Quantum Inf Process (2011) 10:189–202
DOI 10.1007/s11128-010-0188-8

Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits

Eugene V. Vasiliu

Received: 7 March 2010 / Accepted: 7 July 2010 / Published online: 20 July 2010

Abstract The non-coherent attack on the ping-pong protocol with completely entangled pairs of three-dimensional quantum systems (qutrits) is analyzed. The expression for the amount of the eavesdropper's information as functions of attack detection probability is derived. It is shown that the security of the ping-pong protocol with pairs of qutrits is higher than the security of the protocol with pairs of qubits. It is also shown that with the use by legitimate users in a control mode of two mutually unbiased measuring bases, the ping-pong protocol with pairs of qutrits possesses only asymptotic security, as well as the protocol with entangled qubits.

Keywords Ping-pong protocol · Non-coherent attack · Eavesdropper's amount of information · Asymptotic security

1 Introduction

Nowadays the quantum cryptography is one of the rapidly developing applications of the quantum information theory. It offers a new based on the quantum physics' laws approach to the solving the important problem of telecommunication channels protection from eavesdropping by the non-authorised persons. One of the quantum cryptography directions is the quantum secure direct communication protocols [1–10, 12–16, 20–22, 24–30], where a confidential message coded in quantum states is transmitted by a quantum communication channel without preliminary enciphering.

One of the quantum secure direct communication protocol is the ping-pong protocol which can be realised with completely entangled states of pairs or groups of

E. V. Vasiliu (✉)
Odessa National Academy of Telecommunications named after O.S. Popov,
Koval'ska 1, 65029 Odessa, Ukraine
e-mail: vasiliu@ua.fm

qubits. Some variants of the ping-pong protocol with qubits are developed, and also their security against various attacks is investigated [1–8,14,20–22,29]. Usage instead of qubits the quantum systems with high dimension will allow increase of the source information capacity. So the protocol with completely entangled three-dimensional quantum systems (qutrits) and quantum superdense coding for qutrits have the capacity of $\log_2 9 = 3.17$ bits on a cycle instead of two bits on a cycle for the protocol with pairs of qubits. Notice that operating with qutrits is more difficult from the technological point of view than with qubits, however, a series of experiments on creation of entangled qutrit pairs is carried out in present time [11,19,23].

The quantum secure direct communication protocol with entangled pairs of qutrits, using the scheme of the ping-pong protocol, and also the transmission of qutrits by blocks has been offered by Wang et al. [25]. However, such protocol with qutrits transmitted by blocks requires great quantum memory from the both users. At the same time the original scheme of the ping-pong protocol requires quantum memory only for storage of one qubit (or qutrit) from the receiver of the message during one cycle of the protocol. Therefore, the ping-pong protocol is more convenient for practical use with today's technologies. On the other hand, ping-pong protocol with groups of entangled qubits in Bell and Greenberger–Horne–Zeilinger (GHZ) states possesses only asymptotic security against non-coherent attack [1,2,4,7,21,22,24]. For the protocol with qutrits such attack by this time is not analysed. In this work the analysis of non-coherent attack against the ping-pong protocol with entangled pairs of qutrits is carried out; also the comparison of security of this protocol with security of the protocols with qubits is made.

2 The ping-pong protocol with completely entangled pairs of qutrits

The ping-pong protocol with completely entangled qubit pairs, quantum superdense coding for qubits and two mutually unbiased bases for eavesdropping control, that are necessary while using of quantum superdense coding, has been offered by Cai and Li [4]. The scheme described below is a generalisation of this protocol on three-dimensional quantum systems.

There are nine completely entangled orthonormalized states of qutrit pair (three-dimensional Bell-basis states) [25]:

$$
\begin{aligned}
&|\Psi_{00}\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}; && |\Psi_{10}\rangle = (|00\rangle + e^{2\pi i/3}|11\rangle \\
& && \quad +e^{4\pi i/3}|22\rangle)/\sqrt{3}; \\
&|\Psi_{20}\rangle = (|00\rangle + e^{4\pi i/3}|11\rangle + e^{2\pi i/3}|22\rangle)/\sqrt{3}; && |\Psi_{01}\rangle = (|01\rangle + |12\rangle \\
& && \quad +|20\rangle)/\sqrt{3}; \\
&|\Psi_{11}\rangle = \left(|01\rangle + e^{2\pi i/3}\,|12\rangle + e^{4\pi i/3}\,|20\rangle\right)/\sqrt{3}; && |\Psi_{21}\rangle = (|01\rangle + e^{4\pi i/3}|12\rangle \\
& && \quad +e^{2\pi i/3}|20\rangle)/\sqrt{3}; \\
&|\Psi_{02}\rangle = (|02\rangle + |10\rangle + |21\rangle)/\sqrt{3}; && |\Psi_{12}\rangle = (|02\rangle + e^{2\pi i/3}|10\rangle \\
& && \quad +e^{4\pi i/3}|21\rangle)/\sqrt{3}; \\
&|\Psi_{22}\rangle = \left(|02\rangle + e^{4\pi i/3}\,|10\rangle + e^{2\pi i/3}\,|21\rangle\right)/\sqrt{3}.
\end{aligned}
\tag{1}
$$

These states can be transformed one into another by the action of local unitary operations on one of qutrits from pair [25]. Thus, there is a possibility to realise quantum superdense coding for pair of qutrits, i.e. transmitting by a quantum communication channel only one qutrit from pair pass two classical trit of information.

The receiver (Bob) prepares one of two-qutrit states (1), e.g. the state $|\Psi_{00}\rangle$, and then sends one of qutrits to the sender (Alice). Let Bob stores the first qutrit, "home" qutrit and sends the second, the "travel" qutrit.

Alice performs one of the nine coding operations on the received qutrit, according to pair classical trits (ternary bigram) which she wishes to send. E.g., the state $|\Psi_{00}\rangle$ corresponds to "00", $|\Psi_{10}\rangle$ corresponds to "10", $|\Psi_{20}\rangle$ corresponds to "20" etc. Alice and Bob agree about such conformity in advance. Then Alice sends the travel qutrit back to Bob, and he performs a Bell-basis measurement on both qutrits, representing a set from nine operators $\{|\Psi_{ij}\rangle\langle\Psi_{ij}|\}$, where $i, j = 0 \ldots 2$. Bob precisely defines states created by Alice's coding operation, and, accordingly, ternary bigram, which she has sent. The described sequence of operations is called a message mode.

Alice's coding operations, that transform state $|\Psi_{00}\rangle$ into states $|\Psi_{00}\rangle \ldots |\Psi_{22}\rangle$, are given by:

$$
\begin{aligned}
&U_{00} = |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|; && U_{10} = |0\rangle\langle 0| + e^{2\pi i/3}|1\rangle\langle 1| \\
& && \quad + e^{4\pi i/3}|2\rangle\langle 2|; \\
&U_{20} = |0\rangle\langle 0| + e^{4\pi i/3}|1\rangle\langle 1| + e^{2\pi i/3}|2\rangle\langle 2|; && U_{01} = |1\rangle\langle 0| + |2\rangle\langle 1| + |0\rangle\langle 2|; \\
&U_{11} = |1\rangle\langle 0| + e^{2\pi i/3}|2\rangle\langle 1| + e^{4\pi i/3}|0\rangle\langle 2|; && U_{21} = |1\rangle\langle 0| + e^{4\pi i/3}|2\rangle\langle 1| \\
& && \quad + e^{2\pi i/3}|0\rangle\langle 2|; \\
&U_{02} = |2\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 2|; && U_{12} = |2\rangle\langle 0| + e^{2\pi i/3}|0\rangle\langle 1| \\
& && \quad + e^{4\pi i/3}|1\rangle\langle 2|; \\
&U_{22} = |2\rangle\langle 0| + e^{4\pi i/3}|0\rangle\langle 1| + e^{2\pi i/3}|1\rangle\langle 2|.
\end{aligned}
\tag{2}
$$

As the eavesdropper (Eve) has no access to home qutrit, stored in Bob quantum memory during one cycle of the protocol, she cannot gain any information having simply intercepted travel qutrit on the way Alice $\rightarrow$ Bob and having measured its state. The state of travel qutrit is completely mixed; its reduced density matrix is $\rho_{red} = (|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|)/3$. However, Eve has the possibility to perform an attack with the additional quantum systems (ancillas) entangled with travel qutrit on the way Bob $\rightarrow$ Alice (Fig. 1). Then Eve performs measurement on the composite quantum system "travel qutrit—ancilla" on the way Alice $\rightarrow$ Bob. Therefore, except the message mode the ping-pong protocol also requires the control mode, which allows detecting of eavesdropper's operation.

Alice randomly switches to control mode with some probability q. In this mode Alice does not perform coding operations (2), but randomly chooses one of two mutually unbiased measuring bases and measures state of the travel qutrit in this basis. Then Alice informs Bob via public classical channel about a result of measurement and the chosen basis.

There are four mutually unbiased bases for qutrits from which two are called z-basis and x-basis [25], and other two we will designate as v-basis and t-basis:

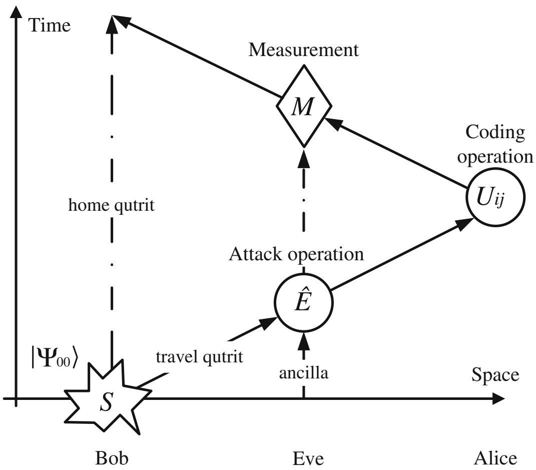

Fig. 1 The attack scheme on the ping-pong protocol with pairs of qutrits; S is a source of entangled qutrit pairs

$$|z_0\rangle = |0\rangle\,, \quad |z_1\rangle = |1\rangle\,, \quad |z_2\rangle = |2\rangle\,; \tag{3}$$

$$\begin{aligned} |x_0\rangle &= (|0\rangle + |1\rangle + |2\rangle)\big/\sqrt{3}, \\ |x_1\rangle &= \Big(|0\rangle + e^{2\pi i/3}\,|1\rangle + e^{-2\pi i/3}\,|2\rangle\Big)\Big/\sqrt{3}, \\ |x_2\rangle &= \Big(|0\rangle + e^{-2\pi i/3}\,|1\rangle + e^{2\pi i/3}\,|2\rangle\Big)\Big/\sqrt{3}; \end{aligned} \tag{4}$$

$$\begin{aligned} |v_0\rangle &= \Big(e^{2\pi i/3}\,|0\rangle + |1\rangle + |2\rangle\Big)\Big/\sqrt{3}, \\ |v_1\rangle &= \Big(|0\rangle + e^{2\pi i/3}\,|1\rangle + |2\rangle\Big)\Big/\sqrt{3}, \\ |v_2\rangle &= \Big(|0\rangle + |1\rangle + e^{2\pi i/3}\,|2\rangle\Big)\Big/\sqrt{3}; \end{aligned} \tag{5}$$

$$\begin{aligned} |t_0\rangle &= \Big(e^{-2\pi i/3}\,|0\rangle + |1\rangle + |2\rangle\Big)\Big/\sqrt{3}; \\ |t_1\rangle &= \Big(|0\rangle + e^{-2\pi i/3}\,|1\rangle + |2\rangle\Big)\Big/\sqrt{3}; \\ |t_2\rangle &= \Big(|0\rangle + |1\rangle + e^{-2\pi i/3}\,|2\rangle\Big)\Big/\sqrt{3}. \end{aligned} \tag{6}$$

Measurement in any of these bases gives one of three possible results: “0”, “1” or “2”, each with probability equal to 1/3. Having received from Alice the result of measurement and the chosen basis, Bob performs measurement of home qutrit state. Thus Bob should choose measuring basis according to the rules which follow from the form of $|\Psi_{00}\rangle$ in all four bases (3)–(6):

$$\begin{aligned} |\Psi_{00}\rangle &= (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3} = (|x_0x_0\rangle + |x_1x_2\rangle + |x_2x_1\rangle)/\sqrt{3} \\ &= (|t_0v_0\rangle + |t_1v_1\rangle + |t_2v_2\rangle)\,/\sqrt{3} = (|v_0t_0\rangle + |v_1t_1\rangle + |v_2t_2\rangle)/\sqrt{3}. \end{aligned} \tag{7}$$

This expression is derived by direct calculation of projective operators' actions in bases (4)–(6) on the state $|\Psi_{00}\rangle$, which has been written in computational basis (3), i.e. $|\Psi_{00}\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$.

Bob measurement rules follow from the formula (7). So if Alice has chosen z-basis and drawn the result "0" Bob should choose also z-basis and its result with determinacy will be "0". Similarly, if Alice result at measurement in z-basis is "1" or "2", then Bob also should draw "1" or "2" in this basis accordingly. If Alice has chosen x-basis, so Bob should choose this basis. At Alice results are "0", "1" or "2" (corresponding to the states $|x_0\rangle$, $|x_1\rangle$ and $|x_2\rangle$) Bob with determinacy will draw "0", "2" or "1" accordingly.

If Bob results differ from above, this means that the state $|\Psi_{00}\rangle$ is changed by the transmission of qutrit from Bob to Alice. It can be caused by two reasons: Eve's attack or noise in a quantum communication channel. In this paper the implementation of the ping-pong protocol with entangled qutrits in noise channel had not been considered. It was assumed that legitimate users communicate via the ideal quantum channel. In that case the discrepancy of Bob's measurement result to the expected means Eve's attack and legitimate users should immediately interrupt a communication session. However, for the ping-pong protocol with groups of entangled qubits Eve's attack does not lead to the situation that Alice and Bob will find out the change of the state prepared by Bob at the first control mode. In protocols with qubits Eve's attacking operation is detected only for one round of the control mode with some probability and legitimate users should perform a certain quantity of rounds to make probability of attack detection closer to unit [1,4,7,21,24]. For the ping-pong protocol with entangled pairs of qutrits the situation will be the same. One can obtain a concrete number of control mode rounds which are necessary for attack detection with the given probability by analysis of the Eve's eavesdropping attack. Results of such analysis are presented in the following section of the paper.

3 Non-coherent attack using quantum ancillas against the ping-pong protocol with entangled pairs of qutrits

According to the scheme of the ping-pong protocol Alice informs Bob via the public channel on switching to control mode after reception of travel qutrit from Bob. Eve listening in this channel learns about switching to control mode after attacking operation $\hat{E}$, but before its final measurement (see Fig. 1). Hence, in this case Eve will not perform the measurement. Thus, legitimate users can detect only an attacking operation $\hat{E}$ on a Bob $\rightarrow$ Alice line.

Due to the Stinespring dilation theorem [18] Eve's attacking operation $\hat{E}$ can be realised by an unitary operator on a Hilbert space of ancillas H_E which dimension satisfies the condition $\dim H_E \leq (\dim H_B)^2$, where $\dim H_B = 3$ is the dimension of Hilbert space of travel qutrit. Thus, Eve can use for attack the ancillas consisting of one or two qutrits. Attack using two-qutrits ancillas is more general and accordingly powerful, therefore we will analyse this attack.

As for Eva the state of travel qutrit is indistinguishable from the complete mixture, it is possible to replace this state by the a priori mixture, which corresponds to the situation when Bob sends qutrit in one of the states $|0\rangle$, $|1\rangle$ or $|2\rangle$ with identical probability equal to $1/3$. The security analysis for the ping-pong protocol with qubits is carried out in the same way [1,7,21]. Let's notice that as legitimate users in a control mode should use two bases, e.g., z- and x-basis, it is possible to consider also, that Bob sends qutrit in one of the states $|x_0\rangle$, $|x_1\rangle$ or $|x_2\rangle$ (4). Let's examine at first a z-basis case.

States of composite system "travel qutrit–Eve's ancilla" after an attack $\hat{E}$ can be written as

$$\begin{aligned}\left|\psi^{(0)}\right\rangle &= \hat{E}\,|0,\varphi\rangle = \alpha_0\,|0,\varphi_{00}\rangle + \beta_0\,|1,\varphi_{01}\rangle + \gamma_0\,|2,\varphi_{02}\rangle\,,\\ \left|\psi^{(1)}\right\rangle &= \hat{E}\,|1,\varphi\rangle = \alpha_1\,|0,\varphi_{10}\rangle + \beta_1\,|1,\varphi_{11}\rangle + \gamma_1\,|2,\varphi_{12}\rangle\,,\\ \left|\psi^{(2)}\right\rangle &= \hat{E}\,|2,\varphi\rangle = \alpha_2\,|0,\varphi_{20}\rangle + \beta_2\,|1,\varphi_{21}\rangle + \gamma_2\,|2,\varphi_{22}\rangle\,,\end{aligned} \tag{8}$$

where $\left\{\left|\varphi_{ij}\right\rangle\right\}$ $(i, j = 0\ldots 2)$ is set of two-qutrit states of Eve's ancilla.

Matrix representation of Eve's attacking operation is:

$$\hat{E} = \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \\ \gamma_0 & \gamma_1 & \gamma_2 \end{bmatrix} \tag{9}$$

Since $\hat{E}$ has to be unitary the following relations between parameters of Eve's ancillas had to be fulfilled:

$$\alpha_i^*\alpha_j + \beta_i^*\beta_j + \gamma_i^*\gamma_j = \delta_{ij}, \tag{10}$$

where δ_{ij} is Kronecker delta, $i, j = 0\ldots 2$.

Also for the reason that a state of travel qutrit is completely mixed the following relations had to be fulfilled:

$$|\alpha_0|^2 = |\beta_1|^2 = |\gamma_2|^2\,; \quad |\alpha_1|^2 = |\beta_2|^2 = |\gamma_0|^2\,; \quad |\alpha_2|^2 = |\beta_0|^2 = |\gamma_1|^2\,. \tag{11}$$

Let's consider at first the case when Bob "sends $|0\rangle$". In this case the state of system "travel qutrit–Eve's ancilla" after attack $\hat{E}$ becomes $\left|\psi^{(0)}\right\rangle$ (see (8)).

After the performance (by Alice) of coding operations $U_{00}, U_{10}, U_{20}, U_{01}, \ldots$ (2) with probabilities $p_{00}, p_{10}, p_{20}, p_{01}, \ldots$ respectively, the density operator of system "travel qutrit–Eve's ancilla" will look like:

$$\rho^{(0)} = \sum_{i,j=0}^{2} p_{ij}\left|\psi_{ij}^{(0)}\right\rangle\left\langle\psi_{ij}^{(0)}\right|, \tag{12}$$

where

$$\left|\psi_{00}^{(0)}\right\rangle = U_{00}\left|\psi^{(0)}\right\rangle = \alpha_0\,|0,\varphi_{00}\rangle + \beta_0\,|1,\varphi_{01}\rangle + \gamma_0\,|2,\varphi_{02}\rangle\,,$$

$$\begin{aligned}
\left|\psi_{10}^{(0)}\right\rangle &= U_{10}\left|\psi^{(0)}\right\rangle = \alpha_0\left|0,\varphi_{00}\right\rangle + \beta_0 e^{2\pi i/3}\left|1,\varphi_{01}\right\rangle + \gamma_0 e^{4\pi i/3}\left|2,\varphi_{02}\right\rangle,\\
\left|\psi_{20}^{(0)}\right\rangle &= U_{20}\left|\psi^{(0)}\right\rangle = \alpha_0\left|0,\varphi_{00}\right\rangle + \beta_0 e^{4\pi i/3}\left|1,\varphi_{01}\right\rangle + \gamma_0 e^{2\pi i/3}\left|2,\varphi_{02}\right\rangle,\\
\left|\psi_{01}^{(0)}\right\rangle &= U_{20}\left|\psi^{(0)}\right\rangle = \alpha_0\left|1,\varphi_{00}\right\rangle + \beta_0\left|2,\varphi_{01}\right\rangle + \gamma_0\left|0,\varphi_{02}\right\rangle,\\
\left|\psi_{11}^{(0)}\right\rangle &= U_{11}\left|\psi^{(0)}\right\rangle = \alpha_0\left|1,\varphi_{00}\right\rangle + \beta_0 e^{2\pi i/3}\left|2,\varphi_{01}\right\rangle + \gamma_0 e^{4\pi i/3}\left|0,\varphi_{02}\right\rangle,\\
\left|\psi_{21}^{(0)}\right\rangle &= U_{21}\left|\psi^{(0)}\right\rangle = \alpha_0\left|1,\varphi_{00}\right\rangle + \beta_0 e^{4\pi i/3}\left|2,\varphi_{01}\right\rangle + \gamma_0 e^{2\pi i/3}\left|0,\varphi_{02}\right\rangle,\\
\left|\psi_{02}^{(0)}\right\rangle &= U_{02}\left|\psi^{(0)}\right\rangle = \alpha_0\left|2,\varphi_{00}\right\rangle + \beta_0\left|0,\varphi_{01}\right\rangle + \gamma_0\left|1,\varphi_{02}\right\rangle,\\
\left|\psi_{12}^{(0)}\right\rangle &= U_{12}\left|\psi^{(0)}\right\rangle = \alpha_0\left|2,\varphi_{00}\right\rangle + \beta_0 e^{2\pi i/3}\left|0,\varphi_{01}\right\rangle + \gamma_0 e^{4\pi i/3}\left|1,\varphi_{02}\right\rangle,\\
\left|\psi_{22}^{(0)}\right\rangle &= U_{12}\left|\psi^{(0)}\right\rangle = \alpha_0\left|2,\varphi_{00}\right\rangle + \beta_0 e^{4\pi i/3}\left|0,\varphi_{01}\right\rangle + \gamma_0 e^{2\pi i/3}\left|1,\varphi_{02}\right\rangle.
\end{aligned} \tag{13}$$

The maximal amount I_0 of classical information which is accessible to Eve after measurement on composite system "travel qutrit–ancilla" is bounded by the Holevo quantity [17]:

$$I_0 = S\left(\rho^{(0)}\right) - \sum_{i,j=0}^{2} p_{ij} S\left(\rho_{ij}^{(0)}\right) = S\left(\rho^{(0)}\right), \tag{14}$$

where $\rho_{ij}^{(0)} = \left|\psi_{ij}^{(0)}\right\rangle\left\langle\psi_{ij}^{(0)}\right|$; S is von Neumann entropy and all $S\left(\rho_{ij}^{(0)}\right)$ are equal to zero. Thus,

$$I_0 = S\left(\rho^{(0)}\right) \equiv -Tr\left\{\rho^{(0)}\log_3\rho^{(0)}\right\} = -\sum_i \lambda_i \log_3 \lambda_i (trit), \tag{15}$$

where λ_i are eigenvalues of the density operator $\rho^{(0)}$ (12).

The quantity of I_0 shows how much information Eve can gain after the final measurement on a composite system "travel qutrit–ancilla".

For finding of eigenvalues λ_i density operator $\rho^{(0)}$ (12) has been written in a matrix kind in the following orthogonal basis:

$$\begin{aligned}
&\{\left|0,\varphi_{00}\right\rangle, \left|1,\varphi_{00}\right\rangle, \left|2,\varphi_{00}\right\rangle, \left|0,\varphi_{01}\right\rangle, \left|1,\varphi_{01}\right\rangle, \left|2,\varphi_{01}\right\rangle, \left|0,\varphi_{02}\right\rangle,\\
&\left|1,\varphi_{02}\right\rangle, \left|2,\varphi_{02}\right\rangle\}.
\end{aligned} \tag{16}$$

The deduced matrix has the size of 9×9 and here is not shown so the resultant expression is cumbersome.

It has been found, that the equation of ninth power on eigenvalues for this density matrix can be factorized to three cubic equations of a following kind:

$$
\begin{aligned}
&\lambda^3 - (p_{00} + p_{10} + p_{20})\,\lambda^2 + 3\left(|\alpha_0|^2|\beta_0|^2 + |\alpha_0|^2|\gamma_0|^2 + |\beta_0|^2|\gamma_0|^2\right)\\
&\quad \times (p_{00}p_{10} + p_{00}p_{20} + p_{10}p_{20})\,\lambda - 27\,|\alpha_0|^2|\beta_0|^2|\gamma_0|^2\,p_{00}p_{10}p_{20} = 0;\\
&\lambda^3 - (p_{01} + p_{11} + p_{21})\,\lambda^2 + 3\left(|\alpha_0|^2|\beta_0|^2 + |\alpha_0|^2|\gamma_0|^2 + |\beta_0|^2|\gamma_0|^2\right)\\
&\quad \times (p_{01}p_{11} + p_{01}p_{21} + p_{11}p_{21})\,\lambda - 27\,|\alpha_0|^2|\beta_0|^2|\gamma_0|^2\,p_{01}p_{11}p_{21} = 0;\\
&\lambda^3 - (p_{02} + p_{12} + p_{22})\,\lambda^2 + 3\left(|\alpha_0|^2|\beta_0|^2 + |\alpha_0|^2|\gamma_0|^2 + |\beta_0|^2|\gamma_0|^2\right)\\
&\quad \times (p_{02}p_{12} + p_{02}p_{22} + p_{12}p_{22})\,\lambda - 27\,|\alpha_0|^2|\beta_0|^2|\gamma_0|^2\,p_{02}p_{12}p_{22} = 0.
\end{aligned}
\tag{17}
$$

Other cases in (8) are similarly considered, i.e. when Bob instead of $|0\rangle$ "sends $|1\rangle$ or $|2\rangle$". In these cases the eigenvalues of the density matrix $\rho^{(1)}$ and $\rho^{(2)}$ taking into account relations (11) are defined by the same Eq. (17).

As it follows from the first expression in (8), in the case when Bob "sends $|0\rangle$" and in control mode the measurement basis z is used, probability to detect an attack is:

$$d_z = |\beta_0|^2 + |\gamma_0|^2 = 1 - |\alpha_0|^2\,. \tag{18}$$

Similarly, if Bob "sends $|1\rangle$ or $|2\rangle$" then

$$
\begin{aligned}
d_z &= |\alpha_1|^2 + |\gamma_1|^2 = 1 - |\beta_1|^2 = 1 - |\alpha_0|^2 \ \text{ and } d_z = |\alpha_2|^2 + |\beta_2|^2\\
&= 1 - |\gamma_2|^2 = 1 - |\alpha_0|^2
\end{aligned}
\tag{19}
$$

accordingly, taking into account relations (11). Thus, the general expression for probability of attack detection using z-basis in a control mode is defined by (18).

Using the expression (18) from the Eq. (17) it is possible for a case of Eve's *symmetric* attack ($|\beta_0|^2 = |\gamma_0|^2 = d_z/2$) to exclude parameters α_0, β_0 and γ_0 of ancillas having entered in the Eq. (17) probability of an attack detection d_z. It will finally allow to express Eve's amount of information I_0 (15) through d_z.

As at symmetric attack $|\alpha_0|^2|\beta_0|^2 = |\alpha_0|^2|\gamma_0|^2 = (1 - d_z)\,d_z/2$, $|\beta_0|^2|\gamma_0|^2 = d_z^2/4$ and $|\alpha_0|^2|\beta_0|^2|\gamma_0|^2 = (1 - d_z)\,d_z^2/4$ the Eq. (17) become:

$$
\begin{aligned}
&\lambda^3 - (p_{00} + p_{10} + p_{20})\,\lambda^2 + 3\left(d_z - \frac{3}{4}d_z^2\right)(p_{00}p_{10} + p_{00}p_{20} + p_{10}p_{20})\,\lambda\\
&\quad -\frac{27}{4}\left(d_z^2 - d_z^3\right)p_{00}p_{10}p_{20} = 0;\\
&\lambda^3 - (p_{01} + p_{11} + p_{21})\,\lambda^2 + 3\left(d_z - \frac{3}{4}d_z^2\right)(p_{01}p_{11} + p_{01}p_{21} + p_{11}p_{21})\,\lambda\\
&\quad -\frac{27}{4}\left(d_z^2 - d_z^3\right)p_{01}p_{11}p_{21} = 0;\\
&\lambda^3 - (p_{02} + p_{12} + p_{22})\,\lambda^2 + 3\left(d_z - \frac{3}{4}d_z^2\right)(p_{02}p_{12} + p_{02}p_{22} + p_{12}p_{22})\,\lambda\\
&\quad -\frac{27}{4}\left(d_z^2 - d_z^3\right)p_{02}p_{12}p_{22} = 0.
\end{aligned}
\tag{20}
$$

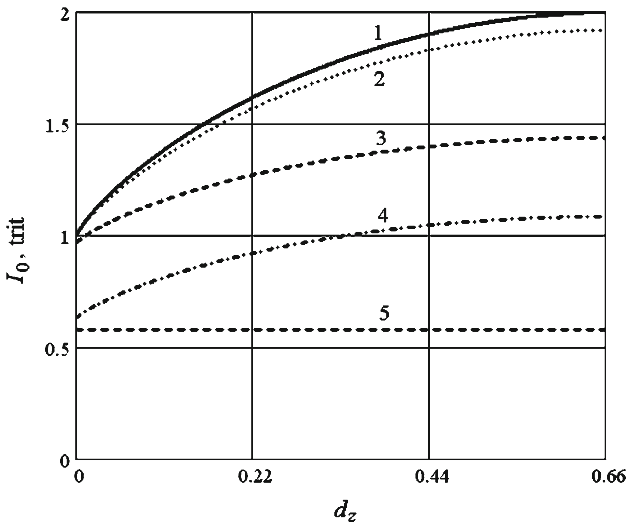

Fig. 2 Dependences of Eve's amount of information I_0 from probability d_z of attack detection

Table 1 Probabilities $p_{00}\ldots p_{22}$ of ternary bigram and corresponding entropy $H = -\sum_{i,j=0}^{2} p_{ij} \log_3 p_{ij}$ of a message source (trit/bigram)

Number of curve on Fig. 2	p_{00}	p_{10}	p_{20}	p_{01}	p_{11}	p_{21}	p_{02}	p_{12}	p_{22}	H
1	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	2.000
2	1/6	1/9	1/18	1/6	1/18	1/9	1/18	1/9	1/6	1.921
3	2/9	0	2/9	0	2/9	0	2/9	0	1/9	1.439
4	0.4	0.1	0	0	0.4	0.1	0	0	0	1.086
5	2/3	0	0	0	1/3	0	0	0	0	0.579

In the Fig. 2 dependences of I_0 from d_z are shown at Eve's symmetric attack and various values of probabilities $p_{00}\ldots p_{22}$ of Alice's coding operations (Table 1). For acquisition of these dependences the Eq. (20) were solved numerically at some values of $p_{00}\ldots p_{22}$ and the obtained nine values $\lambda_1\ldots\lambda_9$ were substituted in the Eq. (15).

As it can be seen from the Fig. 2, for the majority of sets $p_{00}\ldots p_{22}$ amount of Eve's information I_0 monotonously grows with increase of attack detection probability d_z and reaches a maximum at $d_z = 2/3$ (for some special sets of bigram probabilities the I_0 does not depend on d_z at all and is a constant). It is possible to consider the value $d_z = 2/3$ as a maximum so at $d_z > 2/3$ amount of Eve's information starts to decrease (it is not shown in Fig. 2). Accordingly, Eve will not choose parameters of the ancillas on which the d_z depends so that d_z would exceed 2/3, since for her does not make sense to increase probability of attack detection at reduction of information accessible for her. Also as it is visible from the Fig. 2 that a maximum of Eve's amount of information corresponding to $d_z = 2/3$ is equal to entropy of a message source at any sets of probabilities $p_{00}\ldots p_{22}$. It means that at $d_z = 2/3$ and only at such value of d_z Eve have the full information. Also the fact that I_0 is equal to H at $d_z = 2/3$ testifies about correct asymptotics of (20).

Let's discuss now Eve's attack considering that owing to full mixing of a travel qutrit state this qutrit is now in one of the states$|x_0\rangle$, $|x_1\rangle$ or $|x_2\rangle$ (4). Then formulas (8) are replaced with the following:

$$\begin{aligned} \left|\psi_x^{(0)}\right\rangle &= \hat{E}\,|x_0, \varphi\rangle = a_0\,|x_0, \varphi_{00}\rangle + b_0\,|x_1, \varphi_{01}\rangle + c_0\,|x_2, \varphi_{02}\rangle\,; \\ \left|\psi_x^{(1)}\right\rangle &= \hat{E}\,|x_1, \varphi\rangle = a_1\,|x_0, \varphi_{10}\rangle + b_1\,|x_1, \varphi_{11}\rangle + c_1\,|x_2, \varphi_{12}\rangle\,; \\ \left|\psi_x^{(2)}\right\rangle &= \hat{E}\,|x_2, \varphi\rangle = a_2\,|x_0, \varphi_{20}\rangle + b_2\,|x_1, \varphi_{21}\rangle + c_2\,|x_2, \varphi_{22}\rangle\,. \end{aligned} \tag{21}$$

Further, all formulas (9)–(17) remain correct after replacement $\alpha_0 \to a_0, \beta_0 \to b_0, \gamma_0 \to c_0, \alpha_1 \to a_1, \beta_1 \to b_1$ etc. Thus, expression (18) is replaced with an expression:

$$d_x = |b_0|^2 + |c_0|^2 = 1 - |a_0|^2\,. \tag{22}$$

Using (8) and (21) it is possible to derive the following expressions connecting parameters α_0, β_0 and γ_0 with parameters a_0, b_0 and c_0:

$$\begin{aligned} &|\alpha_0|^2 = \frac{1}{3}\,|a_0 + b_0 + c_0|^2\,,\ |\beta_0|^2 = \frac{1}{3}\left|a_0 + e^{2\pi i/3} b_0 + e^{-2\pi i/3} c_0\right|^2, \\ &|\gamma_0|^2 = \frac{1}{3}\left|a_0 + e^{-2\pi i/3} b_0 + e^{2\pi i/3} c_0\right|^2. \end{aligned} \tag{23}$$

In the Table 2 some calculated sets of parameters a_0, b_0 and c_0 satisfying the relations similar to (10) and (11), and also values of d_x and d_z corresponded to these parameter sets are presented. Values of d_z are obtained with the use of (18) and the first formula in (23).

The unitarity of Eve's attacking operation leads to the important dependence between d_z and d_x, namely: the second is always equal to the maximum value without dependence from value of one of these quantities.

While using in control mode of two measuring bases (e.g., z and x) the probability to detect Eve's attacking operation is

$$d = q_z d_z + q_x d_x, \tag{24}$$

where q_z and q_x are probabilities of use by Alice and Bob z- and x-bases accordingly ($q_z + q_x = 1$). The least values of d_z and d_x are equal to zero but when one of these quantities is equal to zero, another is equal to maximum value of 2/3. As legitimate users do not foreknow what attack strategy will be chosen by Eve, i.e. in what bases she will desire to create a smaller value of detection probability, values of q_z and q_x will be reasonable for choice when they equal to each other, i.e. $q_z = q_x = 1/2$. Then the least value of d will turn out, when or $d_z = 0$ and $d_x = 2/3$, or on the contrary.

Table 2 Parameters of attacking operation and corresponding to them values of d_x and d_z

a_0	b_0	c_0	d_x	d_z
Unsymmetrical attack: $\|b_0\|^2 \neq \|c_0\|^2$				
−0.910684	0.244017	−0.333333	0.170655	0.666667
−0.807162	0.309719	−0.502558	0.348490	0.666667
−0.709081	0.331451	−0.622370	0.497204	0.666667
−0.666667	0.333333	−0.666667	0.555556	0.666667
0.530210 − 0.8i	0.169304 − 0.1i	0.014630 + 0.2i	0.078878	0.666667
−0.909127 + 0.1i	−0.133042 − 0.2i	0.125653 − 0.3i	0.163489	0.666667
0.737034 + 0.3i	−0.031581 − 0.5i	0.160573 − 0.3i	0.366781	0.666667
0.674712 + 0.3i	0.525520 + 0.2i	−0.220436 − 0.3i	0.454764	0.666667
−0.531662 + 0.3i	0.463325 + 0.2i	−0.531662 + 0.3i	0.627335	0.666667
−0.497557 + 0.293i	0.459068 + 0.2i	−0.570890 + 0.3i	0.666667	0.666667
Symmetrical attack: $\|b_0\|^2 = \|c_0\|^2$				
−0.953939 + 0.1i	−0.2i	−0.2i	0.08	0.666667
0.305505 + 0.8i	0.305505 − 0.2i	0.305505 − 0.2i	0.266667	0.666667
0.027387 + 0.7i	0.463276 − 0.2i	0.463276 − 0.2i	0.50925	0.666667
0.577350	−0.288675 + 0.5i	−0.288675 + 0.5i	0.666667	0.666667
0.577350i	0.5 − 0.288675i	0.5 − 0.288675i	0.666667	0.666667
0.577350	0.288675 + 0.5i	0.288675 + 0.5i	0.666667	0.222222

According to (24) under such circumstances $d = (1/2) \cdot (2/3) = 1/3$, i.e. the minimum value of attack detection probability at use in control mode two measuring bases equals to 1/3. Notice, that at such strategy Eve will obtain only partial information about the transmitted string of trits. If Eve wants to obtain full information it should choose parameters of ancillas so that $d_z = d_x = 2/3$ and thus, according to (24), $d = 2/3$.

4 Comparison of security level of protocols with qutrits and with qubits

Let's now compare dependences of Eve's amount of information on probability of attack detection for protocol with Bell pairs of qutrits and protocols with groups of qubits. In Fig. 3 dependences I_0 from d_z for protocol with pairs of qutrits are shown at $p_{00} = \cdots = p_{22} = 1/9$, and also for protocol with pairs of qubits and quantum superdense coding [7], protocol with GHZ–triplets [21] and protocol with GHZ–quadruples of qubits [22] at identical values of probabilities of Alice's coding operations. It can be seen, that the curve $I_0\,(d_z)$ for the protocol with qutrits lays close to corresponding curve for the protocol with GHZ–triplets of qubits. Also information capacities of these two variants of the ping-pong protocol are also close: 3.17 bits on a cycle for protocol with pairs of qutrits and 3 bits on a cycle for protocol with GHZ–triplets of qubits.

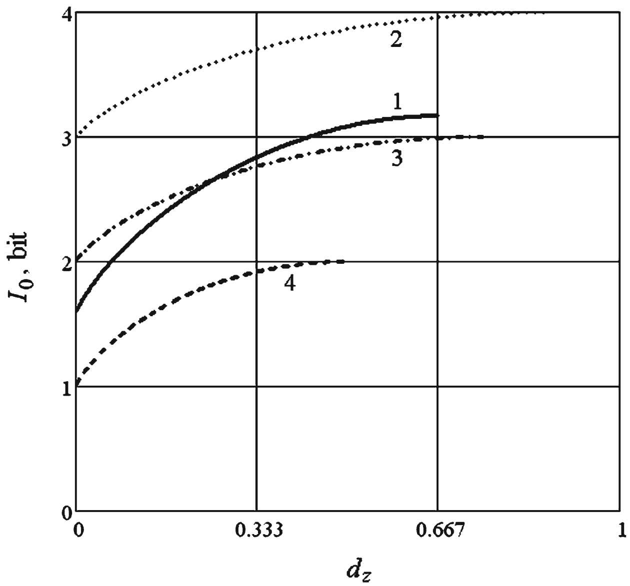

Fig. 3 Dependences of Eve's amount of information on probability of attack detection. The ping-pong protocol: with Bell pairs of qutrits (*1*); with GHZ-quadruples of qubits (*2*); with GHZ-triplets of qubits (*3*); with Bell pairs of qubits (*4*)

Table 3 Minimum d_{min} and maximum d_{max} values of attack's detection probability using in control mode of two measuring bases with equal probabilities

Protocol	d_{min}	d_{max}
With Bell pairs of qutrits	1/3	2/3
With Bell pairs of qubits	1/4	1/2
With GHZ–triplets of qubits	3/8	3/4
With GHZ–quadruples of qubits	7/16	7/8

In the Table 3 the minimum and maximum values of attack detection probability for these four variants of the ping-pong protocol are shown at use in control mode two measuring bases with the same probabilities $q_z = q_x = 1/2$.

5 Conclusions

In this work a non-coherent attack on the ping-pong protocol with Bell pairs of three-dimensional quantum systems is analysed. The density matrix of composite quantum system "travel qutrit–eavesdropper's ancilla" is obtained and after calculation of density matrix eigenvalues the expression is obtained for amount of eavesdropper's information as attack's detection probability functions.

It is shown, that at use for protocol implementation Bell pairs of qutrits instead of Bell pairs of qubits not only information capacity increases, but also the security level of protocol to attack, as the maximum probability of eavesdropping detection (at the one-time run of control mode) for protocol with qutrits is equal to 2/3, and for protocol with qubits is equal to 1/2. Security of the protocol with pairs of qutrits appears approximately the same, as the protocol with GHZ–triplets of qubits.

At use in control mode two measuring bases the ping-pong protocol with Bell pairs of qutrits possesses only *asymptotic* security as for detection of eavesdropping with the probability as close to unit, it is necessary for legitimate users to perform a certain quantity of control mode rounds. Thus, as the control mode is necessary for alternating with the message mode (otherwise the eavesdropper will not make attacking operations at all as he will know that the message is not transmitted) some amount of information will leak to the eavesdropper. An estimation of this amount depends on parameters of protocol and eavesdropping strategy, and also necessary arrangements on security amplification of the ping-pong protocol with qutrits will be a subject of the further researches.

References

1. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
2. Boström, K., Felbinger, T.: On the security of the ping-pong protocol. Phys. Lett. A **372**(22), 3953–3956 (2008)
3. Cai, Q.Y.: The “ping-pong” protocol can be attacked without eavesdropping. Phys. Rev. Lett. **91**(10), 109801 (2003)
4. Cai, Q.Y., Li, B.W.: Improving the capacity of the Boström-Felbinger protocol. Phys. Rev. A **69**(5), 054301 (2004)
5. Cai, Q.Y., Li, B.W.: Deterministic secure communication without using entanglement. Chin. Phys. Lett. **21**(4), 601–603 (2004)
6. Chamoli, A., Bhandari, C.M.: Secure direct communication based on ping-pong protocol. Quantum Inf. Process. **8**(4), 347–356 (2009)
7. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**(4), 042317 (2003)
8. Deng, F.G., Long, G.L.: Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys. Rev. A **70**(1), 012311 (2004)
9. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**(5), 052319 (2004)
10. Gao, T., Yan, F.L., Wang, Z.X.: Deterministic secure direct communication using GHZ–states and swapping quantum entanglement. J. Phys. A Math. Theor. **38**(25), 5761–5770 (2005)
11. Joo, J., Rudolph, T., Sanders, B.C.: A heralded two-qutrit entangled state. J. Phys. B At. Mol. Opt. Phys. **42**(11), 114007 (2009)
12. Lee, H., Lim, J., Yang, H.: Quantum direct communication with authentication. Phys. Rev. A **73**(4), 042305 (2006)
13. Li, X.H., Deng, F.G., Li, C.Y., et al.: Deterministic secure quantum communication without maximally entangled states. J. Korean Phys. Soc. **49**(4), 1354–1359 (2006)
14. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A **74**(5), 054302 (2006)
15. Li, X.H., Li, C.Y., Deng, F.G., et al.: Quantum secure direct communication with quantum encryption based on pure entangled states. Chin. Phys. **16**(8), 2149–2153 (2007)
16. Lin, S., Wen, Q.Y., Gao, F., Zhu, F.C.: Quantum secure direct communication with chi-type entangled states. Phys. Rev. A **78**(6), 064304 (2008)
17. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
18. Stinespring, W.F.: Positive functions on C*-algebras. In: Proceedings of the American Mathematical Society, vol. 6, pp. 211–216 (1955)
19. Thew, R., Acin, A., Zbinden, H., Gisin, N.: Experimental realization of entangled qutrits for quantum communication. Quantum Inf. Comput. **4**(2), 093–101 (2004)

20. Vasiliu, E.V., Vasiliu, L.N.: Ping-pong protocol with three- and four-qubit Greenberger–Horne–Zeilinger states. Work. Odessa Polytech. Univ. **1**(29), 171–176 (2008) (in Russian) http://nbuv.gov.ua/portal/natural/Popu/2008_1/3-4.pdf
21. Vasiliu, E.V.: Asymptotic security of the ping-pong quantum direct communication protocol with three-qubit Greenberger–Horne–Zeilinger states. Georgian Elec. Sci. J. Comput. Sci. Telecomm. **3**, 3–15 (2009) (in Russian) http://gesj.internet-academy.org.ge/gesj_articles/1427.pdf
22. Vasiliu, E.V., Nikolaenko, S.V.: Synthesis of the secure system of direct messages transfer based on the ping-pong protocol of quantum communication. Sci. Work. Odessa Natl. Acad. Telecomm. **1**, 83–91 (2009) (in Russian) http://sbornik.onat.edu.ua/?art=338
23. Vaziri, A., Pan, J., Jennewein, T., Weihs, G., Zeilinger, A.: Concentration of higher dimensional entanglement: Qutrits of photon orbital angular momentum. Phys. Rev. Lett. **91**(22), 227902 (2003)
24. Wang, Ch, Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multi-particle Greenberger–Horne–Zeilinger state. Opt. Communic. **253**(1), 15–20 (2005)
25. Wang, Ch, Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high dimension quantum superdense coding. Phys. Rev. A **71**(4), 044305 (2005)
26. Wang, J., Zhang, Q., Tang, C.J.: Multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state. Opt. Communic. **266**(2), 732–737 (2006)
27. Yan, F.L., Zhang, X.Q.: A scheme for secure direct communication using EPR pairs and teleportation. Eur. Phys. J. B **41**(1), 75–78 (2004)
28. Yen, C.A., Horng, S.J., Goan, H.S., et al.: Quantum direct communication with mutual authentication. Quantum Inf. Comput. **9**(5–6), 0376–0394 (2009)
29. Zhang Zh, J., Li, Y., Man Zh, X.: Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss. Phys. Lett. A **341**(5–6), 385–389 (2005)
30. Zhu, A.D., Xia, Y., Fan, Q.B., Zhang, S.: Secure direct communication based on secret transmitting order of particles. Phys. Rev. A **73**(2), 022338 (2006)