DOI 10.1007/s10559-019-00107-w
Cybernetics and Systems Analysis, Vol. 55, No. 1, January, 2019

QUANTUM COMPUTING: SURVEY AND ANALYSIS

M. M. Savchuk[1†] **and A. V. Fesenko**[1‡]

UDC 004.383

Abstract. *The authors survey and analyze the main concepts and postulates of the quantum computing model, efficient quantum algorithms, and recent results, capabilities, and prospects in constructing a scalable quantum computer. A certain class of algebraic problems in the quantum computing model is considered for which there exists an efficient quantum solution algorithm. A detailed analysis of available quantum computer implementations was carried out, and it is shown that sufficient progress has not yet been made in constructing a scalable quantum computing device; nevertheless, most researchers expect that a full-fledged quantum computer will be created in the next 10–15 years.*

Keywords: *quantum computing model, quantum cryptography, quantum computer, efficient quantum algorithm, postquantum cryptographic primitive.*

INTRODUCTION

We are fortunate to be witnesses and contemporaries of great theoretical discoveries and practical inventions and achievements in the information sphere, which have changed our whole life, our world, and its understanding. It is even hard to imagine what new changes are awaiting us already in the near future owing to new achievements in the field of telecommunication and classical computer and quantum computing.

It is obvious that the level of development of society in the economic and other spheres of its life directly depends on the amount of information that can be actively used by different layers of society and on the ability to efficiently store it and to quickly process and transmit it. Recall that the levels of development of a society were also closely associated earlier with information revolutions. In particular, the formation of the tribal way of life is connected with the origin and development of languages and language communication; the creation of states of the ancient world took place simultaneously with the invention and development of writing systems that allowed to realize long-term information storage on material carriers and to efficiently transmit it in space and time; the European renaissances and industrial revolution are connected with book-printing, which tens of thousands of times increased the amount of information used. According to different estimated data, the approximate amount of information used by society after these information revolutions amounted to 10^9, 10^{11}, and 10^{17} information bits.

At the beginning of the modern information era, the first electronic digital computer ENIAC (1945) weighed 27 tons, consumed 174 kW, and had a memory size of 20 numbers-words and a clock frequency of 100 kHz. It is interesting that, four years later, in the book "Popular mechanics" of 1949, the following forecast was given: "Computers of the future can weigh no more than 1.5 tons." Today, the miniaturization and operation speed of digital computing devices have reached a level that makes it possible to speak about intelligent systems with almost fantastic capabilities, and the boundary in this direction has not yet been reached. Assume that the size of a processor will reach the size of a hydrogen atom with its diameter of an order of 10^{-10} m. Then the frequency of such a processor will be no more than

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," Kyiv, Ukraine, [†]*mikhail.savchuk@gmail.com*; [‡]*andrey.fesenko@gmail.com*. Translated from Kibernetika i Sistemnyi Analiz, No. 1, January–February, 2019, pp. 14–29. Original article submitted September 9, 2018.

 1060-0396/19/5501-0010

the number of times the light passes through one atom in 1 second, which will be equal to $3 \cdot 10^{18}$ operations per second or approximately 10^{26} operations per year. This is not enough to break, for example, an asymmetric RSA cryptosystem with a modulus length of 1024 bits. And an RSA cryptosystem with a modulus length of 2048 bits will not be broken even by such a computer for a billion years of continuous operation. At the same time, here, as well as in problems with an exponential growth of complexity in the general case, parallelization will not help. At present, the operation speed of the fastest supercomputers is close to 10^{17} flops. Will humankind be restricted in calculations to only problems of polynomial complexity?

An alternative computing model is the quantum computing model, which can be fully applied in practice after the creation of a scalable quantum computer. This article analyzes basic theoretical concepts, ideas concerning the substantiation of quantum computing, and perspectives of construction of a scalable quantum computer.

1. QUANTUM CRYPTOGRAPHY

Quantum computing is considered to be not only computing on a quantum computer. This sphere also includes quantum cryptography, quantum teleportation, and other directions. In the traditional cryptography, information carriers during transition are pulses of current and light, bundles of radio waves, and, after all, paper and other material objects. To represent and code one bit of information, a great many of electrons, photons, radio waves, and particles are always used. To code one bit in quantum cryptography, the quantum state of one elementary particle (atom, ion, electron, or photon) or their pair is usually used.

Unlike traditional cryptography, which uses mathematical methods for transforming texts and messages to ensure their protection from the intruder and to preserve the secrecy of information, physical laws and laws of quantum mechanics are used as the basis of quantum cryptography for information protection, and information is coded and transferred using objects of quantum mechanics, for example, electrons in an electric current or photons in fiber-optic communication lines. The reception of messages or wiretapping (interception of a message) can be considered as measuring definite parameters of quantum objects-carriers of information.

The idea of protecting information using quantum objects was first proposed by S. Wiesner in 1970. The first and most well-known protocol BB84 of quantum cryptography proposed by C. Bennett and G. Brassard in 1984 and based on S. Wiesner's ideas makes it possible to solve the following problem of symmetric cryptography: the transfer of a secret key using only open communication channels [1]. In the 70s of the XXth century, owing to the rapid development of computer networks, telecommunication channels, exponential growth of the amount of information, and the need to protect information in almost all areas, the transfer of keys by special closed channels became a problem that seemed unsolvable. In 1976, U. Diffie and M. Hellman clearly formulated the concept of a hardly invertible function and a hardly invertible function with a trapdoor and proposed a new conception in cryptography, namely, asymmetrical cryptography or cryptography with public keys. It is the public key distribution protocol for open channels that was the first protocol of asymmetrical cryptography, and such keys were used in symmetric cryptography for cryptographic information security transformations. The quantum key distribution protocol is constructed based on other principles.

The task of quantum key distribution protocol BB84 is to transmit a random sequence of zeros and ones from a sender A to a receiver B without using closed channels, and then the users A and B choose the secret key from this sequence. A binary random sequence that is generated by the sender A and in which each character 0 and 1 is encoded by the direction of polarization of a single photon (the direction of oscillations of the electric field of the photon) is transmitted by a sequence of photons via a fiber-optic line. The direction of polarization of photons can be controlled and measured, for example, with the help of optically active crystals.

A sequence of bits is transmitted by a sequence of photons in the rectangular or diagonal basis selected randomly by the sender A for each bit. In the rectangular basis, 0 or 1 are encoded by the horizontal and vertical direction of polarization of a photon, and, in the diagonal basis, they are encoded with a slope at an angle of 45 and of 135 degrees. In fact, before a measurement, information is in quantum bits called qubits, and only after the measurement turns into usual classical bits. For measurement, the receiver B randomly chooses its sequence of bases. If the bases of the users A and B coincide for a separate photon, then, during measurement, B will obtain the same character of the sequence (0 or 1) that was sent by the user A. If the bases of A and B do not coincide, then the corresponding characters for A and B will

be the same with a probability of 0.5 according to the laws of quantum physics. After measurement, A and B use any open channel and find out which of their bases have coincided. In the absence of wiretapping by the intruder, the users A and B will have, on the average, 50% of identical characters of the initial sequence from which secret keys for the symmetric encryption systems of the users A and B are chosen.

The cryptographic resistance of the quantum protocol for transmitting a secret key is stipulated by the following fact: a connection to a fiber-optical line and wiretapping by an unauthorized person can be guaranteedly revealed by the users A and B. This, in turn, is ensured by the laws of quantum mechanics and the exchange of some specializing information between A and B after quantum transmission using any open channel. The intruder does not know the bases selected by the user A and, therefore, during wiretapping, also the characters of the receiver B will be disfigured that must coincide under the condition of selection of identical bases by the users A and B, which will be revealed by the users. In this case, the sequence received by the users A and B is not used. If there was no wiretapping attempt, then a part of the sequence can be used as a secret key (known only to the sender and receiver) and can be applied later on in symmetric cryptosystems.

The quantum protocol was first implemented on a physical device in 1989 with transmitting at a distance less than one meter. Later on, the transmission range has been repeatedly increased. At present, it is assumed that transmission is sufficiently stable at a distance, as a rule, up to 200 km. The transmission range is mainly bounded by the damping of light signals in fiber-optical cables, loss of photons, and also external noises.

With the advent of quantum cryptography, its enthusiasts predicted that quantum cryptography will soon create competition with “usual” cryptography and will even be more reliable and efficient. But so far this has not happened primarily due to a number of technical difficulties. In particular, for example, whereas in classical information transmission by fiber-optical channels, electronic or optical amplifiers are necessarily placed every few tens of kilometers, it is impossible to do this in quantum protocol BB84 since it is impossible to reproduce the state of a photon after measurement according to the quantum laws if the bases of the sender A are not known. This immediately imposes tight constraints on the transmission range. To date, the longest distance achieved in the case of transmission through fiber-optical channels according to the quantum protocol amounts to 404 km.

Another type of the quantum cryptography protocol is based on entangled quantum states of two particles, for example, photons. At present, different countries conduct intensive investigations of quantum communication and quantum cryptography protocols using artificial satellites. The range of quantum transmissions using satellites reaches hundreds of kilometers and even exceeds thousands of kilometers. This opens up new prospects for the development of quantum communication and quantum cryptography.

2. BASIC CONCEPTS OF THE QUANTUM COMPUTING MODEL

2.1. Chronology of Ideas and First Postulates. In [2], nine classical works in the field of quantum computers and quantum computing are presented including works of D. Deutsch, R. Jozsa, and P. Shor that are devoted to investigating efficient quantum algorithms. Let us briefly mention the following main stages of the theory of constructing a quantum computer and quantum algorithms:

- 1980 — Yu. I. Manin advanced the idea of quantum automata in the preface to the book “Computable and non-computable;”
- 1982 — P. Beniof and R. Feynman analyzed physical constraints and the possibility of construction of a quantum computer (a quantum simulator);
- 1985 — D. Deutsch gave a concrete form to the R. Feynman idea, namely, efficiency in the case of quantum parallelism;
- 1992 — D. Deutsch and R. Jozsa proposed an algorithm for solving the problem of distinguishing (recognizing) a constant Boolean function of n variables from a balanced one using n operations on a quantum computer;
- 1994 — P. Shor developed factorization and discrete logarithmization algorithms that allow to solve corresponding problems in polynomial time on a quantum computer;
- 1996 — L. Grover developed a quantum algorithm for searching in an unordered set, in particular, his algorithm provides a solution to the exhaustive search problem, for example, finding a solution of the equation $f(x)=1$ for a Boolean function f of n variables in $O(2^{n/2})$ calls of the function f using $O(n)$ qubits.

The monographs [2–4] presents detailed information on the mentioned stages of development, basics of the theory of quantum computing, modern investigations, prospects for constructing a quantum computer, and possible implications for society and understanding of physical and information processes. A short description of the results of investigations of the Kiev School of Theoretical Cryptography in this area is given in [5].

2.2. Quantum States and a General Conception of Quantum Computing.

One-qubit quantum system. In a quantum computer, information unit is qubit (quantum bit) whose physical implementation is described by a wave function of probabilities in a two-dimensional Hilbert space.

One classical bit can be only in one of two states denoted (encoded) by 0 and 1. The state of a quantum bit (qubit) is described using the Dirac bra-ket notation with the help of the expression $|\psi\rangle = a|0\rangle + b|1\rangle$, where a and b are complex numbers and $|a|^2 + |b|^2 = 1$. So to speak, a qubit simultaneously is in all points of space but with different probability. As a result of qubit measurement that is actually the projection on orthogonal subspaces, we obtain the following coded value of the classical bit: 0 with probability $|a|^2$ or 1 with probability $|b|^2$. Thus, after measurement, a qubit immediately assumes one of the basis states that corresponds to the classical result. For example, after measuring the qubit described by the state $|\psi\rangle = \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$, we obtain the corresponding value 0 with probability 0.36 and value 1 with probability 0.64.

Quantum system with two and more qubits. The state of a system consisting of two qubits can be written mathematically as a unit vector in a 4-dimensional Hilbert space as follows: $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, where a, b, c, and d are complex numbers and $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. The basis quantum states are $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ that correspond to the four classical values 00, 01, 10, and 11 each of which has the probability $|a|^2$, $|b|^2$, $|c|^2$, and $|d|^2$, respectively, after complete measurement. By analogy, a system containing N qubits is described in a 2^N-dimensional Hilbert space and has 2^N basis states that correspond to 2^N classical values. Thus, the result of complete measurement of an N-qubit quantum system is one of 2^N different classical values whose total number exponentially increases with the number of qubits and each value can be obtained as a result of measurement with some probability. Let there be a sequence of transformations of a quantum system that can be implemented physically and such that it considerably increases the probability of the state that corresponds to the sought-for solution to this problem. Then, after repeated implementations and measurements, such a quantum system can find the solution with high probability to a problem that is possibly unsolvable by the classical computer.

General conception of quantum computing. A simplified computation scheme can be described as follows. A system with a sufficient number of jointly operating qubits is set to a definite initial state corresponding to the conditions of a problem. Then the state of the system or its subsystems is changed using a sequence of transformations to which correspond unitary transformations in the mathematical model in the Hilbert space (unitary matrices). In a certain sense, a quantum system simultaneously performs computations with all possible classical states whose number exponentially increases with increasing the number of qubits, and the answer is a unified classical value. After applying all unitary transformations, as a rule, the system state is measured and the obtained classical value is the result of computations. The quantum system usually yields the correct result only with a definite probability. To increase the confidence probability, computations and the corresponding measurements are repeated the necessary number of times. If errors do not increase very quickly during measurement (for example, exponentially with increasing the number of qubits), this probability can be made arbitrarily close to 1. It may be said that this quantum system is an analog of a quantum computer.

This conception of a quantum computer and quantum gates, i.e., simple unitary transformations that correspond to logical operations in the classical computer, was proposed by D. Deutsch in 1989. In 1995, D. Deutsch invented a universal logical block that makes is possible to execute any quantum computing. It turns out that, to construct an algorithm for any computation, it suffices two basic operations, i.e., quantum gates.

Theoretically, a quantum computer allows to execute intuitively understandable algorithms just as the classical computer. According to the Grover result, the complexity of any computing task performed using a quantum computer, can be decreased by at least a square root compared to the complexity of this task performed on the classical computer, and some exponentially complex problems can be solved in polynomial time. Unfortunately, to date, a small number of problems are known whose solution using a quantum computer can give a significant gain. These problems include the problems of factorization and discrete logarithmization whose complexity underlie the cryptoresistance of about 95% of implementations of algorithms and protocols of asymmetrical cryptography.

The main problems in constructing a quantum computer are as follows:

— the possibility in principle to construct a scalable quantum computer;

— instability (decoherence) because of the influence of external environment;

— a physical implementation of a scalable quantum computer with a sufficient (for practical problems) number of jointly operating qubits;

— the uncertainty of the degree of dependence of errors since a very fast accumulation of errors with increasing the number of qubits will give no way to obtain the sought-for result when executing computations with an acceptable number of repetitions;

— the construction of new mathematical algorithms that will allow to considerably accelerate computations and the search for solutions for a wide class of problems.

2.3. Basic Mathematical Concepts of the Quantum Computing Model. The basis of a quantum computer is a quantum-mechanical system that is necessarily isolated from its environment in such a way that its behavior could be externally controlled, but any event that is not associated with control procedures cannot change this behavior.

A model for such a system is created according to the following postulates [6]:

— the state space of this system is the vector space over the field of complex numbers with a defined scalar product (a Hilbert space), which is associated with an isolated quantum-mechanical system; the system state at any instant is completely described by the state vector that is a unit vector in the state space;

— the evolution of a state (a state change) of the closed quantum mechanical system is described only by a unitary transformation. If the system is at a state $|\psi_1\rangle$ at an instant of time t_1 and at a state $|\psi_2\rangle$ at an instant of time t_2, then these states are connected by a unitary transformation U that depends only on the moments t_1 and t_2 and is such that $|\psi_2\rangle = U|\psi_1\rangle$;

— a measurement of a quantum system is composed of a set of linear operators that act on the state space of the system and are actually a projection onto orthogonal subspaces;

— the state space of such a complex quantum-mechanical system is the tensor product of the state spaces of its components.

Consider the concept of parallel quantum computing. The family of functions described below is the main tool in operations of this scheme.

Definition 1. The Walsh–Hadamard one-qubit transformation is the unitary operator H that acts on a one-qubit system and is specified by the relations $H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

The operator H can be briefly written in the form $H(|x\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{k=0}^{1}(-1)^{kx}|k\rangle$. Direct calculation also allows to check that the operator H is involutive, i.e., $H^2 = I_2$. Moreover, if complex coefficients are ignored, then H is a symmetric mapping with respect to the straight line that forms an angle of $\frac{\pi}{8}$ with the $|0\rangle$-axis.

Note that the Walsh–Hadamard n-qubit transformation H_n is defined as $H^{\otimes n}$ (the operation $\otimes$ signifies tensor product). Since H is an involutive operator, we have $H_n^2 = I_2^{\otimes n} = I_{2^n}$, i.e., H_n also is an involutive operator. In the case of applying to the state $|0\rangle^{\otimes n}$, the operator H_n generates a homogeneous linear combination of integer numbers from 0 to $2^n - 1$, i.e., $H_n(|0\ldots0\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$.

The Walsh–Hadamard transformations allow to prepare input data for parallel computing. Let us consider the procedure of computation as such. Let $f: Z_2^m \to Z_2^k$ be some function that is not necessarily invertible. Since the invertibility of the function f is not required, it is impossible to use it in this form as a transformation in a quantum computer. However, owing to the use of a definite additional memory size, it is possible to create a unitary transformation for modeling the function f. To this end, a quantum system V is required that is the tensor product of an m-qubit and a k-qubit quantum systems. Recall that the system V has a basis composed of vectors $|x\rangle \otimes |y\rangle$, where x and y are binary representations of integer numbers in Z_2^m and Z_2^k, respectively. We define a linear transformation $U_f: |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle$, where $\oplus$ denotes the addition

operation in the group Z_2^k (well-known also as *XOR*). For a fixed value of x, the quantity $y \oplus f(x)$ assumes each value in Z_2^k exactly once since y assumes values from Z_2^k. Therefore, the result of the transformation U_f is simply a permutation of all 2^{m+k} elements of the basis V, and this means that it is unitary. Moreover, $U_f(|x\rangle \otimes |0\rangle) = |x\rangle \otimes |f(x)\rangle$. In this regard, U_f models the computation of the value of the function f. Such a mapping U_f is called the standard oracle for the function f. Thus, a standard oracle can be used to model any function, invertible or not, on a quantum computer. In turn, this implies that any function that can be computed using the classical computer can also be computed with the help of a quantum computer.

In the case when the function f is bijective (and only under this condition), a simpler and more obvious oracle $|x\rangle \to |f(x)\rangle$ can be defined. It is called a minimal or erasing oracle for f (there is a problem for which it is shown that the use of such a minimal oracle to solve it is exponentially more advantageous as to the amount of resources than the standard oracle).

This can be considered as the simultaneous computation of the function f for all possible values of the argument x, though the fact that $|f(x)\rangle$ is related to the state $|x\rangle$ for all x can sometimes create difficulties. The formation of a state of this form is often called quantum parallelism. It is a simple and standard first step in many cases of quantum computing. The most difficult stage is the obtaining of useful information from this (extremely intricate) resulting state.

Likewise the classical computing model, a model of any quantum circuit can be created using only simple unitary transformations (i.e., quantum gates) of the vector space. Each quantum gate operates with only several qubits at a time. In a quantum model, there are finite collections of gates that allow to construct an arbitrary unitary transformation with desirable accuracy. A. Kitaev showed that such an approximation can be performed with a minimal increase in the resources being used [7], i.e., in a quantum model, all computations can be simulated using a definite collection of simple circuits. Moreover, in [8], A. Yao showed the equivalence of a model using circuits and the quantum Turing computer proposed by D. Deutsch. As well as in the classical computing model, efficient computations in the quantum model are those that can be performed using a polynomially bounded sequence of elementary gates.

Definition 2. The size of a quantum circuit (transformation) is the minimum number of elementary operations over a fixed collection of simple gates that is required to construct this circuit (transformation).

In this way, the complexity of quantum operations or transformations can be estimated. Moreover, this estimate is not qualitatively changed in the case of replacing a collection of forming gates with another generally accepted collection.

It is precisely efficient quantum computing that is of main interest. As a rule, quantum computing is composed of the following two parts that rather often are independent: an efficient quantum process and efficient classical data processing that are obtained as a result of performed measurements during the quantum process.

Quantum computers are probabilistic by nature. Therefore, the absolute majority of algorithms are also probabilistic, but this is sufficient to efficiently solve a problem (under the condition of the efficiency of a probabilistic algorithm). It suffices to make an experiment several times and to determine its final result from the majority of the experimental results. This approach can guarantee the right answer with probability arbitrarily close to 1.

3. EFFICIENT QUANTUM ALGORITHMS

To date, the hidden subgroup problem is a successful combination of examples of problems that can be efficiently solved using a quantum computer, unlike the existing algorithms for the classical computer; this was first noted in [9].

Problem 1 (hidden subgroup problem (HSP)). Let the set of generators of a group G, some finite set X, and a mapping $f: G \to X$ be given under the additional condition that there is a subgroup $H \subseteq G$ such that, for arbitrary elements $g_1, g_2 \in G$, the identity $f(g_1) = f(g_2)$ holds if and only if $g_1 H = g_2 H$ (under such conditions, we say that the mapping f hides the subgroup H). It is necessary to find the set of generators of the subgroup H with the help of calculating the function f.

Comment 1. The special case of the hidden subgroup problem when the group G is Abelian is called the Abelian hidden subgroup problem.

Statement 1 [7]. If, under the conditions of Problem 1, the function f is efficiently computable in the classical computing model and the group G is Abelian, then there is an efficient algorithm for solving this problem in the quantum computing model.

In [7], A. Kitaev singled out the property of the commutativity of a group as a sufficient condition for the existence of an efficient solution to Problem 1 in the quantum computing model. Until now, in most of the works on proving the existence of an algorithm designed for solving a certain problem and efficient in the quantum computing model, its reduction to the Abelian hidden subgroup problem, i.e., to Statement 1, is used.

The main problem is the construction of quantum algorithms such that the processing of the results of recovery of the hidden subgroup is performed in polynomial time on the classical computer. In the Abelian case, the Euclidean algorithm and an efficient algorithm for solving a system of linear equations make it possible to do this.

The difference between quantum computing and a probabilistic solution method is only that the matrices of transformations in the quantum case may contain arbitrary complex numbers but, in the probabilistic case, only non-negative real numbers, and unitary transformations preserve the vector norm in the space L_2 and probabilistic transformations preserve it in L_1.

D. Deutsch was the first to show that, possibly, the quantum computing model has an advantage over the classical model. But it should be noted that the point is that the complexity is estimated relative to the number of requests to the oracle computing the function being investigated. A function $f: Z_2 \to Z_2$ is called constant if $f(0) = f(1)$ and balanced if $f(0) \neq f(1)$. Let some function $f: Z_2 \to Z_2$ be given with the help of an oracle. Using requests to the oracle for computing function values, it is necessary to determine its type. In the case of using classical deterministic computations, two requests to the oracle should be made, and, in the quantum computing model, it suffices to make one request.

The above problem is generalized in [10] where functions $f: Z_2^m \to Z_2$, $m \in N$, are considered. A function f is called balanced if the cardinalities of the preimages of 0 and 1 are identical and constant if the values of the function f are the same on the entire domain of definition. The Deutsch–Jozsa algorithm in the quantum computing model allows to distinguish between these two cases using one request to the oracle for computing the function f [10]. This problem is a particular case of hidden subgroup Problem 1 where the group $G = Z_2^m$, set $X = Z_2$, and the mapping $f: Z_2^m \to Z_2$ hides the subgroup H that coincides with the group G when the function f is constant and contains a half of elements of the group G when the function f is balanced. When $m = 1$, the problem is reduced to the original Deutsch problem.

In 1993, E. Bernstein and U. Vazirani considered the following problem: for a mapping $f: \{0,1\}^n \to \{0,1\}$, it is known that there is a value of $a \in \{0,1\}^n$ such that $f(x) = a \cdot x$ for all values $x \in \{0,1\}^n$, where the operation "$\cdot$" is the designation of the sum modulo 2 of products of the corresponding bits (similar to the scalar product over Z_2), and it is necessary to find an unknown value of a. This problem was efficiently solved in the quantum computing model using one request for computing the function f, though, in the classical computing model, n requests are required. The Bernstein–Vazirani problem also is a particular case of the Abelian hidden subgroup problem when the group $G = Z_2^n$, set $X = Z_2$, and the mapping $f: Z_2^n \to Z_2$ hides the subgroup $H = \{y \mid a \cdot y = 0\}$.

In 1994, D. Simon considered a mapping $f: Z_2^m \to Z_2^m$ about which it is well known that all values of $f(x)$, $x \in Z_2^m$, are different (case 1–1) or there is a value $s \in Z_2^m$ such that, for arbitrary elements $x, y \in Z_2^m$, the equality $f(x) = f(y)$ holds if and only if $x = y$ or $x = y \oplus s$ (case 2–1). He proposed a quantum algorithm for solving the problem of distinguishing between these cases using at the average $O(m)$ requests to the oracle for computing the function f (later on, G. Brassard and P. Hoyer improved the result $O(m)$ requests at the average up to $O(m)$ requests in the worst case). For any algorithm, even probabilistic, in the classical computing model, the required number of requests to solve this problem equals $\Omega(2^{m/2})$. Hence, it is the Simon quantum algorithm that was the first algorithm that solved a definite problem exponentially faster than any algorithm in the classical computing model in terms of the necessary number of requests to the oracle. The considered problem is a particular case of hidden subgroup Problem 1 where the group $G = Z_2^m$ with the operation $\oplus$, the set $X = Z_2^m$, and the mapping $f: Z_2^m \to Z_2^m$ hides the subgroup H that coincides with the trivial $H = \{0\}$ in case 1–1 and with $H = \{0, s\}$ in case 2–1.

In 1994, P. Shor published [11], which until now is one of the greatest results of investigating the quantum computing model. In [11], polynomial algorithms for solving problems of factorization of integer numbers and discrete

logarithmization in the quantum computing model are presented. More precisely, in [11] and in the next work [12] published in 1997, P. Shor used the well-known reduction of the problem of factorization of an integer number $n \in N$ to the problem of searching for the exponent δ to which belongs a randomly chosen integer number $1 < a < n$ modulo n.

The problem of searching for exponent, discrete logarithmization problem, and other mentioned problems are reduced to the Abelian hidden subgroup problem, which allows to use Statement 1.

Despite the fact that quite a lot of effort was applied to search for efficient quantum solutions of the hidden subgroup problem for non-Abelian groups G, almost all well-known quantum algorithms with polynomial time were found for groups very close to Abelian. A whole class of problems was proposed that are similar to the hidden subgroup problem and, as a result, are related to it.

Problem 2 (hidden shift problem or hidden translation problem, DHSP) [13]. Let the set of generators of a group G and two injective functions f_0 and f_1 be given that map the group G into some set X with the additional condition that there is an element $u \in G$ that is called a shift and is such that, for any value of $g \in G$, the relation $f_0(g) = f_1(g \circ u)$ holds. It is necessary to find an unknown value of the shift u using the computation of the functions f_0 and f_1.

Statement 2. The Abelian hidden shift problem for a cyclic group Z_N is equivalent to the hidden subgroup problem for a dihedral group D_N.

The considerable flexibility of the statements on the hidden subgroup and hidden shift problems allows to use them in solving a rather large number of different problems, for example, as was done in [14] for some problems of combinatorial group theory.

4. OVERVIEW OF EXISTING IMPLEMENTATIONS OF QUANTUM COMPUTING DEVICES

The construction of a sufficiently powerful quantum computer in the form of a real physical device is one of fundamental problems of the modern physics. To date, there are only limited implementations of quantum computing devices.

It is well known that there are the following two main types of implementations of quantum computing devices: universal (for example, the 50-qubit quantum computer of IBM) and non-universal (for example, devices of the D-Wave company). The main distinction is that universal quantum computing devices are developed with a view to executing arbitrary allowed operations and solving arbitrary problems. Non-universal computing devices are created to solve some limited class of problems, for example, to optimize definite machine learning algorithms.

According to D. DiVincenzo, there is a certain collection of requirements on a real universal quantum computing device, namely,

— scalability (the possibility to increase) of the number of qubits;

— possibility to initialize quantum registers (qubits) to any start state;

— ability of quantum gates to operate throughout a time smaller than the decoherence time;

— implementation of the complete set of (Turing) gates;

— ability of reading information from quantum registers.

Among the main technologies of implementing a quantum computing device, the following ones should be single out:

— solid-state quantum points (the logical qubit is the direction of the electronic or nuclear spin at a quantum point, and control is performed using external potentials or a laser pulse);

— superconducting elements (the logical qubit is the presence or absence of the Cooper pair in a definite area, and control is performed with the help of an external potential or a magnetic flux);

— ions in vacuum Raphael traps (the logical qubit is the ground or excited state of an outer electron in an ion, and control is performed using laser pulses);

— using entangled states of photons.

The main problems in constructing sufficiently large quantum computing devices are external influences that can destroy the state of a quantum system or considerably distort it and errors arising during measurements and execution of elementary transformations.

As long ago as 2007, the young Canadian company D-Wave (https://www.dwavesys.com/) announced the creation of a 16-qubit quantum computer. The computer could solve sudoku puzzles and other tasks of pattern search.

The researchers claimed that they will be able to create practical systems by 2008. Sceptics immediately objected that the creation of practical quantum computers will require several more decades.

At the end of 2007, it was reported about the 28-qubit quantum processor Orion. Already on May 11, 2011, the new processor One was announced, which was called "the first commercial quantum computer" and operated on a 128-qubit chipset. In 2012, it was claimed in [15] that the company D-Wave Systems has constructed a quantum device operating with 84 qubits. In the same year, the quantum computer Vesuvius (or D-Wave Two) with 512 qubits was announced, and the D-Wave 2X version with 1152 qubits was created on August 20, 2015.

On January 24, 2017, the company D-Wave Systems Inc. published the report according to which the company Temporal Defense Systems Inc. (TDS, http://temporaldefense.com), which is engaged in the cyber protection of state and commercial organizations, became the first buyer of the future new D-Wave 2000Q device that costs 15 million dollars and operates with 2000 qubits.

Despite implicit proofs of existence of entangledness in the process of computation of the D-Wave device, which are given in some works, most researchers do not recognize the D-Wave device as a quantum one. Though it is shown that some well-known quantum algorithms such as the Simon and Bernstein-Vazirani algorithms can be used in the adiabatic quantum model, but there are no messages on attempts to do this on D-Wave devices. Moreover, the above-mentioned company emphasized that the Grover and Shor algorithms cannot be implemented on D-Wave devices.

In 2015, researchers of the Google company claimed (without direct evidences) that, according to their investigations, D-Wave devices use quantum effects, but, in this case, in the so-called "1000-qubit" computer, qubits are actually clustered by 8 qubits in each cluster. In [16], the entire available information on D-Wave devices was analyzed, and, as a result, it was concluded that D-Wave devices do not provide any computational advantage over the classical computer.

In 2001, scientists from the IBM company announced successful testing of a quantum computer with a capacity of 7 qubits (3 qubits in the first register and 4 qubits in the second register) implemented based on the phenomenon of nuclear magnetic resonance. They factorized the number 15 using Shor's algorithm.

In 2007, a group of scientists of the University of Queensland reported on an experimental demonstration of execution of Shor's algorithm using quantum logical gates based on photon polarization. For demonstration purposes, the number 15 was also factorized using 7 qubits (3 qubits in the first register and 4 qubits in the second register).

In the same 2007, scientists of the University of Science and Technologies of China also reported on an experimental demonstration of the implementation of Shor's algorithm using photon-based quantum logical gates. They also factorized the number 15 using only 6 qubits (2 qubits in the first register and 4 qubits in the second register).

In 2009, a successful experimental demonstration of Shor's algorithm using an integrated waveguide based on a silicon chip is described. Four qubits based on photons were used to factor the number 15 as follows: 1 qubit in the first register and 3 qubits in the second register.

In 2012, a group of researchers of the University of California reported on a new experimental demonstration of Shor's algorithm using phase qubits and superconducting wave resonators. This group also factorized the number 15 using 4 qubits as follows: 2 qubits in the first register and 2 qubits in the second register.

Also in 2012, E. Martin-Lopez et al. presented an experimental demonstration of Shor's algorithm for factoring the number 21 using only two photon-based qubits.

In 2012, a quantum algorithm for factoring integer numbers based on nuclear magnetic resonance was experimentally demonstrated by factoring the number 143 using 4 qubits and the adiabatic approach. The main distinction of this work is the implementation not Shor's algorithm but its alternative, namely, the transformation of the problem of factorization of integer numbers into an optimization problem. This idea was first presented by K. Burgess in 2001 and was improved by G. Schaller and R. Shutzhold in 2010.

In 2015, a group of researchers led by T. Montz reported on a new experimental demonstration of Shor's algorithm using ion traps to decompose the number 15. To this end, five $^{40}Ca^{+}$ ions in a linear Paul trap were used. A scalable scheme of Shor's algorithm with a reduced number of qubits was used, namely, 1 qubit in the first register and 4 qubits in the second register.

The above works describe real experimental demonstrations of implementing Shor's algorithm, and the results of N. Dattani and N. Bryans [17] are representative in this case. In the first edition, the paper was called "Quantum factorization of 44929 with 4 qubits" and contained information on the decomposition of the numbers 3599, 13081, and 44929 with the help of a quantum algorithm that uses 4 qubits. The third edition of [17] was called "Quantum

factorization of 56153 with 4 qubits" and contained information on the factorization of a larger number, 56153, and, additionally, the number 11663. These results may be considered as a peculiar kind of record achievement since previous works described the factorization of much more smaller numbers. The peculiarity of this work is that the authors did not make any new experiments but only used previous experimental results and showed that it is possible to factorize a definite class of integer numbers using additional computations within the classical computing model.

In the original version of Shor's quantum algorithm for factoring integer numbers, to decompose a number N, which actually means the search for the period of the function $f(x) = a^x \bmod N$, $x \in Z_N$, for some value of $a \in Z_N^*$ (i.e., the search for the multiplicative order of an element $a \in Z_N^*$), the first register must have a size of $2\log N$ qubits (to compute the quantum Fourier transform and to ensure a bounded error in the case of using corresponding fractions), and the second register must be of a size of $\log N$ qubits sufficient for function values. Thus, the total number of necessary qubits equals $3\log N$. In his investigations, K. Zalka showed that the number of necessary qubits can be reduced to $2+\frac{3}{2}\log N$. Later on, this idea was confirmed, and actually only one qubit and the so-called semiclassical Fourier transform is used in the first register. Since the condition of achieving such a reduction in necessary resources is the repeated use and re-initialization of one qubit by assigning a zero value to it within a single pass of the quantum algorithm scheme, this method was called qubit recycling. It is used in almost all the above-mentioned experimental demonstrations of Shor's algorithm.

Moreover, in all the mentioned works, information on the sought-for result is used directly during its computation since the decomposition of small numbers is already well known. There are some numbers whose multiplicative order is small, but the value of such a number allows to obtain the desirable decomposition of an input integer number. Therefore, the number of necessary qubits will considerably be reduced if definite computations are executed in advance using the classical model. This version of Shor's algorithm is called Shor's compiled algorithm. It is this version that is used in the majority of practical implementations. Moreover, the number 15 has a certain peculiarity, namely, all elements of the multiplicative group of the ring of residues Z_{15} have multiplicative order equal to 2 or 4, that is, a degree of 2. This means that there is no need in using the corresponding fractions and additional qubits even if the original version of Shor's algorithm is used. The number 11 that corresponds to the exponent 2 and allows to decompose the number 15 can also be used, which was done in some experiments.

Recently, J. Zhu and M. Geller showed how the numbers 51 and 85 can be factorized using only 8 qubits (without conducting an experiment). As well as the number 15, the numbers 51 and 85 are the product of two prime Fermat numbers (of the form $2^{2^k}+1$). It was shown how to found numbers that have a small multiplicative order modulo the product of Fermat prime numbers.

J. Smolin and others developed this idea and proved that, for an arbitrary composite number pq, where p and q are prime numbers, there is a number a that belongs to the exponent 2 modulo pq and allows to decompose the number pq into multipliers.

From the viewpoint of demonstration of possibilities of modern experimental quantum computing devices, it is necessary to stop to use compiled versions of algorithms and, for example, instead of demonstration of Shor's algorithm, to concentrate on its main quantum part, i.e., the search for the period of a periodic function. In other words, the result of the implementation of the algorithm must be the finding of the period of an arbitrary function under a constraint concerning the sizes of its domain and values. Taking into account the data on the number of the qubits being used that are given in well-known works, it can be concluded that over the past 15–20 years almost no changes occurred in the computational capabilities of the corresponding experiments. In particular, changes took place in methods and technologies that allow to improve control and external conditions rather than capabilities for finding the period of a periodic function with a larger domain.

In 2016, the IBM company announced the creation of a quantum computer with a capacity of 5 qubits one of which is used to correct errors. This computing device is based on a five-qubit superconducting chip with star geometry and implementation of the complete Clifford algebra. It is programmable and allows to create gates and to model their operation.

In May 2017, the IBM company announced the implementation of quantum computing devices with 16 and 17 qubits and, in November 2017, IBM announced a 50-qubit quantum computing device (for computations, only

20 qubits are used, and the rest are used to correct errors). In this device, each qubit can be in the coherent state up to 90 microseconds, and this means that the time for all operations cannot exceed this value. However, it should be noted that the IBM 50-qubit quantum computing device is sufficiently energy-efficient since it consumes from 10 to 15 kW, which approximately equals to the energy consumption of 10 typical serial microwave ovens (without regard for the energy required for cooling of the device before work during 36 hours).

The program Quantum Experience allows to get remote access to this computing device and to model and to launch different algorithms including Shor's algorithm using the classical Internet network to connect to the IBM cloud. To date, the Quantum Experience program provides access to two 5-qubit devices and one 16-qubit device and has about 75 thousand users who launched about two and a half million experiments. Most of them are scientists who published a few tens of works by the results of modeling.

In January 2018, the Intel company also joined the race of quantum computing devices and declared the creation of a superconducting quantum chip, which is called Tangle Lake and contains 49 qubits.

On March 5, 2018, Google presented a new quantum processor called Bristlecone with a capacity of 72 qubits and constructed based on a 9-qubit quantum device presented by the company several years ago. The initial 9-qubit quantum device provided for using qubits combined into a linear array. For this device, it was managed to achieve a rather low level of errors, namely, the error rate was at the level of 1% for data reading, 0.1% for one-qubit quantum gates, and 0.6% for two-qubit quantum gates. The new quantum device uses two-dimensional structures. Qubits form two square 6×6 arrays located one above the other, due to which the system can track and correct errors during computations. At the time of the announcement, the detailed characteristics of the new device were not disclosed, but the researchers hope that it will demonstrate approximately the same level of errors as its predecessor. Moreover, they have an optimistic hope of achieving the so-called quantum advantage.

By the term "quantum advantage" we understand the demonstration of the fact that a quantum computing device will solve a certain computing task (possibly, specially created for such a purpose) faster than any classical modern supercomputer (or all modern supercomputers together). Reaching this level will actually mean the beginning of the era of quantum devices and the quantum computing model. Most scientists hope that, with the current level of errors, this will happen when quantum devices will operate with 100 or more qubits. However, the results of calculations performed by Google's specialists show that 49 qubits are sufficient to this end if the number of gates exceeds 40 and the error of two-qubit quantum gates is less than 0.5%. Further studies of this device will make it possible to more accurately calculate the level of the corresponding errors and to analyze its capabilities.

It seems that quantum computing devices from IBM, Google, and Intel are universal devices with real characteristics. However, the number of qubits available for use is usually significantly smaller than the declared number due to the need for additional operations for error correction. Therefore, it is still a bit early to claim that a quantum advantage has been achieved since today even an ordinary laptop can model the operation of 30–40 qubits using software tools. For example, 20 qubits available for computations make it possible to find periods of periodic functions that, in the case of implementation of the usual Shor algorithm, can guarantee a successful factorization of a number that is no larger than 89. This suggests that experiments, technology, and experience are now being accumulated and that it is still early to set records on devices with such numbers of qubits, but the general problem of searching for the period of a periodic function can be an efficient measure of the power and "quant nature" of future computing devices.

CONCLUSIONS

This article proposes a survey and an analysis of basic concepts and postulates of the quantum computing model, efficient quantum algorithms, and recent results, possibilities, and prospects in the field of constructing a scalable quantum computer. The results of recent studies on solving algebraic problems in the quantum computing model and possible applications of these results to construct new and analyze long-known cryptographic transformations are considered. It has been clarified that today there are only a small number of problems for which there exist efficient quantum algorithms that will solve them in practice in polynomial time as opposed to the classical computer. The class of such problems includes problems of factoring large numbers and discrete logarithmization whose complexity underlie the stability of the overwhelming majority of algorithms and protocols for asymmetric cryptography. In other words, after creating a scalable quantum computer, these algorithms and protocols will be broken. But even if the range of efficiently

solved problems will not be extended, owing to Grover's algorithm, the complexity of any problem on a quantum computer will be a square root of times smaller than that on the classical computer. Then scalable quantum computers can be used to solve problems in the fields of economy, planning, combinatorial optimization, etc.

The experimental and practical results obtained to date testify to the lack of sufficient progress in constructing a scalable quantum computing device in terms of the implementation of well-known quantum algorithms. Until practical implementations of quantum systems will not operate with a larger number of qubits than the number of qubits whose operation can be modeled in a reasonable time on the classical computer, it is hard to assert about any advantages and methods of estimation. However, most researchers expect the creation of a full-fledged quantum computer that will be able to break, for example, RSA-4096, within the next 10–15 years, albeit with a forecast probability of 0.5. Therefore, already now it is necessary to prepare appropriate replacement options for post-quantum cryptographic transformations and protocols with estimating the protection strength and complexity of an implementation, as well as to elaborate in detail various modifications of the transformations taking into account the capabilities of the Grover algorithm.

REFERENCES

1. C. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," in: Proc. Intern. Conf. on Computers, Systems and Signal Processing (Bangalore, India) (1984), pp. 175–179.
2. Quantum Computer and Quantum Computing, Izhevsk Republican Printing House, Izhevsk (1999).
3. J. Preskill, Quantum Information and Computation [Russian translation], Volume 1, Research Center "Regular and chaotic dynamics;" Computer Research Institute, Moscow–Izhevsk (2008).
4. S. Aaronson, Quantum Computing since Democritus [Russian translation], Alpina Non-Fiction, Moscow (2018).
5. M. N. Savchuk, "Works of the Kiev school of theoretical cryptography," Cybernetics and Systems Analysis, Vol. 46, No. 3, 386–404 (2010).
6. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge (2000).
7. A. Kitaev, "Quantum Computations: Algorithms and Error Correction," Russian Mathematical Surveys, Vol. 52, No. 6, 53–112 (1997).
8. A. Yao, "Quantum circuit complexity," in: Proc. 34th Annual Symposium on Foundations of Computer Science (1993), pp. 352–361.
9. R. Boneh and R. Lipton, "Quantum cryptanalysis of hidden linear functions," in: Proc. 15th Annual International Cryptology Conference (Santa Barbara, California, USA, August 27, 1995), Advances in Cryptology (Crypto'95); Lecture Notes in Computer Science, Vol. 31, 424–437 (1995).
10. D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," Proc. Royal Society of London, Series A, No. 439, 553–558 (1992).
11. P. W. Shor, "Algorithms for quantum computation: Discrete logs and factoring," in: Proc. 35th Symposium on the Foundations of Computer Science (Santa Fe, NM, USA, Nov. 20–22, 1994) (1994), pp. 124-134.
12. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing, Vol. 26, Iss. 5, 1484–1509 (1997).
13. W. Van Dam, S. Hallgren, and L. Ip, "Quantum algorithms for some hidden shift problems," SIAM Journal on Computing, Vol. 36, No. 3, 763–778 (2006).
14. A. V. Fesenko, "Vulnerability of cryptographic primitives based on power conjugacy search problem in quantum computing," Cybernetics and Systems Analysis, Vol. 50, No. 5, 815–816 (2014).
15. Z. Bian, F. Chudak, W. Macready, L. Clark, and F. Gaitan, "Experimental determination of Ramsey numbers," Physical Review Letters, Vol. 111, Iss. 13, p. 130505 (2013). DOI: https://doi.org/10.1103/PhysRevLett. 111.130505. URL: https://arxiv.org/abs/1201.1842.
16. A. Cho, "Quantum or not, controversial computer yields no speedup," Science, Vol. 344, No. 6190, 1330–1331 (2014). DOI: https://doi.org/10.1126/science.344.6190.1330.
17. N. S. Dattani and N. Bryans, Quantum Factorization of 56153 with Only 4 Qubits, Quantum Physics Archive. arXiv:1411.6758 [quant-ph]. 2014. URL: https//arxiv.org/abs/1411.6758.