Detecting two-party quantum correlations in quantum-key-distribution protocols

Marcos Curty,[1] Otfried Gühne,[2,3] Maciej Lewenstein,[2] and Norbert Lütkenhaus[1]

[1]*Quantum Information Theory Group, Institut für Theoretische Physik I, and Max-Planck Research Group, Institute of Optics, Information and Photonics, Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany*

[2]*Institut für Theoretische Physik, Universität Hannover, Appelstraße 2, 30167 Hannover, Germany*

[3]*Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, 6020 Innsbruck, Austria*

(Received 8 September 2004; published 11 February 2005)

A necessary precondition for secure quantum key distribution is that sender and receiver can prove the presence of entanglement in a quantum state that is effectively distributed between them. In order to deliver this entanglement proof one can use the class of entanglement witness (EW) operators that can be constructed from the available measurements results. This class of EWs can be used to provide a necessary and sufficient condition for the existence of quantum correlations even when a quantum state cannot be completely reconstructed. The set of optimal EWs for two well-known entanglement-based (EB) schemes, the six-state and the four-state EB protocols, has been obtained recently [M. Curty *et al.*, Phys. Rev. Lett. **92**, 217903 (2004).] Here we complete these results, now showing specifically the analysis for the case of prepare and measure (PM) schemes. For this, we investigate the signal states and detection methods of the four-state and the two-state PM schemes. For each of these protocols we obtain a reduced set of EWs. More importantly, each set of EWs can be used to derive a necessary and sufficient condition to prove that quantum correlations are present in these protocols.

DOI: 10.1103/PhysRevA.71.022306 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Mn

I. INTRODUCTION

One of the most important problems in modern cryptography is the transmission of secret information from a sender (usually called Alice) to a receiver (Bob) over an insecure communication channel [1]. The goal is to guarantee that any possible eavesdropper (Eve), with access to the channel, is unable to obtain useful information about the message.

Secret systems were studied from an information-theoretic perspective by Shannon [2]. He analyzed the natural scenario where Eve has always access to exactly the same information received by Bob. This information, denoted as C (from the term ciphertext), is typically obtained by Alice as a function of the message to be sent, M, and a secret key K that she needs to share previously with Bob. In this context, Shannon defined a cryptographic system to be perfectly secret and uniquely decodable if it satisfies the following two conditions: first, the ciphertext C and the message M must be statistically independent. This means that Eve cannot obtain any useful information about the message M from C. This condition can be expressed as $I(M;C)=0$, where I denotes the mutual information measured in bits [2]. The second condition states that Bob can recover the original message M from C and K. It can be formulated as $H(M|C,K)=0$, with H the Shannon entropy measured also in bits [2]. With this definition, Shannon proved the well-known pessimistic result that every perfectly secret uniquely decodable system must satisfy $H(K)\geqslant H(M)$. An example of a secret cryptographic system satisfying this condition is the so-called one-time-pad or Vernam cipher [3].

The result from Shannon relies in a fundamental way on considering that both Bob and Eve have perfect access to the same ciphertext C. However, there are scenarios, such a is the case in quantum key distribution (QKD), where the proper exploitation of particular quantum effects can prevent Bob and Eve from receiving precisely the same information. The laws of quantum mechanics can guarantee some minimal uncertainty between both signals, and this fact can be used by Alice and Bob to expand a previously shared secret key K in an unconditionally secure manner [4–7]. This means that QKD together with the Vernam cipher can in principle be used to achieve perfectly secret communications even when $H(K)\ll H(M)$.

In any realization of QKD one can typically distinguish two phases in order to expand a secret key. In the first phase, an effective bipartite quantum mechanical state is distributed between Alice and Bob. This state creates correlations between them and it might contain as well hidden correlations with Eve. Next, a (restricted) set of measurements is used by the legitimate users to measure these correlations. As a result, Alice and Bob obtain a classical joint probability distribution $P(A,B)$ representing the measurement results. In the second phase, usually called *key distillation*, Alice and Bob use an authenticated public channel to process the correlated data in order to obtain a secret key. This procedure involves, typically, postselection of data, error correction to reconcile the data, and privacy amplification to decouple the data from Eve [8].

Two types of schemes are used to create the correlated data in the first phase of QKD. In *entanglement-based* (EB) schemes an, in general, untrusted third party distributes a bipartite state to Alice and Bob. This party may be even Eve who is in possession of a third subsystem that may be entangled with those given to Alice and Bob. While the subsystems measured by Alice and Bob result in correlations described by $P(A,B)$, Eve can use her subsystem to obtain information about the data of the legitimate users.

In *prepare and measure* (PM) schemes Alice prepares a random sequence of predefined non orthogonal states $|\varphi_i\rangle$ that are sent to Bob through an untrusted quantum channel (possibly controlled by Eve). On the receiving side, Bob performs a positive-operator-value measure (POVM) on every signal he receives. Generalizing the ideas introduced by Bennett *et al.* [9], the signal preparation process in PM schemes can be thought of as follows. Alice prepares an entangled bipartite state of the form $|\Psi\rangle_{AB}=\Sigma_i\sqrt{p_i}|\alpha_i\rangle|\varphi_i\rangle$, where the states $|\alpha_i\rangle$ form an orthonormal basis and $\{p_i\}_i$ represents the *a priori* probability distribution of the signal states $|\varphi_i\rangle$. If now Alice measures the first system in the basis $|\alpha_i\rangle$, she effectively prepares the (nonorthogonal) signal states $|\varphi_i\rangle$ with probabilities p_i. The action of the quantum channel on the state $|\Psi\rangle_{AB}$ leads to an effective bipartite quantum state shared by Alice and Bob. One important difference between PM schemes with effective entanglement and EB schemes with real entanglement is that in the first case the reduced density matrix of Alice, $\rho_A=\mathrm{Tr}_B(|\Psi\rangle\langle\Psi|_{AB})$, is fixed and known and cannot be modified by Eve.

An essential question in QKD now is whether the correlated data generated in the first phase enable Alice and Bob to extract a secret key. In Ref. [10] it has been proven that a necessary precondition for secure key distillation is the provable presence of quantum correlations in $P(A,B)$. That is, it must be possible to interprete $P(A,B)$, together with the knowledge of the corresponding measurements, as coming *exclusively* from an entangled state. Moreover, this result applies both for EB and PM schemes (for EB schemes see also [11]). Alice and Bob need to be able to detect the presence of entanglement in the quantum state that is effectively distributed between them, otherwise no secret key can be obtained. Among all separability criteria available nowadays to deliver this entanglement proof (see, e.g., [12] and references therein), entanglement witnesses (EWs) [13–15] are particularly suited for this purpose since they give rise to a necessary and sufficient condition for the existence of quantum correlations in $P(A,B)$, even when the state shared by Alice and Bob cannot be completely reconstructed [10]. In Ref. [10] a detailed analysis of two well-known EB protocols, the six-state and the four-state EB protocols [5–7], is included and the set of optimal EWs to detect quantum correlations in both protocols has been found. The purpose of this paper is to complete the results contained in Ref. [10], now showing specifically the analysis for the case of PM schemes. In particular, we investigate the signal states and detection methods of the four-state and the two-state PM schemes [5,16], and we obtain a reduced set of EWs that can be used to derive a necessary and sufficient condition to prove that quantum correlations are present in these protocols. As a side point, we put into context recent results that can be useful in the search of quantum correlations for higher-dimensional QKD schemes [17].

The paper is organized as follows. In Sec. II we review the role of quantum correlations as precondition for secure QKD. Section III introduces the concept of EWs and shows how to detect quantum correlations by using the class of EW operators that can be constructed from the available data. This formalism is then used in Sec. IV to analyze well-known QKD protocols. Our starting points are the EB schemes studied in Ref. [10]: The six-state and four-state EB schemes. Then we present the results for PM schemes, analyzing in detail the four-state and the two-state PM schemes. The last part of the section gives a brief outlook on the study of quantum correlations in higher-dimensionsal QKD schemes and in practical QKD. Finally, Sec. V concludes the paper with a summary.

II. QUANTUM CORRELATIONS AND QUANTUM KEY DISTRIBUTION

As mentioned in the Introduction, the provable presence of quantum correlations in $P(A,B)$ has been shown to be a necessary precondition for secure QKD [10]. The starting point for such a proof is an upper bound for the distillation rate of a secure key from correlated data via authenticated public communication, which is given by the *intrinsic information* $I(A;B\downarrow E)$, introduced by Maurer and Wolf [18]. These authors considered the problem of key distillation in the classical scenario where Alice, Bob, and Eve have access to repeated independent realizations of three random variables, denoted as A, B, and E, characterized by a probability distribution $P(A,B,E)$. In this context, Maurer and Wolf proved that the rate of secret bits, denoted as $S(A;B\|E)$, that Alice and Bob can get by communicating to each other through a public authenticated channel satisfies [18]

$$S(A;B\|E) \leqslant I(A;B\downarrow E) = \min_{E\to\bar{E}} I(A;B|\bar{E}), \tag{1}$$

where the minimization runs over all possible channels $E\to\bar{E}$ characterized by the conditional probability $P(\bar{E}|E)$, and $I(A;B|\bar{E})$ is the mutual information between Alice and Bob given the public announcement of Eve's data based on the probabilities $P(A,B,\bar{E})$. This quantity is defined in terms of the conditional Shannon entropy $H(X|\bar{e})=\Sigma_{x\in X}-p(x|\bar{e})\log_2 p(x|\bar{e})$ as

$$I(A;B|\bar{E}) = \sum_{\bar{e}\in\bar{E}} P(\bar{e})[H(A|\bar{e}) + H(B|\bar{e}) - H(A,B|\bar{e})]. \tag{2}$$

More important for QKD, the result of Maurer and Wolf can as well be adapted to the case where Alice, Bob, and Eve start sharing a tripartite quantum state instead of a joint probability distribution. For this purpose, one can consider all possible tripartite states that Eve can establish using her eavesdropping method, and all possible measurements she could perform on her subsystem. This gives rise to a set of possible extensions $\mathcal{P}$ of the observable probability distribution $P(A,B)$ to $P(A,B,E)$. Now one can define the intrinsic information as

$$I(A;B\downarrow E) = \inf\nolimits_{\mathcal{P}} I(A;B|E). \tag{3}$$

The main consequence of this fact is that whenever the observable data $P(A,B)$ can be explained as coming from a tripartite state with a separable reduced density matrix for Alice and Bob, the intrinsic information vanishes and therefore no secret key can be established.

Observation 1 [10]. Assume that the observable joint probability distribution $P(A,B)$ together with the knowledge of the corresponding measurements performed by Alice and Bob can be interpreted as coming from a separable state σ_{AB}. Then the intrinsic information vanishes and no secret key can be distilled via public communication from the correlated data.

Proof. This is easy to see for EB schemes as we extend a separable reduced density matrix $\sigma_{AB}=\Sigma_i q_i|\phi_i\rangle_A\langle\phi_i| \otimes|\psi_i\rangle_B\langle\psi_i|$ to a tripartite pure state of the form $|\Phi\rangle_{ABE}=\Sigma_i\sqrt{q_i}|\phi_i\rangle_A|\psi_i\rangle_B|e_i\rangle_E$. (See also [11].) Here $|e_i\rangle_E$ is a set of orthonormal vectors spanning a Hilbert space of sufficient dimension. If Eve measures her subsystem in the corresponding basis, the conditional probability distribution conditioned on her measurement result factorizes such that for this measurement $I(A;B|E)=0$. As a consequence, the intrinsic information vanishes and no secret key can be distilled.

In the case of PM schemes we need to show additionally that the state $|\Phi\rangle_{ABE}$ can be obtained by Eve by interaction with Bob's system only. The initial state $|\Psi\rangle_{AB}=\Sigma_i\sqrt{p_i}|\alpha_i\rangle|\varphi_i\rangle$ can be written in the Schmidt decomposition as $|\Psi\rangle_{AB}=\Sigma_i c_i|u_i\rangle_A|v_i\rangle_B$. Then the state $|\Phi\rangle_{ABE}$ from above is in the Schmidt decomposition, with respect to system A and the composite system BE, of the form $|\Phi\rangle_{ABE}=\Sigma_i c_i|u_i\rangle_A|\tilde{e}_i\rangle_{BE}$ since c_i and $|u_i\rangle_A$ are fixed by the known reduced density matrix $\rho_A=\mathrm{Tr}_B(|\Psi\rangle\langle\Psi|_{AB})$ to the corresponding values of $|\Psi\rangle_{AB}$. Then one can find always a suitable unitary operator U_{BE} such that $|\tilde{e}_i\rangle_{BE}=U_{BE}|v_i\rangle_B|0\rangle_E$ where $|0\rangle_E$ is an initial state of an auxiliary system. ■

The natural question that arises now is whether the presence of quantum correlations is also a sufficient condition for secure QKD. Let us mention already here that this is still an open question in the field of quantum cryptography. In EB schemes, it is clear that it is possible to obtain a secret key whenever the distributed bipartite states are entangled qubit states *and* each party is allowed to perform collective quantum manipulations on their respective states. This is true since in this situation one can first distill maximally entangled states from the initial states and subsequently measure them out in the standard basis [19]. The verification that the entanglement distillation process succeeded allows one to give the security statement about the resulting perfectly correlated and random measurement data, which can then be used as a secret key.

A completely different scenario arises once Alice and Bob have already performed their respective measurements on the given states and they can only use classical operations on their correlated data. This last case has been partially addressed under additional assumptions, namely, that the eavesdropping attack employed by Eve is restricted to the so-called "incoherent symmetric strategies," in [20]. In this situation it has been proven that for a particular class of QKD protocols key distillation is possible if and only if the initially distributed states are distillable [20]. In the same spirit, Acín *et al.* [21] showed that one can always distill a secret key from any two-qubit and one-copy distillable states by adapting the local measurements to the quantum states and performing subsequently a classical protocol. All these results suggested the idea of a correspondence between entanglement distillation and secret key distillation. See also [22]. The main conjecture was that a quantum state could lead to a secret key if and only if it is distillable, which is not equivalent to containing quantum correlations [23]. However, this point of view changed recently, since it has been shown that it is also possible to generate a secret key even from certain nondistillable entangled states, known as bound entangled or positive partial transposed (PPT) entangled states [24]. These are states that require entanglement to be created but do not allow one to distill entanglement from them [23]. This shows that the focus on entanglement-distillation-guided protocols in QKD is too narrow, though the interesting example introduced in Ref. [24] does not answer the question whether all entangled states can be transformed into a private key.

More recently, going back to the quantum correlations point of view, Acín and Gisin [25] proved that it is an equivalent statement to show that there has been (real or effective) entanglement in the distributed quantum state and that the intrinsic information is nonzero. In particular, this result implies that there exists a one-to-one relation between the detection of entanglement in $P(A,B)$ and the fact that such probability distribution cannot be obtained by classical means using only local operations and classical communication [25,26]. That is, $P(A,B)$ contains secret bits. More important for QKD, this means that either it is possible to distill a secret key from *any* bi-partite entangled state or there exits a classical analog of bound entanglement, the so-called bound information [11]. This is information shared by Alice, Bob, and Eve such that Alice and Bob cannot obtain a secret key from it although this information cannot be distributed by local operations and classical communication. However, so far the existence of bound information has been proven for the multipartite case [27] (for the case of coherent manipulations of multiparty quantum states see also [28]), but not for the bipartite case relevant for QKD.

III. DETECTING QUANTUM CORRELATIONS

Given that quantum correlations are necessary for distilling a secure secret key, the question now is how to detect these quantum correlations in a given QKD scheme. More precisely, we have to answer the question whether the joint probability distribution $P(A,B)$, coming from the measurements performed by Alice and Bob during the protocol, allows them to conclude that the effectively distributed state was entangled or not. In principle any separability criteria (see, e.g., [12] and references therein) might be employed to deliver this entanglement proof. The important question here is whether the chosen criterion can be used to provide a necessary and sufficient condition to detect entanglement when the knowledge about the state is not tomographic complete. As we will see below, it is a property of EWs that they allow one to obtain a necessary and sufficient criterion for separability even when the state cannot be completely reconstructed [10].

Let us first consider EB schemes. In these schemes, Alice and Bob perform some measurements on a bipartite quantum state distributed by an, in general, untrusted third party and retrieve the probability distribution $P(A,B)$ of the outcomes.

Before showing that in this scenario EWs are specially appropriated to detect entanglement, let us recall some facts about witnesses [13–15].

A witness is a Hermitian observable W with a positive expectation value on all separable states. So if a state ρ obeys $\mathrm{Tr}(\rho W) < 0$, the state ρ must be entangled. We say then that the state ρ is detected by W. In general, for every entangled state there exists a witness detecting it; however, this witness is in most cases very difficult to construct. Witnesses can be *optimized* in the following sense: A witness W_1 is called *finer* than another witness W_2 if W_1 detects all the states which are detected by W_2 and some states in addition. Finally, a witness W is called *optimal*, when there is no other witness which is finer than W [15]. Now we can state the following (see also [10]).

Theorem 1. Assume that Alice and Bob can perform some local measurements with POVM elements $A_i \otimes B_i$, $i = 1, \ldots, n$, to obtain the probability distribution of the outcomes $P(A,B)$ on the distributed state ρ. Then the correlations $P(A,B)$ cannot originate from a separable state if and only if there is an EW of the form $W = \Sigma_i c_i A_i \otimes B_i$ which detects the effectively distributed state, i.e., $\mathrm{Tr}(W\rho) = \Sigma_i c_i P(A_i, B_i) < 0$.

Proof. One direction of the above theorem is clear: If such a witness with the properties from above exists, then the effectively distributed state is clearly entangled. To prove the other direction, let us look at the the following map, which maps a quantum state ρ to a real vector $\mathfrak{A}(\rho) \in \mathbb{R}^n$:

$$\mathfrak{A}: \rho \mapsto \mathfrak{A}(\rho) = \{\mathfrak{A}(\rho)_0, \ldots, \mathfrak{A}(\rho)_n\}, \tag{4}$$

where $\mathfrak{A}(\rho)_i = P(A_i, B_i) = \mathrm{Tr}(A_i \otimes B_i\ \rho)$. That is, it maps a state onto the set of probabilities or expectation values of the POVM elements. This map is linear and, in general, not injective. It maps the convex set S of separable states onto the convex set $S' := \mathfrak{A}(S)$. An entangled state ρ with the property $\mathfrak{A}(\rho) \in S'$ cannot be detected with the given probabilities, since then there is a separable state ρ_s being mapped to the same $\mathfrak{A}(\rho_s) = \mathfrak{A}(\rho)$; thus ρ and ρ_s are indistinguishable. So a state ρ_e for which $P(A,B)$ cannot originate from a separable state must obey $\mathfrak{A}(\varrho_e) \notin S'$, Now we have the usual construction of witnesses. There must exist a hyperplane separating $\mathfrak{A}(\varrho_e)$ from S'. This means that there is a vector $w = (w_1, \ldots, w_n)$ with $\Sigma_i w_i \mathfrak{A}(\varrho_e)_i < 0$ while $\Sigma_i w_i \mathfrak{A}(\varrho)_i > 0$ for all ρ with $\mathfrak{A}(\rho) \in S'$. The observable $W = \Sigma_i w_i A_i \otimes B_i$ is now the desired EW, since $\mathrm{Tr}(W\rho) = \Sigma_i w_i P(A_i, B_i)$. ■

We refer to witnesses that can be evaluated with the given POVM elements and the corresponding correlations $P(A,B)$ as *accessible*. According to Theorem 1, the set of all accessible witness operators gives rise to a necessary and sufficient condition for verifiable entanglement contained in the correlations $P(A,B)$: The joint probability distribution $P(A,B)$ can come exclusively from an entangled state if and only if at least one accessible witness in the set gives rise to a negative expectation value when it is evaluated with $P(A,B)$. Of course, in this set there is some redundancy. Typically, it contains witnesses that are finer than others, and therefore one can construct smaller sets of witnesses that are accessible and still have the property of being necessary and sufficient for verifying entanglement. Whenever this property holds, we refer to a set of witnesses $\mathcal{W}$ as being a *verification set*. The ultimate goal will be to obtain a *minimal verification set* in a compact description that contains no further redundancies to allow an efficient systematic search for verifiable entanglement by evaluating the members of this set. The rest of this paper is mainly concerned with the search of these minimal verification sets, although in the case of the four-state PM protocol and in the two-state PM protocol we find only *reduced verification sets*, which still may contain some redundancies.

Before starting our quest for minimal verification sets, let us consider the case of PM schemes since in this section we have considered, so far, only EB schemes. As we mentioned previously, in these kinds of schemes the reduced density matrix of Alice is fixed since Eve has no access to the state of Alice to try to modify it. However, this situation also can be incorporated in the theorem from above. We can add to the observables $A_i \otimes B_i$ other observables $C_i \otimes \mathbb{1}$ such that the observables C_i form a tomographic complete set of Alice's Hilbert space. Those witnesses that can be evaluated with this combined set of measurements can clearly be evaluated with the measurements $A_i \otimes B_i$ and the knowledge of the reduced density matrix of Alice.

In the geometric picture obtained in the proof of the theorem from above, the knowledge of the expectation value of some of the observables implies that we know that our state lies on some hyperplane in the space of all expectation values. Then, we want to decide for a point on this hyperplane whether is is in S' or not, and this can be done by witnesses. The knowledge of the mean values of some observables may be used to argue that only a smaller set of witnesses is relevant for such a PM scheme. We will see an example of this later.

Finally, let us emphasize again that there are many other separability criteria besides EWs which might be used for the detection of entanglement in quantum cryptographic schemes. For instance, the security of the first EB scheme proposed by Ekert in 1991 [6], the four-state EB scheme, was based on the detection of quantum correlations by looking at possible violations of Bell inequalities [29]. This criterion, or for example those based on uncertainty relations [30], is directly linked to experimental data, which makes the implementation simple. Another interesting criterion that seems to be particularly suited for the case of PM schemes, where the reduced density matrix of Alice is fixed and known, is, for instance, the reduction criterion [31]. However, it is not clear whether these criteria guarantee detection of *all* entangled states which can be detected with the given set of measurements. In fact, in the case of the four-state scheme, the knowledge of the performed measurements together with $P(A,B)$ allows us to detect entangled states beyond those that violate Bell-like inequalities.

IV. QKD PROTOCOLS

We will now illustrate the consequences of this view for some well-known QKD protocols. First we start reviewing the recent results obtained in Ref. [10] for the six-state and the four-state EB protocols [6,7], which include a minimal verification set to detect quantum correlations in both protocols. Then we present the analysis for the case of PM schemes. We investigate the four-state and the two-state PM schemes [5,16], and we obtain a reduced verification set for each of these protocols. Finally, the last part of the section gives a brief outlook at the study of quantum correlations in higher-dimensional QKD schemes and in practical QKD [17].

A. Six-state protocol

For the case of the six-state EB protocol, Alice and Bob perform projection measurements onto the eigenvectors of the three Pauli operators σ_x, σ_y, and σ_z on the bipartite qubit states distributed by Eve. In the corresponding PM scheme Alice prepares the eigenvectors of those operators by performing the same measurements on a maximally entangled two-qubit state. Note that here we are not using the general approach introduced previously, $|\Psi\rangle_{AB}=\Sigma_i\sqrt{p_i}|\alpha_i\rangle|\varphi_i\rangle$, to model PM schemes, since for this protocol it is sufficient to consider that the effectively distributed quantum state consists only of two qubits. In both cases Alice has complete tomographic knowledge of her subsystem and therefore the class of EWs, that can be constructed in both protocols coincides. The set of three measurement bases used in the protocol allows Alice and Bob to construct any EW of the form

$$W=\sum_{i,j=\{0,x,y,z\}} c_{ij}\sigma_i\otimes\sigma_j, \tag{5}$$

where $\sigma_0=\mathbb{1}$ and c_{ij} are real numbers. Note that the set of operators $\{\sigma_i\otimes\sigma_j\}_{i,j}$ constitutes an operator basis in $\mathbb{C}^2\otimes\mathbb{C}^2$. This means that Alice and Bob can in principle evaluate all EWs, in particular, the class of optimal witnesses for two-qubit states. This class, denoted by OEW, is given by the witnesses operators of the form [32]

$$W=|\phi_e\rangle\langle\phi_e|^{T_P}, \tag{6}$$

where $|\phi_e\rangle$ denotes any entangled state of two-qubit systems and T_P is the partial transposition, that is, the transposition with respect to one of the subsystems [33]. Therefore, in the six-state protocol, for both EB and PM schemes, all entangled states can be detected and the optimal witnesses OEWs form the minimal verification set.

Alternatively to the witness approach, Alice and Bob can employ as well quantum state tomography techniques to reconstruct the effectively distributed quantum state and then use the Peres-Horodecki criterion [13,34] to determine whether that state was entangled or not. This criterion establishes that a two-qubit state is separable if and only if its partial transposition is positive. For higher-dimensional systems, however, note that although all operators with nonpositive partial transposition are entangled, there exist PPT entangled states [23].

B. Four-state protocol

While the analysis of the six-state protocol is quite simple, due to the complete tomographic information that Alice and Bob share, the four-state protocol needs a deeper examination. As we will show below, the class of the OEW for two-qubit systems cannot be evaluated with the given correlations either in the EB or in the PM version of the protocol. In the EB case Alice and Bob perform projection measurements onto two mutually unbiased bases, say the ones given by the eigenvectors of the two Pauli operators σ_x and σ_z. In the corresponding PM scheme, Alice can use as well the same set of measurements but now on a maximally entangled state. Here again, as in the six-state protocol, we use the fact that the approach $|\Psi\rangle_{AB}=\Sigma_i\sqrt{p_i}|\alpha_i\rangle|\varphi_i\rangle$ to model PM schemes can be reduced to employ only two-qubit states for this protocol. Let us begin our analysis for the EB scheme [10].

1. Entanglement-based

In the case of the four-state EB protocol we will denote the set of EWs that can be evaluated with the resulting correlations as W_4^{EB}. All elements are of the form

$$W_4^{EB}=\sum_{i,j=\{0,x,z\}} c_{ij}\ \sigma_i\otimes\sigma_j. \tag{7}$$

This class of EWs can be characterized with the following observation.

Observation 2 [10]. Given an entanglement witness W we find $W\in W_4^{EB}$ if and only if $W=W^T=W^{T_P}$.

Proof. To see this, we start with the general ansatz of Eq. (5) and we impose the conditions $W=W^T=W^{T_P}$. This directly constraints W to the form (7) since σ_y is the only skew-symmetric element in the operator basis. The reverse direction is then trivial. ■

It is straightforward to see that the elements of the OEW do not satisfy this condition. Below, we will provide a criterion to decide if an entangled state can be detected by $W\in W_4^{EB}$. This means that, in contrast to the case of the six-state protocol, in the four-state EB protocol there can be entangled states that give rise to correlations $P(A,B)$ that are not sufficient to prove the presence of entanglement.

The concept of optimal witnesses introduced in Sec. III for general witness operators can as well be extended to the witnesses that are accessible with the given set of measurements. This way we call a witness W *optimal in class C* if and only if there is no other element in C that detects all entangled states detected by W. Our goal now is to characterize a complete family of witness operators that are optimal in the class W_4^{EB}. This family forms the minimal verification set. Then it is sufficient to check this family to decide whether the presence of entanglement can be verified from the given data. To do this we start presenting a necessary and sufficient condition for a bipartite state to contain entanglement that can be detected by elements of W_4^{EB}.

Observation 3 [10]. An entangled state ρ can be detected with a $W\in W_4^{EB}$ if and only if the operator $\Omega=\frac{1}{4}(\rho+\rho^{T_A}+\rho^{T_B}+\rho^T)$ is a nonpositive operator.

Proof. To see this, let us start by the observation that the symmetries of the witness operators in W_4^{EB} give rise to the identity $\mathrm{Tr}(W\rho)=\mathrm{Tr}(W\Omega)$. Now let us assume that the operator Ω is non-negative. Then one can interpret it as a density matrix. Since it is invariant under partial transposition, it must be a separable state. Since W is a witness operator, we must therefore find $\mathrm{Tr}(W\rho)\geqslant 0$. As a result, we find that the nonpositivity of Ω is a necessary condition to detect entanglement of the state ρ with witnesses in W_4^{EB}. The reverse direction is included here only for completeness and the proof is included implicitly in Theorem 2. ■

Next we present a set of EWs composed of optimal witnesses in the class W_4^{EB} which forms a minimal verification set of the four-state EB protocol.

Theorem 2 [10]. Consider the family of operators $W=\frac{1}{2}(Q+Q^{T_P})$, where $Q=|\phi_e\rangle\langle\phi_e|$ and $|\phi_e\rangle$ denotes a real entangled state. The elements of this family are witness operators that are optimal in W_4^{EB} (OEW$_4^{EB}$) and detect all the entangled states that can be detected within W_4^{EB}.

Proof. Let us start by checking that this family, indeed, can detect all entanglement that can be detected in W_4^{EB}. From Observation 3 we know that we need only consider bipartite states ρ such that $\Omega=\frac{1}{4}(\rho+\rho^{T_A}+\rho^{T_B}+\rho^{T})$ is nonpositive. We have, therefore, that there exists always an (entangled) state $|\phi_e\rangle$ such that $\langle\phi_e|\Omega|\phi_e\rangle<0$. Moreover, since $\Omega=\Omega^T$, this operator has a real representation. In this representation, also the state $|\phi_e\rangle$ has a real representation [35]. Let us define the projector $Q=|\phi_e\rangle\langle\phi_e|$. Then we find $\langle\phi_e|\Omega|\phi_e\rangle=\mathrm{Tr}\left[\frac{1}{4}(Q+Q^{T_A}+Q^{T_B}+Q^{T})\rho\right]$. This means that we can define the operator $W=\frac{1}{4}(Q+Q^{T_A}+Q^{T_B}+Q^{T})$ which can be further simplified to $W=\frac{1}{2}(Q+Q^{T_P})$ thanks to the real representation of Q. This operator is a witness operator, since $\mathrm{Tr}(W\sigma)\geqslant 0$ for all separable states σ, while $\mathrm{Tr}(W\rho)<0$ for the chosen ρ. Moreover, by construction the family of these witness operators detects all entanglement that can be detected within W_4^{EB}.

Finally, we need to show that all witnesses of this new set $W=\frac{1}{2}(Q+Q^{T_P})$ are optimal within W_4^{EB} so they form OEW$_4^{EB}$. In Ref. [15] it has been proven that, given a set of witness operators S_W, $W\in S_W$ is optimal in S_W if and only if for all positive semidefinite operators P and $\epsilon>0$, $W'=(1+\epsilon)W-\epsilon P\notin S_W$. When a P can be subtracted, it has to satisfy $\langle e,f|P|e,f\rangle=0$ for all product vectors $|e,f\rangle\in\mathbb{C}^2\otimes\mathbb{C}^2$ with $\langle e,f|W|e,f\rangle=0$ since otherwise we would not have a witness anymore. In the case of witness operators of the form $W=\frac{1}{2}(Q+Q^{T_P})$, where $Q=|\phi_e\rangle\langle\phi_e|$ and

$$|\phi_e\rangle=\sum_{i=0}^{1}c_i|i\rangle|i\rangle \tag{8}$$

denotes the Schmidt decomposition of $|\phi_e\rangle$, we have that the $|e,f\rangle$ that satisfy $\langle e,f|W|e,f\rangle=0$ are given by $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, and the unnormalized states

$$|\phi(\lambda)\rangle=(\lambda|0\rangle\pm\sqrt{1-\lambda^2}|1\rangle)(c_1\sqrt{1-\lambda^2}|0\rangle\mp c_0\lambda|1\rangle), \tag{9}$$

with $\lambda\in(0,1)$. These product vectors span a three-dimensional subspace that is orthogonal to $|\phi_e\rangle$. This means that P cannot be subtracted from W unless $P=Q$. But $(1+\epsilon)W-\epsilon Q=\frac{1}{2}[(1-\epsilon)Q+(1+\epsilon)Q^{T_P}]\notin W_4^{EB}$ for all $\epsilon>0$. Therefore all witness operators $W=\frac{1}{2}(Q+Q^{T_P})$ with $Q=|\phi_e\rangle\langle\phi_e|$ and $|\phi_e\rangle$ real are OEW$_4^{EB}$‘s. ■

2. Prepare and measure

Once we have presented a set of witness operators that is optimal for the EB scheme, we will show below that this family is also sufficient to detect all entangled states that can be detected in the PM version of the four-state protocol. That is, with respect to the ability to detect quantum correlations, both schemes can use the same verification set. As we showed in Sec. III, in the case of PM schemes one can add to the set of observables measured in the protocol other observables $C_i\otimes\mathbb{1}$ such that the observables C_i form a tomographic complete set of Alice's Hilbert space. So we have to add the operator $\sigma_y\otimes\sigma_0$ to the observables in Eq. (7). This way one obtains all the witnesses that can be evaluated in the four-state PM protocol. This new set, which we shall denote as W_4^{PM}, is of the form

$$W_4^{PM}=\sum_{i,j=\{0,x,z\}}c_{ij}\sigma_i\otimes\sigma_j+c_{y0}\sigma_y\otimes\sigma_0, \tag{10}$$

where c_{y0} is as well a real number.

Now we present a result, Observation 4, that applies to the observables given by Eq. (7) and that will be useful to prove that the set of OEW$_4^{EB}$ obtained in Theorem 2 is also sufficient to detect all entangled states that can be detected in the four-state PM scheme and, therefore, it forms a reduced verification set of this protocol.

Observation 4. Given an observable W with $W=W^T=W^{T_P}$, then $\mathrm{Tr}(W\sigma)\geqslant 0$ for all σ separable if and only if $\mathrm{Tr}(W\sigma_r)\geqslant 0$ for all σ_r real and separable.

Proof. (If) Using the fact that $W=W^T$ we have $\mathrm{Tr}(W\sigma)=\frac{1}{2}\mathrm{Tr}[W(\sigma+\sigma^T)]$. Note that the symmetric matrix $\sigma+\sigma^T$ is real and positive semidefinite because σ is Hermitian and positive semidefinite and transposition is a positive operation. Moreover $(\sigma+\sigma^T)^{T_P}$ is positive semidefinite since σ^{T_P} is positive semidefinite for all σ separable. This means that $\frac{1}{2}(\sigma+\sigma^T)$ is a real separable quantum state. Therefore if $\mathrm{Tr}(W\sigma_r)\geqslant 0$ for all σ_r real and separable then $\mathrm{Tr}(W\sigma)\geqslant 0$ for all σ separable. (Only if) The proof is trivial. ■

Theorem 3. The family of OEW$_4^{EB}$, $W=\frac{1}{2}(Q+Q^{T_P})$ with $Q=|\phi_e\rangle\langle\phi_e|$ and $|\phi_e\rangle$ a real entangled state, is sufficient to detect all entangled states that can be detected in the four-state PM scheme.

Proof. To be EWs, the operators W_4^{PM} given by Eq. (10) must satisfy $\mathrm{Tr}(W_4^{PM}\sigma)\geqslant 0$ for all σ separable. In particular, it must satisfy $\mathrm{Tr}(W_4^{PM}\sigma_r)\geqslant 0$ for all σ_r real and separable. We have that the term $\sigma_y\otimes\sigma_0$ satisfies

$$\mathrm{Tr}[(\sigma_y\otimes\sigma_0)\sigma_r]=0,\quad\forall\,\sigma_r. \tag{11}$$

This means, therefore, that we need to guarantee that the first term in Eq. (10) satisfies

$$\sum_{i,j=\{0,x,z\}}c_{ij}\mathrm{Tr}[(\sigma_i\otimes\sigma_j)\sigma_r]\geqslant 0,\quad\forall\,\sigma_r. \tag{12}$$

According to Observation 4, we obtain that the term $\Sigma_{i,j=\{0,x,z\}}c_{ij}\sigma_i\otimes\sigma_j$ in Eq. (10) has to be an EW which belongs to the class W_4^{EB}. That is, $W_4^{PM}=W_4^{EB}+c_{y0}\sigma_y\otimes\sigma_0$.

To conclude the proof, now we have to take into account that in the four-state PM scheme the reduced density matrix of Alice is fixed and given by $\rho_A = \frac{1}{2}\mathbb{1}$. This means that

$$\mathrm{Tr}(W_4^{PM}\rho) = \mathrm{Tr}(W_4^{EB}\rho) \tag{13}$$

for all ρ such that $\mathrm{Tr}_B(\rho) = \frac{1}{2}\mathbb{1}$, since $\mathrm{Tr}[(\sigma_y \otimes \sigma_0)\rho] = 0$. That is, the entangled states that can be detected in the PM protocol are also detected by the class of witnesses W_4^{EB}. We have, therefore, that it is sufficient to consider the set of OEW_4^{EB}.■

3. Evaluation

From the set of witness operators OEW_4^{EB} given by $W = \frac{1}{2}(Q + Q^{T_P})$, with $Q = |\phi_e\rangle\langle\phi_e|$ and $|\phi_e\rangle$ a real entangled state, one can obtain a necessary and sufficient condition for the presence of entanglement in the observable correlations $P(A,B)$. This result applies to both versions of the four-state protocol: EB and PM. Note that for the case of an EB scheme all the witnesses in OEW_4^{EB} are optimal and form a minimal verification set. However, for a PM scheme some of them might be redundant and therefore this set of EWs forms a reduced verification set for this version of the protocol. The set OEW_4^{EB} includes an infinity number of witness operators, but, as we will see below, these EWs can be easily parametrized with only three real parameters. From a practical point of view, this means that Alice and Bob can easily check the conditions $\mathrm{Tr}(W\rho)$ with $W \in \mathrm{OEW}_4^{EB}$ numerically.

Let us briefly analyze the implications of our results in the relationship between the bit error rate e in the four-state and in the six-state protocols and the presence of correlations of quantum mechanical nature [10]. Here the error rate e quantifies the rate of events where Alice and Bob obtain different results. It refers to the shifted key, i.e., considering only those cases where the signal preparation and detection methods employ the same polarization basis. In an intercept-resend attack Eve measures every signal emitted by Alice and prepares a new one, depending on the result obtained, that is given to Bob. This action corresponds to an entanglement-breaking channel [36], i.e., it is a channel Φ such as $I \otimes \Phi(\rho)$ is separable for any density matrix ρ on a tensor product space. Such a channel gives rise to $e \geqslant 25\%$ (four-state protocol) and $e \geqslant 33\%$ (six-state protocol), respectively [7,37], which might seem to indicate that these values represent an upper bound for the tolerable error rate in the protocols (see also [38]). However, it turns out that for some asymmetric error patterns, it is possible to detect the presence of quantum correlations even for error rates above 25% (33%) [10]. Let us illustrate this fact with two examples that are motivated by the propagation of the polarization state of a single photon in an optical fiber.

In the first example we will consider a channel described by a unitary transformation that changes on a time scale much longer than the repetition cycle of the signal source, so it can be thought to be constant over that time: for instance, the channel given by the unitary transformation $U(\theta) = \cos\theta\mathbb{1} - i\sin\theta\sigma_y$. In this scenario, the resulting distributed state for both QKD protocols is given by $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|01\rangle - \sin\theta|10\rangle + \cos\theta|11\rangle$. The corresponding bit error rate is $e = \sin^2\theta$ and $e = \frac{2}{3}\sin^2\theta$ for the four-state and the six-state protocols, respectively. Nevertheless, it can be shown that in both cases the existence of quantum correlations can be detected for all angles θ. The case of the six-state protocol is clear, since a unitary transformation preserves the entanglement and all entanglement can be verified in this protocol. With respect to the four-state protocol, note that there is always an entanglement witness $W \in \mathrm{OEW}_4^{EB}$ that detects quantum correlations in $P(A,B)$. In particular, let us use $W = \frac{1}{2}(|\phi_e\rangle\langle\phi_e| + |\phi_e\rangle\langle\phi_e|^{T_P})$, with $|\phi_e\rangle$ as the eigenvector of the operator $\frac{1}{2}|\psi\rangle\langle\psi|^{T_P}$ which corresponds to its negative eigenvalue. Then we find in a suitable representation as a *pseudomixture* [39] for the entanglement witness that $\mathrm{Tr}(W\rho) = \Sigma_i c_i P(a_i, b_i) = -\frac{1}{4}$.

TABLE I. Example of a $P(A,B)$ for the four-state EB protocol, where $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$. The table is normalized such that $\Sigma_i P(A_i, B_i) = 1$.

	B			
A	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\|0\rangle$	0.08058	0.04757	0.02106	0.10709
$\|1\rangle$	0.04623	0.07560	0.11349	0.00834
$\|+\rangle$	0.11808	0.01690	0.09319	0.04179
$\|-\rangle$	0.00873	0.10627	0.04136	0.07364

For the second example, we focus on the four-state EB protocol only and we consider the particular joint probability distribution $P(A,B)$ given by Table I, where the states $|\pm\rangle$ are defined as $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$. In principle, it is not straightforward to decide whether these correlations can be explained as coming exclusively from an entangled state or not. This is specially so since in this case the resulting bit error rate is given by $e \approx 35.4\%$. To decide that question systematically we can use the verification set defined by OEW_4^{EB}: $W = \frac{1}{2}(|\phi_e\rangle\langle\phi_e| + |\phi_e\rangle\langle\phi_e|^{T_P})$. The real states $|\phi_e\rangle$ can be parametrized as $|\phi_e\rangle = \cos\phi|00\rangle + \sin\phi[\cos\psi|01\rangle + \sin\psi(\cos\theta|10\rangle + \sin\theta|11\rangle)]$, with only three real parameters $\phi, \psi, \theta \in [0, 2\pi)$. Moreover, since the state $|\phi_e\rangle$ is entangled these parameters satisfy additionally the condition $\sin\phi\sin\psi(\sin\phi\cos\psi\cos\theta - \cos\phi\sin\theta) \neq 0$ [40]. However, from a practical point of view it might be easier just to consider all angles ϕ, ψ, and θ and allow the evaluation of some positive operators. After expressing the witness operators as a *pseudomixture* [39] the condition $\mathrm{Tr}(W\rho) < 0$ can be rewritten as $\Sigma_i f_i(\phi, \psi, \theta)\ P(A_i, B_i) < 0$, with $c_i = f_i(\phi, \psi, \theta)$ for some functions f_i. Now it is easy to search numerically through the space of parameters ϕ, ψ, and θ for quantum correlations in $P(A,B)$. This fact is illustrated in Fig. 1, where some combinations of these parameters detecting entanglement when they are evaluated on the $P(A,B)$ given in Table I are marked.

To finish this section we show now that the family of witness operators OEW_4^{EB} allow us to detect entangled states beyond those that violate Bell-like inequalities [29]. Note that, as we mentioned previously, the security of the original four-state EB scheme [6] was based on the detection of entanglement by looking at possible violations of Bell inequali-

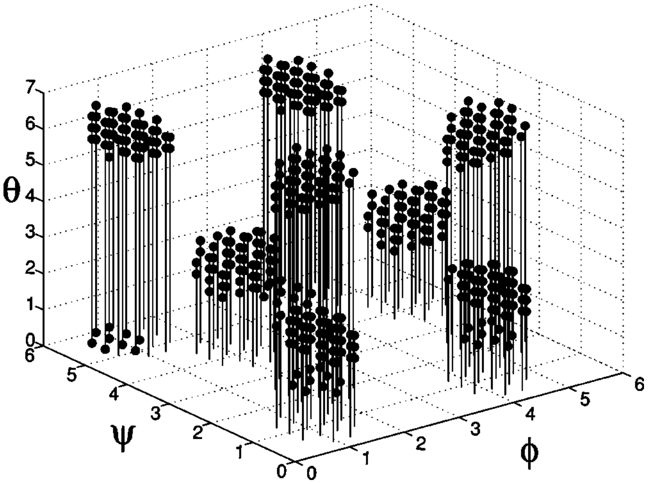

FIG. 1. Illustration of several regimes of the parameters ϕ, ψ, and θ leading to negative expectation values of the operators $\mathrm{OEW}_4^{EB}=(1/2)(|\phi_e\rangle\langle\phi_e|+|\phi_e\rangle\langle\phi_e|^{T_P})$, with $|\phi_e\rangle=\cos\phi|00\rangle+\sin\phi[\cos\psi|01\rangle+\sin\psi(\cos\theta|10\rangle+\sin\theta|11\rangle)]$, when they are evaluated on the joint probability distribution $P(A,B)$ given in Table I. The angles ϕ, ψ, and θ are represented in radians.

ties, which is in principle more restrictive than detection of quantum correlations. It is known that a violation of a Bell inequality can be formally expressed as an EW [14], while the contrary does not hold always. An interesting question then is to ask whether the family of OEW_4^{EB} corresponds to Bell inequalities or not. It is easy to see that the knowledge of the performed measurements in the four-state protocol together with the joint probability distribution $P(A,B)$ allow us to detect entangled states that do not violate Bell-like inequalities. Consider for instance the two-qubit entangled states introduced by Werner in [41] and which are defined as

$$\rho_W = p|\psi^-\rangle\langle\psi^-| + \frac{1}{4}(1-p)\mathbb{1}, \tag{14}$$

with $|\psi^-\rangle=1/\sqrt{2}(|01\rangle-|10\rangle)$. In the probability range $1/3<p<1/\sqrt{2}$ Werner states do not violate any known Bell inequalities [42] but nevertheless they can be detected with the witnesses OEW_4^{EB} for $p>\frac{1}{2}$. To see this, note that the operator $\Omega=1/4(\rho_W+\rho_W^{T_A}+\rho_W^{T_B}+\rho_W^{T})$ is a nonpositive operator for $p>\frac{1}{2}$.

C. Two-state protocol

The two-state protocol [16] is one of the simplest QKD protocols, since it is based on the random transmission of only two nonorthogonal states $|\varphi_0\rangle$ and $|\varphi_1\rangle$. Alice chooses randomly a bit value i, and prepares a qubit in the state $|\varphi_i\rangle=\alpha|0\rangle+(-1)^i\beta|1\rangle$, with $0<\alpha<1/\sqrt{2}$ and $\beta=\sqrt{1-\alpha^2}$, that is sent it to Bob. On the receiving side, Bob measures the qubit he receives in a basis chosen, independently and at random, within the set $\{\{|\varphi_0\rangle,|\varphi_0^{\perp}\rangle\},\{|\varphi_1\rangle,|\varphi_1^{\perp}\rangle\}\}$, with $|\langle\varphi_i|\varphi_i^{\perp}\rangle|=0$. Note that alternatively to this detection method, Bob could also perform a POVM defined by the operators $F_0=|\varphi_1^{\perp}\rangle\langle\varphi_1^{\perp}|/2$, $F_1=|\varphi_0^{\perp}\rangle\langle\varphi_0^{\perp}|/2$, and $F_{null}=\mathbb{1}-F_0-F_1$. Using the ideas introduced by Bennett *et al.* [9], one can also think of the preparation process in the following way. Alice prepares an entangled bipartite state of the form

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|\varphi_0\rangle_B + |1\rangle_A|\varphi_1\rangle_B), \tag{15}$$

and then she measures her subsystem in the basis $\{|0\rangle,|1\rangle\}$. Note that in this scheme the fact that the reduced density matrix of Alice is fixed and equal to $\rho_A=\mathrm{Tr}_B(|\Psi\rangle\langle\Psi|_{AB})$ with $|\Psi\rangle_{AB}$ given by Eq. (15) is vital to detect quantum correlations in $P(A,B)$. Otherwise, the joint probability distribution $P(A,B)$ alone does not allow Alice and Bob to distinguish between the entangled state $|\Psi\rangle_{AB}$ and the separable one $\sigma_{AB}=\frac{1}{2}\sum_{i=0}^{1}|i\rangle\langle i|_A\otimes|\varphi_i\rangle\langle\varphi_i|$.

We obtain, therefore, that the set of EWs that can be evaluated in the two-state protocol, and which we shall denote as W_2, is of the form

$$W_2 = \sum_{\substack{i=\{0,z\}\\ j=\{x,z\}}} c_{ij}\sigma_i\otimes\sigma_j + \sum_{k=\{0,x,z,y\}} c_k\sigma_k\otimes\sigma_0, \tag{16}$$

where the second term in Eq. (16) includes a set of observables such that Alice can reconstruct completely the state of her subsystem. This family of witness operators can equivalently be rewritten as

$$W_2 = |0\rangle\langle 0|\otimes A + |1\rangle\langle 1|\otimes B + x\,C(\theta), \tag{17}$$

where A and B represent two real symmetric operators $A=A^T$ and $B=B^T$, given by

$$A = \sum_{i=\{0,x,z\}} (c_{0i}+c_{zi})\sigma_i \tag{18}$$

and

$$B = \sum_{i=\{0,x,z\}} (c_{0i}-c_{zi})\sigma_i, \tag{19}$$

respectively, the parameter x is given by $x=|c_x+ic_y|\geqslant 0$, and

$$C(\theta) = \left(\begin{array}{c|c} 0 & e^{i\theta}\,\mathbb{1} \\ \hline e^{-i\theta}\,\mathbb{1} & 0 \end{array}\right), \tag{20}$$

with $\theta=\tan^{-1}(c_y/c_x)$. That is, we have included the two observables $\sigma_x\otimes\mathbb{1}$ and $\sigma_y\otimes\mathbb{1}$ that appear in Eq. (16) in the term $x\,C(\theta)$ of Eq. (17), while the remaining observables in Eq. (16) are included in the first two terms $|0\rangle\langle 0|\otimes A+|1\rangle\langle 1|\otimes B$ of Eq. (17).

It is straightforward to see that, as in the case of the four-state (EB and PM) protocol, the class of witness operators W_2 does not allow us to evaluate the OEW given in Eq. (6). Note that the elements W in OEW satisfy $W\ngeqslant 0$ and $W^{T_P}\geqslant 0$. The witnesses in the class W_2, on the contrary, satisfy $W_2=W_2^{T_B}$, which means that $W_2^{T_B}$ cannot be a positive semidefinite operator unless W_2 is also positive semidefinite. Therefore, in the two-state protocol there can be also entangled states that give rise to correlations $P(A,B)$ that are not sufficient to prove the presence of entanglement. In the same way, it is interesting to note also that there are no witnesses in the set of W_2 that belongs to the family of

OEW$_4^{EB}=\frac{1}{2}(|\phi_e\rangle\langle\phi_e|+|\phi_e\rangle\langle\phi_e|^{T_P})$. To see this, note that the representation given in Eq. (17) is incompatible with the fact that the state $|\phi_e\rangle$ is a real entangled state. In the rest of this section we obtain a reduced verification set of the two-state protocol (Theorem 4).

The first requirement that an operator of the form given by Eq. (17) must satisfy to be an EW is $\mathrm{Tr}(W_2\sigma)\geqslant 0$ for all separable states σ. Since the set of separable states is convex, this condition is equivalent to asking $\mathrm{Tr}(W_2|\phi\rangle\langle\phi|_A\otimes|\psi\rangle\times\langle\psi|_B)\geqslant 0$ for all states $|\phi\rangle_A|\psi\rangle_B$. Let us start by considering states of the form $|0\rangle_A|\psi\rangle_B$. We have that $\mathrm{Tr}(W_2|0\rangle\langle 0|_A\otimes|\psi\rangle\times\langle\psi|_B)=\langle\psi|A|\psi\rangle$, which means that the operator A must be positive semidefinite, i.e., $A\geqslant 0$. In the same way, but now using the separable pure states $|1\rangle_A|\psi\rangle_B$, one obtains $B\geqslant 0$. This means that the first two terms of Eq. (17), $|0\rangle\langle 0|\otimes A+|1\rangle\langle 1|\otimes B$, represent a positive semidefinite operator and the only term responsable to detect quantum correlations is the one given by $xC(\theta)$. Note that this implies that the class W_2 does not allow us to detect maximally entangled states $|\phi_e\rangle=1/\sqrt{2}\Sigma_{i=0}^{1}|\psi_i\rangle|\varphi_i\rangle$, with $\langle\psi_i|\psi_j\rangle=\langle\varphi_i|\varphi_j\rangle=\delta_{ij}$, since in that case it turns out that $\langle\phi_e|C(\theta)|\phi_e\rangle=0$. This fact is not too surprising since the distributed states in this protocol are not maximally entangled. Let us now come back to the general case: $\mathrm{Tr}(W_2|\phi\rangle\langle\phi|_A\otimes|\psi\rangle\langle\psi|_B)\geqslant 0$. If we express the state $|\phi\rangle_A$ as $|\phi\rangle_A=\alpha|0\rangle+\beta|1\rangle$, this condition reduces to

$$2|\alpha\beta|x\leqslant\langle\psi|(|\alpha|^2A+|\beta|^2B)|\psi\rangle,\quad\forall\,|\psi\rangle,\tag{21}$$

and for all α and β such that $|\alpha|^2+|\beta|^2=1$. After optimizing over the parameters α and β, Eq. (21) can be further simplified to

$$x\leqslant\min_{|\psi\rangle}\sqrt{\langle\psi|A|\psi\rangle\langle\psi|B|\psi\rangle}.\tag{22}$$

That is, whenever the value of the parameter x is below the bound given by Eq. (22), W_2 has a positive expectation value on all separable states.

Now we will provide a necessary and sufficient condition for the operators W_2 in order to detect entanglement, i.e., to guarantee $W_2\ngeq 0$. First, it is straightforward to see that the operators A and B have to be of full rank, otherwise according to Eq. (22) we have $x=0$ and $W_2=|0\rangle\langle 0|\otimes A+|1\rangle\langle 1|\otimes B\geqslant 0$. Now we can prove the following observation.

Observation 5. An operator $W_2=|0\rangle\langle 0|\otimes A+|1\rangle\langle 1|\otimes B+xC(\theta)$, with A and B being two real symmetric positive operators, $A>0$ and $B>0$, and the operator $C(\theta)$ given by Eq. (20) with $\theta\in[0,2\pi)$ satisfies $W_2\ngeq 0$ if and only if $x>x_{min}$ with

$$x_{min}=\sqrt{\frac{\alpha}{2}-\sqrt{\frac{\alpha^2}{4}-\det(A)\det(B)}},\tag{23}$$

and where $\alpha=\mathrm{Tr}(AB)$.

Proof. See Appendix A.

Theorem 4. The family of witness operators $W_2=|0\rangle\langle 0|\otimes A+|1\rangle\langle 1|\otimes B+xC(\theta)$, with A and B being two real symmetric positive operators, $A>0$ and $B>0$, the operator $C(\theta)$ given by Eq. (20) with $\theta\in[0,2\pi)$, and such that $x=\min_{|\psi\rangle}\sqrt{\langle\psi|A|\psi\rangle\langle\psi|B|\psi\rangle}>x_{min}$ is sufficient to detect all entangled states that can be detected in the two-state protocol.

Proof. According to the results presented above, we only need to prove that given a witness operator $W_2\ngeq 0$ with a value of x that saturates the bound of Eq. (22), and that we shall denote as $W_2(x_{max})$, it is finer than the same witness $W_2(x)$ with an $x<x_{max}$. That is,

$$\mathrm{Tr}[W_2(x_{max})\rho]\leqslant\mathrm{Tr}[W_2(x)\rho]\tag{24}$$

for all ρ entangled and detected by $W_2(x)$. Since $W_2(x_{max})$ and $W_2(x)$ share the same operators A and B by definition, Eq. (24) can be further simplified to

$$(x_{max}-x)\mathrm{Tr}[C(\theta)\rho]\leqslant 0.\tag{25}$$

Finally note that this condition is always satisfied, since $(x_{max}-x)>0$ and $\mathrm{Tr}[C(\theta)\rho]<0$, otherwise ρ cannot be detected by $W_2(x)$. ■

The coefficients of the pseudomixture decomposition of the witness operators given by Theorem 4 can be parametrized in this case with six real parameters.

D. Higher-dimensional QKD protocols

So far we have searched for quantum correlations in qubit-based QKD protocols which means we have restricted ourselves to operators in $\mathbb{C}^2\otimes\mathbb{C}^2$. This fact makes the characterization of a given class of witness operators easier, since for systems defined in $H=\mathbb{C}^2\otimes\mathbb{C}^2$ and $H=\mathbb{C}^2\otimes\mathbb{C}^3$ all witness operators belong to the class of so-called *decomposable entanglement witnesses* (DEWs) which has a simple well-known form: $W=\epsilon P+(1-\epsilon)Q^{T_P}$, with $P\geqslant 0$ and $Q\geqslant 0$ satisfying $\mathrm{Tr}(P)=\mathrm{Tr}(Q)=1$, and $\epsilon\in[0,1)$ [43]. In the case of systems of higher dimension than those in $H=\mathbb{C}^2\otimes\mathbb{C}^2$ and $H=\mathbb{C}^2\otimes\mathbb{C}^3$ not all the witness operators are DEWs; for example DEWs cannot detect PPT entangled states [23]. It is necessary to use also the so-called *nondecomposable entanglement witnesses* (NDEWs). This fact makes the characterization of witness operators more subtle and so far it is still not clear how to construct such witness operators even when the information about the state is tomographic complete [14,15,44]. As we mentioned already before, ideally the goal is to obtain a compact description of the minimal verification set for a given QKD protocol in order to systematically search for entanglement in $P(A,B)$. However, due to the fact that the characterization of NDEWs is not easy to handle it might be of interest to obtain, at least, *one* relevant EW within the proper class as a first step toward the demonstration of successful QKD.

Recently, it has been shown that a good deal of new insight into the optimization of NDEWs can come from the theory of convex optimization [17,45,46]. More important for QKD, the problem of the minimization of expectation values of witness operators W with respect to pure product states,

$$\min_{|a,b\rangle}\mathrm{Tr}(W|a,b\rangle\langle a,b|),\tag{26}$$

can also be formulated as a convex optimization problem [17]. Solving Eq. (26) allows us to obtain new witness operators which are finer than W, even within a restricted class

$W_{\mathcal{C}}$ of them [17]. To see this, let $W \in W_{\mathcal{C}}$ and denote the result of the minimization problem in Eq. (26) as $\epsilon = \min_{|a,b\rangle} \mathrm{Tr}[|a,b\rangle\langle a,b|W] > 0$. Then the unnormalized new witness operator given by $\widetilde{W} = W - \epsilon\mathbb{1}$ is finer than W and moreover it is guaranteed that $\widetilde{W} \in W_{\mathcal{C}}$ since the observable $\mathbb{1}$ is always accessible. At first sight it seems that this procedure requires one to have already a valid entanglement witness W for the given QKD protocol. However, this operator does not need to be an entanglement witness in the strict sense, but can be also a positive operator from the restricted set which is more easy to characterize than an entanglement witness [47]. With respect to the minimization problem itself, it has been shown that although the polynomial constraints parametrizing the pure states $|a,b\rangle$ are nonconvex and computationally expensive to handle, one can apply results from relaxation theory of nonconvex problems [48,49], notably the method of Lasserre [49], to find hierarchies of solutions to that problem in such a way that each step of the hierarchy is a better approximation than the previous one [17]. Each step itself amounts to solving an efficiently implementable semidefinite program [50] and the hierarchy is asymptotically complete, in the sense that the exact solution is asympotically attained. This means that during several steps of the optimization method, better witness operators $\widetilde{W}$ can be obtained from W, belonging to the same restricted class $W_{\mathcal{C}}$.

Finally, let us mention that, of course, not all higher-dimensional QKD protocols require the use of NDEWs to derive a necessary and sufficient condition for the presence of entanglement in $P(A,B)$. For instance, consider the class of EB protocols in $H = \mathbb{C}^2 \otimes \mathbb{C}^N$, where Alice realizes projection measurements onto the eigenvectors of the two Pauli operators σ_x and σ_z. In all these EB protocols the accessible witness operators satisfy the condition $W = W^{T_A}$. One can show that this fact implies for the given dimensionalities that it is a necessary condition for a state ρ to be detected by W that the operator $\Omega = \frac{1}{2}(\rho + \rho^{T_A})$ is a nonpositive operator. To prove this, note that $\mathrm{Tr}(W\rho) = \mathrm{Tr}(W\Omega)$. From the work by Kraus *et al.* [53] we learn that whenever Ω is a non-negative operator it represents a separable state. To summarize this remark, we learn that all detectable states for this class of protocols are negative partial transposed entangled states and can be detected by using *only* DEWs. The situation changes once Alice performs also a projection measurement onto the eigenvectors of σ_y.

E. Outlook to practical QKD systems

The idea to check for quantum correlations in the observed data with the help of a verification set of witnesses applies also, in principle, to real implementations of QKD setups [51]. One can incorporate any imperfection of the sources and the detection devices into the corresponding investigation within the framework of trusted devices. In that framework one characterizes detection devices by the use of an appropriate POVM description, e.g., on the infinite dimensional Hilbert space of optical modes. For PM schemes, one has to characterize additionally the given source via the reduced density matrix of the virtual internal preparation state, as described before. This idea then needs to be generalized to signal states that are described by mixed quantum states. For this purpose, one uses still a pure state as internal preparation, but Alice's signal preparation corresponds now no longer to a projection onto an orthogonal set of pure states, but to projections onto orthogonal subspaces, thereby effectively preparing mixed states.

In those general scenarios, it will be difficult to provide the minimal verification set of witnesses. Instead, one can fall back to the approach to search for just one accessible witness via numerical methods such as presented in the previous section. In this way, one can search through restricted classes of accessible witnesses at the price that the result of this search will not be conclusive, i.e., this search yields only a sufficient condition.

V. CONCLUSION

A necessary precondition for secure quantum key distribution is that sender and receiver can use their available measurement results to prove the presence of entanglement in a quantum state that is effectively distributed between them. Moreover, this result applies both to prepare and measure (PM) and to entanglement-based (EB) schemes. This means that to construct practical and efficient new QKD protocols, it is vital to separate the generation of two-party correlations from the public discussion protocol which extracts a key from those data. Among all separability criteria to deliver this necessary entanglement proof, entanglement witnesses (EWs) are especially appropriate since from them one can derive a necessary and sufficient condition for the existence of quantum correlations even when the state shared by the users cannot be completely reconstructed.

In a recent work [10], the set of optimal witness operators for two well-known EB schemes, the six-state and the four-state EB protocols, was obtained and a necessary and sufficient condition to detect entanglement in both protocols was derived. The purpose of this paper was to complete these results, now showing specifically the analysis for the case of PM schemes where, contrary to the case of EB schemes, now the reduced density matrix of the sender is fixed and cannot be modified by the eavesdropper. In particular, we have investigated the signal states and detection methods of the four-state and the two-state PM schemes, and we have obtained a reduced set of EWs that can be used to provide a necessary and sufficient condition for the existence of quantum correlations in both protocols.

Finally, we have discussed very briefly how to detect quantum correlations in higher-dimensional QKD schemes and in practical QKD, where the characterization of EWs is not as easy to handle as in the case of qubit-based QKD schemes. In this scenario it might be still of interest to obtain one relevant EW as a first step toward the demonstration of successful QKD. Here, mathematical results from the field of convex optimization theory can be used to get new insights into the construction of finer EWs within a given class.

ACKNOWLEDGMENTS

The authors wish to thank A. Dolinska, Ph. Raynal, and especially K. Tamaki for very useful discussions, P. van

Loock for his comments on the manuscript, and P. Horodecki for helpful discussions about Sec. II. This work has been supported by the DFG (Emmy Noether program and the Graduiertenkolleg 282), the European Commission (Integrated Project SECOQC), and the network of competence QIP of the state of Bavaria.

APPENDIX: CONDITION FOR $W_2 \not\geqslant 0$

In this appendix we provide a proof for Observation 5. Our starting point is the most general form of the operators $W_2 = |0\rangle\langle 0| \otimes A + |1\rangle\langle 1| \otimes B + xC(\theta)$. That is, if we write the matrix element of W_2 explicitly we have

$$W_2 = \begin{pmatrix} a & c & xe^{i\theta} & 0 \\ c & b & 0 & xe^{i\theta} \\ xe^{-i\theta} & 0 & e & g \\ 0 & xe^{-i\theta} & g & f \end{pmatrix}. \tag{A1}$$

Now we have to understand what the condition $W_2 \geqslant 0$ imposes on the elements of W_2. We have by definition of the class W_2 $A \geqslant 0$ and $B \geqslant 0$ or, since A and B are of full rank, we can assume at this point $A > 0$ and $B > 0$. Under this assumption, we can use the well-known fact that such a block matrix as in Eq. (A1) is positive if and only if its Schur complement is positive [52], which implies here

$$A - x^2 B^{-1} \geqslant 0. \tag{A2}$$

Introducing the notation $y = x^2/\det(B)$ the 2×2 matrix

$$X = \begin{pmatrix} a - yf & c + yg \\ c + yg & b - ye \end{pmatrix} \geqslant 0 \tag{A3}$$

has to be positive. This is the case, if and only if $\det(X) \geqslant 0$ and $\mathrm{Tr}(X) \geqslant 0$. After a short calculation, this implies that

$$ab - c^2 - (ae + bf + 2cg)y + (ef - g^2)y^2 \geqslant 0, \tag{A4}$$

$$(a + b) - y(e + f) \geqslant 0. \tag{A5}$$

When are these inequalities satisfied for different values of $y \geqslant 0$? For $y = 0$ the matrix X is clearly positive. If y increases X get first one negative eigenvalue. Thus Eq. (A4) is violated, while Eq. (A5) is still valid. If y increases further, the eigenvalues decrease and Eq. (A5) gets violated. Finally, X gets two negative eigenvalues, and Eq. (A4) is valid, while Eq. (A5) is still violated. So we have to look for the smallest zero of Eq. (A4) which is given by

$$y_0 = \frac{\alpha}{2\det(B)} - \sqrt{\frac{\alpha^2}{4\det(B)^2} - \frac{\det(A)}{\det(B)}}, \tag{A6}$$

where we have used $\alpha = \mathrm{Tr}(AB) = (ae + bf + 2cg)$. We obtain, therefore, that W_2 is positive if and only if

$$x \leqslant x_{min}, \tag{A7}$$

with

$$x_{min} = \sqrt{\frac{\alpha}{2} - \sqrt{\frac{\alpha^2}{4} - \det(A)\det(B)}}. \tag{A8}$$

[1] B. Schneier, *Applied Cryptography*, 2nd ed. (John Wiley & Sons, Inc., New York, 1996); A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, FL, 1996).

[2] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[3] G. S. Vernam, Trans. Am. Inst. Electr. Eng. **45**, 295 (1926).

[4] It is necessary to require an initial secret key to authenticate the public communication channel between Alice and Bob. They need to be sure that Eve is not trying to impersonate them ("man-in-the-middle attack").

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

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

[7] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[8] N. Lütkenhaus, Appl. Phys. B: Lasers Opt. **69**, 395 (1999).

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

[10] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[11] N. Gisin and S. Wolf, in *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science Vol. 1880 (Springer, Berlin, 2000), p. 482.

[12] M. Horodecki, P. Horodecki, and R. Horodecki, in *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*, edited by G. Alber *et al.* (Springer, Heidelberg, 2001), p. 151; M. Lewenstein, D. Bruß, J. I. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera, and R. Tarrach, J. Mod. Opt. **47**, 2841 (2000); K. Eckert, O. Gühne, F. Hulpke, P. Hyllus, J. Korbicz, J. Mompart, D. Bruß, M. Lewenstein, and A. Sanpera, in *Quantum Information Processing*, edited by G. Leuchs and T. Beth (Wiley-VCH, Weinheim, 2003), p. 79.

[13] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[14] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).

[15] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).

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

[17] J. Eisert, P. Hyllus, O. Gühne, and M. Curty, Phys. Rev. A **70**, 062317 (2004).

[18] U. Maurer and S. Wolf, IEEE Trans. Inf. Theory **45**, 499 (1999).

[19] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997); D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *ibid.* **77**, 2818 (1996).

[20] N. Gisin and S. Wolf, Phys. Rev. Lett. **83**, 4200 (1999); D. Bruß, M. Christandl, A. Ekert, B. G. Englert, D. Kaszlikowski, and C. Macchiavello, *ibid.* **91**, 097901 (2003); A. Acín, N. Gisin, and V. Scarani, Quantum Inf. Comput. **3**, 563 (2003).

[21] A. Acín, L. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).

[22] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004); e-print quant-ph/0306078.

[23] P. Horodecki, Phys. Lett. A **232**, 333 (1997).

[24] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, e-print quant-ph/0309110.

[25] A. Acín and N. Gisin, e-print quant-ph/0310054.

[26] R. Renner and S. Wolf, in *Proceedings of EUROCRYPT 2003*, Lecture Notes in Computer Science Vol. 2656 (Springer-Verlag, Berlin, 2003), p. 562.

[27] A. Acín, J. I. Cirac, and Ll. Masanes, Phys. Rev. Lett. **92**, 107903 (2004).

[28] R. Augusiak and P. Horodecki, e-print quant-ph/0405187.

[29] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964); J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969); **24**, 549 (1970); C. Śliwa, Phys. Lett. A **317**, 165 (2003); D. Collins and N. Gisin, J. Phys. A **37**, 1775 (2004).

[30] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003); O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004); V. Giovannetti, Phys. Rev. A **70**, 012102 (2004); O. Gühne and M. Lewenstein, *ibid.* **70**, 022316 (2004).

[31] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999); N. J. Cerf, C. Adami, and R. M. Gingrich, *ibid.* **60**, 898 (1999).

[32] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).

[33] Given an operator $O \in H_{AB}$ and an orthonormal basis $\{|\alpha_i\rangle\} \in H_B$, with $i=1,\ldots,N$, the partial transposed of O with respect to the subsystem B in that basis is defined as$O^{T_B} = \Sigma_{i,j=1}^{N} \langle\alpha_i|O|\alpha_j\rangle|\alpha_j\rangle\langle\alpha_i|$.In the same way, one can also define the partial transposed of O with respect to the subsystem A.

[34] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[35] G. Strang, *Linear Algebra and Its Applications*, 2nd ed. (Academic Press, New York, 1980).

[36] M. Horodecki, P. W. Shor, and M. B. Ruskai, Rev. Math. Phys. **15**, 629 (2003); M. B. Ruskai, *ibid.* **15**, 643 (2003).

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

[38] G. M. Nikolopoulos and G. Alber, e-print quant-ph/0403148.

[39] A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A **58**, 826 (1998); O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, *ibid.* **66**, 062305 (2002).

[40] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998); T. Wellens and M. Kuś, Phys. Rev. A **64**, 052302 (2001).

[41] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

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

[43] S. L. Woronowicz, Rep. Mod. Phys. **10**, 165 (1976).

[44] S. L. Woronowicz, Commun. Math. Phys. **51**, 243 (1976); P. Kryszyński and S. L. Woronowicz, Lett. Math. Phys. **3**, 319 (1979); M. D. Choi, Proc. Symp. Pure Math. **38**, 583 (1982).

[45] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002); Phys. Rev. A **69**, 022308 (2004); e-print quant-ph/0407143.

[46] F. G. S. L. Brandao and R. O. Vianna, e-print quant-ph/0405008; e-print quant-ph/0405063.

[47] G. Kimura, Phys. Lett. A **314**, 339 (2003); M. S. Byrd and N. Khaneja, Phys. Rev. A **68**, 062322 (2003).

[48] N. Z. Shor, Sov. J. of Circuits Syst. Sci. **25**, 1 (1987); M. Kojima and L. Tuncel, Math. Program. **89**, 79 (2000); A. Takeda, K. Fujisawa, Y. Fukaya, and M. Kojima, J. Global Optim. **24**, 237 (2002); M. Kojima, S. Kim, and H. Waki, J. Oper. Res. Soc. Jpn. **46**, 125 (2003); D. Henrion and J. B. Lasserre, IEEE Control Syst. Mag. **24**, 72 (2004); P. A. Parrilo, Ph.D thesis, California Institute of Technology, Pasadena, CA, 2000.

[49] J. B. Lasserre, SIAM J. Optim. **11**, 796 (2001).

[50] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996); C. Helmberg, Eur. J. Oper. Res. **137**, 461 (2002).

[51] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995); T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000); D. S. Bethune, M. Navarro, and W. P. Risk, Appl. Opt. **41**, 1640 (2002); R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002); D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, *ibid.* **4**, 41 (2002); C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature (London) **419**, 450 (2002).

[52] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, U.K., 1985); G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. Lett. **87**, 167904 (2001).

[53] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, Phys. Rev. A **61**, 062302 (2000).