Journal of Theoretical and Applied Information Technology
31st November 2021. Vol.99. No 22

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

COGNITIVE PROPERTIES OF CYBERSECURITY: POSTQUANTUM CRYPTOGRAPHY

[1]AKTAYEVA AL., [2]MAKATOV E., [3]YESMAGAMBETOVA G., [4]KUBIGENOVA A., [5]NIYAZOVA R., [6]ZAKIROVA A.

[1] Sh.Ualikhanov Kokshetau University, Kokshetau, 020000, Kazakhstan
[2] L. Gumilyov Eurasian National University, Nur-Sultan, 010000, Kazakhstan
[3]Mongolian University of Science and Technology, 14191, Sukhbaatar, Mongolia
[4] S. Seifullin Kazakh Agrotechnical University, Nur-Sultan, 010000, KAZAKHSTAN
[5]L. Gumilyov Eurasian National University, Astana, 010000, Kazakhstan
[6]L. Gumilyov Eurasian National University, Astana, 010000, Kazakhstan

E.mail: [1]aaktaewa@list.ru, [2]erhanmk@list.ru, [3]gal.esm@mail.ru , [4]akku_kubigenova@mail.ru , [5]rozamgul@list.ru, [6]alma_zakirova@mail.ru

ABSTRACT

This paper provides background information on post-quantum security. It explores the security threats against communication security and particularly against key exchange that is enabled by the development of quantum computers. The applied and theoretical aspects of quantum-cryptographic technologies are considered. The systematic analysis of quantum algorithms, quantum cryptography, and quantum hashing are presented. The interrelated elements that make up to the concept and content determined by the application of quantum cryptography are analyzed. The development of specialized quantum computers focused on solving cryptographic problems is justified. Terms which must be taken into account in the selection of elliptic curves for cryptographic applications are determined. The proper concept vehicle over is brought, in particular, the concepts of singularity and super singularity are determined for elliptic curves and theoretical positions, lying in their basis, are examined.

Keywords: *Elliptic Curve, Singularity, Super-singularity, Quantum Cryptography, Qubit, Cognitive Technology.*

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 modeling of quantum systems.

Cognitive technologies are methods and algorithms for achieving the goals of subjects based on data on the processes of cognition, learning, communication, information processing, on the presentation of neuroscience, on the theory of self-organization, computer information technologies, mathematical modeling of elements of cyberspace, a number of other scientific areas that have recently belonged to the sphere of fundamental science.

Cognitive technologies allow at a new level to give an answer to the problems posed by the information revolution - the achievement of a new quality of management of increasingly complex and increasingly unstable cyberspace security.

The dynamic information theory has become one of the foundations of an interdisciplinary mathematical direction that allows you to analyze alternative models and methods and make a forecast in the field of cyberspace security.

When describing complex phenomena or systems, a hierarchy of simplified models is usually built. In such a hierarchy, lower-level models are a simpler special case or a rougher approximation for the processes described by higher-level models.

A remarkable property of cyber reality is that the models that arise at the lower levels of the hierarchy for many complex phenomena and processes coincide or are close. This allows for the exploration and use of cognitive technologies for cybersecurity.

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

It is possible to predict, by extrapolating the tendency of the universal properties of many non-linear systems to the growth of the intellectual component of computer technologies, an increase in attention to the algorithms and complex problems close to the limiting potential capabilities of computing 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 inbounding the efficiency of entanglement distillation protocols. An abundance of other resource theories has 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 [20 – 24].

A quantum transmits information that promises completely secure communication. However, using quantum bits or qubits to carry information requires a radically new piece of innovation technology - quantum computing. This innovative technologies needs to store quantum information and convert it into the 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.

2. BACKGROUND AND RELATED LITERATURE

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 years.

The harbingers of this are the scientific revolution in discrete mathematics, the theory of algorithms, and number theory, associated with the development of classical and quantum public-key cryptography. But cognitive technologies are focused on solving poorly formalized tasks, on identifying and effectively using their cognitive potential.

The specificity of cognitive infrastructures leads to the fact that instead of Q connections M.

The cognitive factor $\mathfrak{z} = \mathbf{M / Q = N \ln N / N 2 = \ln N / N}$ shows that the “smart structures” that are formed in the information space give the greater the gain (in comparison with the obvious strategy “all are absolute”), the more the number of nodes N they connect.

The smaller the value of $\mathfrak{z}$, the greater the effect, the more “smart” structure appears. If we translate the reasoning about the relationship of cybersecurity into the sphere of the existence of threats concerning cognitive activity, then we should clearly understand that information operations differ significantly from cognitive ones aimed at destroying the integrity of the information space.

With the rapid progress of cognitive technologies, to the transformation of this area into a powerful industry, mankind is urged by the objective need to rapidly achieve a new quality of management in an increasingly complex and unstable world.

Cognitive technologies are the tools of this struggle, which allow you to manage the processes of cognition of network users: sensation, perception, assessment, categorization, highlighting the main thing, building cause-effect relationships, connecting the perceived with the goals, motives, needs of the behavior and activities of participants in communication networks.

Therefore, the National Institute of Standards and Technology (NIST) is currently standardizing algorithms and the first standards for post-quantum cryptographic 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).

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 the scalability of modules in larger solutions that the natural quantity of interest is the number of qubits realized in an experiment.

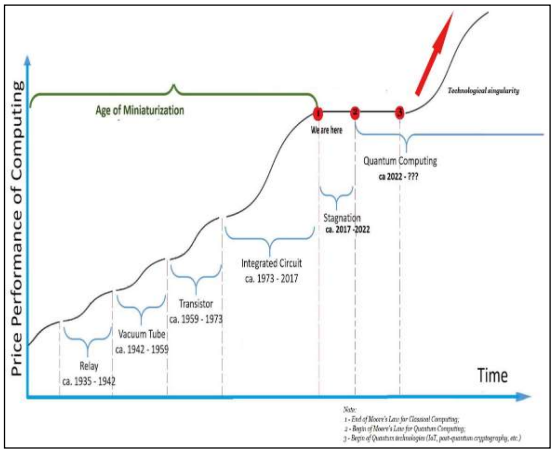

Figure 1: Moore's Law for Quantum Computers [18]

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 [19 -24].

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 [19 - 24].

3. RESEARCH FRAMEWORK AND HYPOTHESIS

One of the known prospects for post-quantum cryptography is the isogeny of supersingular elliptic curves with as many subgroups of their points as possible. The problem of the discrete logarithm of classical elliptic cryptography is replaced by the problem of finding one isogeny of a great set of subgroups of such a non-cyclic curve, which is sufficiently resistant to the attacks of a virtual quantum computer. Today, the growing interest in isogeny is associated with the smallest key length in the proposed algorithms in comparison with other known candidates for post-quantum cryptography at a given level of security.

The new algorithms rely on several cryptographic schemes that are believed to be post-quantum-resistant and include the following:

1. Code-based cryptography;
2. Multivariate Cryptography;
3. Lattice-based Cryptography;
4. Hash-based Cryptography;
5. Isogeny-based Cryptography.

Each of these cryptographic schemes has advantages and disadvantages, and the algorithms vary in both their performance measures and maturity. Supersingular isogeny-based cryptography is one of the more recent advances based on the arithmetic of elliptic curves.

In 2011 has proposed Supersingular Isogeny Diffie-Hellman (SIDH) is a key exchange protocol that would offer postquantum security. Isogeny-based algorithms rely on the structure of large isogeny graphs, and the cryptographically interesting properties of these graphs are tied to their expansion properties.

A quantum transmits information that promises completely secure communication. However, using quantum bits or qubits to carry information requires a radically new piece of innovation technology - quantum computing. These innovative technologies need 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.

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 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 correction 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 $|\varphi_1|, \ldots |\varphi_a|$, it the probabilities $p_1, \ldots p_a$ (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 $|\psi\rangle = a|H\rangle + b|V\rangle$, where a and b are 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 [1-5].

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 on the basis, the qubit can be represented in a variety of physical systems [1-5].

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.

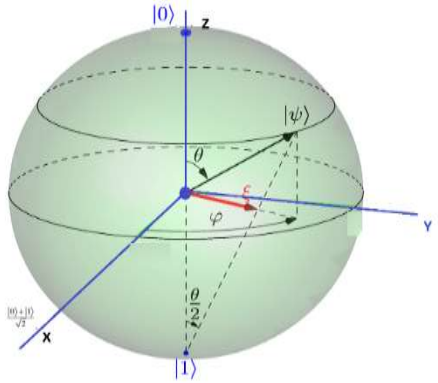

Figure 2: Qubit on the Bloch Sphere

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 computation in one go, and spits out the result almost instantaneously, in a single process.

4. MATERIALS AND. RESEARCH METHODOLOGY

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 of 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 wavelength 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 [1,2].

In all cases, the quantum algorithm solves the problem more effectively than the classical one [3].

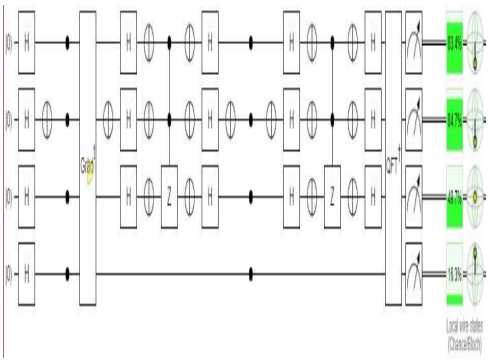

Figure 3: Quantum Circuit Implementing Grover's Search Algorithm

At the moment, the quantum threat is theoretical as quantum computers that fulfill the requirements of Shor's algorithm are not available. 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,

Journal of Theoretical and Applied Information Technology
31st November 2021. Vol.99. No 22

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

a quantum computer of around 1000 qubits is needed [21, 22, 23].

According to the most optimistic views, a million-qubit system, corresponding to 1000 errors corrected qubits might be conceivable within 10 years. 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 of 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** 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-key cryptosystems, including Rivest – Shamir – Adleman (RSA), Digital Signature Algorithm (DSA), Diffie – Hellman (DH) key exchange, as well as Elliptic Curve Cryptography (ECC) (See Figure 3).

• **Grover's algorithm** will weaken symmetric cryptography (See Figure 3-5). 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) [1 - 3].

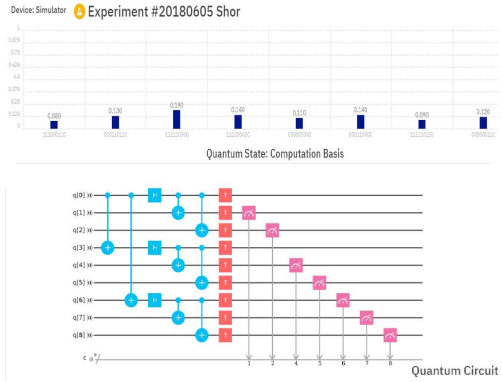

Figure 4: Encoding Circuit for the Shor Nine Qubit Code

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 the same scaling continues even further, 2048-bit RSA keys would come under attack somewhere between 2052 and 2059.

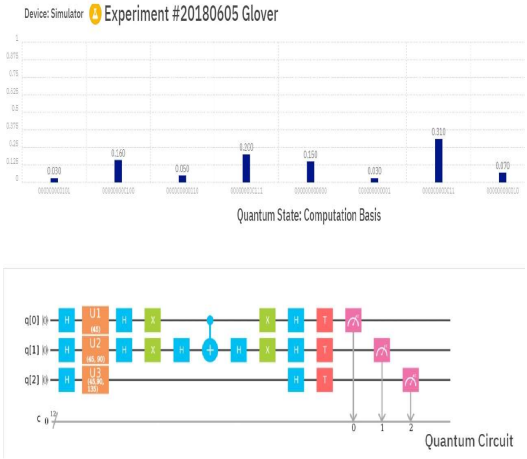

Figure 5: Circuit for the Grover's Algorithm

Figure 5 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. Figures 3 - 5 illustrate two different threat models in post-quantum scenarios.

The figure 6 combines elements that are relevant both for the physical layer security as well as for cryptographic security.

In both figures, we have Alice and Bob communicate via a wireless channel. In figure 6, 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, resolves 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.

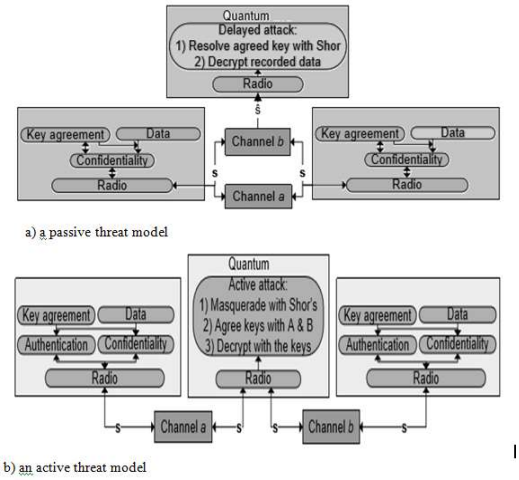

Figure 6: A Physical Layer Eavesdropper with Quantum Capabilities in the Future [21]

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 fulfilled, 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.

During 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 ciphertext 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 for quantum computers, it is safe to use classical authentication mechanisms as long as other parts of the security system are quantum immune [22].

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 the 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;
- 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. (See Figure 7) [1-5, 7, 24].

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.

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 from quantum states of photons (See Fig.3).

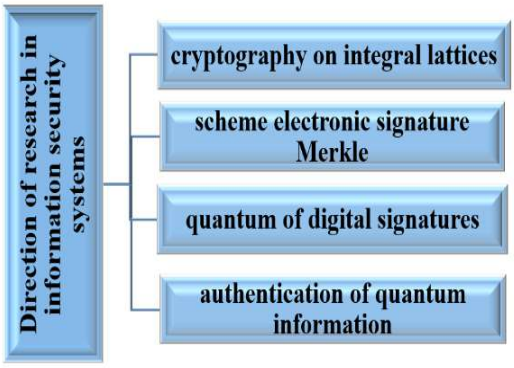

Figure 7: Main Directions of Studies in the Cybersecurity System [7]

In contrast with traditional cryptography, which uses mathematical methods to ensure the secrecy of information, quantum cryptography works with the physics of information transmission [1 - 5, 7, 24].

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.

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 was based on the computational intractability of the so-called "hard problems" of the discrete log and integer factorization is under threat of both eavesdrop and attacks by future adversaries in possession of quantum computers.

5. RESULTS AND DISCUSSION

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 [21-25].

Public key information security systems are based on the difficulty of solving the discrete logarithm problem. The problem of discrete logarithm on an elliptic curve (ECDLP - Elliptic Curve Discrete Logarithm Problem) is formulated as follows.

Given an elliptic curve E, defined over a prime field F_p, a point $P \in E(F_p)$ of order **n** and a point $Q \in \langle P \rangle$, find $l \in [1, n-1]$ such that $Q = lP$. The integer l is the discrete logarithm Q to the base and is denoted $= \log_P Q$

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 specifies 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

$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in K$.

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

Where $a_1; a_2; a_3; a_4; a_6 \in K$ and $\Delta \neq 0$, where Δ is the discriminant of E that can be computed as follows [26]:

$\Delta = -d_2^2 d_8 - 8 d_4^3 - 27 d_6^2 + 9 d_2 d_4 d_6$;

$d_2 = a_1^2 + 4a_2$;

$d_4 = 2a_4 + a_1a_3$;

$d_6 = a_3^2 + 4a_6$;

$d_8 = a_1^2a_6 + 4\, a_2a_6 - a_1a_3\, a_4 + a_2a_3^2 - a_4^2$.

It can be justifying by 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

$ax^2+y^2 = 1+dx^2y^2$, *for a* $2f \pm 1g$, leaving one variable d *is* free. The group order for an Edwards curve is divisible by 4.

The addition formula for twisted Edwards curves is the same as in the case of Edwards curves in the generalized form, where $c = 1$ in the case of twisted Edwards curves.

Theoretically, it would be possible to work with a more general model given by the equation

$ax^2+y^2 = c^2 (1+dx^2y^2)$.

However, as the curves defined according to that model are always isomorphic to twisted Edwards curves, in practice it is not used [4].

The most interesting characteristic of complete twisted Edwards curves is that the equations for both adding two points P_1 and P_2 such that $P_1 \neq \pm P_2$ and doubling a point are exactly the same. Moreover, it is not necessary to implement any logic for detecting if the points to be added are such that $P_2 = -P_1$, as the Edwards addition equations also take into account that circumstance.

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

$y^2 = f(x)$, *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 ***if (x) = (x-α) (x^2+ βx+γ), where α, β, γ*** - are real numbers.

If a polynomial has one real root, a, since ***y = 0***, when ***x = α.***

If ***f (x)*** has all three real roots. In this case, the real points from 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.

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.

The discriminant D (f) of the algebraic equation $f(x)= a\,x^n + a_{n-1}\,x^{n-1} + \ldots + a_1 x + a_0,\ a_n \neq 0$ 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 (*The 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

$$W\ (x_1,\ x_2,\ .\ .\ .\ ,\ x_n\ ) = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ . & . & \cdots & . \\ 1 & x_n & \cdots & x_n^{n-1} \end{vmatrix} =$$

$$\prod_{i>k}(x_i - x_k)$$

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) ≠ 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 [25].

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 and **(C)** is noncommutative. For the 'supersingularity' of the curve **E**, which is given by the equation

$E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,\ a_i \in K.$

$y^2 = x^3 + a\,x + b$ - one can use the fulfillment of the any following conditions:

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

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.

Cybersecurity means being protected from the effects of malicious cyberspace information. Ensuring cybersecurity at its various levels and in various aspects takes on the features of confrontation and becomes an ongoing process.

The focus only on the protection of cyberspace resources becomes insufficient to maintain security, the technology for ensuring it already requires one or

another attacking or pre-emptive action on a potential adversary.

This is due to the total informatization of the socio and technosphere, all life support and management systems, the very way of life of the vast majority of the population, the transfer of conflicts to cyberspace.

Our observations demonstrate that further improvement incoherence and controllability could be obtained by encoding qubits into hyperfine sub-levels 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 with 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.

The existing public-key cryptography is based on the complexity of solving the factorization problem and calculating discrete logarithms, for example, elliptic curves. In post-quantum cryptography, algorithms are built on different mathematical mechanisms than modern algorithms.

Ideally, the postquantum-safe cryptography or hybrid key-exchange algorithm should drop directly into well-known protocols. In reality, post-quantum-safe algorithms are complex compared to legacy algorithms both concerning difficulties of implementation, and in parameter characteristics.

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.

In addition to that, it is also important to note that, using standard coordinates, short Weierstrass curves outperform Edwards and Montgomery curves when computing scalar-multiplication operations. As is usually the case, having a higher level of security by default comes at a cost.

Careful study of the protocols and optimization of the algorithms will reduce the performance impact of using a hybrid-key exchange scheme.

Simulation of continuous processes in time to identify some qualitative trends or patterns, test scenarios with variations in initial conditions, coefficients, space of phase variables representing dissimilar factors.

6. CONCLUSION AND FUTURE SCORE

Cybersecurity, today is preemptive, proactive security, the creation strategy of which should be based on nature-like and Nano and quantum technologies.

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 had worked to ensure a quantum-safe future.

In this study analyses articles primarily published on post-quantum security in open sources to select the purpose of research.

Obviously, as the study shows, the moment of transition to postquantum cryptography will require a radical restructuring of the entire critical infrastructure of information security and all means of cryptographic information protection using modern asymmetric cryptographic algorithms. The following main results were obtained in the study:

The analysis of publications on the problems of the theoretical and applied aspects of quantum-cryptographic technologies;

The explore of the security threats against communication security and particularly against key exchange that is enabled by the development of quantum computers;

The development of specialized quantum computers focused on solving post quantum cryptographic problems is justified.

Furthermore, terms which must be taken into account in the selection of elliptic curves for cryptographic applications are determined, in particular, the concepts of singularity and super singularity are determined for elliptic curves and theoretical positions, lying in their basis, are examined.

The proposed methodology of quantum-cryptographic technologies provides an assessment of the damage prevention from a cyber-attack, and an analysis of the characteristics of simulation tools is conducted.

In this research, that the urgency of switching to quantum or postquantum cryptography for a particular cyber system depends on three simple parameters:

1. **Storage time**: the number of years during which the data must be protected by the crypto system.
2. **Transition time:** the number of years for the system to transition to a quantum solution.
3. **Threat duration:** The number of years before the relevant threat actors can break into quantum vulnerable systems.

Thus, in solving problems of post-quantum cryptography, there is a need to use a formal apparatus that allows, if not to formulate a particular conclusion or to justify a recommendation, then, at least, having agreed on the basic statements of the model, objectively check the results of experiments on it for various scenarios and initial conditions.

Finally, we note that postquantum cryptography is a set of encryption tools that are resistant to attacks carried out using the quantum computer.

The obtained research results make it possible to expand the tools of cybersecurity analysts in the synthesis and analysis of security future contours of the methodology of quantum cryptographic technologies of critical infrastructure resources of informatization of any scale.

Therefore, the aspects of the post quantum cryptography technologies are important to pay attention to and manage to ensure the success of cybersecurity in developing countries.

Thus, there is an urgent need to develop cognitive models of postquantum cryptographic mechanisms, which must be solved not only within the framework of scientific and practical work, but also by the efforts of the entire cryptographic community.

Future research in this field could overcome some of the limitations discussed in this study:

First, this is an empirical study; a practical study may improve the results in the future.

Second, this framework should be tested with cybersecurity technicians to confirm this research's findings in the future.

Third, the data analysis for this study is based on data collected from R&D reports.

Consequently, our study is restricted to data from opensource information's who were available and willing to provide data.

Therefore, future studies are encouraged to expand the current research landscape's effects by including data obtained from cybersecurity technicians.

REFERENCES

[1] American National Standards Institute. Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. - ANSI X9.63. 2001.

[2] American National Standards Institute. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). - ANSI X9.62. 2005.

[3] D.J. Bernstein, P. Birkner and et. "Twisted Edwards curves", Cryptology ePrint Archive, Report 2008/013 - http://eprint.iacr.org/2008/013.

[4] H.M.Edwards "A normal form for elliptic curves". *Bulletin of the American Mathematical Society*, Vol.44, 2007, pp. 393–422,

[5] A. Aktayeva and et. "Innovative technologies in the information security system: quantum technologies", *Proceedings of Conference "Modern Information Technologies and IT-Education*", Vol. 1, No. 1 (9), 2014, pp. 320-326.

[6] A. Aktayeva and et. "Quantum Informatics: Methods of date protection, *International Scientific Journal "Modern Information Technologies and IT-Education*, Vol.12, No. 2, 2016, pp. 6 -14, - http://sitito.cs.msu.ru/ index.php / SITITO/ issue/ view/4

[7] A. Aktayeva and et. "Quantum technologies: simulation of information communication", *International Journal of Engineering Sciences & Research Technology*, Vol. 5, Issue 6 - June 2016, pp. 608-618 - http://www.ijesrt.com/June- 2016.html

[8] T. ElGamal 'A public-key cryptosystem and a signature scheme based on discrete logarithm', *IEEE Transactions on Information Theory*, Vol.31, 1985, pp. 469-472.

[9] Alwen "What is lattice-based cryptography and why should you care". - https://medium.com/ cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717

[10] L. Beshaj, A. Elezi and T. Shaska "Isogenous components of Jacobian surfaces", *European Journal of Mathematics*, 2019.

[11] D. Charles, K. Lauter. "Computing Modular Polynomials", *LMS Journal of Computation and Mathematics*, Vol. 8, 2005, pp. 195-204.- doi:10.1112/S1461157000000954/

[12] S. Chen, Y. Jordan, D. Liu, R.Moody, and et. "Report on post-quantum cryptography", *National Institute of Standards and Technology Internal Report*, NIST.IR.8105. 2016.

[13] S. Contini, A. K. Lenstra and Ron Steinfeld, "VSH, an efficient and provable collision-resistant hash function," *Advances in cryptology – EUROCRYPT 2006, Lecture Notes in Comput. Sci.*, vol. 4004, , 2006, pp. 165–182, Springer, Berlin, MR 2423542.

[14] C. Costello and H Hisil "A simple and compact algorithm for SIDH with arbitrary degree isogenies', *Proceedings of Conference International Conference on the Theory and Application of Cryptology and Information*

Security ASIACRYPT, Advances in Cryptology (ASIACRYPT), 2017, pp. 303–329.

[15] D. Stehlé, R. Steinfeld and et. "A simple and compact algorithm for SIDH with arbitrary degree isogenies" *In: Matsui M. (eds) Advances in Cryptology – ASIACRYPT 2009, Lecture Notes in Computer Science*, Vol 5912, 2009, pp. 617-635, Springer, Berlin, Heidelberg.

[16] L. C. Washington "Elliptic Curves: Number Theory and Cryptography", *London: Chapman and Hall/CRC*, 2008.

[17] M. Zhandry "A note on the quantum collision and set equality problems", *Proceedings of Quantum Inf. Comput.,* Vol. 15, No. 7-8, 2015, pp.557–567.

[18] http://philosophyworkout.blogspot.com/2016/01/a-decade-of-economic-stagnation-looms.html

[19] https://arxiv.org/abs/1707.04344

[20] http://www.quantenblog.net/physics/moores-law-quantum-computer

[21] https://www.mdpi.com/2410-387X/2/1/5/htm

[22] https://ieeexplore.ieee.org/document/6107841

[23] https://ieeexplore.ieee.org/xpl/conhome/6095473/proceeding

[24] https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange/

[25] https://www.geeksforgeeks.org/implementation-diffie-hellman-algorithm/