BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 2, Number 372 (2018), 6 – 16

UDC004.056.55: 004.421.5

B. Ahmetov[1], S. Gnatyuk[2], V. Kinzeryavyy[2], Kh. Yubuzova[1]

[1]Satbayev University, Almaty, Kazakhstan,
[2]National aviation University, Kiev, Ukraine.
E-mail: bakhytzhan.akhmetov.54@mail.ru s.gnatyuk@nau.edu.uas.gnatyuk@nau.edu.ua hali4a@mail.ru

MODEL OF SIMULATION OF OPERATION OF THE DETERMINISTIC PROTOCOL OF SAFE COMMUNICATION IN THE QUANTUM CHANNEL WITH NOISE

Abstract. Technologies of quantum cryptography do not depend on the computational capabilities of the intruder, because they use the unique properties of quantum particles, and are based on the principles of inviolability of the laws of quantum physics. There are many methods and approaches used to solve the tasks of securing the privacy of message transmission without the use of encryption. The most advanced technology of quantum cryptography is quantum direct safe communication, which allows information to be transmitted by an open channel without prior encryption. For this purpose, experimental studies of a deterministic protocol model in a channel with noise using a couple of qutrites in the eavesdropping control mode were carried out.

Key words: information protection, quantum cryptography, deterministic protocol, quantum key distribution, quantum direct secure communication, qubit, qutrit.

Introduction. Quantum cryptography, based on the theory of quantum mechanics, allows to develop new methods for ensuring the stability and security of information transfer, to solve the problems of classical cryptography related to the distribution of keys. In addition, it makes it possible to provide resistance to various kinds of quantum key search algorithms [1]. The use of quantum protocols of direct safe communication allows to solve the problem of message transmission secrecy without the use of encryption. This secrecy is guaranteed by the laws of quantum physics [2-4].

With the help of quantum states of quantum systems groups (two- or multilevel, photons are often used) is coded the source text of the secret message, then they are transmitted by a quantum communication channel. The laws of quantum physics also guarantee the detection of eavesdropping in the channel. Therefore, during a communication session legitimate users (A and B) can immediately detect the intruder (E) and interrupt the communication session.

Objects and methods of research. There are many different types of quantum secure communication protocols. For example, ping-pong protocol [2], for practical implementation of which there is enough a small amount of quantum memory, and it can be realized on the basis of already used technical equipment [5]. This type of the protocol uses two Bell states of an entangled pair of qubits, which allows to transmit one bit of classical information for one protocol cycle [2]. If we use all four states of Bell's qubits pair, that is, quantum super dense coding, then it is possible to increase the number of bits per cycle twice, that is, there will be two bits [3]. In order to increase the information capacity instead of the

entangled pairs of qubits there can be used their triples, quarks, etc. In particular, the work [4] investigates the protocol with the entangled states of the Greenberger-Horn-Zeilinger (GHZ) triples and quadruples of qubits. These states provide an information capacity equal to n bits per cycle, that is, the number of qubits in the used states of the GHZ.

Also, in order to increase the information capacity of the protocol it is possible to use entangled states of multilevel quantum systems. For example, in works [6, 7] there was studied a protocol using Bell states of a three-level systems pair (qutrits) and quantum super dense coding for qutrits. Its information capacity is a bit per cycle, not two bits per cycle, as for the Bell protocol with qubit states.

In works [8-13] there are considered various types of attacks, analyzed a general incoherent attack on various variants of the protocol, including a protocol with qutritpairs [8]. During the attack, the intruder E can take some information off before this attack will be detected [8, 11-13]. In work [13] there was investigated the method of reverse message hashing, based on multiplication by random inverse matrices. Then, the resulting multiply message is transmitted by a quantum channel, at the same time, legitimate users have the opportunity to analyze the error level by applying the protocol eavesdroppingcontrol mode. So, for example, if the permissible level is not exceeded, then the matrices transmit by the classical (non-quantum) channel, as a result this allows the other side to obtain the source text by multiplying the received message on the corresponding inverse matrices. The model of the protocol makes it possible to compare the error levels with a certain average noise level emitted by the quantum channel and according to the result of this comparison makes it possible to confirmthe presence or absence of the fact of eavesdropping.

The researches carried out in work [16] confirm the statements that the error levels, caused by the actions of the intruder and natural noise in the channel, are not of a simple nature. In this connection, there is arisen the problem of synchronously fixing the changes that arise in the states of transmitted photons from the combined influence of the actions of the intruder and natural noise in the channel. Further researches will help to create a model that simulates the operation of the protocol in the eavesdropping control mode and to obtain a number of practical recommendations on the use of a quantum protocol in a channel with noise.

The purpose of this article is an experimental research of the simulation model of a deterministic protocol with qutrit pairs in the eavesdropping control mode in a channel with noise.

Results and discussion

1. The eavesdropping control mode for a protocol with pairs of completely entangled qutrits. If we take as a basis the researches carried out in work [7], in particular, the behavior of the deterministic protocol in the noise channel, it can be concluded that in the eavesdroppingcontrol mode of the protocol (figure 1) both users check the initial entangledstates prepared by the second user for their invariability $|\Psi_{00}\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$, as the attack of the intruder on the channel will make changes to these states.

Both users measure the state of each qutrite separately from each other, and this measurement is carried out in two different bases, switched randomly. An example are two mutually unshifted basesz and x:

$$|z_0\rangle = |0\rangle, \quad |z_1\rangle = |1\rangle, |z_2\rangle = |2\rangle;$$
$$|x_0\rangle = (|0\rangle + |1\rangle + |2\rangle)/\sqrt{3}, \quad |x_1\rangle = (|0\rangle + e^{2\pi i/3}|1\rangle + e^{-2\pi i/3}|2\rangle)/\sqrt{3}, \qquad (1)$$

With the probability equal to $1/3$ the user A in each of the bases will receive one of three possible results - "0", "1" or "2". On the other side, the user B after receiving the measurement results with the selected basis will also measure the state of his prepared, "home" qutrit (figure 1).

Thus, in work [7] it is proved that the user B can obtain a result with the probability equal to 1, that follows from the state $|\Psi_{00}\rangle$ in the $z-$ and $x-$basises:

$$|\Psi_{00}\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3} = (|x_0x_0\rangle + |x_1x_2\rangle + |x_2x_1\rangle)/\sqrt{3}. \qquad (2)$$

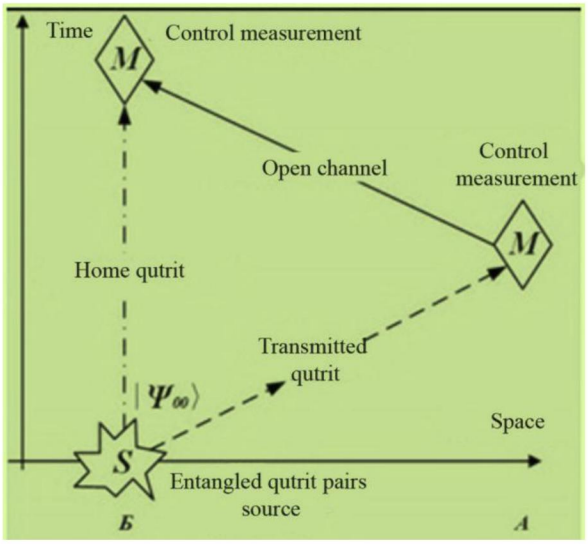

Figure1 – Quantum channel in eavesdropping control mode

However, the user B can obtain accurate results only if there is no natural interference or noise or an intruder's attack in the quantum channel. There is no method of error recognition in the case when there are natural interferences in the channel, and interferences from the actions of intruder E [1]. In this regard, the problem of model construction that allows to investigate a joint attack of the intruder and natural quantum noise in the channel is very actual.

2. Model of the eavesdropping control mode of a deterministic protocol in a quantum channel with noise. The nature of the quantum channel can have many errors associated with phase change or with rotation of the qubit quantum state in the Hilbert space. The main and important property of the quantum code, correcting some discrete set of errors, is the ability to correct automatically a continuous set of errors [14]. This property is explained by measuring the error syndrome or by designing a state with a small error on the state without error, or by designing a false state on some state of most of the discrete set of errors. In other words, there is a discretization of quantum errors, which makes it possible to generate quantum codes in order to correct a certain discrete set of errors, and to correct automatically any error in the state of quantum systems [14].

The operation of the channel is as follows: with the probability p the qubit state becomes completely mixed, i.e. is depolarized, but with the probability $(1-p)$ it remains unchanged. It follows from the work [14]: the operator of the depolarized channel for qubits is described by the equation:

$$\varepsilon(\rho) = (1-p)\rho + p/3 \cdot \left(\sigma_x \rho \sigma_x + \sigma_y \rho \sigma_y + \sigma_z \rho \sigma_z\right), \tag{3}$$

The $\sigma_x$operator describes the "classical" qubit overturn error, the σ_z operator describes the phase overturn errors, and the σ_y operator describes combinations of these two errors, phase errors. The depolarized channel influences on the qubit as a superposition of these three large discrete quantum errors.

Although a depolarized channel cannot transmit all potentially possible types of quantum errors, but takes into account the essential types of the majority of discrete quantum errors [14]. Therefore, this channel is widely used in quantum information theory as a model of quantum noise.

In accordance with the work [15] the action of the depolarized channel of an individual qutrit is described by the operator:

$$\varepsilon_{qutrit}(\rho) = (1-p)\rho + p/8 \cdot \left(Y\rho Y^{\dagger} + Z\rho Z^{\dagger} + Y^2\rho\left(Y^2\right)^{\dagger} + YZ\rho(YZ)^{\dagger} + Y^2Z\rho\left(Y^2Z\right)^{\dagger} + \right.$$
$$\left. + YZ^2\rho\left(YZ^2\right)^{\dagger} + Y^2Z^2\rho\left(Y^2Z^2\right)^{\dagger} + Z^2\rho\left(Z^2\right)^{\dagger}\right), \tag{4}$$

where $Y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{2\pi i/3} & 0 \\ 1 & 0 & e^{4\pi i/3} \end{pmatrix}$.

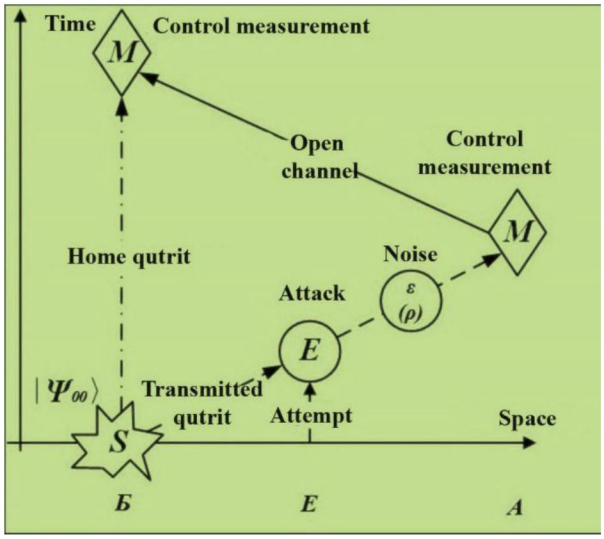

Figure 2 – The eavesdropping control mode in a depolarized channel at incoherent attack

Figure 2 shows the eavesdropping control mode of a deterministic protocol with entangled qutrit pairs for the case when the noise operator (4) influenced on the transmitted qutrit. The transmitted qutrit is initially affected by the attack of the intruder, then the noise operator acts. In accordance with the conducted analysis by the scheme of work [2] and its generalization to the protocol with qutrit pairs, given in work [8], the state of the quantum system "transmitted qutrit – the attempt of the intruder" after the attack of the intruder can be represented as:

$$\begin{aligned}
\left|\psi^{(0)}\right\rangle &= E\left|0,\varphi\right\rangle = \alpha_0\left|0,\varphi_{00}\right\rangle + \beta_0\left|1,\varphi_{01}\right\rangle + \gamma_0\left|2,\varphi_{02}\right\rangle,\\
\left|\psi^{(1)}\right\rangle &= E\left|1,\varphi\right\rangle = \alpha_1\left|0,\varphi_{10}\right\rangle + \beta_1\left|1,\varphi_{11}\right\rangle + \gamma_1\left|2,\varphi_{12}\right\rangle,\\
\left|\psi^{(2)}\right\rangle &= E\left|2,\varphi\right\rangle = \alpha_2\left|0,\varphi_{20}\right\rangle + \beta_2\left|1,\varphi_{21}\right\rangle + \gamma_2\left|2,\varphi_{22}\right\rangle,
\end{aligned} \tag{5}$$

As a result of the combined state of the transmitted qutrit it can be conditionally assumed that the user B sends the qutrit in the state either $\left|0\right\rangle$, or $\left|1\right\rangle$, or $\left|2\right\rangle$ with the probability equal to 1/3. In the equations (5) $(i,j=0)\{\left|\varphi_{ij}\right\rangle\}(i,j=0\ldots 2)$ there is presented the set of qutrit states - the attempts of the intruder E.

The attack of the intruder E can be represented in the form of a matrix:

$$E = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \\ \gamma_0 & \gamma_1 & \gamma_2 \end{pmatrix}. \tag{6}$$

In the case when the user B sends $\left|0\right\rangle$, then the state of the transmitted qutrit after the combined operation of the intruder E is presented in the following form:

$$\left|\psi\right\rangle = \alpha_0\left|0\right\rangle + \beta_0\left|1\right\rangle + \gamma_0\left|2\right\rangle, \tag{7}$$

Andits density matrix in the basis $\left|0\right\rangle$, $\left|1\right\rangle$, $\left|2\right\rangle$:

$$\rho = \left|\psi\right\rangle\left\langle\psi\right| = \begin{pmatrix} \left|\alpha_0\right|^2 & \alpha_0\beta_0^* & \alpha_0\gamma_0^* \\ \beta_0\alpha_0^* & \left|\beta_0\right|^2 & \beta_0\gamma_0^* \\ \gamma_0\alpha_0^* & \gamma_0\beta_0^* & \left|\gamma_0\right|^2 \end{pmatrix}. \tag{8}$$

After the transformation of the formula (4) with substitution of the formula (8), we obtain:

$$\rho_{out}=\frac{1}{8}\begin{pmatrix}\left(3p\left(|\beta|^2+|\gamma|^2\right)+(8-6p)|\alpha|^2\right) & (8-9p)\alpha\beta^* & (8-9p)\alpha\gamma^* \\ (8-9p)\beta\alpha^* & \left(3p\left(|\alpha|^2+|\gamma|^2\right)+(8-6p)|\beta|^2\right) & (8-9p)\beta\gamma^* \\ (8-9p)\gamma\alpha^* & (8-9p)\gamma\beta^* & \left(3p\left(|\alpha|^2+|\beta|^2\right)+(8-6p)|\gamma|^2\right)\end{pmatrix}. \quad (9)$$

The indices «0» α, β, and γ for the reduction of the record are not considered further.

The probability of an erroneous result R_z is equal to the sum of two other diagonal elements (or to the difference between the unit and the upper left element of the matrix ρ_{out}):

$$R_z=1-1/8\cdot\left(3p\left(|\beta|^2+|\gamma|^2\right)+(8-6p)|\alpha|^2\right). \quad (10)$$

R_z indicates a change in the state of the transmitted qutrit, measuring in the $z-$ basis of the user B.

The probability of detecting the attack of the intruder E during the implementation of the protocol in an ideal quantum channel according to work [8] is:

$$d_z=|\beta|^2+|\gamma|^2=1-|\alpha|^2. \quad (11)$$

Transforming the expression (11) with the help of (12), we obtain:

$$R_z=d_z+\frac{3}{4}p\left(1-\frac{3}{2}d_z\right). \quad (12)$$

The result (12) will not change even if the transmitted qutrit will be affected by the noise and then the attack of the intruder E. The calculations show that the diagonal elements of the density matrix (9) do not depend on who made the interferences, was it the attack of the intruder E or the interferences of the depolarized channel itself.

In cases where the user B sends $|1\rangle$ or $|2\rangle$ this corresponds to the wave functions $|\psi^{(1)}\rangle$ and $|\psi^{(2)}\rangle$ in (5), then because of the relationship between the parameters according to work [8]:

$$|\alpha_0|^2=|\beta_1|^2=|\gamma_2|^2;\quad |\alpha_1|^2=|\beta_2|^2=|\gamma_0|^2;\quad |\alpha_2|^2=|\beta_0|^2=|\gamma_1|^2 \quad (13)$$

These cases will also have the result of expression (12). Therefore, the total probability of the error at the measurement of the user B in the basis $z$will be:

$$R_{полна-z}=\frac{1}{3}\cdot 3R_z=R_z=d_z+\frac{3}{4}\cdot p\left(1-\frac{3}{2}d_z\right). \quad (14)$$

Similarly, it is possible to make the same calculations for the control measurement of the user B in the basis$x$, then we will obtain the identical structure of the expression for the probability of the error $R_{полна-x}$:

$$R_{полна-x}=d_x+\frac{3}{4}p\left(1-\frac{3}{2}d_x\right), \quad (15)$$

where d_x – probability of the error at the measurement of the user B in the basis $x$at the implementation of a deterministic protocol in an ideal quantum channel.

According to the work [8] the maximum value corresponding to the complete information of the intruder E is equal to 2/3. Figure 3a shows the dependence of $R_{полна-z}$ from d_z and ρ. From Figure 3a we can see that the superposition of the operation of the intruder E and of the noise in the depolarized channel leads to the fact that at $d_z=2/3$ $R_{полна-z}$ does not depend on $\rho$and is also equal to 2/3. From the obtained results it follows that at the incoherent attack the maximum value of the error probability at the protocol execution in the eavesdropping control mode in the depolarized channel will be the same with or without noise.

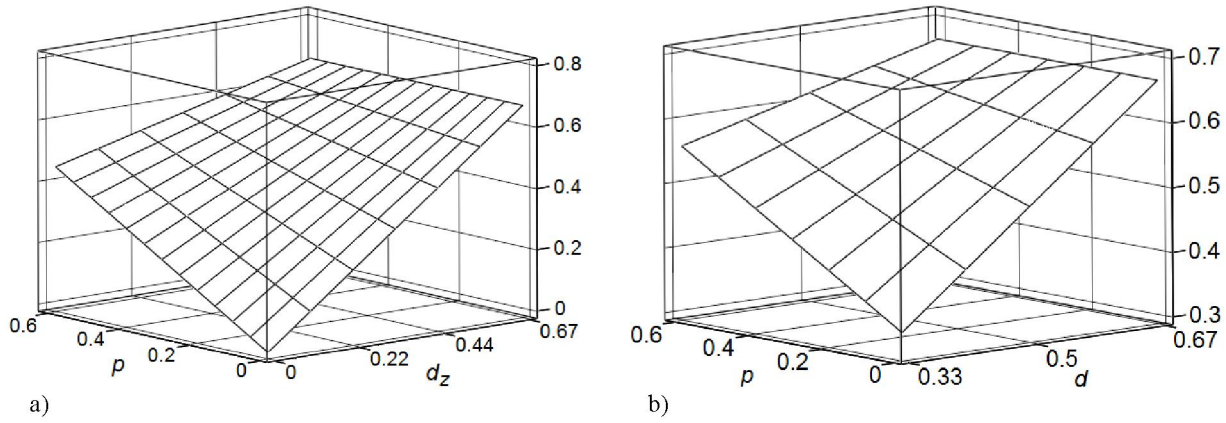

Figure 3 – Dependences of the total error probability
at the measurement of the user B in one of the bases (a) and at the middle error probability in two bases (b) for the DPC

In the basis x the attack of the intruder creates the maximum level $d_x = 2/3$, regardless of the level of errors d_z created by it in the basis z, and vice versa [8]. Figure 3b shows the dependence:

$$R_{полна} = 1/2 \cdot \left(2/3 + R_{полна-z}\right) \tag{16}$$

from$\rho$and middle error level created by the attack, according to the both bases: $d = 1/2 \cdot (2/3 + d_z)$, under the condition that legitimate users switch between the bases $z-$ and $x-$with equal probability 1/2, that is the most reasonable eavesdropping control strategy for them [8].

3. Experimental research of the simulation model of a deterministic protocol with qutrit pairs in a quantum channel with noise in the eavesdropping control mode. The model simulates the operation of a deterministic protocol with qutrit pairs in a depolarized channel at the presence of an intruder E. During the research and modeling process of the deterministic protocol in the eavesdropping control mode there were obtained statistical data on error levels in $x-$, $z-$basises and their middle values. The obtained statistical data make it possible to obtain practical recommendations on the possibilities of using a deterministic protocol in a quantum channel with noise.

In addition, this model used a non-quantum method of enhancing the security of the ping-pong protocol, which is described in detail in work [14].

In order to start the message transfer process the user A converts his ternary message $a (a = (a_1, \dots, a_l), i = 1, \dots, l)$ of some fixed length $r \cdot$, then for each block a random ternary sequence G $(G = (G_1, \dots, G_l), i = 1, \dots, l$ with the length $r \cdot l$ is separately generated, each block of which G_i is summed bit by bit according to the module 3 with the corresponding message blocks a_i:

$$b_i = a_i + G_i \tag{17}$$

Further, using the quantum protocol according to the quantum channel the resulting message $b, (b = (b_1, \dots, b_l), i = 1, \dots, l)$ is transmitted to the user B. If the intruder E intercepts the message, he will not be able to use it, because without randomly generated sequences G_i he cannot restore the initial message.

After the transmission on the quantum channel, only if both sides are sure that the transmission session has not been overheard by the intruder E, the randomly generated sequences G_i are transmitted to the user B by the classical open channel. In order to restore the initial message, the user B should use the received random sequences by combining them with the corresponding blocks of the message:

$$a_i = b_i - G_i. \tag{18}$$

The length of the block $r$was chosen in order to reach a high level of stability, and also that the probability $s(s(I, q, d) = \left(\frac{1-q}{1-q\cdot(1-d)}\right)^{I/I_0}$ of a successful attack of the intruder E after the transmitting of one block was insignificant. The length of the block should be determined by the formula:

$$r = -kI_0 / \lg((1-q)/(1-q\cdot(1-d))), \quad (19)$$

where k – the value for calculating the probability of the not detected attack of the intruder E, I_0 – the amount of information that the intruder E can receive by one cycle of the message transmission mode, q – the probability of switching to the eaves dropping control mode, d – the level of error sarising from the actions of the intruder E [13].

For the modeling of the operation of a deterministic protocol with qutrit pairs the following parameters were used:

1) the length of the transmitted ternary data is $length = 100\,000$ trits;

2) an value of the degree of ten for calculating the probability of an unidentified attack of the intruder E -$k = 4$, that is$s(I, q, d,)$=10^{-k};

3) the probability of switching the protocol to the eavesdropping control mode and $q$message transmission can take values from 0.1 to 0.9;

4) in order to calculate the values r (19) we choose:

$I_0 = 2$ - the possible amount of information that can be removeв by the intruder E by one round of transmission, $d = 1/3$ - the level of errors that may arise from the actions of the intruder E in accordance with the work [13];

5) the probability of detecting an attack measured in the basis$x$ - $d_x = 0 \ldots 2/3$;

6) the probability of detecting an attack measured in the basis$z$ - $d_z = 2/3$;

7) the probability of depolarization of the qubit state - $\rho = 0 \ldots 0.5$ and the probability of the unchanged qubit state $(1-\rho)$;

8) the probability of switching of the users A and B between the bases $x-$ and $q_x = q_z = 0{,}5$.

Before the modeling the following values should be specified: $length$, q , d_x andρ, and then the following operations should be performed:

1. Determination of the average probability of detecting an attack according to two bases in an ideal channel, that is, the value d_{Eva} by the expression $d_{Eva} = q_z d_z + q_x d_x$

This parameter determines the average level of errors recorded in the eavesdropping control mode in an ideal channel and is needed for comparison with the corresponding value in a channel with noise $R_{полна}$ (17), taking into account the simultaneous change in the states of the transmitted photons as a result of the actions of the intruder E and of the natural noise.

2. Determination of the length of the data block r(19) and the amount of these blocks$l$, into which the transmitted data is divided, l is determined by the expression $l = length/r$.

3. Determination of the error probabilities at the measurements in bases x, zandthe average value for two bases, i.e. parameters Err_x, Err_z, Err_{mean} by the expressions:

$$Err_x = d_x + 3/4\cdot p\cdot(1-3/2\cdot d_x),$$
$$Err_z = d_z + 3/4\cdot p\cdot(1-3/2\cdot d_z),$$
$$Err_{mean} = q_x\cdot Err_x + q_z\cdot Err_z. \quad (20)$$

4. Generating a pseudo-random ternary sequence a with size $length$ (the probability of generating "0", "1", "2" was taken equal to $1/3$).

5. Separation of the obtained in the previous paragraph ternary sequence a, $(a = (a_1, \ldots, a_l)$, $i = 1, \ldots, l)$ with the size $r\cdot$on$l$ blocks of smaller volume, the last block, if necessary, is supplemented with random trits in order to obtain the required length r, then perform following operations:

- generating a random sequence in a GF (3) field $G(G = (G_1, \ldots, G_l), i = 1, \ldots, l)$ with the size$r\cdot l$.

- addition $a_i + G_i$ in the Galois GF field (3), as a result we obtained b_i (18).

- transmission of b_i by means of a deterministic protocol in a quantum channel with noise.

Switching between the eavesdropping control modes and message transmission occurs with probabilities $q$and $(1-q)$. In the message transmission mode on the quantum channel the user B receives a couple of qutrits, the errors occur due to the attack of the intruder E and to the natural noise of the channel, the errors were not modeled. With equal probabilities $q_x = q_z = 1/2$ in the eavesdropping control mode there is selected a certain basis and calculated the total number of transitions to a certain basis (Kp_x, Kp_z). Then, an error is modeled for the basis x with the probability Err_xor for a basis $z$with the probability Err_z, then the amount of errors $Co_{D_x}$and $Co_{Dz}$is counted. The process of switching between the modes is repeated until the block $b_i$is fully transmitted.

Then, after all the blocks $b_i$are received the user A transmits to the user B by the open channel G $(G_1, \ldots, G_l), i = 1, \ldots, l)$, after which we will obtain a_i:$a_i = b_i - g_i$.

- calculation of the average level of errors in the bases $x, z$and the average error level for the two bases according to each transferred block b_i: $b_i\_Errlvl_x$, $b_i\_Errlvl_z$ and $b_i\_Errlvl_{mean}$ and by the expressions:

$$b_i\_Errlvl_x = Co_{Dx}/Kp_x; \quad b_i\_Errlvl_z = Co_{Dz}/Kp_z;$$
$$b_i\_Errlvl_{mean} = (Co_{Dx} + Co_{Dz})/(Kp_x + Kp_z). \qquad (21)$$

6. According to the obtained values there were calculated the minimum ($MinErrlvl_x$,$MinErrlvl_z$, $MinErrlvl$) and maximum ($MaxErrlvl_x$,$MaxErrlvl_z$,$MaxErrlvl$) values of the error levels, the average values ($MeanErrlvl_x$,$MeanErrlvl_z$,$MeanErrlvl$) for all the transferred blocks l.

Figures 4, 5 presents the results of the probabilities of the qutrit states depolarization during the modeling of the protocol at different values $q, Dx, Dz, Deva$.

Table summarizes all modeling results.

1. According to the results we see that within the statistical error the average values of the error level for all transmitted blocks $MeanErrlvl$are equal to the corresponding theoretical values $Errmean$, obtained by the formula (21). However, it is possible only in the case of transmission of a sufficiently large volume of transmitted data blocks. But at the same time, the minimum error levels for both bases ($MinErrlvl$) are small enough and in most cases less than the level of natural noiseρ, especially at large ρ (table).) All this is a consequence of the random nature of quantum measurements. Therefore, transmitting one block and checking the error level in the eavesdropping control mode theusers A and B can make the

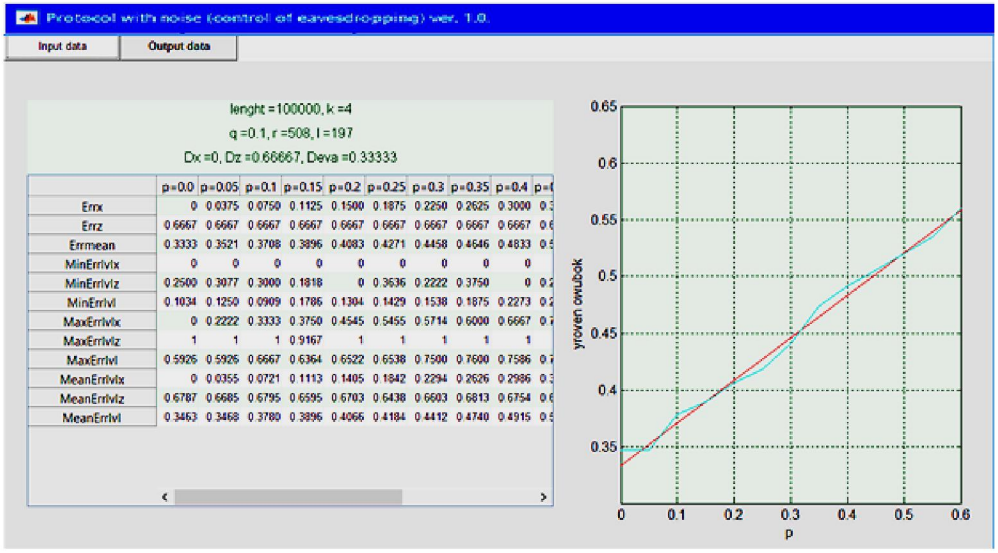

Figure 4 –The error levels values at modeling from$q = 0.1, Dx = 0, Dz = 0.6667, Deva = 0.3333$ and the probability of the qutrit states depolarization from$\rho = 0.0$ till $\rho = 0.4$

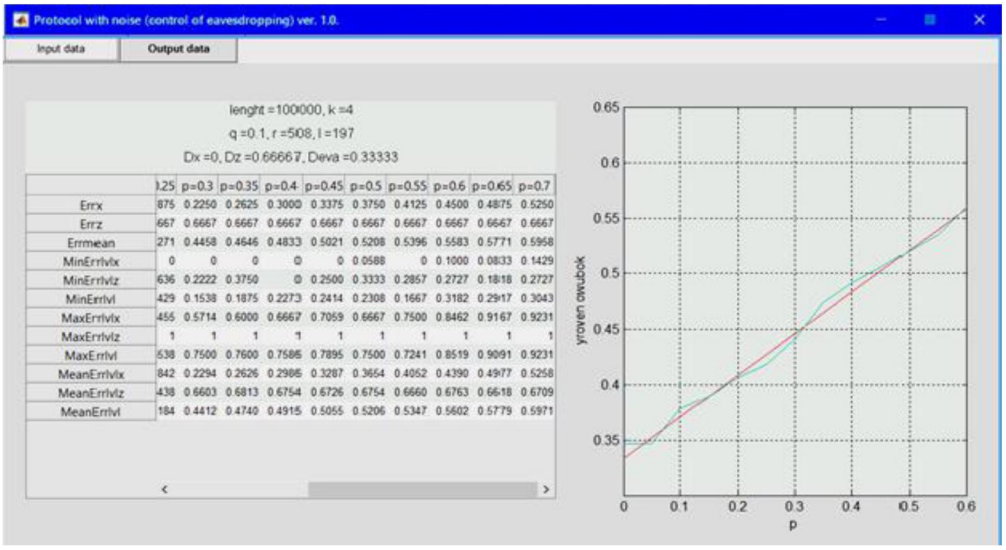

Figure 5 – The error levels values at modeling from$q = 0.1, Dx = 0, Dz = 0.6667, Deva = 0.3333$ and the probability of the qutrit states depolarization from$\rho = 0.3$till$\rho = 0.7$

Modeling results

d			d_x=0;d_z=0,667; d_{Eva}=0,333				d_x=0,333;d_z=0,667; d_{Eva}=0,5				d_x=0,667;d_z=0,667 ;d_{Eva}=0,667			
p			**p=0,1**	**p=0,3**	**p=0,5**	**p=0,7**	**p=0,1**	**p=0,3**	**p=0,5**	**p=0,7**	**p=0,1**	**p=0,3**	**p=0,5**	**p=0,7**
Errx			0,075	0,225	0,375	0,525	0,371	0,446	0,521	0,596	0,667	0,667	0,667	0,667
Errz			0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667
Errmean			0,371	0,446	0,521	0,596	0,519	0,556	0,594	0,631	0,667	0,667	0,667	0,667
k=4;length=100000	q=0,5;r=66;l=1516	MinErrlvlx	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,143	0,286	0,143	0,250	0,200
		MinErrlvlz	0,167	0,143	0,300	0,200	0,167	0,143	0,200	0,286	0,000	0,167	0,273	0,154
		MinErrlvl	**0,080**	**0,154**	**0,240**	**0,296**	**0,120**	**0,267**	**0,280**	**0,273**	**0,381**	**0,370**	**0,353**	**0,320**
		MaxErrlvlx	0,375	0,600	0,875	1	1	0,909	1	1	1	1	1	1
		MaxErrlvlz	1	1	1	1	1	1	1	1	1	1	1	1
		MaxErrlvl	0,655	0,809	0,794	1	0,857	0,920	0,833	0,875	0,960	0,929	0,952	0,949
		MeanErrlvlx	0,075	0,224	0,378	0,521	0,372	0,444	0,519	0,594	0,668	0,666	0,664	0,667
		MeanErrlvlz	0,663	0,666	0,665	0,670	0,661	0,666	0,663	0,665	0,665	0,667	0,673	0,666
		MeanErrlvl	**0,369**	**0,445**	**0,522**	**0,596**	**0,517**	**0,554**	**0,591**	**0,630**	**0,666**	**0,666**	**0,668**	**0,667**
	q=0,25;r=176;l=569	MinErrlvlx	0,000	0,000	0,000	0,100	0,000	0,000	0,143	0,125	0,120	0,333	0,200	0,273
		MinErrlvlz	0,308	0,333	0,200	0,200	0,286	0,200	0,273	0,200	0,200	0,273	0,231	0,111
		MinErrlvl	**0,115**	**0,167**	**0,200**	**0,360**	**0,263**	**0,290**	**0,320**	**0,343**	**0,385**	**0,333**	**0,381**	**0,375**
		MaxErrlvlx	0,375	0,667	0,800	0,933	0,875	0,846	0,857	0,929	1	1	1	1
		MaxErrlvlz	1	1	1	1	1	1	1	1	1	1	1	1
		MaxErrlvl	0,654	0,711	0,793	0,936	0,905	0,813	0,852	0,905	0,917	0,909	0,931	0,931
		MeanErrlvlx	0,076	0,225	0,376	0,536	0,363	0,451	0,535	0,598	0,667	0,664	0,669	0,667
		MeanErrlvlz	0,677	0,660	0,664	0,665	0,665	0,657	0,666	0,666	0,663	0,663	0,666	0,668
		MeanErrlvl	**0,374**	**0,441**	**0,518**	**0,599**	**0,516**	**0,556**	**0,601**	**0,632**	**0,666**	**0,663**	**0,667**	**0,668**
	q=0,1;r=508;l=197 q=0,1;r=508;l=197	MinErrlvlx	0,000	0,000	0,059	0,143	0,083	0,000	0,000	0,250	0,333	0,211	0,300	0,273
		MinErrlvlz	0,300	0,222	0,333	0,273	0,200	0,273	0,333	0,286	0,200	0,308	0,375	0,333
		MinErrlvl	**0,091**	**0,154**	**0,231**	**0,304**	**0,226**	**0,227**	**0,318**	**0,353**	**0,382**	**0,367**	**0,423**	**0,419**
		MaxErrlvlx	0,333	0,571	0,667	0,923	0,779	1	0,917	0,889	1	1	1	1
		MaxErrlvlz	1	1	1	1	0,933	1	1	1	1	0,947	1	1
		MaxErrlvl	0,667	0,750	0,750	0,923	0,800	0,828	0,833	0,900	0,944	0,929	0,947	0,909
		MeanErrlvlx	0,072	0,229	0,365	0,526	0,375	0,454	0,508	0,589	0,673	0,653	0,672	0,662
		MeanErrlvlz	0,679	0,660	0,675	0,671	0,651	0,657	0,677	0,669	0,677	0,653	0,679	0,664
		MeanErrlvl	**0,378**	**0,441**	**0,521**	**0,597**	**0,514**	**0,556**	**0,593**	**0,629**	**0,671**	**0,655**	**0,675**	**0,662**

wrong conclusion that there is no eavesdropping.Thus, in a noisy channel, in particular at a sufficiently high level of natural noises, the legitimate users must transmit sufficiently large amount of blocks, at least a few dozen, and only then make a conclusion whether or not there is the attack of the intruder E (and on the need to interrupt the operation of the protocol, or to transmit a pseudo-random sequence $G$from user A to user B). All this is the basis for developing recommendations for the practical implementation of a deterministic protocol with entangled qutrit pairs in a depolarized channel.

2. The average error levels are almost independent from the probability of switching to the control eavesdropping mode of (table).

But the probability significantly affects the speed of data transmission by a deterministic protocol: the smaller q is, the more often the data is transmitted and the higher the speed is. But the length of the block $r$also depends on q, with decreasing of $q$according to the exponential law it increases [16].

3. At $\rho = 0{,}7$and at the attack of the intruder E with zero error level in one of the basises (for example, d_x=0,d_{Eva} = 0,333), the average level of errors *MeanErrlvl* almost does not exceed p, therefore the legitimate users can make the wrong decision about the absence of attack. Therefore, it is necessary to check the average errors level in each of the bases x and $z$separately, in one of these basises the error level will be close to the value 2/3. In addition, we can conclude that for reliable detection of an attack the legitimate users should use a quantum channel with a natural noise level, on practice this means using a channel of a limited length.

Conclusions. In this work there was developed a model of the deterministic protocol in the eavesdropping control mode with qutrit pairs in a channel with noise and there is modeled its work in a channel with noise. Obtained a formula for the total probability of an erroneous result at measuring in the eavesdropping control mode. The equality of the values of the maximum error probability in the eavesdropping control mode is substantiated at the implementation of the protocol in an ideal and noisy depolarized channels. There is established that in a depolarized channel, especially at a sufficiently high level of noise, the legitimate users must transmit a sufficiently large amount of blocks of information (at least several dozen) and only then decide whether or not an attack exists. It was also been established that the legitimate users need to use a limited-length quantum channel with a natural noise level $\rho \leq 0{,}5$ for reliable detection of an attack on practice.

This model can be further improved by taking into account errors in the message transmission mode and using noise-immune coding for the qutrits.

REFERENCES

[1] Baumejster D.Physics of Quantum Information. Moscow.*Postmarket*. **2002**. P.376.

[2] Bostrom K. Deterministic secure direct communication using entanglement.*Physical Review Letters*. **2002**. Vol. 89, issue18. doi = {10.1103/PhysRevLett.89.187902}

[3] Cai Q. Y. Improving the capacity of the Bostrom Felbinger protocol.*Physical ReviewA***2004**. Vol. 69,issue5. Doi054301.

[4] Vasiliu E. V.Ping-pong protocol with three and four qubit states of Greenberger-Horn-Zeilinger. // Proceedings of the Odessa Polytechnic University.**2008**. Vol. 1 (29).p. 171-176. (In Russian)

[5] Ostermeyer M On the implementation of a deterministic secure coding protocol using polarization entangled photons. *Optics Communications*.**2008**. Vol. 281, issue17. P. 4540- 4544

[6] Wang Ch. Quantum secure direct communication with high dimension quantum superdense coding.*Physical ReviewA*.**2005**. Vol. 71, issue4doi = {10.1103/PhysRevA.71.044305}

[7] Vasiliu E. V.Ping-pong protocol with completely entangled states of triplets of three-dimensional quantum systems. // Digital technologies.**2009**. № 5.p. 18- 26. (In Russian)

[8] Vasiliu E. V.Analysis of the passive interception on the ping-pong protocol with completely entangled qutrit pairs. // East-European Journal of Advanced Technologies. **2009**. № 4/ 2(40). p. 4 -11. (In Russian)

[9] Zhang Zh. J. Improved Wojcik s eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss.*PhysicsLettersA*.**2005**. Vol. 341, issue5-6. P. 385-389doi.org/10.1016/j.physleta.2005.05.023

[10] CaiQ Y. The Ping-pong protocol can be attacked without eavesdropping. *Physical Review Letters*. **2003**. Vol. 91.Issue10. doi = {10.1103/PhysRevLett.91.109801}

[11] DengF. G. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Physical ReviewA*. **2003**. Vol. 68.Issue4.doi.org/10.1103/PhysRevA.68.042317

[12] Vasiliu E. V.Persistence of the ping-pong protocol with Greenberger-Horn-Zeilinger triplets to the attack using auxiliary quantum systems. // Informatics: Joint Institute for Informatics Problems of the National Academy of Sciences of Belarus. **2009**. № 1(21).p. 117-128. (In Russian)

[13] Vasiliu E. V.Synthesis of a Ping-Pong-based quantum communication protocol for a secure, direct messaging system. // *Naukov prats ONAZ im. O. S. Popova*.**2009**. № 1.p. 83 -91.(In Russian)

[14] Nilsen M. CHang I.Quantum Computing and Quantum Information. Moscow.*Mir***2006**.P. 824. — ISBN 5-03-003524-9
[15] Ramzan M. Noisy non-transitive quantum games.*J Phys A Math Theor.***2010**. Vol. 43. N 26. doi.org/10.1088/1751-8113/43/26/265304
[16] Vasiliu E. V.Estimating the computational complexity of a non-quantum method of enhancing the security of the ping-pong protocol. // Applied Radio electronics.**2009**.№3. p. 396 -404.(In Russian)

Б. Ахметов[1], С. Гнатюк[2], В. Кинзерявый[2], Х. Юбузова[1]

[1]Қ. И. Сәтбаев атынағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан,
[2]Ұлттық авиациялық университеті, Киев, Украина

ШУЫ БАР КВАНТТЫҚ АРНАДА ҚАУІПСІЗ БАЙЛАНЫСТЫҢ ДЕТЕРМИНИСТИКАЛЫҚ ХАТТАМАНЫҢ ЖҰМЫСЫНЫҢ ИМИТАЦИЯЛЫҚ ҮЛГІСІ

Аннотация. Кванттық криптографияның технологиялары бұзушының есептеу мүмкіндіктеріне тәуелді емес, себебі кванттық демеуліктердің айрықша бірегей қасиеттерін қолданады, кванттық физика заңдарының беріктілік қағидаларында негізделген. Хабарларды шифрлауды қолданбай құпия жіберуді қамтамасыз ету есебін шешу үшін қолданатын көптеген әдістер мен тәсілдемелер белгілі. Кванттық криптографияның ең дамыған технологиясы – алдын ала шифрлаусыз ашық арнамен ақпаратты жіберуге мүмкіндік беретін кванттық түзу қауіпсіз байланыс. Осы мақсатпен жұмыста жасырын тыңдауды бақылау режимінде кутриттер жұбын қолданумен шуы бар арнада кванттық хаттама үлгісінің эксперименттік зерттеулері жүргізілген.

Түйін сөздер: ақпаратты қорғау, кванттық криптография,детерминистикалық хаттама, кванттық кілттерді тарату, кванттық түзу, қауіпсіз байланыс, кубит, кутрит.

Б. Ахметов[1], С. Гнатюк[2], В. Кинзерявый[2], Х. Юбузова[1]

[1]Сатпаев университет, Алматы, Казахстан,
[2]Национальный авиационный университет, Киев, Украина

ИМИТАЦИОННАЯ МОДЕЛЬ РАБОТЫ ДЕТЕРМИНИСТИЧЕСКОГО ПРОТОКОЛА БЕЗОПАСНОЙ СВЯЗИ В КВАНТОВОМ КАНАЛЕ С ШУМОМ

Аннотация. Технологии квантовой криптографии не зависят от вычислительных возможностей нарушителя, так как используют специфические уникальные свойства квантовых частиц, основываются на принципах нерушимости законов квантовой физики. Известно много методов и подходов, используемых для решения задач обеспечения секретности передачи сообщений без применения шифрования. Самая развитая технология квантовой криптографии – квантовая прямая безопасная связь, позволяющая передавать информацию открытым каналом без предварительного шифрования.С этой цельюв работе дано описание проведеных экспериментальных исследованиймодели детерминистического протокола в канале с шумом с использованием пары кутритов в режиме контроля подслушивания.

Ключевые слова: защита информации, квантовая криптография,детерминистический протокол, квантовое распределение ключей, квантовая прямая безопасная связь, кубит, кутрит.

Information about authors:
Akhmetov Bakhytzhan Srazhatdinovich – Doctor of Technical Sciences, Professor, Satbayev University
Gnatyuk Sergey Aleksandrovich – Doctor of Science, Associate Professor, National Aviation University
Kinzeryavyy Vasiliy Nikolaevich – Candidate of Technical Sciences, Associate Professor, National Aviation University
Yubuzova Khalicha Ibragimovna – doctoral student of Satbayev University, hali4a@mail.ru