Comparative characteristics of quantum key distribution protocols with alphabets corresponding to the regular polyhedrons on the Bloch sphere

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

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

ABSTRACT

Possibilities of improving characteristics of quantum key distribution (QKD) protocols via variation of character set in quantum alphabets are investigated. QKD protocols with discrete alphabets, letters of which form regular polyhedrons on the Bloch sphere (tetrahedron, octahedron, cube, icosahedron, and dodecahedron, which have 4, 6, 8, 12, and 20 vertexes), and QKD protocol with continuous alphabet, which corresponds to the limiting case of a polyhedron with infinitive number of vertexes, are considered. Stability of such QKD protocols to the intercept-resend and optimal eavesdropping strategies at the individual attacks, is studied in detail. It is shown that in case of optimal eavesdropping strategy, after safety bases reconciliation, critical error rate of the QKD protocol with continuous alphabet surpasses all other protocols. Without basis reconciliation the highest critical error rate have the protocol with tetrahedron-type alphabet.

Keywords: Quantum information, quantum cryptography, quantum key distribution

1. INTRODUCTION

Since 1970s, when 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 a basic "no-cloning" principle of quantum mechanics—impossibility of copying arbitrary quantum states [6]. 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 a critical error rate 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. Therefore, one of the reasons for developing novel QKD protocols is increasing their critical error rates.

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

In two-dimensional case, there is a commonly accepted opinion that six-state protocol has the best efficacy [11]. However, there is no proof of this statement for all possible eavesdropping strategies and in this paper we will clarify

*E-mail: sych@comsim1.phys.msu.ru

whether increasing the number of letters in the alphabet in the Hilbert space of fixed dimension could improve the QKD protocol efficacy or not. In other words, whether we could surpass six-state protocol efficacy, even in two-dimensional case, due to the increasing the number of letters in the alphabet or not?

In order to answer this question, we introduce QKD protocols with discrete alphabets, letters of which form regular polyhedrons on the Bloch sphere (tetrahedron, octahedron, cube, icosahedron, and dodecahedron, which have 4, 6, 8, 12, and 20 vertexes), and QKD protocol with continuous alphabet, which corresponds to the limiting case of a polyhedron with infinitive number of vertexes. By analogy with well known six-state protocol, we will call such protocols 4-, 6-, 8-, 12-, 20-, and ∞-state protocols. Their efficacy can be calculated the same way as for other standard QKD protocols, i.e. with the help of regular information analysis based on 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 Section 2, we outline 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 Section 3 we provide a comparative quantum-information analysis of the considered QKD protocols. Future trends of using Hilbert spaces with arbitrary dimension in QKD protocols are considered in Section 4. We conclude the paper by summarizing the results and discussing possibilities of experimental realization in Section 5.

2. SPECIFIC PROPERTIES OF THE ∞-STATE QKD PROTOCOL

In the following, we assume that before eavesdropping Alice–Bob system is described entirely by a totally entangled pair of photons.[†] In other words, we will analyze EPR version of the QKD protocols, which is similar to the Eckert's version of the BB84 protocol [2]. Obviously, such representation of the QKD protocols is equivalent to the variance when Alice simply transmits to Bob single photons, without any source of EPR pairs.

From theoretical point of view, key difference in analysis of ∞-state protocol and QKD protocols with discrete alphabets lies in calculation of the amount of information that can be encoded with the help of 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 [13].

Specific of continuous alphabet is shown up in calculation of the joint probability distribution, defined on the 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 choice of a set of elementary events can be given by defining a set of positive operators $\hat{E}_\nu = |\nu\rangle\langle\nu|$, representing a non-orthogonal expansion of the unit operator [14] or the positive operator valued measure (POVM) [15]:

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

In our case, when the information exchange between two quantum systems employs all states of the Hilbert space, expansion (2) transforms into the continuous non-orthogonal expansion of the form [16]:

$$\hat{1} = \int_\nu |\nu\rangle\langle\nu| \, \mathrm{d}V_\nu, \tag{3}$$

where $\mathrm{d}V_\nu$ is the volume differential normalized to the dimension of Hilbert space D: $\int \mathrm{d}V_\nu = D$. The corresponding joint probability distribution has the form:

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

[†]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 conditional density matrix $\hat{\rho}_B(\alpha)$ of Bob that depends on the classical parameter α corresponding to the transmitted by Alice state $|\alpha\rangle$. However, the description of Alice–Bob system as an entangled pair of states has definite methodological benefit as it allows to describe all the participants of the information exchange in the system Alice–Eve–Bob as peering parties.

where $\hat{E}_{A,B}(d\nu) = |\nu\rangle_{A,B}\langle\nu|_{A,B}\, dV_\nu$, and defines the so called *non-selected* mutual information [16,17]

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

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

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

By contrast with discrete alphabet, one cannot performs exact basis reconciliations procedure for the ∞-states protocol, because one needs to transmit an infinitive amount of information about a point from continuum. Therefore, we suggest to apply *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 bases reconciliation procedure, Alice and Bob will transmit number of an area to which belongs the information basis, an will decide then that they used equal bases if they belong to the same area.

Clearly, such approximate bases reconciliation procedure introduces additional errors, or *internal noise*, into the transmitted message due to the differences between quantum letters of the same area. However, the smaller size for 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 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 bases reconciliation, 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 bases reconciliation with the help of continuous expansion of unit operator at the given rounded area. The respective amount of information I_{AB} for the approximate bases reconciliation depends on the size of the area or, in fact, on the number of areas we split the Hilbert space in. This dependency is shown in Fig. 1.

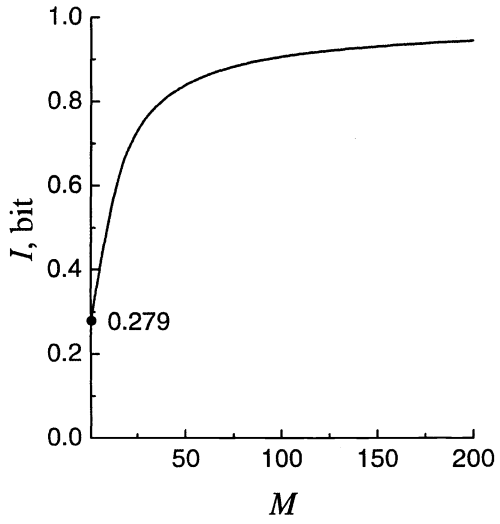

Figure 1. The amount of information I per transmission versus the number of areas M in which two-dimensional Hilbert space of states is split.

With increasing the total number or areas (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, bases reconciliation is *de facto* vanishes, the amount of information is equal to the accessible information $I_{AB} \simeq 0.279$ bit [16, 18]. With increasing the 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 *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 essential number of areas $M < \infty$.[‡]

Note, that reduction of the area size leads to increasing of the number of areas we split the Hilbert space in and, therefore, to the responding increase of the additional information on the number of area transmitted via a public channel. The amount of messages selected after the bases reconciliation procedure is also decreasing proportionally to the size of the area. In practice, however, there is no need in infinite increase of the accuracy in bases reconciliation; it is enough to choose a reasonable level of accuracy in bases reconciliation for every specific case.

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

However, in the case of ∞-states protocol, when due to the approximate bases 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 the Eve interference because it equally takes into account external noise due to the possible eavesdropping and internal noise due to the QKD protocol specifics, namely, an approximate bases reconciliation.

In order to resolve this contradiction with the definition of QBER (see also Ref. [19]), we suggest to use 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 a 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 QBER, the *mutual information error rate* or MIER.

By contrast with QBER, MIER correctly reflects the degree of Eve's interference for an arbitrary QKD protocol—either with the exact or approximate bases reconciliation procedure. In absence of any noise both measures QBER and MIER have the same value, $Q = \tilde{Q} = 0$, which correctly reflects an *a priori* expected value. However, in the case of maximal Eve's interference, 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 the MIER as the most adequate measure of Eve's interference, or QBER with under limiting assumption that the bases for the ∞-states protocol are reconciled exactly.

[‡]The fact that there are no any principal limitations on the physically allowed complexity of the bases reconciliation procedure allow us to use in the following for the estimation of the maximal error rate of the QKD protocol the respective value for the number of areas $M \to \infty$.

3. COMPARISON OF THE QKD PROTOCOLS

For determining the critical error rate in the transmitted message up to which the QKD protocol ensures the absolute security of transmitted data one needs generally to prove the absolute security of the QKD protocol [20,21]. However, in this work we are not going to repeat the ultimate security proof, but perform a *comparative* analysis of one of the best by now six-states protocol with the 4-, 8-, 12-, 20- and ∞-states under Eve's attacks. We will limit our consideration by considering only two key strategies of eavesdropping—intercept–resend and optimal eavesdropping and will compare the critical error rate for two QKD protocols.

3.1. 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 strategy Eve knows exactly information received by Bob and therefore secure data transmission between Alice and Bob is impossible. Therefore, maximal possible level of errors, which can be corrected and 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 the upper bound of the protocol efficacy at any applied strategy of eavesdropping.

Let us assume that after bases reconciliation procedure Alice and Bob found that Alice transmitted to Bob state $|\alpha\rangle$ and Eve used an orthogonal basis $\{|\psi\rangle, |\psi_\perp\rangle\}$ to eavesdrop the information. Then, Eve measured the information resulting to either $|\psi\rangle$ with probability $|\langle\psi|\alpha\rangle|^2$ or to $|\psi_\perp\rangle$ with probability $|\langle\psi_\perp|\alpha\rangle|^2$ and transmitted the resulted state to Bob. After measurement of states $|\psi\rangle$ and $|\psi_\perp\rangle$ in 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 $|\langle\psi_\perp|\alpha_\perp\rangle|^2$. Total probability of getting correct result $|\alpha\rangle$ by Bob is equal to $F_{\alpha\psi} = |\langle\psi|\alpha\rangle|^4 + |\langle\psi_\perp|\alpha\rangle|^4$. Respectively, probability of getting wrong result is equal to $Q_{\alpha\psi} = 1 - F_{\alpha\psi}$.

In order to get QBER Q, one needs to average $Q_{\alpha\psi}$ over all Alice's bases $\{\alpha\}$ and minimize then the result of the averaging over the 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 is the number of bases in the Alice's and Eve's alphabet. For the QKD protocol with continuous alphabet averaging means integration instead of summation.

Calculating Q for the considered QKD protocols, we get $Q_{4-\text{state}} = Q_{6-\text{state}} = Q_{\infty-\text{state}} = 1/3 \simeq 0.333$ and $Q_{12-\text{state}} = Q_{20-\text{state}} = 74/225 \simeq 0.329$. It is interesting to note that despite geometrical symmetry of all discussed alphabets, they have, nevertheless, different error rates: 4-, 6- and ∞-state protocols have equal error rates but exceed 12- and 20-state protocols ones.

3.2. 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 information Eve received either from Alice or Bob [22]. This condition can be written as

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

We will call Eve's eavesdropping strategy as *optimal* if Eve extracts from the transmitting message maximum information at the given level of interference, which causes the respective level of errors (note that this can differs from the optimal cloning of the transmitting message [23]).

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

$$\left.\begin{aligned} |0\rangle_B |0\rangle_E &\xrightarrow{U_{BE}} |0\rangle_B |\Phi_{00}\rangle_E + |1\rangle_B |\Phi_{01}\rangle_E, \\ |1\rangle_B |0\rangle_E &\xrightarrow{U_{BE}} |0\rangle_B |\Phi_{10}\rangle_E + |1\rangle_B |\Phi_{11}\rangle_E. \end{aligned}\right\} \tag{10}$$

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

$$\left.\begin{array}{l} \langle\Phi_{00}|\Phi_{10}\rangle + \langle\Phi_{01}|\Phi_{11}\rangle = 0, \\ |\Phi_{00}|^2 + |\Phi_{01}|^2 = |\Phi_{10}|^2 + |\Phi_{11}|^2 = 1. \end{array}\right\} \tag{11}$$

Taking into account conditions (11) and due to the symmetry of the alphabets of the considered QKD protocols, we can present a set $\overrightarrow{|\Phi\rangle}$ of all the states $|\Phi_{ij}\rangle$ as a superposition of only 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 coefficients

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

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

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 an initial Eve's state $|0\rangle_E \langle 0|_E$ after transformation of optimal eavesdropping (10) is transferred into the final state $\hat{\rho}^{(2)}_{ABE}$ that is an entangled state of Alice, Bob, and Eve: $\hat{\rho}^{(1)}_{ABE} \xrightarrow{U_{BE}} \hat{\rho}^{(2)}_{ABE}$.

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

$$\begin{array}{l} \hat{\rho}^{(2)}_{AB} = \mathrm{Tr}_E \hat{\rho}^{(2)}_{ABE} \rightarrow I_{AB}, \\ \hat{\rho}^{(2)}_{AE} = \mathrm{Tr}_B \hat{\rho}^{(2)}_{ABE} \rightarrow I_{AE}, \\ \hat{\rho}^{(2)}_{BE} = \mathrm{Tr}_A \hat{\rho}^{(2)}_{ABE} \rightarrow I_{BE}. \end{array} \tag{13}$$

Optimal eavesdropping condition, which must be checked, can be written as

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

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 equations (10) and (13) versus parameters θ and φ controlled by Eve, one can easily show that for all values of θ, φ we have $I_{AE} \geq I_{BE}$, thus we will not discuss I_{BE} in the following.

The security condition $I_{AB} > I_{AE}$ due to the symmetry $I_{AB}(\theta, \varphi) = I_{AE}(\varphi, \theta)$ is fulfilled up to a certain critical level $\theta^{(1)}_0 = \varphi^{(1)}_0 = \pi/8$ until 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 0.650, 0.630, 0.607, 0.597, 0.589, and 0.600 for the 4-, 6-, 8-, 12-, 20-, and ∞-state protocols, respectively.

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

Let us assume now that Alice and Bob uses *safety* bases 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 bases reconciliation. In other words, she gain no additional information from basis reconciliation procedure. Urgency 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 physical point of view. In order to retrieve additional information from bases reconciliation, Eve has to have unlimited

quantum memory, which allow 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, respectively to the loss of information. If the legitimate parties of the QKD protocol (Alice and Bob) make a pause between data transmission and bases reconciliation, which exceeds the typical decoherence time in the system, then the bases reconciliation will not give any additional information to Eve.

Second, though the assumption that Eve does not retrieve additional information from the bases reconciliation is definitely a limitation, it is, however, equally applicable to the analysis of all QKD protocols of interest. Calculated critical error rates with limitations on eavesdropping strategies do not serve then as the absolute security criterions, but our goal is to compare different QKD protocols, and, with some restrictions on Eves strategies, this analysis seems to be suitable for this purpose.

After such safety bases reconciliation, information received by Bob from Alice proportionally increases by contrast with case when no bases reconciliation made, and reaches its maximum value of 1 bit per message (in the limit of exact bases reconciliation for the QKD protocol with continuous alphabet). Information in the system Alice–Eve remains the same according to the assumption made.

After the bases reconciliation, the security condition $I_{AB} > I_{AE}$ is fulfilled up to a certain, depending on a specific protocol, critical value $\theta_0^{(2)} = \varphi_0^{(2)}$, different from value $\theta_0^{(1)} = \varphi_0^{(1)}$ corresponding to the case without bases reconciliation. Also, critical error rate $\tilde{Q}_0$ becomes significantly higher and is equal to 0.788, 0.806, 0.805, 0.804, 0.805, and 0.811 for the 4-, 6-, 8-, 12-, 20-, and ∞-state protocols, respectively.

The calculation results for the critical error rate are summarized in Table 1.

Table 1. Critical error rate $\tilde{Q}_0$ for 4-, 6-, 8-, 12-, 20- and ∞-state QKD protocols with and without bases reconciliation.

Number of letters	4	6	8	12	20	∞
Before basis reconciliation	0.650	0.630	0.607	0.597	0.589	0.600
After basis reconciliation	0.788	0.806	0.805	0.804	0.805	0.811

We do not consider case of two-way communication, when one capable to establish a secure connection even at $\tilde{Q} > \tilde{Q}_0$ [12]. Then, at the 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 critical error rate $\tilde{Q}_0$, the more stable the QKD protocol to the eavesdropping attacks, because it allows greater level of interference.

Summarizing, our information analysis shows that without bases reconciliation the 4-state protocol has the best maximum value of the critical error rate. But after safety bases reconciliation procedure applied we see, however, that the ∞-state protocol has a higher critical error rate in comparison with the considered QKD protocols. In other words, information characteristics of six-state protocol can be surpassed even in case of two-dimensional Hilbert space due to a better choice of the alphabet.

4. MULTIDIMENSIONAL CASE

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

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

First, Alice transmits a random letter to Bob from randomly selected bases. If Eve guesses this basis, the letter will be transmitted to Bob without distortion: this scenario happens with the probability $1/L_D$. Otherwise, if Eve does not guesses the right basis (it happens with probability $1 - 1/L_D$), then the transmitted to Bob letter will be

replaced by Eve during resending with equal probability (due to the above suggestion of the symmetrical alphabet) to a different one from another basis. Bob receives a right letter, which was transmitted by Alice, with probability $1/D$, otherwise he received a wrong letter.

Total probability that Eve does not distort the transmitted by Alice letter (when Eve guesses correctly or incorrectly the basis) is equal to $F_D = 1/L_D + (1 - 1/L_D)/D$ and the respective 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 BB84 ($L_D = 2, D = 2$) and six-state ($L_D = 3, D = 2$) protocols, we get 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 maximum number of mutually unbiased letters are more favorable. For the maximum number $D + 1$ of mutually unbiased bases in D-dimensional space [24] we get the error rate $Q_\infty = 100$ %:

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

For infinite–dimensional case, maximum possible error rate is equal to 100%, by contrast with 50% for the two-dimensional case. This is due to the fact that in two-dimensional case non-guessing a letter by Eve 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 vise versa, achieving $Q_2^{(2)} = 1 - Q_2^{(1)} < 0.5$. In multidimensional case, this trick does not work—the higher the dimension of the Hilbert space, the higher the maximum possible error rate.

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

Keeping this specifics of QKD protocols with multidimensional alphabets, let us consider now an extension of the ∞-state protocol on the case of multidimensional Hilbert space.

Note that in multidimensional case, maximum possible selected information between two systems $I^D_{\max} = \log_2 D$ grows infinitively at $D \to \infty$ whereas maximum possible non-selected information is bounded: it is equal to the amount of *accessible* information [18]

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

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

In case when Eve does not extract additional information from bases reconciliation procedure and disengage oneself from a specific eavesdropping strategy, we can estimate the upper limit of maximum amount of non-selected information, which is received by Eve, by the accessible information. In fact, information received by Eve will be even smaller.

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

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

The critical mutual information error rate $\tilde{Q}_0$ calculated by formula (17) versus the dimensionality of the Hilbert space is shown in Fig. 2. This result shows qualitatively novel property of the multidimensional ∞-state protocol with respect to two-dimensional case—with increasing the dimensionality of the Hilbert space the critical error rate for this protocol increases and in the limit of infinite-dimensional space the protocol becomes non-threshold.

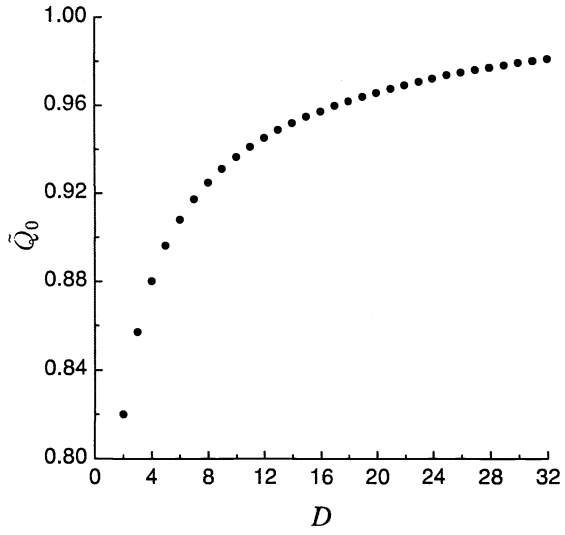

Figure 2. Critical error rate $\tilde{Q}_0$ versus the dimension D of the Hilbert space.

Such behavior of the critical error rate does not depend on 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 bases reconciliation, Alice and Bob can select only maximally correlated messages for which they choose approximately similar bases. As a result, information bond between Alice and Bob per one message will be significantly improved. Eve, in her turn, cannot affect the processes of messages selection and her information remains the same. Therefore, Eve with increasing the dimensionality of the Hilbert space retrieves much less information than Bob, which leads finally to the non-threshold property of the QKD protocol with continuous alphabet. In the reasoning above, we made the only assumption about safety basis reconciliation, which was discussed in Section 3.2.

5. CONCLUSIONS

In conclusion, our information analysis shows that critical error rate of the six-state protocol can be surpassed even in case of two-dimensional Hilbert space due to a better choice of the alphabet. Namely, without bases reconciliation the 4-state protocol has the best maximum value of the critical error rate. But after bases reconciliation procedure is applied, use of continuous alphabet in case when an eavesdropper has no ability to store the intercepted information in a quantum form leads to a slightly higher critical error rate than that one of the six-state protocol, even in the two-dimensional case.

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

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

This work was partially supported by RFBR grants Nos. 02–03–32200, 04–02–17554, and INTAS grant INFO 00–479.

REFERENCES

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 Transactions Inf. Theory **49**, 457 (2003); LANL e-print quant-ph/0105121 (2001).
12. N. Gisin, Rev. Mod. Phys. **74**, 145 (2002).
13. R. G. Gallagher, *Information Theory and Reliable Communication* (John Wiley and Sons, New York, 1968).
14. B. A. Grishanin, Izv. Akad. Nauk SSSR, Ser. Tekh. Kiber. **11**, 127 (1973); LANL e-print quant-ph/0301159 (2003).
15. J. Preskill, *Lecture notes on Physics 229: Quantum information and computation*, located at http://www.theory.caltech.edu/people/preskill/ph229/.
16. B. A. Grishanin and V. N. Zadkov, J. of Commun. Technology and Electronics **47**, 933 (2002).
17. B. A. Grishanin, Problemi Peredachi Informatsii **38**, 31 (2002).
18. C. M. Caves and C. A. Fuchs, LANL e-print quant-ph/9601025 (1996).
19. C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
20. H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
21. P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
22. C. H. Bennett, G. Brassard and J. M. Robert, SIAM J. Comput. **17**, 210 (1988).
23. C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
24. W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).