Vol. 6, No. 12 December 2015 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Quantum Technologies: Information Communication

[1] A. Aktaeva, [2] O. Baimuratov, [3] N. Galiyeva

[1,2] Assoc. Prof., Dr. PhD Department of Computer Science and Information Systems, Kazakh Academy of Transport and Communication after named M. Tynyshbayev, Shevchenko, Almaty, Kazakhstan

[3] Researcher, MSc. Department of Computer Science and Information Systems, Kazakh Academy of Transport and Communication after named M. Tynyshbayev, Shevchenko, Almaty, Kazakhstan

[1] aakhtaewa@gmail.com, [2] alimzhan1@mail.ru, [3] nggaliyeva@gmail.com

ABSTRACT

The article discusses the importance of information resources requiring reliable methods of unauthorized access protection in the modern information-oriented society. The article describes the structure and basic principles of the quantum cryptography technology based on properties of quantum systems. Quantum information is a physical quantity characterizing changes occurring in the system during interaction between the information flow and the external environment. It offers a method for improving data security and confidential information protection using quantum teleportation within infrared laser communication channels. The theoretical development was implemented experimentally by the authors using the unit for laser communications.

Keywords: *Quantum Information Science, quantum communication channels, quantum crypto graphy, quantum computer, photon, qubit, laser*

1. INTRODUCTION

There are a large and constantly increasing number of information resources requiring reliable methods of unauthorized access protection in the modern information-oriented society. In recent years, the problem of the quantum technology application in supporting the information security system and protection of confidential information transmitted over open communication channels became highly relevant and popular. The reasons for this were scientific discoveries and technological advances having made it fundamentally possible to solve the whole classes of most complicated computational technologies of strategic value for critically important technologies such as innovative technologies: quantum, laser and optical [20].

At the present time, Quantum Information Science is a new rapidly developing branch of science relating to the use of quantum technologies for the implementation of innovative methods of information and telecommunications, as well as computations: quantum information, quantum information science, quantum communication channels, quantum cryptography, quantum computer [15-21].

Quantum information is a new type of information that can be transmitted, but not reproduced. A quantum bit, or a qubit, is described as a unit vector in a two-dimensional complex vector space and represents a two-level quantum system. Ions, atoms, electrons, photons, spins of atomic nuclei, structures of superconductors and many other physical systems can serve as qubits [7, 28, 29].

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

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 $|\psi_1\rangle, \ldots, |\psi_a\rangle$ with 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:

$$w = (x_1, \ldots, x_n),\ x_j \in \{1, \ldots, a\}.$$

Experimentally, these operations are performed using a bire fringent 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 (Fig.1).

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:

a. Algorithms based on the quantum Fourier transform;
b. Quantum search algorithms;
c. Algorithms of quantum system simulation [1,2].

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

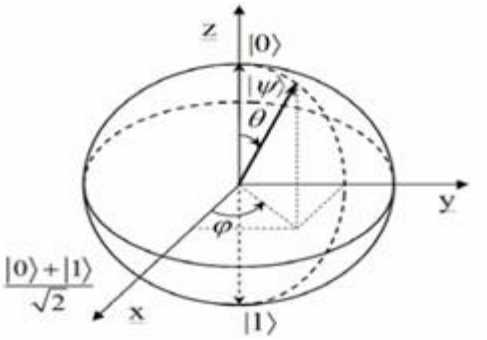


Figure 1: Qubit on the Bloch sphere.

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 and protocols resistant to capabilities of quantum computers (Fig. 2). 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.) [1 -5, 7, 28, 29].

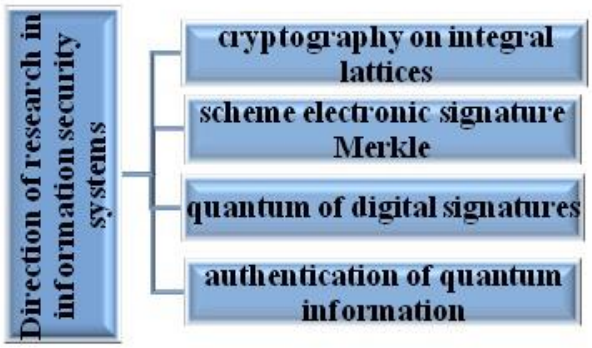


Figure 2: Main directions of studies in the information security system [7]

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 (Fig.3) [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 [27].

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.

Information is sent and received by physical means using photons within fiber-optic communication lines, the natural environment or vacuum. Coherent optical states can involve a large number of photons. On the one

hand, the transmission range for secret messages is increased, and on the other hand, additional problems concerning information security occur.

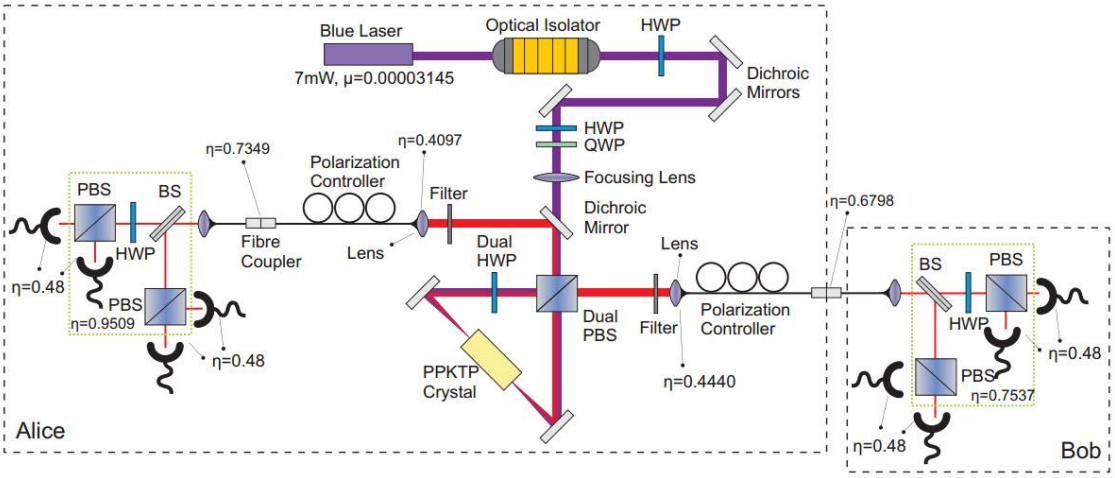


Figure 3: Quantum cryptography implementation scheme [27]

The peculiarity of quantum information lying in the fact that the quantum system cannot be measured without changing the state thereof is the basis for creating quantum communication channels transmitting classical information without any risk of uncontrolled interception.

Quantum "entanglement" is a fundamental property of quantum mechanics. It allows distributing quantum information over tens of thousands of kilometers and is limited only to the speed and distance the components of the "entangled" pair will be able to travel in space.

It is clear that quantum methods of data transmission are generally disadvantageous in view of the limited measurability; however, it is possible to design and create a communication system that can always detect eaves dropping by using quantum phenomena. This is achieved by the fact that the attempt to measure related parameters in the quantum system disturbs it by destroying original signals, and therefore, users can recognize the degree of activity of the interceptor by the level of noise in the channel.

When creating crypto systems based on quantum key distribution, the following problems may occur:

- Low transmission speed– transmission speed over long distances is ~ Kbit, transmission speed over short distances is ~ 10 - 100 Kbit;
- Short distances –up to 100 km – at a speed of~ Kbit;
- Intensity of quantum pulses – photons are typically emitted in a beam, which allows an attacker to separate the part of photons and analyze their state;
- Emission of single photons of a predetermined polarization is possible only with a certain probability [11, 18].

Currently, the most appropriate medium for implementation of quantum channels in the quantum cryptography scheme is optical fiber, which property allows transmitting data up to a distance of 120 km. The use of fiber limits the ability to work with polarization encoding, since optical fiber has noticeable fluctuations in birefringence. For this reason, quantum cryptography uses the phase modulation with interferometric detection. The fundamental principles of data protection in quantum communication lines include the inability to copy a quantum state unknown before hand of a single quantum object, and inability to obtain any information about quantum states of this object without disturbance. Thus, the fundamental laws of quantum mechanics guarantee the security of information transmitted [11, 18, 26].

Quantum teleportation is a process of transmission of an unknown quantum state at a distance by means of the EPR pair separated in space and divided between two correspondents and classical communication channels.

Quantum teleportation, compared to the dense coding, takes place in the absence of a quantum communication channel, i.e., without transferring qubits (Fig. 4).

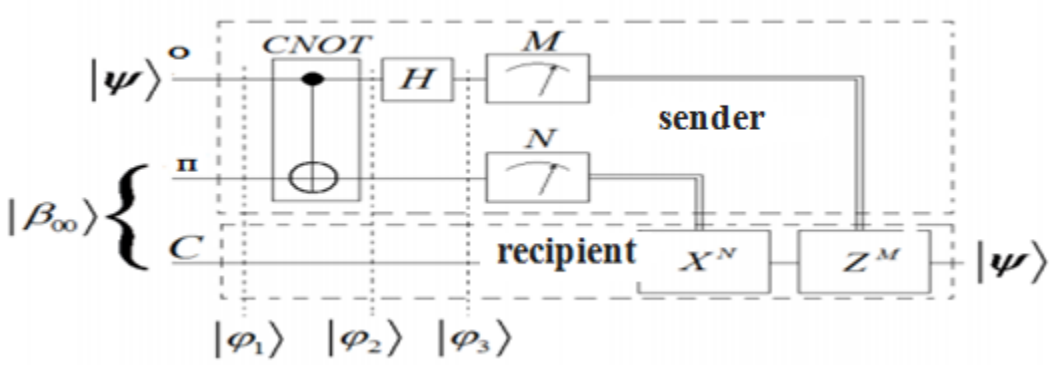


Figure 4: Quantum teleportation scheme: single lines are quantum communication channels; double lines are classical communication channels [17]

Teleportation is the perfect way to transmit secret information, as well as:

a. Teleportation procedure does not violate the theorem of nonclonability;
b. Quantum information can be transmitted from photon to photon at arbitrary distances (more than 144 km in the open space, and 102 km via optical fiber);
c. Teleportation does not transmit information about the fact of transmission;
d. Classical channels (about the fact of information transmission);
e. If Bell states are not measured and the only projection on the fermionic state is taken into account, the teleportation will be successfully performed on average once of four attempts [11, 18, 26].

Quantum teleportation does not make it possible to transmit information faster than the speed of light, as it might seem at first glance, since the integral part of the protocol of teleportation includes information transmission over classical communication channels, and the classical channel is limited to the speed of light (Fig. 5).

Quantum teleportation used as a basic component in the quantum scheme offers attractive opportunities for solving this and a number of other experimental problems occurring as a result of implementation of quantum computers; it makes possible to perform a variety of quantum logic operations that are impossible when using direct unitary operations. In this case the formation of jam-resistant quantum logic gates is limited to the preparation of the relevant subsidiary entangled state in the single qubit teleportation scheme [11].

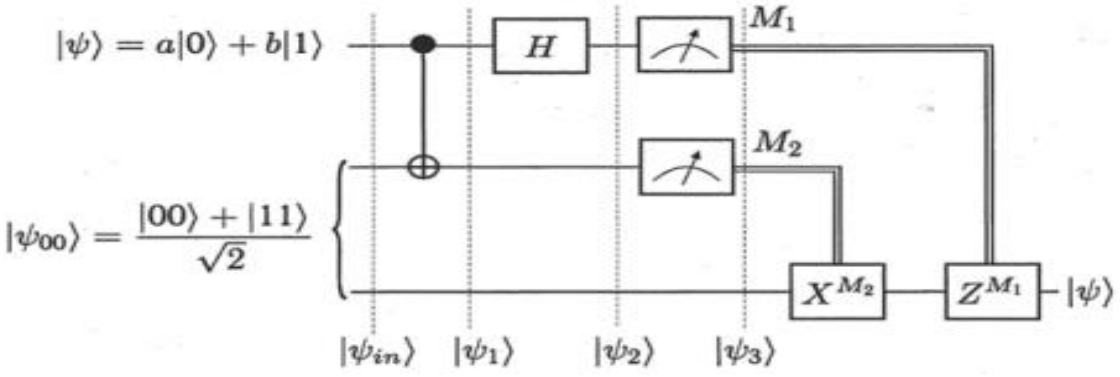


Figure 5: Quantum teleportation scheme for an unknown state | Ψ>qubit [20]

New opportunities of infrared lasers to implement quantum teleportation of states open the advantage of solving the problem concerning the transmission of superposition states, which can be easily destroyed, at large distances without losing their coherence.

3. RELATED WORK

The laser generates a light beam mildly diverging in the air (about 1 mm in diameter). This allows the transfer by the open beam at a relatively long distance (10 km). Note that the emission flux of the sun in the infraredrangeis not less than in the visible range. Optical channels are expected to use two parallel beams, one for each direction

of transmission. The diameter of the sensitive surface of the detector is typically less than 1 mm [25].

And for the purpose of excluding the effect of convective air flows, beam defocusing is generally used, so that even in case of the beam axis deviation, the flare spot does not leave the sensitive range of the detector. This method assumes that there is excess luminosity of the transmitting laser. The open infrared beam provides a sufficiently high level of security, and this is a consequence of the nature of the signal transmission, and it is not provided with any special methods. The most important property of the wireless optical communication is a high level of unauthorized access protection of the channel. The channel is technically very difficult to intercept –pursuant to the acute beam directionality and the use of a unique model for each method of information encoding by pulses of emission. However, a lot of measures based on different principles –wave front reversal, analysis of changes in the signal received, and others – have been developed to detect attempts of unauthorized access, and this fact further increases the security of communication channels [24].

When designing such communication channels, the signal loss $\boldsymbol{\alpha^0}$[dB] related to the geometry of the beam should be taken into account:

$$\boldsymbol{\alpha^0 = 20\log(\alpha^0 R * d^0)}, \quad \{\text{dB}\}$$

Where$\boldsymbol{\alpha^0}$is the divergence angle in radians;

Ris the transmission range in meters;
d^0 is the input window diameter in meters.

The loss due to the absorption and scattering should be taken into account as well:

$$\boldsymbol{\alpha^1 = \frac{17}{S} * (\frac{0.55^{0.195*S}}{\lambda})}, \quad \{\text{dB/km}\}$$

Where$\boldsymbol{\alpha^1}$is the strength loss in decibels per kilometer?

$\boldsymbol{\lambda}$ is the wavelength in microns;
S is the visibility range [km] [25].

Signals of input system interface are used for signal modulation within an open optical channel.

Transmission technology itself is based on data transmission by modulated emission of the infrared spectrum through atmosphere. Semiconducting emitting diode acts as a transmitter. Highly sensitive photodiode is used as a receiver. Emission affects a photodiode as the result an original modulated signal is regenerated. Then the signal is demodulated and converted into signals of output interface. The lens system is used from the both sides, at transmitting side – in order to receive a collimated beam and at receiving one – in order to focus the emission received on the photodiode. The same reverse channel is arranged for duplex transmission. The main unpredictable element of the system is transmission medium – unpredictability of the atmosphere with its weather conditions [24]. Information transmission range and reliability with the use of infrared laser communication depends on weather conditions (Fig. 6).

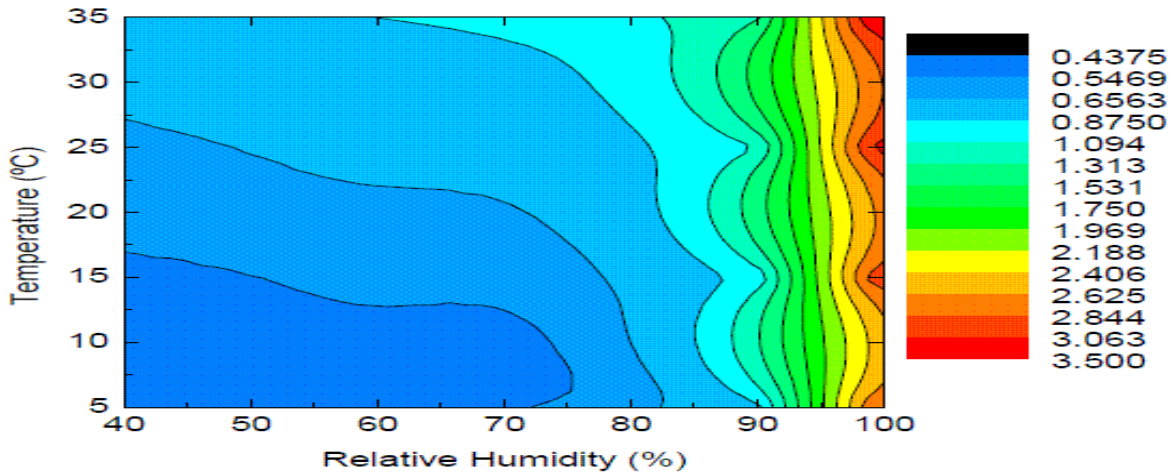


Figure 6: Dependence of signal absorption on temperature and humidity at the base located in 1 km [24]

4. RESULTS

The information is generally transmitted by powerful laser pulses. Random sequence of bits is coded in their quantum state (polarization, phase, time). One bit is coded into one photon and transmitted to a receiver. The main problem is that single photons get lost very intensively. Having passed several dozens of kilometers, 99% of single photons scatter. Thus, it is necessary to use

quantum repeaters, operating principle of which is based on quantum teleportation technology.

During the research advantages of quantum teleportation technology use by laser communication and possibilities of path trace design were studied and the comparison of high rise buildings in Almaty were done (Fig.7).

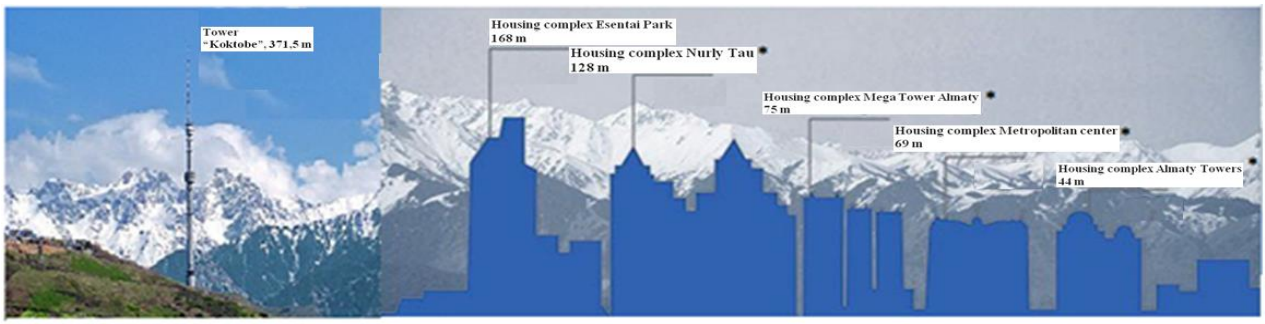


Figure 7: Comparison of high-rise buildings in Almaty

Logic of laser communication channel routing was analyzed simultaneously with path tracing with due regard to location of the Customer's facilities and an option of infrared laser communication channels design were offered (Fig. 8).

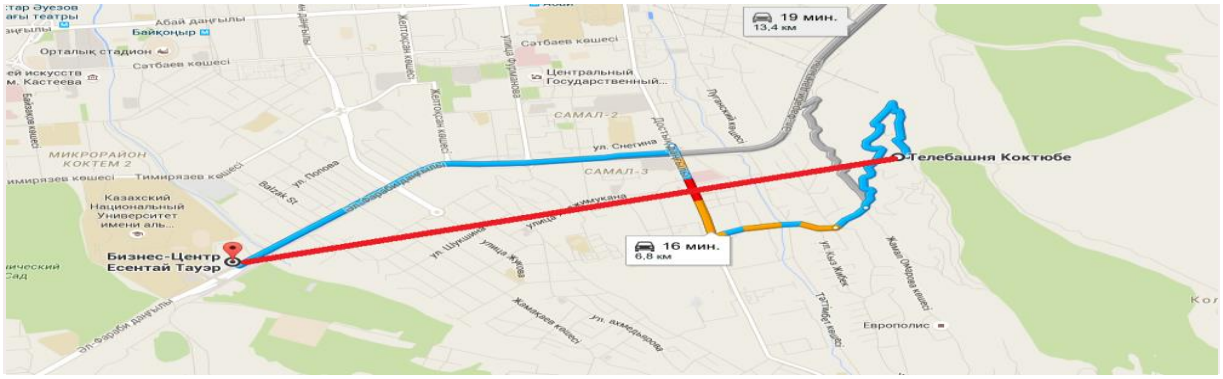


Figure 8: Offered laser communication channel

When designing communication line the server is traditionally installed, optical fiber is pulled to each consumer of information services and instead we offer to use two laser receiver-transmitters (LRTs) directed at one another, through which data are transmitted over open space by means of laser light (Fig. 9).

Teleportation issue involves a range of questions of principles, in particular, exchange of quantum information within complicated spaced diverse molecular structures, biological ones included. Neither wireless transmission technology is able to offer such communications security as laser does. Signal can be intercepted but only if scanning receivers are installed within a narrow beam of the transmitters.

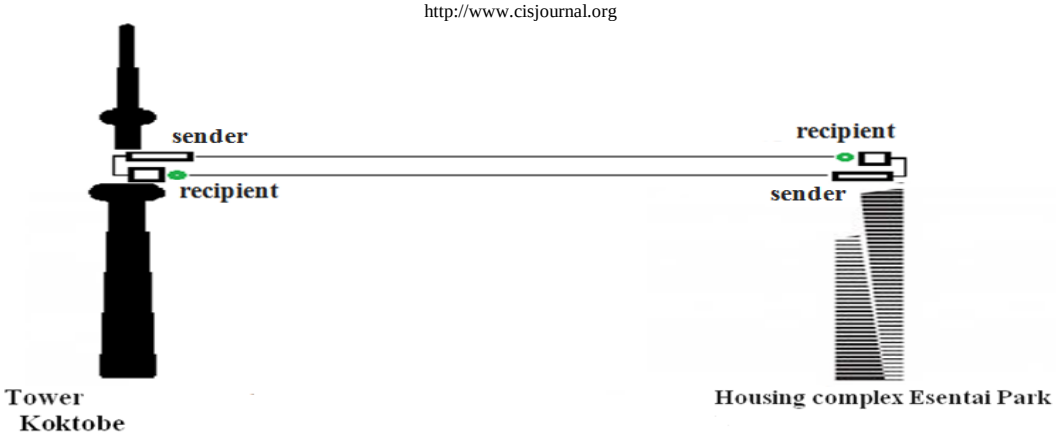


Figure 9: Information flow transmission scheme

Actual difficulty of this requirement fulfillment makes such intercept almost impossible. Laser beams cannot be detected by different scanners. Diverse own data transmission protocols are also used ensuring additional communications security. Laser systems are already used for various applications where high level of data transmission security is necessary, including financial, healthcare and military establishments. They are analyzed through routing logic, as well.

5. DISCUSSIONS

Entanglement is the potential for quantum states to exhibit correlations that cannot be accounted for classically. From a computational standpoint, entanglement seems intuitive enough -- it is simply the fact that correlations can exist between different qubits -- for example if one qubit is in the $|1\rangle$ state, another will be in the $|1\rangle$ state.

However, from a physical standpoint, entanglement is little understood. The questions of what exactly it is and how it works are still not resolved. What make it so powerful (and so little understood) are the facts that since quantum states exist as superpositions, these correlations exist in superposition as well. When the superposition is destroyed, the proper correlation is somehow communicated between the qubits, and it is this "communication" that is the crux of entanglement. Mathematically, entanglement may be described using the density matrix formalism [30].

The performance of new Elman - neural network (Elman - NN) filter was examined through simulations. The system given in figure 10 was modeled the Elman's two – layer neural network structure under Matlab/nntool environment.

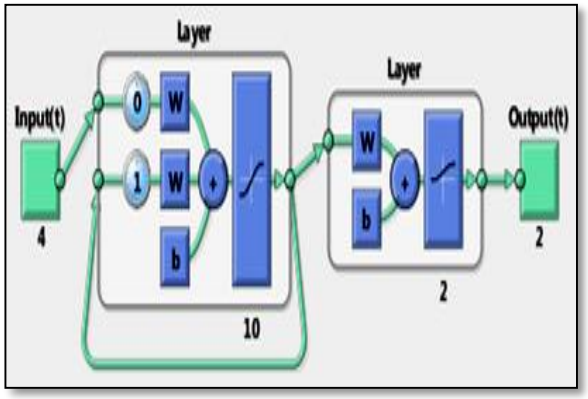
Table 1: Corresponding concepts from the domains of classical neural networks and quantum [30]

Classical neural networks	Quantum
$x_i \in \{0,1\}$ - Neuronal State	$\|x\rangle = a\|0\rangle + b\|1\rangle$ - Qubit
$\{w_{ij}\}_{ij=1}^{p-1}$ - Connections	$\|x_0 x_1 \ldots x_{p-1}\rangle$ - Entanglement
$\sum_{s=1}^{p} x_i^s x_j^s$ - Connections	$\sum_{s=1}^{p} x_i^s x_j^s$ - Superposition of entangled states

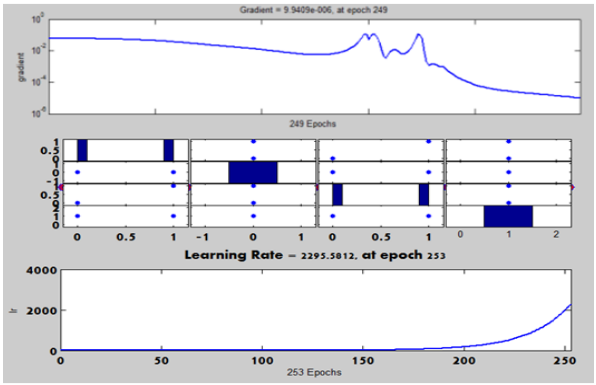
Elman NN has architecture as that of SLP with an additional feedback loop of hidden layer with a single delay. The output of hidden layer is called internal state. The feedback layer is referred as context layer and is represented below the input layer with a connection to the input of the hidden layer (Fig. 10). The weights of recurrent connections from hidden layer to the context layer are fixed.

These fixed back connections result in the context units always maintaining a copy of the previous values of the hidden units or in other words have a memory unlike EE_NNs. It is a partially recurrent architecture retaining layered configuration. It is also referred as locally recurrent, but globally feed forward NN. Yet, the capacity to retain the history of past information is limited. It is trained with BP algorithm. Hyperbolic, tangent, sigmoid and log sigmoid are used as transfer functions in the hidden and output layers in later versions of Elman model. But, generally

purelin TF is preferred in the output layer. 3D- contours are more informative than 3D-surfaces except visual appreciation. Figurative representation of NNs also does not give more information than mathematical object orientation notation. Keeping this view, we reported Math lab m-files for Elman, Jordan, RBF, MLP and SLP [31].



a) The Elman's two-layer neuron network structure



b) The schedule of training of a neuron network structure of Elman

Figure 10: The Elman's two-layer neuron network structure on Matlab

Fig. 10 (a – circuit of Elman back propagation network) and Fig. 10 (b - circuit the training of Elman) are showing the result of the proposed action filter controlled by the Elman back propagation network controller with MATLAB. Elman NN has architecture as that of SLP with an additional feedback loop of hidden layer with a single delay. Elman NN is the finest controller in all the controllers, but it has some drawbacks like redundancy and iteration problems. So one has to choose the membership functionality on the basis of system complexity. It shows the performance of active filter under unbalanced sinusoidal voltage condition.

6. CONCLUSIONS

Due to intensive development of innovation technologies the research conducted in the field of electronics, creation of intellectual software and hardware solutions of the applied information science and quantum technologies is of key importance. Quantum information and technologies based on unusual properties will in future influence the basics and further development of information space and the quantum information theory itself will drastically change modern points of view of the scientific community concerning information security systems.

Conducted trials and studies on provision of information security are of great academic interest in relation to search for solution of major tasks and issues faced by the quantum cryptographic systems: a task of detecting single photons with high probability in the set quantum state with low level of false responses, absence of controlled sources of single photons, an issue of transmission range increase and low speed of quantum key generation. Use of quantum technologies in the field of information security system provision is one of the most paradoxical manifestations of quantum technology that has recently excited much interest among the specialists, primarily, when transmitting coded messages over two communication channels – quantum and traditional ones.

7. FUTURE WORK

Quantum information teleportation is one of the most rapidly developing applied directions of the quantum physics and it provides for informing on an attempt to intercept information transmitted due to irreversibility of wave function collapse. Research in the field of quantum information teleportation can lead not only to positive results but also to negative ones. Quantum cryptography based on the use of quantum teleportation will in future substitute all the cryptographic systems used at present and will be used on an equal basis with common information telecommunication means. Relevance and scale of the issues connected with provision of information security will grow day by day and development of quantum information will in the immediate future bring its results and, possibly, lead to a significant change of a scientific world view in the field of IT.

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, V. 22, r. 563–591

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

[3] Cleve R., Ekert A., Macchiavello C., Mosca M. Quantum algorithms revisited // Phil. Trans. Royal Soc. - London,1998, V. A454,p. 339–354

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

[5] Halyapin D.B. Zashita informacii. Vas podslushivayut? Zashishaites'. -M.: BAYaRD, 2004

[6] Baumester D., Ekert A., Cailinger A. Fizika kvantovoi informacii. -M.: Post market, 2002

[7] Aktaeva A.U., Ilipbaeva L.I. Innovacionnye tehnologii v sisteme informacionnoi bezopasnosti: kvantovye tehnologii // Sovremennye innovacionnye tehnologii i IT- obrazovanie.-2014, tom 1, ¹ 1(9), 320-326 p.

[8] Belokurov V.V., Timofeevskaya O.D., Hrustalev O.A. Kvantovaya teleportaciya–obyknovennoe chudo. - Izhevsk: RHD, 2000

[9] Broil' L. Revolyuciya v fizike. -M: Atomizdat, 1965

[10] Valiev K.A. Kvantovaya informatika: komp'yutery, svyaz' i kriptografiya.-M.: Vestnik RAN, 2000

[11] Valiev K.A., Kokin A.A. Kvantovye komp'yutery: nadezhda i real'nost'. -Izhevsk: Regulyarnaya i haoticheskaya dinamika, 2001

[12] Geizenberg V. Fizika i filosofiya.- M.:Nauka,1989, perevod–Akchurin I.A., Andreev E.P.

[13] Kadomcev B.B. Dinamika i informaciya.- M.:Uspehi fizicheskih nauk, 1999

[14] Klyshko D.N. Fizicheskie osnovykvantovoie lektroniki.-M.: Nauka, 1986

[15] Mandel' L., Vol'f E. Opticheskaya kogerentnost' i kvantovaya optika. -M.: Fizmatlit, 2000

[16] Preskill Dzh. Kvantovaya informaciya i kvantovyevy chisleniya.-M.: RHD, 2008

[17] Holevo A.S. Vvedenie v kvantovuyu teoriyu informacii. – M.: MCNMO, 2002

[18] Einstein A., Podol'skii B., Rozen N. // «Mozhno li schitat', chto kvantovo-mehanicheskoe opisanie fizicheskoi real'nostiya vlyaetsya polnym? » //UFN, 1934, Tom XVI, vypusk 4. - perevod–Lyubina A.G., pod redakciei Foka A. V.

[19] Dolgov V.A. i dr. Kriptograficheskie metody zashity informacii.-Habarovsk, 2008

[20] Emel'yanov V.I. Kvantovaya fizika: Bity i Kubity.-M.:Izd.MGU,2012

[21]http://www.gartner.com/newsroom/id/2819918?fnl=search&srcId=1-3478922254

[22] http://www.itsec.ru

[23] http://sci-article.ru

[24] http://works.tarefer.ru/71/100019/index.html

[25] http://book.itep.ru/3/optic_32.htm

[26] Kilin S.Ya Kvantovaya informaciya // Uspehi fizicheskoi nauki, 1999, Tom 169, ¹5

[27] http://www.kurzweilai.net/a-new-quantum-cryptography-scheme-to-secure-anonymous-transactions

[28] Aktaeva A.U., Ilipbaeva L.I., Baimuratov O.A., Galieva N.G. Informacionnaya bezopasnost': kvantovye tehnologii // Informacionnaya bezopasnost' v sveteStrategii Kazakhstan - 2050», 2015. str.16-25

[29] Aktaeva A.U., Baimuratov O.A., Galieva N.G., Ilipbaeva L.I., Iskodzhaeva I. Kvantovaya informatika: bezopasnost' informacii // Sovremennye innovacionnye tehnologii i IT - obrazovanii. 2015

[30] http://www.triniti.ru/ /Ezhov1.pdf

[31] http://www.mathworks.com/

AUTHOR PROFILES

A. Aktayeva received the degree in applied mathematical science at Kazakh State University after named S.M.Kirova from Kazakhstan, in 1987. Currently, she is an Associate Professor at Kazakh Academy of Transport and Communication after named M. Tynyshbayeva.

N. Galiyeva received the degree in computer science at Kazakh National Technical University after named K.I.Satpayev from Kazakhstan, in 2000. Currently, she is an researcher at Kazakh Academy of Transport and Communication after named M. Tynyshbayeva.

O. Baimuratov received the degree in computer science at Korkyt Ata Kyzylorda University from Kazakhstan, in 2010. Currently, he is an Associate Professor at Kazakh Academy of Transport and Communication after named M. Tynyshbayeva.