Unselected quantum information as an effective tool for quantum cryptography

Denis V. Sych, Boris A. Grishanin, and Victor N. Zadkov

International Laser Center and Faculty of Physics, M.V.Lomonosov Moscow State University, Moscow 119899, Russia

ABSTRACT

A novel quantum key distribution (QKD) protocol, based on all unselected states of a quantum system, which set the alphabet with continuous set of letters, is proposed. Employing all states of the Hilbert space leads to the maximal quantum uncertainty of transmitted states and therefore an eavesdropper receives the minimal amount of information. For the case of two-dimensional Hilbert space, our protocol allows secure transmission at the error rate higher than that one for the BB84-protocol and comparable with the characteristics of the best known QKD-protocols. However, with increasing the dimensionality of the Hilbert space the critical error rate for our protocol increases and in the limit of infinite-dimensional space the protocol becomes non-threshold.

Keywords: Quantum information, quantum cryptography, quantum key distribution

1. INTRODUCTION

Quantum cryptography could well be the first practical application of the rapidly developing field of quantum information [1]. Since 1970s, when the idea of quantum cryptography was proposed first [2,3], a number of different quantum key distribution (QKD) protocols implementing it have been suggested [3–6]. Despite their diversity all of them are based on a beautiful idea employing a basic "no-cloning" principle of quantum mechanics—impossibility of copying arbitrary quantum states [7]. Thanks to this, an eavesdropper cannot intercept the quantum communication channel without disturbing a transmitting message if it contains a set of *incompatible*, i.e., essentially quantum, not governed by the rules of classical logic, states. Moreover, any attempt of obtaining any information about this set of states inevitably disturbs the transmitted message.

Keeping this advantage of quantum physics for cryptography in mind, any QKD-protocol uses messages entirely composed of an incompatible set of quantum states or so called *quantum alphabet* that consists of incompatible "letters". Various QKD protocols are distinguished in essence only by different alphabets, which ensure secure message transmission up to an error level that determines the protocol efficiency. Analyzing distortions in received messages one can reveal an eavesdropping attack, but in order to establish a secure connection one should also be capable to resist such attacks. All discussed in the literature QKD-protocols have relatively low critical quantum bit error rate (QBER) [1,8] above which they do not ensure secure transmission.

It is eventually assumed that all perturbations in the transmitted information are caused by an eavesdropper. However in reality, imperfections of the apparatus used for realization of the QKD schemes and external sources of noise in the quantum channel (besides the eavesdropper) also perturb the information and therefore set a limit to the maximum length of the secure quantum channels used in the QKD schemes [1]. Such limitations significantly bound the applications of quantum cryptography making impossible secure transmission over an arbitrary distance and in order to overcome this obstacle one has to develop more efficient QKD protocols.

For the optimal efficiency analysis of various protocols different efficiency criteria are used in the literature [9], which is inconvenient for the objective comparison of the protocols. In this paper, we use the most appropriate, in our view, criterion based on the estimation of classical Shannon information transmitted through the secure channel of the QKD scheme [10].

Typical QKD scheme includes three basic players, Alice, Bob, and Eve (the conventional names for the sender, receiver, and eavesdropper, respectively), which communicate via a quantum channel. Despite the

Send correspondence to D.V.S.: E-mail: sych@comsim1.phys.msu.su

communication channel between Alice, Bob, and Eve is quantum, they in the final analysis exchange classical information. Therefore, the classical Shannon information can serve as a valid measure for the quantitative analysis of the QKD-protocols. It corresponds to the joint probability distribution of the measurement results (which are classical) in the quantum system Alice-Eve-Bob.

Any QKD alphabet is formed by selection of a set of quantum states at the input and output of the quantum channel. The selection rules determine different QKD-protocols. For example, the QKD-protocol proposed in 1992 by Bennett, hence the name B92 [4], uses only *two* quantum states, which is the minimum limit of incompatible "letters" composing the alphabet. The first QKD-protocol proposed in 1984 by Bennett and Brassard (BB84) [3] gives another example of the protocol in which *four* quantum incompatible states are used.

In the other limiting case, when selection of quantum states is not performed and, therefore, the alphabet consists of *all* states of the Hilbert space, we have a new QKD-protocol, which we analyze in this paper. We will show that this protocol has essential advantages in comparison with other known QKD-protocols. Specifically, its critical QBER exceeds that one for the BB84 protocol and generalization of our protocol to the case of multidimensional Hilbert space further significantly increases the critical QBER. In the limit of infinite-dimensional Hilbert space, the protocol has no error threshold and the critical QBER approaches its maximum possible value. This means that our QKD-protocol can basically work at *any* level of external errors or eavesdropping attacks (except most brutal intercept–resend attacks), which is the novel feature for the QKD-protocols.

2. COMPATIBLE INFORMATION AS A QUANTUM INFORMATION MEASURE FOR QKD

In quantum cryptography, Alice (A), Bob (B), and Eve (E) are different, kinematically independent quantum systems. Thus, the quantum events related to these systems represented by the different Hilbert spaces are mutually compatible. Due to this property, any pair of quantum events at the input and output of the quantum channel can be considered classically. Quantum specific of the channel reveals then only in the form of intrinsic quantum uncertainty of events at the input and output of the channel. We will call information related to the mutually compatible events in two quantum systems the *compatible* quantum information [11, 12]. A natural quantitative measure for the compatible information is the standard mutual Shannon information functional of the classical input–output (Alice-Bob) joint probability distribution P_{AB}:

$$I_{AB}[P_{AB}] = S_A[P_A] + S_B[P_B] - S_{AB}[P_{AB}], \tag{1}$$

where $S[P]$ is the classical Shannon entropy functional for the joint, $P = P_{AB}$, and marginal, $P = P_A, P_B$, probability measures [10].

In quantum information theory, like in the classical theory of information, one has to clarify which quantum events are used for the information exchange between quantum systems and define a set of elementary events of which any message is composed. Elementary events for a quantum system are given by the wave functions representing the state vectors of the system. Mathematically, a choice of basis events or the *information basis* can be given by defining a set of positive operators $\hat{E}_\nu$ representing a non-orthogonal expansion of the unit operator [13] or the positive operator valued measure (POVM) [14]:

$$\hat{1} = \sum \hat{E}_\nu. \tag{2}$$

For simplicity, we will in the following consider two-dimensional spaces, when not defined otherwise.

Two limiting cases of the compatible information, completely *selected* and *non-selected* information, are defined by the two limiting cases of the unit operator expansion—two-component orthogonal POVM [15]

$$\hat{1} = |\mu\rangle\langle\mu| + |\tilde{\mu}\rangle\langle\tilde{\mu}| \tag{3}$$

and continuous non-orthogonal [12]

$$\hat{1} = \int_\nu |\nu\rangle\langle\nu|\, \mathrm{dV}_\nu, \tag{4}$$

where $|\mu\rangle$ and $|\tilde{\mu}\rangle$ are the arbitrary pair of the orthogonal wave functions and $\mathrm{dV}_\nu = \sin\theta \mathrm{d}\theta \mathrm{d}\varphi/(2\pi)$ with the standard angular parameters on the Bloch sphere.

The completely selected information determines an information exchange between two quantum systems A and B with the joint density matrix $\hat{\rho}_{AB}$ through the selected set of orthogonal quantum events. The orthogonal basis determined by the unitary two-parametric transformations $U_A(\alpha)$ and $U_B(\beta)$ in the quantum systems A and B, respectively, can be chosen differently and the selected information also depends on the choice made:

$$I_{AB}(\alpha,\beta) = \sum_{k,l} P^{\alpha\beta}_{AB}(k,l) \log_2 \frac{P^{\alpha\beta}_{AB}(k,l)}{P^{\alpha}_{A}(k) P^{\beta}_{B}(l)}, \tag{5}$$

where parameters $\alpha = (\theta_1, \varphi_1)$ and $\beta = (\theta_2, \varphi_2)$ are given by the standard Bloch sphere angles. Joint distribution

$$P^{\alpha\beta}_{AB}(k,l) = \mathrm{Tr_{AB}}\big(\hat{E}^{\alpha}_{A}(k) \otimes \hat{E}^{\beta}_{B}(l)\big)\hat{\rho}_{AB},$$

where $\hat{E}^{\nu}_{A,B}(k) = |k\rangle^{\nu}_{A,B} \langle k|^{\nu}_{A,B}$, is defined on the basis states $|k\rangle^{\alpha}_{A}$ and $|l\rangle^{\beta}_{B}$ of the input (Alice) and output (Bob) of the channel, which are the orthogonal basis states of the respected Hilbert spaces H_A and H_B.

For the non-selected information, the information exchange equally includes all participating in the exchange states. Therefore, the information basis states of the information channel are *all* wavefunctions of the Hilbert spaces of a pair of participating in the exchange quantum systems. The respected non-selected information is then given as

$$I_{AB} = \iint\limits_{\alpha\,\beta} P_{AB}(\mathrm{d}\alpha, \mathrm{d}\beta) \log_2 \frac{\mathrm{P_{AB}}(\mathrm{d}\alpha, \mathrm{d}\beta)}{\mathrm{P_A}(\mathrm{d}\alpha)\mathrm{P_B}(\mathrm{d}\beta)}, \tag{6}$$

where $P_{AB}(\mathrm{d}\alpha, \mathrm{d}\beta) = \mathrm{Tr_{AB}}\big(\hat{\mathrm{E}}_{\mathrm{A}}(\mathrm{d}\alpha) \otimes \hat{\mathrm{E}}_{\mathrm{B}}(\mathrm{d}\beta)\big)\hat{\rho}_{\mathrm{AB}}$, $\hat{E}_{A,B}(\mathrm{d}\nu) = |\nu\rangle_{\mathrm{A,B}} \langle\nu|_{\mathrm{A,B}} \mathrm{dV}_\nu$.

Note that the non-selected information is equal to the selected one, which is averaged over all orientations of the orthogonal bases:

$$I_{AB} = \iint\limits_{\alpha\,\beta} I_{AB}(\alpha,\beta) \frac{\mathrm{dV}_\alpha \mathrm{dV}_\beta}{V^2}, \quad V = \int \mathrm{dV}_\nu = 2. \tag{7}$$

3. QKD PROTOCOL EMPLOYING ALL STATES OF THE HILBERT SPACE

In quantum cryptography, the purpose of Alice and Bob is to establish a secure connection, which prevents copying of useful transmitted information by Eve. It has been proved that such secure connection is possible if the amount of information Bob received from Alice exceeds information Eve received either from Alice or Bob [16]. This condition can be written as

$$I_{AB} > \max\big(I_{AE}, I_{BE}\big). \tag{8}$$

If the condition (8) is fulfilled, it is possible with the help of special methods of privacy amplification to reduce up to zero the amount of useful information Eve can gain eavesdropping the quantum channel. Even if the condition (8) is not fulfilled, Alice and Bob can establish a secure connection using the advantage distillation protocols [1]. We do not consider this option in the paper, but keep in mind that if one uses it the security criterion for our QKD-protocol can be improved.

Eve, in her turn, also tries to use optimal strategies of eavesdropping, i.e., Eve tries to gain maximum information about the transmitting message at the given error rate, performing any physically allowed transformations and minimizing the error level she causes:

$$I_{AE,BE} = \max_{I_{AB}=const} I_{AE,BE}. \tag{9}$$

All known QKD-protocols using finite-dimensional spaces of states are built on the alphabets with the finite discrete set of incompatible quantum "letters", which can be realized as the pure states of a quantum system.

In this paper, we suggest a qualitatively new QKD-protocol, which is based on the alphabet including *all* states of the Hilbert space. In other words, this alphabet consists of an infinite number of quantum "letters", which are formed by the arbitrary superpositions of the orthogonal basis states of the Hilbert space H_A.

Let us first consider the case of two-dimensional space (multidimensional case is considered in section 4).

Elementary step of the QKD-protocol, i.e., the transmission of a single "letter" or state from Alice to Bob, can be outlined as follows:

1. Alice generates and transmits via a quantum channel to Bob a *randomly* chosen state $|\beta\rangle$.
2. Eve eavesdrops the channel performing an unitary bipartite transformation U_{BE} with her initial probe state $|0\rangle_E$ and with transmitted by Alice to Bob state $|\beta\rangle_B$ and measures her final probe state. Despite Eve does not measure the transmitted from Alice to Bob state directly, she disturbs it by the transformation U_{BE}.
3. Bob reads the perturbed state using for the measurement an *arbitrary* projector because he has no *a priori* information about the received message, but the dimension of the Hilbert space H_A.

When the transmission of the entire message, which consists of an essential number of elementary QKD-steps, is completed, Alice and Bob should perform on the transmitted raw key classical post-transmission procedures.

First, they determine the mutual probability distribution $P_{AB}(\alpha, \beta)$ and calculate the average amount of the information I_{AB} per the transmission. For this, Alice and Bob disclose and then discard random part of the measurement results transmitting them over an insecure classical channel. The information transmitted from Alice to Bob, I_{AB}, can be calculated with the help of Eq. (7), whereas the information transmitted between Eve and Alice and Bob, I_{AE}, I_{BE}, can be calculated using theoretical model of eavesdropping, which we will discuss in the following subsection.

Second, they need to check the security condition (8). If it is fulfilled, Alice and Bob decide that the secret key transfer is completed and perform then classical error correction and privacy amplification algorithms with the raw key. Otherwise, the transmitted key is not used.

3.1. Information analysis of the protocol

For the information analysis of our protocol let us first calculate the amount of information Bob received from Alice, I_{AB}, and Eve received from Alice and Bob, $I_{AE,BE}$, at the condition (9) of optimal eavesdropping.

Initial state of the quantum system Alice-Eve-Bob $\hat{\rho}^{(1)}_{ABE} = \hat{\rho}^{(1)}_{AB} \otimes |0\rangle_E \langle 0|_E$, which is described by the tensor product of the entangled antisymmetric pair Alice-Bob $\hat{\rho}^{(1)}_{AB} = ||-\rangle\rangle_{AB} \langle\langle -||_{AB}$ and an initial Eve's state $|0\rangle_E$, is transferred after eavesdropping the channel by Eve into the final state that is an entangled state of Alice, Bob, and Eve, $\hat{\rho}^{(2)}_{ABE}$: $\hat{\rho}^{(1)}_{ABE} \xrightarrow{U_{BE}} \hat{\rho}^{(2)}_{ABE}$. Let us assume that the Alice's state $|\alpha\rangle$ is totally entangled with the transmitting state $|\beta\rangle$ and is, for example, the antisymmetric Bell state $||-\rangle\rangle = \left(|\alpha\rangle \left|\tilde{\beta}\right\rangle - |\tilde{\alpha}\rangle |\beta\rangle\right)/\sqrt{2}$, which means that Alice perfectly knows the transmitting state $|\beta\rangle$, because maximal value of mutual selected information is equal to unity for the entangled states.

We can assume (without reducing the generality of our consideration) that the unitary transformation U_{BE} performed by Eve has the form:

$$\begin{cases} |0\rangle_B |0\rangle_E \xrightarrow{U_{BE}} |0\rangle_B |\Phi_{00}\rangle_E + |1\rangle_B |\Phi_{01}\rangle_E \\ |1\rangle_B |0\rangle_E \xrightarrow{U_{BE}} |0\rangle_B |\Phi_{10}\rangle_E + |1\rangle_B |\Phi_{11}\rangle_E . \end{cases} \tag{10}$$

The unitarity imposes the following restrictions, which are due to the orthogonality and normalization conditions:

$$\langle \Phi_{00} \mid \Phi_{10}\rangle + \langle \Phi_{01} \mid \Phi_{11}\rangle = 0, \quad |\Phi_{00}|^2 + |\Phi_{01}|^2 = |\Phi_{10}|^2 + |\Phi_{11}|^2 = 1. \tag{11}$$

It was suggested in reference [9] based on the numerical estimations and then proved in reference [17] that in the QKD-protocols BB84 and B92 the Eve's state at the optimal eavesdropping lies in two-dimensional Hilbert space. This is also true (and can be proved by analogy with reference [9]) for our QKD-protocol. Therefore, the states $|\Phi_{ij}\rangle$ can be written, taking into account the conditions (11), as a superposition of the two basis states:

$$\overrightarrow{|\Phi\rangle} = \begin{pmatrix} |\Phi_{00}\rangle \\ |\Phi_{01}\rangle \\ |\Phi_{10}\rangle \\ |\Phi_{11}\rangle \end{pmatrix} = \begin{pmatrix} \gamma_{00} & \gamma_{01} \\ \gamma_{10} & \gamma_{11} \\ \gamma_{11} & \gamma_{10} \\ \gamma_{01} & \gamma_{00} \end{pmatrix} \begin{pmatrix} |0\rangle_E \\ |1\rangle_E \end{pmatrix}, \tag{12}$$

where the transformation parameters

$$\gamma_{mn} = (-1)^{mn} \cos(\theta - m\frac{\pi}{2}) \cos(\varphi - n\frac{\pi}{2}) \tag{13}$$

are determined via the two angles θ, φ, controlled by Eve.

Resulted bipartite density matrices Alice-Bob, Alice-Eve, and Bob-Eve obtained by averaging of the three-partite density matrix over the third system enable us to calculate the respective mutual information:

$$\begin{aligned} \hat{\rho}^{(2)}_{AB} &= \mathrm{Tr}_{\mathrm{E}} \hat{\rho}^{(2)}_{ABE} \rightarrow I_{AB}, \\ \hat{\rho}^{(2)}_{AE} &= \mathrm{Tr}_{\mathrm{B}} \hat{\rho}^{(2)}_{ABE} \rightarrow I_{AE}, \\ \hat{\rho}^{(2)}_{BE} &= \mathrm{Tr}_{\mathrm{A}} \hat{\rho}^{(2)}_{ABE} \rightarrow I_{BE}. \end{aligned} \tag{14}$$

In our QKD-protocol Alice sends Bob any pure state with equal probability and neither Bob nor Eve have an *a priori* chosen basis for the measurement, thus both Eve and Bob use each an arbitrary chosen bases. After averaging over a large number of measurements we receive due to the equation (7) that the non-selected information is exactly the information measure for our QKD-protocol.

3.2. Calculations results

Results for the mutual Alice-Bob, Alice-Eve, and Bob-Eve non-selected information (I_{AB}, I_{AE}, and I_{BE}, respectively) calculated with the help of equations (6), (10), (12), and (14) are shown in figure 1 versus parameters θ and φ controlled by Eve (see equation (13)). One can clearly see from the figure that for the all values of θ, φ we have $I_{AE} \geq I_{BE}$, thus we will focus in the following only on I_{AE}.

The optimal eavesdropping condition (9) requires that we look for the maximal $I_{AE} = I_{AE}(\theta, \varphi)$ at the given value of $I_{AB} = I_{AB}(\theta, \varphi)$. Detailed analysis of data in figure 1 reveals that the optimal eavesdropping can be realized at $\theta = \pi/4 - \varphi$, which corresponds to the solid line in figure 1d.

For the most purposes it is enough to consider only the case of optimal eavesdropping, which corresponds to the solid line at $\theta = \pi/4 - \varphi$ shown in figure 2. From analysis of this figure one can see that at $\theta = 0$ the level of eavesdropping attacks and the respected losses of information are equal to zero. At $\theta = \pi/4$ the intervention of Eve is maximal and she acts similar to Bob gaining maximal possible information.

The security condition (8) is fulfilled up to a certain critical value $\theta_0^{(1)} = \pi/8$, which is the intersection point (1) of the curves for I_{AB} and I_{AE} in the figure 2. If Eve performs the unitary transformation (10) with $\theta < \theta_0^{(1)}$, then Alice and Bob can establish a secure connection, otherwise it is not established.

3.3. Definitions of the error rate in the QKD-protocols

In order to estimate the error rate in the different QKD-protocols and, therefore, their efficiency different quantitative characteristics can be introduced. One of the most accepted in the literature characteristics—the quantum bit error rate (QBER)—was suggested to characterize the error rate in the sifted key. It is defined as the ratio of wrong bits in the transmitted message to the total number of received bits. Obviously, the QBER for an ideal quantum channel without noise is equal to zero and one can use the QBER for estimation of the Eve's interference. Generally, any QKD-protocol works up to a certain critical error rate level, which is defined as the

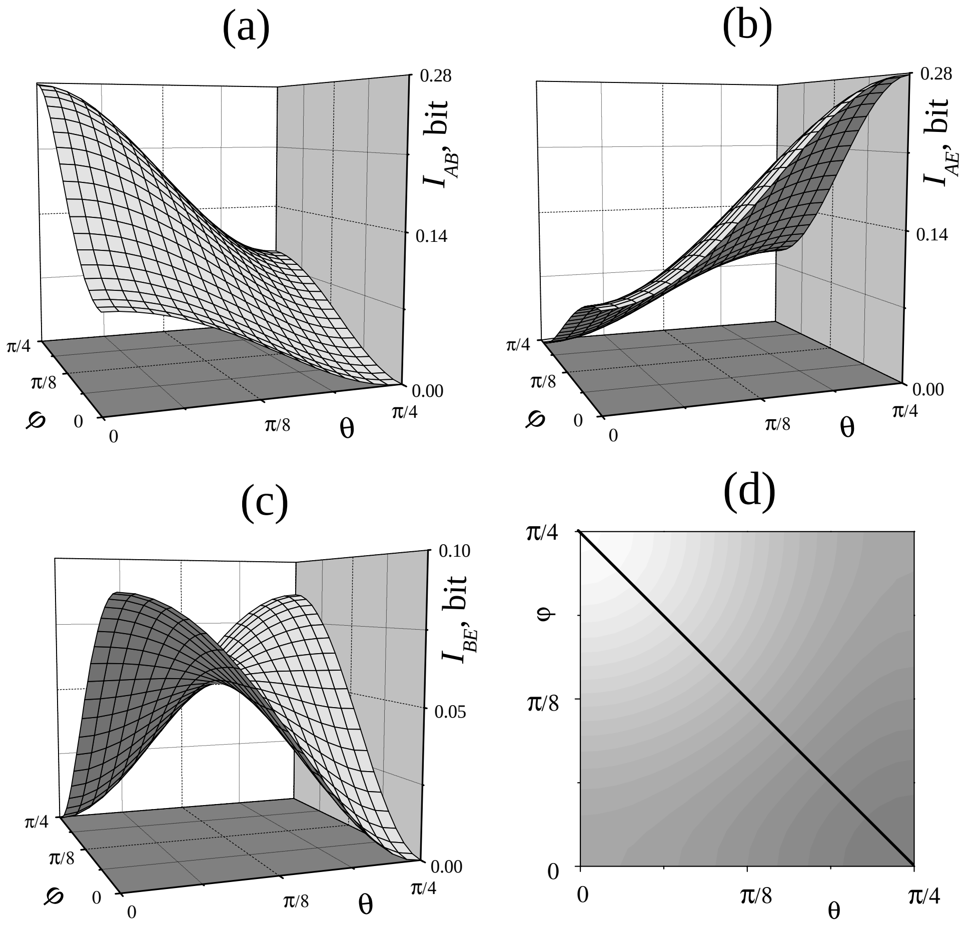

Figure 1. Alice-Bob (a), Alice-Eve (b), and Bob-Eve (c) mutual Shannon information versus Eve's eavesdropping parameters θ, φ. Figure (d) shows results of figure (a) for the Alice-Bob mutual Shannon information (I_{AB}) as a contour plot; solid line corresponds to the case of optimal eavesdropping.

critical QBER. The larger the critical QBER value, the better stability of the protocol to the errors caused by Eve.

However, if the QKD-scheme without external noise does not show the QBER equal to zero, then we cannot use the QBER characteristic for estimation of the QKD-protocol efficacy and for comparison with other QKD-protocols. In this case, the QBER as it has been defined previously simply does not reflect the real level of the Eve interference.

Keeping in mind that Eve performs the unitary transformation (10), we can define the QBER, which we will define as q, as the probability that Eve flips the transmitted to Bob bit of information:

$$q = \langle \Phi_{01} \mid \Phi_{01} \rangle = \langle \Phi_{10} \mid \Phi_{10} \rangle = \sin^2 \theta.$$

This definition is essentially rely on the structure of the transformation (10) performed by Eve. It is worth also to note that, as it was shown in [9], the QBER is not always an adequate characteristic of the degree of Eve eavesdropping attacks, for instance in the B92 protocol.

Therefore, we suggest to use another characteristic, which we call the *compatible information error rate* (CIER) and designate as Q, that naturally represents the degree of the Eve interference into the information

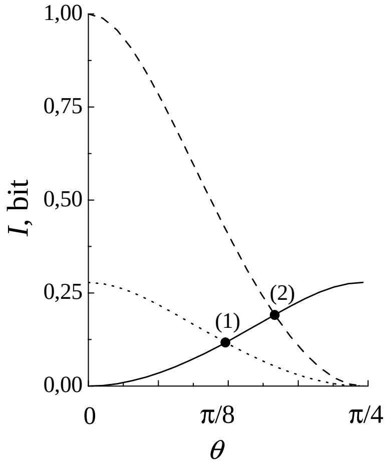

Figure 2. Alice-Bob (dotted and dashed lines for the reconciliated and non-reconciliated basis states of Alice and Bob, respectively) and Alice-Eve (solid line) mutual Shannon information at the optimal eavesdropping condition.

transmission in terms of the compatible information:

$$Q = 1 - \frac{I_{AB}}{I_{AB}^{max}} \in [0, 1]. \tag{15}$$

Here I_{AB} is the Alice–Bob compatible information with the presence of eavesdropping and I_{AB}^{max} is its maximal possible value without Eve attacks. Qualitatively, the CIER is the error rate of the secret key that can be distilled from the correlations per transmission. By contrast with the QBER (q), the CIER (Q) is, in our view, the most adequate parameter for the information properties of the QKD-protocols, even in the presence of internal noise caused by the protocol itself.

Without Eve eavesdropping attacks, both parameters q and Q are equal to zero, which means that there are no transmission errors. At the maximal level of Eve interference with the transmitting information, we have $Q = 1$ and $q = 0.5$, which correspond to the maximal possible level of errors caused by Eve. At the critical point $\theta_0^{(1)}$, where the amount of information gained by Eve is equal to the amount of information received by Bob, $Q_0^{(1)} \simeq 0.6$ and $q_0^{(1)} \simeq 0.15$.

At the error level exceeding critical, i.e., at $Q > Q_0^{(1)}$, the protocol does not ensure security of the transmitted data and Alice and Bob decide that the transmission is not completed.

Note that the described scheme does not require bases reconciliation of Alice and Bob, i.e., selection of only that part of the message for which Alice and Bob used the same information basis, via an additional information exchange over the classical channel. However, one can significantly improve stability of the protocol for a noisy quantum channel using the bases reconciliation considered in the next section.

3.4. Basis reconciliation

After transmission of the entire message through a noisy quantum channel Alice and Bob can select only those transmitted data for which they used approximately similar orthogonal bases. In our case, the set of basis states is continuous, thus it is necessary to split it into several approximately equal areas and count the bases similar, if they are in the same area on the Bloch sphere. Depending on the number of such areas, the mutual information in the system Alice-Bob per single transmission is raised from 0.28 to 1 bit.

This can be clearly understood because for an initial state of the Alice-Bob system in the form of antisymmetric Bell state the mutual selected information is equal to unit when one uses similar bases of Alice and Bob. If the bases of Alice and Bob are different, the amount of information in a single transmission will be less than unit.

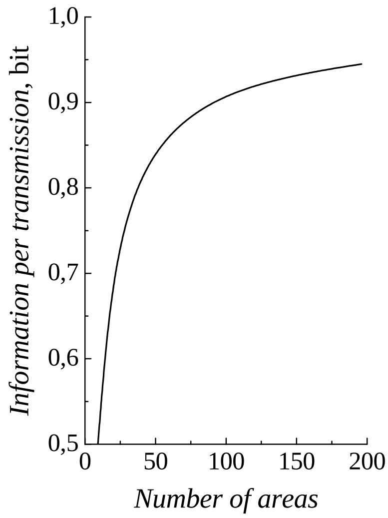

Figure 3. Maximal amount of information per single transmission versus the number of areas the Hilbert space is split in.

The calculated dependency of the maximal amount of information per single transmission versus the number of areas in which we split the Hilbert space is shown in figure 3.

We restrict the actions of Eve by the measurement of the probe state immediately after the the unitary transformation (10). Therefore, one can suppose that Eve does not affect the data selection with the reconciling bases and does not use additional transformations after the bases have been reconciled. Then, she gains no additional information.

Information that Bob receives from Alice per the entire message transmission after the bases reconciliation is shown in figure 2 (dashed line). The new critical value $\theta_0^{(2)}$ is bigger than $\theta_0^{(1)}$ and, therefore, the critical error rate Q_0 and q_0 are then significantly higher: $Q_0^{(2)} \simeq 0.81$ and for the QBER we have $q_0^{(2)} \simeq 0.254$.

Note that the bases reconciliation procedure significantly increases the required number of messages transmitted over an insecure classical channel, because we have to transmit information about the area in which the randomly chosen basis lies. Respectively, the number of filtered messages transmitted through a quantum channel is also decreased. It is not necessary, however, to infinitely increase the accuracy. As a rule, errors during the data transmission have typical for a specific experimental QKD setup finite level. Therefore, for the bases reconciliation it is sufficient to increase the accuracy according to the external noise conditions up to the level that ensures the error rate less than the critical one at which the QKD-protocol guarantees the secure transmission of data in accordance with the security condition (8).

4. MULTIDIMENSIONAL CASE

We can fundamentally improve the properties of our QKD-protocol using multidimensional Bob's and Alice's spaces ($D > 2$). In multidimensional case, the maximally possible amount of mutual selected information is equal to $I^D_{\max} = \log_2 D$ and grows infinitely at $D \to \infty$. Maximally possible amount of non-selected information is equal to the amount of accessible information [18]:

$$I^D_{\text{accesible}} = \log_2 D - \frac{1}{\ln 2} \sum_{k=2}^{D} \frac{1}{k},$$

which in the limit $D \to \infty$ is restricted by the value of $I^\infty \simeq 0.61$ bit.

After bases reconciliation of Alice and Bob the amount of information in the system Alice-Bob is given by the maximally possible selected information, whereas in the Alice-Eve system—by the maximally possible non-selected information, independently from a specific type of unitary transformation performed by Eve in the multidimensional case. Then, the critical CIER in the limit of $D \to \infty$ is equal to unit:

$$Q_0^\infty = \lim_{D\to\infty} Q_0^D = 1 - \lim_{D\to\infty} \frac{I^D_{\text{accessible}}}{I^D_{\text{max}}} \simeq 1 - \lim_{D\to\infty} \frac{0.61}{\log_2 D} = 1. \tag{16}$$

This means that increasing the dimensionality of the Alice-Bob system one can reach the critical error rate (QBER or CIER), which exceeds any given value (below the unit). The dependency of the critical CIER versus the dimensionality of the Hilbert space is shown in figure 4.

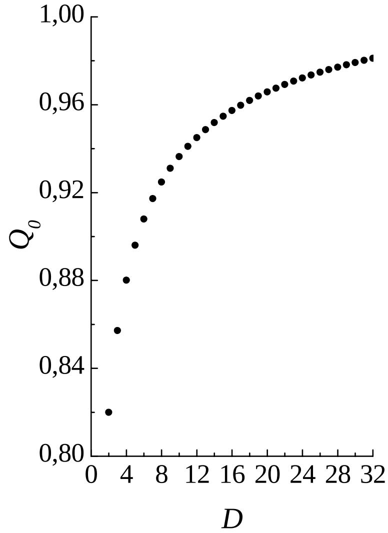

Figure 4. Critical CIER Q_0 versus the dimensionality D of the Hilbert space.

The essential qualitative novelty of our QKD-protocol that employs all states of the Hilbert space is that it can work, in principle, at any imperfections or noise in the quantum channel (either internal or external) and has no any critical CIER value after which the protocol becomes insecure. For any given CIER value one can select the required dimensionality of the Alice-Bob space in order to meet this value of CIER (figure 4). Essentially more difficult is the question about Eve's transformation structure to perform optimal eavesdropping in the multidimensional case, but the outlined above result is qualitatively correct, despite any specific structure of the Eve's transformation.

The described above advantage of our QKD-protocol can be clarified as follows. When Alice sends a message, neither Eve nor Bob do not know *a priori* in which basis it is transferred. Therefore, both Eve and Bob are perplexed in the multidimensional space—they can retrieve less amount of information from the transmitted message with the increasing dimensionality of the Hilbert space. After the *partial* bases reconciliation, which is described in section 3.4, Bob significantly increases the amount of information per single transmission filtering only strongly correlated transmissions, i.e., the transmissions for which Alice and Bob used approximately equal bases. Eve, in her turn, cannot filter the transmissions and the amount of information she can retrieve remains the same. Therefore, the larger the dimension of the Hilbert space, less equally Eve and Bob receive the information.

5. EXPERIMENTAL SETUP FOR QKD PROTOCOL WITH CONTINUOUS ALPHABET

An experimental setup for our QKD-protocol with continuous alphabet "letters" of which are coded with polarizations of the photons is shown in figure 5. In these notations, a random "letter" of the alphabet corresponds to an arbitrary photon polarization.

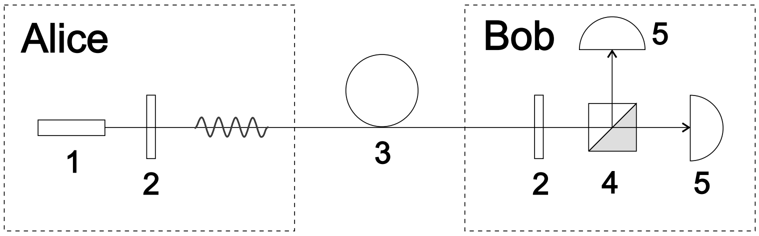

Figure 5. Experimental setup for the QKD-protocol with continuous alphabet. At the Alice side, the laser (1) generates single photons polarization of which is rotated by the polarizer (2) at a random angle. These photons are transmitted to Bob via the quantum channel (3). The measurement part of the QKD-setup at the Bob side includes the polarizer (2) that rotates polarization of the incident photon, polarizing beamsplitter (4), and the photon counting detectors (5). A supplementary classical channel over which Alice and Bob reconcile their bases states by exchanging non-secure public information is not shown in the figure.

At the Alice side of the QKD-setup random “letters” from the continuous alphabet are generated. Laser at this side generates single photons with determined polarization, which is rotated by polarization plate at a random angle for each photon. Alice knows these random angles for each photon. Generated photons are transmitted then to Bob via a quantum channel (for instance, a fiber optical link preserving the polarizations of the photons). Bob for the measurement in an arbitrary basis first rotates polarization of the incident photon by polarization plate to the random angle value and then performs measurement in the fixed basis. Alice and Bob reconcile their bases states by exchanging non-secure public information over a classical channel, a telephone line, for instance.

In the described QKD-setup, the case of multidimensional Hilbert space for the quantum channel input and output can be, in principle, realized by transmitting of information with the help of several entangled qubits (photons). This, however, is an experimental difficulty to generate, operate, and measure arbitrary states in multidimensional spaces, i.e., difficulty to generate and operate multiple entangled photons.

6. CONCLUSIONS

In conclusion, a new QKD-protocol based on the quantum alphabet with infinitive number of “letters” (i.e., employing all quantum states of the Alice-Bob quantum system) is proposed. It has a number of advantages in comparison with other known QKD-protocols.

In two-dimensional case, the critical QBER for our protocol exceeds 25% and can be increased further with the help of special classical methods of advantage distillation.

The essential qualitative novelty of our QKD-protocol in multidimensional case is that it can work, in principle, at any imperfections or noise in the quantum channel (either internal or external) and has no any critical bit error rate value after which the protocol becomes insecure.

For estimation of the Eve’s intervention into the data transmission through a quantum channel we use new classical mutual Shannon information-based criterion, which adequately reflects the information aspect of the eavesdropping and can be effectively used for both constructing and analyzing the QKD-protocols.

The only restriction on the Eve’s strategy of eavesdropping is that she measures her probe state before the bases reconciliation. This restriction does not contradict with the experimental realizations of the QKD-protocols—Alice and Bob should simply reconcile their bases after the finite decoherence time in the quantum system. Obviously, such an experimental trick gives no 100% guarantee of the secure transmission, but in the real QKD-schemes it seems reasonable.

ACKNOWLEDGMENTS

This work was partially supported by RFBR grants Nos. 01–02–16311, 02–03–32200, and INTAS grant INFO 00–479.

REFERENCES

1. Gisin N, Ribordy G, Tittel W, and Zbinden H, "Quantum cryptography", *RMP*, **74**, 145, 2002.
2. Wiesner S, "Conjugate coding", *SIGAT News*, **15**, 78, 1983.
3. Bennett Ch H and Brassard G, *Proc. IEEE Int. Conf. on Computer, System, and Signal Processing (Bangalore, India)*, 175, IEEE Publishers, New York, 1984.
4. Bennett Ch H, "Quantum cryptography using any two nonorthogonal states", *PRL*, **68**, 3121, 1992.
5. Bruss D, "Optimal eavesdropping in quantum cryptog-raphy with six states", *PRL*, **81**, 3018, 1998.
6. Grosshans F and Grangier P, "Continuous variable quantum cryptography using coherent states", *PRL*, **88**, 057902, 2002.
7. Wootters W K and Zurek W H, "A single quantum cannot be cloned", *Nature*, **299**, 802, 1982.
8. Gottesman D and Hoi-Kwong Lo, *IEEE Transactions Inf. Theory*, **49**, 457, 2003; *LANL e-print*, quant-ph/0105121.
9. Fuchs C A and Peres A, "Quantum state disturbance vs. information gain: uncertainty relations for quantum information", *PRA*, **53**, 2038, 1996.
10. Gallagher R G, *Information Theory and Reliable Communication*, John Wiley and Sons, New York, 1968.
11. Grishanin B A, *Problemi Peredachi Informatzii*, **38**, 31, 2002.
12. Grishanin B A and Zadkov V N, "Measurement and physical content of quantum information", *J. of Commun. Technology and Electronics*, **47**, 933, 2002.
13. Grishanin B A, *Izv. A. N. USSR, Tekhnicheskaya Kybernetika*, **11**, 27, 1973.
14. Preskill J, *Lecture notes on Quantum Information*, www.theory.caltech.edu/people/preskill/ph229/.
15. von Neumann J, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, 1955
16. Bennett C H, Brassard G and Robert J M, "Privacy amplification by public discussion", *SIAM J. Comput.*, **17**, 210, 1988.
17. Fuchs C A, Gisin N, Griffiths R B, Niu C S and Peres A, "Optimal eavesdropping in quantum cryptography. I. information bound and optimal strategy", *PRA*, **56**, 1163, 1997.
18. Caves C M and Fuchs C A, "Quantum information: how much information in a state vector?", *LANL e-print*, quant-ph/9601025.