PACS numbers: 03.67.Dd; 03.67.Pp
DOI: 10.1070/QE2005v035n01ABEH002886

Analysis of limiting information characteristics of quantum-cryptography protocols

D.V. Sych, B.A. Grishanin, V.N. Zadkov

***Abstract*. The problem of increasing the critical error rate of quantum-cryptography protocols by varying a set of letters in a quantum alphabet for space of a fixed dimensionality is studied. Quantum alphabets forming regular polyhedra on the Bloch sphere and the continual alphabet equally including all the quantum states are considered. It is shown that, in the absence of basis reconciliation, a protocol with the tetrahedral alphabet has the highest critical error rate among the protocols considered, while after the basis reconciliation, a protocol with the continual alphabet possesses the highest critical error rate.**

Keywords: *optical quantum-information processing, quantum cryptography.*

1. Introduction

Since the advent of the idea of quantum cryptography (QC) [1] up to now, several protocols have been proposed for its realisation [2 – 5]. All these protocols are based on the principle excluding copying of arbitrary quantum states [6], which excludes exact copying of an arbitrary message transmitted through a quantum channel if the message is coded by letters representing the mutually nonorthogonal states of a quantum data carrier, for example, a photon. Moreover, any attempt to eavesdrop the message will inevitably produce errors in it, and by analysing these errors, one can not only uncover the eavesdropping itself but also calculate the maximum eavesdropped information volume possible for the given message.

Recall the main steps of standard QC protocols by using the commonly accepted terminology: Alice is a data transmitter, Bob is a data receiver, and Eve is an eavesdropper. Different QC protocols have similar operating algorithms and differ in fact only in their alphabets, i.e., sets of quantum states playing the role of letters from which a message is constructed. The first step is a choice of the alphabet, i.e., the coding of classical information, which Alice wants to communicate to Bob, by quantum states, when a set of several mutually nonorthogonal to each other but internally orthogonal pairs of states is related to a logic pair of bits '0' and '1'. For example, the alphabet of the first QC protocol, referred to as BB84 by the names of its creators [1], consists of four states: $\{|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Here, the first two states correspond to '0', and the second two to '1'. To code a specific bit, a specific state is selected randomly from this set. For example, the sequence $|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |0\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), |1\rangle$ can correspond to the line 0, 0, 1, 1, 1. Alice sends to Bob the bit sequence coded in this way. To extract classical information, Bob measures the received state in the basis randomly selected from the alphabet common with Alice and recovers from the measurement the transmitted classical bit. If he has guessed a 'correct' basis, i.e., measured the state in the same basis in which it was encoded, he should correctly recover the classical bit. If he has failed to guess a correct basis, the probability of a correct recovery of the classical bit is 1/2 (for the BB84 protocol). Thus, at the Bob side the so-called 'raw key' – a sequence of classical bits is formed, which inevitably contains errors.

Then, the basis reconciliation is performed: by communicating through an open classical channel in what basis the measurement has been made (but not reporting its result), Alice and Bob will select only a part of messages for which Bob 'has guessed' the basis correctly. In a 'sifted' key obtained in this way, the data at the Alice and Bob sides should coincide because the presence of mutually nonorthogonal states guarantees the impossibility of an imperceptible eavesdropping. However, in reality there always exist additional errors caused by the natural noise in communication channels, the imperfection of the equipment, etc. For this reason, after obtaining the sifted key, Alice and Bob perform additional classical procedures to correct errors and improve the security [7].

A common feature of all the QC protocols is the presence of a *critical* error rate above which the protocol cannot guarantee the possibility of sharing a secret message. The existence of this critical error rate restricts the range of secret data transmission due to the natural noise in the communication channel. At present the maximum distance of secret data transmission in the open air is approximately 100 km [7].

One of the aims of the development of new QC protocols is increasing the critical error rate to make the protocol more stable against the eavesdropper attacks and natural noises in the experimental setup and information channel,

D.V. Sych, B.A. Grishanin, V.N. Zadkov Department of Physics, M.V. Lomonosov Moscow State University; International Teaching and Research Laser Center, M.V. Lomonosov Moscow State University, Vorob'evy gory, 119992 Moscow, Russia;
e-mail: sych@comsim1.phys.msu.ru, grishan@comsim1.phys.msu.ru, zadkov@comsim1.phys.msu.ru

Received 22 September 2004
Kvantovaya Elektronika **35** (1) 80 – 84 (2005)
Translated by M.N. Sapozhnikov

which allows the transmission of secret data over longer distances. The critical error rate can be increased by varying the alphabet and the dimensionality of the space of states. It is widely accepted (although is not proved) that in the two-dimensional case the protocol with the alphabet consisting of three mutually unbiased bases, the six-state protocol, has the maximum critical error rate [4, 8, 9]. It is assumed, as a rule, that the critical error rate can be further increased only by increasing the dimensionality of the space of states [10–12].

In this paper, we consider the possibility of increasing the critical error rate above that of the six-state protocol by varying the alphabet in the two-dimensional space.

Noting that a set of six letters of the six-state protocol forms an octahedron on the Bloch sphere (which is also called the Poincare sphere in some papers [13]), we consider alphabets whose letters form regular polyhedra: tetrahedron, cube, icosahedron, and dodecahedron having 4, 8,12, and 20 vertices, respectively, and as a limiting case of a polyhedron with an infinite number of vertices, the continual alphabet, which equally includes all the quantum states. Protocols, which use such alphabets, repeat all the main steps of standard QC protocols, for example, the BB84 protocol [1] (the raw key formation, basis reconciliation, security improving, etc.). Some specific features are inherent only in a protocol with the continual alphabet (section 2) and in a protocol with the tetrahedral alphabet (section 3). In other respects, these protocols can be analysed using a standard scheme based on the calculation of the mutual information in bipartite subsystems of the tripartite Alice–Eve–Bob system [14].

2. Peculiarities of a protocol with the continual alphabet

From the practical point of view, a protocol with the continual alphabet differs from protocols with the discrete alphabet in the basis-reconciliation procedure. For discrete alphabets, an exact reconciliation of bases is fulfilled, i.e., Alice and Bob select only the part of messages that were transmitted and received by using the same basis. For the continual alphabet, the bases cannot be reconciled exactly because the amount of information about a point of a continuum is infinite. Therefore, we propose to reconcile the bases for the continual alphabet *approximately*. For this purpose, we divide the entire space of states into several regions with approximately identical states and will reconcile the bases by transmitting information on the number of the region to which the basis belongs. The two bases found in the same region are considered coincident.

It is clear that such a procedure will produce additional errors caused by the nonzero projection of the state vector coding the message '0' in the basis $\{|\nu\rangle, |\tilde{\nu}\rangle\}$ to the state vector coding the message '1' in another basis $\{|\mu\rangle, |\tilde{\mu}\rangle\}$, even if these bases fell into the same region. Let us calculate the amount of information I in one qubit in the case of approximately reconciled bases:

$$I = 1 + \int |\langle\mu|\nu\rangle|^2 \log_2 |\langle\mu|\nu\rangle|^2 \mathrm{d}V_\nu \mathrm{d}V_\mu \Big/ \int |\langle\mu|\nu\rangle|^2 \mathrm{d}V_\nu \mathrm{d}V_\mu, \quad (1)$$

where integration is performed over the selected basis-reconciliation region into which the states $|\nu\rangle$ and $|\mu\rangle$ fall; and $\mathrm{d}V_\nu$, and $\mathrm{d}V_\mu$ are the differentials of the volume on the Bloch sphere. We assume for simplicity that the regions into which the Bloch sphere is divided are circular with the radius R and that $2N^2$ circles with the radius $\pi/2N$ can certainly cover the entire Bloch sphere (with the unit radius). Then, we obtain the dependence of the amount of information in a qubit on the number of regions presented in Table 1.

Table 1. Dependence of the amount of information per qubit on the number of regions in the case of approximately reconciled bases.

Number of regions	2	8	18	32	50	72	98
Amount of information (bit)	0.469	0.801	0.906	0.946	0.965	0.976	0.982

As the number of regions increases and, hence, the size of each region decreases, information contained in one qubit increases approximately from 0.47 bit for two regions to 1 bit in the limit of an infinite number of regions. Note that the increase in the number of regions results in the proportional increase in the amount of additional information about the region number in the basis reconciliation and also in a proportional decrease in the number of messages selected after the basis reconciliation.

Another specific feature of the protocol with the continual alphabet is the quantitative estimate of the measure of eavesdropper interference. One of the most widespread characteristics is the quantum bit error rate (QBER): $Q = 1 - N/N_{\max}$, where N is the number of correctly transmitted letters and $N_{\max}$ is the total number of transmitted letters. The use of the QBER as the measure of eavesdropper interference assumes implicitly that QBER is zero in the absence of the eavesdropping. Indeed, a message transmitted through a perfect quantum channel with exactly reconciled bases contains no errors. However, in the protocol with the continual alphabet it is impossible to reconcile bases exactly, and the QBER is nonzero even in the absence of eavesdropping, so that it obviously does not characterise the real measure of eavesdropper interference.

To solve this contradiction, we propose to estimate the data transmission accuracy by the relative amount of correctly transmitted information rather than by number of correctly transmitted letters. Then, the error rate can be defined as $\tilde{Q} = 1 - I/I_{\max}$, where I is the amount of information per qubit in the presence of eavesdropping, and $I_{\max}$ is the maximum amount of information in the absence of eavesdropping. Similarly to the QBER, this quantity can be called the mutual information error rate (MIER). One can see that the MIER correctly characterises the level of eavesdropper interference even for the protocol with the continual alphabet with the approximately reconciled bases. Below, it is convenient to use both these characteristics, the QBER and MIER, assuming on default that when the QBER is used, the limiting case of exactly reconciled bases takes place.

3. The intercept–resend strategy

The simplest eavesdropping strategy is the measurement by Eve of the transmitted qubit in some basis and the subsequent transmission of the result of the measurement to Bob – the so-called intercept–resend strategy. It is clear that in this case, Eve exactly knows what Bob receives, and no secret communication between Alice and Bob can be achieved. Therefore, the maximum error rate, at which the secret communication is possible, does not exceed the error rate caused by the intercept – resend strategy, i.e., the calculation of these errors gives the upper bound of the efficiency of the QC protocols.

Let us assume that Alice sent a state $|\alpha\rangle$ to Bob, while Eve eavesdropped this state by using the basis $\{|\psi\rangle, |\psi_\perp\rangle\}$. Then, Eve obtained the result $|\psi\rangle$ with the probability $|\langle\psi|\alpha\rangle|^2$ or the result $|\psi_\perp\rangle$ with the probability $|\langle\psi_\perp|\alpha\rangle|^2$ and sent the obtained result to Bob. After measuring the transmitted states $|\psi\rangle$ and $|\psi_\perp\rangle$ in the basis $\{|\alpha\rangle, |\alpha_\perp\rangle\}$, Bob will obtain a correct result – the state $|\alpha\rangle$ with the probabilities $|\langle\psi|\alpha\rangle|^2$ and $|\langle\psi_\perp|\alpha\rangle|^2$ and an incorrect result – the state $|\alpha_\perp\rangle$ with the probabilities $|\langle\psi|\alpha_\perp\rangle|^2$ and $|\langle\psi_\perp|\alpha_\perp\rangle|^2$. The total probability for obtaining a correct result by Bob is $|\langle\psi|\alpha\rangle|^4 + |\langle\psi_\perp|\alpha\rangle|^4$, and the error appearing probability is correspondingly $Q_{\alpha\psi} = 1 - |\langle\psi|\alpha\rangle|^4 - |\langle\psi_\perp|\alpha\rangle|^4$.

To calculate the QBER, it is necessary to average $Q_{\alpha\psi}$ over all the Alice bases $\{\alpha\}$ and to minimise the result of averaging over the Eve bases $\{\psi\}$:

$$Q = \sum_{\{\alpha\}} \sum_{\{\psi\}} Q_{\alpha\psi}/(N_\alpha N_\psi),$$

where N_α and N_ψ are the numbers of bases in the Alice and Eve alphabets. For the protocol with the continual alphabet, the corresponding integration is performed instead of summation. The results of calculations are presented in Table 2. The maximum possible error rate equal to 1/3 is provided by protocols with alphabets containing 6 and 8 letters and by the protocol with the continual alphabet. Protocols with 12 and 20 letters have a somewhat lower error rate equal to $74/225 \simeq 0.329$. Note a specific feature of the four-letter protocol with the tetrahedral alphabet, which is absent in Table 2. Because tetrahedron has no central symmetry, the letters in such an alphabet do not form the sets of orthogonal bases, and the basis-reconciliation procedure in the standard form is not performed for this protocol.

Table 2. QBER caused by the intercept – resend strategy.

Number of alphabet letters	6	8	12	20	∞
QBER	0.333	0.333	0.329	0.329	0.333

4. Optimal eavesdropping strategy

It was proved [15] that a safe connection between Alice and Bob is possible if Bob receives from Alice more information than Eve from Alice or Bob, i.e.,

$$I_{\mathrm{AB}} > \max\left(I_{\mathrm{AE}}, I_{\mathrm{BE}}\right). \tag{1}$$

Consider the optimal eavesdropping strategy, when Eve extracts the maximum of information from the eavesdropped message at the given level of interference producing the corresponding error rate, which can be written as

$$I_{\mathrm{AE,BE}} = \max_{I_{\mathrm{AB}}=\mathrm{const}} I_{\mathrm{AE,BE}}. \tag{2}$$

Note that this strategy can differ from optimal cloning [16].

Without loss of generality we can assume that in the case of optimal eavesdropping, Eve performs the unitary transformation U_{BE} with the state $|\beta\rangle_{\mathrm{B}}$ transmitted from Alice to Bob and with the probe Eve state $|0\rangle_{\mathrm{E}}$ connected to the information channel (if the transformation performed by Eve is nonunitary, it corresponds to some unitary transformation in an extended system with the subsequent averaging over a part of variables, which adds no new information to her and presents no additional problems for Alice and Bob). This unitary transformation acts on the basis elements as

$$\begin{aligned} |0\rangle_{\mathrm{B}}|0\rangle_{\mathrm{E}} &\xrightarrow{U_{\mathrm{BE}}} |0\rangle_{\mathrm{B}}|\Phi_{00}\rangle_{E} + |1\rangle_{\mathrm{B}}|\Phi_{01}\rangle_{\mathrm{E}}, \\ |1\rangle_{\mathrm{B}}|0\rangle_{\mathrm{E}} &\xrightarrow{U_{\mathrm{BE}}} |0\rangle_{\mathrm{B}}|\Phi_{10}\rangle_{E} + |1\rangle_{\mathrm{B}}|\Phi_{11}\rangle_{\mathrm{E}}. \end{aligned} \tag{4}$$

The unitarity assumes the existence of restrictions following from the conditions of the orthogonality preservation $\langle\Phi_{00}|\Phi_{10}\rangle + \langle\Phi_{01}|\Phi_{11}\rangle = 0$ and the normalisation $|\Phi_{00}|^2 + |\Phi_{01}|^2 = |\Phi_{10}|^2 + |\Phi_{11}|^2 = 1$.

Taking these restrictions into account, the set of all the states $|\Phi_{ij}\rangle$ can be represented as a superposition of only two basis states

$$\begin{pmatrix} |\Phi_{00}\rangle \\ |\Phi_{01}\rangle \\ |\Phi_{10}\rangle \\ |\Phi_{11}\rangle \end{pmatrix} = \begin{pmatrix} \gamma_{00} & \gamma_{01} \\ \gamma_{10} & \gamma_{11} \\ \gamma_{11} & \gamma_{10} \\ \gamma_{01} & \gamma_{00} \end{pmatrix} \begin{pmatrix} |0\rangle_{\mathrm{E}} \\ |1\rangle_{\mathrm{E}} \end{pmatrix}, \tag{5}$$

where all the coefficients of transformation (5) are expressed in terms of two parameters (θ and φ) controlled by Eve: $\gamma_{mn} = (-1)^{mn}\cos(\theta - m\pi/2)\cos(\varphi - n\pi/2)$.

The initial density matrix $\hat{\rho}^{(1)}_{\mathrm{EB}}(\alpha) = |0\rangle_{\mathrm{E}}\langle 0|_{\mathrm{E}} \otimes |\alpha\rangle_{\mathrm{B}}\langle\alpha|_{\mathrm{B}}$ of the Bob – Eve system is transformed to the final matrix $\hat{\rho}^{(2)}_{\mathrm{EB}}(\alpha)$, which is used to obtain the joined tripartite probability distribution:

$$P_{\mathrm{ABE}}(\alpha, \beta, \varepsilon) = \mathrm{Tr}_{\mathrm{BE}}[(|\varepsilon\rangle_{\mathrm{E}}\langle\varepsilon|_{\mathrm{E}} \otimes |\beta\rangle_{\mathrm{B}}\langle\beta|_{\mathrm{B}})\hat{\rho}^{(2)}_{\mathrm{EB}}(\alpha)]\mathrm{d}V_{\mathrm{E}}\mathrm{d}V_{\mathrm{B}}. \tag{6}$$

The natural characteristic for the calculation of the amount of information is the standard information Shannon functional

$$I_{XY}[P_{XY}] = S[P_X] + S[P_Y] - S[P_{XY}], \tag{7}$$

where $S[P]$ is the classical Shannon entropy [17] defined on the joined ($P = P_{XY}$) and partial ($P = P_X, P_Y$) probability distributions. By averaging (6) over the third system, we obtain bipartite probability distributions and, by using (7), the corresponding dependences of the information I_{AB}, I_{AE}, and I_{BE} on the parameters θ and φ in the Alice – Bob, Alice – Eve, and Bob – Eve systems.

A comparison of these dependences shows that the condition $I_{\mathrm{AE}} \geqslant I_{\mathrm{BE}}$ is fulfilled for any values of the parameters θ and φ. Therefore, there is no need to consider below the dependence of the information I_{BE}, and the safety condition (2) is transformed to the relation $I_{\mathrm{AB}} > I_{\mathrm{AE}}$.

Analysis of the optimal eavesdropping condition (3) shows that this condition is fulfilled in the region of values of parameters $\theta = \pi/4$. Taking into account that the dependences of I_{AE} and I_{AB} are symmetric with respect to $\theta = \varphi$, Fig. 1 shows only one-parametric dependences $I_{\mathrm{AB}}(\theta)$ when the optimal eavesdropping condition (3) is fulfilled.

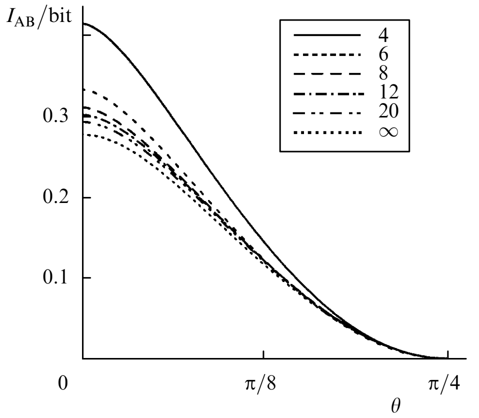

Figure 1. Dependence of the amount of information I_{AB} in the Alice–Bob system on the parameter θ for protocols using 4, 6, 8, 12, and 20 letters and the protocol with the continual alphabet (infinite number of letters).

Because of the symmetry $I_{AB}(\theta, \varphi) = I_{AE}(\varphi, \theta)$ and the optimality condition $\theta = \pi/4 - \varphi$, the security condition $I_{AB} > I_{AE}$ is fulfilled up to the critical value $\theta_0 = \pi/8$ at which the information eavesdropped by Eve is equal to the information received by Bob. The critical error rates $\tilde{Q}_0$ for protocols under study are presented in Table 3, from which it follows that, when the bases are not reconciled, the protocol with the tetrahedral alphabet has the highest critical error rate.

Table 3. Critical error rate $\tilde{Q}_0$ in the absence of the basis reconciliation.

Number of alphabet letters	4	6	8	12	20	∞
MIER	0.650	0.630	0.607	0.597	0.589	0.600

Note that the direct calculation of the amount of information is not connected with its *coding*. Most often binary coding is used, when '0' is assigned to one of the states from the orthogonal pair and '1' is assigned to another state, which is related to the basis-reconciliation procedure. Coding in the continual alphabet is similar to standard QC protocols because for any letter from the continual alphabet the orthogonal letter exists. The method of dividing the Bloch sphere into orthogonal pairs is arbitrary, only the division into regions should be taken into account by reconciling approximately the bases. It can be divided, for example, into the upper part of the Bloch sphere coding '0' and the lower part coding '1'.

Because the letters of the tetrahedral alphabet do not form orthogonal pairs, another coding should be used for them, where '0' is assigned to two arbitrary letters and '1' is assigned to the two remaining letters.

Consider now the role of the basis reconciliation. We assume that Alice and Bob perform security reconciliation of the bases, i.e., Eve does not affect the selection of data, does not introduce any false messages into the open communication channel and does not perform additional transformations with her probe state after the basis reconciliation, i.e., her information does not increase after basis reconciliation.

The information I_{AB} that Bob receives from Alice after the basis reconciliation proportionally increases compared to the case without the basis reconciliation and achieves a maximum value of 1 bit per message (an exact basis reconciliation for the protocol with the continual alphabet is assumed). The security condition $I_{AB} > I_{AE}$ is now fulfilled up to the other values of θ_0 (compared to the case of the absence of the basis reconciliation), which depend on the specific protocol. In this case, the critical error rate also increases (see Table 4).

Table 4. Critical error rate $\tilde{Q}_0$ in the case of the basis reconciliation.

Number of alphabet letters	6	8	12	20	∞
MIER	0.806	0.805	0.804	0.805	0.811

After the basis reconciliation, the protocol with the continual alphabet has the highest error rate, which is valid in the limiting case of an exact basis reconciliation. For the tetrahedral alphabet, the basis-reconciliation procedure is not performed in a standard form, so that Table 4 does not contain the corresponding result.

5. Experimental realisation

Figure 2 shows the experimental scheme for realisation of the QC protocols considered above, where the letters are coded by polarisation of photons.

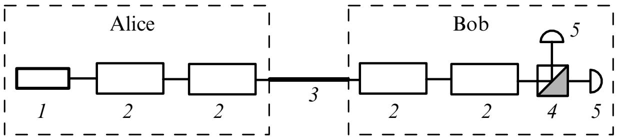

Figure 2. Experimental scheme for realising QC protocols: (*1*) source of single photons; (*2*) Pockels cell; (*3*) quantum channel; (*4*) polarisation beamsplitter; (*5*) photon counter.

On the Alice side, photons are generated with an arbitrary quantum polarisation state. This can be realised using source (*1*) of single photons with fixed polarisation, for example, a laser emitting single photons. A set of letters forming the alphabet of the protocol being realised is specified by a set of point at the Bloch sphere and is determined by a set of the angles of rotation of the polarisation basis, for example, with the help of two Pockels cells (*2*), where the first cell rotates the vertical component of polarisation, while the second cell rotates the horizontal component. Instead of Pockels cells, quarter-wave polarisation plates can be also used by rotating them through the angles corresponding to the selected alphabet. To the alphabets with a finite discrete set of letters, a finite discrete set of the angles of rotation of polarisation will correspond, while to the continual alphabet – a continuous set of the angles of rotation of polarisation.

The received photon with an arbitrary polarisation state is then transmitted to Bob through polarisation-preserving quantum channel (*3*), for example, in the open space. On the Bob side, the polarisation of each photon is transformed according to the selected alphabet, as has been done on the Alice side, but in the reverse order, so that a photon after the transformation would be in the fixed polarisation basis, in which it is measured with the help of polarisation beamsplitter (*4*) and photon counter (*5*).

The above scheme for the transmission of quantum letters should be supplemented with a classical unclassified communication channel, which Alice and Bob use for communicating the unclassified information to realise the open stages of the transmission of the quantum key, for example, to calculate the error rate, basis reconciliation, testing the security condition, etc.

6. Conclusions

Our analysis has shown that even when the two-dimensional space of quantum states is used, the critical error rate of the six-state protocol can be exceeded by varying the alphabet used. In the absence of the basis reconciliation, the protocol with the tetrahedral alphabet has a higher critical error rate than the six-state protocol, while in the case of the reconciled bases, the protocol with the continual alphabet has the highest critical error rate.

Acknowledgements. This work was partially supported by the Russian Foundation for Basic Research (Grant Nos 02-03-32200 and 04-02-17554) and the INTAS Grant INFO 00-479.

References

1. Bennett Ch.H., Brassard G., in *Proc. IEEE Intern. Conf. on Computer, System Signal Processing* (New York: IEEE, 1984) p. 175.
2. Ekert A.K. *Phys. Rev. A*, **67**, 661 (1991).
3. Bennett Ch.H. *Phys. Rev. Lett.,* **68**, 3121 (1992).
4. Bruss D. *Phys. Rev. Lett.*, **81**, 3018 (1998).
5. Grosshans F., Grangier P. *Phys. Rev. Lett.*, **88**, 057902 (2002).
6. Wootters W.K., Zurek W.H. *Nature* (London), **299**, 802 (1982).
7. Stucki D., Gisin N., Guinnard O., Ribordy G., Zbinden H. *New J. Phys.*, **4**, 41.1 (2002).
8. Bechmann-Pasquinucci H., Gisin N. *Phys. Rev. A*, **59**, 4238 (1999).
9. Gottesman D., Lo H.-K. *IEEE Trans. Inf. Theory*, **49**, 457 (2003).
10. Bechmann-Pasquinucci H., Tittel W. *Phys. Rev. A*, **61**, 062308 (2000).
11. Bourennane M., Karlsson A., Bjork G. *Phys. Rev. A*, **64**, 012306 (2001).
12. Cerf N.J., Bourennane M., Karlsson A., Gisin N. *Phys. Rev. Lett.*, **88**, 127902 (2002).
13. Born M., Wolf E. *Principles of Optics, 4th ed.* (Oxford: Pergamon Press, 1969; Moscow: Nauka, 1973) p. 50.
14. Gisin N., Ribordy G., et al. *Rev. Mod. Phys.*, **74**, 145 (2002).
15. Bennett C.H., Brassard G., Robert J.M. *SIAM J. Comput.*, **17**, 210 (1988).
16. Fuchs C.A., Gisin N., Griffiths R.B., Niu C.-S., Peres A. *Phys. Rev. A*, **56**, 1163 (1997).
17. Gallagher R.G. *Information Theory Reliable Communication* (New York: John Wiley and Sons, 1968).