Optimal Eavesdropping in Quantum Cryptography with Six States

Dagmar Bruß
ISI, Villa Gualino, Viale Settimio Severo 65, 10133 Torino, Italy

(Received 7 May 1998)

A generalization of the quantum cryptographic protocol by Bennett and Brassard is discussed, using three conjugate bases, i.e., six states. By calculating the optimal mutual information between sender and eavesdropper it is shown that this scheme is safer against eavesdropping on single qubits than the one based on two conjugate bases. We also address the question for a connection between the maximal classical correlation in a generalized Bell inequality and the intersection of mutual informations between sender/receiver and sender/eavesdropper. [S0031-9007(98)07272-X]

PACS numbers: 03.67.Dd, 03.65.Bz

In 1984 Bennett and Brassard [1] suggested a quantum cryptographic protocol, in the following called BB84, which enables two parties to establish a secret key, using principles of quantum mechanics. In this scheme the sender of the quantum information, usually called Alice, transmits quantum bits in the basis $|0\rangle, |1\rangle$ or the conjugate basis $|\bar{0}\rangle, |\bar{1}\rangle$, defined by

$$\begin{aligned} |\bar{0}\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |\bar{1}\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \end{aligned} \tag{1}$$

to the receiver Bob, who performs measurements in these bases. After classical communication via a public channel, a secret key can be established by using only those cases in which the bases of Alice and Bob coincide.

In this paper we want to discuss a generalized scheme which is based on the use of three rather than two bases. The third one used in addition to the previous ones is denoted by $|\bar{\bar{0}}\rangle, |\bar{\bar{1}}\rangle$ and defined by

$$\begin{aligned} |\bar{\bar{0}}\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \\ |\bar{\bar{1}}\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle). \end{aligned} \tag{2}$$

In the Bloch vector picture a density matrix ϱ is written as $\varrho = \frac{1}{2}(\mathbb{1} + \vec{s} \cdot \vec{\sigma})$, with $\vec{s}$ being the Bloch vector and $\vec{\sigma}$ the Pauli matrices. The six states can be viewed as Bloch vectors pointing along the positive and negative x, y, and z directions. Alice sends one of these, denoted as $|\psi^{in}\rangle$, with equal probability.

Such a scenario is a straightforward extension of the traditional protocol and its possibility has been mentioned at various occasions [2]. Our main purpose is to point out that this generalized scheme is principally more secure than the one in [1]. This is due to the fact that the optimal strategy an eavesdropper, traditionally called Eve, can design to gather information by performing some unitary transformation on the quantum bit in transit gives her, in our scenario, less information for a fixed disturbance of Bob's qubit. As Alice increases the set of inputs, it is more difficult for Eve to learn something in transit.

It was conjectured in [3] and shown in [4] that in the BB84 scenario the disturbance corresponding to Bob and Eve possessing the same information with respect to Alice exhibits a connection to the Clauser-Horne-Shimony-Holt (CHSH) inequality. After deriving Eve's optimal strategy we will ask whether, in the generalized protocol, the crossing point between the two relevant mutual informations has a connection to a generalized Bell inequality where Alice and Bob use the observables $\vec{a}_i \cdot \vec{\sigma}^a$ and $\vec{b}_i \cdot \vec{\sigma}^b$, $\{i = 1, 2, \ldots, n\}$, respectively, with the Bloch vectors $\vec{a}_i, \vec{b}_i$ spanning not only a plane, but the Bloch sphere.

After this introduction and outline of the paper, let us derive the eavesdropping strategy that is optimal with respect to the mutual information between Alice and Eve, I^{AE}. We do not consider collective or coherent attacks, but only interaction with single qubits. The most general unitary transformation Eve can design is of the form

$$U|0\rangle|X\rangle = \sqrt{F}\,|0\rangle|A\rangle + \sqrt{1-F}\,|1\rangle|B\rangle, \tag{3}$$

$$U|1\rangle|X\rangle = \sqrt{F}\,|1\rangle|C\rangle + \sqrt{1-F}\,|0\rangle|D\rangle. \tag{4}$$

The first qubit is the one sent to Bob and acted on by Eve. Eve's initial state is $|X\rangle$, and $|A\rangle, |B\rangle, |C\rangle, |D\rangle$ refer to her normalized states after the interaction. It was shown in [5] that it is sufficient for Eve to use two qubits in order to extract the maximal information. The fidelity of Bob's bit is F and is taken to be in the interval $1/2 \leq F \leq 1$.

We assume Eve to be clever enough to treat all six possible states in the same way (i.e., with same disturbance for Bob)—otherwise Alice and Bob could find out about her existence by comparing error rates in different bases. This assumption results in three constraints which the scalar products of Eve's states have to fulfill:

$$\begin{aligned} \langle B \,|\, D\rangle &= 0, \\ \mathrm{Re}\langle C \,|\, A\rangle &= 2 - \frac{1}{F}, \\ \langle A \,|\, B\rangle + \langle D \,|\, C\rangle &= 0. \end{aligned} \tag{5}$$

Unitarity of the matrix U means

$$\langle A \,|\, D\rangle + \langle B \,|\, C\rangle = 0. \tag{6}$$

The mutual information between Alice and Bob is given by

$$I^{AB} = 1 + D \log D + (1 - D)\log(1 - D), \tag{7}$$

© 1998 The American Physical Society

where D is the disturbance of Bob's qubit, defined by

$$D = 1 - F = 1 - \langle \psi^{in} | \varrho^B | \psi^{in} \rangle, \qquad (8)$$

and ϱ^B is the right-hand side of Eqs. (3) and (4), traced over Eve's bits. All logarithms are taken to base 2. By construction, Bob's disturbance is the same no matter which state was sent by Alice. The procedure to calculate the mutual information between Alice and Eve is more involved. We expand

$$|A\rangle = \alpha_A |00\rangle + \beta_A |10\rangle + \gamma_A |01\rangle + \delta_A |11\rangle, \qquad (9)$$

where the complex coefficients have to satisfy

$$|\alpha_A|^2 + |\beta_A|^2 + |\gamma_A|^2 + |\delta_A|^2 = 1, \qquad (10)$$

and similarly for $|B\rangle, |C\rangle, |D\rangle$. We are free to choose $|B\rangle$ as one of the four basis vectors; e.g., $|B\rangle = |00\rangle$ and can fulfill the first constraint in Eq. (5) by setting $|D\rangle = |11\rangle$, without loss of generality. We then find for the mutual information the form

$$I^{AE} = 1 + \tfrac{1}{2} \{ \tau[F|\alpha_A|^2 + (1 - F), F|\alpha_C|^2] + \tau[F|\beta_A|^2, F|\beta_C|^2] + \tau[F|\gamma_A|^2, F|\gamma_C|^2] + \tau[F|\delta_A|^2 + (1 - F), F|\delta_C|^2] \}, \qquad (11)$$

where we define

$$\tau[x, y] = x \log x + y \log y - (x + y) \log(x + y). \qquad (12)$$

Note that $-\tau[x, 1 - x]$ is the entropy function. Equation (11) is the mutual information which Eve reaches when postponing the measurement until she learns which basis was used by listening to the public channel.

The task is to maximize I^{AE} with the constraints of Eqs. (5) and (6). The method of Lagrange multipliers leads to a set of equations which cannot be simultaneously fulfilled unless $\alpha_A = \alpha_C = 0$ and $\delta_A = \delta_C = 0$. This means that the best solution for Eve is to use states such that $\langle A | B \rangle = 0 = \langle C | D \rangle$, which one would have expected.

Now we have only two parameters, $|\beta_A|$ and $|\beta_C|$ for I^{AE}, and can write

$$I^{AE} = 1 + \tfrac{1}{2} F \{ \tau[|\beta_A|^2, |\beta_C|^2] + \tau[(1 - |\beta_A|^2), (1 - |\beta_C|^2)] \}, \qquad (13)$$

which is a concave function. Here we have used

$$\tau[Fx, Fy] = F \tau[x, y]. \qquad (14)$$

It is straightforward to write down the system of equations which has to be fulfilled in order to maximize I^{AE}. Because of their high symmetry, one can find one solution easily, namely,

$$|\beta_A|^2 = 1 - |\beta_C|^2, \qquad (15)$$

and thus

$$I^{AE} = 1 + F \tau[|\beta_A|^2, 1 - |\beta_A|^2]. \qquad (16)$$

By checking the higher derivatives, one confirms that this is a maximum, which is, due to concavity, the absolute maximum. Inserting into the second line of Eq. (5) allows us to find the "best" relative phase between $|A\rangle$ and $|C\rangle$ and thus leads to the solution for the highest mutual information that Eve can extract from measuring her two qubits,

$$I^{AE} = 1 + (1 - D) \{ f(D) \log f(D) + [1 - f(D)] \times \log[1 - f(D)] \}, \qquad (17)$$

$$f(D) = \tfrac{1}{2} \left(1 + \frac{1}{1 - D} \sqrt{D(2 - 3D)} \right).$$

This function is shown in Fig. 1, where we also give the corresponding mutual information for BB84, taken from [4], for the purpose of comparison. (I^{AB} is identical in both cases.) Note that our curve lies everywhere below the one for the BB84 case. The six-state protocol is therefore more secure against eavesdropping on single qubits.

In our case, both bits of Eve carry mutual information, unlike the one described by [4]. If she would either measure only one of her two bits, or if she would use a one-bit probe from the beginning, her maximal information would be

$$I^{AE,1\,\mathrm{bit}} = 1 + f_1(D) \log f_1(D) + [1 - f_1(D)] \log[1 - f_1(D)], \qquad (18)$$

$$f_1(D) = \tfrac{1}{2} [1 + D + \sqrt{D(2 - 3D)}],$$

which is the lowest curve in Fig. 1. The calculation for the one-bit probe follows the same line as explained above for the two-bit probe, but is less involved. Note that in order to maximize her mutual information in the six-state scheme

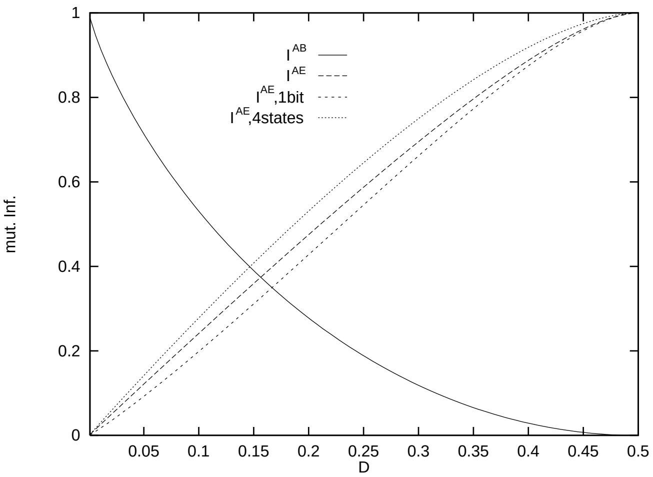

FIG. 1. Maximal mutual information I^{AE} between Alice and Eve as a function of Bob's disturbance D. The upper curve holds for BB84 [4] and is shown for the purpose of comparison. The lower curves refer to the six-state protocol. Their analytic forms are shown in Eqs. (17) and (18). The mutual information between Alice and Bob is in both scenarios given by the curve I^{AB}.

Eve necessarily needs two qubits as a resource, whereas for BB84 a one-bit probe is sufficient to reach optimality [6].

It is worth mentioning that the optimal unitary transformation which leads to Eq. (17) disturbs *all* Bloch vectors in the same way, not only the six states used by Alice, and allows Eve to gain the same information in *all* possible bases. In other words, the optimal eavesdropping action for six states is a universal transformation. This means that using a bigger number of states cannot increase security. The gain in security described in this paper is due to the fact that the three bases are spanning the full Bloch sphere, as opposed to the case of BB84 where only a two-dimensional plane is spanned.

The scheme described in [1] can also be realized by Alice and Bob sharing a singlet, i.e., a maximally entangled state. This was discussed in [7,8]. In this case, which we will consider for the rest of this article, Alice and Bob can test for eavesdropping by calculating S, the correlation coefficient in the CHSH inequality. Without any disturbance of Bob's bit they will find $|S| = 2\sqrt{2}$. This value is decreased when Eve interacts unitarily with Bob's bit. As was shown in [4], the intersection of the two curves for I^{AB} and I^{AE} corresponds to $|S| = 2$; i.e., at disturbances $D \geq \frac{1}{2}(1 - 1/\sqrt{2})$ the CHSH inequality (between Alice and Bob) is not violated.

The natural question arises whether the corresponding intersection for the generalized scheme is related to a generalized Bell inequality. In the six-state protocol the reduced density matrix of Alice and Bob after Eve's interaction reads

$$\rho^{AB} = \frac{1}{2}\begin{pmatrix} D & 0 & 0 & 0 \\ 0 & 1-D & 2D-1 & 0 \\ 0 & 2D-1 & 1-D & 0 \\ 0 & 0 & 0 & D \end{pmatrix}, \qquad (19)$$

where the matrix elements are written in the order 00, 10, 01, 11. For *any* number of measurement directions that Alice and Bob can use to test a Bell inequality, we find

$$|S(D)| = |S_q|(1 - 2D), \qquad (20)$$

where S_q denotes the correlation for $D = 0$, i.e., the undisturbed singlet. Thus in our case the measurement directions that are optimal for the singlet are also optimal for $D \neq 0$, i.e., a mixed state. This does not hold in general [9]. We will refer to the disturbance where $|S(D)| = |S_c|$, i.e., where S reaches the classical limit, as D_c.

Let us first look at the case where Alice and Bob are using two measurement directions each that do not necessarily lie in a plane. Here the inequality for a model with local hidden variables reads $|S| \leq 2$.

We can make use of Cirel'son's inequality [10] in which the norm of the operator

$$\begin{aligned} C = {}& \vec{a}_1 \cdot \vec{\sigma}^a \otimes \vec{b}_1 \cdot \vec{\sigma}^b + \vec{a}_2 \cdot \vec{\sigma}^a \otimes \vec{b}_1 \cdot \vec{\sigma}^b \\ & + \vec{a}_2 \cdot \vec{\sigma}^a \otimes \vec{b}_2 \cdot \vec{\sigma}^b - \vec{a}_1 \cdot \vec{\sigma}^a \otimes \vec{b}_2 \cdot \vec{\sigma}^b \qquad (21) \end{aligned}$$

is shown to obey $\|C\| \leq 2\sqrt{2}$. (Here $\vec{a}_i$ refer to Alice's directions of measurement and $\vec{b}_i$ to those of Bob.) This means that the maximal value the quantum correlation can take is $|S_q| = 2\sqrt{2}$, no matter whether the measurement directions span a plane or a sphere. This value is reached in the CHSH scenario. One can intuitively understand this in the following way: in order to maximize the sum of scalar products of the measurement directions, their relative angles have to be as small as possible; i.e., they have to lie on a great circle of the sphere. Thus we cannot find a ratio for $|S_q/S_c|$ that is higher than $\sqrt{2}$, and therefore we cannot establish a Bell inequality in the sphere that corresponds to the intersection of I^{AE} with I^{AB} for the generalized protocol, because here D_c is larger than in BB84.

We can generally exclude such a correspondence for n measurements by each party, i.e., chained Bell inequalities [11]: the inequality reads now $|S| \leq 2n - 2$. The relevant operator C for this case can be written as a sum of operators of the form used in Cirel'son's inequality which we call $C_1, \ldots, C_{n-1}$. Because of the inequality

$$\begin{aligned} \|C\| &= \|C_1 + C_2 + \ldots + C_{n-1}\| \\ &\leq \|C_1\| + \ldots + \|C_{n-1}\| \leq (n-1)2\sqrt{2}, \qquad (22) \end{aligned}$$

we know an upper limit of the quantum correlation. Thus we find $|S_q/S_c| \leq \sqrt{2}$ as in the paragraph above and can generally exclude the mentioned connection.

Note that inequalities such as the original Bell inequality and a recent suggestion by Ardehali [12] where two directions of measurement coincide cannot be used for our purpose: the eavesdropping interaction causes the expectation value $\langle \vec{a} \cdot \vec{\sigma}^a \otimes \vec{a} \cdot \vec{\sigma}^b \rangle$ to be smaller than 1 if $D > 0$.

In summary, we have discussed a quantum cryptographic protocol based on six quantum states and shown that it is safer against eavesdropping on single qubits than the BB84 scheme, because Eve's maximal mutual information is smaller than in the BB84 scenario. Furthermore, in order to reach the maximal mutual information the eavesdropper needs to use a two-bit probe and thus has to perform a more complicated transformation than in BB84. If her resource consists of only one qubit, she gains even less information. We have to mention some practical disadvantage: in order to establish a key, one will here lose 2/3 of the signals rather than 1/2 in the BB84 scenario, when using equal probabilities for all states. We have also shown that the best way to test a CHSH inequality is to use measurement directions that lie in a plane. In the six-state protocol there is no natural relation between the classical limit of a Bell-type correlation coefficient and the intersection of the information curves. We hope that this cryptographic scheme may reach practical relevance in the light of recent suggestions to produce maximally entangled pairs of distant atoms [13] (see also [14]).

Valuable criticism and comments by Asher Peres and inspiring discussions with Alois Würger are gratefully acknowledged. Questions by Charles Bennett and Chris Fuchs motivated the paragraph about the use of more than six states. This work was supported by the European TMR Research Network ERP-4061PL95-1412.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[2] C. A. Fuchs (private communication); N. Gisin, contribution to the Torino Workshop, 1997; A. Peres (private communication).

[3] N. Gisin and B. Huttner, Phys. Lett. A **232**, 463 (1997).

[4] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

[5] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).

[6] C.-S. Niu and R. B. Griffiths (unpublished); E. Biham and T. Mor, Phys. Rev. Lett. **79**, 4034 (1997).

[7] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[8] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[9] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **200**, 340 (1995).

[10] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980); see also A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1995), p. 175.

[11] L. Braunstein and C. M. Caves, Ann. Phys. (N.Y.) **202**, 22 (1990).

[12] M. Ardehali, Phys. Rev. A **57**, 114 (1998).

[13] H.-J. Briegel, W. Dür, S. J. van Enk, J. I. Cirac, and P. Zoller, quant-ph/9712027.

[14] M. Pavičić, Opt. Commun. **142**, 308 (1997).