# BASIC ALGORITHMS QUANTUM CRYPTANALYSIS

*Petrenko A.S.[1], Petrenko S.A.[2]*

***Abstract***

***Purpose of the article:*** *development of quantum algorithms for efficient solution of cryptanalysis problems of asymmetric encryption schemes (RSA, ElGamal) and digital signature (DSA, ECDSA or RSA-PSS), based on computationally difficult problems of factorization and discrete logarithm.*

***Research methods:*** *Methods of quantum cryptanalysis based on the algorithms of Shor, Grover, Simon, etc.*

***Results:*** *algorithms for solving problems of quantum cryptanalysis of two-key cryptography schemes in polynomial time.*

***Practical relevance:*** *consists in developing a solution for computationally difficult problems of factorization and discrete logarithm in polynomial time, taking into account the security of the discrete algorithm (DLP) and the discrete elliptic curve algorithm (ECDLP). The obtained scientific results formed the basis for the development of a special Software Development Kit, SDK for cryptanalysis "Kvant-K". The Certificate of state registration of the computer program No. 2020665981 was received.*

***Keywords:*** *quantum security threat, cryptographic attacks, quantum cryptanalysis, quantum algorithms Shor, Grover and Simon algorithms, quantum Fourier transform, factorization, and discrete logarithm problems.*

**DOI:**10.21681/2311-3456-2023-1-100-115

## Implementation of the Shor factorization algorithm

Shor's algorithm is a quantum algorithm for factoring a number $N$ for $O\left((\log N)^3\right)$ time and $O(\log N)$ resources [1,2,8]. The algorithm exposes the RSA key (a popular cryptographic method) to the danger of being easily hacked if it is run on a quantum computer large enough for this. Shor's algorithm can do this in polynomial time [22,29].

Like many of the quantum computer algorithms, Shor's algorithm is probabilistic: it gives the correct answer with any predetermined probability. This is achieved by repeatedly re-executing the algorithm. Since the proposed solution is verifiable in polynomial time, the algorithm can be modified to work in the expected polynomial time with zero error.

Shor's algorithm was developed in 1994, but the classical part was developed before *J.L. Miller*. Seven years later, in 2001, Shore's quantum algorithm was demonstrated by a group at IBM, which carried out the factorization of the number 15 into 3 and 5 using a quantum computer with 7 qubits. In 2016, scientists at the Massachusetts Institute of Technology and the University of Innsbruck designed a quantum computer that implements a scalable version of the Shor algorithm proposed by a Russian physicist. *By Alexey Kitaev* [8]. This significantly reduced the number of qubits used to perform operations.

The task to be solved was to find the integer divisor of an $p$ integer $N$ in the interval between $1$and $N$.

Shor 's algorithm consists of two parts:

1) Reduction of the factorization problem to the order search problem, which can be solved on a classical computer.

2) Execution of a quantum algorithm to solve the problem of finding the order.

**The classical part** of Shor 's algorithm looks like this:

1) We select a random number $a < N$.

2) We calculate GCF $(a, N)$ (the GCF is the largest common divisor). This can be done using Euclid's algorithm.

3) If GCF $(a, N) \neq 1$, then there is a nontrivial divisor $N$, then the execution of the algorithm ends.

4) Otherwise, we use the period search routine (below) to find the $r$ period of the following function: $f(x) = a^x mod\, N$, i.e., the smallest integer $r$ for which $f(x+r) = f(x)$.

5) If $r$ is odd, go back to step 1.

6) If $a^{r/2} \equiv -1 mod\, N$ , go back to step 1.

1 Alexei S. Petrenko, Postgraduate student in the direction 10.06.01 "Information Security" Saint-Petersburg State Electrotechnical University «LETI», finalist of the All-Russian competition of scientific projects, Saint-Petersburg, Russia. Orcid.org/ 0000-0002-9954-4643, E-mail: A.Petrenko1999@rambler.ru

2 Sergei A. Petrenko, Dr.Sc. (in Tech.), Professor Saint-Petersburg State Electrotechnical University «LETI», laureate of the year-2022 and the Russian Awardand "Knowledge", Saint-Petersburg, Russia. Orcid.org/0000-0003-0644-1731, E-mail: S.Petrenko@rambler.ru

7) The divisors of $N$ are GCF $\left(a^{\frac{r}{2}} \pm 1, N\right)$.

**The quantum part** of the Shor algorithm is a subroutine for searching for the period of the function:

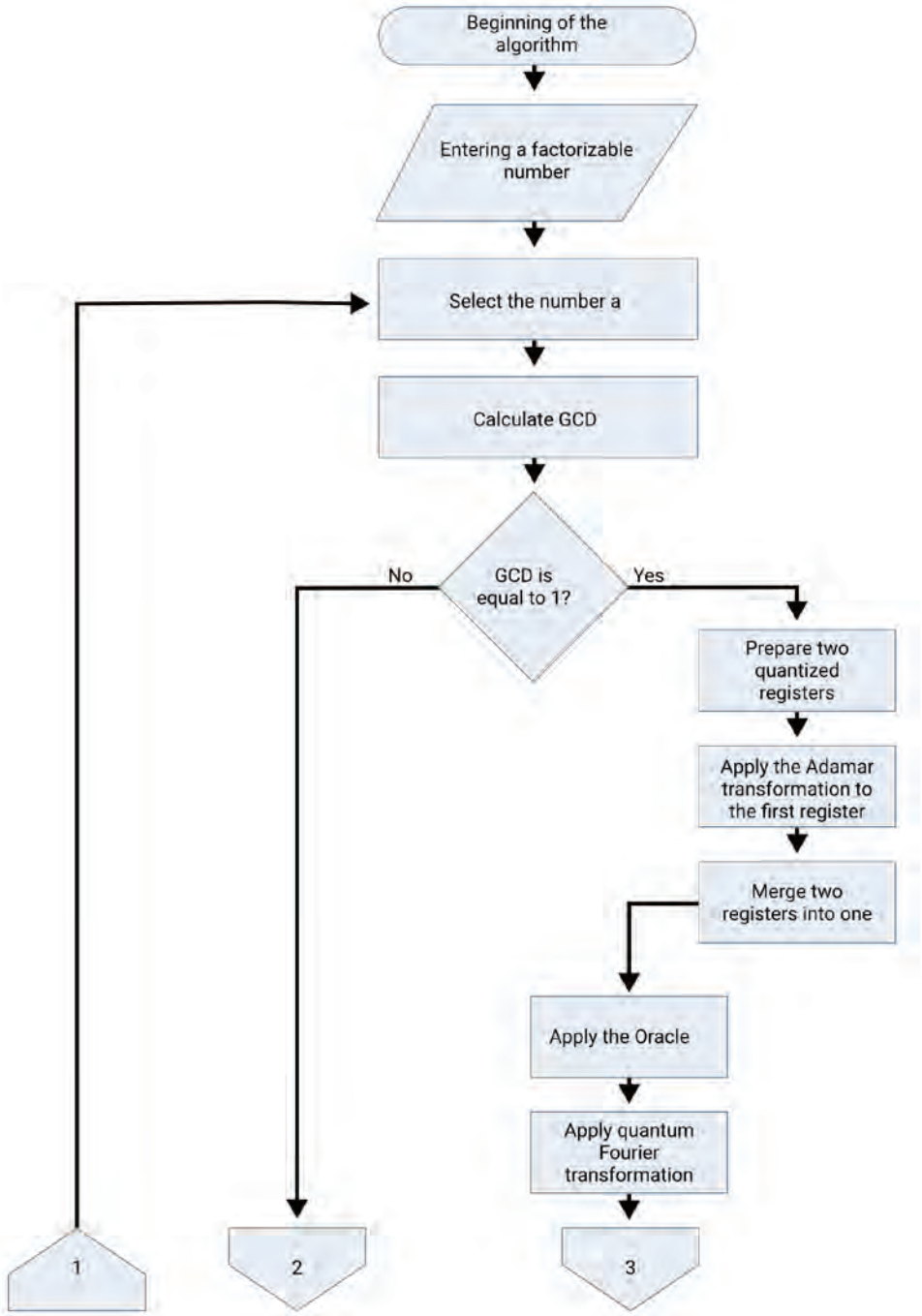
1) A pair of initial and output qubit registers with $\log_2 N$ qubits are each initialized in a state $N^{-1/2}\sum_x |x\rangle|\theta\rangle$ where $x$ runs from $0$ to N - 1.

2) Constructing $f(x)$ as a quantum function and applying it to the above state, we get:

$$U_{QFT}|x\rangle = N^{-1/2}\sum_y e^{-2\pi ixy/N}|y\rangle.$$

3) This leaves us in the following state:

$$N^{-1}\sum_x\sum_y e^{-2\pi ixy/N}|y|f(x)\rangle;$$



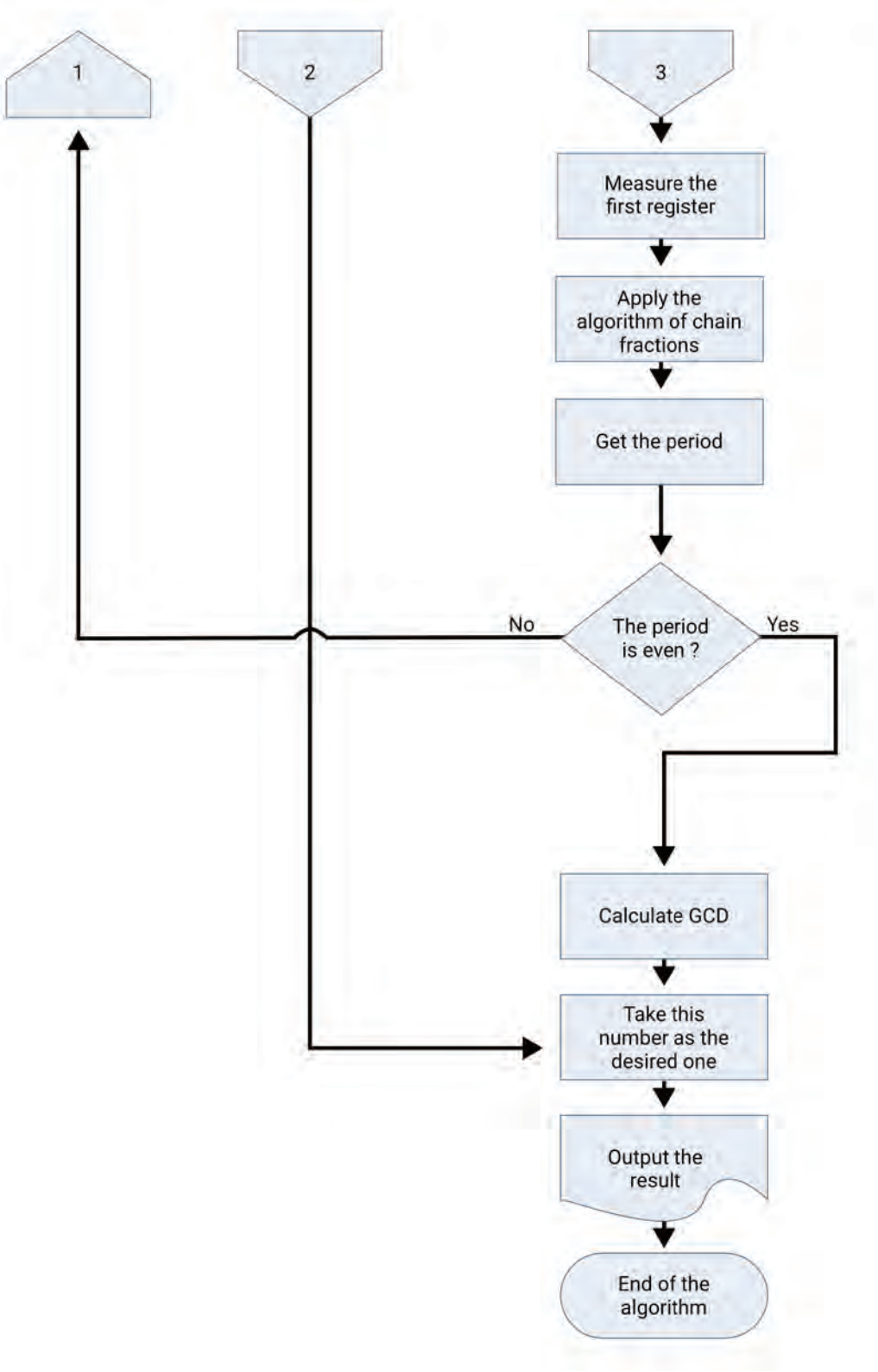



*Figure 1. Diagram of the Shore factorization algorithm*

4) Let's make a measurement. We will get some output $y$ in the introductory register and $f(x_0)$ in the output register. Since $f$ is periodic, the probability of obtaining a certain pair during measurement of $y$ and $f(x_0)$ is given by the expression:

$$\left| N^{-1} \sum_{x: f(x)=f(x_0)} e^{-2\pi i x y / N} \right|^2 = \left| N^{-2} \sum_{b} e^{-2\pi i (x_0 + rb) y / N} \right|^2 .$$

5) The analysis shows that this probability becomes higher, when $yr/N$ becomes closer to the whole.

6) Convert $yr/N$ to an irreducible fraction and find the denominator $r^i$ that is a candidate for $r$.

7) Let's check if $f(x)=f(x+r')$ is being executed. If yes, then the problem is solved.

8) Otherwise, we get more candidates for $r$, using values close to $y$, or multiples of $r^i$. If one of these candidates is suitable, the problem is solved. Otherwise, we return to step 1 of the subroutine.

Thus, the classical Shor factorization algorithm consists of two parts (Figure 1). The first part of the algorithm reduces the factorization problem to the problem of detecting the period of the function and can be implemented classically. The second part finds the period of the function using the inverse quantum Fourier transform (it generates quantum acceleration).

Therefore, in the first stage there are divisors by period. Integers that are less than $N$ and mutually prime with $N$ form a finite multiplication group modulo $N$, which is usually denoted by $(Z/NZ)^x$. By the end of step 3, there is an integer $a$ in this group. Since the group is finite, $a$ must have a finite order $r$, the smallest positive integer such that $a^r \equiv 1 mod\, N$.

Suppose there is an opportunity to find $r$, and it is even. Then $a^r-1=(a^{r/2}-1)(a^{r/2}+1)\equiv \equiv 0 mod\, N, \Rightarrow N\,|\,(a^{r/2}-1)(a^{r/2}+1)$, where $r$ is the smallest positive integer such that $a^r \equiv 1$, therefore $N$ is not a divisor $a^{r/2}-1$. If $N$ is also not a divisor of $a^{r/2}+1$, then $N$ must have a nontrivial common divisor with each of $(a^{r/2}-1)8(a^{r/2}+1)$, which leads us to factorization $N$. If $N$ is the product of two primes, then this is the only possible factorization.

The second part of the algorithm is devoted to finding the period. Here, Shor's algorithm relies on the ability of a quantum computer to be in a superposition of states. The function is calculated at all points simultaneously in order to calculate the period of $f$ function. Quantum mechanics does not allow access to this information directly. The measurement will result in only one of all possible values, destroying all the others. Therefore, it is necessary to transform the superposition into another state, which will return the correct answer with a high probability. This is achieved by the inverse quantum Fourier transformation [1-12].

Shore had to solve the following three "implementation" problems, and all of them had to be implemented "quickly". This means that they can be implemented with a set of quantum gates that are polynomial in $logN$ [13-18, 22, 29]. So, it is necessary:

1. Create superpositions of states. This can be done by applying Hadamard gates to all qubits of the input register. Another approach would be to use the quantum Fourier transformation.

2. Apply function *f* as a quantum transformation. Shor used multiple squaring for his modular exponential transformation to achieve this. Note that this step is more difficult than the quantum Fourier transformation, which requires auxiliary qubits and a significantly larger number of gate triggers.

3. Perform the inverse quantum Fourier transformation. When using controlled rotation gates, and Hadamard gates, Shor constructed a circuit for the quantum Fourier transformation, which uses only $O((\log N)^2)$ gates.

After all these transformations, the measurement will give an approximate value of the $r$ period. For simplicity, let's assume that there exists such $y$ that $yr/N$ is an integer. Then the probability to measure $y$ is $1$. We then notice that $e^{2\pi ibyr/N}=1$ for all $b$ integers. Therefore, the sum which square gives the probability to get when measured $y$ will be equal to $N/r$, since $b$ roughly takes values of $N/r$ and thus the probability is equal to $1/r^2$. There are such $yr$ that $yr/N$ is an integer, and also probabilities for $f(x_0)$, so the sum of probabilities is 1 [19-22].

### Implementation of the Grover's search algorithm

Consider Grover's algorithm, a quantum algorithm for fast search in an unordered database [6, 23-26]. With the existing technical means, one of the fastest classical search algorithms is linear search, which requires $O[N]$ time. Grover's algorithm, using the capabilities of quantum computers, solves the problem of searching in *N* records for the desired time $O\sqrt{N}]$ using $O[Log\, N]$ space. It is proved that it is the fastest quantum algorithm for searching in an unordered database and that there are no classical algorithms of the same efficiency. Grover's algorithm provides a quadratic increase in speed, while some other quantum algorithms, for example, the Shor factorization algorithm, give an exponential gain compared to the corresponding classical algorithms. Despite this, the quadratic increase is significant for sufficiently large values of $N$ [26-31].

Although the main purpose of Grover's algorithm is considered to be a database search, it can be more accurately described as a "function reversal" algorithm. Technically speaking, having a function $y=F(E)$ that can be calculated using a quantum computer, Grover's algorithm calculates $x$ knowing *y*. The search in the

database corresponds to the call of a function that takes a certain value if the argument x corresponds to the desired record in the database. Grover's algorithm can also be used to find the median and the arithmetic mean of a number series. In addition, it can be used to solve $NP$ complete problems by an exhaustive search among a variety of possible solutions. This can lead to a significant increase in speed compared to classical algorithms, although it does not provide a "polynomial solution" in general form [6,26,32-34].

Like most quantum computer algorithms, Grover's algorithm is probabilistic in the sense that it gives the correct answer with some probability (generally speaking, with any given in advance). The probability of an incorrect answer can be reduced by increasing the number of repetitions of the algorithm (an example of a deterministic quantum algorithm is the Deutsch-Joz algorithm [23,24], which always gives the correct answer with fixed confidence). As an example, let's give Grover's algorithm, which searches for a single matching record.

Suppose there is an unordered database with $N$ records. The algorithm requires a $N$ -dimensional state space $H$ that can be generated by $\log_2 N$ qubits. Let's number the database entries in this way: $0,1,2,\ldots,N-1$.

Let's choose an observable $Q$ acting in $H$ with $N$ different eigenvalues, which are all known. Each of the eigenstates $Q$ encodes one of the records in the database in the way described below. Let's denote the eigenstates (using Dirac notation) as $|0\rangle,|1\rangle,\ldots,|N-1\rangle$ as their corresponding eigenvalues $\{f0, f1,\ldots,fN-1\}$ .

Consider a unitary operator $U_w$ that acts as a subroutine comparing database records by some search criterion. The algorithm does not specify how this subroutine works, but it should be a quantum subroutine that works with superpositions of states. Further, the operator $U_w$ must act only on its own state $w$, which corresponds to the database record that falls under the search criterion. We will require that $U_w$ performs the following transformation: $U_w|w\rangle = -|w\rangle$ and $U_w|v\rangle = |-v\rangle$ for every $v \neq w$. The goal is to identify the eigenstate $|w$, or equivalently, the eigenvalue of $\omega$, on which the operator acts $U_w$.

Grover's algorithm (Figure ) consists of the following steps [6,26,33]:

1. Initialize the system in the state $|s\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle$.
2. Perform the following "Grover iterations" $r(N)$ times.
3. Function $r(N)$ is described below.
   a. Apply the $U_\omega$ operator.
   b. Apply the $U_s = 2|s\rangle\langle s| - 1$ operator.
4. Let's take a $\Omega$ measurement. The result of the measurement will be $\lambda_\omega$ with a probability tending to 1at $N \gg 1$. With $\lambda_\omega$ can be obtained $\omega$.

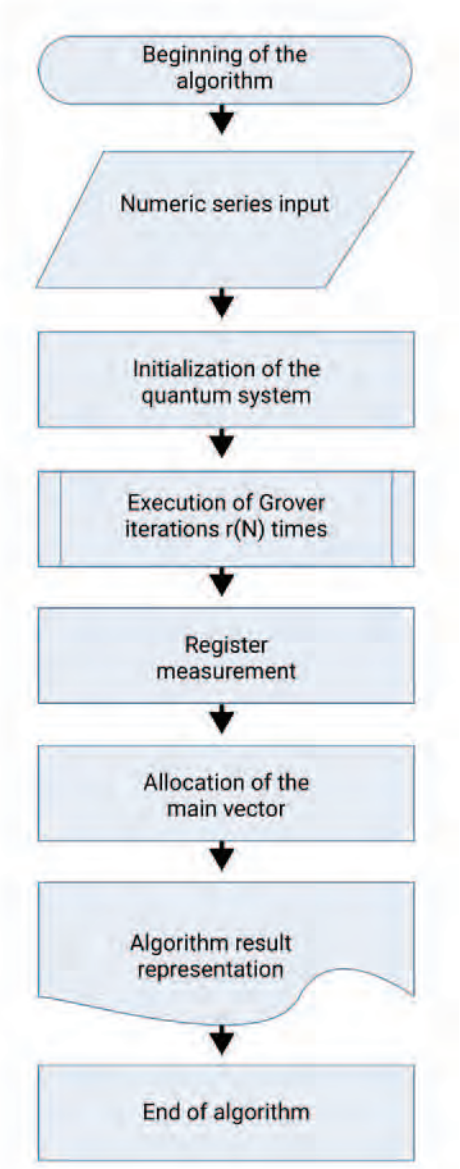



*Figure 2. Diagram of Grover's quantum search algorithm*

Our initial state is $|S\rangle = \frac{1}{\sqrt{N}}\sum_x |X\rangle$. Consider a plane spanned by vectors $|s\rangle$ and $|w\rangle$. Let $|w^x\rangle$ be a ket vector in this plane perpendicular to the $w$ vector. Since $|w\rangle$ is one of the basis vectors, the overlap is equal to $\langle w|s\rangle = \frac{1}{\sqrt{N}}$. In geometric interpretation, between $|w$

and the $|s\rangle$ angle is $\Pi/2-\theta$, where $w$ is determined from $\cos(2\Pi-\theta)=\frac{1}{\sqrt{N}}$ and $\sin\theta=\frac{1}{\sqrt{N}}$. The operator $U_w$ acts as a reflection in a hyperplane orthogonal to $|w\rangle$; for vectors in a plane spanned by vectors $|s\rangle$ and $|w\rangle$, it acts as a reflection relative to a straight line defined by a $|w^x\rangle$ vector. The $U_s$ operator is a reflection relative to a line defined by a $|s$ vector. Consequently, the state vector remains in the plane stretched over the vectors $|s$ and $|w$, after each action of the $U_s$ operator and $U_w$ operator, and it can be directly verified that the $U_sU_w$ operator of each iterative step of the Grover algorithm rotates the state vector by an angle $20$ in the $|w\rangle$ direction [6,26,31-34].

It is necessary to stop when the state vector passes close to the $|w$ vector; after that, the subsequent iterations rotate the state vector in the direction from $|w$, reducing the probability of getting the correct answer. The number of required iterations is equal to $r$. You need $\frac{\Pi}{2}-\theta=2\theta_r$, $r=1/4(\Pi/\theta-2)$ to combine the state vector exactly with $|w\rangle$. However, the number $r$ must be an integer, so, in general, it can only be selected as the closest to $1/4(\Pi/\theta-2)$. The angle between $|w\rangle$ and the final state vector is equal $O(\theta)$, so the probability of getting an incorrect answer is equal to $O(1-cos^2\theta)=O(sin^2\theta),\theta\approx N^{-\frac{1}{2}}$, at $N\gg1$, therefore $r\to\frac{\Pi\sqrt{N}}{4}$. Moreover, the probability of getting an incorrect answer becomes $O(1/N)$, and tends to zero for large $N$ [1,6,26].

### Development of an algorithm for recovering a symmetric encryption key

Grover's algorithm is usually described as a search algorithm in an unordered array [26]. We modify Grover's algorithm into an algorithm for recovering the symmetric encryption key from the message text and ciphertext (Figure 3.). When using a classic computer, this will require a complete search with complexity $O(2^m)$, where $m$ is the length of the key. For a quantum computer, this complexity can be greatly reduced as follows.

Consider the function $y=f(k,x)$. This function encrypts the message $x$ on the key $k$ where $x, y\in Z_{2^n}$. Let the message-ciphertext pair be known: $x1, x2$

Consider the function:

$$f(k)=\begin{cases}1, if A(k,x1)=y_1\\0, if\ A(k,x2)\neq y_1\end{cases}$$

Find the value of the argument at which this function is equal to 1.

We propose the following quantum algorithm for solving the problem.

### Grover's algorithm implemented on a quantum circuit

*Step 1.* Let's start the algorithm by bringing the quantum register to the state:

$$\frac{1}{\sqrt{2^m}}\sum_{t=0}^{2^m-1}|t\rangle$$

*Step 2.* Calculating the function $f$ from this register:

$$\frac{1}{\sqrt{2^m}}\sum_{t=0}^{2^m-1}|t\rangle\langle f(t)\rangle$$

*Step 3.* Repetition $\frac{\pi\Pi}{4}\sqrt{2^m}$ times of the procedure of increasing the amplitude of all $t_i$ for which $f(t_i)=1$ (the description of the procedure is given below).

*Step 4.* Measurement of the state of the register. The result will be equal to the desired key with probability $2^{-n}$.

*Step 5.* Checking the result. In case of unreliability, the algorithm is executed again. The end of the algorithm.

The procedure for increasing the amplitude consists of two stages.

1. The change in amplitude from $a_j$ to is $-a_j$ for all $t_i$ such that $f(t_i)=1$. This operation is a transformation $Z$ over the last quantum bit of the register.
2. Inversion relative to the mean. This transformation can be written as follows:

$$\sum_i|t_i\rangle\to\sum_i(2a_{cp}-a_it|t_i\rangle,$$

where $a_{cp}$ is the average amplitude.

The inversion relative to the mean can be written as a matrix:

$$D=\begin{pmatrix}\frac{2}{N}-1 & 2/N & K & 2/N\\ 2/N & \frac{2}{N}-1 & L & 2/N\\ L & L & L & L\\ 2/N & 2/N & L & 2/N-1\end{pmatrix}.$$

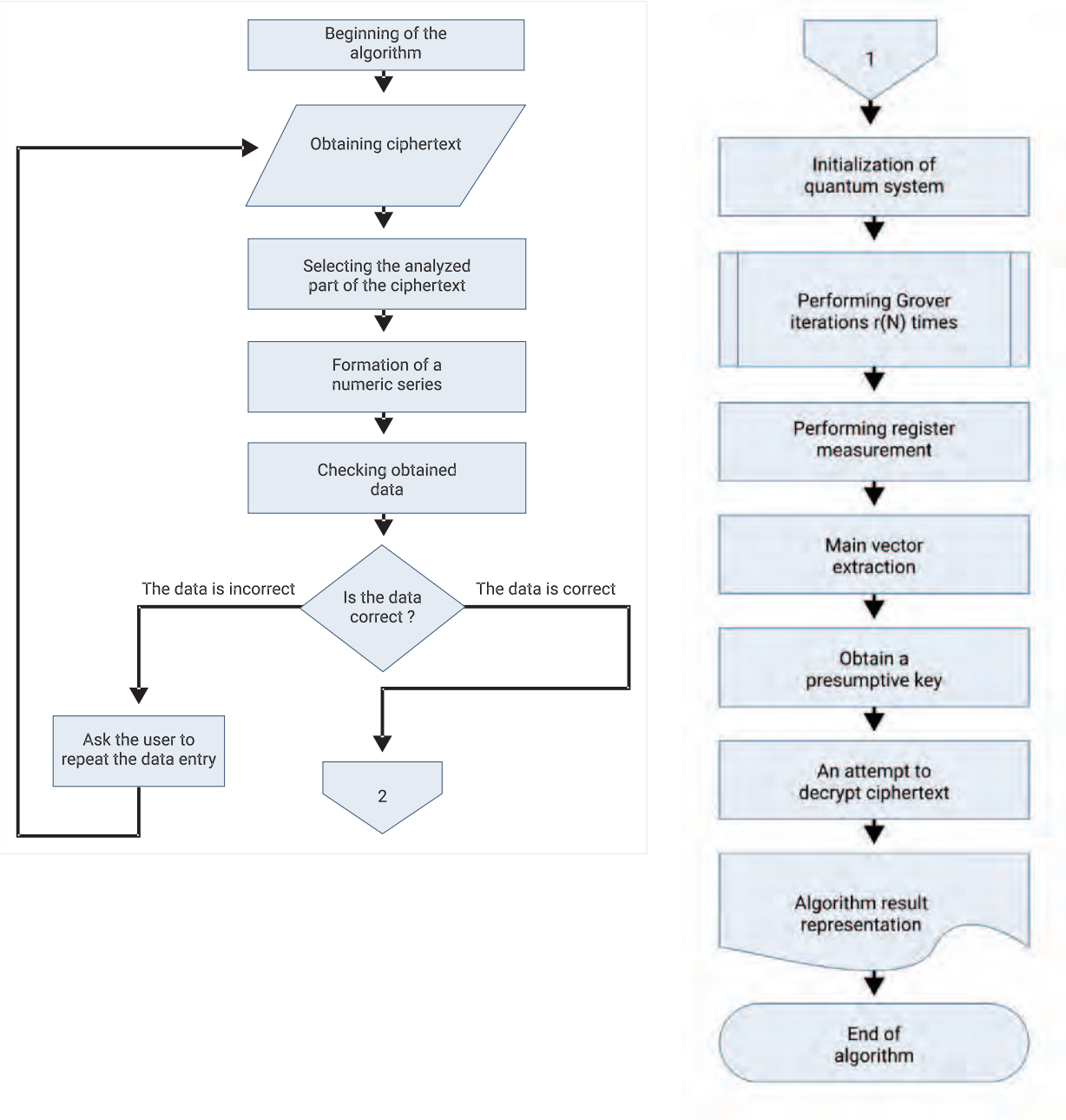



*Figure 3. Quantum algorithm for symmetric encryption key recovery based on the message text and ciphertext has been developed*

L. Grover showed [26] that this transformation can be efficiently implemented on a quantum computer, and the complexity of the corresponding $O\left(2^{n/2}\right)$ *algorithm.* Thus, the advent of quantum computers will reduce the effective key length by half. This suggests that symmetric ciphers with a key length of at least *256* bits should already be used.

In addition, a similar algorithm can be used to crack hash functions, and therefore hash functions with a block length of at least *256* bits should be used.

## Development of an algorithm for cryptanalysis of the RSA asymmetric encryption system

The stability of the RSA asymmetric encryption system is based on the superpolynomial computational complexity of factorization of natural numbers. However, there is a quantum algorithm which complexity is polynomial.

Let's set the problem as follows: for a natural $N$ number having exactly two prime divisors, find these divisors. Note that for some $a$ number, its order modulo

$N$, is such that it is $a^r = 1 mod\ N -$ even. Then we will write the expression in the following form:

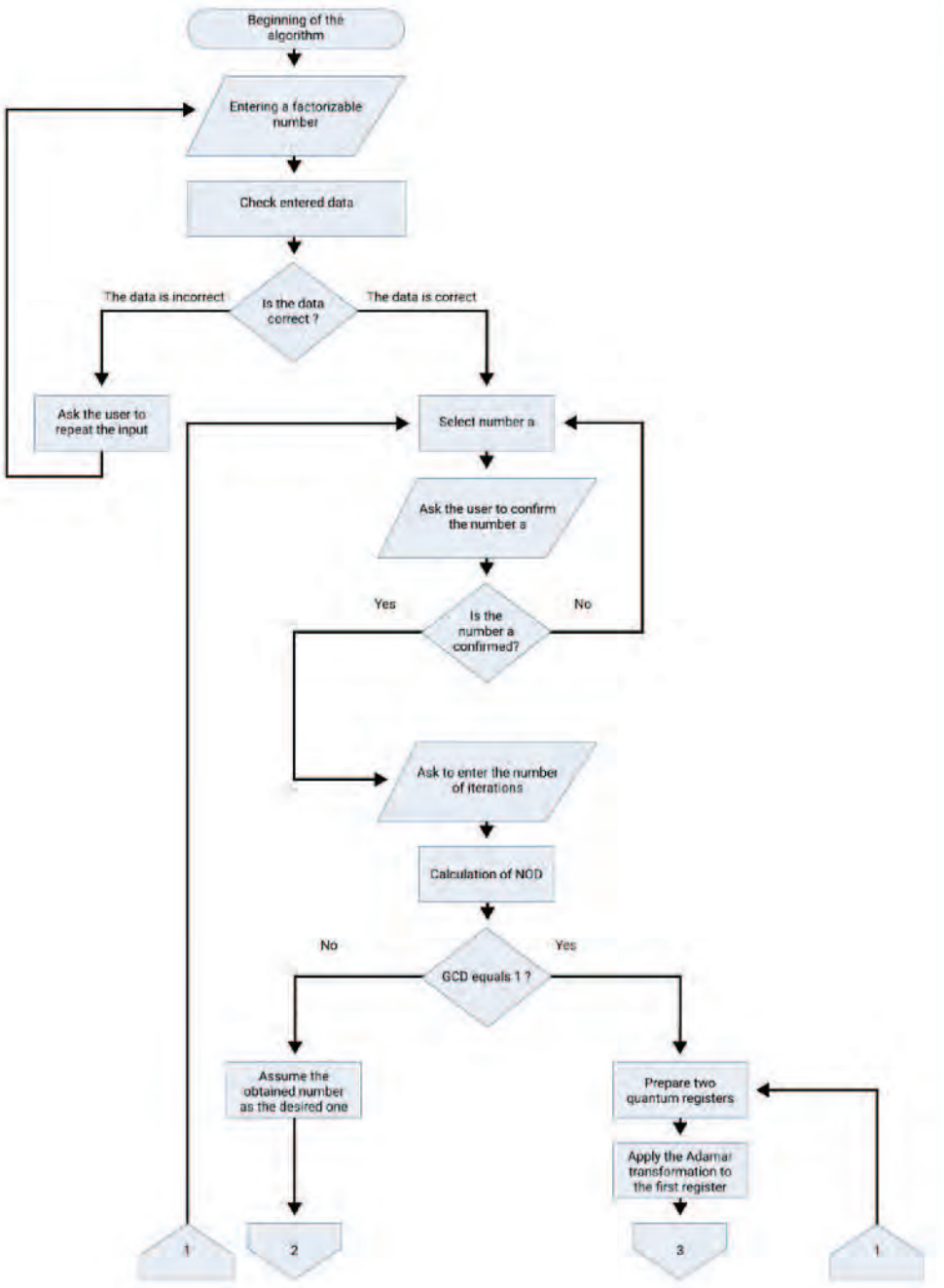
$$\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) = 0 mod\ N$$

Thus, knowing $r$, we can efficiently find the divisors of a number $N$. Note that the order $r$ is actually the period of the function $a^x\ mod\ N$.

There is the following quantum algorithm (Figure ) to find the period of the function. Consider the periodic function $f(x)$. The domain of definition and the domain of values of this function are sets of integers, with $0 \le x \le 2^n - 1$ and $0 \le f(x) \le 2^m - 1$. A quantum register consisting of $n+m$ quantum bits is required to find the period of this function. Let 's bring it to the following state:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle.$$

Now we calculate the function $f$ so that we get the state:



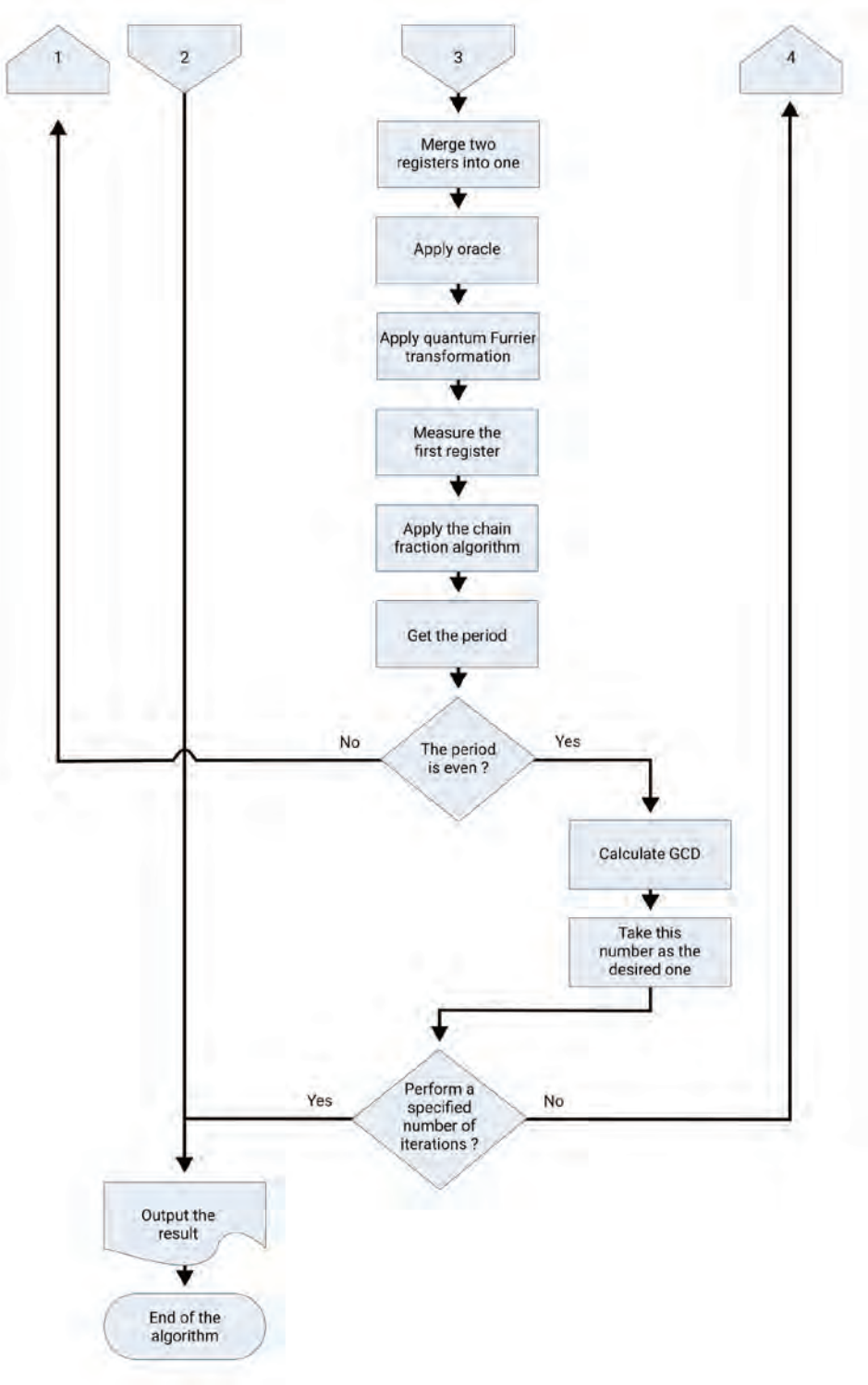



*Figure 4. Quantum algorithm for cryptanalysis of the RSA asymmetric encryption system*

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x, f(x)\rangle.$$

Let's measure the last $m$ quantum bits, i.e., the quantum bits related to $f(E)$. Then the quantum register will switch to the state:

$$\sum_{x:f(x)=u}|x,u\rangle.$$

Let's carry out the quantum Fourier transformation (the algorithm is given below), as a result we get the state:

$$\sum_j c_j \left| j \frac{2^n}{r} \right\rangle$$

where $c_j$ are equal to zero for all $j$ non-multiples of $2^{nr}$. If the $r$ period does not divide $2^{nn}$, the transformation is performed inaccurately, with a large amplitude concentrated near integer multiples of /[$2^{n:r}$].

Let 's measure the resulting state and get a $v$ number.

If the period is equal to the power of two, then $v = j\frac{2^n}{r}$. Since in most cases *are* mutually simple, the reduction of the $\frac{v}{2^n}$ fraction will give a fraction, the denominator of which is the period.

In general, either we will have to run the entire algorithm several times until we get the correct value of the period (the maximum amplitude corresponds to it, and, consequently, the maximum probability), or use the infinite fraction decomposition known from number theory [1,5,7, 21-34].

The quantum Fourier transformation is defined as:

$$U_{QFT}\left(|x\right) = \frac{1}{\sqrt{2^m}} \sum_{t=0}^{2^m-1} e^{\frac{2\pi icx}{2^m}} |c\rangle$$

P. Shor [29] showed that such a transformation can be constructed using only two types of quantum gates $m(m+1)/2$. One of them is a *Hadamard transformation* applied to $j$ the quantum bit (let's denote it to $H_j$). Another gate implements a two-bit transformation of the form:

$$S_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\frac{\pi}{2^{k-j}}} \end{pmatrix}$$

At the same time, the quantum Fourier transformation can be set as follows:

$$H_0 S_{0,1} K S_{0,m-1} H_1 K H_{m-3} S_{m-3,m-2} S_{m-3,m-1} H_{m-2} S_{m-2,m-1} H_{m-1} = \\ = \prod_{k=0}^{m=1} H_k \prod_{t=k+1}^{m=1} S_{k,t}.$$

After this conversion, the bit order should be reversed. This can be done either by an appropriate quantum scheme, or, if a measurement takes place immediately after the quantum Fourier transformation, in a classical way.

The considered quantum factorization algorithm has $O(n^3)$ complexity. At the same time, the best classical factorization algorithm — the number field sieve algorithm [32] has complexity:

$$O\left(exp\left(c(\log n)^{1/3}(\log\log n)^{1/3}\right)\right),$$

Where $c = \sqrt{\frac{64}{9}}$. In other words, Shor's algorithm has polynomial complexity, and the best classical algorithm has superpolynomial complexity [1,2,4-11,29].

### Development of an algorithm for cryptanalysis of the El Gamal system

El-Gamal system is based on the difficulty of calculating a discrete logarithm, i.e., if $g$ *i*s the forming element of a finite G — group, then, knowing that $a \in G$, it is necessary to find $r \in G$ such that $a = g^i$. Most often this system is used for a group $Z_p$ and for a group of points of an elliptic curve.

There is a quantum Shor algorithm [29] for calculating the discrete logarithm (Figure ). Here is its original version, which is intended for the group $Z_p$ (where p- - simple).

First, we will find $q$ - the power of two, such that $p < q < 2p$ . Let 's bring the quantum register to the state:

$$\frac{1}{p-1} \sum_{a=0}^{p-2} \sum_{b=0}^{p-2} \left| a, b, q^a x^{-b} \left(mod\ p\right) \right\rangle.$$

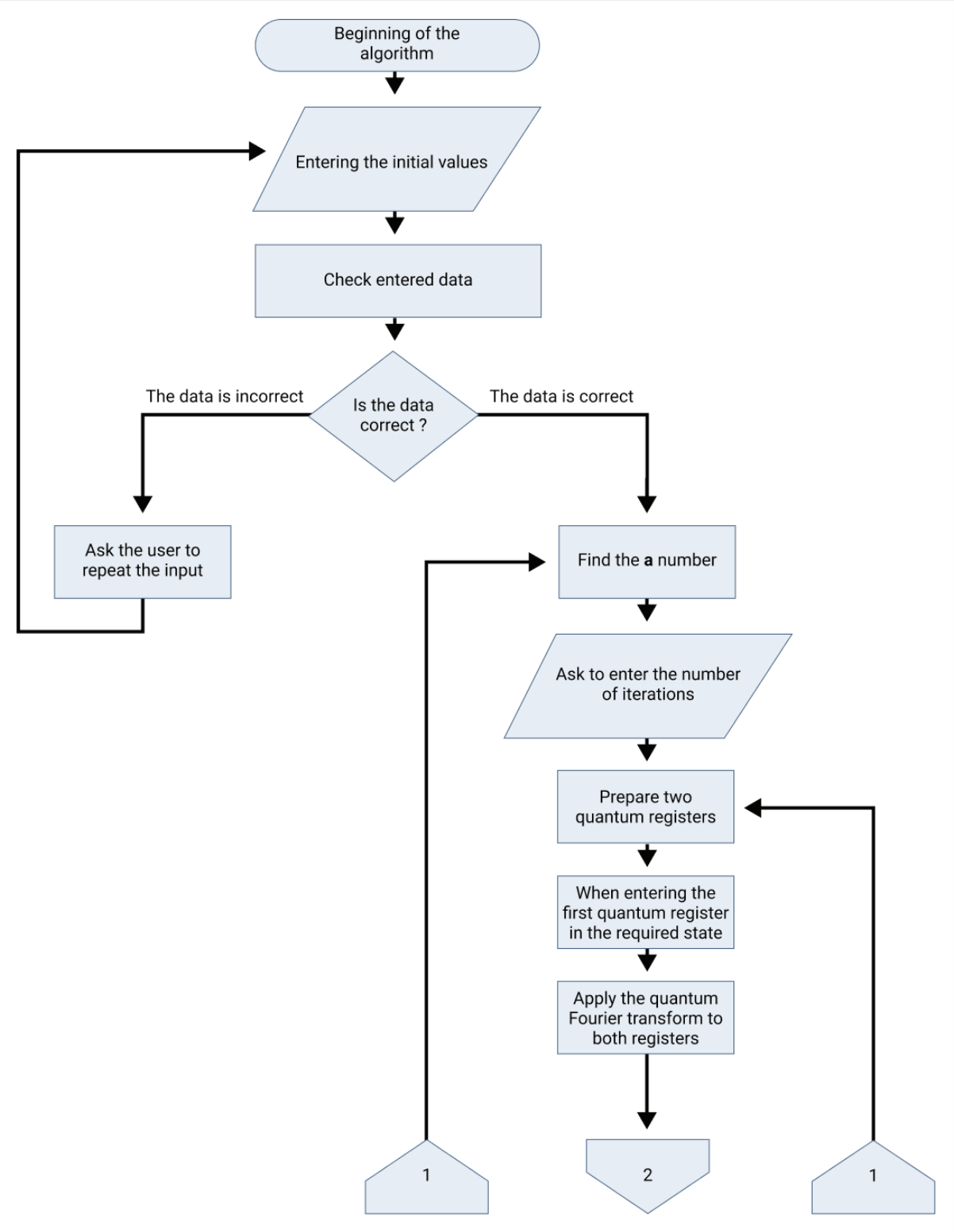
Applying the Fourier transformation to the first and second parts of the register, we obtain the state of the register:

$$\frac{1}{q(p-1)} \sum_{c=0}^{q-2} \sum_{d=0}^{q-2} e^{\frac{2\pi i}{q}(ac+bd)} \left| c, d, q^a x^{-b} \left(mod\ p\right) \right\rangle.$$

Let's measure the state of the quantum register. As a result, with a probability of at least $1/480$, we will get $A$and $d$ such that:

$$-\frac{1}{2q} \le \frac{d}{q} + r\left(\frac{c(p-1) - \{c(p-1)\}q_q}{(p-1)q}\right) \le \frac{1}{2q} (mod\, 1).$$

In order to get a candidate for $r$, it is necessary to round $d/q$ to the nearest multiple $1/p-1$, then divide modulo $p-1$ on $\frac{c(p-1) - \{c(p-1)\}q}{q}$. The


Beginning of the algorithm
Entering the initial values
Check entered data
Is the data correct ?
The data is incorrect
The data is correct
Ask the user to repeat the input
Find the **a** number
Ask to enter the number of iterations
Prepare two quantum registers
When entering the first quantum register in the required state
Apply the quantum Fourier transform to both registers
1
2
1

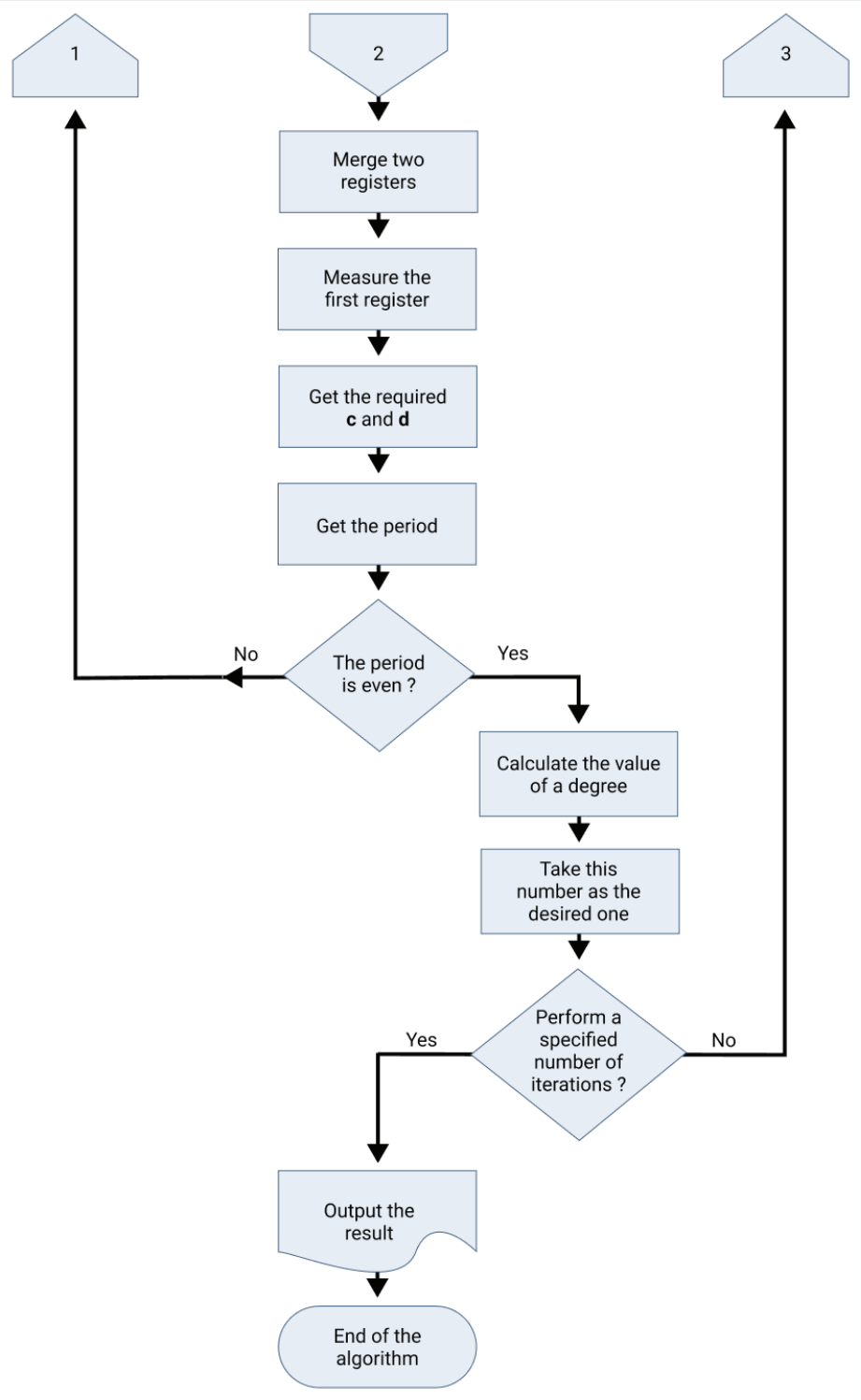



*Figure 5. Quantum cryptanalysis algorithm of El Gamal system*

complexity of this algorithm is estimated as $O\left(n^3\right)$. Note that the complexity of the best classical algorithm for a discrete logarithm is estimated as superpolynomial.

Note that there is a variant of Shor's algorithm for a group of points of an elliptic curve over a field $GP\left(p\right)$ that has $O\left(n^3\right)$ complexity, and it is also hypothesized that a similar algorithm exists for elliptic curves over other fields [1-29, 31-34].

Thus, the appearance of existing samples of quantum computers will lead to the fact that many cryptosystems, primarily asymmetric, will become unstable, which will lead to the impossibility of using asymmetric cryptosystems and, consequently, to the impossibility of secure data transmission in dual-use and military systems. Electronic signatures and key distribution schemes will also cease to be secure. It means that it is already necessary to develop new asymmetric crypto algorithms. At the same time, symmetric encryption algorithms will remain stable, but the effective key length of such algorithms will decrease by half [1,2,29,31-34].

## Conclusions

The stability analysis of the discrete algorithm *(DLP)* and the discrete algorithm with an elliptic curve *(ECDLP)* on the example of a number of applications improved the implementation of the original quantum Shor factorization algorithm. The algorithm is polynomial and is different from the known fundamental ability of software and hardware implementation in a hybrid computing environment (quantum computer IBM Q (16,20 and 100 cubits), and*/or Super-computer 5-generation IBM BladeCenter (2020), PBC on FPGA Virtex UltraScale (2020), VS RFNC-VNIIEF (2021) and SKIF P-0.5 (2018).*

In the course of the work, a variant of the Grover quantum search algorithm was developed, the analysis of the limiting possibilities of which helped to establish that the overkill problem does not receive exponential quantum acceleration. However, it becomes possible to reduce the effective key length of symmetric encryption systems by exactly two times.

Modification of the Grover search algorithm for solving problems of cryptanalysis of symmetric encryption schemes developed an original quantum algorithm for restoring the symmetric encryption key from the message text and ciphertext. The proposed algorithm solves the mentioned cryptanalysis problems with acceptable complexity and labor intensity.

Analysis of the durability of RSA asymmetric encryption schemes based on the computational complexity of the integer factorization problem (DLP) allowed us to develop a polynomial quantum algorithm for cryptanalysis of the RSA asymmetric encryption system. The algorithm is polynomial and is different from the known fundamental ability of software and hardware implementation in a hybrid computing environment (quantum computerIBM Q (16,20 and 100 cubits), and/or Super-computer 5-generation *IBM BladeCenter (2020), PBC on FPGA Virtex UltraScale (2020), VS RFNC-VNIIEF (2021) and SKIF P-0.5 (2018).*

Analysis of the strength of asymmetric encryption schemes, based on the computational complexity of the discrete logarithm problem (ECDLP), developed a polynomial quantum algorithm for cryptanalysis of the El-Gamal system. This made it possible to determine the requirements for the length of quantum registers (from several hundred qubits), sufficient to solve cryptanalysis problems in practice.

*The article was prepared based on the results of research carried out with the support of the RFBR grant (No. 20-04-60080).*

**References**

1. Alexei Petrenko, Applied Quantum Cryptanalysis (научная монография «Прикладной квантовый криптоанализ»), ISBN: 9788770227933, e-ISBN: 9788770227926, River Publishers, 2022. — 256 pp. (SCOPUS) https://www.riverpublishers.com/book_details.php?book_id=1028
2. Shor's algorithm, its implementation in Haskell and the results of some experiments [Electronic resource] / Programmer's Notes. — Access mode: http://eax.me/shors-algorithm — 14.05.2021 p .
3. Bogdanov A.Yu. Quantum algorithms and their impact on the security of modern classical cryptographic systems / A.Yu. Bogdanov, I.S. Kizhvatov // RGGU. — 2005. — 18 p.
4. Valiev K.A. Quantum computers and quantum computations / K.A. Valiev.-M.:Institute of Physics and Technology, 2005.- 387c.
5. Vasilenko O. N. Number-theoretic algorithms in cryptography / O. N. Vasilenko. — M.: ICNMO, 2003. — 328 p.
6. Denisenko D.V., Marshalko G.B., Nikitenkova M.V., Rudskoy V.I., Shishkin V.A. Evaluation of the complexity of implementing the Grover algorithm for sorting the keys of block encryption algorithms GOST R 34.12-2015, Journal of Experimental and Theoretical Physics, RAS, P.L. Institute of Physical Problems. Kapitsy RAS (Moscow), 2019, volume 155, issue 4, pp. 645-653, 2019.

7. Ishmukhametov Sh.T. Methods of factorization of natural numbers.: textbook / Sh.T. Ishmukhametov. — Kazan: Kazan University. — 2011. — 192 p.
8. Kitaev A., Shen A., Vyaly M. Classical and quantum computing / M.: ICNMO, Publishing House of Chero, 1999. — 192 p.
9. Kolmogorov, A.N. Information theory and theory of algorithms. USSR Academy of Sciences, Moscow: Nauka, 1987.
10. Kotelnikov V. A. The fate that engulfed the century. In 2 t. / comp. N. V. Kotelnikova. Moscow: Fizmatlit, 2011. 312 p.
11. Korolkov A.V. On some applied aspects of quantum cryptography in the context of the development of quantum computing and the emergence of quantum computers. / A.V. Korolkov // Issues of cybersecurity No. 1(9) — 2015. — M.: Journal “Issues of cybersecurity”, 2015. — pp. 6-13.
12. Korzh O.B., Andreev D.Yu., Korzh A.A., Korobkov V.A., Chernyavsky A.Yu., Modeling of an ideal quantum computer on a Lomonosov supercomputer, Journal “Computational Methods and Programming”, Ed. Research Computing Center of Moscow State University named after M.V. Lomonosov, 2013, No. 14, issue 2, pp. 24-34
13. Korzh O.B., Chernyavsky A.Yu., Korzh A.A.,Simulation of the quantum Fourier transform with noise on the Lomonosov supercomputer, CollectionScientific service on the Internet: all facets of parallelism: Proceedings of the International Supercomputer Conference (September 23-28, 2013, Novorossiysk), Ed. of the Moscow State University. Lomonosova, Moscow, pp. 188-193.
14. Klyucharev P.G. Abstract of the dissertation for the Candidate of Technical Sciences. Algorithmic and software for modeling a quantum computer. Moscow State Technical University named after N.E. Bauman, 2009, 18 p.
15. Manin Yu .I. Computable and non-computable. Moscow: Sovetskoe radio, 1980. 128 p.
16. Moldovyan A.A., Moldovyan N.A. New forms of the hidden discrete logarithm problem. Proceedings of SPIIRAN 2019. Volume 18 No. 2. Pp. 504-529.
17. Moldovyan N.A.,Introduction to Public Key Cryptosystems / N.A. Moldovyan,Moldovyan A.A./, Publishing House of BHV-Petersburg, 2005, 286 p. — 2005.
18. Moldovyan N.A., Workshop on cryptosystems with a public key, Publishing House BHV-Petersburg, 2005, 298 p. — 2007.
19. Nikolenko S.I. New constructions of cryptographic primitives based on semigroups, groups and linear algebra. Dissertation for the Candidate of Physical and Mathematical Sciences. St. Petersburg, Institution of the Russian Academy of Sciences St. Petersburg Department of the Mathematical Institute named after V.A. Steklova RAS, 2008 — 120 p.
20. Shannon K. Works on information theory and cybernetics / edited by R. L. Dobrushina, O. B. Lupanova. — M. : Publishing House of Foreign Literature, 1963 — 830 p.
21. Schneier B. Applied cryptography: protocols, algorithms, source code in the C language. Williams Publishing House, 2016– — 816 p.
22. Shor P. Algorithms for quantum computation: discrete logarithms and factoring [Text] /Shor P. // Foundations of Computer Science.—1994.—№10. —134p.
23. Deutsch D., Quantum theory, the Church-Turing principle and the universal quantum computer, Proceedings of the Royal Society A. 400 (1818), 97 — 117 (1985)
24. Deutsch D., Jozsa R., Rapid solution of problems by quantum computation, Proceedings of the Royal Society of London A, 439, (1907), 553-558 (1992)
25. Feynman R, Simulating physics with computers, Internat. J. Theoret. Phys. 21, 467 — 488 (1982)
26. Grover L.K., A fast quantum mechanical algorithm for database search, In Proceedings of the twenty-eighth, annual ACM symposium on Theory of computing, 212 – 219, ACM (1996)
27. Huang C, Zhang F., Newman M/, Classical Simulation of Quantum Supremacy Circuits, arxiv.org/abs/2005.06787 (2020) 19. A. Zlokapa, S. Boixo, D. Lidar, Boundaries of quantum supremacy via random circuit sampling, arxiv.org/abs/2005.02464 (2020)
28. Johnston, Eric R., Nic Harrigan, and Mercedes Gimeno-Segovia (2019). Programming Quantum Computers: Essential Algorithms and Code Elements. Sebastopol, CA: O’Reilly.
29. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Computing 26, 1484 – 1509 (1997)
30. Simon D.R., On the power of quantum computation, SFCS ‘94: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 116 – 123 (1994)
31. S.E. Yunakovsky, M. Kot, N.O. Pozhar, D. Nabokov, M.A. Kudinov, A. Guglya, E.O. Kiktenko, E. Kolycheva, A. Borisov, A.K. Fedorov. Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. EPJ Quantum Technology (2021) arXiv: 2105.01324
32. Grebnev S.V. Post-quantum cryptography: Trends, problems and prospects. Information Security. 2019, 2.
33. I.S. Kabanov, R.R. Yunusov, Y.V. Kurochkin, and A.K. Fedorov. Practical cryptographic strategies in the post-quantum era, AIP Conference Proceedings 1936, 020021 (2018); arXiv:1703.04285
34. V. S. Belsky, I. V. Chizhov, A. A. Chichaeva, V. A. Shishkin. Physically unclonable functions in cryptography. International Journal of Open Information Technologies ISSN: 2307-8162 vol. 8, no.10, 2020

# ОСНОВНЫЕ АЛГОРИТМЫ КВАНТОВОГО КРИПТОАНАЛИЗА

***Петренко А.С.[3], Петренко С.А.[4]***

***Цель работы:*** *разработка квантовых алгоритмов для результативного решения задач криптоанализа схем асимметричного шифрования (RSA, Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS), базирующихся на вычислительно трудных задачах факторизации и дискретного логарифмирования.*

***Методы исследования:*** *Методы квантового криптоанализа на основе алгоритмов Шора, Гровера, Саймона и др.*

***Результаты исследования:*** *алгоритмы решения задач квантового криптоанализа схем двухключевой криптографии за полиномиальное время.*

***Научная и практическая значимость*** *результатов статьи состоит в выработке решения для вычислительно трудных задач факторизации и дискретного логарифмирования за полиномиальное время с учетом стойкости дискретного алгоритма (DLP) и дискретного алгоритма с эллиптической кривой (ECDLP). Полученные научные результаты легли в основу разработки специального Комплекта для разработки программного обеспечения, SDK криптоанализа «Квант-К». Получено Свидетельство о государственной регистрации программы для ЭВМ №2020665981.*

***Ключевые слова:*** *квантовая угроза безопасности, криптографические атаки, квантовый криптоанализ, квантовые алгоритмы, алгоритмы Шора, Гровера и Саймона, квантовое преобразование Фурье, задачи факторизации и дискретного логарифмирования.*

*Статья подготовлена по результатам исследований, выполненных при поддержке гранта РФФИ (№ 20-04-60080).*

**DOI:** 10.21681/2311-3456-2023-1-100-115

**References**

1. Alexei Petrenko, Applied Quantum Cryptanalysis (научная монография «Прикладной квантовый криптоанализ»), ISBN: 9788770227933, e-ISBN: 9788770227926, River Publishers, 2022. — 256 pp. (SCOPUS) https://www.riverpublishers.com/book_details.php?book_id=1028
2. Shor's algorithm, its implementation in Haskell and the results of some experiments [Electronic resource] / Programmer's Notes. — Access mode: http://eax.me/shors-algorithm — 14.05.2021 p .
3. Bogdanov A.Yu. Quantum algorithms and their impact on the security of modern classical cryptographic systems / A.Yu. Bogdanov, I.S. Kizhvatov // RGGU. — 2005. — 18 p.
4. Valiev K.A. Quantum computers and quantum computations / K.A. Valiev.-M.:Institute of Physics and Technology, 2005.- 387c.
5. Vasilenko O. N. Number-theoretic algorithms in cryptography / O. N. Vasilenko. — M.: ICNMO, 2003. — 328 p.
6. Denisenko D.V., Marshalko G.B., Nikitenkova M.V., Rudskoy V.I., Shishkin V.A. Evaluation of the complexity of implementing the Grover algorithm for sorting the keys of block encryption algorithms GOST R 34.12-2015, Journal of Experimental and Theoretical Physics, RAS, P.L. Institute of Physical Problems. Kapitsy RAS (Moscow), 2019, volume 155, issue 4, pp. 645-653, 2019.
7. Ishmukhametov Sh.T. Methods of factorization of natural numbers.: textbook / Sh.T. Ishmukhametov. — Kazan: Kazan University. — 2011. — 192 p.
8. Kitaev A., Shen A., Vyaly M. Classical and quantum computing / M.: ICNMO, Publishing House of Chero, 1999. — 192 p.
9. Kolmogorov, A.N. Information theory and theory of algorithms. USSR Academy of Sciences, Moscow: Nauka, 1987.
10. Kotelnikov V. A. The fate that engulfed the century. In 2 t. / comp. N. V. Kotelnikova. Moscow: Fizmatlit, 2011. 312 p.
11. Korolkov A.V. On some applied aspects of quantum cryptography in the context of the development of quantum computing and the emergence of quantum computers. / A.V. Korolkov // Issues of cybersecurity No. 1(9) — 2015. — M.: Journal "Issues of cybersecurity", 2015. — pp. 6-13.

3 Петренко Алексей Сергеевич, Исследователь по направлению 10.06.01 «Информационная безопасность» ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)», финалист Всероссийского конкурса научных проектов, Санкт-Петербург, Россия. orcid.org/ 0000-0002-9954-4643, E-mail: A.Petrenko1999@rambler.ru

4 Петренко Сергей Анатольевич, Профессор кафедры информационной безопасности (ИБ), доктор технических наук, профессор ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)», лауреат года-2022 просветительской Премии «Знание», Санкт-Петербург, Россия. orcid.org/0000-0003-0644-1731, E-mail: S.Petrenko@rambler.ru

12. Korzh O.B., Andreev D.Yu., Korzh A.A., Korobkov V.A., Chernyavsky A.Yu., Modeling of an ideal quantum computer on a Lomonosov supercomputer, Journal “Computational Methods and Programming”, Ed. Research Computing Center of Moscow State University named after M.V. Lomonosov, 2013, No. 14, issue 2, pp. 24-34
13. Korzh O.B., Chernyavsky A.Yu., Korzh A.A.,Simulation of the quantum Fourier transform with noise on the Lomonosov supercomputer, CollectionScientific service on the Internet: all facets of parallelism: Proceedings of the International Supercomputer Conference (September 23-28, 2013, Novorossiysk), Ed. of the Moscow State University. Lomonosova, Moscow, pp. 188-193.
14. Klyucharev P.G. Abstract of the dissertation for the Candidate of Technical Sciences. Algorithmic and software for modeling a quantum computer. Moscow State Technical University named after N.E. Bauman, 2009, 18 p.
15. Manin Yu .I. Computable and non-computable. Moscow: Sovetskoe radio, 1980. 128 p.
16. Moldovyan A.A., Moldovyan N.A. New forms of the hidden discrete logarithm problem. Proceedings of SPIIRAN 2019. Volume 18 No. 2. Pp. 504-529.
17. Moldovyan N.A.,Introduction to Public Key Cryptosystems / N.A. Moldovyan,Moldovyan A.A./, Publishing House of BHV-Petersburg, 2005, 286 p. — 2005.
18. Moldovyan N.A., Workshop on cryptosystems with a public key, Publishing House BHV-Petersburg, 2005, 298 p. — 2007.
19. Nikolenko S.I. New constructions of cryptographic primitives based on semigroups, groups and linear algebra. Dissertation for the Candidate of Physical and Mathematical Sciences. St. Petersburg, Institution of the Russian Academy of Sciences St. Petersburg Department of the Mathematical Institute named after V.A. Steklova RAS, 2008 — 120 p.
20. Shannon K. Works on information theory and cybernetics / edited by R. L. Dobrushina, O. B. Lupanova. — M. : Publishing House of Foreign Literature, 1963 — 830 p.
21. Schneier B. Applied cryptography: protocols, algorithms, source code in the C language. Williams Publishing House, 2016– — 816 p.
22. Shor P. Algorithms for quantum computation: discrete logarithms and factoring [Text] /Shor P. // Foundations of Computer Science.—1994.—№10. —134p.
23. Deutsch D., Quantum theory, the Church-Turing principle and the universal quantum computer, Proceedings of the Royal Society A. 400 (1818), 97 — 117 (1985)
24. Deutsch D., Jozsa R., Rapid solution of problems by quantum computation, Proceedings of the Royal Society of London A, 439, (1907), 553-558 (1992)
25. Feynman R, Simulating physics with computers, Internat. J. Theoret. Phys. 21, 467 — 488 (1982)
26. Grover L.K., A fast quantum mechanical algorithm for database search, In Proceedings of the twenty-eighth, annual ACM symposium on Theory of computing, 212 – 219, ACM (1996)
27. Huang C, Zhang F., Newman M/, Classical Simulation of Quantum Supremacy Circuits, arxiv.org/abs/2005.06787 (2020) 19. A. Zlokapa, S. Boixo, D. Lidar, Boundaries of quantum supremacy via random circuit sampling, arxiv.org/abs/2005.02464 (2020)
28. Johnston, Eric R., Nic Harrigan, and Mercedes Gimeno-Segovia (2019). Programming Quantum Computers: Essential Algorithms and Code Elements. Sebastopol, CA: O’Reilly.
29. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Computing 26, 1484 – 1509 (1997)
30. Simon D.R., On the power of quantum computation, SFCS ‘94: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 116 – 123 (1994)
31. S.E. Yunakovsky, M. Kot, N.O. Pozhar, D. Nabokov, M.A. Kudinov, A. Guglya, E.O. Kiktenko, E. Kolycheva, A. Borisov, A.K. Fedorov. Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. EPJ Quantum Technology (2021) arXiv: 2105.01324
32. Grebnev S.V. Post-quantum cryptography: Trends, problems and prospects. Information Security. 2019, 2.
33. I.S. Kabanov, R.R. Yunusov, Y.V. Kurochkin, and A.K. Fedorov. Practical cryptographic strategies in the post-quantum era, AIP Conference Proceedings 1936, 020021 (2018); arXiv:1703.04285
34. V. S. Belsky, I. V. Chizhov, A. A. Chichaeva, V. A. Shishkin. Physically unclonable functions in cryptography. International Journal of Open Information Technologies ISSN: 2307-8162 vol. 8, no.10, 2020