum calculations pose severe threats to modern security systems, especially in cryptography. The potential of quantum computers to break encryption systems represents a severe challenge to today's established cryptography. The threat is not just theoretical but a real and imminent danger. Quantum algorithms like Grover's and Shor's, with their exponential processing capacity, threaten both symmetric and asymmetric cryptosystems like AES and RSA [5]. The gravity of the situation cannot be overstated.

Because creating a scalable quantum computer remains a technical challenge, the fundamental threat to digital security and privacy, particularly in the context of sensitive data like personally identifying information, is undeniable. The advent of quantum computing also raises significant concerns in the realm of network security, particularly in key management and distribution, further broadening the scope of the threat [6].

The potential for attackers to disrupt the global quantum state of quantum systems, compromising their ability to operate covertly, is a serious concern [7]. Furthermore, the reliance of the quantum computing stack on third parties introduces the risk of intellectual property theft, manipulation, and malicious code insertion. This underscores the urgent need for enhanced security protocols and increased quantum security research [8 - 10].

Quantum computing is more efficient at resolving some difficult problems than conventional algorithms. For example, Google announced that their 53 qubits quantum chip managed to solve complex mathematical problems within seconds that traditional computers took years to solve. In regard to effective quantum computing, research on the design of quantum computers has attracted the attention of many researchers. The application of fundamentally new computing and communication techniques (such as quantum communication channels, quantum cryptography, and quantum computers) using quantum systems is currently the focus of the young, rapidly expanding field of science known
as quantum information science (quantum computation) [11 - 12].

The state of a qubit (the type of bit used in quantum computers), which is based on the superposition of photons, a quantum mechanical phenomenon, means that it is 0 and 1 at the same time. A further feature of quantum computers is qubit entanglement in which each qubit's probability state is directly influenced by another entangled qubit. If two qubits are entangled, even if they are polar opposites, the moment we measure the state of one of them, we can immediately know the state of the other qubit. Given two entangled qubits, the probability of their state during measurement is four (00,01,10,11), and adding just one qubit to the system will double the probability range to eight. This property mathematically guarantees an exponential growth of qubit state probabilities with every entangled qubit in this system.

Certain fundamental quantum effects that are typically thought of as barriers to accessing micro- and Nano electronics technology may actually be the source of groundbreaking improvements in quantum and postquantum computation in the fields of big data and cybersecurity.

The application of efficient means to represent traditional data with a logical structure of quantum data can create possibilities for improving various IT implementation methods and is crucial in quantum computing with three-digit logic.

The application of efficient means to represent traditional data with a logical structure of quantum data can create possibilities for improving various IT implementation methods and is crucial in quantum computing.

The research offers insightful security recommendations and preparations for the shift from quantum-vulnerable to quantum-resistant systems. The goal is to help them protect their encrypted data from the threat that quantum computers may pose in the future, guaranteeing critical information's long-term security.

2. MATERIALS AND METHODS

The basis of the methodological approach in this research is a combination of methods of system analysis of the key aspects of the formation of quantum computation systems with data science analytical research on the basic principles of building information knowledge bases used today in various fields.

The main scientific research is preceded by a theoretical framework, which is an analysis of the research results of a number of researchers who have studied the problematic aspects of the practical application of knowledge quantum computation technology. To ensure a comprehensive and systematic literature review, we meticulously searched several academic databases, including Scopus and Google Scholar [11,12].

The keywords used for this search included “classic computers “, “supercomputers”,” quantum computers “and “other computers”. Our time filter was set to include studies published within the last 20 years to ensure contemporary relevance. In total, we included 277 studies published between 1988 and 2023. Our exclusion criteria were stringent: studies not available in English, those not directly addressing the implementation of intelligent information systems in educational settings, and those lacking empirical data were omitted. To extract and analyse data from these studies, we employed a standardised form called PRISMA (see Figure 3).

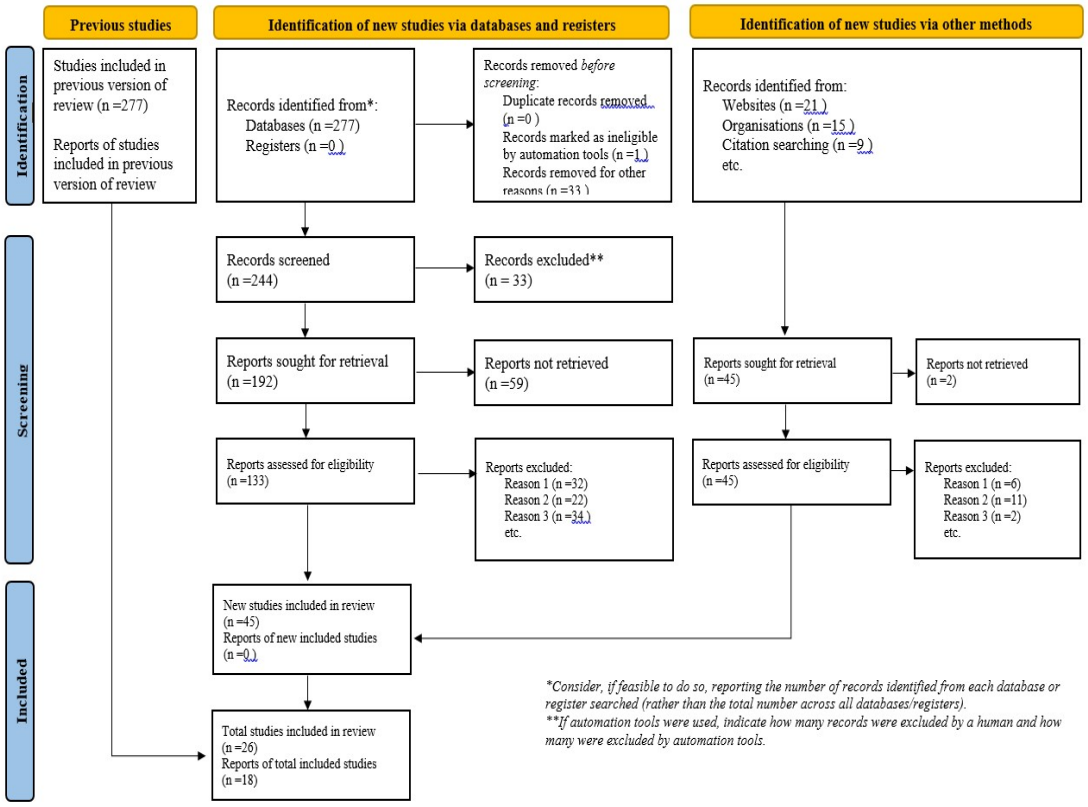

Figure 3: PRISMA 2020 flow diagram for updated systematic reviews

This form was designed to uniformly capture key findings, methodologies, and conclusions from each study, thereby maintaining consistency in data handling and interpretation. This rigorous approach underpins the reliability and validity of our review findings, ensuring a comprehensive synthesis of the current state. Practical application of the method of systematic analysis of the main aspects made it possible to derive the definition and essence of the concept of intelligent information systems, as well as to define their role in the world of quantum technology. In this research work, an analytical comparison was made between the results obtained in this research and those of other researchers who have worked on topics similar to this research study. This allowed the results to be refined and the final conclusions to be formed on their basis, which are a logical representation and summarize the whole range of research in the field of quantum computations: the impact on contemporary security systems and the future.

Classical computing has traditionally been based on the notion that electrical circuits are always either on or off, which is a classic phenomenon. The bit is a voltage or charge value; low is 0, and high is 1. It is used for information storage and manipulation. Two bits on a computer can be in four possible states {00, 01, 10, or 11}, but only one at a time, which restricts the computer to processing one entry at a time. The performance of the circuit is subject to classical physics. The central processing unit (CPU), which is made up of an arithmetic and logic unit (ALU), processor registers, and a control unit (CU), processes data in conventional computers [13].

Quantum computing utilizes qubits, namely, 0 and 1, as well as the superposition states of both 0 and 1; in other words, the symbols are 0 and 1 at the same time (and all points in between). Quantum physics or quantum mechanics controls the behavior of the circuitry. Quantum computing represents a subdivision of the science of quantum information. Quantum cryptography and quantum correspondence are two important applications that use quantum mechanics to perform various data operations. Entanglement, superposition, and decoherence are just a few characteristics of quantum computing.

Quantum theory offers a particularly accurate description of the fundamental processes of physics. The idea is that if the answer is yes, it must be possible to use quantum theory to model complex systems that include scientists who use quantum theory. Researchers' conclusions, even though they are all derived from quantum theory, are therefore incoherent. Indeed, quantum computers will introduce uncertainty into most existing public-key cryptosystems.

The cryptographic requirement here is that transmitted messages remain inaccessible to anyone other than the intended recipients, even if the communication channel is not trustworthy. Nevertheless, there is good reason to believe that cryptographers will eventually gain the upper hand over crypto analysts.

Within a quantum computer, two qubits can represent exactly the same four states (00, 01, 10, or 11). The difference is that because of the superimposition, qubits can represent all four states at once (with "n" qubits, one can simultaneously represent 2^n states). Example: Three qubits give 23, which means eight states at a time; four qubits give 24, which means 16. What about 64 qubits? They give 264, which equals 18,446,744,073,709,600,000 possibilities! That is approximately 1 million terabytes. Whereas 64 regular qubits can also represent that many (264) states, they can only represent one state at a time. It would take approximately 400 years to review all these combinations at $2 billion per second (which is a typical speed for a modern PC).

Quantum cryptography uses the principles of quantum physics to secure information. It allows us to build communication schemes whose secrecy relies on the laws of physics and minimal assumptions about cryptographic hardware. However, from an algorithmic point of view, quantum issues are complex, making them unenforceable for calculations on a classical computer. However, it may also denote an abstract model of cellular automata performing true quantum computations, initially proposed by Feynman. Feynman and Yuri Manin, guided by this long-known and negative observation, managed to draw the positive conclusion that, because nature is capable of successful management of complicated problems, perhaps humanity could use quantum systems as a new elemental system on which to base the calculations [14, 15].

Quantum theory is a mathematical toolkit for modeling quantum contextually, or the contextual actualization of possibilities, representing a fundamental principle of organizing the dynamic processes of nature. The development of quantum theory gave rise to an alternative methodology in IT, which states that the processes under study are determined by the research technique applied and may also produce fundamentally unpredictable multivariance.

Systems in quantum methodology may possess a quality of integrity that is no identical to the sum of the qualities of individual parts. Computers based on quantum logic gates could be much more powerful than their classical counterparts.

Quantum computers are by design ternary; therefore, their working principles may be described by the familiar term "*qubit*", but it is even better to use the notion "*qutrit*" or "*quantum trit*", thus describing quantum reality with the term first introduced into the field of logic and computer science by N.P. Brusentsov's theory of three-digit dialectical logic [16,17].

The task is to estimate the number of quantum resources required to solve some asymmetric cryptographic problems using derivatives of Shor's algorithm against various parameters and to compare the complexity of this process with that of solving the problem of searching for the key of a shared-key cryptosystem. Shor's algorithm is a polynomial-time quantum computer algorithm for integer factorization that runs in polynomial time.

This elapsed time for integer factorization is a polynomial in log N of the size of the integer given as input.

The efficiency of the factorization method is higher than that of classical factorization algorithms since Shor's algorithm uses the methods of repeated squaring, quantum Fourier transform, and modular exposure.

Using the described quantum Shor factorization algorithm, a quantum computer made up of two quantum registers with a combined length of approximately 4096 qubits is required to successfully decrypt the RSA cryptosystem (within polynomial quantum time), with the used module having a 2048-bit length. This setup requires approximately $34 \cdot 10^9$ quantum operations. To solve the classically equivalent elliptic curve discrete logarithm problem (ECDLP), 1300 qubits and $4 \cdot 10^9$ quantum operations are needed.

Table 1 provides further comparative data [18 – 19], reflecting the number of quantum resources required to solve the factorization problem and the discrete logarithm in a group of points on an elliptic curve with the following value of *f (n)*:

$$f(n) = 5n + 8\sqrt{n} + 2log_2 n + \varepsilon, \quad (1)$$

where ε = 10.

Table 1. Comparative Data Reflecting The Number Of Quantum Resources [7 – 9].

Factorization			ECDLP			
n	number of qubits	sq. time	n	number of qubits	sq. time	sq. time
	$2n$	$4n^3$	$f(n)$	$360n^3$		
512	1024	$0{,}54 \cdot 10^9$	110	700	$0{,}5 \cdot 10^9$	$6{,}39 \cdot 10^{16}$
1024	2048	$4{,}3 \cdot 10^9$	163	1000	$1{,}6 \cdot 10^9$	$3{,}03 \cdot 10^{24}$
2048	4096	$34 \cdot 10^9$	224	1300	$4{,}0 \cdot 10^9$	$9{,}20 \cdot 10^{33}$
3072	6114	$120 \cdot 10^9$	256	1500	$6{,}0 \cdot 10^9$	$6{,}03 \cdot 10^{38}$
15360	30720	$1{,}5 \cdot 10^{13}$	512	2800	$50 \cdot 10^9$	$2{,}05 \cdot 10^{77}$

Table 1 provides further comparative data, reflecting the number of quantum resources required to solve the factorization problem and the discrete logarithm of a group of points on an elliptic curve [18 – 20]. This table is based on data from NIST (National Institute of Standards and Technology) and the research results of authors J. Proos and Ch. Zalka in terms of quantum computing and is supplemented with classical complexity data calculated using the formula $\sqrt{\pi}2^n$, where n is the length in bits of the binary representation of the order of a group of points corresponding to an elliptic curve [20, 21].

Table 1 lists the asymmetric key lengths that determine the complexity of the factorization and discrete logarithm problem in a group of points on an elliptic curve, which require an approximately equal number of operations performed on a classical computer. The number of qubits and quantum steps for factorization corresponds to the modification of the Beauregard scheme for the Shor algorithm [22].

This complexity is given in the last line of Table 1, and for classically equivalent factorization problems, as well as for the ECDLP, it is stated as follows:

Hypothesis 1: The quantum solution to the ECDLP problem requires fewer resources than the solution to the factorization problem (qubits and quantum time).

Hypothesis 2: The difference between the number of resources needed and the increase in traditional complexity.

The initial stages of the development of quantum cryptography presumed the composition of the quantum key secrecy criterion in response to the detection of eavesdropping, which means that once an intruder is detected, legitimate participants refuse secure communication. With the development of theoretical and experimental studies, the problem of formulating a numerical criterion for the secrecy of a key arose.

3. RESULTS

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn.

Quantum computers provide an alternative platform to implement computing methods because they provide an efficient way to access high-dimensional Hilbert spaces into which classical data can be embedded. The states of the quantum system in the standard formulation of quantum mechanics are determined by either vectors $|\psi\rangle$ in the Hilbert space or density operators acting in the Hilbert space. Vectors in the Hilbert space are associated with wave functions (x) of pure quantum states, and density operators are associated with pure or mixed states described by density matrices or matrix elements of the density operators in some representations [23].

The quantum bit (qubit), which functions similarly to traditional bits, is regarded as the core basis of quantum computation. In quantum theory, two basic levels of the qubit are defined by $|0\rangle$ and $|1\rangle$, which are equivalent to the traditional bit states of 0 and 1. However, a qubit $|\psi\rangle$ can be expressed based on a superposition state of $|0\rangle|$ and $|1\rangle$ regarding complex coefficients of α and β, given as [24]: $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$.

Quantum computing is currently being researched in many countries. If implemented in the near future, it may pose a threat to existing encryption standards. In the quantum computer environment, asymmetric encryption can be solved by Shor's algorithm in polynomial time, and the difficulty of breaking symmetric encryption using brute force is reduced from *N* times to square root *N* times by Grover's algorithm. Hence, we conclude that these approaches constitute an effective and relatively inexpensive toolbox that could be applied in many realistic scenarios to systematically improve the performances of quantum classification algorithms.

Quantum encryption can be "unconditionally secure" based on the Heisenberg uncertainty principle because of quantum features such as quantum entanglement, coherence, parallelism, and superposition. Quantum encryption employs the "no-cloning theorem", derived from the Heisenberg uncertainty principle, to encrypt image data, whereas conventional encryption typically restricts the timeliness of decryption operations. That is, because the basis of replication is measurement and because measurement often modifies the quantum state, it is impossible to accomplish accurate duplication of any unknown quantum state in quantum mechanics.

When individual measurements are attacked, Eve's intervention in the quantum channel leads to an error in receiving a logical bit in the Alice-Bob channel with probability Q (QBER – quantum bit error rate) and to an error in the Alice-Eve interception channel with the following value:

$$Q_E = \frac{1}{2} - \sqrt{Q(1-Q)} \qquad (2)$$

A relationship between the error probabilities in the legitimate and interception channels takes place due to the quantum nature of information transmission. Suppose that the error in a legitimate channel emerges due to the intruder's actions. Then, the error probability Q measured in the Alice-Bob channel (within 5%) gives a corresponding and, generally speaking, rather large estimate of the error probability QE in the Alice-Eve interception channel.

There are no obvious reasons to refuse secure communication, but direct use of the values of the transmitted logical bits as an encryption key becomes problematic because, on the one hand, errors must be corrected, and on the other hand, the probability distribution of Eve key selection, given the distorted sequence of secret logical bits becomes, albeit not heavily, but unequally probable (a posteriori).

In [23-25] was given what for information encryption between arbitrary network nodes, it is necessary to have an agreement on the keys distributed in different segments of the network through a public classical communication channel. Thanks to the secrecy criterion for keys independently distributed in different network segments were formulated in terms of the trace distance. These are the so-called ε–secret keys, and it is sufficient that the keys on the individual segments are ε/2–secret. The ε-secrecy criterion is closely related to the hashing procedure, by applying the leftover-hash lemma, that the obtained quantum key satisfies the secrecy criterion [23-25].

The criterion of ε-secrecy consists of calculating the variational distance averaged over all of Eve's observations from the posterior distribution of the quantum key to the equally probable distribution. It is essential to determine the conditions under which the average distance is equal to or less than the given value ε. The last stage in assessing the strength of a quantum key entails the construction and assessment of the complexity of algorithms for recovering a ε-secrecy quantum key. In summary, this paper considers individual mathematical problems of quantum cryptography related to the following:

a) the protocol for encoding logical bits by quantum states,
b) the attack on individual measurements,
c) the error correction procedure,
d) the procedure for enhancing secrecy,
e) the criterion of ε-secrecy of the quantum key, and
f)the complexity of restoring a quantum key that has the property of ε-secrecy.

Alice applies a physical random number generator (FRNG) and generates a random equally probable sequence of logical bits

$$x_1, \dots, x_{\mathcal{L}},\ x_i \in \{0,1\} \qquad (3)$$

along with a random equally probable binary "*basic*" sequence

$$b_1^A, \dots, b_{\mathcal{L}}^A, b_i^A \in \{R, D\}, i = \overline{1,\mathcal{L}}, \qquad (4)$$

In the legend, R is a rectangular basis, and D is a diagonal basis. To describe the attack on individual measurements, it is necessary to consider a particular problem of distinguishing quantum states $|\varphi_1\rangle$ and $|\varphi_2\rangle$ having an equally probable a priori distribution at the input of the measuring device. In this case the states $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are the variate $\varphi \in \{|\varphi_1\rangle$ and $|\varphi_2\rangle\}$ "*outcomes*". The key insights in the error

correction procedures are that Alice forwards over the classical open channel bits

$$b = Hx, b \in \{0,1\}^C, C < L, \quad (5)$$

where $x \in \{0,1\}^L$ is the sequence transmitted by Alice over the quantum channel, and H is a special check matrix of some corrective code.

The bit sequence $b \in \{0,1\}^C$ is available to Eve and carries certain information about the transmitted sequence $x \in \{0,1\}^L$. An "*ill*" contribution of this information shall hereinafter be considered when substantiating the secrecy of the key. Now, suppose that the errors are corrected, and Alice and Bob have a common bit sequence $x \in \{0,1\}^L$ because Bob corrects the errors. Sharing a common sequence $x \in \{0,1\}^L$, Alice and Bob aim to generate a common binary encryption key $k \in \{0,1\}^n$, $n < L$, which would be inaccessible to Eve the intruder.

The procedure for enhancing secrecy consists of compressing (hashing) $x \in \{0,1\}^L$ into the final key $k \in \{0,1\}^n$, $n < L$, using a randomly chosen function (mapping) g of class G of universal hash functions of the second order:

$$g: \{0,1\}^L \to \{0,1\}^n. \quad (6)$$

$$\text{functions class } g: \{0,1\}^L \to \{0,1\}^n, L > n, \quad (7)$$

where g is called a class of second-order universal hash functions if for any fixed $x_1 \neq x_2 \in \{0,1\}^L$ with a random and equally probable choice $g \in G$ probability

$$P_r(g(x_1) = g(x_2)) = \sum_{a\in\{0,1\}^n} P_r(g(x_1) = a, g(x_2) = a) \leq 2^{-n}. \quad (8)$$

The Galois field $GF(2^L)$ is considered. Each field element $\omega \in GF(2^L)$ is brought to a single-valued correspondence with a bit vector $x \in \{0,1\}^L$: $\omega \leftrightarrow x$. The field element $g \in GF(2^L)$ is selected, following which the function (expression) g(x): $\{0,1\}^L \to \{0,1\}^n$ is considered, which assigns to each value of the argument x the first n bits of the bit vector $x' \leftrightarrow g * \omega$, which is equal to the product $g * \omega$, where * is a multiplicative field group operation. Renyi entropy properties are as follows:

$$H_2(x) = R(x) = -log_2 \sum_{k=1}^{N} p_k^2 = -log_2 \Pr(x = y). \quad (9)$$

- Renyi entropy of the second order, where random variables x,y possess the same distribution $(p_1,\ldots p_N)$ and independence, and P_r (x=y) stands for the collision probability.

$$H_{min}(x) = \lim_{\alpha\to\infty} H_\alpha(x) = -\log_2 \max_k p_k \quad (10)$$

where $H_{min}(x)$ represents minimum entropy.

Central to quantum cryptography is the secrecy enhancement lemma of 1999 (leftover–hash lemma), supported by the use of universal hash functions and the concept of Renyi entropy [26-29].

The statistical distance SD (…) between the disposals on the compressed space $\{0,1\}^n$ is estimated in terms of the probability characteristic R(x) on the original hash space $\{0,1\}^L$.

As the length L expands, given reasonable expectations concerning the observations' distribution υ=(u,b), the Renyi entropy R (x |υ) might be expected to simultaneously grow. Therefore, for a given n, it will always be possible to find a large L for which the right side in

$$\frac{1}{2}\sum_{x\in Z}\sum_{k=1}^{N} | P_{KZ}(k,z) - \frac{1}{N}P_Z(z)| \leq \frac{1}{2}\sqrt{2^{-R(X|\upsilon)+n}} \quad (11)$$

is less than ε set well in advance. When implementing the error correction procedure, Alice calculates C of linear relations over the bit sequence $x \in \{0,1\}^L$, the values of which Alice forwards to Bob through the classical open channel. The transmitted bits are represented as

$$H(x) = b \in \{0,1\}^C, C < L \quad (12)$$

where H stands for the matrix of the corresponding dimension. The value of C depends on the Q error probability. For example, x is the input, and (y, b) is the output of the communication channel, where y are the distorted bits in a slightly symmetric communication channel with distortion probability Q. In total, there are 2^L sequences x in the input. The bandwidth is equal to

$$C = \max_{P_x(x)} (H(y,b) - H(y,b|x)), \quad (13)$$

where $H(y,b), H(y,b|x)$ stands for the entropy and Shannon's mean conditional entropy, respectively.

The value of 2^C may be considered the maximum number of non-overlapping groups of sequences {y, b} at the channel output, which determines the optimal code (x, {y, b}), {y, b} represents the set of "typical" sequences generated by the sequence x.

When Condition $2^L \leq 2^C$ is true, the decoding error tends to zero at L growth. In this case, the

inequality $2^L \leq 2^C$, considering $C \leq L + C - L * h(Q)$, provides the essential condition of efficient decoding $C \geq L * h(Q)$. This estimate allows obtaining a lower bound on the number of linear relationships required to correct errors at the receiving end. For convenience, the estimates are normally presented

$$C = L * f * h(Q), \text{ where } f \geq 1. \quad (14)$$

The peculiarity is that the bit sequence $x \in \{0,1\}^L$ is not a code vector but is a slight vector chosen randomly and with equal probability. Field trials give reason to believe that at this stage, the most effective corrective codes in quantum cryptography, from the point of view of the proximity of the value f to unity, are LDPC codes, for which the value f = 1,1 ÷ 1,2 is achieved in the formula

$$C = L * f * h(Q). \quad (15)$$

The LDPC (low-density parity check) code is set by a large check matrix with a low unit density. The number of lines (the length of the syndrome) depends on the probability of the correctable error Q. The check matrix of the code H may be chosen, for example, from the matrices of the IEEE standard, where the number of columns is $L \approx \approx 2*10^3$, and the number of lines is L/3 ÷ L/2. The number of units in each row is equal to or less than 10; in the column, it is equal to or less than 15. At the same time, filling with units follows a specific method to achieve maximum efficiency in correcting errors.

Decoding for LDPC codes occurs iteratively, which means actual revaluation of the posterior probability of a single bit in the transmitted sequence (code vector) at each step, and the decision is 0 or 1, depending on whether this probability is less or more than 1/2.

This approach is generally called soft decoding. If the maximum number of iterations is reached and the test conditions are not met, then the decoding algorithm generates an error. In quantum cryptography, the classical version of the LDPC code algorithm is modified to adapt the size of the matrix H to the correctable error level Q. The specific density of information recording is described by the following function:

$$Y(a) = \frac{\ln (a)}{a} = \frac{ln(a)}{a}, \quad (16)$$

which reaches its maximum at ε = ≈ 2.718, i.e., the three-digit number system (of integers) turns out to be the best in terms of information recording density [30] – [34].

Table 2 contains the number of qubits, corresponding to the classical complexities from Table 1, of the length k of the key of a symmetric cryptosystem, the number of qubits required to solve the problem with Grover's search algorithm, and the number of quantum steps.

Table 2: Resources for the quantum solution of the problem of finding the key of a symmetric cryptosystem.

symmetric cryptosystem key	number of qubits	sq. time	middle class time
k	k	$(\pi/4)\sqrt{2^k}$	
57	57	$2{,}8 \cdot 10^8$	$6{,}39 \cdot 10^{16}$
82	82	$1{,}93 \cdot 10^{12}$	$3{,}03 \cdot 10^{24}$
113	113	$1{,}06 \cdot 10^{17}$	$9{,}20 \cdot 10^{33}$
129	129	$2{,}76 \cdot 10^{19}$	$6{,}03 \cdot 10^{38}$
258	258	$5{,}03 \cdot 10^{38}$	$2{,}05 \cdot 10^{77}$

Ternary logic may aid in improving security, which is especially important in the age of big data technology and the Internet of Things when all electronic devices are exposed to cyber-attacks. Modern ternary encryption schemes show high efficiency in solving cryptographic problems and may improve the reliability of information transmitted through insecure communication channels. They can also be used as auxiliary codes when creating legacy binary codes.

3.1 Discussion and Future Prospects

Quantum computers provide different computation results. An algorithm is said to be reliable if the desired result is found, perhaps by repeatedly running the algorithm with a sufficiently high probability. The possibility of obtaining a solution to a problem that the classical computer fails to resolve but that might be obtained with a high probability of a correct result represents, in the case of a quantum computer, a good incentive for further

research on quantum computing and practical attempts to create such a computer.

The aforementioned underlines how essentially the quantum computer differs from a classical computer, which always obtains an unambiguous result, and its correctness is determined by the correctness of the algorithm. Modern crypto algorithms used in certain digital transformation projects, such as big data and the Internet of Things may require replacement, which is associated with the allocation of additional resources and new risks (see Figure. 4).

Notably, research in the field of data representation and information coding might soon serve as the basis for shifting to a more economical ternary number system instead of the traditional binary system in the implementation of digital computing devices and systems. For example, a full-scale simulation of the quantum properties of an iron atom requires considering the motion of all its 26 electrons in three-dimensional space, for which the solution to the Schrödinger equation is needed in the configuration space of 26 * 3 = 78 dimensions (exclusive of the spins of electrons, which complexity the dynamics even further).

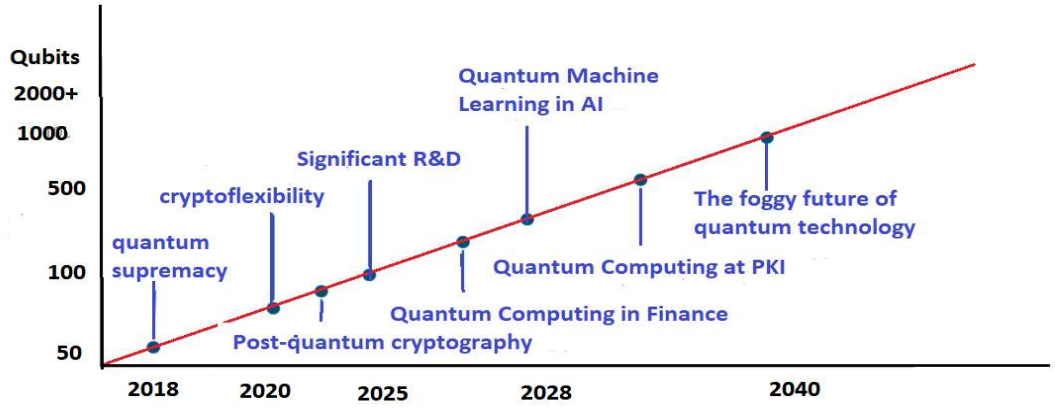

Figure 4: Compatibility of the capabilities of quantum computers and traditional cryptography [6]

Assuming a relatively coarse grid that would divide each coordinate into 10 parts only, then 10^{78} nodes are needed to implement the corresponding difference scheme. This kind of simulation, however, is impossible simply because the total number of elementary particles such as protons and neutrons in the universe is also "*simplified*" to approximately 10^{78}. Thus, modelling one atom, far from being the most complicated case, requires a resource that exceeds the mechanical potential of the entire universe. New computational approaches using quantum computing systems may shortly replace the entire algorithmic basis that has been successfully used for many decades.

Forecasts regarding the timing of the appearance of the first efficient quantum computers are also marked with a high level of ambiguity. Some of these systems are almost guaranteed to be developed privately to resolve non-public problems. Therefore, it is necessary to prepare for the transition to postquantum cryptography using the algorithm of a more economical ternary number system immediately.

Quantum computers are a security issue that society has to be ready for in advance since they can break existing encryption techniques. The impending threat to privacy and digital security emphasises how critical it is to keep up with cybersecurity best practices, particularly when safeguarding personally identifiable information. In the face of emerging technological threats, communities may better protect their encrypted data and preserve data secrecy by implementing proactive measures and embracing quantum-resistant security solutions.

3.2 Limitations

Post-quantum cryptography solutions hold significant potential in reducing risks, with research primarily focusing on the vulnerabilities introduced by quantum computing. While not extensively explored in technical aspects, this promising field could provide the reader with a sense of optimism about potential countermeasures for quantum security threats. The study analyses weaknesses in popular security protocols, including TLS, IPsec, SSH, and PGP, but it might not offer a thorough examination of all network protocols currently in use. As a result, it might overlook information on the hazards related to quantum security present in other, lesser-known protocols. This constraint may limit how broadly the results may be applied to solve

problems. The research thoroughly examines how quantum computing affects each protocol; however, it does not provide in-depth case studies or actual instances to show how adversaries might use these weaknesses with access to quantum technology. By including realistic scenarios or simulations, the paper could have increased its practical applicability and provided readers with better knowledge of the outcomes of quantum security issues. While the study emphasises the need for countermeasures to mitigate quantum security threats, it underscores the importance of offering specific advice or standards on how to do so to policymakers, protocol designers, and implementers. Providing concrete insights and practical methods could empower and equip these parties to protect the document with the necessary tools to handle quantum security threats.

4. CONCLUSIONS AND FUTURE WORK

Quantum computers based on three-digit logic technologies provide unconditional cyber security because they produce well-controlled but unpredictable results instead of pseudo-random results. According to the findings of the proposed research, security problems are solved by generating random numbers from inherently non-deterministic quantum processes that, being inherently random, provide reliable, transparent, and well-controlled unpredictable results. After that, we show ways to develop an optimisation using the theoretical foundation of the basic principles of the functioning of ternary computers, ternary logic, and arithmetic, compare ternary and binary systems, and explain how to implement structural elements using ternary technology.

The researchers completed their investigation by employing, in the future, semi-self-testing devices with ternary logic that need to be developed with the intent to balance speed and trustworthiness. We argue that while quantum security functionality will reset the innovation cycle for many common security solutions in traditional computing, the real concern is the cost of transitioning to new quantum security technologies.

By examining the emerging techniques used in research that enrich quantum security research in the age of quantum technologies, we aim to make a significant contribution to the development of effective defence strategies. It has been recommended in the current research that this process should take place in parallel in several areas of modern science and technology for which there is the necessary theoretical groundwork and a minimum experimental base available.

Although the research offers insightful information about how quantum computing affects security and suggestions for resolving quantum security issues, it highlights the need to investigate the moral or legal ramifications of implementing quantum-safe network protocols. By considering ramifications beyond technical details, it could have been possible to provide the audience with a more comprehensive understanding of the difficulties in switching to quantum-safe protocols, making them feel more informed and aware.

Further areas of research. The acceptability of the idea of algorithmic development of quantum and postquantum cryptography based on ternary logic mentioned in this article is one of the specific questions requiring a separate examination. With a few exceptions to meet national security requirements, this strategy seems appropriate for Kazakhstan.

The future direction is connecting the hybrid classical-quantum approach for developing quantum computer-means algorithms with the quantum platform, which would open unimaginable technological doors.

REFERENCES

[1]. Dr. Ian *Cutress Intel's manufacturer Roadmap from 2019 to 2029. https://www.anandtech.com/Show/15217/Intels- manaufacturn-Roadmap-fromap -2019-to-2029.*

[2]. Burg, D.; Ausubel, J.H. Moore's Law revisited through Intel chip density. *Journal PLoS ONE* 2021, vol.16 (8): e0256245, *https://doi.org/10.1371/journal.pone.0256245.*

[3]. Aktayeva, Al.; Makatov, E.; Yesmagambetova, G.; Kubigenova, A.; Niyazova, R.; Zakirova, A. Cognitive Properties of Cybersecurity: Postquantum Cryptography. *Journal of Theoretical and Applied Information Technology* 2021, vol.99(22), pp.6589-6609.

[4]. NIST. Post-quantum cryptography standardization. *https://csrc.nist.gov/Projects/post-quantum -cryptography/post-quantum -cryptography-standardization, 2022.*

[5]. Joshua J. Tom, Nlerum P. Anebo, Bukola A. Onyekwelu, Adigwe Wilfred, Richard E. Eyo Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems International Journal of Engineering and Advanced Technology (IJEAT), vol.12(5),

2023, *https://doi.org/10.35940/ijeat.E4153.0612523*

[6]. Sadullah Khan,Chintan Jain,Sudhir Rathi,Prakash Kumar Maravi,Arun Jhapate,Divyani Joshi Quantum Computing in Data Security:A Critical Assessment *https://doi.org/10.1002/9781394167401.ch22*

[7]. Fernando Javier Gómez-Ruiz, Ferney Rodríguez, Luis Quiroga and Neil F. Johnson Vulnerability of Quantum Information Systems to Collective Manipulation, Quantum Theory *https://doi.org/10.5772/intechopen.1004935*

[8]. Swaroop Ghosh,Surya Prakash Upadhyay,Abdullah Ash Saki A Primer on Security of Quantum Computing Quantum Physics (quant-ph), 2023, *https://doi.org/10.48550/arXiv.2305.02505*

[9]. Joseph J.Kearney,Carlos A.Perez-Delgado Vulnerability of blockchain technologies to quantum attacks Array,Vol. 10, 2021, *https://doi.org/10.1016/j.array.2021.100065*

[10]. Atefeh Mashatan, Ozgur Turetken Preparing for the Information Security Threat from Quantum Computers MIS Quarterly Executive vol.19(2), pp.157 -164, *https://aisel.aisnet.org/misqe/vol19/iss2/7*

[11]. 5Chen, S.; Jordan,Y.; Liu, D.; Moody R. and et al. Report on post-quantum cryptography. In Proceedings of National Institute of Standards and Technology: Internal Report, NIST.IR.8105, 2016.

[12]. Quantum technologies. In Proceedings of the Technical Report, December 2020, *https://doi.org/10.13140/RG.2.2.12246.88645.*

[13]. Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, IEEE Computer Society, Los Alamitos, CA, 1994, pp. 124–134, *https://doi.org/10.1109/SFCS.1994. 365700.*

[14]. Shor, Peter W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing* 1997, vol.26(5), *https://doi.org/10.1137/ S0097539795293172* .

[15]. Shor, Peter W. Introduction to Quantum Algorithms. 2001, *https://doi.org/ 10.48550/arXiv.quant-ph/0005003.*

[16]. Brusentsov, N.P. Three -digit dialectical logic. In Proceedings of the Software systems and tools: thematic collection 2001, vol.2, pp. 36–44.

[17]. Brusentsov, N.P. and Derkach, A.Yu. Three -digit logic, fuzzy sets and probability theory. In Proceedings of the Software systems and tools: thematic collection, series Software systems and tools 2001, vol.2, pp. 88–91.

[18]. Volovich, I.V. Quantum Computing and Shor's Factoring Algorithm. *https://doi.org/10.48550/arXiv.quant-ph/0109004*.

[19]. Razumov, P.V.; Smirnov, I.A.; Pilipenko, I.A.; Selyova, A.V.; Cherkesova, L.V. Comparative Analysis of NTRUEncrypt Modified Post-Quantum Cryptographic System and Standard RSA Cryptosystem. *Journal Vestnik of Don State Technical University* 2019, vol.19(2), pp.185-194, *https://doi.org/10.23947/1992-5980-2019-19-2-185-194.*

[20]. Proos J. and Zalka, Ch. Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves. *Journal Quantum Information & Computation 2003,* vol.3(4), pp.317-344, *https://doi.org/ 10.48550/arXiv.quant-ph/0301141.*

[21]. NIST. Revised Draft of Key Management Guideline, Second Key Management Workshop, *http://csrc.nist.gov/encryption/ kms/,* 2001.

[22]. Beauregard, S. Circuit for Shor's Algorithm Using 2^{n+3} Qubit. *Journal Quantum Information and Computation* 2003, vol.3(2), pp.175-185, *https://doi.org/10.48550/arXiv.quant-ph/0205095.*

[23]. Arbekov, I. M. and Molotkov, S. N. Secret keys agreement in communication networks with quantum key distribution and trusted nodes. *Laser Physics Letters* 2020, vol. 17(5), 055202, *http://dx.doi.org/ 10.1088/1612-202X/ab77ce*

[24]. Kuriyama, K.; Sano, S. and Furuichi, S. A Precise Estimate of the Computational Complexity in Shor's Factoring Algorithm. *Applied Mathematics and Information Science* 2007, vol.1, pp.313-322, *https://Arxiv.quant-ph/0406145.*

[25]. Lenstra, A.K. and Lenstra, H.W. The Development of the Number Field Sieve. *Lecture Notes in Mathematics* 1993, *https://doi.org/ 10.1007/BFb0091534*.

[26]. Coppersmith, D. An Approximate Fourier Transform Useful in Quantum Factoring. In Proceedings of the IBM Research Report RC 1994, 19642.

[27]. Portmann, C. and Renner, R. Security in quantum cryptography. *Reviews of Modern Physics* 2022, vol.94(2), 025008, *https://doi.org/10.1103/revmodphys. 94.025008.*

[28]. Lenstra A.K. and Verheul, E.R. Selecting Cryptographic Key Sizes. In Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000, Lecture Notes in Computer Science, 2000, vol. 1751, Springer, Berlin, Heidelberg, *https://doi.org/10.1007/978-3-540-46588-1_30.*

[29]. Vasilenko, O.N. *Theoretical and appropriate algorithms in cryptography*, Moscow, MCNMO, 2003.

[30]. Grover, Crying K. Quantum mechanics helps to find a needle in a haystack. *Physic Review Letters*, 1997, vol.79(2), pp.325-328, *https:// doi:10.1103/ Phys RevLett.79.325.*

[31]. Zhandry, A note on the quantum collision and set equality problems. In Proceedings of Quantum Inf. Comput. 2015, vol.15, no. 7-8, pp.557–567.

[32]. Ampatzis, M. and Andronikos, T. QKD Based on Symmetric Entangled Bernstein-Vazirani. *Entropy* 2021, vol.23 (7), 870, *https:// doi.org/10.3390/e23070870.*

[33]. Djordjevic, I.B. Quantum information processing, quantum computing, and quantum error correction: an engineering approach. 2nd ed., Elsevier/Academic Press: London, UK; San Diego, CA, USA, 2021, ISBN 978-0-12821-987-4

[34]. Lizama-Pérez, L.A.; López, R.J.M. and Samperio, E.H. Beyond the Limits of Shannon's Information in Quantum Key Distribution. *Entropy* 2021, vol.23 (2), 229.