Eavesdropping on quantum-cryptographical systems

Artur K. Ekert
Merton College and Department of Physics, University of Oxford, Oxford OX1 4JD, United Kingdom

Bruno Huttner*
Department of Physics, Clarendon Laboratory, University of Oxford, Oxford OX1 4JD, United Kingdom

G. Massimo Palma
Istituto di Fisica, Università di Palermo, via Archirafi 36, I-90123 Palermo, Italy

Asher Peres
Department of Physics, Technion–Israel Institute of Technology, 32 000 Haifa, Israel
(Received 9 September 1993)

Quantum cryptography cannot prevent eavesdropping, but any eavesdropping attempt can be detected by the legitimate users of the communication channel. This is because eavesdropping affects the quantum state of the information carriers and results in an abnormal error rate. In this paper, we analyze various eavesdropping techniques, which may be either translucent or opaque to the transmitted photons, and we estimate the error rate above which the key distribution is deemed unsafe and should be abandoned.

PACS number(s): 03.65.Bz, 89.70.+c, 42.50.Wm

I. INTRODUCTION

Quantum cryptography [1–4], a new branch of physics and cryptology, relies on the impossibility of ascribing definite values to noncommuting variables in order to assure secrecy of communication. Theoretical and experimental efforts in this area have been concentrated mainly on one of the basic cryptographic techniques, namely key distribution [4–8]. Other cryptographic techniques, such as quantum bit commitment and quantum oblivious transfer, have also been analyzed and can play an important role in practical implementations of quantum-cryptographical systems [9,10].

Secure key distribution is a procedure allowing two legitimate users of a communication channel to produce two identical copies, one copy for each user, of a random and secret sequence of bits. This random sequence, meaningless as such, is called *a key*. It can subsequently be used for encrypting messages between the two users. The security of any encrypted communication depends directly on the security of the key distribution.

Conventional cryptography provides no tools to guarantee the security of the key distribution. Any encoding by means of classical objects is vulnerable to passive interception. Such interception may be difficult from the technological point of view, but as long as it is allowed by the laws of physics, the two legitimate users can never be sure that no third party has acquired a copy of their key. In a schematic way, passive eavesdropping can be viewed as a two-stage process. The first stage amounts to making copies of the carrier of information without altering the state of the latter, and the second to reading from these copies (or "clones") the values of the observables used for the encoding of the key. The intercepted original carrier is then sent over to the legitimate receiver, who is unable to check whether that carrier has been intercepted or not, because the state of the carrier is not altered by the cloning process.

However, the first stage of passive eavesdropping cannot in general be achieved in the case of a quantum transmission. According to quantum theory, cloning can give a faithful replica, while leaving the state of the original intact, only if it is known in advance that the carrier of information is in a quantum state belonging to a definite set of *orthonormal* states [11,12]. If this is not the case, the eavesdropper will not be able to construct even an imperfect cloning device, which would give some information on the carrier *without modifying it:* a device of this sort would violate unitarity. Therefore coding based on nonorthogonal quantum states (which cannot be cloned) gives a possibility to detect any eavesdropping attempt.

In this article we analyze conceptually the simplest quantum-cryptographical system based on two nonorthogonal states [5], from the point view of its robustness to various eavesdropping strategies. In particular, we compare "translucent" eavesdropping, whereby the information carrier is only gently disturbed by an incomplete measurement yielding only a small amount of information, with conventional "opaque" eavesdropping, in which the information carrier is captured, measured, and then resent. Other aspects of quantum eavesdropping were recently discussed by Barnett and Phoenix [13,14].

As an example, if the information carrier is a polarized

*Present address: NTT Basic Research Laboratories, 3-1 Morinosato Wakamya, Atsugi, Kanagawa 243-01, Japan.

 ©1994 The American Physical Society

photon, a conceptual method for translucent eavesdropping could be to let the photon pass through a small birefringent crystal, and then measure the recoil of that crystal (due to momentum conservation). An elementary calculation shows that if a freely moving crystal of mass m deflects a photon of wavelength λ by an amount b, the crystal recoil is $b(\lambda_C/\lambda)$, where $\lambda_C = h/mc$ is the Compton wavelength of the crystal. If the crystal is very thin, so that b is smaller than the width of the photon beam, the emerging photons are only very slightly depolarized. In the present paper we shall not discuss this particular method of translucent eavesdropping, but two others, whose mathematical description is simpler (but for which we provide no concrete physical model).

II. COMMUNICATION PROTOCOL

The two legitimate users, traditionally called Alice and Bob, want to establish a cryptographic key. Alice starts the key distribution with a quantum transmission, sending to Bob a random sequence of quanta in two nonorthogonal states $\mathbf{u}$ and $\mathbf{v}$, which represent bits 0 and 1, respectively [5].

By a suitable choice of phases and of the basis, the two quantum states $\mathbf{u}$ and $\mathbf{v}$, whose overlap is $|\langle \mathbf{u}|\mathbf{v}\rangle|^2 = \sin^2 2\alpha$, can always be written as

$$\mathbf{u} = \begin{bmatrix} \cos\alpha \\ \sin\alpha \end{bmatrix} \quad \text{and} \quad \mathbf{v} = \begin{bmatrix} \sin\alpha \\ \cos\alpha \end{bmatrix} . \tag{1}$$

On the receiving side, Bob has to distinguish between these two nonorthogonal states for each incoming carrier. Of course he cannot do that with certainty. He can, however, perform a test which sometimes fails to provide an answer, but once it does give an answer, the latter is always the correct one. In the language of information theory [15], this situation corresponds to Alice and Bob having at their disposal a communication channel known as a "binary erasure channel," schematized in Fig. 1(a).

To achieve this result, the simplest (but not the most efficient) approach for Bob is to measure, say with the same probability, one of the projection operators

$$\mathbf{P}_{\neg u} = \mathbf{1} - \mathbf{u}\mathbf{u}^\dagger \quad \text{or} \quad \mathbf{P}_{\neg v} = \mathbf{1} - \mathbf{v}\mathbf{v}^\dagger . \tag{2}$$

A positive result for $\mathbf{P}_{\neg u}$ indicates with certainty that the information carrier was in the $\mathbf{v}$ state, and vice versa. A null result is of no use if only unambiguous conclusions are acceptable. (It only gives the *a posteriori* probabilities for $\mathbf{u}$ and $\mathbf{v}$.)

The probability of getting this inconclusive result is $(1+\langle \mathbf{u}|\mathbf{v}\rangle^2)/2$. That probability can be reduced somewhat by a more sophisticated measurement process [16,17] which uses an auxiliary quantum system prepared in a known initial state. After a suitable unitary evolution of the combined system, the latter is left in an entangled state for which the probability of an inconclusive answer is only $\langle \mathbf{u}|\mathbf{v}\rangle$ (recall that $1+x^2 > 2x$ for any $x \neq 1$). In the language of modern measurement theory [18,19], Bob uses a *positive operator valued measure* (POVM) consisting of the operators

$$\begin{aligned} \mathbf{A}_u &= \mathbf{P}_{\neg v}/(1+S) , \\ \mathbf{A}_v &= \mathbf{P}_{\neg u}/(1+S) , \\ A_? &= \mathbf{1} - \mathbf{A}_u - \mathbf{A}_v , \end{aligned} \tag{3}$$

where $S = \langle \mathbf{u}|\mathbf{v}\rangle = \sin 2\alpha$, and the index "?" refers to an inconclusive test. The probability of obtaining the answers $\mathbf{u}$, $\mathbf{v}$, or ?, following the preparation of a carrier in any state ρ, is $\mathrm{Tr}(\rho\,\mathbf{A}_u)$, $\mathrm{Tr}(\rho\,\mathbf{A}_v)$, and $\mathrm{Tr}(\rho\,\mathbf{A}_?)$, respectively. (Note that the various $\mathbf{A}_i$ do not commute, contrary to von Neumann's projection operators in elementary measurement theory. Moreover, the final state of the carrier is *not* in general an eigenstate of $\mathbf{A}_i$, so that the result of such a generalized measurement is not, in general, repeatable).

In the following, we assume that Bob uses this more efficient detection method, so that the probability of an inconclusive result is

$$R_0 = \sin 2\alpha . \tag{4}$$

After completion of the quantum transmission, Alice and

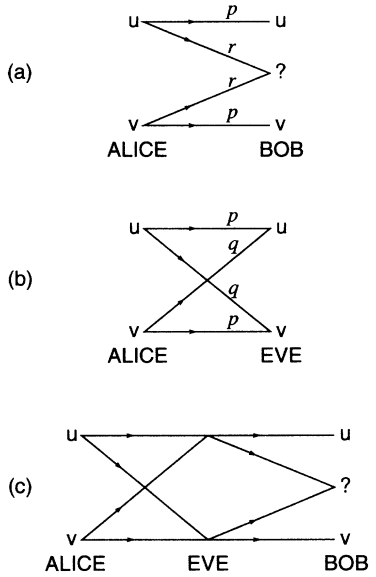

FIG. 1. (a) In the absence of an eavesdropper. Alice and Bob share a binary erasure channel. Alice encodes two bit-values "0" and "1" in two nonorthogonal vectors $\mathbf{u}$ and $\mathbf{v}$. Bob's detection procedure can produce three possible outcomes; it can either, with probability p, determine correctly the encoded bit value (0 or 1) or, with probability r, give an inconclusive result ($p+r=1$). The probability of obtaining the inconclusive result depends on the detection procedure, and is at least $|\langle \mathbf{u}|\mathbf{v}\rangle| = \sin 2\alpha$. (b) In a binary symmetric channel, such as this one shared by Alice and Eve, there are no inconclusive results, but the detection events are subject to errors. The probability of a correct transmission in p, and the probability of an error is q, such that $p+q=1$. This type of channel is entirely characterized by its error rate, Eq. (6). (c) By attempting to eavesdrop on the transmission, Eve modifies the transmission channel between Alice and Bob. In the opaque eavesdropping strategy, Eve receives bits from Alice via a binary symmetric channel and resends them to Bob via a binary erasure channel, masquerading Alice in front of Bob.

Bob communicate in public and discard all inconclusive results, so that in the absence of external disturbances, the remaining instances are perfectly correlated: they consist entirely of cases in which Alice sent 0 and Bob detected 0, or Alice sent 1 and Bob detected 1. Alice and Bob can check whether this is effectively the case by revealing to each other in public the parities of random substrings of bits (and subsequently discarding one bit of each substring).

As we shall show in the following, an eavesdropper, conventionally called Eve, may change the rate of inconclusive results, and will unavoidably introduce some errors. Bob will thus look for eavesdropping by first comparing the actual rate of inconclusive results R with the expected value R_0—a significant discrepancy will indicate eavesdropping. However, as will be shown in Sec. IV A, there exists an eavesdropping strategy which does not modify the rate of inconclusive results. This first test may thus reveal an eavesdropper (if $R \neq R_0$), but a negative result does not guarantee the safety of the transmission. Alice and Bob have to go one step further and to estimate the error rate in the transmission (by "error" we mean a mismatch between Alice's and Bob's data). If the error probability before discarding the inconclusive results is q, then the fraction of erroneous readings after discarding the inconclusive results is $Q = q/(1-R)$. In principle, any nonzero error rate Q may indicate eavesdropping; however, in practice, the transmission is subject to noise, and there will be some discrepancies even in the absence of eavesdropping.

The problem facing Alice and Bob is now to decide on the maximum tolerable discrepancy allowed, which would still give them a secure key. Since the issue is the *security* of a transmission, Alice and Bob cannot take any chance: they must consider the worst possible scenario and assume that Eve has acquired as much information as possible, subject only to the constraints of quantum mechanics. It is then quite possible that they will consider a key transmission unsafe because they fear that too much information has leaked to Eve, while actually it is Eve's eavesdropping attempt which failed. However, if security is their prime concern, this is the only reasonable decision that can be taken under the given circumstances.

III. ROBUSTNESS TO EAVESDROPPING

After completing the first part of the protocol for the quantum key distribution and discarding the inconclusive results, the three participants, Alice, Bob, and Eve, have a string of bits each. The three strings are different due to random errors, and to the errors introduced by Eve. As Alice and Bob cannot reliably distinguish between these two types of errors, they shall assume that they are all caused by an eavesdropper. Their task is thus, for a given error rate Q, to estimate the amount of information that may have leaked to an eavesdropper, and decide whether they can still use their data to obtain a secure key. (The only parameter used by Alice and Bob at this stage is the error rate Q, because R, the fraction of inconclusive results, may not be affected by some clever methods, as shown below). For a significant error rate Q, the key distribution must be set up again; but there is usually a "safety zone" within which Alice and Bob can implement various cryptographic techniques to communicate in perfect secrecy. The more robust the cryptographical system is to eavesdropping, the larger the safety zone it has. Cryptographical systems with no robustness, i.e., those operating properly only at the zero error rate, cannot be regarded as practical due to the residual errors from the environmental noise, which one cannot eliminate completely.

Before we proceed any further let us briefly introduce some basic concepts from information theory, which will later be used in the paper [15]. Let A and B be two binary random variables with joint probability distribution $p(A,B)$. The mutual information

$$I_{AB} = \sum_{A,B} p(A,B) \log_2 \frac{p(A,B)}{p(A)p(B)} , \tag{5}$$

to get the information in bits, quantifies the dependence between the two random variables. It is symmetric in A and B and always non-negative. If we have three (or more) random variables with the joint probability distribution $p(A,B,X)$, the mutual information I_{AB} is calculated with the reduced probability distribution $p(A,B)$, obtained from $p(A,B,X)$ by summing over X. For a communication channel with input A and output B, we define the *information* channel capacity as the maximum of I_{AB} taken over all possible probabilities of input $p(A)$. The *operational* channel capacity is defined as the highest rate, in bits, at which information can be sent with arbitrarily low probability of error. The Shannon channel-coding theorem asserts that the information channel capacity is equal to the operational channel capacity, and that the capacity limit can be achieved by using codes with a long block length. However, the theorem does not provide any method for building such codes. Nevertheless, the channel capacity is a very clear dividing point: at rates below the capacity there exist codes that support error-free communication, and at rates above the capacity, regardless of the codes employed, an abundance of errors is guaranteed.

The basic example of a noisy channel is a binary symmetric channel, which is schematized in Fig. 1(b). The channel is entirely characterized by its error rate q. In this case, the capacity of the channel can be calculated to be [15]

$$I = 1 + q \log_2 q + (1-q)\log_2(1-q) \tag{6}$$

bits per transmission. In the following, I_{XY} denotes the maximal mutual information between two parties X and Y, or the capacity of the channel established by X and Y. In our scenario, after Alice and Bob have discarded the inconclusive results, all the information flow between Alice-Bob, Alice-Eve, and Eve-Bob can be modeled as a transmission over binary symmetric channels. (Note that a careless eavesdropper could introduce a different error rate for the two input states **u** and **v**, thus creating an asymmetric channel between Alice and Bob. As this would be easily discovered by Alice and Bob, we assume that Eve is clever enough to avoid this pitfall.)

The problem of secret communication involving three parties has been analyzed in the context of classical cryptography. Wyner [20] considered a communication scenario in which Alice wants to transmit data as reliably as possible to Bob while keeping the wiretapper Eve as ignorant as possible. Wyner proved that when Eve receives Bob's channel output through an additional cascaded independent channel (i.e., the effective channel Alice-Eve is more noisy than the channel Alice-Bob) then Alice can send information to Bob in perfect secrecy by choosing an appropriate data coding. Wyner's wiretap channel was later generalized by Csiszár and Körner [21] who considered the following scenario: Alice prepares the input bit A with some probability $p(A)$. It is then received by Bob and Eve as bit B and E, respectively; the transmission is completely specified by the conditional probability distribution $p(B,E|A)$. Csiszár and Körner defined the secrecy capacity C_s of the channel with transition probabilities $p(B,E|A)$ as the maximum rate at which Alice can reliably send information to Bob such that the rate at which Eve obtains this information is arbitrarily small. They also provided a lower bound for C_s, which for the purpose of our analysis, can be written as

$$C_s \geq I_{AB} - I_{AE} . \tag{7}$$

Therefore, if $I_{AB} > I_{AE}$, Alice and Bob can use the fact that their channel is better than the channel available to Eve. Alice can send data to Bob at some rate below I_{AB}, which allows error-free communication; at the same time, this rate is above I_{AE}, so that there is no valid decoding procedure for correcting errors at the output of Eve's channel. These errors will effectively leave Eve ignorant of data sent to Bob.

A further generalization of the scenario outlined above allows Alice and Bob to supplement their data transmission with an exchange of messages over a public channel. The data flow becomes more complicated and so-called "conceptual channels" between the parties must be analyzed [15]. Applied to our considerations, this generalization requires including Eve's information on Bob's data and extending formula (7) to

$$C_s \geq \max(I_{AB} - I_{AE}, I_{AB} - I_{BE}) . \tag{8}$$

In the following, we use condition (8) and we assume that whenever I_{AB} is greater than either I_{AE} or I_{BE}, then at least *in principle* there is a way for Alice and Bob to distribute a string of secret information. On the other hand, if the result of eavesdropping is that $I_{AB} \leq \min(I_{AE}, I_{BE})$, we shall *assume* that the transmission is unsafe. This assumption may be overcautious, as (8) provides only a lower limit for C_s. It was indeed shown by Maurer [22] that for some classical broadcasting channels this condition is too restrictive.

Of course, the information available to Eve depends on the strategy adopted and, for a given I_{AB} (or equivalently for a given error rate Q), different strategies would give different values for I_{AE} and I_{BE}. In this work we shall compare three eavesdropping strategies and show that, by choosing the best one, Eve can acquire more information than with the others, without causing a larger increase of the error rate. We make no claims as to whether there exist even better methods. There may be clever ones, not investigated by us, which give Eve still a larger amount of information on the key, while keeping the same error rate Q.

On the practical side, Shannon's coding theorem, on which our analysis is based, has a nonconstructive proof: we know that there exists an encoding procedure which will provide a secret transmission, but the theorem does not specify the procedure itself. This is the reason why practical key distribution schemes rely on different techniques, known as error correction via reconciliation protocol and privacy amplification [4]. These techniques provide a practical way of extracting a corrected key from the corrupted one, and of enhancing the secrecy of this key. However, to our knowledge, there is no generally accepted limit on the information on the final key (after error correction and privacy amplification) known to Eve as a function of the error rate [23].

IV. THREE STRATEGIES FOR EAVESDROPPING

We shall now analyze three eavesdropping strategies. The first one is opaque and the other two translucent. For each strategy, we calculate R and Q, and we plot I_{AE} and I_{BE} as functions of Q (see Fig. 2). In order to compare these results with the information shared by Alice and Bob, we also plot $I_{AB}(Q)$, which is given by Eq. (8). For the ideal, eavesdropping-free case we have, of course, $R \equiv R_0 = \sin 2\alpha$ and $Q = 0$.

A. Opaque eavesdropping

Eve intercepts the quantum carrier on its way from Alice to Bob and performs a measurement which maximizes her information as to which one of the two states, **u** or **v**, was chosen for preparing the carrier. The best procedure in this case is the measurement of a Hermitian operator whose two orthogonal eigenvectors are symmetrically related to the signal states **u** and **v** [24]. In the same basis as used in Eq. (1), these two eigenvectors are simply $\binom{1}{0}$ and $\binom{0}{1}$.

After the measurement, Eve sends to Bob another quantum carrier, prepared in state **u** or **v**, according to the outcome of her measurement on the real carrier. This strategy can be modeled as a flow of information from Alice to Eve through a binary symmetric channel [15] and then from Eve to Bob through a binary erasure channel, as shown in Fig. 1(c).

Firstly, let us notice that this strategy does not affect R; Eve is masquerading Alice and sending to Bob, with the same probability, carriers in states **u** or **v**, so that Bob will detect the same fraction of inconclusive results as if it were Alice preparing and sending them. On the other hand, Eve wrongly identifies some fraction of the bits sent by Alice. By resending them to Bob, she will affect Q. For each carrier intercepted, Eve's error rate is $\sin^2\alpha$ and the maximum information she can have on Alice's string of bits is given by Eq. (6), with $q = \sin^2\alpha$. In order to lower Bob's error rate, Eve may decide not to intercept and resend all the quantum carriers, but only some frac-

tion of them, say η. The information available to her thus becomes

$$I_{AE}=\eta(1+\sin^2\alpha\log_2\sin^2\alpha+\cos^2\alpha\log_2\cos^2\alpha)\ . \quad (9)$$

Bob will observe, on the average, a fraction $\sin 2\alpha$ of inconclusive results. After discarding them he can, by communicating with Alice in public, estimate the error rate between him and Alice in the remaining string of bits. This error rate, after discarding the inconclusive results, is $Q=\eta\sin^2\alpha$. This gives the information I_{AE} as a function of the error rate

$$I_{AE}=(Q/\sin^2\alpha)\times(1+\cos^2\alpha\log_2\cos^2\alpha+\sin^2\alpha\log_2\sin^2\alpha)\ . \quad (10)$$

Moreover, we have

$$I_{BE}=\eta=Q/\sin^2\alpha\ . \quad (11)$$

In the extreme case, when Eve eavesdrops on each bit ($\eta=1$, whence $Q=\sin^2\alpha$), her information on Bob's data, after discarding the inconclusive results, is maximal—she knows each bit of Bob's data. Clearly any public error correction and privacy amplification is useless in this case as Eve, by listening to the public channel, can follow each step agreed by Alice and Bob. In Fig. 2, we show how I_{AE} and I_{BE} depend on Q (dotted lines). This strategy invalidates any key distribution with an error rate $Q>\sin^2\alpha$, even when the rate of inconclusive results is unchanged ($R=R_0$).

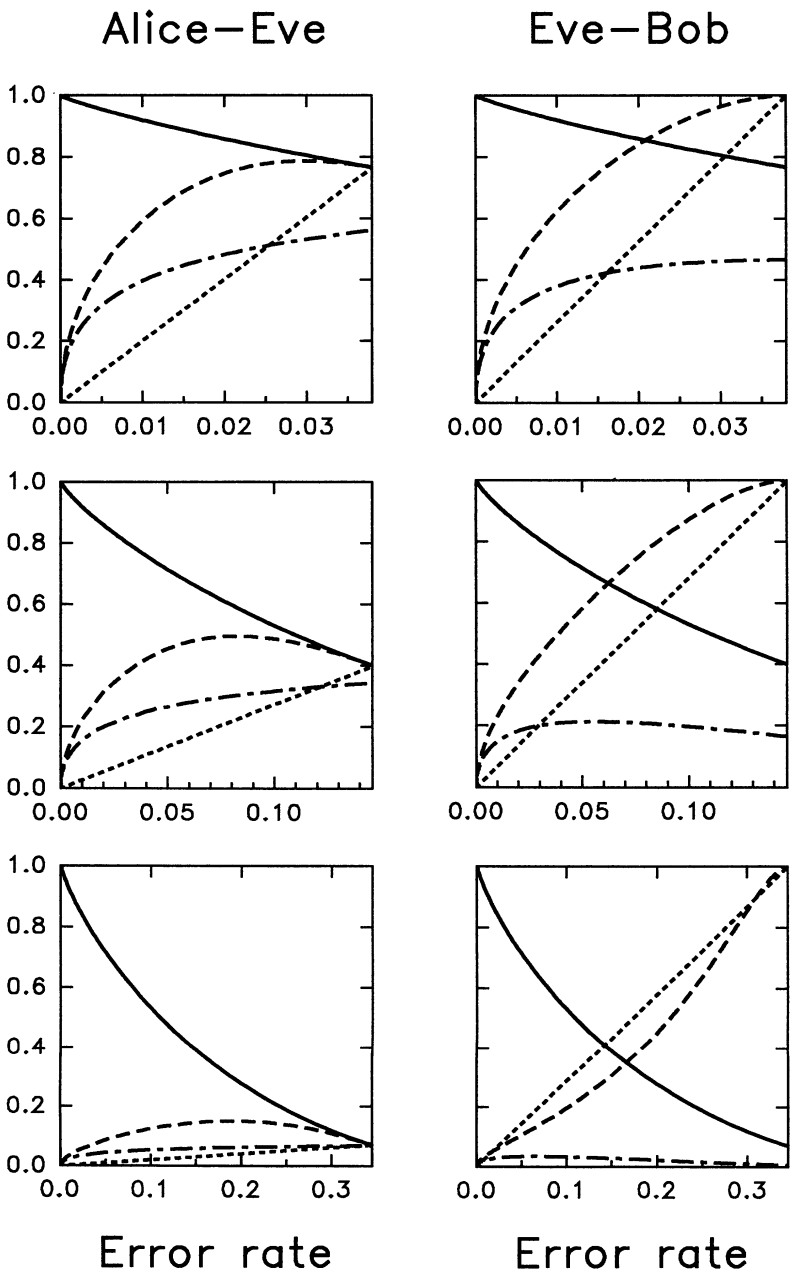

FIG. 2. These plots show how the mutual information between Alice, Bob, and Eve depends on Bob's error rate Q, for three values of α: from top to bottom, $\alpha=\pi/16$, $\pi/8$, and $\pi/5$. Dotted lines refer to the opaque eavesdropping strategy (Sec. IV A); dash-dot and dashed lines refer, respectively, to the first and the second translucent eavesdropping method (Secs. IV B and IV C). The solid lines show $I_{AB}(Q)$, the mutual information between Alice and Bob. It is of course exactly the same for all six subplots.

B. Translucent eavesdropping (without entanglement)

In this strategy Eve attempts to gain some information on each signal sent by Alice, while minimizing the damage to the state of the latter. In opposition to the previous case, she does *not* perform a standard quantum measurement on the carrier, but rather uses a POVM [18,19] as explained above. That POVM can be realized by making the information carrier interact unitarily with a probe, and then letting it proceed to Bob, in a slightly modified state. In principle, Eve could store her probe and make her measurement much later. The potential advantage of this scheme is that it enables Eve to decide on the type of measurement to perform on her probe only after Alice and Bob have gone through the whole procedure of error correction and privacy amplification. In particular, she can decide, for each bit, whether to try to obtain as much information as possible (this will provide her with probabilistic information) or to have definite results with probability less than 1 (and get deterministic information on fewer bits). In this work we shall assume that Eve chooses to maximize her information, so that she can determine bit values with a certain probability rather than knowing some fraction of them precisely and knowing nothing about the rest (it is likely that this is the best Eve can do).

Eve thus supplies a probe in a known initial state ψ, and, according to the state sent by Alice, the combined system evolves either as

$$\begin{pmatrix}\cos\alpha\\ \sin\alpha\end{pmatrix}\otimes\psi\equiv\mathbf{u}\otimes\psi\rightarrow\mathbf{u}'\otimes\mathbf{e}_{\mathbf{u}}\equiv\begin{pmatrix}\cos\beta\\ \sin\beta\end{pmatrix}\otimes\begin{pmatrix}\cos\gamma\\ \sin\gamma\end{pmatrix}, \tag{12}$$

or as

$$\begin{pmatrix}\sin\alpha\\ \cos\alpha\end{pmatrix}\otimes\psi\equiv\mathbf{v}\otimes\psi\rightarrow\mathbf{v}'\otimes\mathbf{e}_{\mathbf{v}}\equiv\begin{pmatrix}\sin\beta\\ \cos\beta\end{pmatrix}\otimes\begin{pmatrix}\sin\delta\\ \cos\delta\end{pmatrix}. \tag{13}$$

This evolution is *unitary* (and therefore it is always possible to concoct some Hamiltonian which generates it) provided that

$$\sin2\alpha=\sin2\beta\sin(\gamma+\delta)\ . \tag{14}$$

The idea is to cause minimal damage to the information carrier ($\sin2\beta$ would be only slightly larger than $\sin2\alpha$) while obtaining some information from the probe thanks to the fact than $\sin(\gamma+\delta)<1$ (it was 1 before the interaction). For any other initial state of the information carrier, the final state of the composite system will not be a direct product as in (12) and (13). It will be entangled, and the final states of the information carrier and of the probe, considered separately, will be impure density matrices. In the following discussion, we shall assume that $\gamma=\delta$, for the sake of symmetry.

After sending the modified carrier to Bob, Eve is left with her probe in one of the two states: $\mathbf{e}_{\mathbf{u}}$ corresponding to an input state **u**, or $\mathbf{e}_{\mathbf{v}}$ corresponding to an input state **v**. In general, these two states are not orthogonal and, as we already mentioned, the largest information gain may be achieved by testing for the two eigenvectors $\binom{0}{1}$ vs $\binom{1}{0}$. In this case, Eve can only learn *a posteriori* probabilities for **u** and **v**. The latter are either $\cos^2\gamma$ or $\sin^2\gamma$. Her information gain is

$$I_{AE}=1+\cos^2\gamma\log_2\cos^2\gamma+\sin^2\gamma\log_2\sin^2\gamma\ . \tag{15}$$

We now turn our attention to Bob, who attempts to identify the incoming signal as efficiently as possible by using the POVM in Eqs. (3). Now, however, if the signal sent by Alice was in state **u**, the one actually received by Bob is, because of Eve's intervention, in a different state, namely **u**′. The probability that Bob will observe the result which is orthogonal to **u** and therefore is interpreted as **v** is

$$q=\langle\mathbf{u}'|\,\mathbf{A}_{\mathbf{v}}|\mathbf{u}'\rangle=\frac{(\cos\alpha\sin\beta-\sin\alpha\cos\beta)^2}{(\cos\alpha+\sin\alpha)^2}=\frac{\sin^2(\alpha-\beta)}{(1+\sin2\alpha)}\ . \tag{16}$$

This is the probability of a *wrong identification* of the incoming signal. The probability of no identification (inconclusive test) is

$$R=\langle\mathbf{u}'|\,\mathbf{A}_{?}|\mathbf{u}'\rangle=\sin2\alpha\frac{(\cos\beta+\sin\beta)^2}{(\cos\alpha+\sin\alpha)^2}=\sin2\alpha\frac{1+\sin2\beta}{1+\sin2\alpha}=R_0\frac{1+\sin2\beta}{1+\sin2\alpha}\ . \tag{17}$$

In this situation, Bob will be alerted by an unexpectedly high rate in inconclusive tests, even before he compares his parity checks with those of Alice. Eve can reduce this effect by occasionally absorbing Alice's signals, and replacing them by fake signals, say **u**″ and **v**″, with smaller overlap than **u** and **v**. As these signals are less likely to give an inconclusive result than **u** and **v**, this will enable Eve to reduce the rate of inconclusive results, and even bring it back to R_0. Of course, this will increase the error rate and can be detected by parity checks. We shall not analyze this more complicated strategy further. Its main interest is to show that the rate of inconclusive results along is not a reliable test for eavesdropping.

After discarding the inconclusive results, Bob, in public discussion with Alice, will estimate his error rate as

$$Q=q/(1-R)=\sin^2(\alpha-\beta)/(1-\sin2\alpha\sin2\beta)\ . \tag{18}$$

Equations (14), (15), and (18) determine I_{AE} as a function of Q.

The mutual information between Eve and Bob can be calculated on the basis of the error rate between Eve's and Bob's data. This error rate is given by

$$q_{BE}=Q\cos^2\gamma+(1-Q)\sin^2\gamma\ . \tag{19}$$

In Fig. 2 we plot I_{AE} and I_{BE} as functions of Q (dash-dot lines).

We note that this strategy is especially interesting for "weak" eavesdropping ($\gamma\simeq\pi/4$), i.e., when Eve attempts to obtain a small amount of information while causing only a slight disturbance. In this case, as seen in Fig. 2, the amount of information obtained increases as the *square root* of the error rate; it was *linear* in the error rate for the previous strategy. For "strong" eavesdropping,

however (that is, $\gamma \simeq \alpha$), as Eve attempts to get as much information as possible on the bits sent by Alice, this strategy clearly fails. The reason for that is that Eve ends up ultimately affecting the state of the carriers in such way that Bob can obtain no information at all: regardless of the initial state $\mathbf{u}$ or $\mathbf{v}$, the state sent to Bob becomes $\binom{1/\sqrt{2}}{1/\sqrt{2}}$.

Therefore, we shall now turn to a third eavesdropping strategy that tries to combine the best characteristics of the previous two. In particular, it can be reduced to the opaque intercept-resend strategy for strong eavesdropping, and to the translucent strategy for weak eavesdropping. The new strategy is a variant of the translucent strategy in which the carrier and the probe do not disentangle at the end of interaction.

C. Translucent eavesdropping (with entanglement)

As explained above, the main drawback of the preceding strategy is that, as Eve attempts to obtain more information on the bits sent by Alice, she increases the overlap between the two states sent to Bob and thus reduces the information shared with Bob. In order to increase this mutual information, Eve may attempt to entangle the states of her probe and of the carrier that she is resending. This can be done as follows (see Fig. 3).

Eve supplies a probe in a known initial state ψ, and the combined system evolves either as

$$\mathbf{u}\otimes\psi \rightarrow a\,\mathbf{u}\otimes\mathbf{e}_u + b\,\mathbf{v}\otimes\mathbf{e}_v \tag{20}$$

or

$$\mathbf{v}\otimes\psi \rightarrow b\,\mathbf{u}\otimes\mathbf{e}_u + a\,\mathbf{v}\otimes e_v \ , \tag{21}$$

where, as previously, e_u and e_v represent the states of Eve's probe: $\mathbf{e}_u = \binom{\cos\gamma}{\sin\gamma}$ and $\mathbf{e}_v = \binom{\sin\gamma}{\cos\gamma}$.

This evolution is *unitary* provided that the real coefficients a and b satisfy the following two conditions:

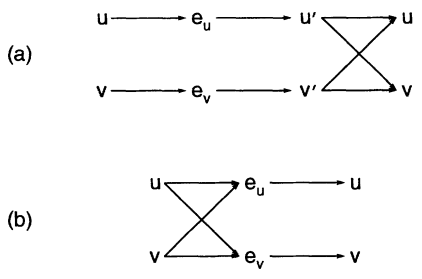

FIG. 3. This figure shows (in a very simplified way) the difference between translucent eavesdropping without entanglement (Sec. IV B) and translucent eavesdropping with entanglement (Sec. IV C). (a) In the first case, if Alice sends $\mathbf{u}$, Eve always obtains $\mathbf{e}_u$ and Bob obtains $\mathbf{u}'$, which can be read by him either as $\mathbf{u}$ or as $\mathbf{v}$. Therefore the state obtained by Eve is perfectly correlated with the state sent by Alice, but not with the state read by Bob. (b) In the second strategy, Eve attempts to keep a perfect correlation with Bob's state, e.g., $\mathbf{e}_u$ is always paired with Bob's $\mathbf{u}$. However, in this case, the correlation with Alice's state is not perfect.

$$1 = a^2 + b^2 + 2ab\,\sin 2\alpha \sin 2\gamma \ , \tag{22}$$

$$\sin 2\alpha = 2ab + (a^2 + b^2)\sin 2\alpha \sin 2\gamma \ . \tag{23}$$

Note that for weak eavesdropping ($\gamma \approx \pi/4$), the states $\mathbf{e}_u$ and $\mathbf{e}_v$ are very close to each other so that the probe and the information carrier are hardly entangled, as in the previously analyzed case of translucent eavesdropping. However, for strong eavesdropping ($\gamma \rightarrow 0$) the whole strategy looks as if Eve, after obtaining maximum information about the state of the carrier, tosses a biased coin and sends to Bob, with probability $|a|^2 = \cos^2\alpha$, a carrier in the state she detected, and with probability $|b|^2 = \sin^2\alpha$, one in the opposite state. The latter case therefore is a modification of the opaque eavesdropping method. The comparison between the two translucent strategies is shown in Fig. 2–dash-dot versus dashed lines.

A convenient parametrization for a and b is

$$\begin{aligned} a &= \cos(\alpha+\phi)/\cos 2\phi \ , \\ b &= \sin(\alpha-\phi)/\cos 2\phi \ , \end{aligned} \tag{24}$$

with the additional condition,

$$\sin 2\phi = \sin 2\alpha \sin 2\gamma \ . \tag{25}$$

Using this parametrization, the strategy can be written in a way which is similar to the previous one where two nonorthogonal input states $\mathbf{u}\otimes\psi$ and $\mathbf{v}\otimes\psi$ are transformed into two output states $\mathbf{u}'\otimes\mathbf{e}_u$ and $\mathbf{v}'\otimes\mathbf{e}_v$, which are direct products of the carrier and the probe states. Here the two input states which evolve into two direct product states are $\mathbf{u}'' = \binom{\cos\phi}{\sin\phi}$ and $\mathbf{v}'' = \binom{\sin\phi}{\cos\phi}$, which are transformed as

$$\mathbf{u}''\otimes\psi \rightarrow \mathbf{u}\otimes\mathbf{e}_u \tag{26}$$

and

$$\mathbf{v}''\otimes\psi \rightarrow \mathbf{v}\otimes\mathbf{e}_v \ . \tag{27}$$

Knowing the evolution of the two states $\mathbf{u}''$ and $\mathbf{v}''$, it is easy to calculate the evolution of $\mathbf{u}$ and $\mathbf{v}$ and verify that it gives Eqs. (20) and (21), together with the unitarity condition, Eq. (25).

We note that in contrast to the previous strategy, when the input states are $\mathbf{u}$ are $\mathbf{v}$, the states of the carrier and the probe become entangled. In order to calculate the error rate Q, we could trace out the probe states and obtain the reduced density matrix as received by Bob. However, the calculations are quite lengthy, and it is preferable to work directly with the entangled state. Assuming the same type of detection as before, we can calculate the probability distributions of various possible outcomes from Alice, Eve, and Bob. For example, $p(0,1,?)$ represents the probability that Eve detected a 1 and Bob registered an inconclusive result "?" when Alice sent a 0. With this notation we obtain

$$p(0,0,0) = a^2(1-\sin 2\alpha)\cos^2\gamma \ , \tag{28}$$

$$p(0,0,?) = \sin 2\alpha(a\cos\gamma + b\sin\gamma)^2 \ , \tag{29}$$

$$p(0,0,1) = b^2(1-\sin 2\alpha)\sin^2\gamma \ . \tag{30}$$

Analogous instances in which Eve registered 1 are obtained from the above formulas by interchanging $\cos\gamma \leftrightarrow \sin\gamma$, for example

$$p(0,1,0)=a^2(1-\sin 2\alpha)\sin^2\gamma \ , \tag{31}$$

and instances in which Alice sent 1 are obtained by interchanging $a \leftrightarrow b$, as in

$$p(1,1,0)=b^2(1-\sin 2\alpha)\sin^2\gamma \ . \tag{32}$$

We calculate the transition probabilities by taking appropriate sums. For the binary erasure channel between Alice and Bob, we sum over all the possible results obtained by Eve to get the error rate (before discarding the inconclusive results),

$$q=\sum_{i=0,1} p(0,i,1)=\sum_{i=0,1} p(1,i,0)=b^2(1-\sin 2\alpha) \ , \tag{33}$$

and the rate of inconclusive results,

$$\begin{aligned} R &= \sum_{i=0,1} p(0,i,?) \\ &= \sum_{i=0,1} p(1,i,?) \\ &= (a^2+b^2+2ab\,\sin 2\gamma)\sin 2\alpha \ . \end{aligned} \tag{34}$$

Similarly, the error rate of the binary symmetric channel between Alice and Eve is

$$q_{AE}=\sum_{i=0,1,?} p(0,1,i)=(a^2+b^2)(1-\sin 2\alpha) \ , \tag{35}$$

and for the binary erasure channel between Eve and Bob,

$$\begin{aligned} q_{BE} &= \sum_{i=0,1} p(i,0,1) \\ &= (a^2+b^2)(1-\sin 2\alpha)\sin^2\gamma \ , \end{aligned} \tag{36}$$

$$\begin{aligned} R &= \sum_{i=0,1} p(0,i,?) \\ &= (a^2+b^2+2ab\,\sin 2\gamma)\sin 2\alpha \ . \end{aligned} \tag{37}$$

Note that R is the same for the Alice-Bob channel and for the Eve-Bob channel. After discarding the inconclusive results, we obtain the error rate for the Alice-Bob channel,

$$Q \equiv q/(1-R)=b^2/(a^2+b^2) \ , \tag{38}$$

for the Alice-Eve channel,

$$Q_{AE} \equiv q_{AE}/(1-R)=Q\cos^2\gamma+(1-Q)\sin^2\gamma \ , \tag{39}$$

and for the Eve-Bob channel,

$$Q_{BE} \equiv q_{BE}/(1-R)=\sin^2\gamma \ . \tag{40}$$

Using the standard formula for the binary symmetric channel capacity given in Eq. (6), together with Eqs. (24), (25), (38), (39), and (40), we can now calculate I_{AE} and I_{BE} as functions of Q. The plots are presented in Fig. 2 (dashed lines).

V. DISCUSSION

We have analyzed the simplest key distribution scheme, with the key encoding based on two nonorthogonal quantum states, and with the usual three *dramatis personae:* Alice, Eve, and Bob. Our analysis of three possible eavesdropping strategies that Eve can choose for her mischievous purposes shows an asymmetry in Eve's knowledge of Alice's and Bob's data. As seen in Fig. 2 (compare the first and the second column), Eve always obtains more information on Bob's string than on Alice's string: $I_{AE} \le I_{EB}$. This shows that in our case, Eq. (8) reduces to Eq. (7). Moreover, by choosing the right strategy, Eve can gain complete knowledge of Bob's string: $I_{BE}=1$ (second column), at the expense of introducing a large error rate in the transmission,

$$Q_{\max}=\sin^2\alpha \ . \tag{41}$$

From Alice's and Bob's point of view, the existence of a strategy which effectively discloses Bob's key to Eve, while creating an error rate $Q_{\max}$, means that all quantum transmissions with an error rate above $Q_{\max}$ should be abandoned. Following formula (7), we can see from the first column of Fig. 2 that the converse is also true: the secrecy capacity is positive for all error rates below $Q_{\max}$, indicating that as long as the error rate Q estimated by Alice and Bob is less than $Q_{\max}$, there exist error-correcting codes allowing Alice and Bob to establish a perfectly correlated, secret string of bits, if they wish to do so. Therefore, $Q_{\max}$ provides us with a well-defined border line: whenever $Q \ge Q_{\max}$, the key distribution failed (there exists a strategy which discloses all the information to Eve); whenever $Q < Q_{\max}$, it is in principle possible for Alice and Bob to communicate in perfect secrecy.

From our approach, we see that when $\langle \mathbf{u}|\mathbf{v}\rangle \ll 1$, a small error rate is enough to invalidate the key distribution. For example, when $\alpha=\pi/16$, corresponding to an overlap $\langle \mathbf{u}|\mathbf{v}\rangle=0.38$, the maximum error rate is only 4%. In order to obtain a robust scheme, Alice and Bob need to use a large overlap: an overlap of about 95%, corresponding to $\alpha=\pi/5$, gives a maximum tolerable error rate of 35%. The disadvantage of using such a large overlap is that it increases the fraction of inconclusive results, to about 95% for $\alpha=\pi/5$, so that most of the bits sent by Alice are useless. This would significantly reduce the speed of the key distribution. There is also another problem with a large overlap: in the interferometric scheme suggested by Bennett [5], where the two states $\mathbf{u}$ and $\mathbf{v}$ are two coherent states of electromagnetic field, the overlap is due to the so-called vacuum component of the states. A large overlap means using very low intensity pulses (a 95% overlap corresponds to an average of only $\frac{1}{40}$ photon per pulse). At such low intensities, the dark counts of the detectors may increase the error rate and swamp the signal. A practical scheme will therefore need to make a trade-off between a larger overlap to increase the robustness of the scheme and larger intensities to increase the speed and decrease the inherent error rate due to dark counts.

The criterion given by Eq. (41) is a well-defined limit

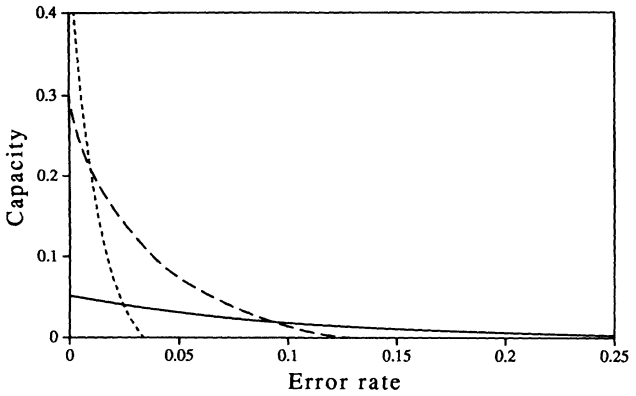

FIG. 4. This plot gives the secrecy capacity of the quantum channel, defined by Eq. (42) as the number of secret bits obtained per transmission, as a function of the error rate, for three different values of α: $\alpha=\pi/16$ (dotted line), $\pi/8$ (dashed line), and $\pi/5$ (solid line).

between failed and successful transmission. However, we see from Eq. (7) that when $Q=Q_{\max}$ the secrecy capacity of the channel is zero: to transmit one bit of secret information, Alice and Bob need to send an infinite number of bits over the channel. In order to quantify the quality of the channel, we shall therefore define the secrecy capacity C_s' of the *quantum* channel as the number of secret bits shared by Alice and Bob per bit sent over the channel. In our case, this gives

$$C_s'=(1-\sin 2\alpha)C_s\ , \tag{42}$$

where C_s is given by (7). This definition is a modification of the "classical" one, and takes into account the rate of inconclusive results obtained by Bob, namely Eq. (4). When Alice and Bob use states with a large overlap, most of the bits will be discarded during the first part of the protocol, as explained in Sec. II. The value of C_s' is plotted in Fig. 4 as a function of the error rate for three values of the overlap, and assuming that Eve chose the transluscent eavesdropping with entanglement (Sec. IV C) which provides here with the largest information. We see that even though a scheme with larger overlap is in principle more robust, it is not necessarily the most practical, as it will lead to a very low capacity. For example, if the error rate is about 5%, the scheme with $\alpha=\pi/8$ (with overlap 0.71) gives a larger capacity than the one with $\alpha=\pi/5$ (overlap 0.95).

We finally stress that in order to implement quantum-cryptographical systems in practice and to guarantee their security, one would have to specify explicitly the encoding procedure for the noisy channel, and to calculate $Q_{\max}$ with respect to all possible eavesdropping strategies. It is crucial to have just enough redundancy in the Shannon block coding to order to overcome the mismatch of the keys: if there is too much redundancy, Eve too will be able to decrypt the messages. Note that successful block encoding is effectively equivalent to preparing two exact replicas of the same key, which could also be done by standard error correction and privacy amplification protocols. If such protocols were followed, the relevant question would be how much information on the common key has leaded to Eve. We did not investigate this issue, which property belongs to classical cryptography and is beyond the scope of the present paper.

ACKNOWLEDGMENTS

We are grateful to C. H. Bennett and G. Brassard for posing the question which led to this work. We also thank C. Crépeau and U. Maurer for stimulating discussions which clarified many details of the paper. Part of this work was done during the "Quantum Computation Workshop" held at the Institute for Scientific Interchange (Turin, Italy) and sponsored by ELSAG-Bailey, Genoa. Work by A.P. was supported by the Gerard Swope Fund and the Fund for Encouragement of Research.

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[3] A. E. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[6] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).
[7] P. D. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. **29**, 634 (1993); **29**, 1291 (1993).
[8] A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).
[9] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, in *Advances in Cryptology—CRYPTO'91*, edited by E. Feigenbaum, Lecture Notes in Computer Science Vol. 576 (Springer-Verlag, Berlin, 1992), pp. 351–366.
[10] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, in the *34th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 1993).
[11] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[12] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[13] S. M. Barnett and S. J. D. Phoenix, Phys. Rev. A **48**, R5 (1993).
[14] S. J. D. Phoenix, Phys. Rev. A **48**, 96 (1993).
[15] R. B. Ash, *Information Theory* (Dover, New York, 1990); T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991); D. Welsh, *Codes and Cryptography* (Clarendon, Oxford, 1988).
[16] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[17] A. Peres, Phys. Lett. A **128**, 19 (1988).
[18] P. Busch, P. J. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement* (Springer, Berlin, 1991).
[19] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993), Chap. 9.

[20] A. D. Wyner, Bell Syst. Tech. J. **54**, 1355 (1975).
[21] I. Csiszár and J. Körner, IEEE Trans. Information Theory **24**, 339 (1978).
[22] U. Maurer, IEEE Trans. Information Theory **39**, 733 (1993).
[23] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer (unpublished).
[24] L. B. Levitin, in *Information Complexity and Control in Quantum Physics,* edited by A. Blaquière, S. Diner, and G. Lochak (Springer, Berlin, 1987), p. 15.