Single-photon quantum key distribution in the presence of loss

Marcos Curty[1,2] and Tobias Moroder[2,3]
[1]*Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario, Canada M5S 3G4*
[2]*Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1*
[3]*Quantum Information Theory Group, Institut für Theoretische Physik I, and Max-Planck Research Group, Institute of Optics, Information and Photonics, Universität Erlangen-Nürnberg, D-91058 Erlangen, Germany*
(Received 14 November 2006; published 31 May 2007)

We investigate two-way and one-way single-photon quantum key distribution (QKD) protocols in the presence of loss introduced by the quantum channel. Our analysis is based on a simple precondition for secure QKD in each case. In particular, the legitimate users need to prove that there exists no separable state (in the case of two-way QKD), or that there exists no quantum state having a symmetric extension (one-way QKD), that is compatible with the available measurements results. We show that both criteria can be formulated as a convex optimization problem known as a semidefinite program, which can be efficiently solved. Moreover, we prove that the solution to the dual optimization corresponds to the evaluation of an optimal witness operator that belongs to the minimal verification set of them for the given two-way (or one-way) QKD protocol. A positive expectation value of this optimal witness operator states that no secret key can be distilled from the available measurements results. We apply such analysis to several well-known single-photon QKD protocols under losses.

DOI: 10.1103/PhysRevA.75.052336 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Mn

I. INTRODUCTION

Quantum key distribution (QKD) protocols typically involve a two-step procedure in order to generate a secret key [1,2]. First, the legitimate users (Alice and Bob) perform a set of measurements on effective bipartite quantum states that are distributed to them. As a result, they end up with a classical joint probability distribution, that we shall denote as $p(a_i,b_j)\equiv p_{ij}$, describing their outcomes. The second step consists of a classical post-processing of the data p_{ij}. It requires an authenticated classical channel, and it includes post-selection of data, error-correction to reconcile the data, and privacy amplification to decouple the data from a possible eavesdropper (Eve) [1,2].

In order to create the correlated data p_{ij}, QKD schemes usually require Alice to prepare some nonorthogonal quantum states $|\psi_i\rangle$ with *a priori* probabilities p_i that are sent to Bob. On the receiving side, Bob measures each received signal with a *positive operator value measure* (POVM) $\{B_j\}$. Generalizing the ideas introduced by Bennett *et al.* in Ref. [3], the signal preparation process in this kind of scheme can alternatively be thought of as follows: Alice produces first bipartite states $|\psi_{source}\rangle_{AB}=\Sigma_i\sqrt{p_i}|\alpha_i\rangle_A|\psi_i\rangle_B$ and, afterwards, she measures the first subsystem in the orthogonal basis $|\alpha_i\rangle_A$ corresponding to the measurement operators $A_i=|\alpha_i\rangle_A\langle\alpha_i|$. This action generates the signal states $|\psi_i\rangle$ with *a priori* probabilities p_i. The reduced density matrix of Alice, $\rho_A=\text{Tr}_B(|\psi_{source}\rangle_{AB}\langle\psi_{source}|)$, depends only on the probabilities p_i and on the overlap of the signals states $|\psi_i\rangle$. This means, in particular, that ρ_A is always fixed by the preparation process and cannot be modified by Eve. In order to include this information in the measurement process one can add to the observables $\{A_i\otimes B_j\}$, measured by Alice and Bob, other observables $\{C_k\otimes \mathbb{1}\}$ such that the observables $\{C_k\}$ form a tomographic complete set of Alice's Hilbert space [4]. From now on, we will consider that the data p_{ij} and the POVM $\{A_i\otimes B_j\}$ include also the observables $\{C_k\otimes \mathbb{1}\}$.

The classical post-processing of p_{ij} can involve either two-way or one-way classical communication. Two-way classical communication protocols can tolerate a higher error rate than one-way communication techniques [5]. On the other hand, one-way post-processing methods typically allow us to derive simpler unconditional security proofs for QKD than those based on two-way communication [6–9]. In this last paradigm, two different cases can be considered: *reverse reconciliation* (RR) refers to communication from Bob to Alice, and *direct reconciliation* (DR) permits only communication from Alice to Bob. (See, for instance, Refs. [10,11].)

An essential question in QKD is to determine whether the correlated data p_{ij} allow Alice and Bob to generate a secret key at all during the second phase of QKD. Here we consider the so-called *trusted device scenario*, where Eve cannot modify the actual detection devices employed by Alice and Bob, as used in Refs. [12,13]. We assume that the legitimate users have complete knowledge about their detection devices, which are fixed by the actual experiment. The case of two-way classical post-processing has been analyzed in Ref. [13], where it was proven that a necessary precondition for secure two-way QKD is the provable presence of quantum correlations in p_{ij}. That is, it must be possible to interpret p_{ij}, together with the knowledge of the corresponding observables $\{A_i\otimes B_j\}$, as coming *exclusively* from an entangled state. Otherwise, no secret key can be distilled from p_{ij}. In order to deliver this entanglement proof any separability criteria (see, for instance, Ref. [14], and references therein) might be employed. The important question here is whether the chosen criterion can provide a necessary and sufficient condition to detect entanglement even when the knowledge about the quantum state is not tomographic complete. It was proven in Ref. [13] that entanglement witnesses (EWs) fulfill this condition. An EW is a Hermitian operator W with a positive expectation value on all separable states [13,15–17]. So, if a state ρ_{AB} obeys $\mathrm{Tr}(\rho_{AB}W)<0$, the state ρ_{AB} must be entangled. With this separability criterion, Refs. [4,13] analyzed three well-known qubit-based QKD schemes, and provided a compact description of a minimal verification set of EWs (i.e., one that does not contain any redundant EW) for the four-state [18] and the six-state [19] QKD protocols, and a reduced verification set of EWs (i.e., one which may still include some redundant EWs) for the two-state [20] QKD scheme, respectively. These verification sets of EWs allow a systematic search for quantum correlations in p_{ij}. One negative expectation value of one EW in the set suffices to detect entanglement. To guarantee that no verifiable entanglement is present in p_{ij}, however, it is necessary to test *all* the members of the set. Unfortunately, to find a minimal verification set of EWs, even for ideal qubit-based QKD schemes, is not always an easy task, and it seems to require a whole independent analysis for each protocol, let alone for higher dimensional QKD schemes [4,13]. (See also Ref. [21].) Also, one would like to include in the analysis the attenuation introduced by the quantum channel, not considered in Refs. [4,13], and which represents one of the main limitations for optical realizations of QKD.

One central observation of this paper is very simple, yet potentially very useful: given *any* qubit-based two-way QKD scheme, one can search for quantum correlations in p_{ij} by just applying the *positive partial transposition* (PPT) criterion [15,22] adapted to the case of a quantum state that cannot be completely reconstructed. This criterion provides a necessary and sufficient entanglement verification condition for any qubit-based QKD protocol even in the presence of loss introduced by the channel, since, in this scenario, only *nonpositive partial transposed* (NPT) entangled states exist. Moreover, it is rather simple to evaluate in general since it can be cast into the form of a convex optimization problem known as semidefinite program (SDP) [23,24]. Such instances of convex optimization problems can be solved efficiently, for example by means of interior-point methods [23,24]. This means, in particular, that this criterion can be applied to any qubit-based QKD scheme in a completely systematic way.

One-way QKD schemes can be analyzed as well with SDP techniques. It was shown in Ref. [25] that a necessary precondition for one-way QKD with RR (DR) is that Alice and Bob can prove that there exists no quantum state having a symmetric extension to two copies of system A (system B) that is compatible with the observed data p_{ij}. These kinds of states (with symmetric extensions) have been analyzed in detail in Refs. [26–28], where it was proven that the search for symmetric extensions for a given quantum state can be stated as a SDP. (See also Refs. [29,30].) Here we complete the results contained in Ref. [25], now presenting specifically the analysis for the case of a lossy channel.

Both QKD verification criteria mentioned above, based on SDP techniques, also provide a means to search for witness operators for a given two-way or one-way QKD protocol in a similar spirit as in Refs. [4,13]. Any SDP has an associated dual problem that represents also a SDP [23,24]. This dual problem can be used to obtain a certificate of infeasibility whenever the primal problem is actually infeasible. Most importantly, it can be proven that the solution to this dual problem corresponds to the evaluation of an optimal witness operator, that belongs to the minimal verification set of them for the given protocol, on the observed data p_{ij}. A positive expectation value of this optimal witness operator indicates that no secret key can be distilled from the observed data p_{ij}.

The paper is organized as follows. In Sec. II we introduce the QKD verification criteria for two-way and one-way QKD in more detail, and we show how to cast them as primal SDPs. Then, in Sec. III, we present the dual problems associated to these primal SDPs, and we show that the solution to these dual problems corresponds to evaluating an optimal witness operator on the observed data p_{ij} for the given protocol. These results are then illustrated in Sec. IV, where we investigate in detail the two-state QKD protocol [20] in the presence of loss. The analysis for other qubit-based QKD schemes is completely analogous, and we include very briefly the results of our investigations on other QKD protocols in Appendix B. Finally, Sec. V concludes the paper with a summary.

II. QKD VERIFICATION CRITERIA

Our starting point is the observed joint probability distribution p_{ij} obtained by Alice and Bob after their measurements $\{A_i \otimes B_j\}$. This probability distribution defines an equivalence class $\mathcal{S}$ of quantum states that are compatible with it,

$$\mathcal{S}=\{\rho_{AB}|\mathrm{Tr}(A_i\otimes B_j\rho_{AB})=p_{ij},\ \ \forall\, i,j\}. \tag{1}$$

By definition, every $\rho_{AB}\in\mathcal{S}$ can represent the state shared by Alice and Bob before their measurements.

In single-photon QKD schemes in the presence of loss, any state $\rho_{AB}\in\mathcal{S}$ can be described on a Hilbert space $\mathcal{H}_2^A\otimes\mathcal{H}_3^B$, with $\mathcal{H}_2^A$ and $\mathcal{H}_3^B$ denoting, respectively, Alice's and Bob's Hilbert spaces, and where the subscript indicates the dimension of the corresponding Hilbert space. To see this, we follow the signal preparation model introduced previously, where Alice prepares states $|\psi_{source}\rangle_{AB}=\sum_{i=0}^{N-1}\sqrt{p_i}|\alpha_i\rangle_A|\psi_i\rangle_B\in\mathcal{H}_N^A\otimes\mathcal{H}_2^B$, and, afterwards, she measures the first subsystem in the orthogonal basis $|\alpha_i\rangle_A$. Using Neumark's theorem [31,32], we can alternatively describe the preparation process as Alice producing first bipartite states on $\mathcal{H}_2^A\otimes\mathcal{H}_2^B$ and, afterwards, she measures the first subsystem with a POVM $\{A_i\}_{i=0}^{N-1}$. (See also Ref. [33].) To include the loss of a photon in the quantum channel, we simply enlarge Bob's Hilbert space from $\mathcal{H}_2^B$ to $\mathcal{H}_3^B$ by adding the vacuum state $|\mathrm{vac}\rangle_B$.

A. Two-way QKD

Let us now consider two-way QKD protocols. Whenever the observed joint probability distribution p_{ij}, together with the knowledge of the corresponding measurements performed by Alice and Bob, can be interpreted as coming from a separable state σ_{sep} then no secret key can be distilled from the observed data [13]. In $\mathcal{H}_2^A\otimes\mathcal{H}_3^B$ only NPT entangled states exist and therefore a simple necessary and sufficient criterion to detect entanglement in this scenario is given by the PPT criterion [15,22]: a state $\rho_{AB} \in \mathcal{H}_2^A \otimes \mathcal{H}_3^B$ is separable if and only if its partial transpose ρ_{AB}^{Γ} is a positive operator. Partial transpose means a transpose with respect to one of the subsystems [34]. Such a result is generally not true in higher dimensions.

Observation 1. Consider a qubit-based QKD scheme in the presence of loss where Alice and Bob perform local measurements with POVM elements A_i and B_j, respectively, to obtain the joint probability distribution of the outcomes p_{ij}. Then, the correlations p_{ij} can originate from a separable state if and only if there exists $\rho_{AB} \in \mathcal{S}$ such as $\rho_{AB}^{\Gamma} \geqslant 0$.

Proof. If p_{ij} can originate from a separable state, then there exists σ_{sep} such as $\sigma_{sep} \in \mathcal{S}$. Moreover, we have that any separable state satisfies $\sigma_{sep}^{\Gamma} \geqslant 0$. To prove the other direction, note that if there exists $\rho_{AB} \in \mathcal{S}$ such that $\rho_{AB}^{\Gamma} \geqslant 0$ then, since $\rho_{AB} \in \mathcal{H}_2^A \otimes \mathcal{H}_3^B$, we find that ρ_{AB} must be separable [15,22]. ■

To determine whether there exists $\rho_{AB} \in \mathcal{S}$ such as $\rho_{AB}^{\Gamma} \geqslant 0$ can be solved by means of a primal semidefinite program (SDP). This is a convex optimization problem of the following form:

$$\text{minimize } c^T\mathbf{x}$$

$$\text{subject to } F(\mathbf{x}) = F_0 + \sum_i x_i F_i \geqslant 0, \tag{2}$$

where the vector $\mathbf{x} = (x_1, \ldots, x_t)^T$ represents the objective variable, the vector c is fixed by the particular optimization problem, and where the matrices F_0 and F_i are Hermitian matrices. The goal is to minimize the linear function $c^T\mathbf{x}$ subjected to the linear matrix inequality (LMI) constraint $F(\mathbf{x}) \geqslant 0$ [23,24]. If the vector $c=0$, then the optimization problem given by Eq. (2) reduces to find whether the LMI constraint can be satisfied for some value of the vector $\mathbf{x}$ or not. In this case, the SDP is called a *feasibility problem*. Remarkably, SDPs can be solved with arbitrary accuracy in polynomial time, for example by means of interior-point methods [23,24].

According to Observation 1, we can find whether there exists a separable state that belongs to the equivalence class $\mathcal{S}$ just by solving the following feasibility problem [35]:

$$\text{minimize } 0$$

$$\text{subject to } \rho_{AB}(\mathbf{x}) \in \mathcal{S},$$

$$\rho_{AB}(\mathbf{x}) \geqslant 0,$$

$$\rho_{AB}^{\Gamma}(\mathbf{x}) \geqslant 0, \tag{3}$$

where the objective variable $\mathbf{x}$ is used to parametrize the density operators ρ_{AB}. The method used to parametrize ρ_{AB} is discussed in detail in Sec. II C.

B. One-way QKD

One-way RR (DR) QKD schemes require from Alice and Bob to show that there exists no quantum state $\rho_{AB} \in \mathcal{S}$ with a symmetric extension to two copies of system A (system B) [25]. A state ρ_{AB} is said to have a symmetric extension to two copies of system A if and only if there exists a tripartite state $\rho_{ABA'} \geqslant 0$, with $\text{Tr}(\rho_{ABA'}) = 1$, and where $\mathcal{H}^A \simeq \mathcal{H}^{A'}$, such that [26]

$$\text{Tr}_{A'}(\rho_{ABA'}) = \rho_{AB}, \tag{4}$$

$$P\rho_{ABA'}P = \rho_{ABA'}, \tag{5}$$

where the swap operator P satisfies $P|ijk\rangle_{ABA'} = |kji\rangle_{ABA'}$. This definition can be easily extended to cover also the case of symmetric extensions of ρ_{AB} to two copies of system B, and also of extensions of ρ_{AB} to more than two copies of system A or of system B [26].

To find whether $\rho_{AB} \in \mathcal{S}$ has a symmetric extension to two copies of system A can be solved with the following feasibility problem:

$$\text{minimize } 0$$

$$\text{subject to } \rho_{AB}(\mathbf{x}) \in \mathcal{S},$$

$$P\rho_{ABA'}(\mathbf{x})P = \rho_{ABA'}(\mathbf{x}),$$

$$\text{Tr}_{A'}[\rho_{ABA'}(\mathbf{x})] = \rho_{AB}(\mathbf{x}),$$

$$\rho_{ABA'}(\mathbf{x}) \geqslant 0. \tag{6}$$

Note that this SDP does not include the constraint $\rho_{AB}(\mathbf{x}) \geqslant 0$ because non-negativity of the extension $\rho_{ABA'}(\mathbf{x})$, together with the condition $\text{Tr}_{A'}[\rho_{ABA'}(\mathbf{x})] = \rho_{AB}(\mathbf{x})$, already implies non-negativity of $\rho_{AB}(\mathbf{x})$. The SDP for one-way QKD with DR can be obtained in a similar way.

C. Parametrization of the SDPs

To actually implement the SDPs given by Eqs. (3) and (6), one can parametrize ρ_{AB} and $\rho_{ABA'}$ such that some constraints are automatically fulfilled.

In particular, one can choose an operator basis of Hermitian matrices $\{\sigma_0, \ldots, \sigma_{d^2-1}\}$ for each Hilbert space $\mathcal{H}_d$. These matrices σ_i can be taken such as they satisfy the following two conditions: $\text{Tr}(\sigma_i) = d\delta_{0i}$, and $\text{Tr}(\sigma_i\sigma_j) = d\delta_{ij}$. In the case of qubit systems, the Pauli matrices $\{\sigma_0, \sigma_x, \sigma_y, \sigma_z\}$ can be selected, where the matrix σ_0 denotes the identity operator $\mathbb{1}$. For systems on $\mathcal{H}_3$, we can use the Gell-Mann operators, that we shall denote as $\{\sigma_i\}_{i=0}^{8}$. With this representation, a general state $\rho_{AB} \in \mathcal{H}_2^A \otimes \mathcal{H}_3^B$ can be written as

$$\rho_{AB} = \frac{1}{6} \sum_{\substack{k=\{0,x,y,z\} \\ l=0,\ldots,8}} x_{kl} S_{kl}, \tag{7}$$

where the operators $S_{kl} = \sigma_k^A \otimes \sigma_l^B$, the coefficients x_{kl} are given by $x_{kl} = \text{Tr}(S_{kl}\rho_{AB})$, and $x_{00} = \text{Tr}(\rho_{AB}) = 1$ because of normalization. Equation (7) allows us to describe any bipartite density operator in terms of a fixed number of real parameters x_{kl}.

The knowledge of Alice and Bob's POVMs $\{A_i\}$ and $\{B_j\}$, respectively, together with the observed probability distribution p_{ij} determines the equivalence class of compatible states $\mathcal{S}$. Each POVM element A_i and B_j can also be expanded in the appropriate operator basis as $A_i=\sum_{k=\{0,x,y,z\}}a_{ik}\sigma_k^A$, and $B_j=\sum_{l=0,\ldots,8}b_{jl}\sigma_l^B$, for some coefficients a_{ik} and b_{jl}, respectively. According to Eq. (1), to guarantee that $\rho_{AB}\in\mathcal{S}$ [first constraint in Eq. (3) and in Eq. (6)], we obtain that the coefficients x_{kl} must satisfy the following conditions:

$$\sum_{kl} a_{ik}b_{jl}x_{kl}=p_{ij} \quad \forall\, i,j. \tag{8}$$

That is, some coefficients x_{kl} are fixed by the known parameters a_{ik}, b_{jl}, and p_{ij}. Any operator $\rho_{AB}\in\mathcal{S}$ can then always be written in the following way [36]:

$$\rho_{AB}(\mathbf{x})=\rho_{\text{fix}}+\sum_{kl\notin I}x_{kl}S_{kl}, \tag{9}$$

where ρ_{fix} corresponds to the part of $\rho_{AB}(\mathbf{x})$ that is completely determined by the parameters a_{ik}, b_{jl}, and p_{ij}. It can be expressed as

$$\rho_{\text{fix}}=\sum_{kl\in I}x_{kl}S_{kl}, \tag{10}$$

where I denotes a multi-index set labeling those combinations of the indexes $k=\{0,x,y,z\}$ and $l=\{0,\ldots,8\}$ such that x_{kl} is fixed by Eq. (8). (See also Ref. [37].)

With this representation for $\rho_{AB}(\mathbf{x})$, the SDP given by Eq. (3) can now be written as [35]

$$\text{minimize } 0$$

$$\text{subject to } \rho_{AB}(\mathbf{x})\oplus\rho_{AB}^{\Gamma}(\mathbf{x})\geq 0, \tag{11}$$

where the symbol $\oplus$ denotes direct sum. Let us compare the second part of Eq. (2) with the second part of Eq. (11). The objective variables x_i are now given by the coefficients x_{kl} of $\rho_{AB}(\mathbf{x})$, with $kl\in I$, the matrix F_0 is given by $\rho_{\text{fix}}\oplus\rho_{\text{fix}}^{\Gamma}$, and the matrices F_i are those operators $S_{kl}\oplus S_{kl}^{\Gamma}$ with $kl\notin I$.

In the SDP given by Eq. (6) we need to parametrize as well the quantum state $\rho_{ABA'}$. The second constraint in Eq. (6) imposes that $\rho_{ABA'}$ must remain invariant under permutation of systems A and A'. This can be done with the following parametrization [26–28]:

$$\rho_{ABA'}=\frac{1}{12}\left(\sum_{\substack{l\\k>m}} f_{klm}(\sigma_k^A\otimes\sigma_l^B\otimes\sigma_m^{A'}+\sigma_m^A\otimes\sigma_l^B\otimes\sigma_k^{A'}) + \sum_{kl} f_{klk}\sigma_k^A\otimes\sigma_l^B\otimes\sigma_k^{A'}\right), \tag{12}$$

with $k,m=\{0,x,y,z\}$ and $l=0,\ldots,8$.

To guarantee that $\text{Tr}_{A'}(\rho_{ABA'})=\rho_{AB}$ [third constraint in Eq. (6)], the state coefficients of ρ_{AB} and $\rho_{ABA'}$ need to fulfill the following conditions:

$$f_{kl0}=x_{kl} \quad \forall\, k,l. \tag{13}$$

That is, some of the state parameters of $\rho_{ABA'}$ are already fixed by the coefficients of ρ_{AB}.

To simplify the notation used later on, we shall collect the objective variables of the SDP given by Eq. (6) within two different groups of them: The vector $\mathbf{x}$ contains those coefficients x_{kl} of ρ_{AB} not fixed by Eq. (8), and the vector $\mathbf{y}$ contains those coefficients f_{klm} of $\rho_{ABA'}$ not fixed by Eq. (13). With this parametrization, the first three constraints in Eq. (6) are fulfilled automatically and the SDP given by Eq. (6) can be reduced to solve the following one:

$$\text{minimize } 0$$

$$\text{subject to } \rho_{ABA'}(\mathbf{x},\mathbf{y})\geq 0. \tag{14}$$

III. WITNESS OPERATORS FOR TWO-WAY AND ONE-WAY QKD

In this section we show how to rephrase the QKD verification criteria introduced in the previous section into a search for appropriate witness operators. In order to do this, we use the dual problems associated with the primal SDPs given by Eqs. (11) and (14), respectively. In particular, we prove that the solutions to these dual problems correspond to the evaluation of an optimal witness operator, that belongs to the minimal verification set of them for the given two-way or one-way QKD protocol, on the observed data p_{ij}. A positive expectation value of this optimal witness operator states that no secret key can be distilled from the observed data p_{ij}. This approach has already been considered for the symmetric extension case in Ref. [27], and also for a slightly different scenario in Ref. [38]. Our main motivation here is to show specifically that this relationship still holds even if we restrict ourselves to partial information about the quantum state. A detailed discussion on some duality properties that guarantee that the solution to these dual problems can actually be associated with a witness operator is included in Appendix A.

Let us first introduce the dual problem associated to the primal SDP given by Eq. (2). It has the following form [23,24]:

$$\text{maximize } -\text{Tr}(F_0Z)$$

$$\text{subject to } Z\geq 0$$

$$\text{Tr}(F_iZ)=c_i \quad \forall\, i, \tag{15}$$

where the Hermitian matrix Z is now the objective variable. This matrix is positive semidefinite $Z\geq 0$ and is subjected to several linear constraints of the form $\text{Tr}(ZF_i)=c_i$ $\forall i$.

A. Two-way QKD

In this section we show that the solution to the dual problem associated with the SDP given by Eq. (11) corresponds to the evaluation of an optimal *decomposable* EW (DEW) [17,39] on the observed data p_{ij}. (See also Ref. [40].) An EW W is called decomposable if and only if there exist two positive operators $P,Q\geqslant 0$, and a real parameter $\epsilon\in[0,1]$, such that $W=\epsilon P+(1-\epsilon)Q^{\Gamma}$ [17,39]. In $\mathcal{H}_2^A\otimes\mathcal{H}_3^B$ all EWs are DEWs. In what follows, we establish this connection explicitly via the dual problem.

The SDP given by Eq. (11) can be transformed into a slightly different, but completely equivalent, form as follows (see Appendix A):

$$\text{minimize } t$$

$$\text{subject to } \rho_{AB}(\mathbf{x})\oplus\rho_{AB}^{\Gamma}(\mathbf{x})+t\mathbb{1}\geqslant 0, \tag{16}$$

where t denotes an auxiliary objective variable. According to Eq. (15), the dual problem associated with Eq. (16) can be written as

$$\text{maximize } -\mathrm{Tr}[(\rho_{\text{fix}}\oplus\rho_{\text{fix}}^{\Gamma})Z]$$

$$\text{subject to } Z\geqslant 0$$

$$\mathrm{Tr}(Z)=1$$

$$\mathrm{Tr}[(S_{kl}\oplus S_{kl}^{\Gamma})Z]=0 \quad \forall\, kl\notin I. \tag{17}$$

The structure of all the matrices which appear in this dual problem is the direct sum of two different matrices. Then, without loss of generality, we can assume that the same block structure is satisfied for Z, i.e., $Z=Z_1\oplus Z_2$. This means, in particular, that the objective function in Eq. (17) can now be re-expressed as

$$\begin{aligned}\mathrm{Tr}[(\rho_{\text{fix}}\oplus\rho_{\text{fix}}^{\Gamma})(Z_1\oplus Z_2)]\\ =\mathrm{Tr}[(Z_1+Z_2^{\Gamma})\rho_{\text{fix}}]\\ \equiv\mathrm{Tr}(W\rho_{\text{fix}}),\end{aligned} \tag{18}$$

where we have used the property $\mathrm{Tr}(Z_2\rho_{\text{fix}}^{\Gamma})=\mathrm{Tr}(Z_2^{\Gamma}\rho_{\text{fix}})$ and, in the last equality, we defined the operator $W\equiv Z_1+Z_2^{\Gamma}$. Next we show that W is a DEW. For that, note that the semidefinite constraint $Z\geqslant 0$ implies $Z_1,Z_2\geqslant 0$. Moreover, the witness is normalized, since $\mathrm{Tr}(Z)=1$ implies $\mathrm{Tr}(W)=\mathrm{Tr}(Z_1+Z_2^{\Gamma})=1$.

To conclude, we use the remaining equality constraints, $\mathrm{Tr}[(S_{kl}\oplus S_{kl}^{\Gamma})Z]=0\ \forall\, kl\notin I$, to show that to evaluate the expectation value of W one only needs to consider ρ_{fix}. That is, W belongs to the minimal verification set of EWs for the given QKD protocol, and its expectation value can be obtained from the observed data p_{ij} only [4]. Using the ansatz $Z_1=\Sigma_{kl}z_{kl}^1S_{kl}$, and $Z_2^{\Gamma}=\Sigma_{kl}z_{kl}^2S_{kl}$, the equality constraints impose $z_{kl}^1+z_{kl}^2=0\ \forall\, kl\notin I$. Hence the DEW W has the following structure:

$$W=\sum_{kl\in I}(z_{kl}^1+z_{kl}^2)S_{kl}\equiv\sum_{kl\in I}w_{kl}S_{kl}, \tag{19}$$

with $w_{kl}=z_{kl}^1+z_{kl}^2$. Combining Eqs. (9) and (19), we obtain $\mathrm{Tr}[W\rho_{AB}(\mathbf{x})]=\mathrm{Tr}(W\rho_{\text{fix}})=\Sigma_{kl\in I}w_{kl}x_{kl}$.

Whenever the solution to the dual problem given by Eq. (17) delivers $\mathrm{Tr}[(\rho_{\text{fix}}\oplus\rho_{\text{fix}}^{\Gamma})Z]\equiv\mathrm{Tr}(W\rho_{\text{fix}})\geqslant 0$ then no secret key can be distilled from the observed data p_{ij} with two-way classical communication. To see this, note that, by definition, Eq. (17) guarantees that there exists no other DEW W', that belongs to a verification set of them for the given QKD protocol, such that $\mathrm{Tr}(W'\rho_{\text{fix}})<\mathrm{Tr}(W\rho_{\text{fix}})$.

B. One-way QKD

In this part we use the dual problem associated with the SDP given by Eq. (14) to show that its solution corresponds to the evaluation of an optimal witness operator for the case of states with symmetric extensions. We shall follow the method introduced in Ref. [27], but now we will consider specifically the case of partial knowledge about the quantum state. (See also Ref. [40].)

Like in the previous section, the feasibility problem given by Eq. (14) can be transformed as follows (see Appendix A):

$$\text{minimize } t$$

$$\text{subject to } \rho_{ABA'}(\mathbf{x},\mathbf{y})+t\mathbb{1}/d_A\geqslant 0, \tag{20}$$

with $d_A=\dim(\mathcal{H}^A)$, e.g., in our case $d_A=2$. The inclusion of the factor d_A in Eq. (20) does not alter its result and, as we will see at the end of this section, it gives the correct normalization for the witnesses.

For convenience, we will express the state $\rho_{ABA'}(\mathbf{x},\mathbf{y})$ in terms of a map $\Lambda:\mathcal{H}_{d_A}^A\otimes\mathcal{H}_{d_B}^B\to\mathcal{H}_{d_A}^A\otimes\mathcal{H}_{d_B}^B\otimes\mathcal{H}_{d_A}^{A'}$ that takes an arbitrary Hermitian operator $A=1/(d_Ad_B)\Sigma_{kl}a_{kl}S_{kl}\in\mathcal{H}_{d_A}^A\otimes\mathcal{H}_{d_B}^B$, with $d_B=\dim(\mathcal{H}^B)$, to the Hermitian operator

$$\Lambda(A)=\frac{1}{d_A^2d_B}\left(\sum_{\substack{l=\{0,\ldots,d_B^2-1\}\\ k=\{1,\ldots,d_A^2-1\}}}a_{kl}(\sigma_k^A\otimes\sigma_l^B\otimes\mathbb{1}^{A'}+\mathbb{1}^A\otimes\sigma_l^B\otimes\sigma_k^{A'})+\sum_{l=\{0,\ldots,d_B^2-1\}}a_{0l}\mathbb{1}^A\otimes\sigma_l^B\otimes\mathbb{1}^{A'}\right). \tag{21}$$

Let ρ_{fix} be again the part of $\rho_{AB}\in\mathcal{S}$ that is fixed by the parameters a_{ik}, b_{jl}, and p_{ij}. Without loss of generality, we consider the following structure for ρ_{fix}: $\rho_{\text{fix}}=1/(d_Ad_B)\Sigma_{kl\in I}x_{kl}S_{kl}$, where the multi-index I has the same meaning as before, i.e., it labels those combinations of the indexes $k=\{0,\ldots,d_A^2-1\}$ and $l=\{0,\ldots,d_B^2-1\}$ such that x_{kl} is fixed by Eq. (8).

Using Eq. (21), we can rewrite $\rho_{ABA'}(\mathbf{x},\mathbf{y})$ in the following compact way:

$$\rho_{ABA'}(\mathbf{x},\mathbf{y})=\Lambda(\rho_{\text{fix}})+\sum_{kl\notin I}x_{kl}\Lambda(S_{kl})+\sum_J y_JG_J, \tag{22}$$

where the Hermitian matrices G_J can be grouped into two different sets,

$$G_{klk}=\sigma_k^A\otimes\sigma_l^B\otimes\sigma_k^{A'}\quad \forall\, l,\ \forall\, k\geqslant 1,$$

$$G_{mlk}=\sigma_m^A\otimes\sigma_l^B\otimes\sigma_k^{A'}+\sigma_k^A\otimes\sigma_l^B\otimes\sigma_m^{A'}\quad \forall\, l,\ \forall\, k>m\geqslant 1, \tag{23}$$

and where the multi-index J is used to label both different combinations of the indices k, l, and m.

The dual problem associated with Eq. (20) can now be written as

$$\text{maximize} \quad -\text{Tr}[Z\Lambda(\rho_{\text{fix}})]$$
$$\text{subject to } Z \geq 0$$
$$\text{Tr}(Z) = d_A$$
$$\text{Tr}[Z\Lambda(S_{kl})] = 0 \quad \forall\, kl \notin I$$
$$\text{Tr}(ZG_J) = 0 \quad \forall\, J. \tag{24}$$

Next we search for the most general form of a possible solution Z for this dual problem. It will enable us to extract the most compact form of a witness operator for the symmetric extendibility problem.

All the linear constraints on the operator Z contained in Eq. (24), as well as the objective function itself, are invariant under the swap operator P, which exchanges the first and the third subsystem. Moreover, the positive semidefinite constraint $\bar{Z}=PZP\geq 0$ is also satisfied since P is a unitary operator, i.e., $P^2=\mathbb{1}$. This means that, if Z is a solution for the dual problem, the operator $\bar{Z}$ is also a possible solution for it, since it fulfills all the constraints and it gives exactly the same expectation value. Following a similar argumentation, also the equal mixture of Z and $\bar{Z}$, i.e., $\tilde{Z}=1/2(Z+\bar{Z})$, is as well a possible solution. Therefore, without loss of generality, we can consider that Z is invariant under the swap operator P. Under this assumption, it turns out that Z can be decomposed as follows:

$$Z = \frac{1}{d_A^2 d_B}\left(\sum_{\substack{l\\k>m}} z_{mlk}(\sigma_m^A \otimes \sigma_l^B \otimes \sigma_k^{A'} + \sigma_k^A \otimes \sigma_l^B \otimes \sigma_m^{A'}) + \sum_{kl} z_{klk}\sigma_k^A \otimes \sigma_l^B \otimes \sigma_k^{A'}\right). \tag{25}$$

Let us now analyze in more detail the linear constraints on Z given in Eq. (24). Each linear constraint cancels one of the coefficients z_{mlk}. For instance, the constraint $\text{Tr}(ZG_{iji})$ imposes $z_{iji}=0$. Then, we can remove all these linear constraints, except the normalization condition $\text{Tr}(Z)=d_A$, by just making the proper coefficients z_{mlk} in Eq. (25) equal to zero. This way we arrive at the following form for the variable Z, which we shall denote by Z^*:

$$Z^* = \frac{1}{d_A^2 d_B}\left(\sum_{\substack{l;k\geq 1\\kl\in I}} z_{kl0}(\sigma_k^A \otimes \sigma_l^B \otimes \mathbb{1}^{A'} + \mathbb{1}^A \otimes \sigma_l^B \otimes \sigma_k^{A'}) + \sum_{\substack{l\\0l\in I}} z_{0l0}\mathbb{1}^A \otimes \sigma_l^B \otimes \mathbb{1}^{A'}\right). \tag{26}$$

That is, if we assume the form Z^* for the variable Z in the dual problem given by Eq. (24), then the linear constraints are fulfilled automatically. Substituting the variable Z with Z^* in Eq. (24) we obtain the following shorter form for the dual problem:

$$\text{maximize} \quad -\text{Tr}[Z^*\Lambda(\rho_{\text{fix}})]$$
$$\text{subject to } Z^* \geq 0$$
$$\text{Tr}(Z^*) = d_A. \tag{27}$$

Now, in order to extract a witness operator from the Hermitian operator Z^*, we follow the method proposed in Ref. [27]. In particular, every map $\Lambda:\mathcal{H}_{d_A}^A \otimes \mathcal{H}_{d_B}^B \to \mathcal{H}_{d_A}^A \otimes \mathcal{H}_{d_B}^B \otimes \mathcal{H}_{d_A}^{A'}$ has associated an adjoint map $\Lambda^\dagger:\mathcal{H}_{d_A}^A \otimes \mathcal{H}_{d_B}^B \otimes \mathcal{H}_{d_A}^{A'} \to \mathcal{H}_{d_A}^A \otimes \mathcal{H}_{d_B}^B$ defined as $\text{Tr}[U\Lambda(V)]=\text{Tr}[\Lambda^\dagger(U)V]$ for any Hermitian operators $V\in\mathcal{H}_{d_A}^A \otimes \mathcal{H}_{d_B}^B$, and $U\in\mathcal{H}_{d_A}^A \otimes \mathcal{H}_{d_B}^B \otimes \mathcal{H}_{d_A}^{A'}$. With this definition, we can rewrite the objective function in Eq. (27) as

$$\text{Tr}[Z^*\Lambda(\rho_{\text{fix}})] = \text{Tr}[\Lambda^\dagger(Z^*)\rho_{\text{fix}}] \equiv \text{Tr}(W_{\text{sym}}\rho_{\text{fix}}), \tag{28}$$

where we defined $W_{\text{sym}}\equiv\Lambda^\dagger(Z^*)$ as the desired witness operator for the symmetric extendibility problem. In the remaining part of this section, we obtain the general structure of the witness operator W_{sym}. For that, we simply apply the adjoint map $\Lambda^\dagger$ to the operator Z^*, set the resulting operator equal to an operator of arbitrary form W^*, solve the equality constraint, and, finally, formulate the dual problem in terms of this new operator W^*.

The map $\Lambda^\dagger$ can be written as [27]

$$\Lambda^\dagger(Z) = \frac{1}{d_A}\left(\text{Tr}_{A'}(Z) + \text{Tr}_{A'}(PZP) - \frac{1}{d_A}\mathbb{1}^A \otimes \text{Tr}_{AA'}(Z)\right). \tag{29}$$

Setting $\Lambda^\dagger(Z^*)$ equal to an arbitrary Hermitian operator $W^* = 1/(d_A d_B)\Sigma_{kl} w_{kl} S_{kl}$ we obtain the following equality constraint:

$$\sum_{kl} w_{kl}S_{kl} = \sum_{\substack{l;k\geq 1\\kl\in I}} \frac{2z_{kl0}}{d_A}S_{kl} + \sum_{\substack{l\\0l\in I}} z_{0l0}S_{0l}. \tag{30}$$

Since we have expressed every operator in terms of an operator basis, the equality constraint can only be fulfilled if the coefficients z_{klm} of Z^* and the coefficients w_{kl} of W^* are related via

$$w_{kl} = 2z_{kl0}/d_A \quad \forall\, l, \forall\, k\geq 1, kl\in I,$$
$$w_{0l} = z_{0l0}/d_A \quad \forall\, l, 0l\in I,$$
$$w_{kl} = 0 \quad kl\notin I. \tag{31}$$

Now, instead of considering the matrix Z^* as the objective variable of the dual problem, we can equivalently consider the matrix W^* as the free variable. In order to do so, we only need to translate the positive semidefinite constraint $Z^*\geq 0$ together with the normalization condition $\text{Tr}(Z^*)=d_A$ included in Eq. (27) into new constraints on W^*. This can be done by using Eq. (31). This way, we arrive at the following form for the dual problem:

$$\text{maximize} \quad -\text{Tr}(W^*\rho_{\text{fix}})$$

$$\text{subject to } W^* \otimes \mathbb{1}^{A'} + P(W^* \otimes \mathbb{1}^{A'})P \geq 0$$

$$\text{Tr}(W^*) = 1, \tag{32}$$

where the variable W^* represents a witness operator for the symmetric extendibility problem. Moreover, from Eq. (31) we obtain that W^* can always be expressed as

$$W^* = \frac{1}{d_A d_B} \sum_{kl \in I} w_{kl} S_{kl}. \tag{33}$$

That is, W^* belongs to the minimal verification set of witnesses for the given one-way (RR) QKD protocol. Like in the previous section, whenever the solution to the dual problem given by Eq. (32) delivers $\text{Tr}(W^*\rho_{\text{fix}}) \geq 0$ then no secret key can be distilled from the observed data p_{ij} with one-way RR. The case of one-way QKD with DR can be analyzed in a similar way.

IV. EVALUATION

In this section we study the two-state QKD protocol [20], both for the case of two-way and one-way classical communication. The analysis for other qubit-based QKD schemes is completely analogous, and we include very briefly the results of our investigations on other well-known QKD protocols in Appendix B. We refer here to single-photon implementations of the qubit. The state of the qubit is described, for instance, by some degree of freedom in the polarization of the photon. In our calculations we follow the approach introduced in Sec. II, although similar results could also be obtained using the witness approach presented in Sec. III. The numerical evaluations are performed with the freely available SDP solver SDPT3-3.02 [41], together with the input tool YALMIP [42].

We shall consider that the observed joint probability distribution p_{ij} originates from Alice and Bob measuring the following quantum state:

$$\rho_{AB} = (1-p)\left((1-e)\mathbb{1}^A \otimes U^B(\theta)|\psi\rangle_{AB}\langle\psi|\mathbb{1}^A \otimes U^{B\dagger}(\theta) + \frac{e}{2}\rho_A \otimes \tilde{\mathbb{1}}^B\right) + p\rho_A \otimes |\text{vac}\rangle_B\langle\text{vac}|, \tag{34}$$

where $p \in [0,1]$ denotes the probability that Bob receives the vacuum state $|\text{vac}\rangle_B$, $e \in [0,1]$ represents an error parameter (or depolarizing rate) of the channel, $\mathbb{1}^A$ is the identity operator on Alice's Hilbert space, $U^B(\theta)$ represents a unitary operator acting on Bob's system, $|\psi\rangle_{AB}$ denotes the effective bipartite state initially prepared by Alice in the given QKD protocol, ρ_A represents Alice's reduced density matrix [i.e., $\rho_A = \text{Tr}_B(|\psi\rangle_{AB}\langle\psi|)$], and the operator $\tilde{\mathbb{1}}^B$ is given by $\tilde{\mathbb{1}}^B = \mathbb{1}^B - |\text{vac}\rangle_B\langle\text{vac}|$.

The quantum state given by Eq. (34) defines one possible eavesdropping interaction. But our analysis can straightforwardly be applied to other quantum channels, as it depends only on the probability distribution p_{ij} that characterizes the results of Alice's and Bob's measurements. We include the operator $U^B(\theta)$ in Eq. (34) to model the collective noise (or correlated noise) introduced by the quantum channel (e.g, optical fiber) [43,44]. This noise arises from the fluctuation of the birefringence of the optical fiber which alters the polarization state of the photons. When this fluctuation is slow in time, its effect can be described with a unitary operation [43,44]. For simplicity, we shall consider that $U^B(\theta)$ is parametrized only with one real parameter θ. In particular, we choose $U^B(\theta) = \cos\theta|0\rangle\langle 0| - \sin\theta|0\rangle\langle 1| + \sin\theta|1\rangle\langle 0| + \cos\theta|1\rangle\langle 1| + |\text{vac}\rangle\langle\text{vac}|$ with $\theta \in [0, \pi/4]$. If $\theta=0$ no collective noise is present and Eq. (34) describes a depolarizing channel with loss.

In order to illustrate our results, we calculate an upper bound on the tolerable depolarizing rate e as a function of the photon loss probability $p \in [0,1]$. Moreover, for simplicity, we take only two different values of the angle θ. For instance, we choose $\theta=0$ and $\theta=\pi/8$. These three parameters, e, p, and θ, allow us to evaluate the performance of a QKD protocol when the quantum channel is described by Eq. (34). One could also select other figures of merit in order to evaluate a protocol, such as the quantum bit error rate (QBER). This is the rate of events where Alice and Bob obtain different results. It refers to the sifted key, i.e., it considers only those events where the signal preparation and detection methods employ the same polarization basis. We include as well an analytic expression for the QBER for the given QKD protocol.

A. Two-state protocol

The two-state protocol [20] is one of the simplest QKD protocols. It is based on the random transmission of only two nonorthogonal states, $|\varphi_0\rangle$ and $|\varphi_1\rangle$. Alice chooses, at random and independently every time, 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 to Bob. On the receiving side, Bob measures the qubit he receives in a basis chosen at random within the set $\{\{|\varphi_0\rangle, |\varphi_0^\perp\rangle\}, \{|\varphi_1\rangle, |\varphi_1^\perp\rangle\}\}$, with $|\langle\varphi_i|\varphi_i^\perp\rangle| = 0$. The loss of a photon corresponds to a projection onto the vacuum state $|\text{vac}\rangle$. Bob could also employ a different detection method defined by a POVM with the following operators: $B_j = 1/(2\beta^2)|\varphi_{1-j}^\perp\rangle\langle\varphi_{1-j}^\perp|$ with $j=0,1$, $B_{null} = |0\rangle\langle 0| + |1\rangle\langle 1| - \Sigma_j B_j$, and $B_{\text{vac}} = |\text{vac}\rangle\langle\text{vac}|$. In this last case, Alice's bit value i is associated with the operator B_i, while the operator B_{null} represents an inconclusive result. This is the approach that we shall consider here.

The preparation process can be thought of as Alice prepares first the bipartite signal state $|\psi\rangle_{AB} = 1/\sqrt{2}(|0\rangle_A|\varphi_0\rangle_B + |1\rangle_A|\varphi_1\rangle_B)$, and then she measures her first subsystem with the POVM operators $A_i = |i\rangle\langle i|$ with $i=0,1$. The fact that the reduced density matrix of Alice is fixed and cannot be modified by Eve is vital to guarantee the security of this scheme. Otherwise, the joint probability distribution p_{ij} alone does not allow Alice and Bob to distinguish between the entangled state $|\psi\rangle_{AB}$ and the separable one $\sigma_{AB} = 1/2\Sigma_{i=0}^{1}|i\rangle_A\langle i| \otimes |\varphi_i\rangle_B\langle\varphi_i|$ [4,13]. We need to add then to the observables

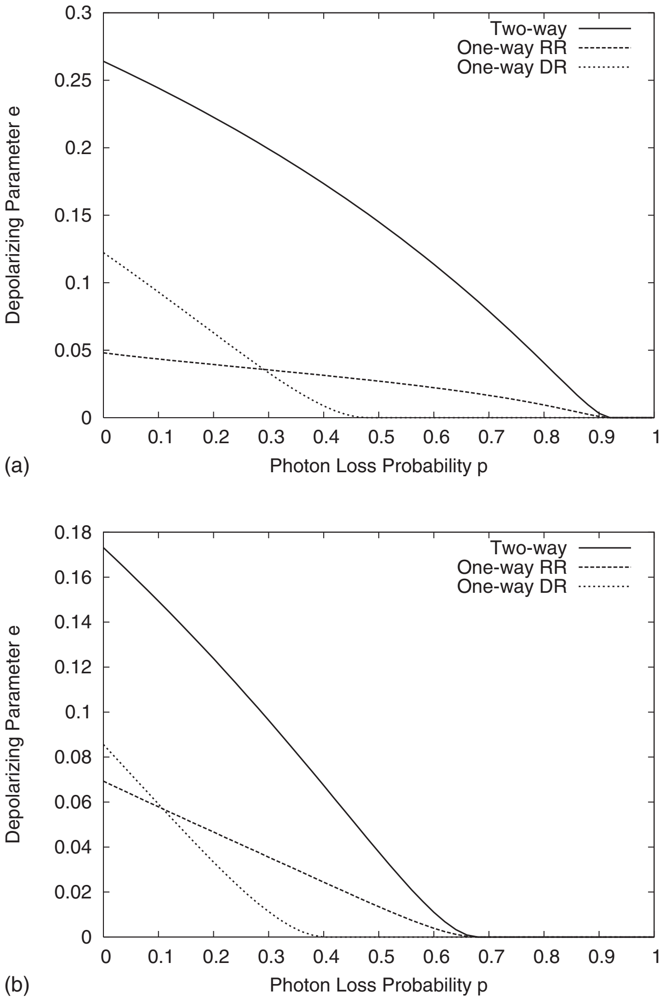

FIG. 1. Upper bound on the depolarizing rate e as a function of the photon loss probability p for the two-state QKD protocol with parameter $\alpha=0.2$ and $\alpha=0.4$. The equivalence class of states $\mathcal{S}$ is fixed by the observed data p_{ij}, which are generated via measurements onto the state given by Eq. (34). Two-way classical post-processing is illustrated with a solid line. One-way classical post-processing is represented with a dashed line for RR, and with a dotted line for DR. The cases $\theta=0$ and $\theta=\pi/8$ provide the same results. It states that no secret key can be obtained from the correlations established by the users.

given above also the operators $\sigma_x\otimes\sigma_0$ and $\sigma_y\otimes\sigma_0$ such as Alice has complete tomographic knowledge of ρ_A.

Following the approach introduced in Sec. II, in Fig. 1 we present an upper bound on the tolerable depolarizing rate e as a function of the photon loss probability p for two different values of the parameter α. It states that no secret key can be distilled from the correlations established by the users. In this example, the results obtained coincide when $\theta=0$ and $\theta=\pi/8$. To obtain an upper bound on the tolerable QBER one can use the following expression:

$$\text{QBER}=\frac{2\sin^2\theta+(1-2\sin^2\theta)e}{2\{2\beta^2+(\alpha^2-\beta^2)[\gamma+(1-\gamma)e]\}}, \qquad (35)$$

with $\gamma=2(\alpha^2\sin^2\theta+\beta^2\cos^2\theta)$. In particular, for given values of the parameters α, β, and θ, one only needs to substitute in Eq. (35) the value of e given in Fig. 1 as a function of the parameter p.

Remarkably, the cutoff point for two-way QKD presented in Fig. 1, i.e., the value of the photon loss probability p that makes $e=0$ and also QBER=0, coincides with the limit imposed by the unambiguous state discrimination attack [45–49]. In the two-state protocol this limit is given by $p=1-2\alpha^2$. (See also Ref. [50].) Figure 1 also shows a difference between one-way classical post-processing with RR and with DR as a function of the parameter p. The reason behind this effect is beyond the scope of this paper and needs further investigation.

V. CONCLUSION

A fundamental question in quantum key distribution (QKD) is to determine whether the legitimate users of the system can use their available measurement results to generate a secret key via two-way or one-way classical post-processing of the observed data. In this paper we have investigated single-photon QKD protocols in the presence of loss introduced by the quantum channel. Our results are based on a simple precondition for secure QKD for two-way and one-way classical communication. In particular, the legitimate users need to prove that there exists no separable state (in the case of two-way QKD), or that there exists no quantum state having a symmetric extension (one-way QKD), that is compatible with the available measurements results.

We have shown that both criteria can be formulated as a convex optimization problem known as a primal semidefinite program (SDP). Such instances of convex optimization problems can be solved efficiently, for example by means of interior-point methods. Moreover, these SDP techniques allow us to evaluate these criteria for any single-photon QKD protocol in a completely systematic way. A similar approach was already used in Ref. [25] for the case of one-way QKD without losses. Here we complete these results, now presenting specifically the analysis for the case of a lossy channel. Furthermore, we have shown that these QKD verification criteria based on SDP provide also a means to search for witness operators for a given two-way or one-way QKD protocol. Any SDP has an associated dual problem that represents also a SDP. We have demonstrated that the solution to this dual problem corresponds to the evaluation of an optimal witness operator that belongs to the minimal verification set of them for the given two-way (or one-way) QKD protocol. Most importantly, a positive expectation value of this optimal witness operator guarantees that no secret key can be distilled from the available measurements results. Finally, we have illustrated our results by analyzing the performance of several well-known qubit-based QKD protocols for a given channel model.

ACKNOWLEDGMENTS

We gladly acknowledge stimulating discussions with K. Tamaki, O. Gühne, C.-H. F. Fung, and X. Ma. We specially thank H.-K. Lo and N. Lütkenhaus for their critical discussion of this paper, and F. Just for help on the numerics. Financial support from NSERC, CIPI, CRC program, CFI, OIT, CIAR, PREA, DFG under the Emmy Noether program, and the European Commission (Integrated Project SECOQC) are gratefully acknowledged. M.C. also thanks the financial support from a post-doctoral grant from the Spanish Ministry of Science (MEC).

APPENDIX A: SOME DUALITY PROPERTIES

In this appendix we present some duality properties of a general SDP [23,24] that guarantee that the solution to the dual problems introduced in Sec. III can be associated with a witness operator.

The primal problem given by Eq. (2) is called feasible (strictly feasible) if there exists $\mathbf{x}$ such as $F(\mathbf{x})\geqslant 0[F(\mathbf{x})>0]$. Similarly, the dual problem given by Eq. (15) is called *feasible (strictly feasible)* if there exists a matrix $Z\geqslant 0$ $(Z>0)$ which fulfills all the desired constraints.

The *weak duality condition*, illustrated in Eq. (A1), allows us to derive simple upper and lower bounds for the solution of either the primal or dual problem. In particular, for every feasible solution $\mathbf{x}$ of the primal problem and for every feasible solution Z of the dual problem, the following relation holds:

$$c^T\mathbf{x} + \text{Tr}(ZF_0) = \text{Tr}[ZF(\mathbf{x})] \geqslant 0. \tag{A1}$$

The *strong duality condition* certifies whether the optimal solution to the primal and dual problem, that we shall denote as p^* and d^*, respectively, are equal. More precisely, $p^*=d^*$ if (i) the primal problem is strictly feasible, or (ii) the dual problem is strictly feasible. Moreover, if both conditions are satisfied simultaneously then it is guaranteed that there is a feasible pair $(\mathbf{x}_{\text{opt}},Z_{\text{opt}})$ achieving the optimal values $p^*=d^*$. This last condition is known as the *complementary slackness condition*.

The SDP given by Eq. (2), when $c=0$, can always be transformed as follows [23,24]:

$$\text{minimize } t$$

$$\text{subject to } F(\mathbf{x},t) = F(\mathbf{x}) + t\mathbb{1} \geqslant 0. \tag{A2}$$

This SDP is always strictly feasible. To see this, note that if $\mathbf{x}=0$ and $t>|\min_i \lambda_i(F_0)|$, where $\lambda_i(F_0)$ denote the eigenvalues of the matrix F_0, then $F(\mathbf{x},t)>0$. Moreover, it can be shown that Eq. (A2) is equivalent to the original SDP. Let t^* be the solution to Eq. (A2). If $t^*>0$, the original problem is infeasible since $F(\mathbf{x})\ngeqslant 0$ $\forall$ $\mathbf{x}$. On the other hand, if $t^*\leqslant 0$ there exists $\bar{\mathbf{x}}$ such that $F(\bar{\mathbf{x}})\geqslant 0$, stating that the original problem is feasible. That is, the solution t^* of the SDP given by Eq. (A2) certifies whether the original problem is indeed feasible or not.

The dual problem associated with Eq. (A2) is given by

$$\text{maximize } -\text{Tr}(F_0Z)$$

$$\text{subject to } Z\geqslant 0$$

$$\text{Tr}(F_iZ)=0 \ \ \forall \ \ i$$

$$\text{Tr}(Z)=1. \tag{A3}$$

If all the matrices F_i are traceless, i.e., $\text{Tr}(F_i)=0$, this dual problem is also always strictly feasible. A trivial strictly feasible solution to this problem is given by $Z=\mathbb{1}/d>0$, where d denotes the dimension of F_i.

If we apply the three duality conditions mentioned above to the SDPs given by Eqs. (A2) and (A3) we find that, if Eq. (A2) delivers an infeasible solution $t^*>0$,

$$\text{Tr}(F_0Z_{\text{opt}}) = -d^* = -t^* < 0. \tag{A4}$$

This arises from the fact that the strong duality relation guarantees that $d^*=t^*$, and the complementary slackness condition certifies that there is a Z_{opt} that achieves the optimal value d^*. When $t^*\leqslant 0$ the weak duality condition assures that

$$\text{Tr}(F_0Z) \geqslant -t^* \geqslant 0 \tag{A5}$$

for every feasible solution Z of the dual problem. Both results together show that the solution to the dual problem given by Eq. (A3) can be associated to a witness operator W. In particular, the ability of W to detect, at least, one state, i.e., $\exists$ ρ such as $\text{Tr}(W\rho)<0$, can be related with Eq. (A4). On the other hand, the requirement that W is positive on all states belonging to a given set of them can be related with Eq. (A5). To achieve the desired equivalence, however, the dual problem must be strictly feasible, otherwise the complementary slackness condition does not hold and the existence of an appropriate witness is not guaranteed. It turns out that all the linear constraints included in the dual problems considered in Sec. III have traceless matrices F_i, such that these dual problems are always strictly feasible.

APPENDIX B: MORE QUBIT-BASED QKD SCHEMES

In this appendix we include very briefly the results of our investigations on other well-known qubit-based QKD protocols. Like in Sec. IV, we shall consider that the observed data p_{ij} are generated via measurements onto the state given by Eq. (34).

1. Six-state protocol

In this scheme, Alice prepares a qubit in one of the following six quantum states: $\{|0\rangle,|1\rangle,|\pm\rangle=1/\sqrt{2}(|0\rangle\pm|1\rangle),|\widetilde{\pm}\rangle=1/\sqrt{2}(|0\rangle\pm i|1\rangle)\}$, and sends it to Bob [19]. On the receiving side, Bob measures each incoming signal by projecting it onto one of the three possible bases. The loss of a photon in the channel is characterized by a projection onto the vacuum state $|\text{vac}\rangle$.

The resulting upper bound on the tolerable depolarizing rate e is illustrated in Fig. 2. The QBER is given by

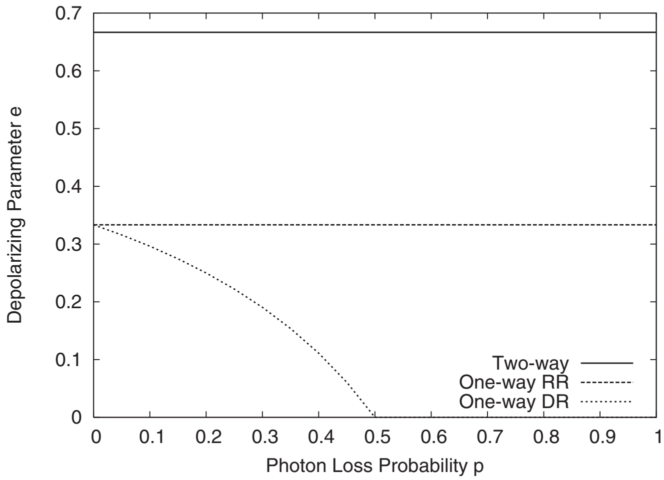

FIG. 2. Upper bound on the depolarizing rate e as a function of the photon loss probability p for the six-state QKD protocol. Two-way classical post-processing is illustrated with a solid line, while one-way classical post-processing is represented with a dashed line for RR, and with a dotted line for DR. The cases $\theta=0$ and $\theta=\pi/8$ provide the same results in this case.

$$\text{QBER} = \frac{1}{6}[4\sin^2\theta + (3-4\sin^2\theta)e]. \tag{B1}$$

For $\theta=0$ we find, as expected, that whenever QBER$\geqslant$33% (corresponding to a value of $e=0.66$) no secret key can be distilled by two-way classical post-processing [19,51]. In the case of one-way classical post-processing (both for RR and DR), and assuming $\theta=0$ and $p=0$, we obtain that secure QKD might only be possible for a QBER$<1/6$ ($e=0.33$). A possible eavesdropping strategy to attain this cutoff point is, for instance, to use a universal cloning machine to clone every signal sent by Alice such as the fidelities of Eve's and Bob's clones coincide [52]. (See also Ref. [25].)

2. Four-state protocol

The four-state protocol [18] is similar to the six-state protocol, but now Alice sends one of four possible signal states instead of one of six. In particular, she chooses one state within the set $\{|0\rangle,|1\rangle,|\pm\rangle\}$ and sends it Bob. Each received signal is projected by Bob onto one of the two possible bases, together with a projection onto the vacuum state $|\text{vac}\rangle$ corresponding to the loss of a photon.

The resulting upper bound on the depolarizing rate e is illustrated in Fig. 3.

The QBER is now given by

$$\text{QBER} = \sin^2\theta + \frac{(1-2\sin^2\theta)e}{2}. \tag{B2}$$

If $\theta=0$ we obtain the well-known result stating that whenever QBER$\geqslant$25% (corresponding to a value of $e=0.5$) no secret key can be distilled by two-way classical post-processing [51]. Similarly, for the case of one-way classical post-processing, and assuming $\theta=0$ and $p=0$, we find that the QBER must be lower than 14,6% ($e=0.292$). This last result coincides with the value of the QBER produced by an eavesdropping strategy where Eve's and Bob's Shannon information are equal [54,55].

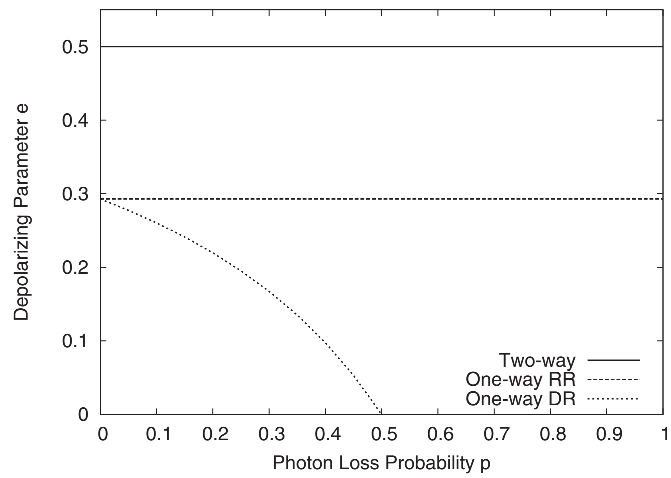

FIG. 3. Upper bound on the depolarizing rate e as a function of the photon loss probability p for the four-state QKD protocol. Two-way classical post-processing is illustrated with a solid line, while one-way classical post-processing is represented with a dashed line for RR, and with a dotted line for DR. The cases $\theta=0$ and $\theta=\pi/8$ provide the same results in this case. This upper bound also coincides for the case of the trine protocol and for the QKD scheme proposed in Ref. [53] when $\theta=0$.

3. Qubit-based four-plus-two-state protocol

This scheme can be seen as a combination of two two-state QKD protocols [56,57]. More precisely, Alice selects, at random and independently each time, one of the following four signal states: $\{|\varphi_k\rangle=\alpha|0\rangle+(-1)^k\beta|1\rangle, |\varphi_k^-\rangle=\alpha|0\rangle+i(-1)^k\beta|1\rangle\}$ with $k=0,1$, and sends it to Bob. On the receiving side, Bob measures each incoming signal by choosing, at random and independently for each signal, one of two possible POVMs. Each POVM corresponds to the one used in the two-state protocol (see Sec. IV A) for the signal states $|\varphi_k\rangle=\alpha|0\rangle+(-1)^k\beta|1\rangle$, with $k=0,1$, and $|\varphi_k^-\rangle=\alpha|0\rangle+i(-1)^k\beta|1\rangle$, with $k=0,1$, respectively.

The resulting upper bound on the depolarizing rate e is illustrated in Fig. 4 for the cases $\alpha=0.2$ and $\alpha=0.4$. The QBER is given by

$$\text{QBER} = \frac{e+(1-e)[1+(\alpha^2-\beta^2)^2]\sin^2\theta}{2\{e+(1-e)[2(\alpha^4+\beta^4)\sin^2\theta+4\alpha^2\beta^2\cos^2\theta]\}}. \tag{B3}$$

In the case of two-way classical post-processing, the maximum tolerable value of e shown in Fig. 4 starts decreasing as the losses in the channel increase, and, at some point, it becomes constant independently of p. Interestingly, the value of p where this inflexion occurs corresponds to the point where Eve can discriminate unambiguously between the two states in the set $\{|\varphi_k\rangle\}$, with $k=0,1$, or between those states in the set $\{|\varphi_k^-\rangle\}$, with $k=0,1$. This happens when $p=1-2\alpha^2$.

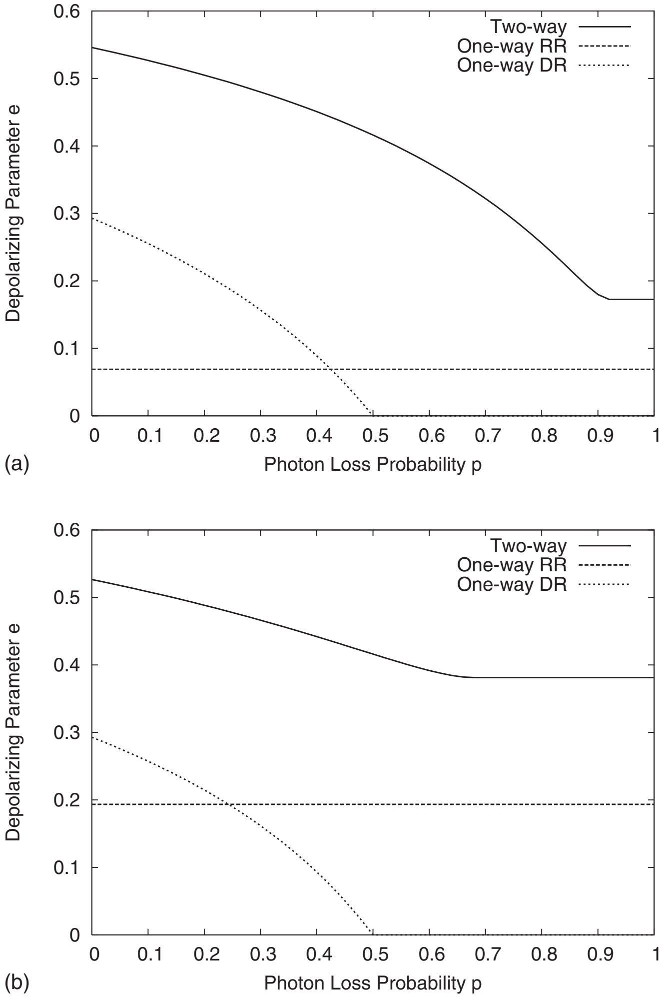

FIG. 4. Upper bound on the depolarizing rate e as a function of the photon loss probability p for the qubit-based four-plus-two-state QKD protocol for parameter α=0.2 and α=0.4. Two-way classical post-processing is illustrated with a solid line, while one-way classical post-processing is represented with a dashed line for RR, and with a dotted line for DR. The cases θ=0 and $\theta=\pi/8$ provide the same results.

4. Three-state protocol

This QKD scheme requires Alice sending to Bob one of the following three quantum states: $|0\rangle$, $|1\rangle$, and $|+\rangle$ [58–61]. On the receiving side, Bob projects each incoming signal onto one of the two possible bases used in the four-state protocol (see Appendix B 2), together with a projection onto the vacuum state $|\text{vac}\rangle$.

The resulting upper bound on the depolarizing rate e is illustrated in Fig. 5. The QBER has now the following form:

$$\text{QBER} = \frac{1}{2}[1 + (1-e)(\sin^2\theta - \cos^2\theta)]. \tag{B4}$$

For the quantum channel given by Eq. (34), and assuming θ=0 or $\theta=\pi/8$, the maximum value of e tolerated by the three-state protocol coincides with the four-state protocol for the cases of two-way and one-way post-processing with DR.

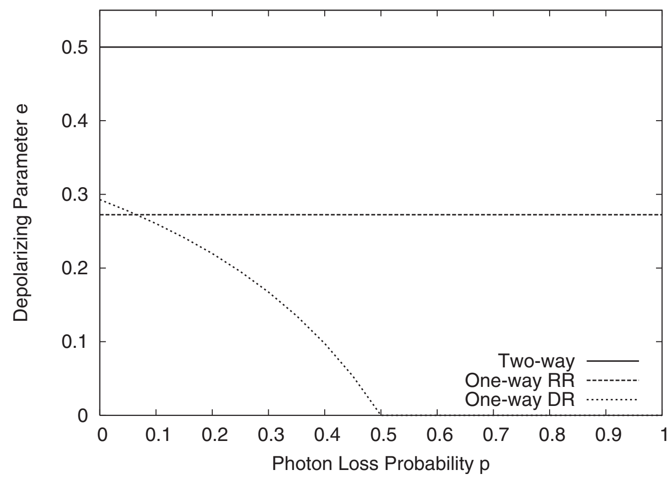

FIG. 5. Upper bound on the depolarizing rate e as a function of the photon loss probability p for the three-state QKD protocol. Two-way classical post-processing is illustrated with a solid line, while one-way classical post-processing is represented with a dashed line for RR, and with a dotted line for DR. The cases θ=0 and $\theta=\pi/8$ provide the same results.

5. Trine protocol

In the trine protocol [62], Alice selects, at random and independently each time, a qubit in one of the following three states: $|0\rangle$, $1/2|0\rangle+\sqrt{3}/2|1\rangle$, and $1/2|0\rangle-\sqrt{3}/2|1\rangle$, and sends it to Bob. Each received signal is measured by Bob with a POVM defined by the following operators: $B_0=2/3|1\rangle\langle 1|$, $B_i=2/3|\psi_i\rangle\langle\psi_i|$, with $i=1,2$, and where $|\psi_i\rangle=\sqrt{3}/2|0\rangle+(-1)^i 1/2|1\rangle$, and $B_{\text{vac}}=|\text{vac}\rangle\langle\text{vac}|$.

For the quantum channel given by Eq. (34), and assuming θ=0 or $\theta=\pi/8$, it turns out that the maximum value of e tolerated by this scheme, both for two-way and one-way post-processing, coincides with the four-state protocol (see Fig. 3). The QBER, however, is given by

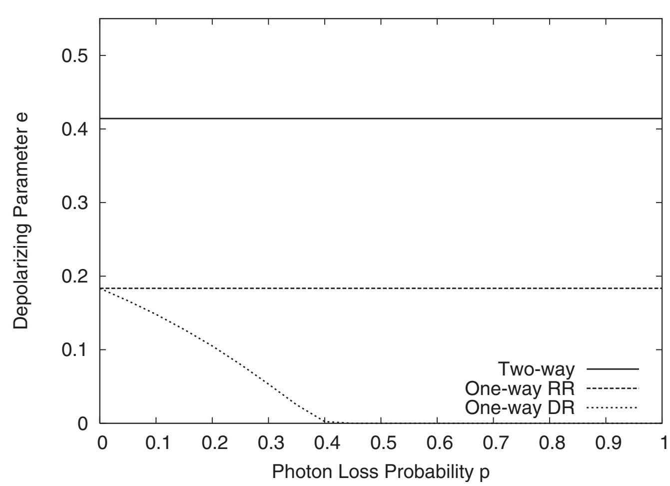

FIG. 6. Upper bound on the depolarizing rate e as a function of the photon loss probability p for the QKD protocol in Ref. [53] when $\theta=\pi/8$. Two-way classical post-processing is illustrated with a solid line, while one-way classical post-processing is represented with a dashed line for RR, and with a dotted line for DR.

$$\text{QBER} = \frac{2e + 4(1-e)\sin^2\theta}{3 + e + 2(1-e)\sin^2\theta}. \tag{B5}$$

6. Acín-Massar-Pironio protocol

In this scheme, Alice sends to Bob one of the following six states: $|+\rangle$, $|-\rangle$, $1/\sqrt{2}(|0\rangle \pm i|1\rangle)$, and $1/\sqrt{2}|0\rangle \pm (1-i)/2|1\rangle$ [53,63]. On the receiving side, Bob measures each incoming signal with one of two possible measurements corresponding to the bases $1/\sqrt{2}(|0\rangle \pm e^{-i\phi}|1\rangle)$ with $\phi = \{\pi/4, -\pi/4\}$, that he selects at random and independently for each signal, together with a projection onto the vacuum state $|\text{vac}\rangle$.

When $\theta = 0$, the maximum value of e tolerated by this protocol, both for two-way and one-way post-processing, coincides with the four-state protocol (see Fig. 3). The case $\theta = \pi/8$ is illustrated in Fig. 6. The QBER is now given by

$$\text{QBER} = \frac{1}{2}[(1-e)\sin^2\theta + e]. \tag{B6}$$

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] M. Dušek, N. Lütkenhaus, and M. Hendrych, *Progress in Optics*, edited by E. Wolf (Elsevier, New York, in press), Vol. 49.

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

[4] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. A **71**, 022306 (2005).

[5] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).

[6] D. Mayers, *Advances in Cryptology—Proceedings of Crypto'96* (Springer, Berlin, 1996), pp. 343–357.

[7] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[8] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).

[9] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

[10] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[11] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).

[12] M. Curty and N. Lütkenhaus, Phys. Rev. A **69**, 042321 (2004).

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

[14] 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; 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, Verlag, 2003), p. 79 (see also second edition, 2005).

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

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

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

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

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

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

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

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

[23] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).

[24] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, England, 2004).

[25] T. Moroder, M. Curty, and N. Lütkenhaus, Phys. Rev. A **74**, 052301 (2006).

[26] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).

[27] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).

[28] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **71**, 032333 (2005).

[29] B. M. Terhal, A. C. Doherty, and D. Schwab, Phys. Rev. Lett. **90**, 157903 (2003).

[30] P. Horodecki and M. Nowakowski, e-print arXiv:quant-ph/0503070.

[31] A. Peres, Found. Phys. **12**, 1441 (1990).

[32] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, 1993).

[33] Using the Schmidt decomposition we have that the state $|\psi_{source}\rangle_{AB}$ can be written as $|\psi_{source}\rangle_{AB} = \sum_{k=0}^{1}\sqrt{q_k}|u_k\rangle_A|v_k\rangle_B$ for some orthogonal states $|u_k\rangle_A = \sum_{i=0}^{N-1}c_i^k|\alpha_i\rangle_A$ and where $|v_k\rangle_B \in \mathcal{H}_2^B$. The orthogonal basis $|\alpha_i\rangle_A$ can always be selected such as $|\alpha_i\rangle_A = |0\rangle_{A'}|\beta_i\rangle_{A''}$ for $i = 0, \ldots, \lfloor\frac{N-1}{2}\rfloor$, and $|\alpha_i\rangle_A = |1\rangle_{A'}|\beta(_{i-\lfloor\frac{N-1}{2}\rfloor-1})\rangle_{A''}$ for $i = \lfloor\frac{N-1}{2}\rfloor + 1, \ldots, N-1$, with A' and A'' denoting two auxiliary systems under Alice's control, and where $|\beta_i\rangle_{A''}$ satisfy $\langle\beta_i|\beta_j\rangle_{A''} = \delta_{ij}$. On the other hand, the states $|u_k\rangle_A$ can always be obtained from the orthogonal states $|k\rangle_{A'}|\beta_0\rangle_{A''}$ by means of a unitary transformation $U_{A'A''}$ i.e., $|u_k\rangle_A = U_{A'A''}|k\rangle_{A'}|\beta_0\rangle_{A''}$. With this notation we can write the initial state prepared by Alice as $(U_{A'A''} \otimes_B)|\psi_{source}\rangle_{A'B}|\beta_0\rangle_{A''}$ with $|\psi_{source}\rangle_{A'B} = \sum_{k=0}^{1}\sqrt{q_k}|k\rangle_{A'}|v_k\rangle_B \in \mathcal{H}_2^{A'} \otimes \mathcal{H}_2^B$. The measurement process in the basis $|\alpha_i\rangle_A$ can then be described as the following: Alice first prepares the signal state $|\psi_{source}\rangle_{A'B}$, and then she measures her subsystem A' with the POVM operators $A_i = {}_{A''}\langle\beta_0|U_{A'A''}^{\dagger}|\alpha_i\rangle_A\langle\alpha_i|U_{A'A''}|\beta_0\rangle_{A''}$ with $i = 0, \ldots, N-1$.

[34] Given an operator $\rho_{AB} \in \mathcal{H}^A \otimes \mathcal{H}^B$, and an orthonormal basis $\{|\beta_i\rangle_B\} \in \mathcal{H}^B$, with $i = 1, \ldots, N$, the partial transpose of ρ_{AB}, with respect to subsystem B, in that basis is defined as

$$\rho_{AB}^{\Gamma} = \sum_{i,j=1}^{N} {}_B\langle\beta_i|\rho_{AB}|\beta_j\rangle_B|\beta_j\rangle_B\langle\beta_i|.$$

In the same way, one can also define the partial transpose of ρ_{AB}, with respect to subsystem A.

[35] Note that given N LMIs constraints $F^0(\mathbf{x}) \geqslant 0, \ldots, F^{N-1}(\mathbf{x}) \geqslant 0$, we can always combine them to a single new LMI constraint as

$$F(\mathbf{x}) = \begin{pmatrix} F^0(\mathbf{x}) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & F^{N-1}(\mathbf{x}) \end{pmatrix} \equiv F^0(\mathbf{x}) \oplus \cdots \oplus F^{N-1}(\mathbf{x}) \geqslant 0.$$

[36] The operator ρ_{fix}, can always be expressed as $\rho_{\text{fix}} = \Sigma_{kl \in I} c_{kl} S_{kl}$, because of the following reason: suppose, for instance, that a given set of measurement operators $\{A_i \otimes B_j\}$, does not form a set of operator basis elements. Then, one can find the minimal set of linear independent measurement operators and then apply the Gram-Schmidt orthogonalization to these elements in order to obtain a minimal set of linear independent operator basis elements. Moreover, from the original data p_{ij}, it is straightforward to compute the observed probability distribution for these new operators. As a result, one finds a fixed part ρ_{fix}, of the form $\rho_{\text{fix}} = \Sigma_{kl \in I} c_{kl} S_{kl}$, and the operator set $\{S_{kl}\}_{kl \in \mathcal{I}}$, can be extended to a full operator basis set. In this procedure we consider the natural case where the original data p_{ij}, are consistent with a quantum-mechanical state.

[37] Alternatively to this method, the equality constraints given by Eq. (8) can also be included directly in the LMI constraint of the SDP. Each of these constraints can be represented by means of two inequality constraints as follows: $\Sigma_{kl} a_{ik} b_{jl} x_{kl} - p_{ij} \geqslant 0$ and $-(\Sigma_{kl} a_{ik} b_{jl} x_{kl} - p_{ij}) \geqslant 0$. This approach, however, increases the number of objective variables to be considered.

[38] P. Hyllus and J. Eisert, New J. Phys. **8**, 51 (2006).

[39] S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976).

[40] T. Moroder, Diploma thesis, Institut für Theoretische Physik I, Universität Erlangen-Nürnberg, Germany, 2005.

[41] K. C. Toh, R. H. Tutuncu, and M. J. Todd, Optim. Methods Software **11**, 545 (1999).

[42] J. Löfberg, in Proceedings of the CACSD Conference, Taipei, Taiwan, 2004 (unpublished), pp. 284–289.

[43] T. Yamamoto, J. Shimamura, S. K. Özdemir, M. Koashi, and N. Imoto, Phys. Rev. Lett. **95**, 040503 (2005).

[44] J.-C. Boileau, R. Laflamme, M. Laforest, and C. R. Myers, Phys. Rev. Lett. **93**, 220501 (2004).

[45] A. Chefles, Contemp. Phys. **41**, 401 (2000).

[46] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[47] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[48] A. Peres, Phys. Lett. A **128**, 19 (1988).

[49] M. Dušek, M. Jahma, and N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).

[50] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. A **67**, 032310 (2003).

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

[52] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[53] A. Acín, S. Massar, and S. Pironio, New J. Phys. **8**, 126 (2006).

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

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

[56] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[57] In its original proposal, the four-plus-two-state protocol was meant to operate with weak coherent pulses as signal states [56]. Here we refer to the single-photon version of this protocol.

[58] S. N. Molotkov and S. S. Nazin, JETP Lett. **63**, 924 (1996).

[59] S. N. Molotkov, JETP **87**, 288 (1998).

[60] B.-S. Shi, Y.-K. Jiang, and G.-C. Guo, Appl. Phys. B: Lasers Opt. **70**, 415 (2000).

[61] Chi-Hang Fred Fung and H.-K. Lo, Phys. Rev. A **74**, 042342 (2006).

[62] J. M. Renes, Phys. Rev. A **70**, 052314 (2004).

[63] The main motivation behind this protocol is that it can be proven to be secure also against a hypothetical Eve only limited by the no-signalling principle [53]. In its original proposal, Alice and Bob share a noisy quantum channel that distributes pairs of qubits in the maximally entangled state $|\psi\rangle_{AB} = 1/\sqrt{2}(|00\rangle + |11\rangle)$. These pairs are then measured by Alice and Bob. Here, however, we consider a prepare-and-measure version of this scheme with Alice being the source of the signal states that are sent to Bob.