Critical error rate of quantum-key-distribution protocols versus the size and dimensionality of the quantum alphabet

Denis V. Sych,* Boris A. Grishanin, and Victor N. Zadkov
International Laser Center and Faculty of Physics, M. V. Lomonosov Moscow State University, 119899 Moscow, Russia
(Received 18 May 2004; published 30 November 2004)

A quantum-information analysis of how the size and dimensionality of the quantum alphabet affect the critical error rate of the quantum-key-distribution (QKD) protocols is given on an example of two QKD protocols—the six-state and ∞-state (i.e., a protocol with continuous alphabet) ones. In the case of a two-dimensional Hilbert space, it is shown that, under certain assumptions, increasing the number of letters in the quantum alphabet up to infinity slightly increases the critical error rate. Increasing additionally the dimensionality of the Hilbert space leads to a further increase in the critical error rate.

DOI: 10.1103/PhysRevA.70.052331 PACS number(s): 03.67.Dd, 03.65.Ta

I. INTRODUCTION

Since the idea of quantum cryptography was proposed first [1], a number of different quantum-key-distribution (QKD) protocols implementing it have been suggested [2–5]. Despite their diversity, all of them are based on a beautiful idea employing the basic "no-cloning" principle of quantum mechanics—the impossibility of copying arbitrary quantum states [6]. Thanks to this, an eavesdropper cannot intercept a quantum communication channel without disturbing a 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 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 a set of quantum states or a 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 a critical error rate that determines the protocol efficiency. By analyzing distortions in received messages, one can reveal an eavesdropping attack, but in order to establish a secure connection, one should also be able to resist such attacks. Therefore, one of the reasons for developing more QKD protocols is increasing their critical error rates.

All known QKD protocols [1,3,4] using carriers of information with a finite-dimensional Hilbert space are based on discrete quantum alphabets, i.e., with fixed number of letters. The first QKD protocol proposed in 1984 by Bennett and Brassard (BB84) [1] gives an example of a protocol in which *four* quantum incompatible states, setting two mutually nonorthogonal bases, are used. The alphabet of the six-state protocol [4] is composed of three mutually nonorthogonal bases $\{\{|0\rangle,|1\rangle\},\{(|0\rangle\pm|1\rangle)/\sqrt{2}\},\{(|0\rangle\pm i|1\rangle)/\sqrt{2}\}\}$ in a two-dimensional Hilbert space, which makes this protocol totally symmetrical on the Bloch sphere and leads to the fact that information characteristics, namely, the critical error rate, of the six-state protocol surpasses that of the BB84 protocol [4,7]. Further increasing the critical error rate, as was discussed in the literature [8–10], is basically connected with an increase in the dimension of the Hilbert space of the quantum channel.

In the two-dimensional case, there is a commonly accepted opinion that the six-state protocol has the best efficacy [11] (however, there is no proof of this statement for all possible eavesdropping strategies). In this paper, we clarify whether increasing the number of letters in the alphabet in a Hilbert space of fixed dimension could improve the QKD protocol efficacy or not. In other words, can we surpass the six-state protocol efficacy, even in the two-dimensional case, due to an increase in the number of letters, or not?

In order to answer this question, we introduce a QKD protocol that has procedures similar to standard QKD protocols (for instance, the six-state protocol), but it employs all arbitrary superpositions of orthogonal basis states that form the continuous alphabet. By analogy with the six-state protocol, we will call such a protocol the ∞-state protocol. The efficacy of the ∞-state protocol can be calculated as for other QKD protocols with the help of a regular information analysis based on the calculation of the mutual Shannon information between different two-partite subsystems of the tripartite system Alice-Eve-Bob [12].

The paper is organized as follows. In Sec. II, we outline some specific properties of the ∞-state protocol and give the basic concept and key mathematical formalism of the compatible information in application to the quantum-information analysis of arbitrary QKD protocols. In Sec. III, we provide a comparative quantum-information analysis of the six-state and ∞-state QKD protocols. The benefits of using Hilbert spaces with arbitrary dimension in QKD protocols are considered in Sec. IV. We conclude the paper by summarizing the results and discussing the possibilities of experimental realization in Sec. V.

II. SPECIFIC PROPERTIES OF THE ∞-STATE QKD PROTOCOL

In the following, we assume that before eavesdropping the Alice-Bob system is described entirely by a totally entangled pair of photons [13].

*Electronic address: sych@comsim1.phys.msu.ru

In other words, we will analyze the Einstein-Podolsky-Rosen (EPR) version of QKD protocols, which is similar to the Ekert version of the BB84 protocol [2]. Obviously, such a representation of QKD protocols is equivalent to the case where Alice simply transmits single photons to Bob, without any source of EPR pairs.

From a theoretical point of view, the key difference in the analysis of the ∞-state protocol and of QKD protocols with discrete alphabets lies in the calculation of the amount of information that can be encoded with the help of a continuous alphabet. A natural quantitative measure for the amount of information is the standard mutual Shannon information functional of the classical input-output (Alice-Bob) joint probability distribution P_{AB}:

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

where $S[P]$ is the classical Shannon entropy functional for the joint, $P=P_{AB}$, and marginal, $P=P_A, P_B$, probability measures [14].

The specifics of a continuous alphabet is apparent in the calculation of the joint probability distribution, defined on a continuous set of elementary quantum events, which can be determined by the wave functions or the state vectors of the quantum-information system. Mathematically, a set of elementary events can be chosen by defining a set of positive operators, $\hat{E}_\nu = |\nu\rangle\langle\nu|$, representing a nonorthogonal expansion of the unit operator [15] or the positive operator-valued measure [16]:

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

In our case, when the information exchange between two quantum systems employs all states of the Hilbert space, expansion (2) transforms into a continuous nonorthogonal expansion of the form [17]

$$\hat{1} = \int_\nu |\nu\rangle\langle\nu| dV_\nu, \tag{3}$$

where dV_ν is the volume differential normalized to the dimension of Hilbert space $D: \int dV_\nu = D$. The corresponding joint probability distribution has the form

$$P_{AB}(d\alpha, d\beta) = \mathrm{Tr}_{\mathrm{AB}}\{[\hat{E}_A(d\alpha) \otimes \hat{E}_B(d\beta)]\hat{\rho}_{AB}\}, \tag{4}$$

where $\hat{E}_{A,B}(d\nu) = |\nu\rangle_{A,B}\langle\nu|_{A,B} dV_\nu$, and defines the so-called *nonselected* compatible information [17,18]:

$$I_{AB} = \int_\alpha \int_\beta P_{AB}(d\alpha, d\beta) \log_2 \frac{P_{AB}(d\alpha, d\beta)}{P_A(d\alpha) P_B(d\beta)}. \tag{5}$$

In the case of information exchange between two quantum systems via an arbitrary discrete quantum alphabet, expansion (2) is defined by a specific set of quantum letters composing a specific quantum alphabet.

From a practical point of view, the most significant difference between a QKD protocol with continuous alphabet and QKD protocols with discrete alphabets lies in the basis reconciliation procedure. In QKD protocols with discrete alphabets, Alice and Bob perform *exact* basis reconciliation, i.e., after the transmission of all messages, they select only that part of the messages for which they have used the same information bases.

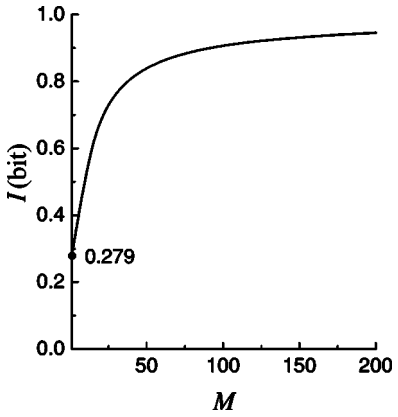

FIG. 1. The amount of information I per transmission versus the number of areas M in which the two-dimensional Hilbert space of states is split.

In contrast to a discrete alphabet, one cannot perform an exact basis reconciliation procedure for the ∞-states protocol, because one needs to transmit an infinite amount of information about a point from the continuum. Therefore, we propose to apply an *approximate* bases reconciliation procedure for the ∞-states protocol, which is outlined below.

Let us split the continuous alphabet into several equal, possibly partially overlapping, areas that are composed of approximately equal quantum letters. During the basis reconciliation procedure, Alice and Bob transmit the number of the area to which the information basis belongs and then, if they belong to the same area, decide that they used equal bases.

Clearly, such approximate basis reconciliation procedure causes additional errors, or *internal noise*, in the transmitted message due to the differences between the quantum letters of the same area. However, the smaller the size of the areas we select, the smaller such errors. We can calculate how the amount of information I in a single transmitted qubit depends on the number of areas M in which we split the Hilbert space with the help of the quantum-compatible-information technique outlined above.

To do that, let us split the Bloch sphere into equal, for simplicity round, areas, which partially overlap each other. After basis reconciliation, the letters of Alice and Bob belong to the same area and continuously fill it. Therefore, a set of elementary events related to the Alice-Bob system can be represented after basis reconciliation with the help of continuous expansion of the unit operator for the collection of areas that include the points corresponding to the basis vectors. The respective amount of information I_{AB} for the approximate basis reconciliation depends on the size of the area or, in fact, on the number of areas we split the Hilbert space into. This dependency is shown in Fig. 1.

With increasing total number of areas (or decreasing their size, respectively), I_{AB} changes from $\simeq 0.279$ to 1 bit. At $M=1$, i.e., when the quantum alphabet is composed of only one area and, therefore, basis reconciliation *de facto* van-

ishes, the amount of information is equal to the accessible information $I_{AB} \simeq 0.279$ bit [17,19]. With increasing number of areas up to $M=100$ we get $I_{AB} \simeq 0.9$ bit and in the limit of $M \to \infty$ we have the *a priori* evident result $I_{AB} \to 1$ bit. In other words, in order to ensure high values of I_{AB} one needs just to select an essential number of areas $M < \infty$ [20].

Note that reduction of the area size leads to increasing the number of areas we split the Hilbert space into and, therefore, to the corresponding increase of the additional information on the number of areas transmitted via a public channel during the basis reconciliation. The number of messages selected after the basis reconciliation procedure also decreases proportionally to the size of the area. Increase of accuracy in the basis reconciliation increases the total traffic in both quantum and classical channels. For transmission of the given amount of secure information it will be higher than those of protocols with discrete alphabets. In practice, however, there is no need for infinite increase of the accuracy in the basis reconciliation because there always exists an external noise in the experimental setup; it is enough to choose a reasonable level of accuracy appropriate for every specific case in accordance with Fig. 1.

One more specificity of the ∞-states protocol, which follows directly from the approximate basis reconciliation procedure, is how to estimate the level of Eve's interference. One of the characteristics most accepted in the literature for estimation of Eve's interference is the quantum bit error rate (QBER). It was suggested to characterize the error rate in the sifted key and it is defined as follows:

$$Q = 1 - \frac{N}{N_{\max}}, \tag{6}$$

where N is the number of correctly transmitted letters and $N_{\max}$ is the total number of transmitted letters. Using this definition of the QBER implies an assumption that without eavesdropping Q is equal to zero. Obviously, the QBER for an ideal quantum channel without noise is equal to zero and one can use the QBER for estimation of Eve's interference.

However, in the case of the ∞-states protocol, when due to the approximate basis reconciliation we have information per message less than a whole bit, and Q is not equal to zero even without eavesdropping, we cannot use the QBER characteristic for estimation of eavesdropping. In this case, the QBER as it has been defined previously simply does not reflect the real level of Eve's interference because it equally takes into account both an external noise due to the possible eavesdropping and internal noise due to the QKD protocol specifics, namely, the approximate basis reconciliation.

In order to resolve this contradiction with the definition of the QBER (see also Ref. [21]), we suggest using another characteristic for the error rate, which correctly reflects the degree of Eve's interference for an arbitrary QKD protocol. Let us define the fidelity of data transmission not as the relative number of correctly transferred letters, but as the relative amount of correctly transferred information. Then, the error rate can be defined as

$$\tilde{Q} = 1 - \frac{I}{I_{\max}} \in [0,1], \tag{7}$$

where I is the amount of information per one message with the presence of eavesdropping and $I_{\max}$ is its maximal possible value without eavesdropping. We will call this measure, by analogy with the QBER, the *mutual information error rate* (MIER).

By contrast with the QBER, the MIER correctly reflects the degree of Eve's interference for an arbitrary QKD protocol—with either the exact or approximate basis reconciliation procedure. In absence of any noise both measures QBER and MIER have the same value, $Q=\tilde{Q}=0$, which correctly reflects the *a priori* expected value. However, in the case of maximal interference by Eve, these measures are significantly different: $Q=0.5$ when $\tilde{Q}=1$, which is due to the different definitions of the error rate measures.

In the following, when it is not indicated otherwise, we will use either the MIER as the most adequate measure of Eve's interference or the QBER under the limiting assumption that the bases for the ∞-states protocol are reconciled exactly.

III. COMPARISON OF THE SIX-STATE AND ∞-STATE QKD PROTOCOLS

For determining the critical error rate in the transmitted message up to which a QKD protocol ensures security of the transmitted data one needs generally to prove absolute security of the QKD protocol [22,23]. However, in this work we are not going in for the ultimate security proof, but perform just a *comparative* analysis of one of the best six-state protocols until now with the ∞-state one. We will limit our consideration by considering only two key strategies of eavesdropping—intercept-resend and optimal eavesdropping and will compare the corresponding critical error rates for these two QKD protocols.

A. Intercept-resend strategy of eavesdropping

One of the simplest strategies of eavesdropping is the intercept-resend strategy [12] when Eve measures a message transmitted over a secure channel in an arbitrary orthogonal basis and then transmits to Bob the results of this measurement. It is clear that using such a strategy Eve knows exactly the information received by Bob and therefore secure data transmission between Alice and Bob is impossible. Therefore, the maximal possible level of errors which can be corrected so that the transmission is a secure one does not exceed the level of errors caused by the intercept-resend strategy of eavesdropping. As a result, calculation of the error rate due to this strategy of eavesdropping gives an upper bound of the protocol efficacy at any applied strategy of eavesdropping.

In order to determine the error rate, Alice randomly selects some messages after the basis reconciliation and informs Bob over a public channel which specific states have been transmitted. Bob then replies to Alice over the same public channel which states he has received. The ratio of

incorrectly and correctly transmitted characters between Alice and Bob in the messages they disclosed gives us the error rate. Random sampling used for calculation of the error rate assures that in the remaining messages the error rate is approximately the same. In the following, disclosed messages are discarded and not used for obtaining the key.

Let us assume that Alice and Bob found that Alice transmitted to Bob state $|\alpha\rangle$. Let us further assume that Eve used an orthogonal basis $\{|\psi\rangle,|\psi_\perp\rangle\}$ to eavesdrop the information. Then, Eve measured the information resulting in either $|\psi\rangle$ with probability $|\langle\psi|\alpha\rangle|^2$ or $|\psi_\perp\rangle$ with probability $|\langle\psi_\perp|\alpha\rangle|^2$ and transmitted the resulting state to Bob. After measurement of the states $|\psi\rangle$ and $|\psi_\perp\rangle$ in the basis $\{|\alpha\rangle,|\alpha_\perp\rangle\}$ Bob receives the correct result (state $|\alpha\rangle$) with probabilities $|\langle\psi|\alpha\rangle|^2$ and $|\langle\psi_\perp|\alpha\rangle|^2$, respectively, and incorrect result (state $|\alpha_\perp\rangle$) with probabilities $|\langle\psi|\alpha_\perp\rangle|^2$ and $|\langle\psi_\perp|\alpha_\perp\rangle|^2$. The total probability of getting the correct result $|\alpha\rangle$ by Bob is equal to $F_{\alpha\psi}=|\langle\psi|\alpha\rangle|^4+|\langle\psi_\perp|\alpha\rangle|^4$. Correspondingly, the probability of getting the wrong result is equal to $Q_{\alpha\psi}=1-F_{\alpha\psi}$.

In order to get the QBER Q, one needs to average $Q_{\alpha\psi}$ over all Alice's bases $\{\alpha\}$ and minimize then the result of averaging over Eve's bases $\{\psi\}$:

$$Q=\frac{1}{N_\alpha N_\psi}\sum_{\{\alpha\}}\sum_{\{\psi\}}Q_{\alpha\psi}, \tag{8}$$

where N_α and N_ψ are the numbers of bases in Alice's and Eve's alphabets, respectively. Averaging in the QKD protocol with continuous alphabet implies integration instead of summation.

Calculating Q, we get $Q_{\text{six-state}}=Q_{\infty\text{-state}}=1/3$. Note that this result does not depend on the bases in which Eve performs the measurements due to the total symmetry of the considered QKD protocols.

B. Optimal eavesdropping strategy

It has been proved that in one-way communication schemes, when only Alice can send qubits to Bob, a secure connection between Alice and Bob is possible if the amount of information Bob received from Alice exceeds the information Eve received from either Alice or Bob [24]. This condition can be written as

$$I_{AB}>\max(I_{AE},I_{BE}). \tag{9}$$

We will call Eve's eavesdropping strategy *optimal* if Eve extracts from the transmitting message maximum information at the given level of interference, which causes the corresponding level of errors (note that this can differ from the optimal cloning of the transmitted message [25]).

If the transformation performed by Eve is nonunitary, then it corresponds to a unitary transformation in an extended quantum system with subsequent averaging over some variables, which gives Eve no additional information and creates no additional problems for Alice and Bob. Therefore, we can assume (without reducing the generality of our consideration) that at optimal eavesdropping Eve performs a unitary transformation U_{BE} on the state transferred from Alice to Bob $|\beta\rangle_B$ and Eve's probe state $|0\rangle_E$, which can be written as

$$|0\rangle_B|0\rangle_E \xrightarrow{U_{BE}} |0\rangle_B|\Phi_{00}\rangle_E+|1\rangle_B|\Phi_{01}\rangle_E,$$

$$|1\rangle_B|0\rangle_E \xrightarrow{U_{BE}} |0\rangle_B|\Phi_{10}\rangle_E+|1\rangle_B|\Phi_{11}\rangle_E. \tag{10}$$

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

$$\langle\Phi_{00}|\Phi_{10}\rangle+\langle\Phi_{01}|\Phi_{11}\rangle=0,$$

$$|\Phi_{00}|^2+|\Phi_{01}|^2=|\Phi_{10}|^2+|\Phi_{11}|^2=1. \tag{11}$$

Taking into account conditions (11) and due to the symmetry of the alphabets of the considered QKD protocols, we can present a set $|\vec{\Phi}\rangle$ of all the states $|\Phi_{ij}\rangle$ as the following superposition of only two basis states $|0\rangle_E$, $|1\rangle_E$:

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

where the transformation coefficients are determined via the two angles θ,φ controlled by Eve:

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

The initial state of the quantum system Alice-Bob-Eve $\hat{\rho}^{(1)}_{ABE}=\hat{\rho}^{(1)}_{AB}\otimes|0\rangle_E\langle 0|_E$, which is described by the tensor product of the maximally entangled pair Alice-Bob and the initial Eve state $|0\rangle_E\langle 0|_E$, after transformation by optimal eavesdropping (10), is transferred into the final three-partite state $\hat{\rho}^{(2)}_{ABE}$ that is an entangled state of Alice, Bob, and Eve: $\hat{\rho}^{(1)}_{ABE}\xrightarrow{U_{BE}}\hat{\rho}^{(2)}_{ABE}$.

The resulting bipartite Alice-Bob, Alice-Eve, and Bob-Eve density matrices obtained by averaging of the density matrix $\hat{\rho}^{(2)}_{ABE}$ over the third system enable us to calculate the respective mutual information amounts:

$$\hat{\rho}^{(2)}_{AB}=\mathrm{Tr}_E\hat{\rho}^{(2)}_{ABE}\rightarrow I_{AB},$$

$$\hat{\rho}^{(2)}_{AE}=\mathrm{Tr}_B\hat{\rho}^{(2)}_{ABE}\rightarrow I_{AE}, \tag{13}$$

$$\hat{\rho}^{(2)}_{BE}=\mathrm{Tr}_A\hat{\rho}^{(2)}_{ABE}\rightarrow I_{BE}.$$

The optimal eavesdropping condition, which must be checked, can be written as

$$I_{AE,BE}=\max_{I_{AB}=\text{const}} I_{AE,BE}, \tag{14}$$

where Eve can vary the parameters θ and φ.

Comparing results for the Alice-Bob, Alice-Eve, and Bob-Eve mutual information (I_{AB}, I_{AE}, and I_{BE}, respectively) calculated with the help of Eqs. (10) and (13) versus the parameters θ and φ controlled by Eve, one can easily show that for all values of θ,φ we have $I_{AE}\geqslant I_{BE}$; thus we will not discuss I_{BE} in the following.

The dependencies of the mutual information I_{AB} and I_{AE} on the parameters θ and φ can be properly displayed in the

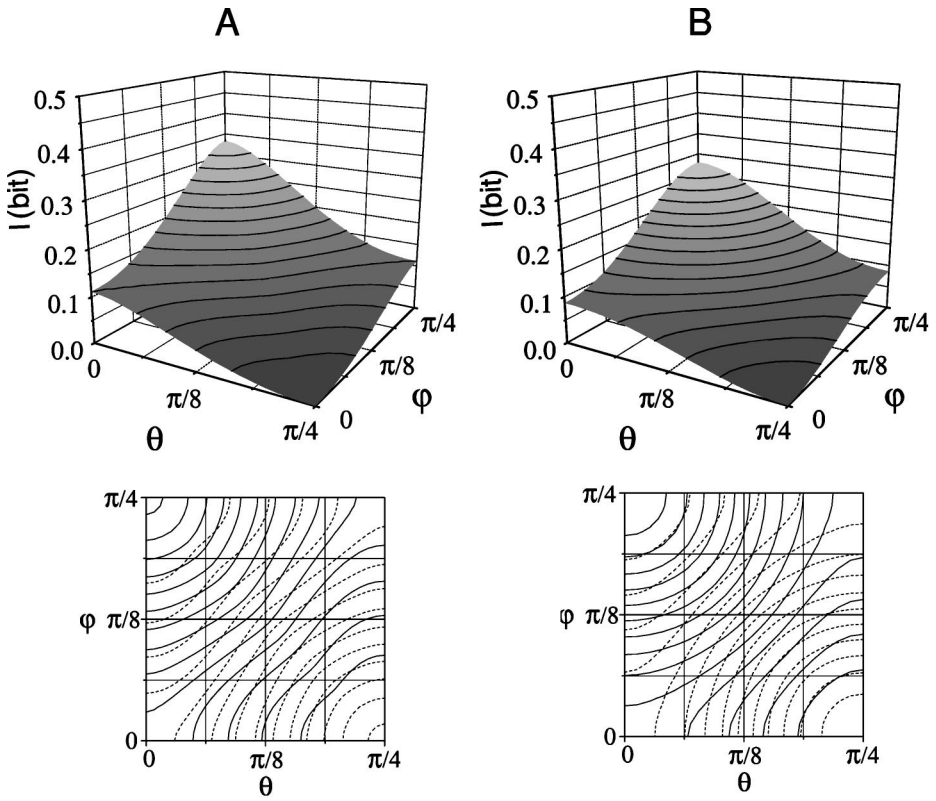

FIG. 2. Alice-Bob mutual Shannon information I_{AB} versus Eve's eavesdropping parameters θ, φ as 3D (upper row) and contour plots (bottom row, solid lines) for the six-state QKD protocol (a) and QKD protocol with continuous alphabet (b). Dashed lines in the bottom figures correspond to the Alice-Eve mutual Shannon information I_{AE} (dashed lines are symmetrical to solid lines with respect to the line $\theta=\varphi$).

form of three-dimensional plots. Keeping in mind that I_{AE} is symmetrical with I_{AB} regarding $\theta=\varphi$, upper plots in Fig. 2 show only the I_{AB} plot. One can easily see that I_{AB} reaches its maximum values 0.333 and 0.279 bit in the upper left corner of the three-dimensional (3D) plot $(\theta=0,\varphi=\pi/4)$ for the six-state and ∞-state protocols, respectively. The minimum value of I_{AB} is equal to zero and is reached in the right bottom corner of the 3D plots $(\theta=\pi/4,\varphi=0)$ for both protocols.

For analysis of the optimal eavesdropping condition (14) it is conventional to show the dependencies I_{AB} and I_{AE} on the same plot, which is done in the bottom plots on Fig. 2 where these dependencies are presented as contour plots (solid and dashed lines correspond to equidistant levels of $I_{AB}=$const and $I_{AE}=$const, respectively). Analysis of these contour plots shows that the optimal eavesdropping condition (14), when Eve reaches the maximum of $I_{AE}=I_{AE}(\theta,\varphi)$ at a given level of $I_{AB}=I_{AB}(\theta,\varphi)$, is achieved at $\theta=\pi/4-\varphi$.

Due to the symmetry $I_{AB}(\theta,\varphi)=I_{AE}(\varphi,\theta)$, the security condition $I_{AB}>I_{AE}$ is satisfied up to a certain critical level $\theta_0^{(1)}=\varphi_0^{(1)}=\pi/8$, at which information retrieved by Eve is equal to the information received by Bob. At this critical point, the critical error rate $\tilde{Q}_0$ is equal to 0.63 and 0.60 for the six-state and ∞-state protocols, respectively.

Up to now, we analyzed the case when Alice and Bob do not perform a basis reconciliation, which can essentially increase the critical error rate and improve the stability of the QKD protocol at a higher level of Eve's interference.

Let us now assume that Alice and Bob use the *safety* basis reconciliation procedure. Safety means that Eve does not affect selection of data by Alice and Bob during this procedure, does not generate false messages in the public insecure channel, and does not use any additional transformations of her probe state after the basis reconciliation. In other words, she gains no additional information from the basis reconciliation procedure. Justification of the assumptions about safety basis reconciliation is based on the following.

First, the assumptions made suit well the reality of up-to-date technologies and look reasonable from the physical point of view. In order to retrieve additional information from basis reconciliation, Eve has to have unlimited quantum memory, which allows storing of the intercepted quantum information infinitely long. At the up-to-date level of experimental techniques in this field, this is impossible to implement. Any imperfections in storing of the intercepted quantum information lead inevitably to decoherence and, correspondingly, to loss of information. If the legitimate parties of the QKD protocol (Alice and Bob) make a pause between data transmission and basis reconciliation that exceeds the typical decoherence time in the system, then the basis reconciliation will not give any additional information to Eve.

Second, though the assumption that Eve does not retrieve additional information from the basis reconciliation is definitely a limitation, it is, however, equally applicable to analy-

TABLE I. Critical error rate $\tilde{Q}_0$ for the six-state and ∞-state QKD protocols with and without basis reconciliation.

QKD protocol	Without reconciliation of bases	With reconciliation of bases
Six-state	0.630	0.806
∞-state	0.600	0.811

sis of both QKD protocols of interest. Calculated critical error rates with limitations on eavesdropping strategies do not serve then as absolute security criterions, but as long as our goal is to compare different QKD protocols with the same reasonable restrictions on Eve's strategies, this analysis seems to be suitable for this purpose.

After such safety basis reconciliation, information received by Bob from Alice proportionally increases by contrast with the case when no basis reconciliation is made, and reaches its maximum value of 1 bit per message (in the limit of exact basis reconciliation for the ∞-state QKD protocol). The contour plots in Fig. 2 remain the same, only the values of information in the Alice-Bob system change. Information in the Alice-Eve system remains the same due to the assumption made.

After the basis reconciliation, the security condition $I_{AB} > I_{AE}$ is satisfied up to a certain critical value $\theta_0^{(2)} = \varphi_0^{(2)}$, depending on the specific protocol, different from the value $\theta_0^{(1)} = \varphi_0^{(1)}$ corresponding to the case without basis reconciliation. Also, the critical error rate $\tilde{Q}_0$ becomes significantly higher and is equal to 0.806 and 0.811 for the six-state and ∞-state QKD protocols, respectively.

The calculation results for the critical error rate are summarized in Table I.

We do not consider the case of two-way communication, when one is capable of establishing a secure connection even at $\tilde{Q} > \tilde{Q}_0$ [12]. Then, at error rates exceeding critical, i.e., at $\tilde{Q} > \tilde{Q}_0$, the QKD protocol does not ensure the security of the transmitted data and the transmission session is not established. So, the higher the critical error rate $\tilde{Q}_0$, the more stable is the QKD protocol to eavesdropping attacks, because it allows a higher level of interference.

Summarizing, our information analysis shows that without basis reconciliation the six-state protocol has the best maximum value of the critical error rate. However, after the safety basis reconciliation procedure applied we see that the ∞-state protocol has a higher critical error rate in comparison with the six-state protocol. In other words, the information characteristics of the six-state protocol can be surpassed even in the case of a two-dimensional Hilbert space due to the enlarging of the alphabet used.

IV. MULTIDIMENSIONAL CASE

In this section, we will discuss the potential of using multidimensional Bob and Alice Hilbert spaces ($D > 2$) for improving the properties of the QKD protocols, which is especially promising for the ∞-state QKD protocol. For the upper estimate of the multidimensional protocol efficacy we will calculate, by analogy with the two-dimensional case, errors caused by the intercept-resend strategy.

Let us consider a quantum alphabet, consisting of L_D mutually unbiased bases in D-dimensional Hilbert space, i.e., alphabet, different letters of which have equal projections onto each other. For such alphabet we will calculate now the accuracy of transmitting an arbitrary letter when Eve uses the intercept-resend eavesdropping strategy.

First, Alice transmits to Bob a random letter from a randomly selected basis. If Eve guesses this basis correctly, the letter will be transmitted to Bob without distortion: this scenario happens with the probability $1/L_D$. Otherwise, if Eve does not guess the right basis (it happens with the probability $1-1/L_D$), then the letter transmitted to Bob will be replaced by Eve during resending with equal probability (due to the above suggestion of the alphabet symmetry) by a different one from another basis. Bob receives the right letter, which was transmitted by Alice, with the probability $1/D$; otherwise he receives a wrong letter.

The total probability that Eve does not distort the letter transmitted by Alice (when Eve correctly or incorrectly guesses the basis) is equal to $F_D = 1/L_D + (1-1/L_D)/D$ and the corresponding probability to distort the letter is equal to

$$Q_D = 1 - F_D = 1 - \frac{1}{L_D}\left(1 + \frac{L_D - 1}{D}\right). \tag{15}$$

Checking this formula for the BB84 ($L_D = 2, D = 2$) and six-state ($L_D = 3, D = 2$) protocols, we get the well-known numbers $1/4$ and $1/3$, respectively.

In the limit of $D \to \infty$, we get $Q_D \to 1 - 1/L_D$. This means that alphabets with higher numbers L_D of mutually unbiased letters are more favorable. For the maximum number $D+1$ of mutually unbiased bases in D-dimensional space [26] we get the 100% error rate

$$Q_\infty = \lim_{D\to\infty} Q_D = 1 - \lim_{D\to\infty} \frac{1}{D}\left(1 + \frac{D}{D}\right) = 1, \tag{16}$$

by contrast with the 50% for the two-dimensional case. This is due to the fact that in the two-dimensional case nonguessing a letter by Bob means guessing the opposite letter and if the error rate $Q_2^{(1)} > 0.5$ then Bob can simply replace all "0" in the message with "1" and vice versa, achieving $Q_2^{(2)} = 1 - Q_2^{(1)} < 0.5$. In multidimensional case, this trick does not work—the higher the dimensionality of the Hilbert space, the higher the maximum possible error rate.

Therefore, one can conclude from the ratio (16) that there are no restrictions in principle on increasing the efficacy of the QKD protocols with increasing dimensionality of the Hilbert space because there is no nontrivial upper threshold set by the intercept-resend strategy.

Keeping these specifics of QKD protocols with multidimensional alphabets, let us consider now the MIER for an extension of the ∞-state protocol onto the case of multidimensional Hilbert spaces.

Note that in the multidimensional case, the maximum possible selected information between two systems $I_{\max}^D = \log_2 D$ grows infinitely at $D \to \infty$ whereas the maximum

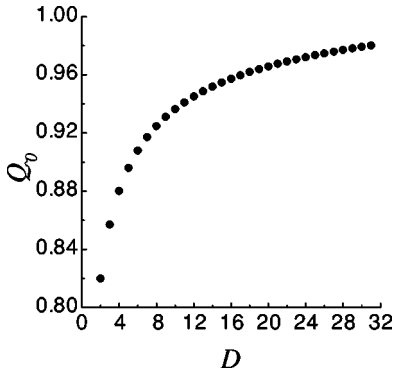

FIG. 3. Critical error rate $\tilde{Q}_0$ versus the dimension D of the Hilbert space.

possible nonselected information is bounded: it is equal to the amount of *accessible* information [19]

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

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

In the case when Eve does not extract additional information from the basis reconciliation procedure and disengage herself from a specific eavesdropping strategy, we can estimate the upper limit of the maximum amount of nonselected information that is received by Eve by the accessible information. In fact, the information received by Eve will be even smaller.

The amount of information in the systems Alice-Bob and Alice-Eve after the basis reconciliation procedure is given by the maximum possible selected or nonselected information in the system, respectively. Then the critical mutual information error rate (7) in the limit $D\to\infty$ is equal to unity,

$$\tilde{Q}_0^{\infty} = 1 - \lim_{D\to\infty}\frac{I^D_{\text{accessible}}}{I^D_{\max}} = 1 - \lim_{D\to\infty}\frac{0.61}{\log_2 D} = 1. \qquad (17)$$

The critical mutual information error rate $\tilde{Q}_0$ calculated by formula (17) versus the dimensionality of the Hilbert space is shown in Fig. 3. This result shows a qualitatively different property of the multidimensional ∞-state protocol with respect to the two-dimensional case: with increasing dimensionality of the Hilbert space the critical error rate increases and in the limit of infinite-dimensional space the protocol becomes nonthreshold.

Such behavior of the critical error rate does not depend on the specific structure of eavesdropping by Eve and can be clarified as follows. When Alice sends a message, then both Eve and Bob have *a priori* minimal information about this message being "maximally entangled" in the multidimensional space. After basis reconciliation, Alice and Bob can select only maximally correlated messages for which they choose approximately similar bases. As a result, information connectivity between Alice and Bob per one message will be significantly improved. Eve, in her turn, cannot affect the processes of message selection and her information remains the same. Therefore, Eve with increasing dimensionality of the Hilbert space retrieves much less information than Bob, which leads finally to the nonthreshold property of the QKD protocol with a continuous alphabet. In the reasoning above, we have made only an assumption about safety basis reconciliation, which was argued in Sec. III B.

V. CONCLUSIONS

In conclusion, it is shown that use of a continuous alphabet in the case when an eavesdropper has no ability to store an intercept information in a quantum form leads potentially to a slightly higher critical error rate than that of the six-state protocol, even in the two-dimensional case.

With increasing dimensionality of the Hilbert space the critical error rate for the ∞-state protocol increases, and in the limit of infinite-dimensional space the protocol becomes nonthreshold. This promising property could, in our view, stimulate efforts in experimental implementation of this protocol.

In the case of two-dimensional Hilbert space, the ∞-state QKD protocol can be experimentally implemented with the help of the standard QKD schemes, based on coding a qubit with photon polarization. Demonstration of the nonthreshold property of the infinite-dimensional ∞-state QKD protocol will, however, require some novel experimental solutions.

ACKNOWLEDGMENTS

This work was partially supported by RFBR Grants No. 02-03-32200, No. 04-02-17554, and by INTAS Grant No. INFO 00-479.

[1] Ch. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computer, System and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[2] A. K. Ekert, Phys. Rev. A **67**, 661 (1991).
[3] Ch. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[4] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
[5] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[6] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[7] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[8] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[9] M. Bourennane, A. Karlsson, and G. Bjork, Phys. Rev. A **64**, 012306 (2001).
[10] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[11] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003); e-print quant-ph/0105121.
[12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[13] The most straightforward description of the information system Alice-Bob, which clearly reflects an experimental implementation of the QKD scheme, is a semiclassical description with the density matrix $\hat{\rho}_B(\alpha)$ of Bob that depends on the classical parameter α corresponding to the state $|\alpha\rangle$ transmitted by Alice. However, the description of the Alice-Bob system as an entangled pair of states has definite methodological benefit as it allows one to equally describe all the participants of the information exchange in the system Alice-Eve-Bob as peering parties.
[14] R. G. Gallagher, *Information Theory and Reliable Communication* (John Wiley and Sons, New York, 1968).
[15] B. A. Grishanin, Izv. Akad. Nauk SSSR, Tekh. Kibern.. **11**, 127 (1973); e-print quant-ph/0301159
[16] J. Preskill, http://www.theory.caltech.edu/people/preskill/ph229/
[17] B. A. Grishanin and V. N. Zadkov, J. Commun. Technol. Electron. **47**, 933 (2002).
[18] B. A. Grishanin, Probl. Inf. Transm. **38**, 26 (2002).
[19] C. M. Caves and C. A. Fuchs, e-print quant-ph/9601025.
[20] The fact that there are no limitations in principle on the physically allowed complexity of the basis reconciliation procedure allows us in the following to use the value $M=\infty$ for the number of areas for the estimation of the maximal error rate of the QKD protocol.
[21] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[22] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[23] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[24] C. H. Bennett, G. Brassard, and J. M. Robert, SIAM J. Comput. **17**, 210 (1988).
[25] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[26] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).