Laser Physics, Vol. 14, No. 10, 2004, pp. 1–8.

Quantum Key Distribution with a Continuous Alphabet

D. Sych, B. Grishanin, and V. Zadkov

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

e-mail: sych@comsim1.phys.msu.su

Received January 15, 2004

Abstract—A novel quantum key distribution protocol (QKD) based on all unselected states of a quantum system that set the alphabet with a continuous set of letters is proposed. Employing all states of the Hilbert space leads to a maximum quantum uncertainty of transmitted states, and, therefore, an eavesdropper receives the minimum amount of information. For the case of a two-dimensional Hilbert space, our protocol allows secure transmission at an error rate better than that for the BB84-protocol and is 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 nonthreshold.

1. INTRODUCTION

Quantum cryptography could well be the first practical application of the rapidly developing field of quantum information [1]. Since the 1970s, when the idea of quantum cryptography was first proposed [2, 3], a number of different quantum key distribution (QKD) protocols for implementing it have been proposed [3–6]. Despite their diversity, all of them are based on the beautiful idea of employing a basic no-cloning principle of quantum mechanics—the impossibility of copying arbitrary quantum states [7]. Thanks to this, an eavesdropper cannot intercept the quantum communication channel without disturbing the transmitting message if it contains a set of incompatible, i.e., essentially quantum, states not governed by the rules of classical logic. Moreover, any attempt to obtain 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 a so-called quantum alphabet consisting of incompatible "letters." Various QKD protocols are distinguished in essence only by their different alphabets, which ensure secure message transmission up to the level of error determining the protocol efficiency. By analyzing distortions in received messages, one can reveal an eavesdropping attack, but, in order to establish a secure connection, one must also be capable of stemming such attacks.

All QKD protocols discussed in the literature have relatively a 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 realizing the QKD schemes and external sources of noise in the quantum channel (in addition to the eavesdropper) also perturb the information and, therefore, set a limit on the maximum length of secure quantum channels used in the QKD schemes [1]. These limitations significantly hinder applications of quantum cryptography to make secure transmission impossible over an arbitrary distance, and, in order to overcome this obstacle, one has to develop more efficient QKD protocols.

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

A 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 communication channel between Alice, Bob, and Eve being quantum, in the final analysis they exchange classical information. Therefore, the classical Shannon information can serve as a valid measure for the quantitative analysis of 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 selecting a set of quantum states at the input and output of the quantum channel. The selection rules determine the 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] is another example of a 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 over other known QKD protocols. Specifically, its critical QBER exceeds that 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 for brutal intercept–resend attacks), which is a novel feature for 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 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 specificity of the channel is revealed 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 compatible quantum information [11, 12]. A natural quantitative measure of compatible information is the standard mutual Shannon information functional of the classical input–output (Alice–Bob) joint probability distribution P_{AB}:

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

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 the 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 nonorthogonal expansion of the unit operator [13] or the positive operator valued measure (POVM) [14]:

$$\hat{1} = \sum \hat{E}_\nu. \quad (2)$$

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

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

$$\hat{1} = |\mu\rangle\langle\mu| + |\tilde{\mu}\rangle\langle\tilde{\mu}| \quad (3)$$

and the continuous nonorthogonal POVM [12]

$$\hat{1} = \int_\nu |\nu\rangle\langle\nu| dV_\nu, \quad (4)$$

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

The completely selected information determines 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:

$$I_{AB}(\alpha, \beta) = \sum_{k,l} P_{AB}^{\alpha\beta}(k, l)\log_2\frac{P_{AB}^{\alpha\beta}(k, l)}{P_A^\alpha(k)P_B^\beta(l)}, \quad (5)$$

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

$$P_{AB}^{\alpha\beta}(k, l) = \mathrm{Tr}_{AB}(\hat{E}_A^\alpha(k) \otimes \hat{E}_B^\beta(l))\hat{\rho}_{AB},$$

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

For the nonselected information, the information exchange equally includes all states participating in the exchange. Therefore, the information basis states of the information channel are all wave functions of the Hilbert spaces of a pair of quantum systems participating in the exchange. The respected nonselected information is then given as

$$I_{AB} = \iint_{\alpha\beta} P_{AB}(d\alpha, d\beta)\log_2\frac{P_{AB}(d\alpha, d\beta)}{P_A(d\alpha)P_B(d\beta)}, \quad (6)$$

where $P_{AB}(d\alpha, d\beta) = \mathrm{Tr}_{AB}(\hat{E}_A(d\alpha) \otimes \hat{E}_B(d\beta))\hat{\rho}_{AB}$, and $\hat{E}_A(d\nu) = |\nu\rangle_A\langle\nu|_A dV_\nu$.

Note that the nonselected information is equal to the selected information averaged over all orientations of the orthogonal bases:

$$I_{AB} = \iint_{\alpha\beta} I_{AB}(d\alpha, d\beta)\frac{dV_\alpha dV_\beta}{V^2}, \quad V = \int dV_\nu = 2. \quad (7)$$

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 a secure connection is possible if the amount of information Bob receives from Alice exceeds the information Eve receives either from Alice or Bob [16]. This condition can be written as

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

If 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 through eavesdropping on the quantum channel. Even if 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 here but keep in mind that using it can improve the security criterion for our QKD protocol.

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

$$I_{AE,\,BE} = \max_{I_{AB} = \text{const}} I_{AE,\,BE}. \quad (9)$$

All known QKD protocols using finite-dimensional spaces of states are built on alphabets with a finite discrete set of incompatible quantum "etters, 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 formed by arbitrary superpositions of the orthogonal basis states of the Hilbert space H_A.

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

The 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:

(i) Alice generates and transmits a randomly chosen state $|\beta\rangle$ via a quantum channel to Bob.

(ii) Eve eavesdrops on the channel by performing a unitary bipartite transformation U_{BE} with her initial probe state $|0\rangle_E$ and with the state $|\beta\rangle_B$ transmitted by Alice to Bob and measures her final probe state. Though Eve does not measure the state transmitted from Alice to Bob directly, she disturbs it through the transformation U_{BE}.

(iii) Bob reads the perturbed state using an arbitrary projector for the measurement because he has no *a priori* information about the received message other than the dimension of the Hilbert space H_A.

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

First, they determine the mutual probability distribution $P_{AB}(\alpha, \beta)$ and calculate the average amount of information I_{AB} per transmission. For this, Alice and Bob disclose and then discard the random part of the measurement results by 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} and I_{BE}, can be calculated using the 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, $I_{AE,\,BE}$, under the condition (9) of optimal eavesdropping.

The 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 Eve's initial state $|0\rangle_E$, is transferred after eavesdropping by Eve into the final state, which 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 Alice's state $|\alpha\rangle$ is totally entangled with the transmitting state $|\beta\rangle$ and is, for example, the antisymmetric Bell state $\|-\rangle\rangle = (|\alpha\rangle|\tilde{\beta}\rangle - |\tilde{\alpha}\rangle|\beta\rangle)/\sqrt{2}$, which means that Alice knows the transmitting state $|\beta\rangle$ perfectly, because the maximum 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

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

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

$$\begin{aligned} \langle\Phi_{00}|\Phi_{10}\rangle + \langle\Phi_{01}|\Phi_{11}\rangle &= 0, \\ |\Phi_{00}|^2 + |\Phi_{01}|^2 &= |\Phi_{10}|^2 + |\Phi_{11}|^2 = 1. \end{aligned} \quad (11)$$

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

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

where the transformation parameters

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

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

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

$$\begin{aligned} \hat{\rho}_{AB}^{(2)} &= \mathrm{Tr}_E \hat{\rho}_{ABE}^{(2)} \longrightarrow I_{AB}, \\ \hat{\rho}_{AE}^{(2)} &= \mathrm{Tr}_B \hat{\rho}_{ABE}^{(2)} \longrightarrow I_{AE}, \\ \hat{\rho}_{BE}^{(2)} &= \mathrm{Tr}_A \hat{\rho}_{ABE}^{(2)} \longrightarrow I_{BE}. \end{aligned} \qquad (14)$$

In our QKD protocol, Alice sends Bob any pure state with equal probability and neither Bob nor Eve has an *a priori* chosen basis for the measurement; thus, both Eve and Bob use an arbitrary chosen basis each. After averaging over a large number of measurements, due to Eq. (7), we find that the nonselected information is precisely the information measure for our QKD protocol.

3.2. Calculation Results

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

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

For most purposes, it is enough to consider only the case of optimal eavesdropping that corresponds to the solid line at $\theta = \pi/4 - \varphi$ shown in Fig. 2. From analyzing 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 $\theta = \pi/4$, Eve's intervention is at a maximum and she acts similar to Bob in gaining the maximum 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 Fig. 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 characteristics most accepted in the literature, 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 to estimate Eve's interference. Generally, any QKD protocol works up to a certain critical rate of error defined as the critical QBER. The larger the critical QBER, the more stable the protocol to errors caused by Eve.

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

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

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

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

Therefore, we suggest using another characteristic, which we call the compatible information error rate (CIER) and designate as *Q*. This characteristic naturally represents the degree of Eve's interference in the transmission of information in terms of the compatible information:

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

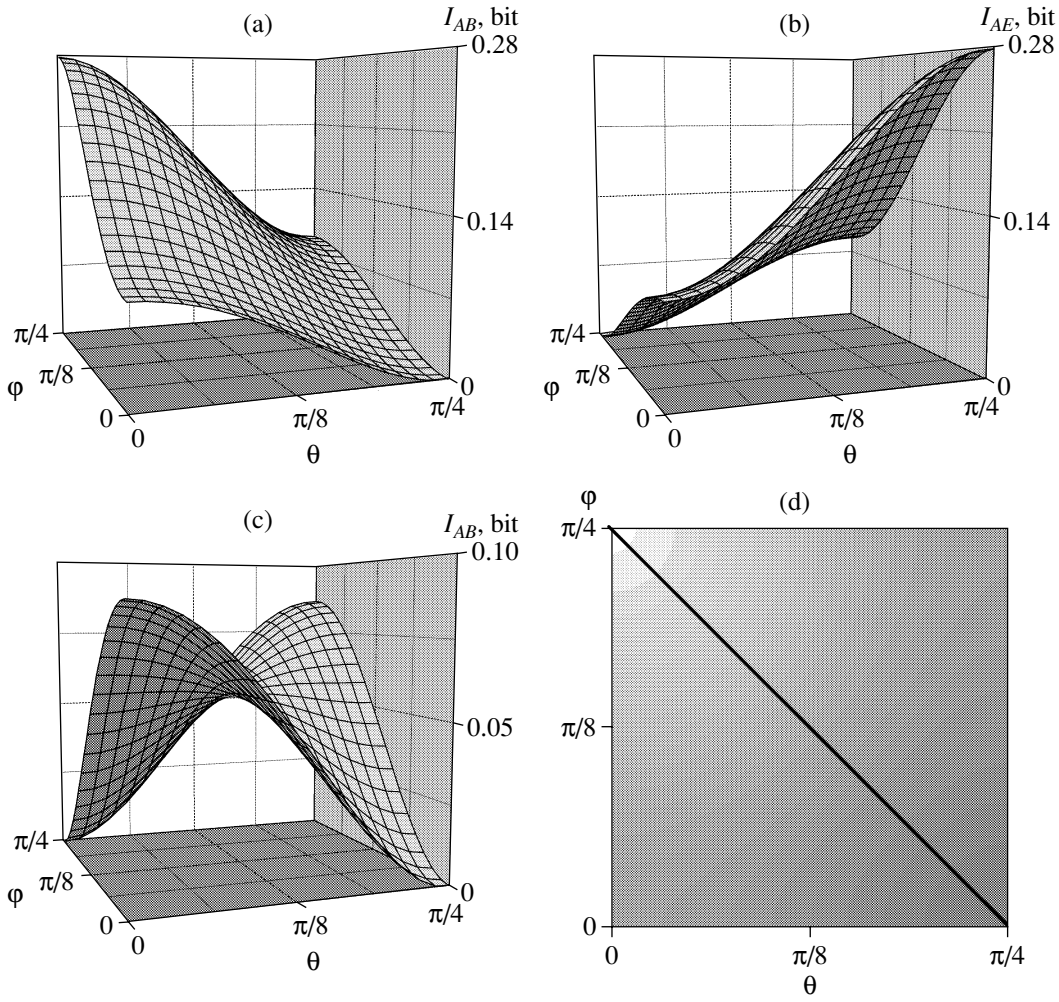

Fig. 1. (a) Alice–Bob, (b) Alice–Eve, and (c) Bob–Eve mutual Shannon information versus Eve's eavesdropping parameters θ and φ. (d) Results of (a) for the Alice–Bob mutual Shannon information (I_{AB}) as a contour plot; the solid line corresponds to the case of optimal eavesdropping.

Here, I_{AB} is the Alice–Bob compatible information with the presence of eavesdropping and $I_{AB}^{\max}$ is its maximum possible value without attacks by Eve. 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 QKD protocols, even in the presence of internal noise caused by the protocol itself.

Without eavesdropping attacks by Eve, both parameters q and Q are equal to zero, which means that there are no transmission errors. At the maximum level of interference from Eve with the transmitted information, we have $Q = 1$ and $q = 0.5$, which correspond to the maximum 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 an 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 complete.

Note that the described scheme does not require bases reconciliation between 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 the 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 an 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

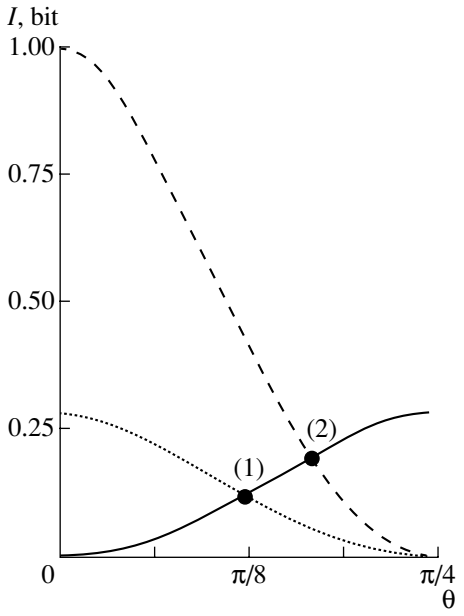

Fig. 2. Alice–Bob (dotted and dashed lines for the reconciliated and nonreconciliated basis states of Alice and Bob, respectively) and Alice–Eve (solid line) mutual Shannon information under the condition of optimal eavesdropping.

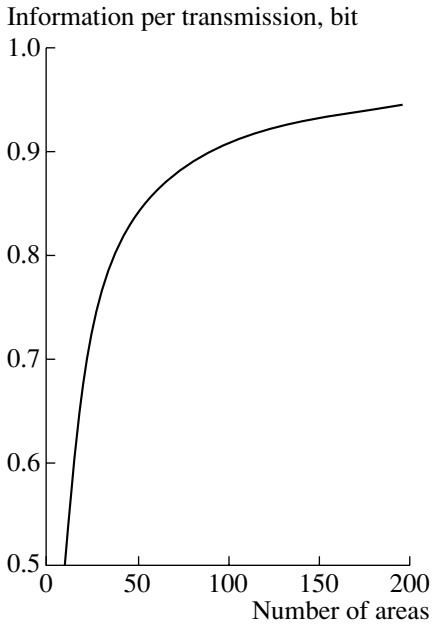

Fig. 3. Maximum amount of information per transmission versus the number of areas the Hilbert space is split into.

basis states is continuous; thus, it is necessary to split it into several approximately equal areas and count the bases that are similar, if they are in the same area on the Bloch sphere. Depending on the number of such areas, the mutual information in the Alice–Bob system per single transmission increases 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 an antisymmetric Bell state, the mutual selected information is equal to unity when one uses similar bases from Alice and Bob. If the bases from Alice and Bob are different, the amount of information in a single transmission will be less than unity. The calculated dependency of the maximum amount of information per single transmission versus the number of areas in which we split the Hilbert space is shown in Fig. 3.

We restrict the actions of Eve by the measurement of the probe state immediately after 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.

The information that Bob receives from Alice per complete message transmission after the bases reconciliation is shown in Fig. 2 (dashed line). The new critical value $\theta_0^{(2)}$ is larger than $\theta_0^{(1)}$, and, therefore, the critical error rates Q_0 and q_0 are 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. Accordingly, 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 data transmission have a typical finite level for the specific experimental QKD setup. Therefore, for the bases reconciliation, it is sufficient to increase the accuracy according to the external noise conditions up to a level that ensures an error rate less than the critical rate at which the QKD protocol guarantees 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 spaces for Bob and Alice ($D > 2$). In the multidimensional case, the maximum possible amount of mutual selected information is equal to $I_{\max}^D = \log_2 D$ and grows infinitely at $D \longrightarrow \infty$. The maximum possible amount of nonselected information is equal to the amount of accessible information [18]:

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

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

After bases reconciliation for Alice and Bob, the amount of information in the Alice–Bob system is given by the maximum possible selected information, whereas, in the Alice–Eve system, it is given by the maximum possible nonselected information, independently of the specific type of unitary transformation performed by Eve in the multidimensional case. Then, the critical CIER in the limit of $D \longrightarrow \infty$ is equal to unity:

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

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

The essential qualitative novelty of our QKD -protocol, which employs all states of the Hilbert space, is that it can work, in principle, with any imperfections or noise in the quantum channel (either internal or external) and has no any critical CIER value above 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 the CIER (Fig. 4). The question regarding Eve's transformation structure for performing optimal eavesdropping in the multidimensional case is essentially more difficult, but the result outlined above is qualitatively correct, despite the specific structure of Eve's transformation.

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

5. EXPERIMENTAL SETUP FOR A QKD PROTOCOL WITH CONTINUOUS ALPHABET

An experimental setup for our QKD protocol with a continuous alphabet whose letters are coded with photon polarizations s is shown in Fig. 5. In the notation

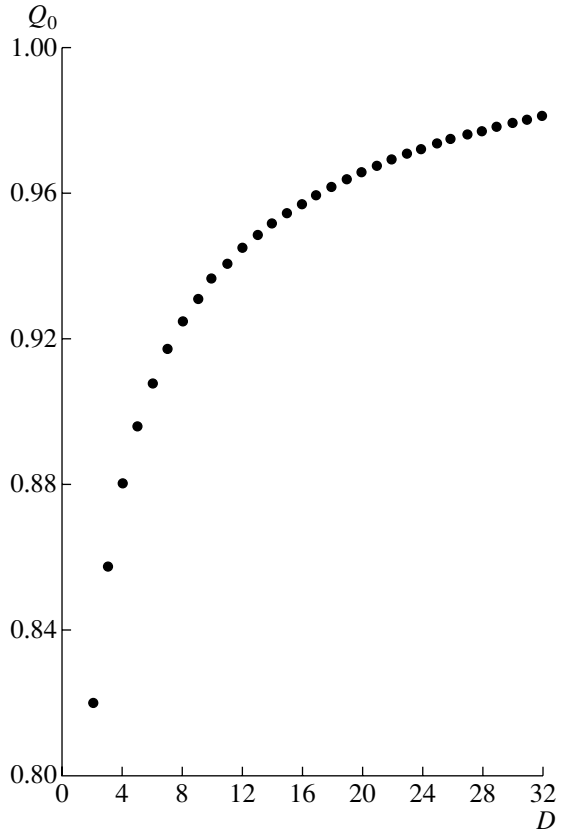

Fig. 4. Critical CIER Q_0 versus the dimensionality D of the Hilbert space.

given, a random letter in the alphabet corresponds to an arbitrary photon polarization.

At the Alice side of the QKD setup, random letters from the continuous alphabet are generated. The laser at this side generates single photons with determined polarization, which is rotated by a 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).

For the measurement in an arbitrary basis, Bob first rotates the polarization of the incident photon through the polarization plate to a random angle value and then performs measurement in the fixed basis.

Alice and Bob reconcile their bases states by exchanging nonsecure public information over a classical channel, for instance, a telephone line.

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 information with the help of several entangled qubits (photons). It is, however, experimentally difficult to generate, operate, and measure arbitrary states in mul-

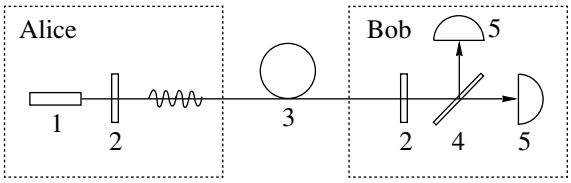

Fig. 5. Experimental setup for the QKD protocol with a continuous alphabet. At the Alice side, the laser (*1*) generates single photons whose polarization is rotated by the polarizator (*2*) at a random angle. These photons are transmitted to Bob via the quantum channel (*3*). The measurement part of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

tidimensional spaces; i.e., it is difficult to generate and operate multiple entangled photons.

6. CONCLUSIONS

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

In the 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 the multidimensional case is that it can work, in principle, for any imperfections or noise in the quantum channel (either internal or external) and does not have a critical bit error rate above which the protocol becomes insecure. For estimating Eve's intervention in data transmission through a quantum channel, we use a 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 QKD protocols.

The only restriction on Eve's strategy of eavesdropping is that she measures her probe state before the bases reconciliation. This restriction does not contradict the experimental realizations of the QKD -protocols; Alice and Bob need simply to reconcile their bases after the finite decoherence time in the quantum system. Obviously, such an experimental trick does not give a 100% guarantee of secure transmission, but, in real QKD schemes, it seems reasonable.

SPELL: 1. resend, 2. etters

ACKNOWLEDGMENTS

This work was partially supported by the Russian Foundation for Basic Research (project nos. 01-02-16311, 02-03-32200) and INTAS (grant no. INFO 00-479).

REFERENCES

1. N. Gisin, "Quantum Cryptography," Rev. Mod. Phys. **74**, 145 (2002).
2. S. Wiesner, "Conjugate Coding," SIGAT News **15**, 78 (1983).
3. Ch. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computer, System, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
4. Ch. H. Bennett, "Quantum Cryptography Using any Two Nonorthogonal States," Phys. Rev. Lett. **68**, 3121 (1992).
5. D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States," Phys. Rev. Lett. **81**, 3018 (1998).
6. F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," Phys. Rev. Lett. **88**, 057 902 (2002).
7. W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot Be Cloned," Nature **299**, 802 (1982).
8. D. Gottesman and Hoi-Kwong Lo, "Proof of Security of QKD with Two-Way Classical Communication," quant-ph/0105121 (2001).
9. C. A. Fuchs and A. Peres, "Quantum State Disturbance versus Information Gain: Uncertainty Relations for Quantum Information," Phys. Rev. A **53**, 2038 (1996).
10. R. G. Gallagher, *Information Theory and Reliable Communication* (Wiley, New York, 1968; Sovetskoe Radio, Moscow, 1974).
11. B. A. Grishanin, Probl. Peredachi Inf. **38**, 31 (2002).
12. B. A. Grishanin and V. N. Zadkov, "Measurement and Physical Content of Quantum Information," J. Commun. Technol. Electron. **47**, 933 (2002).
13. B. A. Grishanin, Izv. Akad. Nauk SSSR, Tekh. Kibern. **11**, 27 (1973).
14. J. Preskill, "Lecture Notes on Quantum Information," http://www.theory.caltech.edu/people/preskill/ph229/.
15. J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton Univ. Press, Princeton, N.J., 1955; Nauka, Moscow, 1964).
16. C. H. Bennett, G. Brassard, and J. M. Robert, "Privacy Amplification by Public Discussion," SIAM J. Comput. **17**, 210 (1988).
17. C. A. Fuchs, N. Gisin, R. B. Griffiths, *et al.*, "Optimal Eavesdropping in Quantum Cryptography. I. Information Bound and Optimal Strategy," Phys. Rev. A **56**, 1163 (1997).
18. C. M. Caves and C. A. Fuchs, Preprint (1996), quant-ph/9601025.