Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy

Christopher A. Fuchs,[1] Nicolas Gisin,[2] Robert B. Griffiths,[3] Chi-Sheng Niu,[3] and Asher Peres[4,*]
[1]*Norman Bridge Laboratory of Physics 12-33, California Institute of Technology, Pasadena, California 91125*
[2]*Group of Applied Physics, University of Geneva, CH 1211 Geneva 4, Switzerland*
[3]*Department of Physics, Carnegie-Mellon University, Pittsburgh, Pennsylvania 15213*
[4]*Institute for Theoretical Physics, University of California, Santa Barbara, California 93106*

(Received 31 January 1997)

We consider the Bennett-Brassard cryptographic scheme, which uses two conjugate quantum bases. An eavesdropper who attempts to obtain information on qubits sent in one of the bases causes a disturbance to qubits sent in the other basis. We derive an upper bound to the accessible information in one basis, for a given error rate in the conjugate basis. Independently fixing the error rates in the conjugate bases, we show that both bounds can be attained simultaneously by an optimal eavesdropping probe. The probe interaction and its subsequent measurement are described explicitly. These results are combined to give an expression for the optimal information an eavesdropper can obtain for a given average disturbance when her interaction and measurements are performed signal by signal. Finally, the relation between quantum cryptography and violations of Bell's inequalities is discussed. [S1050-2947(97)01708-3]

PACS number(s): 03.65.−w, 42.79.Sz, 89.70.+c

I. INTRODUCTION

In quantum cryptography, individual quanta are prepared in nonorthogonal quantum states to encode and carry information about cryptographic keys. In this way, an eavesdropper can acquire information about the key only at the risk of causing a detectable disturbance. The oldest and best known cryptographic scheme BB84 is due to Bennett and Brassard [1]: the information sender, called Alice, encodes each logical bit, 0 or 1, into the linear polarization of a single photon, along one of two conjugate bases of her choice, as shown in Fig. 1. The receiver, Bob, measures the polarization of the photon in one of the two bases, either x-y or u-v, randomly chosen by him. Only after that does Alice reveal to him the basis she used. This information is sent on a public channel that can be monitored, but not modified, by anyone else. Bob then likewise tells Alice whether he used the correct basis. If he did, Alice and Bob know one bit, that no one else ought to know.

After this protocol has been repeated many times, Alice and Bob sacrifice some of these secret bits by publicly comparing their values. This gives them an estimate of the noise on the channel, which may be due to either natural causes or to the presence of an eavesdropper (Eve). In the latter case, the maximal amount of information that Eve could have gathered is, in principle, fixed by the laws of quantum mechanics. If Eve's information is small enough compared to the noise she has induced, Alice and Bob may still be able to use *classical* methods of privacy amplification [2,3] in order to reduce Eve's information to an arbitrarily small level. It is therefore important to estimate the maximal amount of information that Eve may have acquired, for a given error rate observed by Bob.

There are many possible strategies for eavesdropping, some of which have been analyzed by other authors. Ekert and Huttner [4] examined a simple ''intercept-resend'' method, where Eve performs standard von Neumann measurements. Lütkenhaus [5] considered the use of positive operator-valued measures (POVM) [6] under the restriction that Eve performs her measurements before Alice reveals the basis. Recently, Gisin and Huttner [7] investigated an improved strategy for an eavesdropper restricted to a two-dimensional probe (a single qubit) interacting on line with each transmitted signal; in this case, the probe is measured after the basis is revealed. (Note, the result in Ref. [7] turns out not to be optimal, because only real values of certain parameters were employed [8].) These results, along with the optimal ones obtained in the present paper, are plotted in Fig. 2.

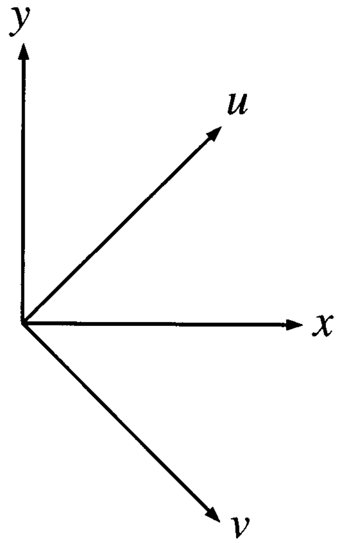

FIG. 1. The orthogonal bases x-y and u-v, that satisfy Eq. (2), are called *conjugate* to each other.

[*] Permanent address: Department of Physics, Technion–Israel Institute of Technology, 32 000 Haifa, Israel.

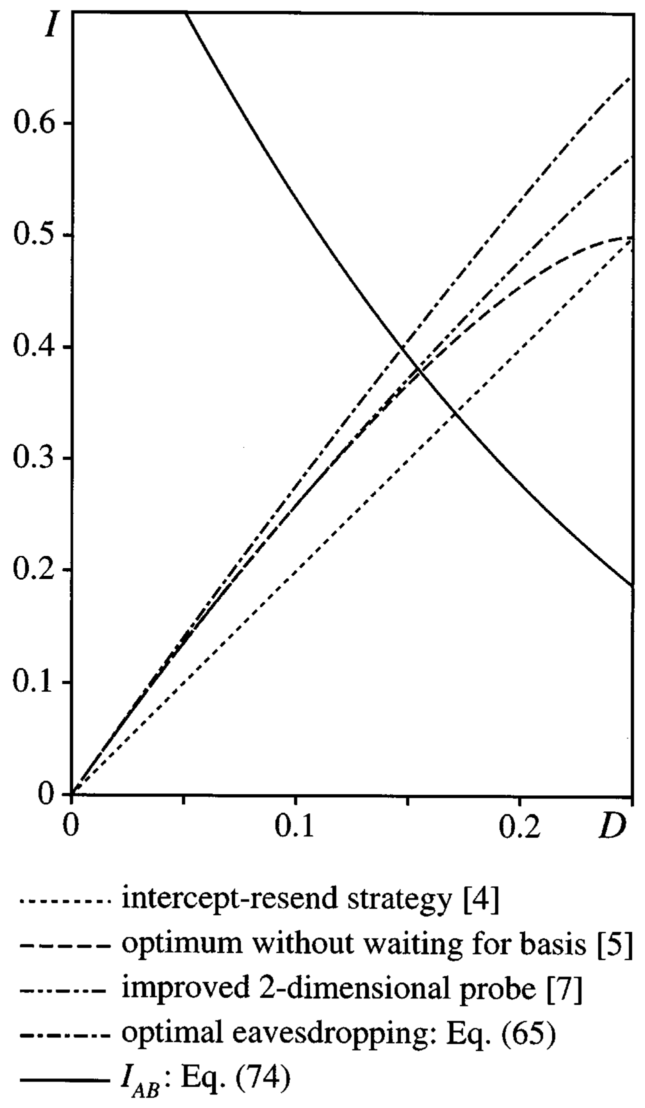

FIG. 2. Information vs disturbance for various eavesdropping methods.

The common feature of all these strategies is that they are restricted to interactions and measurements on each individual signal sent from Alice to Bob; there are no ‘‘collective’’ interactions or measurements on strings of signals, as might be the case if Eve were able perform quantum measurements on systems of an arbitrary size. Furthermore, none of the strategies allow Eve to delay her measurements until the completion of Alice and Bob’s privacy amplification, and none take into account the information leaked to her during the public communication phase of the protocol. The latter kind of information depends upon which bits are ultimately discarded and upon the specific algorithm used in the privacy amplification process. Finally, even within the restrictions set by this paradigm, none of the schemes can claim optimality in the sense of specifying the best possible ratio between Eve’s information gain and her induced disturbance.

The purpose of this paper is twofold. The first is to give a quantitative statement of the physical principle responsible for the operation of the BB84 protocol: an eavesdropper who attempts to obtain information in one basis causes a disturbance to the conjugate basis. The second—more relevant to practical quantum cryptography—is to derive the absolute best achievable information an eavesdropper can obtain about a single qubit, for a given average error rate caused to the signals. In both these tasks, we again work within the paradigm cited above. Namely, we assume that Eve may interact with only one signal at a time and may only make measurements on each individual probe. Furthermore, she may do this after Alice announces her basis, but before the execution of any error testing or privacy amplification protocols.

From the point of view of ultimate security in cryptography, these restrictions may be severe. On the other hand, with respect to experimental science, these assumptions are hardly limiting at all. Indeed it is only now becoming possible to make two qubits interact with one another in a controlled fashion [9], and it will be some time before the elementary quantum circuits [8,10] needed to realize the optimal strategy described here can actually be constructed. Finally, though an expression for the trade-off between information and disturbance in a less restrictive scenario may be eminently important for cryptography, such a relation—because of its dependence on the details of privacy amplification—lies somewhat beyond the scope of basic physics. For detailed discussions of quantum cryptographic security in the presence of collective attacks and privacy amplification, see Refs. [11–14].

The plan of our paper is as follows. In Sec. II, we derive a general bound that refers to the accessible information in one basis, corresponding to a given error rate in the *conjugate* basis. This is obtained without using any particular model for the eavesdropping interaction; the latter is assumed only to be unitary. It had been previously known that a four-dimensional probe (that is, one consisting of two interacting qubits) is the largest needed for achieving the optimal detection of signals emitted in a two-dimensional space [15]. There are, however, some cases for which a two-dimensional probe is sufficient [15]. In Sec. III we present an optimal strategy for BB84 using a four-dimensional probe of two qubits, which allows independent error rates in each basis, and simultaneously achieves both bounds. A quantum computational circuit representing the optimal strategy is described in the following paper [10]. Recently it has been shown that there is an optimal strategy using only a two-dimensional probe [8].

Finally, in Sec. IV, we address issues directly relevant to quantum cryptography by constructing the optimal trade-off relation for Eve’s overall accessible information in terms of the average error rate for both bases. This is obtained by two methods. The first relies on the work of the previous two sections; the second incorporates an argument based on a symmetrization technique. Note that both Secs. II and III concern fundamental physical questions. The ‘‘practically minded’’ cryptographer need only browse through them, and may then proceed directly to Sec. IV to find results relevant to privacy amplification [2]. In the concluding remarks we return to fundamental physics by outlining an intriguing connection between the optimal information-disturbance tradeoff and a violation of Bell’s inequality in the Bennett-Brassard-Mermin modification of the BB84 protocol [16]. This confirms an idea first expressed by Ekert [17] and recently made quantitative by Gisin and Huttner [7].

II. INFORMATION AND DISTURBANCE IN CONJUGATE BASES

If Eve performs standard (von Neumann type) measurements in the x-y basis, she does not disturb signals sent in that basis, but she completely randomizes those sent in the u-v basis, and vice versa. In this section, it will be shown that, quite generally, Eve's ability to obtain partial information on the signals sent in one of the bases is related to the disturbance caused to the signals sent in the other basis. This is relevant to eavesdropping on the BB84 protocol because it is the raw physical fact that allows its operation.

We take the framework for our problem directly from quantum cryptography. In order to take advantage of Alice's delayed information on the basis that was used, Eve's optimal strategy is the following: she lets a probe, initially in some standard state $|\psi_0\rangle$, interact unitarily with the qubit sent by Alice. (There is no loss of generality in this, because any physical nonunitary interaction is equivalent to a unitary one with a higher dimensional probe.) Eve's probe is then stored until Alice announces the basis that was used, and only after that is it measured by Eve.

In a convenient notation, if Alice sends state $|x\rangle$, the result may be written as

$$|x\rangle\otimes|\psi_0\rangle\rightarrow|X\rangle, \tag{1}$$

where $|X\rangle$ is an entangled state of the probe and the photon that Alice sent to Bob. Likewise, for the other signals that Alice may send, the results of Eve's intervention are entangled states, $|Y\rangle$, $|U\rangle$, and $|V\rangle$. Since the interaction is unitary, it follows from

$$|x\rangle=(|u\rangle+|v\rangle)/\sqrt{2},$$

$$|y\rangle=(|u\rangle-|v\rangle)/\sqrt{2}, \tag{2}$$

that

$$|X\rangle=(|U\rangle+|V\rangle)/\sqrt{2},$$

$$|Y\rangle=(|U\rangle-|V\rangle)/\sqrt{2}. \tag{3}$$

Eve's measurement on the probe may be of the standard type (an orthogonal projection valued measure) or, more generally, it may be of the POVM type [6], where the various outcomes correspond to a set of positive semidefinite operators that sum to the identity operator on the probe's Hilbert space. Since Eve waits until Alice reveals her basis, she may choose a POVM $\{E_\lambda\}$ when the x-y basis is sent, and a different POVM $\{F_\lambda\}$ when the u-v basis is sent.

Note that the interaction of Eve's probe with the qubit sent by Alice to Bob completely determines the mean error rate for signals sent in the x-y basis and those in the u-v basis. It also determines Eve's accessible information (i.e., her maximal information) for both types of signals. The aim of this section is to show that the accessible information for x-y signals is simply related to the mean error rate for u-v signals, and vice versa. These mean values are well defined regardless of which signal is sent in any single instance. In particular, there is nothing counterfactual about comparing the information in one basis with the error rate in the other basis.

Let us now set about our task. If Alice sent a signal $|x\rangle$, the probability that Eve detects outcome λ is

$$P_{\lambda x}=\langle X|\mathbf{1}\otimes E_\lambda|X\rangle, \tag{4}$$

and likewise for the other signals. Here, $\mathbf{1}$ is the identity operator for Alice and Bob's qubit. Let p_i be the prior probability that Alice sends signal i. The probability that Eve gets outcome λ when Alice uses the x-y basis is thus

$$q_\lambda=P_{\lambda x}p_x+P_{\lambda y}p_y\,. \tag{5}$$

If Eve observes outcome λ when she tests her probe, the posterior probability (or *likelihood*) Eve assigns signal i is, by Bayes' theorem,

$$Q_{i\lambda}=P_{\lambda i}p_i/q_\lambda\,. \tag{6}$$

How can Eve make use of this result? One possibility is to simply assume that the larger of $Q_{x\lambda}$ and $Q_{y\lambda}$ indicates the signal that was actually sent by Alice. Then, the smaller of $Q_{x\lambda}$ and $Q_{y\lambda}$ is Eve's expected error rate. A convenient measure of her information gain is [18]

$$G_\lambda=|Q_{x\lambda}-Q_{y\lambda}|. \tag{7}$$

For example, this expression would be Eve's expected income, if she were earning one dollar for each correct guess, and paying one dollar for each incorrect guess. This expression is also related in a simple way to Eve's expected error rate [18] in her interpretation of the result λ, which is $\frac{1}{2}(1-G_\lambda)$.

On average, Eve's information gain (in bits) is

$$\sum_\lambda q_\lambda G_\lambda=\sum_\lambda |P_{\lambda x}p_x-P_{\lambda y}p_y|. \tag{8}$$

If the two signals are equiprobable, Eve's average gain is

$$G=\frac{1}{2}\sum_\lambda |P_{\lambda x}-P_{\lambda y}|, \tag{9}$$

and her expected average error rate is $\frac{1}{2}(1-G)$.

A more sophisticated data processing by Eve is to keep track of all the q_λ and $Q_{i\lambda}$ of her observations. These may then be used to compute her *mutual information* on Alice's message [6]. With equiprobable signals, this is given (in nats) by

$$I=\ln 2+\sum_\lambda q_\lambda\sum_i Q_{i\lambda}\ln Q_{i\lambda}\,. \tag{10}$$

This measure of Eve's information is the main concern of this paper. However, in the following, we shall consider first the simple ''information gain'' expression (9), for which a bound is easier to find. This result will then be used to bound the mutual information.

Let us first consider the case where Alice announced that she had sent a signal in the x-y basis, and Eve observed outcome λ. We then have, from Eqs. (6) and (7),

$$q_\lambda G_\lambda=\tfrac{1}{2}|P_{\lambda x}-P_{\lambda y}|=\tfrac{1}{2}|\langle X|\mathbf{1}\otimes E_\lambda|X\rangle-\langle Y|\mathbf{1}\otimes E_\lambda|Y\rangle|. \tag{11}$$

This can also be written, thanks to Eq. (3), as

$$\begin{aligned} q_\lambda G_\lambda &= \tfrac{1}{2}|\langle U|\mathbf{1}\otimes E_\lambda|V\rangle + \langle V|\mathbf{1}\otimes E_\lambda|U\rangle|, \\ &= |\mathrm{Re}\langle U|B_u\otimes E_\lambda|V\rangle + \mathrm{Re}\langle U|B_v\otimes E_\lambda|V\rangle|, \\ &\leq |\langle U_{\lambda u}|V_{\lambda u}\rangle| + |\langle U_{\lambda v}|V_{\lambda v}\rangle|, \end{aligned} \tag{12}$$

where $B_u = |u\rangle\langle u|$ and $B_v = |v\rangle\langle v|$ are projectors onto Bob's states $|u\rangle$ and $|v\rangle$, so that

$$B_u + B_v = \mathbf{1}, \tag{13}$$

and

$$\begin{aligned} |U_{\lambda u}\rangle = B_u\otimes\sqrt{E_\lambda}|U\rangle, \quad |V_{\lambda u}\rangle = B_u\otimes\sqrt{E_\lambda}|V\rangle \\ |U_{\lambda v}\rangle = B_v\otimes\sqrt{E_\lambda}|U\rangle, \quad |V_{\lambda v}\rangle = B_v\otimes\sqrt{E_\lambda}|V\rangle. \end{aligned} \tag{14}$$

Note that $\sqrt{E_\lambda}$ is well defined, since E_λ is a positive semidefinite operator. Of course, $\sqrt{E_\lambda}$ can be replaced by E_λ when E_λ is a projector.

The Schwarz inequality implies that

$$|\langle U_{\lambda u}|V_{\lambda u}\rangle| \leq [\langle U_{\lambda u}|U_{\lambda u}\rangle\langle V_{\lambda u}|V_{\lambda u}\rangle]^{1/2}, \tag{15}$$

with equality if and only if $|U_{\lambda u}\rangle$ and $|V_{\lambda u}\rangle$ are parallel. The physical meaning of the expression $\langle V_{\lambda u}|V_{\lambda u}\rangle$ is that, if instead of the scenario considered here, Alice had actually sent signal $|v\rangle$, Eve would get result λ and Bob would get $|u\rangle$ (that is, a wrong result) with a probability equal to that expression. Therefore, we shall write

$$\begin{aligned} \langle V_{\lambda u}|V_{\lambda u}\rangle &= P_{\lambda v}d_{\lambda v}, \\ \langle V_{\lambda v}|V_{\lambda v}\rangle &= P_{\lambda v}(1-d_{\lambda v}), \end{aligned} \tag{16}$$

where $P_{\lambda v}$ is defined as in Eq. (4), and $d_{\lambda v}$ is the probability that Bob gets a wrong result *conditioned upon* Alice sending $|v\rangle$ and Eve measuring λ. The other terms in Eq. (12) can be handled in the same way, and we finally obtain

$$q_\lambda G_\lambda \leq \sqrt{P_{\lambda u}P_{\lambda v}}\,[\sqrt{d_{\lambda v}(1-d_{\lambda u})} + \sqrt{d_{\lambda u}(1-d_{\lambda v})}]. \tag{17}$$

Let us develop the bound in Eq. (17) further. By the geometric mean-arithmetic mean inequality, we have

$$(P_{\lambda u}P_{\lambda v})^{1/2} \leq \frac{1}{2}(P_{\lambda u} + P_{\lambda v}) = q_\lambda, \tag{18}$$

where the first equality holds if $P_{\lambda u} = P_{\lambda v}$, and where Eq. (5) was used. Let us now define d_λ and w by

$$d_{\lambda u} = d_\lambda + w \quad \text{and} \quad d_{\lambda v} = d_\lambda - w. \tag{19}$$

The square bracket in Eq. (17) is easily seen to be an even function of w, which has its maximum value at $w=0$, that is, when $d_{\lambda u} = d_{\lambda v} = d_\lambda$. That is to say, the bound reaches a maximum when the probability of a detectable disturbance is identical for each of the conjugate basis vectors. We thus have

$$G_\lambda \leq 2[d_\lambda(1-d_\lambda)]^{1/2}. \tag{20}$$

It follows that Eve's information gain averaged over all outcomes is bounded by the expression

$$G = \sum_\lambda q_\lambda G_\lambda \leq 2\sum_\lambda q_\lambda[d_\lambda(1-d_\lambda)]^{1/2}. \tag{21}$$

Since the function $[x(1-x)]^{1/2}$ is concave, we have [19]

$$\sum_\lambda q_\lambda[d_\lambda(1-d_\lambda)]^{1/2} \leq [D(1-D)]^{1/2}, \tag{22}$$

where $D = \Sigma q_\lambda d_\lambda$ is Bob's observable error rate, i.e., the one averaged over all of Eve's outcomes. Equality holds only if all the d_λ are equal to D. Thus, finally,

$$G_{xy} \leq 2[D_{uv}(1-D_{uv})]^{1/2}, \tag{23}$$

where the indices have been introduced to emphasize that Eve's information gain refers to signals sent in the x-y basis, and Bob's error rate refers to signals sent in the u-v basis.

In exactly the same fashion as above, we can derive a bound on the information gain with respect to the x-y basis in terms of the disturbance inflicted upon the u-v basis

$$G_{uv} \leq 2[D_{xy}(1-D_{xy})]^{1/2}. \tag{24}$$

Equations (23) and (24) tell us that Eve's maximal information gain, for the given error rate caused to Bob in the conjugate basis, is bounded in a simple way. The main goal of this section, however, is in finding an analogous bound on the mutual information I, defined by Eq. (10). The latter can be expressed more simply by writing

$$Q_{x\lambda} = (1+r_\lambda)/2 \quad \text{and} \quad Q_{y\lambda} = (1-r_\lambda)/2, \tag{25}$$

since these two expressions sum to unity. We then have

$$I = \tfrac{1}{2}\sum_\lambda q_\lambda[(1+r_\lambda)\ln(1+r_\lambda) + (1-r_\lambda)\ln(1-r_\lambda)]. \tag{26}$$

Note that

$$r_\lambda = Q_{x\lambda} - Q_{y\lambda} = \pm G_\lambda, \tag{27}$$

by virtue of Eq. (7). We can therefore write, instead of Eq. (26),

$$I = \tfrac{1}{2}\sum_\lambda q_\lambda[(1+G_\lambda)\ln(1+G_\lambda) + (1-G_\lambda)\ln(1-G_\lambda)]. \tag{28}$$

To obtain a bound on I, it is convenient to define a function

$$\phi(z) = (1+z)\ln(1+z) + (1-z)\ln(1-z). \tag{29}$$

Since $\phi'(z) = \ln[(1+z)/(1-z)]$ is positive for $0<z<1$, we see that the right-hand side of Eq. (28) will increase if we replace G_λ by a larger expression, such as the right-hand side of Eq. (20). Therefore,

$$I \leq \tfrac{1}{2}\sum_\lambda q_\lambda\phi[2\sqrt{d_\lambda(1-d_\lambda)}]. \tag{30}$$

In Appendix A, it is shown that $\phi[2\sqrt{x(1-x)}]$ is a concave function of x. It follows, just as in Eq. (22), that

$$I_{xy}\leqslant\tfrac{1}{2}\phi[2\sqrt{D_{uv}(1-D_{uv})}], \tag{31}$$

where subscripts have been added, as in Eq. (23), to emphasize that the information gain and error rate refer to signals sent in two different bases. Likewise

$$I_{uv}\leqslant\tfrac{1}{2}\phi[2\sqrt{D_{xy}(1-D_{xy})}] \tag{32}$$

is the counterpart of Eq. (24).

Necessary and sufficient conditions for Eqs. (31) and (32) to hold as equalities are derived easily by tracing back through the chain of inequalities that brought them about. Let us focus on Eq. (31). To begin with, the concavity of $\phi[2\sqrt{x(1-x)}]$ is strict, so all the d_λ's must be equal; thus, in view of the remark following Eq. (19), we have

$$d_{\lambda u}=d_{\lambda v}=d_\lambda=D_{uv}\,. \tag{33}$$

Similarly, Eq. (18) can be a strict equality only if

$$P_{\lambda u}=P_{\lambda v}=q_\lambda\,. \tag{34}$$

Equality in Eq. (12) means that both $\langle U_{\lambda u}|V_{\lambda u}\rangle$ and $\langle U_{\lambda v}|V_{\lambda v}\rangle$ are real and have the same sign

$$\begin{aligned}\sigma_\lambda&=\operatorname{sgn}(\langle U_{\lambda u}|V_{\lambda u}\rangle+\langle U_{\lambda v}|V_{\lambda v}\rangle),\\&=\operatorname{sgn}(P_{\lambda x}-P_{\lambda y})=\operatorname{sgn}(Q_{x\lambda}-Q_{y\lambda}).\end{aligned} \tag{35}$$

Finally, equality in Eq. (15), and its analog with u replaced by v, means that $|U_{\lambda u}\rangle$ is a multiple of $|V_{\lambda u}\rangle$, and $|U_{\lambda v}\rangle$ is a multiple of $|V_{\lambda v}\rangle$. Thus

$$\langle V_{\lambda u}|V_{\lambda u}\rangle=\mu^2\langle U_{\lambda u}|U_{\lambda u}\rangle, \tag{36}$$

and

$$\langle U_{\lambda v}|U_{\lambda v}\rangle=\nu^2\langle V_{\lambda v}|V_{\lambda v}\rangle, \tag{37}$$

for some real numbers μ and ν.

Combining these results gives the necessary and sufficient conditions for equality in Eq. (31): for every λ,

$$|V_{\lambda u}\rangle=\epsilon_\lambda\left(\frac{D_{uv}}{1-D_{uv}}\right)^{1/2}|U_{\lambda u}\rangle \tag{38}$$

and

$$|U_{\lambda v}\rangle=\epsilon_\lambda\left(\frac{D_{uv}}{1-D_{uv}}\right)^{1/2}|V_{\lambda v}\rangle, \tag{39}$$

where $\epsilon_\lambda=\pm1$.

The corresponding conditions for equality in Eq. (32) are derived in an analogous way. Namely, if Eve uses a POVM $\{F_\lambda\}$ for gaining information about the u-v basis—which is different from the POVM $\{E_\lambda\}$ used for the x-y basis—then the conditions that must be satisfied are

$$|Y_{\lambda x}\rangle=\gamma_\lambda\left(\frac{D_{xy}}{1-D_{xy}}\right)^{1/2}|X_{\lambda x}\rangle \tag{40}$$

and

$$|X_{\lambda y}\rangle=\gamma_\lambda\left(\frac{D_{xy}}{1-D_{xy}}\right)^{1/2}|Y_{\lambda y}\rangle, \tag{41}$$

with

$$\gamma_\lambda=\operatorname{sgn}(P_{\lambda u}-P_{\lambda v})=\operatorname{sgn}(Q_{u\lambda}-Q_{v\lambda}), \tag{42}$$

and

$$\begin{aligned}&|X_{\lambda x}\rangle=B_x\otimes\sqrt{F_\lambda}|X\rangle,\quad |Y_{\lambda x}\rangle=B_x\otimes\sqrt{F_\lambda}|Y\rangle,\\&|X_{\lambda y}\rangle=B_y\otimes\sqrt{F_\lambda}|X\rangle,\quad |Y_{\lambda y}\rangle=B_y\otimes\sqrt{F_\lambda}|Y\rangle.\end{aligned} \tag{43}$$

In the cryptographic setting, the fact that Eve can adapt her measurement to the basis that Alice reveals, leads one to question whether there may be a single interaction between Eve's probe and Alice's qubit that saturates both Eq. (31) and Eq. (32). We address the achievement of these bounds in Sec. III.

III. ATTAINABILITY OF BOTH CONJUGATE-BASIS BOUNDS

In this section, we show how Eve can optimize her strategy to attain the bounds in Eqs. (31) and (32) with both D_{xy} and D_{uv} fixed independently. The train of thought that led to the present solution is a long and complex one. First, we performed a ''brute force'' numerical optimization, similar to the one in Ref. [15]. The result was found to saturate the bound on Eve's overall information about both bases (still to be derived in Sec. IV). This led us to look for an exact analytic solution satisfying Eqs. (38)–(41), first with equal error rates, and then with independent error rates. The one described below, for independent error rates, was obtained with a certain amount of guesswork. For the case of equal error rates, as in Sec. IV, there is a symmetrization procedure that leads directly to a solution. It is easy to check that the solution here is correct, but the extent to which it is unique (aside from trivial changes of basis and of phase) remains unknown. A quantum circuit embodying the optimal strategy is described in the following paper [10].

Let us fix both D_{xy} and D_{uv}. A natural ansatz for an optimal interaction on Eve's part is that when Alice sends a signal in the x-y basis, Bob receives a simple mixture of the same two basis vectors; when Alice sends a signal in the u-v basis, Bob receives a simple mixture of these two basis vectors. That is, Bob's density matrix is always diagonal in the basis chosen by Alice. Then, owing to Eq. (33) and the analogous condition for the x-y basis, the Schmidt decompositions for the postinteraction states must be of the form

$$\begin{aligned}|X\rangle&=\sqrt{1-D_{xy}}|x\rangle|\xi_x\rangle+\sqrt{D_{xy}}|y\rangle|\zeta_x\rangle,\\|Y\rangle&=\sqrt{1-D_{xy}}|y\rangle|\xi_y\rangle+\sqrt{D_{xy}}|x\rangle|\zeta_y\rangle,\end{aligned} \tag{44}$$

and

$$\begin{aligned}|U\rangle&=\sqrt{1-D_{uv}}|u\rangle|\xi_u\rangle+\sqrt{D_{uv}}|v\rangle|\zeta_u\rangle,\\|V\rangle&=\sqrt{1-D_{uv}}|v\rangle|\xi_v\rangle+\sqrt{D_{uv}}|u\rangle|\zeta_v\rangle,\end{aligned} \tag{45}$$

where each pair $|\xi_i\rangle$ and $|\zeta_i\rangle$ are normalized vectors that are orthogonal to each other: $\langle\xi_x|\zeta_x\rangle=\langle\xi_y|\zeta_y\rangle=\langle\xi_u|\zeta_u\rangle=\langle\xi_v|\zeta_v\rangle=0$.

The remaining relations between the $|\xi_i\rangle$ and $|\zeta_j\rangle$ cannot be chosen arbitrarily. For instance, the orthogonality of $|X\rangle$ and $|Y\rangle$ requires that

$$\langle\xi_x|\zeta_y\rangle+\langle\zeta_x|\xi_y\rangle=0. \tag{46}$$

Moreover, Eqs. (2) and (3) imply that

$$2\sqrt{1-D_{uv}}|\xi_u\rangle=\sqrt{1-D_{xy}}(|\xi_x\rangle+|\xi_y\rangle)+\sqrt{D_{xy}}(|\zeta_x\rangle+|\zeta_y\rangle),$$

$$2\sqrt{D_{uv}}|\zeta_u\rangle=\sqrt{1-D_{xy}}(|\xi_x\rangle-|\xi_y\rangle)+\sqrt{D_{xy}}(|\zeta_y\rangle-|\zeta_x\rangle), \tag{47}$$

and similar relations for $|\xi_v\rangle$ and $|\zeta_v\rangle$. These in turn, through $\langle\xi_u|\zeta_u\rangle=\langle\xi_v|\zeta_v\rangle=0$, lead to

$$\mathrm{Re}(\langle\xi_x|\zeta_y\rangle-\langle\zeta_x|\xi_y\rangle)=0, \tag{48}$$

and

$$(1-D_{xy})\ \mathrm{Im}(\langle\xi_y|\xi_x\rangle)+D_{xy}\ \mathrm{Im}(\langle\zeta_x|\zeta_y\rangle)=0. \tag{49}$$

These requirements still leave us considerable freedom in the choice of Eve's interaction with Alice and Bob's qubit. For simplicity we shall assume that all inner products between the various $|\xi_i\rangle$ and $|\zeta_j\rangle$ are real numbers. Then Eqs. (46) and (48), when combined, indicate that $\langle\xi_x|\zeta_y\rangle=\langle\zeta_x|\xi_y\rangle=0$.

A particular choice for Eve's interaction that is adequate for our needs can now be specified. Recall that Eve's probe never need have more than a four-dimensional Hilbert space. That is to say, Eve's probe may be taken to be two qubits. It is therefore convenient to introduce the same bases for each of Eve's qubits that we introduced for Alice's qubit, namely, x-y and u-v. In terms of these basis vectors, we may further construct two standard (maximally) entangled bases for the two qubits: a Bell basis [20] with respect to xy

$$|\Phi^{\pm}_{xy}\rangle=(|x\rangle|x\rangle\pm|y\rangle|y\rangle)/\sqrt{2},$$

$$|\Psi^{\pm}_{xy}\rangle=(|x\rangle|y\rangle\pm|y\rangle|x\rangle)/\sqrt{2}, \tag{50}$$

and similarly a Bell basis with respect to uv consisting of $|\Phi^{\pm}_{uv}\rangle$ and $|\Psi^{\pm}_{uv}\rangle$.

In terms of the Bell basis vectors for Eve's probe, we may choose the interaction in such a way that

$$|\xi_x\rangle=\sqrt{1-D_{uv}}|\Phi^{+}_{xy}\rangle+\sqrt{D_{uv}}|\Phi^{-}_{xy}\rangle,$$

$$|\xi_y\rangle=\sqrt{1-D_{uv}}|\Phi^{+}_{xy}\rangle-\sqrt{D_{uv}}|\Phi^{-}_{xy}\rangle,$$

$$|\zeta_x\rangle=\sqrt{1-D_{uv}}|\Psi^{+}_{xy}\rangle-\sqrt{D_{uv}}|\Psi^{-}_{xy}\rangle,$$

$$|\zeta_y\rangle=\sqrt{1-D_{uv}}|\Psi^{+}_{xy}\rangle+\sqrt{D_{uv}}|\Psi^{-}_{xy}\rangle. \tag{51}$$

With respect to the conjugate inputs, the interaction takes a similar form:

$$|\xi_u\rangle=\sqrt{1-D_{xy}}|\Phi^{+}_{uv}\rangle+\sqrt{D_{xy}}|\Phi^{-}_{uv}\rangle,$$

$$|\xi_v\rangle=\sqrt{1-D_{xy}}|\Phi^{+}_{uv}\rangle-\sqrt{D_{xy}}|\Phi^{-}_{uv}\rangle,$$

$$|\zeta_u\rangle=\sqrt{1-D_{xy}}|\Psi^{+}_{uv}\rangle-\sqrt{D_{xy}}|\Psi^{-}_{uv}\rangle,$$

$$|\zeta_v\rangle=\sqrt{1-D_{xy}}|\Psi^{+}_{uv}\rangle+\sqrt{D_{xy}}|\Psi^{-}_{uv}\rangle. \tag{52}$$

The second set of vectors is, of course, related to the first—as it must be by unitarity—through relations such as in Eq. (47). Note that neither collection of relative states is orthonormal. Hence the set of density operators available to Eve after the probe's interaction—i.e., the set of quantum states from which she gains information about Alice's signal—is a noncommuting set.

To see that this interaction is optimal for Eve, we need only find optimal POVMs $\{E_\lambda\}$ and $\{F_\lambda\}$—one for each basis x-y and u-v—to use under these assumptions. Then the optimality of the whole procedure can be checked either by testing the validity of Eqs. (38)–(41), or simply by checking directly that the bound is attained. We opt for the former of these here. In Sec. IV, we shall use a direct check for a different set of $|\xi_i\rangle$ and $|\zeta_i\rangle$.

Suppose Alice announces that a signal from the x-y basis was sent to Bob. Then a natural choice for the observable Eve should measure is the one that minimizes her error in guessing Alice's signal, i.e., the one that maximizes G in Eq. (9). The corresponding basis is well known [21,18]: it simply is the one that diagonalizes the Hermitian operator

$$\Gamma_{xy}=\rho_x-\rho_y, \tag{53}$$

where

$$\rho_x=\mathrm{Tr}_{\mathrm{Alice}}(|X\rangle\langle X|)=(1-D_{xy})|\xi_x\rangle\langle\xi_x|+D_{xy}|\zeta_x\rangle\langle\zeta_x|, \tag{54}$$

and likewise for ρ_y. The corresponding eigenprojectors of Γ_{xy} are then given by

$$E_\lambda=|E_\lambda\rangle\langle E_\lambda|, \tag{55}$$

where

$$|E_0\rangle=|x\rangle|x\rangle,\quad |E_1\rangle=|y\rangle|x\rangle$$

$$|E_2\rangle=|x\rangle|y\rangle,\quad |E_3\rangle=|y\rangle|y\rangle. \tag{56}$$

Arbitrary values, 0, . . . ,3, have been assigned here to the label λ.

Similarly, we make the analogous guess for Eve's measurement in the case that Alice reveals the u-v basis; namely, we use the eigenprojectors

$$F_\lambda=|F_\lambda\rangle\langle F_\lambda| \tag{57}$$

of the operator

$$\Gamma_{uv}=\rho_u-\rho_v, \tag{58}$$

where the density operators ρ_u and ρ_v are partial traces of $|U\rangle$ and $|V\rangle$, respectively. Again, it is easily verified that the appropriate eigenvectors are

$$|F_0\rangle = |u\rangle|u\rangle, \quad |F_1\rangle = |v\rangle|u\rangle,$$
$$|F_2\rangle = |u\rangle|v\rangle, \quad |F_3\rangle = |v\rangle|v\rangle. \tag{59}$$

It should be noted that the measurement optimal for minimizing the error in a guess of the state's identity is generally *not* the same as the measurement for maximizing the mutual information about the state [22]. Thus there is no automatic guarantee that, even with the optimal interaction for Eve's probe, the measurements listed above will be adequate for achieving the maximum possible mutual information. Nevertheless, for the case at hand, as will be seen shortly, circumstances have worked out in our favor.

With all the pieces in place, checking the optimality of the interaction given by Eqs. (44) and (51) and the measurement given by Eq. (56), is just a question of checking that Eqs. (38)–(41) are satisfied. We start by examining the vectors defined in Eq. (14) using the projectors onto the vectors of Eqs. (56). Note that in this case $\sqrt{E_\lambda} = E_\lambda$ is a matrix of rank 1. Therefore, $B_u \otimes E_\lambda$ projects onto a one-dimensional subspace of the qubit-probe Hilbert space, so that $|V_{\lambda u}\rangle$ and $|U_{\lambda u}\rangle$ are parallel. Likewise $|V_{\lambda v}\rangle$ and $|U_{\lambda v}\rangle$ are parallel. Working out the scaling factors between the parallel vectors is a matter of applying the projectors to the expressions in Eq. (45). For example,

$$\begin{aligned} |U_{1u}\rangle = B_u \otimes E_1 |U\rangle &= \sqrt{1-D_{uv}} \langle E_1|\xi_u\rangle |u\rangle|E_1\rangle, \\ &= \sqrt{1-D_{uv}}\sqrt{D_{xy}}|u\rangle|E_1\rangle/\sqrt{2}, \end{aligned} \tag{60}$$

and $|V_{1u}\rangle$ is given by the same expression except that $\sqrt{1-D_{uv}}$ is replaced by $\sqrt{D_{uv}}$. Hence Eq. (38) is satisfied for $\lambda = 1$ with $\epsilon_1 = +1$. One can work out the other cases in the same way, and show that

$$\epsilon_0 = +1, \quad \epsilon_1 = +1, \quad \epsilon_2 = -1, \quad \epsilon_3 = -1. \tag{61}$$

Consequently, the measurement corresponding to Eq. (56) provides a mutual information I_{xy} given by the right side of Eq. (31). It is similarly straightforward to verify Eqs. (40) and (41) by applying projectors of the type $B_x \otimes F_\lambda$ and $B_y \otimes F_\lambda$ to the expressions in Eq. (44), to form the quantities defined in Eq. (43).

Hence there exists a definite choice of qubit-probe interaction, namely, Eqs. (44)–(47), which, together with two distinct measurement strategies, based upon Eqs. (56) and (59) according to the basis announced by Alice, allows Eve to saturate the bounds in Eqs. (31) and (32) simultaneously, for arbitrary choices of D_{uv} and D_{xy}.

As a final point, it is intriguing to note the following. If Eve's concern were only to guess the state Alice prepared–and *not* maximize her mutual information–then, clearly, it is enough for her to bin the outcomes of her measurement two by two. That is to say, if Alice sends a signal in the x-y basis, then Eve upon receiving either outcome E_0 or E_1 should guess that the state $|x\rangle$ was sent; upon receiving either E_2 or E_3, she should guess that $|y\rangle$ was sent. These choices will minimize her probability of making an incorrect guess. Similarly, she should guess $|u\rangle$ when she finds either F_0 or F_1 and $|v\rangle$ when she finds either F_2 or F_3. Interestingly, Eq. (61) along with Eqs. (38) and (39) (and similarly for the conjugate basis) reveals that such a binned measurement is also sufficient for maximizing Eve's mutual information. Moreover, this fact has another remarkable consequence: regardless of which basis Alice used, after Eve's interaction, she can completely ignore the first qubit of her probe. All the accessible information about Alice's signal is contained in the second qubit. Thus, while there are two qubits in the particular probe we constructed for Eve, only one qubit plays a role in the final information-gathering process. Also see the discussions in the following paper [10] and Ref. [8].

IV. OPTIMAL EAVESDROPPING STRATEGY

We are finally in a position to describe the eavesdropping strategy that is most relevant to quantum cryptography with the BB84 protocol. Namely, we should like to know Eve's best *average* mutual information for a fixed *average* disturbance across the two bases x-y and u-v. This is given by combining the two results of Eqs. (31) and (32). Fixing the average disturbance to be

$$D = \tfrac{1}{2}(D_{xy} + D_{uv}), \tag{62}$$

and defining

$$G = \tfrac{1}{2}(G_{xy} + G_{uv}) \quad \text{and} \quad I = \tfrac{1}{2}(I_{xy} + I_{uv}) \tag{63}$$

for the average information gain and mutual information, respectively, we can again use the concavity of the functions $[x(1-x)]^{1/2}$ and $\phi[2\sqrt{x(1-x)}]$ to obtain

$$G \leqslant 2[D(1-D)]^{1/2}, \tag{64}$$

and

$$I \leqslant \tfrac{1}{2}\phi[2\sqrt{D(1-D)}]. \tag{65}$$

Equality can be achieved in either of these bounds only if

$$D_{xy} = D_{uv} = D. \tag{66}$$

The result is plotted in Fig. 3. As intuitively expected, the average error is the same in both channels. If it were not so, different error rates for x-y and u-v signals would be a telltale indication that a clumsy eavesdropper is tampering with the communication line.

The derivation of Eq. (65), as given above, may seem long and arduous. This is due to the generality of the previous sections: Sec. III encompasses strategies that produce asymmetric disturbances in the two conjugate bases and the bounding argument of Sec. II can, with slight modification, be generalized to nonconjugate bases and unequal prior probabilities for those bases. To more firmly place the physics of the optimal eavesdropping strategy in Eq. (65) within context, we now sketch an alternate derivation for it based on a symmetrization argument.

The starting point of the new argument is to notice that for any eavesdropping procedure Eve chooses to use, there exists a symmetrized strategy leading to the same average information I, and the same *or lesser* average disturbance D. For each one of the signals sent by Alice, the mixed states Bob receives can be made to be of the form

$$\rho_{\text{Bob}} = (1-2D)\rho_{\text{Alice}} + D\mathbb{1}, \tag{67}$$

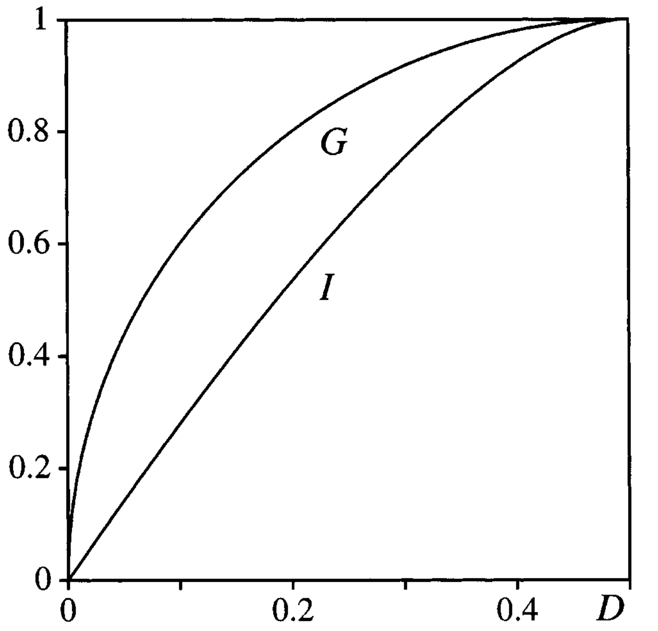

FIG. 3. Eve's information gain G and mutual information I (in bits) as functions of Bob's error rate D.

as if Alice's signals were merely diluted by mixing them with a random component. A formal proof of this result is given in Appendix B.

Therefore with no loss of generality we can obtain Eve's ultimate bound on information versus disturbance by studying symmetric strategies. Note, however, that this may come at the cost of adding extra degrees of freedom to Eve's setup: without these, we would not be able to enact the required random orientation. For instance, if Eve's probe were restricted to consist of a single qubit, as in Ref. [7], there would be no way to carry out this symmetrization. However, by making no *a priori* restrictions on Eve's probe, symmetrized strategies can always be covered within our formal framework. In particular, there must exist an optimal strategy on Eve's part that gives Eqs. (44) and (45) with $D_{xy}=D_{uv}=D$.

Again we use the notation of Eqs. (44) and (45) and, in accordance with the argument that follows these equations, we set

$$\langle\xi_x|\zeta_x\rangle=\langle\xi_y|\zeta_y\rangle=\langle\xi_x|\zeta_y\rangle=\langle\xi_y|\zeta_x\rangle=0. \tag{68}$$

These requirements are enough to ensure that the set of relevant $|\xi_x\rangle$, $|\zeta_x\rangle$, $|\xi_y\rangle$, and $|\zeta_y\rangle$ can all be parameterized by two real numbers. There are now many possibilities open. Instead of Eq. (51), we may try a solution that looks simpler, such as

$$|\xi_x\rangle=|x\rangle|x\rangle,$$

$$|\zeta_x\rangle=|x\rangle|y\rangle,$$

$$|\xi_y\rangle=(\cos\alpha|x\rangle+\sin\alpha|y\rangle)|x\rangle,$$

$$|\zeta_y\rangle=(\cos\beta|x\rangle+\sin\beta|y\rangle)|y\rangle. \tag{69}$$

It then follows from $\langle\zeta_u|\zeta_u\rangle=1$ that

$$D=\frac{1-\cos\alpha}{2-\cos\alpha+\cos\beta}. \tag{70}$$

Let us consider the case where Alice announces that the x-y basis has been used. Then the two density operators that Eve must distinguish are

$$\rho_x=(1-D)|\xi_x\rangle\langle\xi_x|+D|\zeta_x\rangle\langle\zeta_x|,$$

$$\rho_y=(1-D)|\xi_y\rangle\langle\xi_y|+D|\zeta_y\rangle\langle\zeta_y|. \tag{71}$$

The optimal information gathering measurement for these two states proceeds as follows: Eve first performs the preliminary step of distinguishing the vectors—rather than the density operators—by measuring the second qubit, because the set of $|\xi_i\rangle$ are orthogonal to the set of $|\zeta_j\rangle$. The set of $|\xi_i\rangle$ will occur with probability $(1-D)$; the set of $|\zeta_j\rangle$ will occur with probability D. Thereafter, distinguishing the density operators ρ_x and ρ_y becomes a question of distinguishing the (equiprobable) pure states in the appropriate set. The optimal information gathering measurement in either case is defined by the basis that straddles the two nonorthogonal vectors that must be distinguished [24]. In the two cases this leads to an information gain on Eve's part given by [24,22]

$$I_\xi=\tfrac{1}{2}(1+\sin\alpha)\ln(1+\sin\alpha)+\tfrac{1}{2}(1-\sin\alpha)\ln(1-\sin\alpha),$$

$$I_\zeta=\tfrac{1}{2}(1+\sin\beta)\ln(1+\sin\beta)+\tfrac{1}{2}(1-\sin\beta)\ln(1-\sin\beta). \tag{72}$$

On average, Eve's information gain is given by

$$I=(1-D)I_\xi+DI_\zeta. \tag{73}$$

Eve's optimal strategy is obtained with the values of α and β that maximize I when D is fixed. One can readily check that this occurs when $\alpha=\beta$, with $\sin\alpha=2\sqrt{D(1-D)}$. By symmetry, the same result holds when Alice reveals that the u-v basis has been sent (though the detailed protocol for measuring the two qubits is slightly different in that case). We again find Eq. (65) as the optimal information-disturbance tradeoff.

For small values of D, the bound given in Eq. (65) becomes $I\leqslant 2D$. At the other extreme, the maximum value of I is ln2 (that is, one bit): Eve can achieve this result simply by keeping Alice's qubit for herself, and sending to Bob a dummy qubit in a random state. She then has all the information, and Bob gets a 50% error rate. This state of affairs should be contrasted to optimal eavesdropping on the quantum cryptographic protocol B92 of Bennett [23], that uses only two nonorthogonal quantum states. There one finds, for small values of D, that $I\propto\sqrt{D}$ [15]. This suggests that the BB84 protocol is inherently more secure against eavesdropping than the B92 scheme: for a given disturbance, Eve obtains more information about the identity of Alice and Bob's bit in B92 than in BB84.

To this point, we have hardly discussed what Alice and Bob can do with the knowledge of Eq. (65) and Eve's optimal strategy (given our restrictions to the problem). Generally, the users of the BB84 protocol will not have a noiseless communication channel available for their use. If Alice and Bob use a noisy channel, the only truly safe way for them to proceed is to assume that all the noise is due to some Eve using an optimal eavesdropping scheme. Then, if this Eve has not been too invasive, Alice and Bob may still be able to recover a safe cryptographic key by methods of privacy amplification.

As discussed in Refs. [3,25], a good indicator of Alice and Bob's capability of recovering a safe cryptographic key in the face of Eve's presence can be formulated in terms of various mutual informations. In particular, one must compare the mutual information I_{AB} between Alice and Bob (after Eve's eavesdropping) to the mutual informations I_{AE} and I_{EB} between Alice and Eve and between Eve and Bob, respectively. If the natural noise in the channel is such that $I_{AB} \leqslant \min\{I_{AE}, I_{EB}\}$, for any potential eavesdropper, then Alice and Bob should consider the channel inappropriate for quantum cryptographic key generation. They should either move to another channel or give up their quest.

Note that for the optimal scheme derived here $I_{AE}=I_{EB}$ and both are given by the right-hand side of Eq. (65). On the other hand, as far as Alice and Bob are concerned, Eve's action has merely produced a binary symmetric channel between them, with a data-flipping rate D. Therefore [26]

$$I_{AB}=\ln 2 + D\ln D + (1-D)\ln(1-D) = \tfrac{1}{2}\phi(1-2D). \tag{74}$$

Comparing this expression to Eq. (65), we can find the threshold noise level for a potentially safe channel; namely, it occurs when

$$|1-2D| = 2\sqrt{D(1-D)}. \tag{75}$$

That is to say, when

$$D \geqslant \tfrac{1}{2} - \tfrac{1}{4}\sqrt{2} \approx 0.146\,447, \tag{76}$$

the channel should be considered too risky for safe key generation.

Finally, let us discuss an intriguing connection between optimal eavesdropping and the violation of Bell inequalities. A slight modification of the BB84 protocol can be built upon Alice and Bob sharing an entangled pair of qubits (such as the singlet state $|\Psi^-\rangle$) rather than Alice physically sending a qubit to Bob [16]. Alice and Bob simply randomly perform measurements in the x-y and u-v bases, and announce their measurement—though not their result—to each other. Whenever their measurement bases differ, they discard the bit; whenever the bases are the same, they know that they should have opposite bits if there were no eavesdropping or noise on the channel. An eavesdropper in this scenario might be imagined to interact with one qubit of the entangled pair in an attempt to gather information about Alice and Bob's final key.

Ekert [17], in a related scheme, pointed out that an appropriate test for eavesdropping might be a check on whether the Bell inequalities are violated. This can be enacted in our scenario by allowing Bob to rotate his measuring apparatus by 22.5°. Then Alice and Bob will be in position for testing the standard Clauser-Horne-Shimony-Holt (CHSH) inequality [27]. The correlation signature S in that inequality cannot exceed 2 for theories based on local hidden variables. However, in the modified BB84 protocol just discussed, S can reach $2\sqrt{2}$ when there is no eavesdropping involved. The effect on S of our optimal eavesdropping strategy is equivalent to the one caused by a data-flipping error with probability D in one of the detectors [28]

$$S = 2\sqrt{2}(1-2D). \tag{77}$$

It is noteworthy that the CHSH inequality ceases to be violated, i.e., $S \leqslant 2$, just when D satisfies Eq. (76). This confirms the conjecture of Gisin and Huttner [7] and to some extent vindicates the idea of Ekert. We believe this connection between privacy amplification requirements and Bell inequalities may have fundamental implications in quantum information theory and is worthy of further investigation.

ACKNOWLEDGMENTS

We thank the Institute for Theoretical Physics at the University of California at Santa Barbara (under NSF Grant No. PHY94-07194) for their hospitality while this work was being executed. C.A.F. thanks G. Brassard for many discussions and acknowledges the support of the Lee A. DuBridge Foundation and of DARPA through the Quantum Information and Computing (QUIC) Institute administered by ARO. N.G. acknowledges financial support by the Swiss National Science Foundation and the European TMR Network on the Physics of Quantum Information. R.B.G. and C.S.N. acknowledge the support of NSF and ARPA through Grant No. CCR-9633102.

APPENDIX A: PROOF OF CONCAVITY

Consider the function

$$\phi(z) = (1+z)\ln(1+z) + (1-z)\ln(1-z). \tag{A1}$$

We have

$$\phi'(z) = \ln[(1+z)/(1-z)], \tag{A2}$$

and

$$\phi''(z) = 2/(1-z^2). \tag{A3}$$

Now let

$$z(x) = 2[x(1-x)]^{1/2}, \tag{A4}$$

whence

$$z'(x) = (1-2x)/[x(1-x)]^{1/2}, \tag{A5}$$

and

$$z''(x) = -\tfrac{1}{2}[x(1-x)]^{-3/2} = -4/z^3. \tag{A6}$$

We have

$$\frac{d\phi}{dx} = \frac{d\phi}{dz}\frac{dz}{dx}, \tag{A7}$$

whence

$$\frac{d^2\phi}{dx^2} = \frac{d\phi}{dz}\frac{d^2z}{dx^2} + \frac{d^2\phi}{dz^2}\left(\frac{dz}{dx}\right)^2. \tag{A8}$$

Combining all these equations together, we obtain

$$\frac{d^2\phi}{dx^2}=\frac{4}{z^3}\left(2z-\ln\frac{1+z}{1-z}\right). \tag{A9}$$

Recall that $0<z<1$. The parenthesis on the right-hand side of Eq. (A9) vanishes for $z=0$, and its derivative is $2-2/(1-z^2)$, which is always negative. Therefore $(d^2\phi/dx^2)<0$, and it follows that the function $\phi[z(x)]$ is concave.

APPENDIX B: SYMMETRIZED EAVESDROPPING

The purpose of this appendix is to prove Eq. (67). Consider the representation of Alice's four states on a Poincaré sphere. They lie on the equatorial plane, at the ends of two perpendicular diameters. The states that Bob receives are also represented by four points. The latter are located *inside* the sphere, since these are mixed states.

Eve proceeds as follows: before eavesdropping, she randomly rotates Alice's signal by 0°, 45°, 90°, or 135° in the plane of Fig. 1 (that is, she rotates the Poincaré sphere by 0°, 90°, 180°, or 270° around its polar axis). After the eavesdropping interaction, she rotates the signal back, and then sends it to Bob. This causes no change to the *average* amount of information she gathers, but equalizes the disturbances to Alice's four states. By virtue of this symmetrization, the set of Bob's states is now invariant under rotations of the Poincaré sphere by 90°, 180°, and 270°. Therefore, the four points representing these states form a square, lying in a plane parallel to the equatorial plane. If the sides of that square are not parallel to those of the square formed by Alice's states, they can be made parallel by a further rotation around the polar axis. This does not change Eve's I, but this reduces Bob's D, thus improving the eavesdropping method.

Moreover, the four points that represent ρ_{Bob} can be made to lie on the equatorial plane itself, not on a parallel plane above or below it. If they are not on the equatorial plane, this means that the eavesdropping interaction produces a circularly polarized component in the outgoing state (recall that the poles of the Poincaré sphere represent pure circular polarizations). This is indeed possible if the unitary interaction of the probe involves complex coefficients. In that case, Eve ought to have two available probes, whose interactions are described by complex conjugate unitary matrices. The second probe yields Bob's states on the other side of the equatorial plane. By randomly choosing one of the two probes, Eve can bring Bob's states back to the equatorial plane (where Alice's states are). This changes neither I nor D.

This argument proves that the result stated in Eq. (67) can indeed be achieved by symmetrizing any eavesdropping strategy. In particular, there must also be an optimal strategy giving rise to Eq. (67).

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

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Crypto. **5**, 3 (1992).

[3] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).

[4] A. Ekert and B. Huttner, J. Mod. Opt. **41**, 2455 (1994).

[5] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).

[6] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993), p. 282.

[7] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997).

[8] C.-S. Niu and R. B. Griffiths (unpublished).

[9] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995); C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, *ibid.* **75**, 4714 (1995).

[10] R. B. Griffiths and C.-S. Niu, following paper, Phys. Rev. A **56**, 1173 (1997).

[11] D. Mayers, in *Advances in Cryptology – CRYPTO '96*, edited by N. Koblitz (Springer, Berlin, 1996).

[12] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[13] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997); see also E. Biham and T. Mor, Report No. quant-ph/9605010. Recently it has been pointed out to us that Eq. (4) in that work contains an eavesdropping stategy that happens to achieve the bound in our Eq. (65). However, Biham and Mor did not study the optimality issue in their work.

[14] J. I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).

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

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

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

[18] C. A. Fuchs, Report No. quant-ph/9611010.

[19] G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities* (Cambridge University Press, Cambridge, England, 1952), p. 89.

[20] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).

[21] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).

[22] C. A. Fuchs and C. M. Caves, Phys. Rev. Lett. **73**, 3047 (1994).

[23] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[24] L. B. Levitin, in *Workshop on Physics and Computation: Phys Comp '92*, edited by D. Matzke (IEEE Computer Society Press, Los Alamitos, CA, 1993).

[25] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).

[26] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).

[27] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[28] S. L. Braunstein and A. Mann, Phys. Rev. A **47**, 2427 (1993).