Entanglement enhances security in quantum communication

Rafał Demkowicz-Dobrzański,[1] Aditi Sen(De),[2,4] Ujjwal Sen,[3,4] and Maciej Lewenstein[4,5]
[1]*Institute of Physics, Nicolaus Copernicus University, ul. Grudziadzka 5, 87-100 Toruń, Poland*
[2]*School of Physical Sciences, Jawaharlal Nehru University, New Delhi 110067, India*
[3]*Department of Physics, Indian Institute of Technology Delhi, New Delhi 110016, India*
[4]*Institut de Ciències Fotòniques (ICFO), E-08860 Castelldefels, Barcelona, Spain*
[5]*Institució Catalana de Recerca i Estudis Avançats (ICREA), Lluis Companys 23, 08010 Barcelona, Spain*
(Received 27 May 2008; revised manuscript received 18 April 2009; published 13 July 2009)

Secret sharing is a protocol in which a "boss" wants to send a classical message secretly to two "subordinates," such that none of the subordinates is able to know the message alone, while they can find it if they cooperate. Quantum mechanics is known to allow for such a possibility. We analyze tolerable quantum bit error rates in such secret sharing protocols in the physically relevant case when the eavesdropping is local with respect to the two channels of information transfer from the boss to the two subordinates. We find that using entangled encoding states is advantageous to legitimate users of the protocol. We therefore find that entanglement is useful for secure quantum communication. We also find that bound entangled states with positive partial transpose are not useful as a local eavesdropping resource. Moreover, we provide a criterion for security in secret sharing—a parallel of the Csiszár-Körner criterion in single-receiver classical cryptography.

DOI: 10.1103/PhysRevA.80.012311 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Recently, the role of entanglement has been studied extensively in many areas of science, ranging from quantum information [1] to many-body physics [2]. Entanglement has been identified as the essential ingredient in quantum communication without a security aspect, e.g., in quantum dense coding and teleportation [3]. We find that entanglement is also useful in secure quantum communication.

The quantum communication task that we investigate is known as secret sharing [4] (cf. [5]). It is a communication scenario in which a sender Alice (A) wants to provide a (classical) message to two recipients (Bobs—B_1, B_2) in a way that each of the Bobs individually knows nothing about the message, but they can recover its content once they cooperate. For transmitting a binary message string $\{a_i\}$, Alice can then take a sequence of random bits $\{b_{1,i}\}$, send it to B_1, and at the same time send a sequence $\{b_{2,i}\}=\{a_i \oplus b_{1,i}\}$ to B_2, where $\oplus$ denotes addition modulo 2. Thus $a_i=b_{1,i}\oplus b_{2,i}$, assuring that the Bobs can recover the message if they cooperate, and yet none of them can learn anything on the message of Alice on his own, since the sequences $\{b_{1,i}\}$ and $\{b_{2,i}\}$ are random.

An important issue is of course security, i.e., distributing the message in a way that no third (actually fourth here) party learns about it. This can be achieved using quantum cryptography (e.g., by the Bennett-Brassard 1984 (BB84) scheme [6]). Alice simply has to establish secret random keys, independently, with both Bobs, and use them as one-time pads to securely send bits in the way required by secret sharing. We call this the BB84$^{\otimes 2}$ protocol. It has been argued [4] that a more natural way of using quantum states in secret sharing is to send entangled states to the Bobs and, as a result, avoid establishing random keys with each of the Bobs separately by combining the quantum and classical parts of secret sharing in a single protocol. We call the protocol in [4] as E4 (since it uses four entangled states).

In this paper, we consider security thresholds for both E4 and BB84$^{\otimes 2}$, i.e., the highest quantum bit error rates (R_{QBE}'s) below which one-way distillation of secret key is possible. There are four main results obtained in the paper. *First*, we provide a criterion for security of secret sharing, for which the one-way classical distillation of secret key is possible between the sender and the receivers: the parallel of the Csiszár-Körner criterion in (single-receiver, classical) cryptography [7]. *Second*, we find the *optimal* quantum eavesdropping attacks, on both E4 and BB84$^{\otimes 2}$, that are *local*. An attack which acts by local operations and classical communication (LOCC) on the particles sent through the two channels ($A\rightarrow B_1$ and $A\rightarrow B_2$) is physically the appropriate one in this *distributed*-receiver case. We show that the threshold R_{QBE} for E4 is about 18.2% higher than that of BB84$^{\otimes 2}$ for individual eavesdropping attacks without quantum memory. In cryptography with a single receiver, entanglement-based protocols are known to be equivalent, in principle, to protocols that employ quantum channels but do not require entanglement [6–9]. We show that it is advantageous to use entanglement for a cryptographic task with *two* receivers. Entanglement is therefore found to be strictly more useful in a cryptographic scenario. Our results, apart from answering a basic question about the role of entanglement in communication tasks, have the potential of usefulness in the commercial use of quantum cryptographic systems. *Third*, we show that bound entangled states with positive partial transpose are not useful to the eavesdroppers in this LOCC eavesdropping scenario on secret sharing. *Last*, we provide an interesting general method for dealing with local eavesdropping.

This paper is arranged as follows. In Sec. II, we explicitly state the secret sharing protocols using product encoding states and entangled ones. In Sec. III, we give the error-correction and privacy amplification schemes that are required in a scenario where there is a single sender but there are two receivers. Actually, the schemes carry over to the case of an arbitrary number of receivers. It turns out that there are significant differences in the error-correction

 ©2009 The American Physical Society

scheme required in this distributed-receiver scenario as compared to the case of a single receiver. Section IV sets the stage (and notations) for finding the eavesdropping strategies on the secret sharing schemes considered. In particular, in Sec. IV B, we find the Csiszár-Körner criterion for the distributed-receiver scenario. Section IV C formulates the problem of finding the optimal R_{QBE}, which is made more focused in Sec. V. The stage is finally ready for comparing the use of product states with that of entangled states for encoding in a secret sharing protocol (Sec. VI). The optimal LOCC eavesdropping attacks appear in Sec. VI A. The important issue of comparing the R_{QBE} thresholds for a noisy transfer channel is taken up in Sec. VII. A summary is given in Sec. VIII.

II. PROTOCOLS

A secret sharing protocol can be characterized by

$$\{|\psi^{j,0}\rangle,|\psi^{j,1}\rangle,\sigma_1^{j,k}\otimes\sigma_2^{j,k}\}, \tag{1}$$

where j labels the different encoding "bases" used, $|\psi^{j,a}\rangle$ are two-qubit states sent by Alice to the Bobs if she uses basis j and wants to communicate the logical value a, while $\sigma_1^{j,k}\otimes\sigma_2^{j,k}$ is a set of observables compatible with basis j (so that if the corresponding measurement is performed by the Bobs, it allows them to recover a proper logical bit of Alice). In practice, $B_1(B_2)$ randomly measures the observables $\sigma_1^{j,k}(\sigma_2^{j,k})$ (in the protocols that we consider, they will be one of the three Pauli matrices) on states received from Alice in each round. After the transmission is completed, the Bobs announce the observables they have used in each round to Alice, who, judging on whether this combination of observables is present in $\sigma_1^{j,k}\otimes\sigma_2^{j,k}$ for the particular j she had used in that round, tells the Bobs whether to keep or reject their measured results for that round—the sifting phase.

The BB84$^{\otimes 2}$ protocol is defined as

j	$\|\psi^{j,0}\rangle$	$\|\psi^{j,1}\rangle$	$\sigma_1^{j,k}\otimes\sigma_2^{j,k}$
1	$\|x_+\rangle\|x_+\rangle$, $\|x_-\rangle\|x_-\rangle$	$\|x_+\rangle\|x_-\rangle$, $\|x_-\rangle\|x_+\rangle$	$\sigma_x\otimes\sigma_x$
2	$\|x_+\rangle\|y_+\rangle$, $\|x_-\rangle\|y_-\rangle$	$\|x_+\rangle\|y_-\rangle$, $\|x_-\rangle\|y_+\rangle$	$\sigma_x\otimes\sigma_y$
3	$\|y_+\rangle\|x_+\rangle$, $\|y_-\rangle\|x_-\rangle$	$\|y_+\rangle\|x_-\rangle$, $\|y_-\rangle\|x_+\rangle$	$\sigma_y\otimes\sigma_x$
4	$\|y_+\rangle\|y_+\rangle$, $\|y_-\rangle\|y_-\rangle$	$\|y_+\rangle\|y_-\rangle$, $\|y_-\rangle\|y_+\rangle$	$\sigma_y\otimes\sigma_y$

where $|x_\pm\rangle(|y_\pm\rangle)$ are eigenstates of the Pauli $\sigma_x(\sigma_y)$ matrix. The fact that there are two states corresponding to a given $|\psi^{j,a}\rangle$ simply means that each of them is sent randomly with probability 1/2.

The E4 protocol [4] (see also [10]), on the other hand, is defined as

j	$\|\psi^{j,0}\rangle$	$\|\psi^{j,1}\rangle$	$\sigma_1^{j,k}\otimes\sigma_2^{j,k}$
1	$\|\psi_+\rangle$	$\|\psi_-\rangle$	$\sigma_x\otimes\sigma_x$, $-\sigma_y\otimes\sigma_y$
2	$\|\psi_+^j\rangle$	$\|\psi_-^j\rangle$	$\sigma_x\otimes\sigma_y$, $\sigma_y\otimes\sigma_x$,

where

$$|\psi_\pm\rangle=(|00\rangle\pm|11\rangle)/\sqrt{2},|\psi_\pm^j\rangle=(|00\rangle\pm i|11\rangle)/\sqrt{2}, \tag{2}$$

and $|0\rangle$, $|1\rangle$ are eigenstates of the Pauli σ_z operator.

After the sifting phase, let the bits of Alice and the Bobs, obtained in a given set of rounds, be described by the probability distribution $p_{AB_1B_2}(a,b_1,b_2)$, so that

$$R_{\mathrm{QBE}}=\sum_{a,b_1,b_2}p_{AB_1B_2}(a,b_1,b_2)[1-\delta_{a,b_1\oplus b_2}]. \tag{3}$$

In order to decide which of these protocols is better suited for secret sharing purposes, we need to find out which one tolerates a higher R_{QBE}, i.e., allows for a distillation of secure secret sharing key in the presence of a higher level of disturbance.

III. ERROR CORRECTION AND PRIVACY AMPLIFICATION

A. Error correction

Knowing R_{QBE}, a one-way error correction is performed to correct all errors with arbitrarily high probability. In single-receiver cryptography, error correction can be performed from the sender to the receiver, or vice versa.

In secret sharing, there are two *separated* receivers, who cannot communicate (they could in principle not know about each other), and each of them individually has completely random bits. So there is no way for Alice to perform one-way error correction to Bobs—whatever she sends to each of them individually, it will not be enough for them to correct errors, unless she sends the total information, which is of course not the solution we are after.

The only remaining option is that each Bob sends some information to Alice, judging on which she is able to correct her bits $\{a_i\}$ in a way that for every i: $a_i=b_{1,i}\oplus b_{2,i}$. Fortunately, this is indeed possible by using random coding techniques [11].

Let each of the three parties have n bits after the sifting phase. Consider a random coding function

$$f:\{0,1\}^n\rightarrow\{0,1\}^m, \tag{4}$$

known to all three parties (and the rest of the world), where $m\leq n$ will be chosen later. This function assigns a random m-bit codeword to each of the 2^n possible n-bit strings.

Error correction goes as follows: B_1 calculates his m-bit codeword $f(\{b_{1,i}\})$, while B_2 calculates his m-bit codeword $f(\{b_{2,i}\})$. Then they send their respective m-bit codewords to Alice. Subsequent to this, Alice looks for all n-bit sequences $\{b'_{1,i}\}$, $\{b'_{2,i}\}$ such that

$$f(\{b'_{1,i}\})=f(\{b_{1,i}\}),f(\{b'_{2,i}\})=f(\{b_{2,i}\}), \tag{5}$$

and chooses a pair $\{b'_{1,i}\}$, $\{b'_{2,i}\}$, for which the Hamming distance

$$\mathrm{dist}(\{a_i\},\{b'_{2,i}\oplus b'_{2,i}\}) \tag{6}$$

is minimal. It can be shown that for $n\rightarrow\infty$, this strategy is successful with arbitrarily high probability, provided that

$$m\geq n[1+h(R_{\mathrm{QBE}})]/2, \tag{7}$$

where

$$h(p) = -p \log_2 p - (1-p)\log_2(1-p) \tag{8}$$

is the binary entropy function, with $p \in [0,1]$.

This result is quite intuitive, since in a standard bipartite error correction, the length of a codeword has to fulfill

$$m \geq nh(R_{\mathrm{QBE}}). \tag{9}$$

In secret sharing however, the two Bobs together have to provide Alice with

$$n + nh(R_{\mathrm{QBE}}) \tag{10}$$

bits. These additional n bits are needed, since a sequence of one of Bobs taken separately is completely random for Alice. As a result each of the Bobs has to send a code of length that satisfies Eq. (7).

B. Privacy amplification

After the error-correction stage is completed, Alice and the Bobs need to perform privacy amplification in order to obtain a possibly shortened but a completely secure key, on which an eavesdropper has no information. This presents no additional difficulty in secret sharing, as compared to bipartite cryptography, since its performance, in principle, requires no additional communication between Alice and the Bobs. It is enough that all parties apply the same hashing function [12] for shortening the key, and if there were no errors, in the sense that $a_i = b_{1,i} \oplus b_{2,i}$, for all i, then there will be no errors in the shortened key. The only thing left to be determined before the privacy amplification is performed is the amount of information that an eavesdropper possesses by judging on the detected R_{QBE}.

IV. LOCC ATTACKS

In our scenario of distributed receivers, the appropriate class of operations that the eavesdropper will be able to implement are LOCC with respect to the partition of the encoding states between B_1 and B_2. It may be noted here that without the LOCC constraint, the security analyses of the E4 secret sharing protocol and the single-sender single-receiver BB84 cryptographic protocol are isomorphic, as both protocols make use of four nonorthogonal states with the same mutual scalar products.

In our security analyses, the eavesdropper (i) will perform only individual attacks and (ii) will not be allowed any kind of quantum memory. Restriction (i) means that an eavesdropper can interact, in a given round, with only the quantum state sent by Alice to Bobs in that round and is based on limitations of currently available technology. The justification of (ii) is also based on current technology limitations—no long lasting quantum memory has been developed so far.

A. Single-round probability distribution

To analyze eavesdropping attacks, consider the state $|\psi^{j,a}\rangle$ being sent from Alice to the Bobs. Collaborating eavesdroppers E_1 and E_2, acting on channels connecting Alice with B_1 and Alice with B_2, respectively, can perform an arbitrary quantum mechanically allowed LOCC operation $\mathcal{E}$ [trace-preserving (TP) completely positive (CP) LOCC map] to create a state

$$\rho^{j,a}_{B_1B_2E_1E_2} = \mathcal{E}(|\psi^{j,a}\rangle\langle\psi^{j,a}|). \tag{11}$$

The operation is LOCC with respect to the partition $B_1,E_1|B_2,E_2$. Subsequently, E_1 and E_2 perform an LOCC measurement on their subsystems in order to obtain information about the bit shared by Alice with the Bobs, while sending possibly perturbed subsystems B_1 and B_2 to their legitimate recipients. Without loosing generality, we can restrict this measurement to have only two possible outcomes (0 or 1), since only the value of a transmitted bit is of interest to the eavesdroppers. Hence we model the measurement by a two-element positive operator valued measurement (POVM) $\{\Pi_{E_1E_2}(e)\}$, $e=0,1$. Obviously

$$\Pi_{E_1E_2}(e) \geq 0, \quad \Pi_{E_1E_2}(0) + \Pi_{E_1E_2}(1) = \mathbb{1}_{E_1E_2}, \tag{12}$$

but we additionally require that the measurements are LOCC based.

After Alice and the Bobs have performed a sifting procedure and kept measurement results which were obtained in compatible bases, we can write the probability distribution $p_{ABE}(a,b,e)$, describing the distribution of bit values, a, of Alice, the logical bit, $b=b_1 \oplus b_2$, of the Bobs, and the bit e obtained by an eavesdropper couple in the attack, as

$$p_{ABE}(a,b,e) = \sum_j p(j,a)\mathrm{Tr}[\mathcal{E}(|\psi^{j,a}\rangle\langle\psi^{j,a}|)\Pi_{B_1B_2}(j,b) \otimes \Pi_{E_1E_2}(e)], \tag{13}$$

where $p(j,a)$ is the probability that Alice sends the state $|\psi^{j,a}\rangle$ in a given round, whereas $\{\Pi_{B_1B_2}(j,b)\}$ is a POVM corresponding to the measurement by the Bobs in the basis j (compatible with the state sent by Alice), where the sum of their individual measured values, modulo 2, equals b: $b = b_1 \oplus b_2$.

The POVMs used by the Bobs are already set by the corresponding secret sharing protocol used by Alice and the Bobs. Therefore the positivity and normalization conditions

$$\Pi_{B_1B_2}(j,b) \geq 0, \quad \forall\, j, \quad b = 0,1,$$

$$\Pi_{B_1B_2}(j,0) + \Pi_{B_1B_2}(j,1) = \mathbb{1}_{B_1B_2}, \quad \forall\, j, \tag{14}$$

are automatically satisfied. Moreover, the form of the POVMs chosen in the protocols also guarantees that they can be implemented by LOCC.

We assume the convention that if one of the Bobs (locally) performs a σ_i measurement, characterized by a Pauli matrix, then he ascribes the bit value 0 or 1 when he projects on an eigenvector with eigenvalue -1 or 1, respectively. Notice that if in the tables defining the secret sharing protocols in Sec. II, there is an observable $-\sigma_y \otimes \sigma_y$, it simply means

that one of the Bobs measures an observable $-\sigma_y$, and hence he will associate the inverted bit values to measurements which result in projection on a given eigenstate. For example, in the BB84$^{\otimes 2}$ protocol, for $j=1$ and $a=0$, we will have

$$\Pi_{B_1B_2}(1,0) = 1/2(|x_+\rangle\langle x_+| \otimes |x_+\rangle\langle x_+| + |x_-\rangle\langle x_-| \otimes |x_-\rangle\langle x_-|), \tag{15}$$

while in the E4 protocol for $j=1$ and $a=0$ (notice that we have two combinations of observables that are compatible with the state transmitted by Alice), we have

$$\Pi_{B_1B_2}(1,0) = 1/4(|x_+\rangle\langle x_+| \otimes |x_+\rangle\langle x_+| + |x_-\rangle\langle x_-| \otimes |x_-\rangle\langle x_-| + |y_+\rangle\langle y_+| \otimes |y_-\rangle\langle y_-| + |y_-\rangle\langle y_-| \otimes |y_+\rangle\langle y_+|). \tag{16}$$

We introduce non-TP CP operations $\mathcal{E}_0$, $\mathcal{E}_1: \mathcal{H}^{\text{in}}_{B_1} \otimes \mathcal{H}^{\text{in}}_{B_2} \mapsto \mathcal{H}^{\text{out}}_{B_1} \otimes \mathcal{H}^{\text{out}}_{B_2}$, acting on the input and output Hilbert spaces of the Bobs, and defined as

$$\mathcal{E}_e(\varrho_{B_1B_2}) = \text{Tr}_{E_1E_2}[\mathcal{E}(\varrho_{B_1B_2})\Pi_{E_1E_2}(e)], \tag{17}$$

where $\mathcal{E}_e$ represents the disturbance experienced by a state transmitted to the Bobs once the eavesdroppers have obtained the value e. Note that even though each $\mathcal{E}_e$ is not TP, $\mathcal{E}_0+\mathcal{E}_1$ is—the latter corresponds to a situation when one averages over the results of the measurement of the eavesdroppers. Then,

$$p_{ABE}(a,b,e) = \sum_j p(j,a)\text{Tr}[\mathcal{E}_e(|\psi^{j,a}\rangle\langle\psi^{j,a}|)\Pi_{B_1B_2}(j,b)]. \tag{18}$$

It is now clear that the eavesdropping strategy is completely defined by specifying the two operations $\mathcal{E}_0$ and $\mathcal{E}_1$ and, for a given protocol, yields a joint probability distribution $p_{ABE}(a,b,e)$.

B. Security criterion

In single-receiver cryptography, if $p_{ABE}(a,b,e)$ describes the single-round bit values (a of the sender Alice, b of the receiver Bob, and e of an eavesdropper), after the eavesdropper attack and after the sifting stage is completed, the maximal one-way secret-key distillation rate K is given by the Csiszár-Körner criterion [7],

$$K = I(A:B) - \min\{I(A:E), I(B:E)\}, \tag{19}$$

where $I(:)$ is the mutual information between the corresponding parties. Provided that $K>0$, the one-way distillation of a secret key is possible.

The result of a single round of a secret sharing protocol is the probability distribution $p_{ABE}(a,b,e)$, given by Eq. (18), describing the probabilities of bit values (a of Alice, $b=b_1 \oplus b_2$ of the Bobs, and e of the eavesdroppers). As we have discussed in Sec. III, the error-correction stage in secret sharing can only be performed from the Bobs (receivers) to Alice (sender). Therefore, using an analogous reasoning as in the original Csiszár-Körner criterion, one arrives at a formula for the maximal one-way secret-key distillation rate given by

$$K = I(A:B) - I(B:E). \tag{20}$$

In other words, the eavesdropper couple does not at all have to care about their mutual information $I(A:E)$ with Alice but only concentrate on obtaining as much information on the bit b obtained by the Bobs by causing the smallest possible disturbance. Provided that for a given R_{QBE}, the optimal eavesdropping attack, i.e., the one minimizing K, yields $K>0$, a secure "secret sharing key" can be distilled.

C. R_{QBE} threshold

The R_{QBE} threshold for a cryptographic protocol is the level of errors above which it is no longer possible for the legitimate parties to distil a secure key. Therefore, to calculate the R_{QBE} threshold for secret sharing protocols, one should look for the highest value of R_{QBE}, for which it is still possible to find eavesdropping LOCC operations $\mathcal{E}_e$, so that the resulting probability distribution p_{ABE} enjoys the property $I(A:B)=I(B:E)$.

Assuming a natural symmetry, namely, that Alice sends different logical values a with the same frequency, and the eavesdroppers perform a symmetric attack—i.e., does not favor any particular bit value—the reduced probability distributions p_{AB} and p_{BE} depend only on one free parameter. In the case of p_{AB}, this is simply the R_{QBE}. Consequently, the equality $I(A:B)=I(B:E)$ is equivalent to the equality of the reduced probability distributions,

$$p_{AB} = p_{BE} \tag{21}$$

(up to a freedom of inverting bits of some of the parties). This allows us to reformulate the task of finding the R_{QBE} threshold to the following problem: find the maximal R_{QBE} for which an eavesdropper can perform the LOCC attack, resulting in $p_{AB}=p_{BE}$.

V. FORMULATING THE PROBLEM AS A SEMIDEFINITE PROGRAM

Let us for a moment forget about the LOCC condition imposed on the attacks of the eavesdroppers. The problem of finding the R_{QBE} threshold is then a semidefinite program. To see this, denote

$$\mathcal{H}^{\text{out}} = \mathcal{H}^{\text{out}}_{B_1} \otimes \mathcal{H}^{\text{out}}_{B_2}, \quad \mathcal{H}^{\text{in}} = \mathcal{H}^{\text{in}}_{B_1} \otimes \mathcal{H}^{\text{in}}_{B_2} \tag{22}$$

and recall that by using the Jamiołkowski isomorphism [13], we can associate the completely positive maps $\mathcal{E}_e$ with the positive semidefinite operators $P_{\mathcal{E}_e} \in \mathcal{L}(\mathcal{H}^{\text{out}} \otimes \mathcal{H}^{\text{in}})$ in the following manner:

$$P_{\mathcal{E}_e} = \mathcal{E}_e \otimes \mathcal{I}(|\Psi^+\rangle\langle\Psi^+|), \tag{23}$$

where $|\Psi^+\rangle = \Sigma_{i=1}^{\dim\mathcal{H}^{\text{in}}} |i\rangle \otimes |i\rangle$ is an unnormalized maximally entangled state in the space $\mathcal{H}^{\text{in}} \otimes \mathcal{H}^{\text{in}}$ and $\mathcal{I}$ is the identity operation on the second space $\mathcal{H}^{\text{in}}$. Hence our problem variables are entries of two 16×16 matrices, which are required to be positive semidefinite.

The trace-preservation condition of $\mathcal{E}_0+\mathcal{E}_1$ translates to a condition on positive operators,

$$\mathrm{Tr}_{\mathcal{H}^{\mathrm{out}}}(P_{\mathcal{E}_0}+P_{\mathcal{E}_1})=\mathbb{1}_{\mathcal{H}^{\mathrm{in}}}, \tag{24}$$

where the partial trace is performed over the $\mathcal{H}_{B_1}^{\mathrm{out}}\otimes\mathcal{H}_{B_2}^{\mathrm{out}}$ space, while the identity on the right-hand side is acting on $\mathcal{H}_{B_1}^{\mathrm{in}}\otimes\mathcal{H}_{B_2}^{\mathrm{in}}$. This condition is obviously a linear constraint in the matrix elements of $P_{\mathcal{E}_e}$.

Similarly, p_{ABE} is also linear, and hence the "insecurity condition" $p_{AB}=p_{BE}$ is linear as well. Finally, the R_{QBE}, which we want to maximize, is linear.

In order to deal with an LOCC constraint, we first impose the weaker "PPT constraint," positivity after partial transposition of the $P_{\mathcal{E}_e}$ operators—we transpose the subsystem $\mathcal{H}_{B_2}^{\mathrm{out}}\otimes\mathcal{H}_{B_2}^{\mathrm{in}}$. This is a strictly necessary condition for LOCC [14,15], and so in principle this assumption could lead to an optimal attack that is nonlocal (i.e., non-LOCC quantum attack). However, by explicit construction, we will show that the optimal PPT maps we obtain in the end are actually LOCC—this of course implies that these are the optimal LOCC attacks.

VI. ENTANGLED VERSUS PRODUCT ENCODING

We present here the solutions for maximal tolerable R_{QBE} for $\mathrm{BB84}^{\otimes 2}$ and E4 protocols found by solving the semidefinite programs described in Sec. V by using the SEDUMI package. We denote the threshold R_{QBE}'s of the $\mathrm{BB84}^{\otimes 2}$ and E4 secret sharing protocols as $R_{\mathrm{QBE}}(\mathrm{BB84}^{\otimes 2})$ and $R_{\mathrm{QBE}}(\mathrm{E4})$, respectively. Although solving the semidefinite program provided us only with numerical solutions, we were able to recognize their simple analytical form, which agrees perfectly with numerical results. Hence, all the results we present will have an analytical form.

For the $\mathrm{BB84}^{\otimes 2}$ protocol, we have found that

$$R_{\mathrm{QBE}}(\mathrm{BB84}^{\otimes 2})=5/18\approx 0.2778. \tag{25}$$

The optimal operations $\mathcal{E}_e^{\mathrm{BB84}^{\otimes 2}}$ (in the computational basis) are as follows. We have

$$P_{\mathcal{E}_0^{\mathrm{BB84}^{\otimes 2}}}=\begin{bmatrix}
\frac{2}{9} & \cdot & \cdot & \frac{i}{9} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -\frac{i}{9} & \cdot & \cdot & \frac{2}{9}\\
\cdot & \frac{1}{9} & \frac{1}{9} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -\frac{i}{9} & -\frac{i}{9} & \cdot\\
\cdot & \frac{1}{9} & \frac{1}{9} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -\frac{i}{9} & -\frac{i}{9} & \cdot\\
-\frac{i}{9} & \cdot & \cdot & \frac{1}{18} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -\frac{1}{18} & \cdot & \cdot & -\frac{i}{9}\\
\cdot & \cdot & \cdot & \cdot & \frac{1}{9} & \cdot & \cdot & \frac{i}{9} & \frac{1}{9} & \cdot & \cdot & \frac{i}{9} & \cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot & \cdot & \frac{2}{9} & \frac{1}{9} & \cdot & \cdot & \frac{1}{9} & \frac{2}{9} & \cdot & \cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot & \cdot & \frac{1}{9} & \frac{1}{18} & \cdot & \cdot & \frac{1}{18} & \frac{1}{9} & \cdot & \cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot & -\frac{i}{9} & \cdot & \cdot & \frac{1}{9} & -\frac{i}{9} & \cdot & \cdot & \frac{1}{9} & \cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot & \frac{1}{9} & \cdot & \cdot & \frac{i}{9} & \frac{1}{9} & \cdot & \cdot & \frac{i}{9} & \cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot & \cdot & \frac{1}{9} & \frac{1}{18} & \cdot & \cdot & \frac{1}{18} & \frac{2}{9} & \cdot & \cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot & \cdot & \frac{2}{9} & \frac{1}{9} & \cdot & \cdot & \frac{1}{9} & \frac{2}{9} & \cdot & \cdot & \cdot & \cdot & \cdot\\
\cdot & \cdot & \cdot & \cdot & -\frac{i}{9} & \cdot & \cdot & \frac{1}{9} & -\frac{i}{9} & \cdot & \cdot & \frac{1}{9} & \cdot & \cdot & \cdot & \cdot\\
\frac{i}{9} & \cdot & \cdot & -\frac{1}{18} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \frac{1}{18} & \cdot & \cdot & \frac{i}{9}\\
\cdot & \frac{i}{9} & \frac{i}{9} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \frac{1}{9} & \frac{1}{9} & \cdot\\
\cdot & \frac{i}{9} & \frac{i}{9} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \frac{1}{9} & \frac{1}{9} & \cdot\\
\frac{2}{9} & \cdot & \cdot & \frac{i}{9} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -\frac{i}{9} & \cdot & \cdot & \frac{2}{9}
\end{bmatrix}, \tag{26}$$

where the dots denote zeros. The optimal $P_{\mathcal{E}_1^{\mathrm{BB84}^{\otimes 2}}}$ has the same entries on the diagonal, and the antidiagonal, while the remaining ones are multiplied by -1. Below, these optimal PPT maps will be proven to be LOCC.

Moving now to the E4 protocol, we get

$$R_{\mathrm{QBE}}(\mathrm{E4})=2(\sqrt{2}-5/4)\approx 0.3284. \tag{27}$$

The corresponding optimal attack operations, in this case, are as follows. We have

$$P_{\mathcal{E}_0^{\mathrm{E4}}} = \begin{bmatrix}
a & \cdot & \cdot & c & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & c^* & \cdot & \cdot & a \\
\cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
c^* & \cdot & \cdot & d & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & f^* & \cdot & \cdot & c^* \\
\cdot & \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & d & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & d & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot \\
c & \cdot & \cdot & f & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & d & \cdot & \cdot & c \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot \\
a & \cdot & \cdot & c & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & c^* & \cdot & \cdot & a
\end{bmatrix}, \tag{28}$$

where $a=3-2\sqrt{2}$, $b=a/\sqrt{2}$, $c=b\exp(i\pi/4)$, $d=a/2$, and $f=id$. The optimal $P_{\mathcal{E}_1^{\mathrm{E4}}}$ is the same as $P_{\mathcal{E}_0^{\mathrm{E4}}}$, but with c replaced by $-c$. Again these optimal PPT maps will be proven below to be LOCC.

Interestingly

$$R_{\mathrm{QBE}}(\mathrm{E4}) > R_{\mathrm{QBE}}(\mathrm{BB84}^{\otimes 2}), \tag{29}$$

which indicates that indeed the protocol using entangled states is more secure (cf. [16]).

A. Explicit LOCC forms of the optimal attacks

Usually the only way of showing that a given operation is LOCC is to give its explicit LOCC Kraus decomposition. Let us first analyze the optimal attack on the $\mathrm{BB84}^{\otimes 2}$ protocol. First of all, the operations $\mathcal{E}_e^{\mathrm{BB84}^{\otimes 2}}$ are separable, as they can be written in the form

$$\mathcal{E}_e^{\mathrm{BB84}^{\otimes 2}}(\rho) = \sum_{\phi_1,\phi_2\in\{0,\pi\}} K_{e,1}^{\phi_1,\phi_2}\otimes K_{e,2}^{\phi_1,\phi_2}\rho K_{e,1}^{\phi_1,\phi_2\dagger}\otimes K_{e,2}^{\phi_1,\phi_2\dagger}, \tag{30}$$

where the local Kraus operators $K_{e,1}^{\phi_1,\phi_2}$ and $K_{e,2}^{\phi_1,\phi_2}$ read, respectively, as

$$\frac{1}{\sqrt{6}}\begin{bmatrix} (-1)^e\sqrt{2} & \exp[i(\phi_1-\pi/4\ ] \\ \exp[i(\phi_2+\pi/4)] & (-1)^e\sqrt{2}\exp[i(\phi_1+\phi_2)] \end{bmatrix} \tag{31}$$

and

$$\frac{1}{2\sqrt{3}}\begin{bmatrix} \sqrt{2} & \exp[-i(\phi_1+\pi/4)] \\ \exp[-i(\phi_2-\pi/4)] & \sqrt{2}\exp[i(\phi_1+\phi_2)] \end{bmatrix}. \tag{32}$$

Notice that $K_{e,2}$ does not depend on the index e (equivalently we could instead choose $K_{e,1}$ not to depend on e), we will denote it simply as K_2. The full operation

$$\mathcal{E}^{\mathrm{BB84}^{\otimes 2}} = \mathcal{E}_0^{\mathrm{BB84}^{\otimes 2}} + \mathcal{E}_1^{\mathrm{BB84}^{\otimes 2}} \tag{33}$$

reads

$$\mathcal{E}^{\mathrm{BB84}^{\otimes 2}}(\rho) = \sum_{\phi_1,\phi_2\in\{0,\pi\}} \mathbb{1}\otimes K_2^{\phi_1,\phi_2} \times\left(\sum_{e=0}^{1} K_{e,1}^{\phi_1,\phi_2}\otimes\mathbb{1}\rho K_{e,1}^{\phi_1,\phi_2\dagger}\otimes\mathbb{1}\right)\mathbb{1}\otimes K_2^{\phi_1,\phi_2\dagger}. \tag{34}$$

The above operation is indeed LOCC since it can be realized as follows. First an operation given by four Kraus operators $K_2^{\phi_1,\phi_2}$ is performed on the second subsystem, and the measurement result (ϕ_1,ϕ_2) is transmitted to the first subsystem. For given values (ϕ_1,ϕ_2) received by the first subsystem, an operation using two Kraus operators $K_{0,1}^{\phi_1,\phi_2}$, $K_{1,1}^{\phi_1,\phi_2}$ is performed on the first subsystem. This is a legitimate deterministic LOCC operation, since

$$\sum_{\phi_1,\phi_2\in\{0,\pi\}} K_2^{\phi_1,\phi_2\dagger}K_2^{\phi_1,\phi_2} = \mathbb{1}, \tag{35}$$

and for every (ϕ_1,ϕ_2),

$$\sum_{e=0}^{1} K_{e,1}^{\phi_1,\phi_2\dagger}K_{e,1}^{\phi_1,\phi_2} = \mathbb{1}. \tag{36}$$

Additionally, it requires only one-way communication. Summing up, $\mathcal{E}_e^{\mathrm{BB84}^{\otimes 2}}$ are separable trace-decreasing operations such that when added together they form a trace-preserving LOCC operation $\mathcal{E}^{\mathrm{BB84}^{\otimes 2}}$; hence they can be realized via LOCC.

In a similar way we can show that $\mathcal{E}_e^{\mathrm{E4}}$ is an LOCC attack. Separable Kraus decompositions of $\mathcal{E}_e^{\mathrm{E4}}$ read

$$\mathcal{E}_e^{\mathrm{E4}^{\otimes 2}}(\rho) = \sum K_{e,1}^{\phi_1,\phi_2,\phi_3}\otimes K_2^{\phi_1,\phi_2,\phi_3}\rho K_{e,1}^{\phi_1,\phi_2,\phi_3\dagger}\otimes K_2^{\phi_1,\phi_2,\phi_3\dagger}, \tag{37}$$

with the summation being $\phi_1,\phi_2,\phi_3\in\{0,2\pi/3,4\pi/3\}$, and where $K_{e,1}^{\phi_1,\phi_2,\phi_3}$ and $K_2^{\phi_1,\phi_2}$ read, respectively,

$$\sqrt{1+\frac{1}{\sqrt{2}}}\begin{bmatrix} (-1)^e 2^{1/4} & \exp(i\phi_1) \\ \exp(i\phi_2) & (-1)^e 2^{1/4}\exp(i\phi_3) \end{bmatrix} \tag{38}$$

and

$$\frac{1}{\sqrt{27(1+\sqrt{2})}}\begin{bmatrix} 2^{1/4} & \exp[-i(\phi_1+\pi/4)] \\ \exp[-i(\phi_2-\pi/4)] & 2^{1/4}\exp(-i\phi_3) \end{bmatrix}. \tag{39}$$

Again we can write the full operation

$$\mathcal{E}^{\mathrm{E4}} = \mathcal{E}_0^{\mathrm{E4}} + \mathcal{E}_1^{\mathrm{E4}} \tag{40}$$

in a form that is manifestly LOCC,

$$\mathcal{E}^{\mathrm{E4}}(\rho) = \sum_{\phi_1,\phi_2,\phi_3 \in \{0,2\pi/3,4\pi/3\}} \mathbb{1} \otimes K_2^{\phi_1,\phi_2,\phi_3} \times \left(\sum_{e=0}^{1} K_{e,1}^{\phi_1,\phi_2,\phi_3} \otimes \mathbb{1} \rho K_{e,1}^{\phi_1,\phi_2,\phi_3 \dagger} \otimes \mathbb{1} \right) \mathbb{1} \otimes K_2^{\phi_1,\phi_2,\phi_3 \dagger}, \tag{41}$$

since it can be realized by performing operations on the second subsystem by using the 27 Kraus operators $K_2^{\phi_1,\phi_2,\phi_3\dagger}$, communicating the measurement result (ϕ_1,ϕ_2,ϕ_3) to the first subsystem, on which an appropriate operation using two Kraus operators $K_{e,1}^{\phi_1,\phi_2,\phi_3}$ $(e=0,1)$ is performed. The LOCC thus performed is again deterministic, as

$$\sum_{\phi_1,\phi_2,\phi_3 \in \{0,2\pi/3,4\pi/3\}} K_2^{\phi_1,\phi_2,\phi_3\dagger} K_2^{\phi_1,\phi_2,\phi_3} = \mathbb{1}, \tag{42}$$

and for every (ϕ_1,ϕ_2,ϕ_3),

$$\sum_{e=0}^{1} K_{e,1}^{\phi_1,\phi_2,\phi_3\dagger} K_{e,1}^{\phi_1,\phi_2,\phi_3} = \mathbb{1}. \tag{43}$$

B. Bound entangled states with positive partial transpose are not useful for eavesdropping

Consider a situation in which the eavesdroppers E_1 and E_2 are allowed to possess an arbitrary amount of bound entangled states with positive partial transpose [14]. This, in principle, is giving more power to the eavesdropping process, as such states cannot be prepared by LOCC.

However, the eavesdroppers will still be restricted to performing only operations that preserve the positivity of partial transpose. Therefore, the results of the preceding subsection show that for both the protocols considered, the optimal R_{QBE} will still be reached by an LOCC operation.

C. Optimal secret-key rates below thresholds

Using a modified semidefinite program, i.e., imposing a given R_{QBE} [which in our case is equivalent to fixing $I(A:B)$], and trying to maximize the mutual information $I(B:E)$ [which is possible using semidefinite programming, even though $I(B:E)$ is not linear in the problem variables, since a maximization of $I(B:E)$ is equivalent to minimizing the error probability between the bits of E and B, which is a linear quantity], we obtain the maximal secret-key rate as $K=I(A:B)-I(B:E)$. In Fig. 1 we show the maximum achievable secret-key rates for the two protocols as a function of measured R_{QBE}. It is clear that the E4 protocol is better not only because of its higher R_{QBE} threshold but also because of its higher key rate for all R_{QBE}.

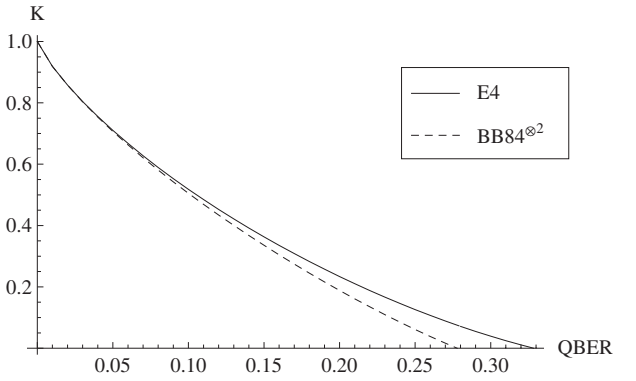

FIG. 1. Maximal achievable secret-key rate (K, measured in bits) for secret sharing protocols based on the use of entangled states (E4—solid line) and product states (BB84$^{\otimes 2}$—dashed line), under the assumption of LOCC individual attacks, is plotted against R_{QBE} (again measured in bits). R_{QBE} thresholds above which no secret key can be generated corresponding, respectively, to $R_{\mathrm{QBE}}(\mathrm{E4})=2(\sqrt{2}-5/4)\approx 0.3284$ and $R_{\mathrm{QBE}}(\mathrm{BB84}^{\otimes 2})=5/18 \approx 0.2778$.

VII. TYPICAL NOISE

Judging the usefulness of cryptographic protocols by comparing their R_{QBE} thresholds may not *a priori* be sensible from an experimental point of view. This is because in an experiment, we face noise caused by natural factors, as well as by the eavesdropper(s). Hence a relevant question is as follows: which protocol allows a secure key transmission in the presence of a higher level of noise, of the type present in an experiment?

Consider a typical situation when we send the two qubits (one being sent from Alice to B_1 and another from Alice to B_2) via two fibers. A usual model of noise here would be that each channel (fibers) is an isotropically depolarizing channel and that they are independent. Given a channel with a fixed level of depolarization, we ask the following: can we securely extract some secret key using either the E4 or the BB84$^{\otimes 2}$ protocol?

This may not be equivalent to comparing R_{QBE} thresholds because different states are used in the two protocols, which under the same noise level may behave differently, and result in different R_{QBE}'s. In particular it could happen that in such a situation it might be advantageous to apply a protocol with a lower R_{QBE} threshold. Therefore, in principle, it could be that the R_{QBE} (the one under a given noise model) for E4 is much higher than that for BB84$^{\otimes 2}$, and it may even be that the R_{QBE} for E4 is higher than the threshold $R_{\mathrm{QBE}}(\mathrm{E4})$ obtained before, while for BB84$^{\otimes 2}$, the R_{QBE}, after the noise affects the sent states, is below the BB84$^{\otimes 2}$ threshold. Then BB84$^{\otimes 2}$ would be more advantageous than E4 in such a noisy environment. We would then use BB84$^{\otimes 2}$, and in this sense BB84$^{\otimes 2}$ would be better than E4.

However, for a depolarizing environment, the R_{QBE}'s for E4 and BB84$^{\otimes 2}$ depend in the same way on the depolarization parameter of the depolarizing channel. If an isotropically depolarizing qubit channel acts as

$$\mathcal{D}(\rho) = (1-p)\rho + p\mathbb{1}/2, \tag{44}$$

then the R_{QBE} caused by the $\mathcal{D}^{\otimes 2}$ channel is

$$R_{\mathrm{QBE}} = p(1-p/2) \tag{45}$$

for *both* the protocols. Comparing protocols using R_{QBE} thresholds as a figure of merit is therefore legitimate here both from theoretical and practical points of view.

VIII. CONCLUSIONS

Entanglement is the essential ingredient of quantum communication in which there is no security aspect, with quantum teleportation and quantum dense coding being spectacular examples. We have shown that entanglement can also enhance security in quantum cryptography [17].

We have considered a cryptographic scenario, called secret sharing, in which there is a single sender and there are two receivers. The security analysis was performed for the secret sharing protocols by calculating quantum bit error rate thresholds. Since we are considering a scenario where there are two information transmission channels (respectively, from the sender to the two receivers), the physically meaningful case is to consider two eavesdroppers who act on the two channels locally but may securely communicate between themselves classically to discuss about the measurement outcomes in their respective local attacks. This is exactly the case that we consider and have found the optimal eavesdropping attacks for the considered secret sharing protocols.

In the process we have been able to show that bound entangled states with positive partial transpose are not a useful resource for the eavesdropper couple. We have also found the parallel of the Csiszár-Körner criterion for security in (single-receiver) cryptography in the distributed-receiver case and usefulness of the protocols in the presence of a depolarizing environment.

ACKNOWLEDGMENTS

We acknowledge support from the Spanish MEC [Grant No. FIS-2005-04627, Consolider QOIT, Acciones Integradas, TOQATA (Grant No. FIS2008-00784), and Ramón y Cajal], ESF/MEC project FERMIX (Grant No. FIS2007-29996-E), Polish Ministry of Science and Higher Education Grant No. 1 P03B 011 29, EU IP SCALA and QAP, EU STREP project NAMEQUAM, and Humboldt Foundation.

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[2] M. Lewenstein, A. Sanpera, V. Ahufinger, B. Damski, A. Sen(De), and U. Sen, Adv. Phys. **56**, 243 (2007); L. Amico, R. Fazio, A. Osterloh, and V. Vedral, Rev. Mod. Phys. **80**, 517 (2008).

[3] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992); C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *ibid.* **70**, 1895 (1993).

[4] M. Żukowski, A. Zeilinger, M. A. Horne, and H. Weinfurter, Acta Phys. Pol. A **93**, 187 (1998); M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[5] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999); A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999); K. Chen and H.-K. Lo, Quantum Inf. Comput. **7**, 689 (2007).

[6] C. H. Bennett and G. Brassard, Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore (IEEE, New York, 1984).

[7] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[8] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); D. Bruß, M. Christandl, A. K. Ekert, B.-G. Englert, D. Kaszlikowski, and C. Macchiavello, Phys. Rev. Lett. **91**, 097901 (2003); M. Curty, M. Lewenstein, and N. Lütkenhaus, *ibid.* **92**, 217903 (2004); A. Acín and N. Gisin, *ibid.* **94**, 020501 (2005).

[9] More precisely, the cases when the eavesdropper *and* the valid users have quantum memory, and when none have it, have the same threshold R_{QBE}. The case when the eavesdropper has quantum memory, but the valid users do not have it, the threshold R_{QBE} is not yet known.

[10] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001); Phys. Rev. A **65**, 012311 (2001); A. Sen(De), U. Sen, and M. Żukowski, *ibid.* **68**, 032309 (2003); C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).

[11] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New Jersey, 1991); G. Brassard and L. Salvail, Adv. Cryptol. **765**, 410 (1994); M. A. Nielsen and I. L. Chuang, *Quantum Computing and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[12] J. L. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979); C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[13] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).

[14] P. Horodecki, Phys. Lett. A **232**, 333 (1997); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[15] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).

[16] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, Phys. Rev. A **74**, 042339 (2006).

[17] We are using the term "quantum cryptography" as an umbrella term for all quantum communication protocols that involves a security aspect.