Date Science: Post Quantum Safe Cryptography

A. Aktayeva[1], R. Niyazova[2], L. Davletkireeva[3], A. Baikenov[4]

[1]Sh.Ualikhanov Kokshetau State University, Abay str. 76, Kokshetau, Kazakhstan, 020000
[2]L.N.Gumilyov Eurasian National University, Satpayev str. 2, Astana, Kazakhstan, 010008
[3]Nosov Magnitogorsk State Technical University, Lenin Avenue 38, Magnitogorsk, Russia, 455000
[4]Almaty University of Power Engineering and Telecommunications, A. Baitursynov str. 126B, Almaty, Kazakhstan, 050013

Abstract. New cryptographic techniques have emerged in recent decades that do provide protection against quantum threats. These techniques are termed “postquantum cryptography” and consist of techniques based on quantum properties of light that prevent interception of messages, as well as classic computational techniques, all of which were designed to resist quantum attacks emerging from the rapidly accelerating research field of quantum computation. This paper provides background information on post-quantum security. It explores the security threats against communication security and particularly against key exchange that are enabled by the development of quantum computers. The applied and theoretical aspects of quantum-cryptographic technologies are considered, which is designed to be a reference for those operating in the ICT space in fields other than information security and postquantum cryptography. The interrelated elements that make up the concept and content determined by the application of quantum cryptography are analyzed. The systematic analysis of quantum algorithms, quantum cryptography and quantum hashing are presented. The proper concept vehicle over is brought, in particular the concepts of singularity and supersingularity are determined for elliptic curves and theoretical positions, lyings in their basis, are examined. Terms which must be taken into account at the selection of elliptic curves for cryptographic applications are determined.

1. Introduction

Quantum resource theories attempt to capture what is quintessentially quantum in a piece of technology. Quantum computing is a relatively young and very rapidly developing field of modern science. Of the most important directions of quantum computing, one can single out quantum computations, quantum cryptography and modelling of quantum systems. Eventually with the successful creation of a quantum computer, the algorithms implemented on it will allow solving some important tasks faster than on classical computers. The resource framework for entanglement finds practical application in bounding the efficiency of entanglement distillation protocols. An abundance of other resource theories have been related to various aspects of quantum theory. Once a quantum computer is made fault-tolerant, some computational operations become relatively easy, and some more difficult [9, 10].

In the past have been looked of quantum computing experiments that one finds an exponential increase in the number of, similar to Moore's law for classical computers. As the qubit scale is

logarithmic, this clearly corresponds to an exponential increase, similar to Moore's law for classical computers and is a fit to the data, indicating a doubling of the number of qubits every 5.7 ±0.4 year.
Therefore, National Institute of Standards and Technology (NIST) is currently standardizing algorithms and the first standards for post-quantum cryptographs are expected in 2022–2023.The quantum computing power doubles about every six years, with quantum computers for real applications arriving in between nine and twelve years if this trend continues (see Fig. 1).

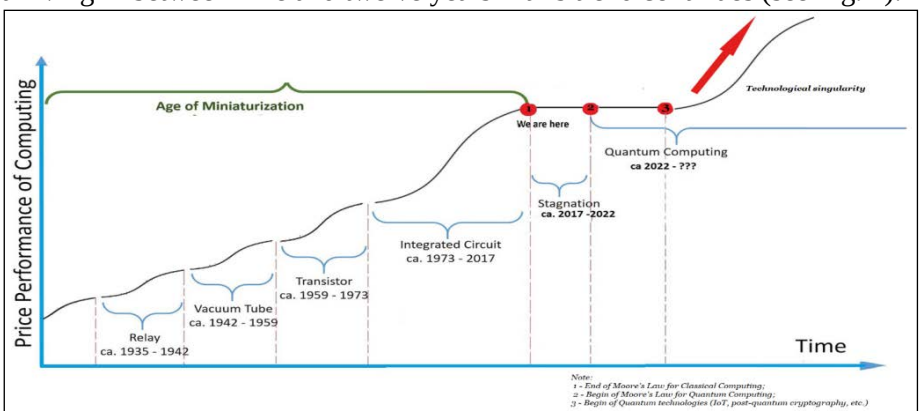

Figure 1. Moore's Law for Quantum Computers [28].

A quantum transmits information promises completely secure communication. However, using quantum bits or qubits to carry information requires a radically new piece of innovation technologies - the quantum computing. This innovate technologies needs to store quantum information and convert it into light to transmit across the network. A major challenge to this vision is that qubits are extremely sensitive to their environment; even the vibrations of nearby atoms can disrupt their ability to remember information. So far, researchers have relied on extremely low temperatures to quiet vibrations, but achieving those temperatures for large-scale quantum networks is prohibitively expensive. Therefore, it is necessary to know the number of qubits for the quantum transmit information that to promise completely secure communication.
More detailed investigation reveals that an empirical analysis of scalability in quantum computing allows making predictions that go beyond the usual saying that practical quantum computers are “twenty years away”. Since we are mostly interested in scalability of modules in larger solutions that the natural quantity of interest is the number of qubits realized in an experiment. First, experiments should be used within strict limits once its value had been demonstrated coherent manipulation of individual quantum objects, such as multi - qubit gates or generation of mutual entanglement that entanglement is not merely generated as a natural process, otherwise the Bell experiments going back to Clauser in 1972.
The first real applications of quantum computers will come in the area of simulating difficult quantum many-body problems arising, such as, in high-temperature superconductivity, quark bound states such as proton and neutrons, or quantum magnets. For these problems, the record for classical simulations is now at 42 qubits, which need to control 51 qubits in the quantum computer to beat classical simulations [26].
In any case, it is perfectly fine to use such natural events as a resource for creating higher order entangled states, as it is done in linear optics quantum computers. While there is certainly some ambiguity with these definitions that the resource for creating higher order entangled states have only little impact on the results. Currently, the world record in mutual entanglement is at 14 qubits, demonstrated by Rainer Blatt's ion trap group in Austria [28].

2. Materials and methods

Quantum states can be used to record the values of a classical bit of information. The basis of a vector space is given only by two orthogonal unit vectors denoted as $|0\rangle$ and$|1\rangle$, respectively. But a qubit can also occupy a state where both values are in superposition.

In the context of the classical information theory, qubits characterize direct resources of a signal transmitted, which can be used to transmit information over the quantum channel. For the purpose of noise immunity of quantum computing, there is another approach that creates such operations on logical qubits, when error propagation among physical qubits would be limited enough to use appropriate corrective codes. This can be achieved by constructing special transversal gates, which would carry out the interaction of qubits of one encoded cluster only with relevant qubits of another cluster [11].

If there is a source that produces pure states $|\varphi_1|, \ldots |\varphi_a|$, ith the probabilities p1,…pa (analogue of the classical alphabet), long sequences of letters of a word can be transmitted, i.e., each word is given as the following sequence:

$$\omega = (x_1, \ldots, x_n), x_j \epsilon \{1, \ldots, a\}.$$

In contrast to, a classical bit, a quantum bit can be represented by a random superposition of basis vectors of photon states

$$|\psi\rangle = a|H\rangle + b|V\rangle, \text{ where a and b}$$

arbitrary complex numbers satisfying the condition

$$|\psi\rangle = a|H\rangle + b|V\rangle,$$

and it can be represented, as in the case of spin, on the Bloch sphere (Fig.2), and single qubit operations represent a rotation of the Bloch vector [5].

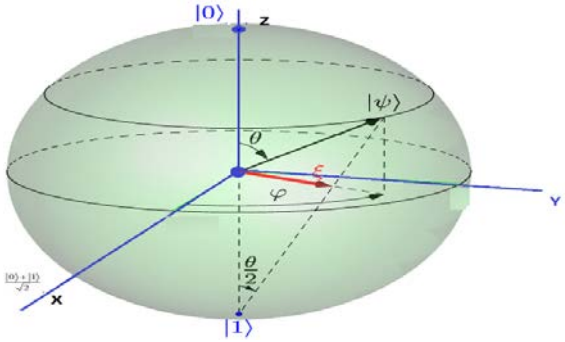

Figure 2. Qubit on the Bloch sphere.

A photon travelling at the speed of light has two states of polarization vector (H) and (V), which are orthogonal to each other and orthogonal to the direction of the photon. The horizontally polarized photon (H) represents the basic state of the qubit $|0\rangle$, and the vertically polarized photon (V) represents the basic state

$$|1\rangle: |0\rangle = |H\rangle, \ |1\rangle = |V\rangle.$$

If measured in the basis, the qubit can be represented in a variety of physical systems [5,7,8].

When two qubits in superposition are also entangled, they together can store all the possible combinations of the quantum states of the qubits, resulting in four values. Adding another qubit to the entangled pair will double the number of combinations and thus the values that can be stored, and so on. After 20 such doublings, 20 entangled qubits can store 220, or 1,048,576 values.

Although this sounds impressive in terms of classical computing, that number is too small to execute a quantum computation. Unlike a classical computer, which processes computations following a large number of sequential steps dictated by the program, the qubit register receives the entire instruction for a computation in one go, and spits out the result almost instantaneously, in a single process. Therefore, the quantum register has to contain sufficient qubits, at least several thousand, to absorb the instruction for the computation. Systems of quantum states with many entangled qubits become very complicated. This will require a lot of fine-tuning and new ways for investigating large numbers of entangled qubits.

Experimentally, these operations are performed using a birefringent wave plate, which retards the phase of one polarization by a certain fraction of a wave length with respect to a polarization orthogonal to it causing the rotation of the Bloch vector on the Bloch sphere (see Fig.2).

Operations with qubits are quantum and probabilistic in nature, and this fact determines some of the features of such operations. In general, there are three classes of quantum algorithms:

1. Algorithms based on the quantum Fourier transform;
2. Quantum search algorithms;
3. Algorithms of quantum system simulation [5,26].

In all cases, the quantum algorithm solves the problem more effectively than the classical one [3].
At the moment, the quantum threat is theoretical as quantum computers that fulfill the requirements of Shor's algorithm are not available (see Fig.3). To break an RSA algorithm with a key size of 2048, a quantum computer of 10,000 qubits or 4000 qubits with 100 million gates is needed. To break a 160-bit ECC key, a quantum computer of around 1000 qubits is needed [21,22,23].

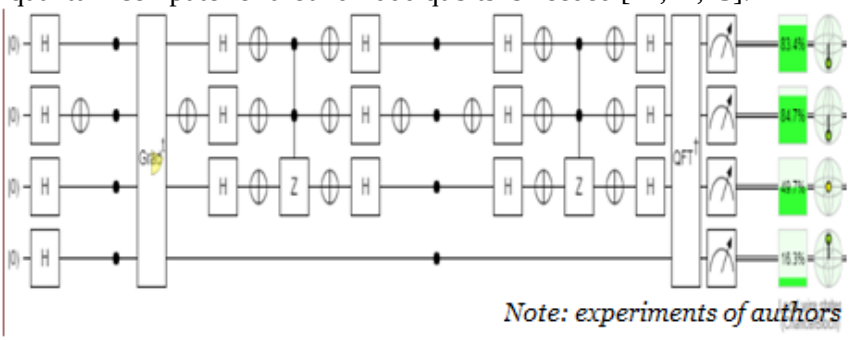

Figure 3. Quantum Circuit Implementing Grover's Search Algorithm.

According to the most optimistic views, a million qubit system, corresponding to 1000 error corrected qubits might be conceivable within 10 years [26]. Many believe that the construction of a quantum computer for Shor's algorithm will take decades should it ever emerge at all. Nevertheless, the potential existence of even one quantum computer offers motivation to secure trillions of connections with solutions, which are not weak against quantum computers.
A prominent application for quantum computers is cryptanalysis, i.e., the breaking of cryptographic protocols. In particular, the following algorithms for quantum computers are efficient and will have a major impact on security:

- Shor's algorithm [1,2] will break asymmetric cryptography. The algorithm can be used to solve integer factorization and (elliptic curve) discrete logarithms, which have been used in many existing public keys cryptosystems, including Rivest – Shamir – Adleman (RSA), Digital Signature Algorithm (DSA), Diffie – Hellman (DH) key exchange, as well as Elliptic Curve Cryptography (ECC) (see Fig.4).
- Grover's algorithm [3] will weaken symmetric cryptography (see Fig.5). The algorithm will speed up brute force attacks against symmetric cryptography, such as Advanced Encryption Standards (AES) and Secure Hash Algorithm versions 2 and 3 (SHA-2, SHA-3).

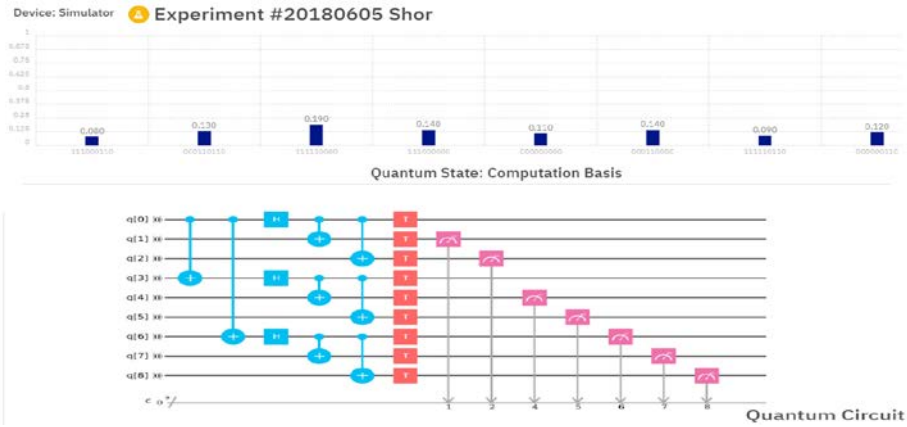

Figure 4. Encoding circuit for the Shor nine qubit code (Note: experiments of authors).

Optimization and search problems benefiting from Grover's algorithm could become tractable somewhat later, but that depends a lot on the problem at hand, but same scaling continues even further, 2048-bit RSA keys would come under attack somewhere between 2052 and 2059.

Figure 5. circuit for the Grover's algorithm (Note: experiments of authors).

This Figure shows a quantum circuit implementing Grover's search algorithm that enables finding any given integer from the list , where , with a probability that is very close to 1, repeating Grover's iterations times, where is the integer part of the number .

Figure 6 illustrate two different threat models in post-quantum scenarios. The figures combine elements that are relevant both for the physical layer security as well as for cryptographic security. In both figures, we have Alice and Bob communicating via a wireless channel. In the first figure, we have the passive eavesdropper Eve. To prevent eavesdropping, Alice and Bob are trying to agree on a secret session key that can be used to protect (with some symmetric cipher) the confidentiality of any subsequent application data.

The key agreement must be confidential, but it can be based on a cryptographic or physical layer scheme. Note that Eve does not need to have run-time quantum breaking capabilities. If she is able to capture all the transmitted key exchange information and subsequent protected communication, she may, later when she has a quantum computer, resolve the session key using Shor's algorithm and decrypt the recorded communication.

Attackers' abilities to capture transmissions have been considered as granted in classical threat models for cryptographic solutions. However, in the case of physical layer security, this assumption is sometimes considered too strong.

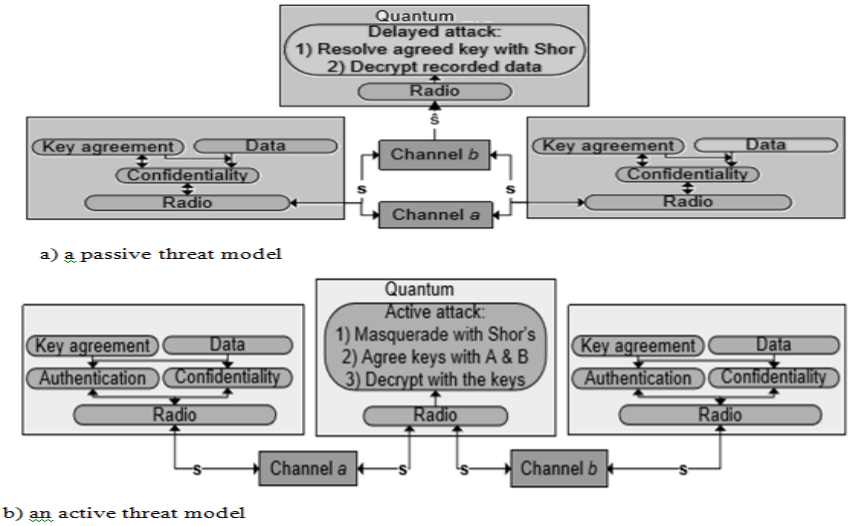

Figure 6. A physical layer eavesdropper with quantum capabilities in the future [24].

In the second scenario, we have the active man-in-the-middle attacker Mal. This threat model requires an additional authentication approach resistant against the man-in-the-middle attacker. This requirement can be fulfill, with cryptographic authentication, but not with secrecy coding in the physical layer that lacks strong authentication capabilities. Consequently, the time when security solutions must be quantum immune is the quantum era (the time when quantum computers for Shor's algorithm exist) minus N years, where N is the time that the protected information must be kept secret. In authentication *N* is zero because, to break an authentication scheme, the attacker must have quantum computer capabilities during the authentication procedure and active attack. In confidentiality protection, on the other hand, the attacker can just store the cipher text and then wait until the quantum computer emerges. This insight is relevant for quantum immune solutions that do not provide authentication. In the era where we are waiting quantum computers, it is safe to use classical authentication mechanisms as long as other parts of the security system are quantum immune [24].

Many experts consider quantum cryptography as the only method that can provide real protection of communication systems, both currently and in the foreseeable future, based on transferring information by quantum states of photons [1 - 5, 7, 28, 29]. In contrast with traditional cryptography, which uses mathematical methods to ensure the secrecy of information, quantum cryptography works with physics of information transmission. The quantum cryptography technology relies on the properties of quantum systems:

- inability to measure the quantum system without disturbing it;
- inability to determine both the position and state of a particle with arbitrarily high precision;
- inability to check the polarization of a photon in vertical and horizontal, as well as in diagonal directions;
- inability to duplicate the quantum state until it is measured [29].

Quantum computing challenges this assumption because it offers a new and powerful set of tools under which many of these cryptosystems may collapse. Any data that has been encrypted using many cryptosystems whose security were based on the computational intractability of the so-called "hard problems" of the discrete log and integer factorization is under threat to both eavesdrop and attacks by future adversaries in possession of quantum computers. Many safe encryption systems technologies have already been demonstrated even purely classical cryptosystems may become insecure about the presence of a quantum computer, including some of the most pervasive cryptosystems such as RSA and Elliptic Curve Cryptography [29].

The attempt to find answers to the quantum challenges in supporting the information security system and data protection is quantum cryptography. The main efforts in this field are focused on problems of the synthesis of cryptographic algorithms, protocols resistant to capabilities of quantum computers and the most important cryptographic primitives used today are:

- AES for symmetric encryption,
- RSA and ECC for public-key encryption,
- DSA and ECDSA for signatures,
- DH and ECDH for key exchange, and
- SHA-1, SHA-2, or SHA-3 for hashing.

These schemes are standardized by various entities, e.g., NIST, ISO, IETF, and BSI. By now, several dozens of secure quantum communication protocols of different purposes have been offered (BB84, EPR, B92 (4+2), SARG04, CSS, LO-CHAU, Goldenberg - Vaidman, Koashi - Imoto, Ping-Pong, and others.) [5, 7, 8, 28, 29].

They are considered secure against powerful attacks with conventional computing systems when secure parameters are used.

Cryptographic schemes rely on the assumption that certain mathematical or computational problems are hard to solve for an attacker. Many of the cryptographic primitives that we use today are based on the assumption that the integer factorization problem and the discrete-logarithm problem are hard to solve. This assumption has proven reliable over the recent decades — in case traditional computing systems are used (see Fig. 7).

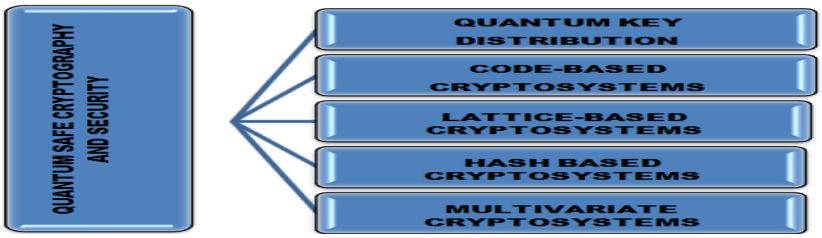

Figure 7. Main directions of studies in the information security system [7].

Many experts consider quantum cryptography as the only method that can provide real protection of communication systems, both currently and in the foreseeable future, based on transferring information by quantum states of photons. In contrast with traditional cryptography, which uses mathematical methods to ensure the secrecy of information, quantum cryptography works with physics of information transmission. The quantum cryptography technology relies on the properties of quantum systems:

- inability to measure the quantum system without disturbing it;
- inability to determine both the position and state of a particle with arbitrarily high precision;
- inability to check the polarization of a photon in vertical and horizontal, as well as in diagonal directions;
- inability to duplicate the quantum state until it is measured [5, 7, 26 - 29].

Quantum computing challenges this assumption because it offers a new and powerful set of tools under which many of these cryptosystems may collapse. Any data that has been encrypted using many cryptosystems whose security were based on the computational intractability of the so-called “hard problems” of the discrete log and integer factorization is under threat to both eavesdrop and attacks by future adversaries in possession of quantum computers. Many safe encryption systems technologies have already been demonstrated even purely classical cryptosystems may become insecure about the presence of a quantum computer, including some of the most pervasive cryptosystems such as RSA and Elliptic Curve Cryptography [30].

Most post quantum standards expect that the elliptic curve cryptography in the point format to be (x; y) on Weierstrass curves. Even when computations want to use the faster Edwards and Hessian formulas, should have been easily justified done specifying the curve in Weierstrass form. This also ensures compatibility backwards with existing implementations that can only use the Weierstrass form. The definition of an elliptic curve over a field K in the generalized Weierstrass form is rightly based on the third-degree equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ , } a_i \in \text{K.}$$

$$y^2=x^3+ax+b$$

Can be justifying the following curve shapes:

1. Weierstrass curves, the most general curve shaped. The usual choice is

$$y^2 =x^3 - 3x + b,$$

leaving one variable *b* is free. For simplicity does not discuss the possibility of choosing values other than -3.

2. Edwards curves, the speed leader in fixed-base scalar multiplication offering to complete in addition laws. The usual choices are

$$ax^2+y^2 = 1+dx^2y^2, \text{ for } a\ 2\ f\pm 1g,$$

leaving one variable *d is* free. The group order for an Edwards curve is divisible by 4.

3. Montgomery curves, the speed leader in variable-base scalar multiplication and the simplest to correctly implement. The usual choices are

$$y^2 = x^3 + Ax^2 + x,$$

leaving one variable *A is* free. The group order for a Montgomery curve is divisible by 4.

4. Hessian curves, a cubic curve shape of complete in addition law for twisted Hessian. The usual choices are

$$ax^3 +y^3 +1 = dxy,$$

where *a* is a small non-cube, leaving one variable *d is* free.
The group order for a Hessian curve is divisible by 3, making twisted Hessian curves the curves with the smallest cofactor while having a complete in addition laws. The following choices depend on the chosen curve shape, hence we consider them separately.
Description of the conditions of non-singularity to elliptic curve. So, our attention has been focused on elliptic curves E, which are given by an equation in the *canonical form of Weierstrass*

$$E: y^2 = x^3+ax^2+bx+c,$$

then a cubic equation of general form is also represented in this form

$$y^2=f(x), \text{ where } f(x)= x^3+ax^2+bx+c,$$

the right-hand side of equality has been regarded as an ordinary polynomial of the third degree. In what follows, we assume that the coefficients a, b, c are rational under the function *f(x)*, in particular, real numbers, and hence the polynomial f (x) of degree 3 has at least one real root. In real numbers, we can factor it as

$$f(x)= (x-\alpha)(x^2+ \beta x+\gamma),$$

where α, β, γ - are real numbers. If a polynomial have one real root, then to curve has a form similar in the Figure 1, a,

since $y = 0$, *when* $x = \alpha$.

If *f (x)* has all three real roots, then the curve has a form like that showed in the Figure 1, b. In this case, the real points form two components. It is true on the condition that the roots of the equation $f(x) = 0$ are different.
By definition, the singular means the point at which the derivative equals zero or does not exist. If the elliptic curve has a singular point, then the curve itself is said to be singular (see Fig.8).

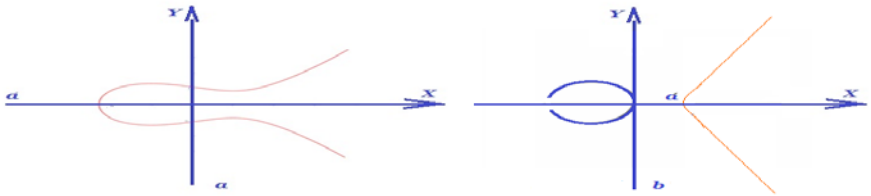

Figure 8. The form of the elliptic curve E for a polynomial: a - with one root, b - with three roots.

Accordingly, it is necessary to have a *non-singular curve* provided that there is no point of the curve in which the partial derivatives simultaneously disappear.

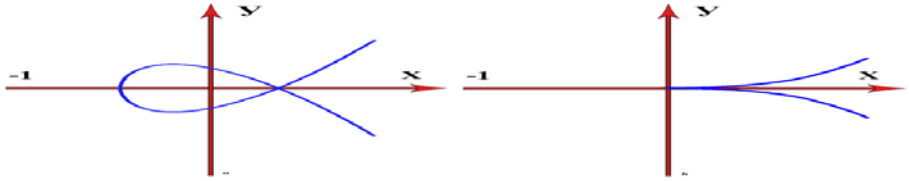

Figure 9. Types of singularity of the elliptical curve.

The discriminant D (f) of the algebraic equation
$f(x)= ax^n+a_{n-1}x^{n-1} +\ldots+a_1x+a_0,\ a_n\neq 0$
is the product an a_n^{2n-2} and the squares of all differences x_i-x_k $(i>k)$ of the roots x_i of the equation (*multiple roots of the order m are considered as m different roots with different indices).*

$$D(f) = a_n^{2n-2}\prod_{i>k}(x_i - x_k)^2 = a_n^{2n-2}[W(x_1, x_2 \ldots x_n)]^2$$

where the Vandermonde determinant

$$W(x_1 , x_2 , \ldots , x_n)=\begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ . & . & \cdots & . \\ 1 & x_n & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i>k}(x_i - x_k)$$

The discriminant *D(f)* is a symmetric function of the roots $x_1,x_2,\ldots,x_n$,, which vanishes if and only if *f (x)* has at least one multiple root that must be a root of *f (x)* and *f '(x).* Let us calculate, such as, the discriminant of a cubic trinomial

$$f(x) = x^3+bx+c,$$

the roots of which are $\alpha_1, \alpha_2, \alpha_3$. Using the above formula for

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b, \alpha_1 + \alpha_2 + \alpha_3 = 0,$$
$$\alpha_1\alpha_2\alpha_3 = -c,$$

obtained through this calculus

$$D(f) = 4b^3 - 27c^2.$$

For a curve in the normal form, the discriminant of the function f (x) is the quantity

$$D(f) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Thus, an elliptic curve with rational coefficients (that is, over a field R) with non-zero discriminant $D(f)\neq 0$ is a smooth curve. In the course of the research, an additional restriction on the choice of elliptic curves was discovered, related to the notion of super singularity. One of the realizations of this construction is exponentiation in a large finite field, which was proposed by Diffie and Hellman [29,30]. These principles have been used, in particular, for the construction of special cryptosystems with public keys and elliptic curves.

An elliptic curve is called supersingular if the endomorphism ring End (C) is noncommutative. For the "supersingularity" of the curve E, which is given by the equation

$$E: y^2+a_1 xy+a_3y=x^3+a_2x^2+a_4x+a_6, a_i \in K.$$
$$y^2=x^3+ax+b$$

one can use the fulfillment of the any following conditions:

$a_1= 0$, *(ii)* $|E(K)|$ is even $K= F(p^m)$,*j*- invariant of *E* is zero.

Nonsupersingular elliptic curves in the construction of cryptosystems open the possibility of a wide choice of many different groups of different orders. This difference proves to be an additional advantage over the use of groups of finite fields, where there is only one candidate for each field.

At the same time, the existence of an isomorphic mapping for some set of points of the elliptic curve

$$E(K) = E(Fq)$$

to the subgroup of the multiplicative extensive group of the field F_q allows us to reduce the discrete logarithm problem for a nonsingular elliptic curve to finding a discrete logarithm in a finite Galois field. For a non-perpsingular curve, one can construct an extension of the field with a small degree of expansion.

The calculation of the complexity of group operations on the Weierstrass curve in these expressions makes it difficult to calculate the sum of the points of the canonical curve

$$W: Vw = 12M + 2S.$$

A similar calculation for doubling the points leads to the result

$$Tw = 7M + 5S.$$

The main advantages of operations on the canonical elliptic Weierstrass curve are the high computational speed, completeness of the addition law, and the presence of affine coordinates of the neutral element of the additive group of curve points.

3. Conclusion

Our observations demonstrate that further improvement in coherence and controllability could be obtained by encoding qubits into hyperfine sublevels of the electronic ground state and using state-selective excitation. Although our current observations already provide insights into the physics associated with transitions into ordered phases and enable us to explore new many-body phenomena in quantum informatics, they can be extended along several directions. These include studies of various aspects of many-body coherence and entanglement in large arrays, investigation of critical dynamics and tests of the quantum hypothesis, and the exploration of stable non-equilibrium phases of matter.

Finally, we note that our approach is well suited for the realization and testing of quantum optimization algorithms, with system sizes that cannot be simulated by post modern classical computing. The challenge of scalability in quantum computing remains an area of vivid speculation in discussions both within the scientific community and beyond it. Yet, to my knowledge, nobody has

ever made an effort to quantify the track record of the field. Nevertheless, as quantum computing advances are reported the notion of “quantum-safeness” is still somewhat of an emerging area, and we expect to hear much more over the coming months and years should be have worked to ensure a quantum safe future.

4. References

[1] Benioff, P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines // J. Stat. Phys. – 1980. – Vol. 22. – P. 563-591.

[2] Deutsch, D. Quantum theory, the Church-Turing principle and the universal quantum computer // Proc. Roy. Soc. – 1985. – Vol. A400. – P. 96-117.

[3] Cleve, R. Quantum algorithms revisited / R. Cleve, A. Ekert, C. Macchiavello, M. Mosca // Phil. Trans. Royal Soc. – 1998. – Vol. A45. – P. 339-354.

[4] Turing, A. On computable numbers with an application to the Entscheidungs problem // Proc. Math. Society. –1937. – Vol. 42. – P. 230-265.

[5] Holevo, A.S. Mathematical fundamentals of quantum informatics. – M.: 2016. – 125 p.

[6] Baumester, D. Physics of quantum information / D. Baumester, A. Ekert. – M.: Post market, 2002.

[7] Aktayeva, A.U. Innovative technologies in an information security system: quantum technologies / A.U. Aktayeva, L.I. Ilipbayeva //Modern innovative technologies and IT education. – 2014. – Vol. 1(9). – P. 320-326.

[8] Aktayeva, A. Artificial intelligent intrusion detection systems: perspectives of innovative technologies / A. Aktayeva, A. Niyasova, N. Gagarina // Modern Information Technologies and IT Education. – 2017. – Vol. 13(3). – P. 45-52.

[9] Valiev, K.A. Quantum computer science: computers, communications and cryptography. – M.: Vestnik RAN, 2000.

[10] Valiev, K.A. Quantum computers: hope and reality / K.A. Valiev, A.A. Kokin // Izhevsk: Regular and chaotic dynamics, 2001.

[11] Einstein, A. Can we assume that the quantum mechanical description of physical reality is complete? / A. Einstein, B. Podol'skii, N. Rozen //UFN. – 1934. – Vol. XVI(4).

[12] Bezobrazov, S.V. Artificial immune systems for protection of information: detection and classification of computer viruses / S.V. Bezobrazov, V.A. Golovko // Papers of science Conf. Neyroinformatika. – Moscow, 2008. – P. 23-28.

[13] Aktayeva, A. Security of information: using of quantum technologies // International Journal of Open Information Technologies. – 2016. – Vol. 4(4). – P. 40-48.

[14] Sandpiper of Page. Classical cryptography // Photonics. – 2010. – Vol. 2. – P. 36-41.

[15] Aeppli, G. Quantum Annealing and Related Optimization Methods / G. Aeppli, T. Rosenbaum. – Heidelberg: Springer Verlag. – 2007. – Vol. 679. – P. 159-169.

[16] Kurochkin, V.L. Experimental installation for quantum cryptography with the single polarized photons // Magazine of technical physics. – 2005. – Vol. 75(6).

[17] Dolgov, V.A. Cryptographic methods of information security. – Khabarovsk, 2008.

[18] Emelyanov, V.I. Quantum physics: bits and qubits. – MGU, 2012.

[19] Aeppli, G. Quantum Annealing and Related Optimization Methods / G. Aeppli, T. Rosenbaum // Heidelberg: Springer Verlag. – 2007. – Vol. 679. – P. 159-169.

[20] [Electronic resource]. – Access mode: http://www.itsec.ru.

[21] [Electronic resource]. – Access mode: http://sci-article.ru.

[22] [Electronic resource]. – Access mode: http://www.securitylab.ru/ contest/299868.php.

[23] [Electronic resource]. – Access mode: http://www.gartner.com /newsroom/id/ 2819918?fnl=search&srcId=1-3478922254.

[24] [Electronic resource]. – Access mode: www.mdpi.com/journal/cryptography-02-00005.pdf.

[25] [Electronic resource]. – Access mode: http://philosophyworkout.blogspot.com/2016/01/a-decade-of-economic-stagnation-looms.html.

[26] [Electronic resource]. – Access mode: arXiv:1707.04344v2, 2017.

[27] [Electronic resource]. – Access mode: http://www.quantenblog.net/physics/moores-law-quantum-computer.
[28] [Electronic resource]. – Access mode: https://www.nist.gov.
[29] Bessalov, A.V. Elliptic curves in the form of Edwards and cryptography: monograph. – Kiev: IVC «Vidavnitvto «Politekhnika», 2017. – 272 p.
[30] Klucharev, P.G. Quantum computer and cryptographic resistance of contemporary encryption systems // Vestnik N.E. Bauman MSTU. – 2007. – Vol. 2.