arXiv:quant-ph/0304035v1 4 Apr 2003

Quantum cryptography with continuous alphabet

Denis Sych*, Boris Grishanin, and Victor Zadkov
International Laser Center and Faculty of Physics,
M. V. Lomonosov Moscow State University, Moscow 119899, Russia

Abstract

A new quantum cryptography protocol, based on all unselected states of a qubit as a sort of alphabet with continuous set of letters, is proposed. Its effectiveness is calculated and shown to be essentially higher than those of the other known protocols.

Typeset using REVTEX

*sych@comsim1.phys.msu.su

I. INTRODUCTION

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

Keeping this advantage of quantum physics for QC in mind, any QC-protocol uses messages entirely composed of an incompatible set of quantum states or so called *quantum alphabet* that consists of incompatible "letters". Various protocols of QC are distinguished in essence only by different alphabets, which ensure secure message transmission up to an error level that determines the protocol efficiency. Analyzing distortions in received messages one can reveal an eavesdropping attack, but in order to raise the information transmission rate it is necessary also to counter such attacks. All discussed in the literature QC-protocols have relatively low, about 15%, quantum bit error rate (QBER) [1] above which they do not ensure secure transmission. Ideally, all perturbations in the transmitted information are caused by an eavesdropper, but in reality imperfections of apparatus used for realization of the QC-protocol and external sources of noise (besides the eavesdropper) also perturb the information.

For the optimal efficiency analysis of various protocols different efficiency criteria are used [8], which is inconvenient for the objective comparison of the protocols. In this paper, we will use most appropriate criteria based on the classical Shannon information approach estimating amount of information transmitted through the information channels of the QC scheme [9]. In QC, typical information system includes three basic components, Alice, Bob, and Eve (the conventional names for the sender, receiver, and eavesdropper, respectively), which communicate through a quantum channel. Despite the communication nature between Alice, Bob, and Eve is quantum, they in the final analysis exchange classical information. Therefore, the classical Shannon information is a valid measure for a quantitative analysis of the quantum cryptography protocols, which corresponds to the joint probability distribution of the measurement results (which are classical) in the quantum system Alice-Eve-Bob.

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

In another 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 QC-protocol, which is analyzed in this paper. It is shown that this protocol surpasses all known QC-protocols by a number of criteria. For instance, its critical QBER exceeds that one for the

BB84 protocol and generalization of our protocol to the case of multidimensional Hilbert space further significantly improves the critical QBER. This means that the new protocol can basically work at any level of external errors or eavesdropping attacks, which is a new feature of the QC-protocols.

II. COMPATIBLE INFORMATION AS A QUANTUM INFORMATION MEASURE IN QC-PROTOCOLS

In QC, Alice (A), Bob (B), and Eve (E) are the different, kinematically independent quantum systems. Thus, the quantum events related to these systems belonging to the different Hilbert spaces are mutually compatible. Due to this property, any pair of quantum events at the input and output of the quantum channel can be considered classically. Quantum specific of the channel 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 the *compatible* quantum information [10, 11]. A natural quantitative measure for the compatible information is the standard mutual Shannon information functional of the classical input–output (Alice-Bob) joint probability distribution P_{AB}:

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

where $S[P]$ is the classical Shannon entropy functional for $P = P_A$, P_B, and P_{AB} [9].

In quantum 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 to define a set of elementary events of which any message is composed. Elementary events for a given quantum system are represented by the wave functions or state vectors of the system. Mathematically, a choice of basis events can be given by defining a set of positive operators $\hat{E}_\nu$ representing a non-orthogonal expansion of unit operator [12, 13], which is an analog of average classical indicator functions of a complete group of classical random events, which are normalized to the indicator of the reliable net event (with the probability equal to unity) and can be written in quantum case as the unit operator:

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

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

Two limiting cases of the compatible information—limiting *selected* and *non-selected* information—are defined by two limiting cases of the unit operator expansion—two-component orthogonal [14]

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

and continual non-orthogonal [11]

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

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

The selected information determines an information link 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 transformation $U_A(\alpha)$ and $U_B(\beta)$ in quantum systems A and B, respectively, can be chosen differently and the selected information also depends on the choice made:

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

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

Joint distribution $P^{\alpha\beta}_{AB}(k,l) = \mathrm{Tr}_{AB}(\hat{E}^{\alpha}_{A}(k) \otimes \hat{E}^{\beta}_{B}(l))\hat{\rho}_{AB}$ is defined on the basis states of the input (Alice) and output (Bob) of the channel $|k\rangle^{\alpha}_{A}$, $|l\rangle^{\beta}_{B}$ numbered by two indices k and l. These states are the orthogonal basis states of respected Hilbert spaces H_A and H_B.

For the non-selected information, the information exchange undergoes through all equally participating in the exchange states. In this case, basis states of the information channel are *all* wavefunctions of the Hilbert spaces of all participating in the exchange quantum systems. The respected non-selected information is then given as

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

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

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

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

III. QC-PROTOCOL EMPLOYING ALL STATES OF THE HILBERT SPACE OF THE CRYPTOGRAPHIC SYSTEM

Key idea of QC is that secure quantum information channel is used first to transfer a secret key from Alice to Bob, which is then used to encrypt messages transmitted via an insecure classical channel. The quantum channel over which the message out of which the secret key will be extracted is transferred can be eavesdropped by Eve who can perform any physically allowed transformations gaining information about the transferring message. The purpose of Alice and Bob is to establish a secure connection, which prevents copying of useful transmitted information by Eve. Ii was proved that such secure connection is possible if the amount of information Bob received from Alice exceeds information Eve received either from Alice or Bob [15]. This condition can be written as

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

If the condition (8) is fulfilled, it is possible with the help of special methods of encrypting/decrypting the information to reduce up to zero the amount of useful information Eve can gain eavesdropping the quantum channel.

Eve, in her turn, also tries to use optimal strategies of eavesdropping at the given level of interference, i.e., Eve tries to gain maximum information about the transmitting message minimizing the error level she causes.

All known QC-protocols using finite-dimensional spaces of states are built on the alphabets with the finite discrete set of incompatible quantum "letters", which can be realized as the pure states of a quantum system. In this paper, we suggest a qualitatively new QC-protocol, which is based on the alphabet including all states of the Hilbert space. In other words, this alphabet consists of an infinite number of quantum "letters", which are formed by arbitrary superpositions of orthogonal basis states of the Hilbert space H_A.

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

Elementary step of the QC-protocol that is transmission of a single "letter" or state from Alice to Bob can be outlined as follows:

1. Alice transmits to Bob via a quantum channel a randomly chosen state $|\beta\rangle$. Let us assume that the Alice's state $|\alpha\rangle$ is totally entangled with the transmitting state $|\beta\rangle$ and is, for example, the antisymmetric Bell state $||-\rangle\rangle = (|\alpha\rangle \left|\tilde{\beta}\rangle - |\tilde{\alpha}\rangle |\beta\rangle\right)/\sqrt{2}$, which means that Alice perfectly knows the transmitting state.

2. Eve eavesdrops the channel performing an unitary transformation U_{BE} with her initial state $|0\rangle_E$ and with transmitted by Alice to Bob state $|\beta\rangle_B$ and readily measures her final state.

3. Bob reads the perturbed state using for the measurement an *arbitrary* projector because he has no *a priori* information about the received message.

When transmission of the message is completed, Alice and Bob disclose part of the measurement results transmitting them over an insecure classical channel in order to determine the mutual probability distribution, which is then used for calculation of an average amount of transmitted information per an elementary step of the QC-protocol. After that, disclosed results are discarded and not used for further generation of a secret key. If the security condition (8) is fulfilled, Alice and Bob decide that the secret key transfer is completed, otherwise the transmitted key is not used. Note that the described protocol does not require bases reconciliation of Alice and Bob, i.e., selection of only that part of the message for which Alice and Bob used the same measurement projectors, via an additional information exchange over the classical channel.

A. Information analysis of the protocol

For information analysis of the suggested protocol let us first calculate the amount of information Bob received from Alice and Eve received from Alice and Bob at the condition of optimal eavesdropping.

Initial state of the quantum system Alice-Eva-Bob $\hat{\rho}^{(1)}_{ABE} = \hat{\rho}^{(1)}_{AB} \otimes |0\rangle_E \langle 0|_E$, which is described by the tensor product of the entangled antisymmetric pair Alice-Bob $\hat{\rho}^{(1)}_{AB} = ||-\rangle\rangle_{AB} \langle\langle -||_{AB}$ and an initial Eve's state $|0\rangle_E$, is transferred after eavesdropping the channel by Eve into the final state that is an entangled state of Alice, Bob, and Eve, $\hat{\rho}^{(2)}_{ABE}$: $\hat{\rho}^{(1)}_{ABE} \xrightarrow{U_{BE}} \hat{\rho}^{(2)}_{ABE}$.

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

$$\begin{cases} |0\rangle_B |0\rangle_E \xrightarrow{U_{BE}} |0\rangle_B |\Phi_{00}\rangle_E + |1\rangle_B |\Phi_{01}\rangle_E \\ |1\rangle_B |0\rangle_E \xrightarrow{U_{BE}} |0\rangle_B |\Phi_{10}\rangle_E + |1\rangle_B |\Phi_{11}\rangle_E . \end{cases} \tag{9}$$

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

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

It was suggested in reference [8] based on the numerical estimations and then proved in reference [16] that in the QC protocols BB84 and B92 the Eve's state at the optimal eavesdropping lies in two-dimensional Hilbert space. This is also true (and can be proved) for our QC-protocol. Therefore, the states $|\Phi_{ij}\rangle$ can be written with the help of condition (10) as a superposition of two basis states:

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

where the transformation parameters

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

are determined via two angles θ, φ on the Bloch sphere.

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

$$\begin{array}{l} \hat{\rho}^{(2)}_{AB} = \mathrm{Tr}_E \hat{\rho}^{(2)}_{ABE} \rightarrow I_{AB}, \\ \hat{\rho}^{(2)}_{AE} = \mathrm{Tr}_B \hat{\rho}^{(2)}_{ABE} \rightarrow I_{AE}, \\ \hat{\rho}^{(2)}_{BE} = \mathrm{Tr}_A \hat{\rho}^{(2)}_{ABE} \rightarrow I_{BE}. \end{array} \tag{12}$$

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

B. Calculations results

Results for the mutual Alice-Bob, Alice-Eve, and Bob-Eve non-selected information (I_{AB}, I_{AE}, and I_{BE}, respectively) calculated with the help of equations (6), (9), (11), and (12) are shown in figure 1 versus parameters θ and φ controlled by Eve. 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 in the following only on I_{AE}.

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

For most purposes it is enough to consider only two-dimensional plots of $I_{AB}(\theta)$ and $I_{AE}(\theta)$ along the solid line $\theta = \pi/4 - \varphi$, which are shown in figure 2. From analysis of this figure one can see that at $\theta = 0$ the level of Eve eavesdropping attacks and the respected losses of information are equal to zero. At $\theta = \pi/4$ the intervention of Eve is maximal and she acts, in fact, as Bob gaining maximal possible information.

The condition for the protocol to be a secure one, $I_{AB} > I_{AE}$, is fulfilled up to a certain critical value $\theta_0 = \pi/8$, which is the intersection point (1) of the curves for I_{AB} and I_{AE} in the figure 2. At this point, the QBER $q = 1 - \mathrm{Tr}\hat{\rho}_B^{(1)}\hat{\rho}_B^{(2)}$, has the critical value of $q_0 = \sin(\pi/8) \simeq 0.15$, which is equivalent to the QBER value provided by the BB84 protocol [1,3]. The respected value of the compatible information is equal to $I_0 = I_{AB}(\theta = \theta_0) \simeq 0.11$ bit.

As it is demonstrated in reference [8], the QBER is not always an adequate characteristic of the degree of Eve eavesdropping attacks, for instance in the B92 protocol. Therefore, we suggest to use another characteristic, the *compatible information error rate* (CIER), which naturally reflects in term of the compatible information the degree of Eve interference to the transmitting information:

$$Q = 1 - \frac{I}{I_{\max}} \in [0, 1], \tag{13}$$

where I is the compatible information I_{AB} with the presence of eavesdropping and $I_{\max}$ its maximal possible value without Eve attacks. By contrast with QBER (q), CIER (Q) is the most adequate parameter for the information properties of the QC-protocols.

Without Eve eavesdropping attacks, both parameters q and Q are equal to zero, which means that there are no transmission errors. At the maximal level of Eve interference with the transmitting information, we have $Q = 1$ and $q = 0.5$, which correspond to the maximal possible level of errors caused by Eve. At the critical point θ_0, where the amount of information gained by Eve is equal to the amount of information received by Bob, $Q_0 \simeq 0.4$ and $q_0 \simeq 0.15$. For our QC-protocol, the larger critical value Q_0 the better stability of the protocol to the errors caused by Eve and, therefore, better information properties. Thus, the protocol ensures the security of transmitted data even at essential errors rate during the data transmission. At the error level exceeding critical, i.e. at $Q > Q_0$, the protocol does not ensure security of transmitted data and Alice and Bob decide that the transmission is not completed.

In suggested QC-protocol the requirement of bases reconciliation for Alice and Bob is lifted because even with no selection of quantum states made at the Bob's end he receives about 0.28 bit for every elementary step of the QC-protocol, if there is no external noise during data transmission. However, one can significantly improve stability of the protocol for a noisy quantum channel reconciling the basis states.

After transmission of all data through a noisy quantum channel Alice and Bob can select only those transmitted data for transmitting which they used approximately similar orthogonal bases. In our case, the set of basis states is the continuum, thus it is necessary to split it into several areas and count the bases similar, if they are in the same area on the Bloch sphere. As a result of such selection, Alice and Bob will receive without any intrusion of Eve maximal information value of about 1 bit during one elementary step of the QC-protocol. This can be clearly understood because for an initial state of the Alice-Bob system in the form of antisymmetric Bell state the mutual selected information is equal to unity when use similar oriented bases of Alice and Bob. One can suppose that Eve does not affect the data selection with the reconciling bases and does not use additional transformations after the bases have been reconciled. Then, she gains no additional information.

Information that Bob receives from Alice after the bases reconciliation is shown in figure 2 (dashed line). The critical error rate Q is then significantly increased and is of the order of value $Q_0 \simeq 0.81$ and for the QBER we have $q_0 \simeq 0.42$, which is much better than for all known QC-protocols.

Note that the bases reconciliation procedure significantly increases the number of messages transmitted over an insecure classical channel, which in the limit of infinitively small areas on which we split the continual quantum alphabet grows up to infinity. Respectively, the number of selected messages transmitted through a quantum channel is decreased. It is not necessary, however, to infinitely increase the accuracy. As a rule, errors during the data transmission have typical for a specific experimental QC setup finite level. Therefore, for the bases reconciliation it is sufficient to increase the accuracy according to the external conditions up to the level that ensures the error rate less than the critical one at which the QC-protocol guarantees the secure transmission of data.

IV. MULTIDIMENSIONAL CASE

We can fundamentally improve the properties of suggested QC-protocol using multidimensional Bob's and Alice's spaces ($D > 2$). In multidimensional case, the maximally possible amount of mutual selected information is equal to $I^D_{\max} = \log_2 D$ and grows infinitely at $D \to \infty$. Maximally possible amount of non-selected information is equal to the volume of accessible information [17]:

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

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

After reconciliation the Alice's and Bob's bases the amount of information in the system Alice-Bob is given by maximally possible selected information, whereas in the Alice-Eve system—by the maximally possible non-selected information. Then, critical level of errors in the limit of $D \to \infty$ is equal to unit:

$$Q_0^\infty = \lim_{D\to\infty} Q_0^D = 1 - \lim_{D\to\infty} \frac{I^D_{\text{accessible}}}{I^D_{\max}} \simeq 1 - \lim_{D\to\infty} \frac{0.61}{\log_2 D} = 1. \tag{14}$$

This means that increasing the dimensionality of the Alice-Bob system one can reach the critical error rate (QBER or CIER), which exceeds any given value. The multidimensional spaces of Alice and Bob can be realized using block coding when information is transmitted simultaneously with the help of several qubits.

Fundamental advantage of the suggested QC-protocol that employs all states of the Hilbert space is that it can work, in principle, at any imperfections or noise in the quantum channel (either internal or external) and has no any critical CIER value after which the protocol becomes insecure. For any given CIER value one can calculate (from technical point of view, calculations in the case of multidimensional space can be readily done) the required dimensionality of the Alice-Bob space in order to meet this value of CIER. Essentially more difficult is the question about Eve's transformation structure to perform optimal eavesdropping in the multidimensional case, but the outlined above result is qualitatively correct, despite any specific structure of the Eve's transformation.

V. EXPERIMENTAL SETUP FOR QC WITH CONTINUOUS ALPHABET

In this section, we suggest an experimental setup for the QC with continuous alphabet "letters" of which are coded with polarization of the photons (figure 3). Then, a random letter corresponds to an arbitrary photon polarization.

A source of EPR-pairs of photons, for instance an optical parametric oscillator (2) generating pairs of photons in antisymmetric entangled state, is located at the Alice's end of the cryptographic setup. Alice receives one of the generated photons, another one is transmitted via a secure quantum channel to Bob.

An arbitrary projector can be realized by rotation to an arbitrary angle the polarization plate (3) with the following measurement in the fixed basis. Photons transmitted from Alice to Bob are in the antisymmetric state, thus Alice knows exactly, after the photon measurement on her end, that photon she sent to Bob is an orthogonal state to that one measured by Alice. As a result of the outlined procedure, Alice sends to Bob a randomly chosen quantum "letter".

Likewise, Bob for the measurement in an arbitrary basis first rotates polarization of the incident photon by polarization plate (3) to the angle value of which he receives from Alice over an insecure classical channel (not shown in the figure) and then performs measurement in the fixed basis.

A case of multidimensional spaces of the quantum channel input and output can be realized when information is transmitted with the help of several entangled qubits (photons). This, however, is an experimental difficulty to generate, operate, and measure arbitrary states in multidimensional spaces, i.e., difficulty to generate and operate multiple entangled photons.

VI. CONCLUSIONS

In conclusion, a new QC-protocol based on the quantum alphabet with infinitive number of "letters" (i.e., employing all the quantum states of the Alice-Bob quantum system) is proposed. It has a number of advantages in comparison with other known QC-protocols. Even in two-dimensional case the protocol shows an essential increase of the QBER. In multidimensional case, the protocol has a fundamental, qualitatively new feature, which allows secure data transmission through practically any noisy quantum channel. For estimation of the Eve's intervention into the data transmission through a quantum channel we use classical mutual Shannon information-based criterion, which adequately reflects the information aspect of the eavesdropping and can be effectively used for both constructing and analyzing the QC-protocols.

ACKNOWLEDGMENTS

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

REFERENCES

[1] Gisin N 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145

[2] Wiesner S 1983 Conjugate coding *SIGAT News* **15** 78

[3] Bennett Ch H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computer, System, and Signal Processing (Bangalore, India)* (New York: IEEE Publishers) p 175

[4] Bennett Ch H 1992 Quantum cryptography using any two nonorthogonal states *Phys. Rev. Lett.* **68**, 3121

[5] Bruss D 1998 Optimal eavesdropping in quantum cryptog-raphy with six states *Phys. Rev. Lett.* **81**, 3018

[6] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states *Phys. Rev. Lett.* **88** 057902

[7] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802

[8] Fuchs C A and Peres A 1996 Quantum state disturbance vs. information gain: uncertainty relations for quantum information *Phys. Rev.* A **53** 2038

[9] Gallagher R G 1968 *Information Theory and Reliable Communication* (New York: John Wiley and Sons)

[10] Grishanin B A 2002 *Problemi Peredachi Informatzii* **38** 31

[11] Grishanin B A and Zadkov V N 2002 Measurement and physical content of quantum information *J. of Commun. Technology and Electronics* **47** 933

[12] Grishanin B A 1973 *Izv. A. N. USSR, Tekhnicheskaya Kybernetika* **11** 27

[13] Preskill J *Lecture notes on Quantum Information* (web page http://www.theory.caltech.edu/people/preskill/ph229/)

[14] von Neumann J 1955 *Mathematical Foundations of Quantum Mechanics* (Princeton: Princeton University Press)

[15] Bennett C H, Brassard G and Robert J M 1988 Privacy amplification by public discussion *SIAM J. Comput.* **17** 210

[16] Fuchs C A, Gisin N, Griffiths R B, Niu C S and Peres A 1997 Optimal eavesdropping in quantum cryptography. I. information bound and optimal strategy *Phys. Rev.* A**56** 1163

[17] Caves C M and Fuchs C A 1996 Quantum information: how much information in a state vector? *Preprint* quant-ph/9601025

FIGURES

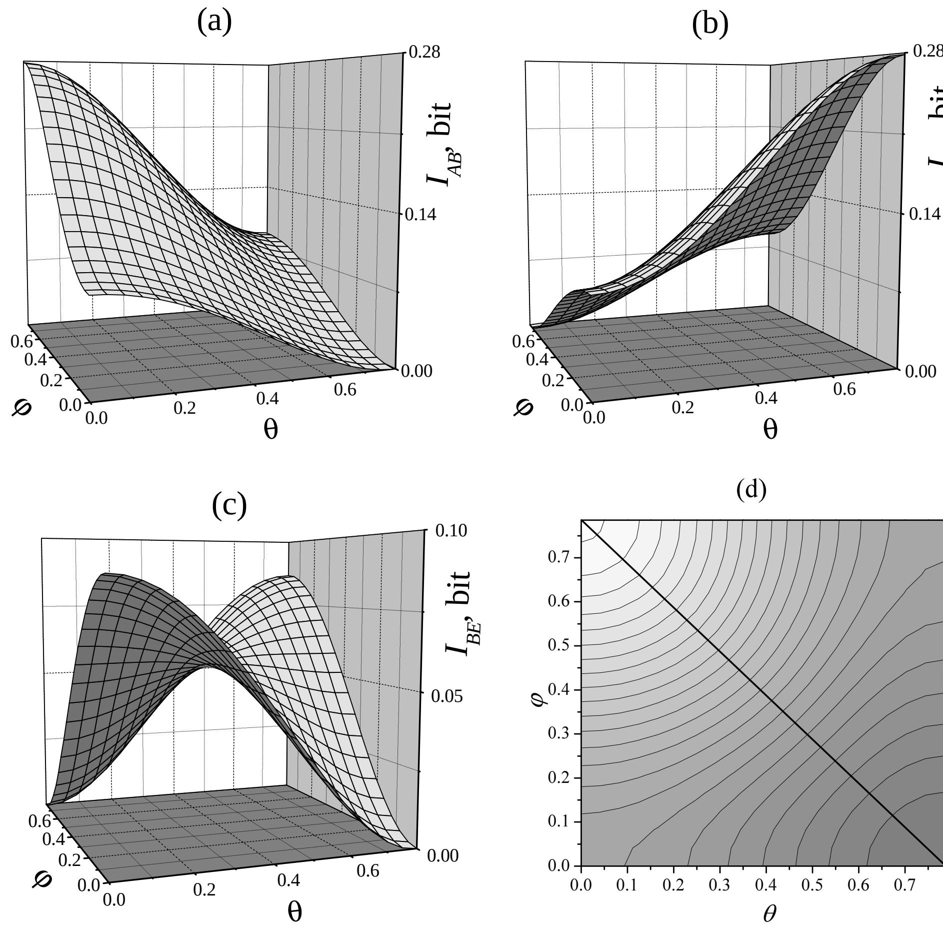

FIG. 1. Alice-Bob (a), Alice-Eve (b), and Bob-Eve (c) mutual Shannon information versus Eve's eavesdropping parameters θ, φ. Figure (d) shows results of figure (a) for the Alice-Bob mutual Shannon information (I_{AB}) as a contour plot; solid line indicates the optimal eavesdropping.

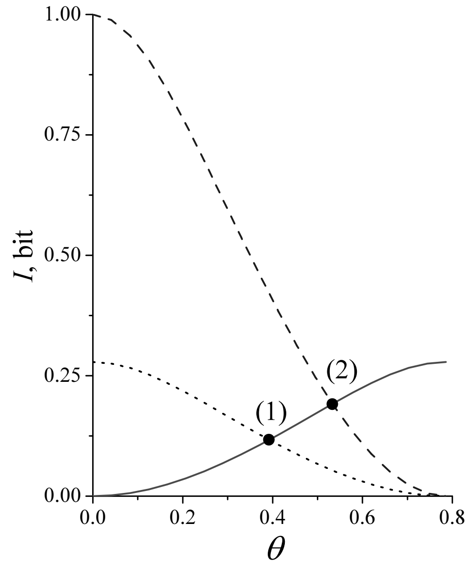

FIG. 2. Alice-Bob (dotted and dashed lines for reconciliated and non-reconciliated basis states of Alice and Bob, respectively) and Alice-Eve (solid line) mutual Shannon information at the optimal eavesdropping condition.

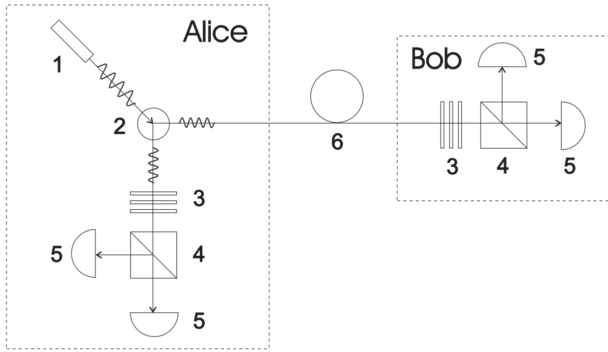

FIG. 3. Experimental setup for the QC with continuous alphabet. Laser (1) pumps an optical parametric oscillator (2), which generates a pair of entangled photons one of which is transmitted then to Alice and another one, via a quantum channel (6), to Bob. Measurement part of the cryptographic scheme consists of a polarization plate (3) that rotates polarization of the incident photon, prism (4), and photon counting detectors (5).