One-way quantum key distribution: Simple upper bound on the secret key rate

Tobias Moroder,[1,2] Marcos Curty,[1] and Norbert Lütkenhaus[1,2]
[1]*Institute of Theoretical Physics I and Max-Planck Research Group, Institute of Optics, Information and Photonics, University Erlangen-Nuremberg, Staudtstrasse 7, 91058 Erlangen, Germany*
[2]*Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1*
(Received 18 April 2006; published 1 November 2006)

We present a simple method to obtain an upper bound on the achievable secret key rate in quantum key distribution (QKD) protocols that use only unidirectional classical communication during the public-discussion phase. This method is based on a necessary precondition for one-way secret key distillation; the legitimate users need to prove that there exists no quantum state having a symmetric extension that is compatible with the available measurements results. The main advantage of the obtained upper bound is that it can be formulated as a semidefinite program, which can be efficiently solved. We illustrate our results by analyzing two well-known qubit-based QKD protocols: the four-state protocol and the six-state protocol.

DOI: 10.1103/PhysRevA.74.052301 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Mn

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] allows two parties (Alice and Bob) to generate a secret key despite the computational and technological power of an eavesdropper (Eve) who interferes with the signals. This secret key is the essential ingredient of the one-time-pad or Vernam cipher [3], which can provide information-theoretic secure communications.

Practical QKD protocols distinguish two phases in order to generate a secret key: a quantum phase and a classical phase. In the quantum phase a physical apparatus generates classical data for Alice and Bob distributed according to a joint probability distribution $p(a_i,b_j)\equiv p_{ij}$. In the classical phase, Alice and Bob try to distill a secret key from p_{ij} by means of a public discussion over an authenticated classical channel.

Two types of QKD schemes are used to create the correlated data p_{ij}. In *entanglement based* (EB) schemes, a source, which is assumed to be under Eve's control, produces a bipartite quantum state ρ_{AB} that is distributed to Alice and Bob. Eve could even have a third system entangled with those given to the legitimate users. Alice and Bob measure each incoming signal by means of two *positive operator valued measures* (POVM) [4] $\{A_i\}$ and $\{B_j\}$, respectively, and they obtain $p_{ij}=\mathrm{Tr}(A_i\otimes B_j\rho_{AB})$.

In an ideal *prepare and measure* (PM) scheme, Alice prepares a pure state $|\varphi_i\rangle$ with probability p_i and sends it to Bob. On the receiving side, Bob measures each received signal with a POVM $\{B_j\}$. The signal preparation process in PM schemes can be also thought of as follows [5]: First, Alice produces the bipartite state $|\psi_{\mathrm{source}}\rangle_{AB}=\Sigma_i\sqrt{p_i}|\alpha_i\rangle_A|\varphi_i\rangle_B$ and, afterwards, she measures the first subsystem in the orthogonal basis $|\alpha_i\rangle_A$ corresponding to the measurements $A_i=|\alpha_i\rangle_A\langle\alpha_i|$. This action generates the (nonorthogonal) signal states $|\varphi_i\rangle$ with probabilities p_i. In PM schemes the reduced density matrix of Alice, $\rho_A=\mathrm{Tr}_B(|\psi_{\mathrm{source}}\rangle_{AB}\langle\psi_{\mathrm{source}}|)$, is fixed and cannot be modified by Eve. 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 they form a tomographic complete set of Alice's Hilbert space [6,7]. In the most general PM scheme Alice is free to prepare arbitrary states ρ_i instead of only pure states $|\varphi_i\rangle$. One can apply the same framework as for the ideal PM scheme, as reviewed in Appendix A. However, in the rest of this paper we only consider the case of an ideal PM scheme, as described above.

From now on, we will consider that p_{ij} and $\{A_i\otimes B_j\}$ refer always to the complete set of measurements, i.e., they include also the observables $\{C_k\otimes\mathbb{1}\}$ for PM schemes.

The public discussion performed by Alice and Bob during the classical phase of QKD can involve either one-way or two-way classical communication. Two-way classical communication is more robust than one-way in terms of the amount of errors that the QKD protocol can tolerate in order to distill a secret key [8]. However, the first security proof of QKD by Mayers [9], and the most commonly known proof by Shor and Presskill [10] are based on one-way communications, and many other security proofs of QKD belong also to this last paradigm [11,12]. Moreover, any two-way communication protocol includes a final nontrivial step that is necessarily only one-way, so that the study of one-way communication is also useful for the study of two-way communication.

In this paper we concentrate on one-way classical communication protocols during the public discussion phase. Typically, these schemes consist of three steps: local preprocessing of the data, information reconciliation to correct the data, and privacy amplification to decouple the data from Eve [13]. Depending on the allowed direction of communication, two different cases must be considered. *Direct communication* refers to communication from Alice to Bob, *reverse reconciliation* allows communication from Bob to Alice only. (See, for instance, Refs. [14,15].) We will consider only the case of direct communication. Expressions for the opposite scenario, i.e., reverse reconciliation, can be directly obtained simply by renaming Alice and Bob. Note that for typical experiments, the joint probability distribution p_{ij} is not symmetric, so that the qualitative statements for both cases will differ.

We address the question of how much secret key can be obtained from the knowledge of p_{ij} and $\{A_i\otimes B_j\}$. This is one of the most important figures of merit in order to compare the performance of different QKD schemes. We consider the so-called *trusted device scenario*, where Eve cannot modify the actual detection devices employed by Alice and Bob. (See Refs. [7,16].) We assume that the legitimate users have complete knowledge about their detection devices, which are fixed by the actual experiment.

In the last years, several lower and upper bounds on the secret key rate for particular one-way QKD schemes have been proposed. The lower bounds come from protocols that have been proven to be secure [10–12,17–19]. The upper bounds are generally derived by considering some particular eavesdropping attack and by determining when this attack can defeat QKD [18–22]. Unfortunately, to evaluate these known bounds for general QKD protocols is not always a trivial task. Typically, it demands to solve difficult optimization problems, which can be done only for some particular QKD protocols [19].

In this paper we present a simple method to obtain an upper bound on the secret key rate for general one-way QKD protocols. The obtained upper bound will not be tight for all QKD schemes, but it has the advantage that it is straightforward to evaluate in general since it can be formulated as a semidefinite program [23,24]. Such instances of convex optimization problems can be efficiently solved, for example, by means of interior-point methods [23,24]. Our analysis is based on a necessary precondition for one-way QKD: The legitimate users need to prove that there exists no quantum state having a symmetric extension that is compatible with the available measurement results [25]. This kind of states (with symmetric extensions) have been recently analyzed in Refs. [26–28].

The paper is organized as follows. In Sec. II we review some known upper bounds on the secret key rate using one-way post-processing techniques. Section III includes the main result of the paper. Here we introduce a straightforward method to obtain an upper bound on the secret key rate for one-way QKD. This result is then illustrated in Sec. IV for two well-known qubit-based QKD protocols: the four-state [2] and the six-state [29] QKD schemes. We select these two particular QKD schemes because they allow us to compare our results with already known upper bounds in the literature [18–22]. Then in Sec. V we present our conclusions. The paper includes also two Appendixes. In Appendix A we consider very briefly the case of QKD based on mixed signal states instead of pure states and translate the necessary precondition into this more general framework. Finally, Appendix B contains the semidefinite program needed to actually solve the upper bound derived in Sec. III.

II. KNOWN UPPER BOUNDS

Different upper bounds on the secret key rate for one-way QKD have been proposed in the last years. These results either apply to a specific QKD protocol [20–22], or they are derived for different starting scenarios of the QKD scheme [17–19], e.g., one where Alice and Bob are still free to design suitable measurements.

Once Alice and Bob have performed their measurements during the quantum phase of the protocol, they are left with two classical random variables A and B, respectively, satisfying an observed joint probability distribution $p(a_i,b_j) \equiv p_{ij}$. On the other hand, Eve can keep her quantum state untouched and delay her measurement until the public-discussion phase, realized by Alice and Bob, has finished.

In order to provide an upper bound on the secret key rate it is sufficient to consider only a particular eavesdropping attack. For instance, we can restrict ourselves to collective attacks [18,19]. This situation can be modelled by assuming that Alice and Bob have access to independent realizations of two classical random variables A and B, respectively, distributed according to the observed probability distribution p_{ij}. On the other hand, Eve has access to a quantum state $\rho_E^{i,j}$ which is conditioned on Alice and Bob's values of their variables. In Refs. [18,19] Renner *et al.* obtain an upper bound for the one-way secret key rate that applies exactly to this scenario, see also Ref. [30].

In particular the authors of Refs. [18,19] let Alice further process her classical random variable A by two *classical to quantum channels*, denoted by $\sigma_U \leftarrow A$ and $\sigma_V \leftarrow A$. This kind of channel, $\sigma \leftarrow A$, defines a map between the values a_i of the random variable A to the corresponding quantum states σ^i. The information which is encoded in the quantum state of system U represents the final secret key, while the information encoded in system V contains the broadcasted information. Once this preprocessing operation has been done, we can assume that Alice, Bob, and Eve share an unlimited number of copies of the quantum

$$\rho_{UVBE} = \sum_{i,j} p_{ij} \sigma_U^i \otimes \sigma_V^i \otimes |j\rangle_B\langle j| \otimes \rho_E^i, \tag{1}$$

with $\rho_E^i = \sum_j p(b_j|a_i)\rho_E^{i,j}$ and $\{|j\rangle_B\}_j$ forming an orthonormal basis. Note that Eve's information is encoded in system E and V, while Bob's information is stored in system B and V.

Let us recall some definitions and notations from information theory. The von Neumann entropy $S(\rho_A) \equiv S(A)$ of a quantum state ρ_A defined on the Hilbert space $\mathcal{H}_A$ is given by $S(A) = -\mathrm{Tr}(\rho_A \ln \rho_A)$. The capital letter identifies the system of the quantum state. The von Neumann entropy $S(A,B)$ of a bipartite quantum state ρ_{AB} is in a similar way, $S(A,B) = -\mathrm{Tr}(\rho_{AB} \ln \rho_{AB})$, while $S(A)$ would now correspond to the entropy of the reduced quantum state $\rho_A = \mathrm{Tr}_B(\rho_{AB})$. The conditional von Neumann entropy $S(A|B)$ is defined as the difference of von Neumann entropies $S(A|B) = S(A,B) - S(B)$.

From Refs. [18,19] we learn that the one-way secret key rate $K_{\rightarrow}$ is bounded from above by

$$K_{\rightarrow} \leq \sup_{\substack{\sigma_U \leftarrow A \\ \sigma_V \leftarrow A}} S(U|E,V) - S(U|B,V), \tag{2}$$

where the supremum runs over all possible classical to quantum channels $\sigma_U \leftarrow A$ and $\sigma_V \leftarrow A$. The conditional von Neumann entropies in Eq. (2) are evaluated on the quantum state ρ_{UVBE} by partial tracing out the remaining systems. Unfortunately, in order to evaluate the upper bound given by Eq. (2) one must solve the optimization over the two classical to quantum channels; a task which is hard to evaluate even for the simplest QKD protocols.

Another upper bound that applies to the QKD scenario that we consider here is the Csiszár and Körner's secret key rate for the one-way *classical* key-agreement scenario [31]. Suppose that Alice, Bob, and Eve have access to many independent realizations of three random variables A, B, and E, respectively, that are distributed according to the joint probability distribution $p(a_i,b_j,e_k)$. Csiszár and Körner showed that the one-way secret key rate is given by [31]

$$R_{\rightarrow}(A;B|E) = \sup_{\substack{U\leftarrow A\\ V\leftarrow U}} H(U|E,V) - H(U|B,V). \tag{3}$$

The single letter optimization ranges over two classical channels characterized by the transition probabilities $Q(u_l|a_i)$ and $R(v_m|u_l)$, and where the conditional Shannon entropy is defined as $H(U|E,V)=-\sum p(u_l,e_k,v_m)\ln p(u_l|e_k,v_m)$. The first channel produces the secret key U, while the second channel creates the broadcasted information V.

Note that Eq. (3) provides also an upper bound on $K_{\rightarrow}$. Eve can always measure her quantum state $\rho_E^{i,j}$ by a POVM $\{E_k\}$. As a result, Alice, Bob, and Eve share the tripartite probability distribution $p(a_i,b_j,e_k)=p_{ij}\,\mathrm{Tr}(E_k\rho_E^{i,j})$. Unfortunately, the optimization problem that one must solve in order to obtain $R_{\rightarrow}(A;B|E)$ is also nontrivial, and its solution is only known for particular examples. (See Ref. [32].)

Finally, an easy computable upper bound on $K_{\rightarrow}$ is given by the classical mutual information $I(A;B)$ between Alice and Bob [33]. This quantity is defined in terms of the Shannon entropy $H(A)=-\sum p(a_i)\ln p(a_i)$ and the Shannon joint entropy $H(A,B)=-\sum p(a_i,b_j)\ln p(a_i,b_j)$ as

$$I(A;B) = H(A) + H(B) - H(A,B). \tag{4}$$

The mutual information represents an upper bound on the secret key rate for *arbitrary* public communication protocols, hence in particular for one-way communication protocols [33], i.e.,

$$K_{\rightarrow} \le R_{\rightarrow}(A;B|E) \le I(A;B). \tag{5}$$

To evaluate $I(A;B)$ for the case of QKD, we only need to use as $p(a_i,b_j)$ the correlated data p_{ij}.

III. UPPER BOUND ON $K_{\rightarrow}$

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

$$\mathcal{S} = \{\rho_{AB}|\mathrm{Tr}(A_i\otimes B_j\rho_{AB}) = p_{ij},\ \forall\ i,j\}. \tag{6}$$

By definition, every state $\rho_{AB}\in\mathcal{S}$ can represent the state shared by Alice and Bob before their measurements [34].

Now the idea is simple: just impose some *particular* eavesdropping strategy for Eve, and then use one of the already known upper bounds. (See also Ref. [35].) The upper bound obtained represents an upper bound for *any* possible eavesdropping strategy. The method can be described with the following three steps.

(1) Select a particular eavesdropping strategy for Eve. This strategy is given by the choice of a tripartite quantum state ρ_{ABE} and a POVM $\{E_k\}$ to measure Eve's signals. The only restriction here is that the chosen strategy must not alter the observed data, i.e., $\mathrm{Tr}_E(\rho_{ABE})\in\mathcal{S}$.

(2) Calculate the joint probability distribution $p_{ijk}=\mathrm{Tr}(A_i\otimes B_j\otimes E_k\rho_{ABE})$.

(3) Use an upper bound for $K_{\rightarrow}$ given the probability distribution p_{ijk}. Here we can use, for instance, the classical one-way secret key rate $R_{\rightarrow}(A;B|E)$ or just the mutual information between Alice and Bob $I(A;B)$ which is straightforward to calculate.

This method can be improved by performing an optimization over all possible measurements on Eve's system and over all possible tripartite states that Eve can access [36]. This gives rise to a set of possible extensions $\mathcal{P}$ of the observed bipartite probability distribution p_{ij} for the random variables A and B to a tripartite probability distribution p_{ijk} for the random variables A, B, and E. Now the upper bound is given by

$$K_{\rightarrow} \le \inf_{\mathcal{P}} B_{\rightarrow}, \tag{7}$$

with $B_{\rightarrow}$ representing the chosen quantity in step (3).

In Sec. III A we present a necessary precondition for one-way QKD. In particular, Alice and Bob need to prove that there exists no quantum state having a symmetric extension that is compatible with the available measurements results [25]. Motivated by this necessary precondition, we introduce a special class of eavesdropping strategies for Eve in Sec. III B. These strategies are based on a decomposition of quantum states similar to the best separability approximation [37,38], but now for states with symmetric extensions. The general idea followed here is similar to that presented in Ref. [35] for two-way upper bounds on QKD.

A. States with symmetric extensions and one-way QKD

A quantum state ρ_{AB} is said to have a symmetric extension to two copies of system B if and only if there exists a tripartite state $\rho_{ABB'}$ with $\mathcal{H}_B=\mathcal{H}_{B'}$ which fulfills the following two properties [26]:

$$\mathrm{Tr}_{B'}(\rho_{ABB'}) = \rho_{AB}, \tag{8}$$

$$P\rho_{ABB'}P = \rho_{ABB'}, \tag{9}$$

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

States with symmetric extension play an important role in quantum information theory, as noted recently. They can deliver a complete family of separability criteria for the bipartite [26,27] and for the multipartite case [28], and they provide a constructive way to create local hidden variable theories for quantum states [39]. Moreover, they are related to the capacity of quantum channels [40]. Most important, a connection to one-way QKD has also been noticed.

Observation 1 [25]. If the observed data p_{ij} originate from a quantum state ρ_{AB} which has a symmetric extension to two copies of system B, then the secret key rate for unidirectional communication $K_{\rightarrow}$ from Alice to Bob vanishes.

Proof. Suppose that the observed data p_{ij} originate from a state ρ_{AB} which has a symmetric extension to two copies of system B. Suppose as well that the third subsystem of the extended tripartite state $\rho_{ABB'}$ is in Eve's hands, i.e., $\rho_{ABE} = \rho_{ABB'}$. This results in equal marginal states for Alice-Bob and Alice-Eve, i.e., $\rho_{AB}=\rho_{AE}$. From Alice's perspective the secret key distillation task is then completely symmetric under interchanging Bob and Eve. Since we restrict ourselves to unidirectional classical communication from Alice to Bob only, we find that it is impossible for Bob to break this symmetry. That is, if Alice tries to generate a secret key with Bob her actions would automatically create exactly the same secret key with Eve. To complete the proof we need to verify that Eve can access the symmetric extension $\rho_{ABB'}$ of ρ_{AB} in both kinds of QKD schemes, EB schemes and PM schemes. It was demonstrated in Ref. [6] that Eve can always create a purification of the original state ρ_{AB}, which means that Eve can have access to the symmetric extension. ■

Remark 1. A quantum state ρ_{AB} has a symmetric extension to two copies of system B if and only if there exists a tripartite state ρ_{ABE} with equal marginal states for Alice-Bob and Alice-Eve, i.e., $\rho_{AB}=\rho_{AE}$.

Proof. If a quantum state ρ_{AB} has a symmetric extension this automatically implies equal marginal states for Alice-Bob and Alice-Eve. For the other direction, suppose that there exists a tripartite state $\tilde{\rho}_{ABE}$ with equal marginals, but which is not symmetric under interchange of subsystems B and E. Then the state $P\tilde{\rho}_{ABE}P$ is also a possible tripartite state with equal marginals. This allows to construct the symmetric extension of the state ρ_{AB} as $\rho_{ABE}=1/2(\tilde{\rho}_{ABE}+P\tilde{\rho}_{ABE}P)$. ■

There exists entangled states which do have symmetric extensions [26,27]. Hence, accordingly to Observation 1, although these states are entangled and therefore potentially useful for two-way QKD [6], they are nevertheless useless for one-way QKD in the corresponding direction.

We define the best extendibility approximation of a given state ρ_{AB} as the decomposition of ρ_{AB} into a state with symmetric extension, that we denote as σ_{ext}, and a state without symmetric extension ρ_{ne}, while maximizing the weight of the extendible part σ_{ext} [41], i.e.,

$$\rho_{AB} = \max_{\lambda} \lambda \sigma_{\text{ext}} + (1-\lambda)\rho_{\text{ne}}. \tag{10}$$

This definition follows the same spirit as the best separability approximation introduced in Refs. [37,38]. Since the set of all extendible quantum states forms a closed and convex set [27], the maximum in Eq. (10) always exists. We denote the maximum weight of extendibility of ρ_{AB} as $\lambda_{\max}(\rho_{AB})$, where $0 \le \lambda_{\max}(\rho_{AB}) \le 1$ is satisfied.

Given an equivalence class $\mathcal{S}$ of quantum states, we define the maximum weight of extendibility within the equivalence class, denoted as $\lambda_{\max}^{\mathcal{S}}$, as

$$\lambda_{\max}^{\mathcal{S}} = \max\{\lambda_{\max}(\rho_{AB}) | \rho_{AB} \in \mathcal{S}\}. \tag{11}$$

This parameter is related to the necessary precondition for one-way secret key distillation by the following observation.

Observation 2. Assume that Alice and Bob can perform local measurements with POVM elements A_i and B_j, respectively, to obtain the joint probability distribution of the outcomes p_{ij} on the distributed quantum state ρ_{AB}. Then the following two statements are equivalent: (1) The correlations p_{ij} can originate from an extendible state. (2) The maximum weight of extendibility $\lambda_{\max}^{\mathcal{S}}$ within the equivalence class of quantum states $\mathcal{S}$ compatible with the observed data p_{ij} satisfies $\lambda_{\max}^{\mathcal{S}}=1$.

Proof. If p_{ij} can originate from an extendible state, then there exists a σ_{ext} such as $\sigma_{\text{ext}} \in \mathcal{S}$. Moreover, we have that any extendible state satisfies $\lambda_{\max}(\sigma_{\text{ext}})=1$. The other direction is trivial. ■

Let us define $\mathcal{S}_{\max}$ as the equivalence class of quantum states composed of those states $\rho_{AB} \in \mathcal{S}$ that have maximum weight of extendibility. It is given by

$$\mathcal{S}_{\max} = \{\rho_{AB} \in \mathcal{S} | \lambda_{\max}(\rho_{AB}) = \lambda_{\max}^{\mathcal{S}}\}. \tag{12}$$

B. Eavesdropping model

An eavesdropping strategy for our purpose is completely characterized by selecting the overall tripartite quantum state ρ_{ABE} and the measurement operators $\{E_k\}$. Again, the only restriction here is that $\text{Tr}_E(\rho_{ABE}) \in \mathcal{S}$. We consider that Eve chooses a purification $\rho_{ABE}=|\Phi\rangle_{ABE}\langle\Phi|$ of a state ρ_{AB} taken from the equivalence class $\mathcal{S}_{\max}$.

The quantum states σ_{ext} and ρ_{ne} of the best extendibility approximation of ρ_{AB} can be written in terms of their spectral decomposition as [42]

$$\sigma_{\text{ext}} = \sum_i q_i |\phi_i\rangle_{AB}\langle\phi_i|, \tag{13}$$

$$\rho_{\text{ne}} = \sum_i p_i |\psi_i\rangle_{AB}\langle\psi_i|, \tag{14}$$

with $\langle\phi_i|\phi_j\rangle=\langle\psi_i|\psi_j\rangle=0$ for all $i \neq j$. A possible purification of the state ρ_{AB} is given by

$$|\Phi\rangle_{ABE} = \sum_i \sqrt{\lambda_{\max}^{\mathcal{S}} q_i} |\phi_i\rangle_{AB}|e_i\rangle_E + \sum_j \sqrt{(1-\lambda_{\max}^{\mathcal{S}})p_j}|\psi_j\rangle_{AB}|f_j\rangle_E, \tag{15}$$

where the states $\{|e_i\rangle_E, |f_j\rangle_E\}$ form an orthogonal bases on Eve's subsystem.

It is important to note that in both kinds of QKD schemes, EB schemes and PM schemes, Eve can always have access to the state $|\Phi\rangle_{ABE}$ given by Eq. (15). This has been shown in Ref. [6]. In an EB scheme this is clear since Eve is the one who prepares the state ρ_{AB} and who distributes it to Alice and Bob. In the case of PM schemes we need to show additionally that Eve can obtain the state $|\Phi\rangle_{ABE}$ by interaction with Bob's system only. In the Schmidt decomposition the state prepared by Alice, $|\psi_{\text{source}}\rangle_{AB}$, can be written as $|\psi_{\text{source}}\rangle = \sum_i c_i |u_i\rangle_A |v_i\rangle_B$. Then the Schmidt decomposition of $|\Phi\rangle_{ABE}$, with respect to system A and the composite system BE, is of the form $|\Phi\rangle_{ABE} = \sum_i c_i |u_i\rangle_A |\tilde{e}_i\rangle_{BE}$ since c_i and $|u_i\rangle_A$ are fixed by the known reduced density matrix ρ_A to the corresponding values of $|\psi_{\text{source}}\rangle_{AB}$. Then one can find 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.

For simplicity, we consider a special class of measurement strategies for Eve. This class of measurements can be thought of as a two step procedure.

(1) First, Eve distinguishes contributions coming from the part with symmetric extension and from the part without symmetric extension of ρ_{AB}. The corresponding measurements are projections of Eve's subsystem onto the orthogonal subspaces $\Pi_{\text{ext}}=\Sigma_i|e_i\rangle_E\langle e_i|$ and $\Pi_{\text{ne}}=\Sigma_j|f_j\rangle_E\langle f_j|$.

(2) Afterwards, Eve performs a refined measurement strategy on each subspace separately. As we will see, only the nonextendible part ρ_{ne} might allow Alice and Bob to distill a secret key by direct communication; from the extendible part no secret key can be obtained.

This special measurement class determines Eve's random variable E. Because of the special design of the measurement strategy, it is convenient to associate an own random variable for each measurement step. Therefore, we consider Eve's random variable E as a pair of two different random variables $E=(T,\tilde{E})$. The variable T corresponds to the outcome of the projection measurement, while $\tilde{E}$ corresponds to the outcome arising from the second step in the strategy. With probability $1-\lambda_{\max}^{\mathcal{S}}$ Eve finds that Alice and Bob share the nonextendible part of ρ_{AB}. After this first measurement step, the conditional quantum state shared by Alice, Bob, and Eve, denoted as $\rho_{ABE}^{\text{ne}}=|\Phi_{\text{ne}}\rangle_{ABE}\langle\Phi_{\text{ne}}|$, corresponds to a purification of ρ_{ne}, i.e.,

$$|\Phi_{\text{ne}}\rangle_{ABE}=\sum_j\sqrt{p_j}|\psi_j\rangle_{AB}|f_j\rangle_E. \tag{16}$$

Next we provide an upper bound for $K_{\rightarrow}$ that arises from this special eavesdropping strategy. Moreover, as we will see, the obtained upper bound is straightforward to calculate.

C. Resulting upper bound

For the special eavesdropping strategy considered in Sec. III B, we will show that we can restrict ourselves to the nonextendible part ρ_{ne} of a given ρ_{AB} only. As a consequence, the resulting upper bound will only depend on this nonextendible part. This motivates the definition of a new equivalence class of quantum states $\mathcal{S}_{\max}^{\text{ne}}$, defined as

$$\mathcal{S}_{\max}^{\text{ne}}=\{\rho_{\text{ne}}(\rho_{AB})|\rho_{AB}\in\mathcal{S}_{\max}\}, \tag{17}$$

where $\rho_{\text{ne}}(\rho_{AB})$ represents the nonextendible part in a valid best extendibility approximation of $\rho_{AB}\in\mathcal{S}_{\max}$ given by Eq. (10). To simplify the notation, from now on we will write ρ_{ne} instead of $\rho_{\text{ne}}(\rho_{AB})$. The possibility to concentrate on the nonextendible parts only is given by the following theorem.

Theorem 1. Suppose Alice's and Bob's systems are subjected to measurements described by the POVMs $\{A_i\}$ and $\{B_j\}$, respectively, and their outcomes follow the probability distribution p_{ij}. They try to distill a secret key by unidirectional classical communication from Alice to Bob only. The secret key rate, denoted as $K_{\rightarrow}$, is bounded from above by

$$K_{\rightarrow}\leq(1-\lambda_{\max}^{\mathcal{S}})\inf_{\mathcal{P}^*}R_{\rightarrow}(A;B|E), \tag{18}$$

where $R_{\rightarrow}(A;B|E)$ denotes the classical one-way secret key rate given by Eq. (3) for a tripartite probability distribution $\tilde{p}_{ijk}\in\mathcal{P}^*$. The set $\mathcal{P}^*$ considers all possible POVMs $\{E_k\}$ which Eve can perform on a purification $|\Phi_{\text{ne}}\rangle_{ABE}$ of the *nonextendible part* $\rho_{\text{ne}}\in\mathcal{S}_{\max}^{\text{ne}}$ only, i.e., $\tilde{p}_{ijk}=\text{Tr}[A_i\otimes B_j\otimes E_k(|\Phi_{\text{ne}}\rangle_{ABE}\langle\Phi_{\text{ne}}|)]$.

Proof. In order to derive Eq. (18) we have considered only a particular class of eavesdropping strategies for Eve as described in Sec. III B. This class defines a subset $\mathcal{P}'$ of the set of all possible extensions $\mathcal{P}$ of the observed data p_{ij} to a general tripartite probability distribution p_{ijk}, which are considered in the upper bound given by Eq. (7). We have, therefore, that

$$K_{\rightarrow}\leq\inf_{\mathcal{P}}R_{\rightarrow}(A;B|E)\leq\inf_{\mathcal{P}'}R_{\rightarrow}(A;B|E). \tag{19}$$

As introduced in Sec. III B, Eve's random variable $E=(T,\tilde{E})$ is modelled as a pair of two random variables T and $\tilde{E}$, corresponding to the special designed measurement strategy. The variable T identifies the projection measurement, while $\tilde{E}$ corresponds to the refined measurement. We denote the secret key rate for this case by $K_{\rightarrow}(A;B|\tilde{E},T)$.

For this one-way secret key rate $K_{\rightarrow}(A;B|\tilde{E},T)$ we get

$$\begin{aligned}K_{\rightarrow}(A;B|\tilde{E},T)&=\sup_{\substack{U\leftarrow A\\V\leftarrow U}}H(U|V,\tilde{E},T)-H(U|V,B)\\&\leq\sup_{\substack{U\leftarrow A\\V\leftarrow U}}H(U|V,\tilde{E},T)-H(U|V,B,T)\\&\leq\sup_{\substack{U\leftarrow(A,T)\\V\leftarrow U}}H(U|V,\tilde{E},T)-H(U|V,B,T).\end{aligned} \tag{20}$$

In the first line we just use the definition of the classical secret key rate given by Eq. (3). The first inequality comes from the fact that conditioning can only decrease the entropy, i.e., $H(U|V,B)\geq H(U|V,B,T)$. For the last inequality, we give Alice also access to the random variable T, additionally to her variable A, over which she can perform the postprocessing with the classical channels. Altogether Eq. (20) tells that if Eve announces publicly the value of the variable T, containing the information whether Alice and Bob share the extendible or nonextendible part, this action can only enhance the ability of Alice and Bob to create a secret key.

Next, we have that

$$\begin{aligned}&\sup_{\substack{U\leftarrow(A,T)\\V\leftarrow U}}H(U|V,\tilde{E},T)-H(U|V,B,T)\\&\quad=\sup_{\substack{U\leftarrow(A,T)\\V\leftarrow U}}\sum_k p(t_k)\{H(U|V,\tilde{E},t_k)-H(U|V,B,t_k)\}\\&\quad=\sum_k p(t_k)\sup_{\substack{U\leftarrow(A,t_k)\\V\leftarrow U}}\{H(U|V,\tilde{E},t_k)-H(U|V,B,t_k)\}\\&\quad=\sum_k p(t_k)R_{\rightarrow}(A;B|\tilde{E},t_k).\end{aligned} \tag{21}$$

First we rewrite the conditional entropies in terms of an expectation value over the different values t_k of the random variable T. The classical channel $U \leftarrow (A,T)$ acts now independent on each term of the sum. Therefore the supremum can be set into the sum, where the random variable T takes now the specific value t_k. Since $\sup_{U \leftarrow (A,t_k)}$ is equal to $\sup_{U \leftarrow A}$ for t_k fixed, we find on the right-hand side the one-way secret key rate for the conditional three party correlation $p(a_i, b_j, \tilde{e}_l | t_k)$, which we denoted as $R_{\rightarrow}(A;B|\tilde{E},t_k)$.

Combining Eq. (20) and Eq. (21) we have, therefore, that

$$R_{\rightarrow}(A;B|\tilde{E},T) \leq \sum_k p(t_k) R_{\rightarrow}(A;B|\tilde{E},t_k). \tag{22}$$

The random variable T can take only two possible values, which indicates whether Alice and Bob share the extendible or the nonextendible part. From Observation 1 we learn that Alice and Bob cannot draw a secret key out of the extendible part σ_{ext}. Therefore, only the nonextendible part ρ_{ne} can contribute to a positive secret key rate. The corresponding nonextendible probability distribution is given by measurements on the quantum state after this first measurement. As shown in the Sec. III B, this state is exactly the purification of the nonextendible part, which defines exactly the considered extensions $\mathcal{P}^*$. This concludes the proof. ■

The upper bound given by Eq. (18) requires to solve the infimum over all possible extensions $\mathcal{P}^*$. Instead of this optimization, one can just pick a particular state in $\mathcal{S}_{\max}^{\text{ne}}$ and calculate the infimum over all possible measurements $\{E_k\}$ employed by Eve.

Corollary 1. Given a state $\rho_{\text{ne}} \in \mathcal{S}_{\max}^{\text{ne}}$, the secret key rate $K_{\rightarrow}$ is bounded from above by

$$K_{\rightarrow} \leq (1-\lambda_{\max}^{\mathcal{S}}) \inf_{E_k} R_{\rightarrow}^{E_k}(A;B|E), \tag{23}$$

with $R_{\rightarrow}^{E_k}(A;B|E)$ being the classical one-way secret key rate of the tripartite probability distribution $\tilde{p}_{ijk} = \mathrm{Tr}[A_i \otimes B_j \otimes E_k(|\Phi_{\text{ne}}\rangle\langle\Phi_{\text{ne}}|)]$, and where $|\Phi_{\text{ne}}\rangle$ denotes a purification of ρ_{ne}.

Proof. The right-hand side of Eq. (23) is an upper bound of the right-hand side of Eq. (18), because in Eq. (23) we take only a particular state $\rho_{\text{ne}} \in \mathcal{S}_{\max}^{\text{ne}}$, whereas in Eq. (18) we perform the infimum over all possible states $\rho_{\text{ne}} \in \mathcal{S}_{\max}^{\text{ne}}$. ■

The upper bounds provided by Theorem 1 and Corollary 1 still demand solving a difficult optimization problem. Next, we present a simple upper bound on $K_{\rightarrow}$ that is straightforward to calculate. Then, in Sec. IV, we illustrate the performance of this upper bound for two well-known QKD protocols: the four-state [2] and the six-state [29] QKD schemes. We compare our results to other well-known upper bounds on $K_{\rightarrow}$ for these two QKD schemes [18–22].

Corollary 2. The secret key rate $K_{\rightarrow}$ is upper bounded by

$$K_{\rightarrow} \leq (1-\lambda_{\max}^{\mathcal{S}}) I^{\text{ne}}(A;B), \tag{24}$$

where $I^{\text{ne}}(A;B)$ denotes the classical mutual information calculated on the probability distribution $\tilde{p}_{ij} = \mathrm{Tr}(A_i \otimes B_j \rho_{\text{ne}})$ with $\rho_{\text{ne}} \in \mathcal{S}_{\max}^{\text{ne}}$.

Proof. According to Eq. (5), the one-way secret key rate $R_{\rightarrow}(A;B|E)$ is bounded from above by the mutual information $I(A;B)$. Note that the mutual information $I(A;B)$ is an upper bound on the secret key rate for *arbitrary* communication protocols [33]. ■

The main difficulty when evaluating the upper bound given by Eq. (24) for a particular realization of QKD relies on obtaining the parameter $\lambda_{\max}^{\mathcal{S}}$ and the nonextendible state ρ_{ne}. In Appendix B we show how this problem can be cast as a convex optimization problem known as semidefinite program [43]. Such instances of convex optimization problems can be efficiently solved, for example, by means of interior-point methods [23,24].

IV. EVALUATION

In this section we evaluate the upper bound on $K_{\rightarrow}$ given by Eq. (24) for two well-known qubit-based QKD protocols: the four-state [2] and the six-state [29] QKD schemes. We select these two particular QKD schemes because they allow us to compare our results with already known upper bounds on $K_{\rightarrow}$ [18–22]. Let us emphasize, however, that our method can also be used straightforwardly to obtain an upper bound for higher dimensional, more complicated QKD protocols, for which no upper bounds have been calculated yet. By means of semidefinite programming one can easily obtain the maximum weight of extendibility $\lambda_{\max}^{\mathcal{S}}$ and the corresponding nonextendible part ρ_{ne} which suffice for the computation of the upper bound. (See Appendix B.)

In the case of the four-state EB protocol, 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. Note that here we are not using the general approach introduced previously, $|\psi_{\text{source}}\rangle_{AB} = \sum_i \sqrt{p_i} |\alpha_i\rangle_A |\varphi_i\rangle_B$, to model PM schemes, since for these two protocols it is sufficient to consider that the effectively distributed quantum states consist only of two qubits. 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.

We model the transmission channel as a depolarizing channel with error probability e. This defines one possible eavesdropping interaction. In particular, the observed probability distribution p_{ij} is obtained in both protocols by measuring the quantum state $\rho_{AB}(e) = (1-2e)|\psi^+\rangle_{AB}\langle\psi^+| + e/2 \mathbb{1}_{AB}$, where the state $|\psi^+\rangle_{AB}$ represents a maximally entangled two-qubit state as $|\psi^+\rangle_{AB} = 1/\sqrt{2}(|00\rangle_{AB} + |11\rangle_{AB})$, and $\mathbb{1}_{AB}$ denotes the identity operator. The state $\rho_{AB}(e)$ provides a probability distribution p_{ij} that is invariant under interchanging Alice and Bob. This means that for this particular example there is no difference whether we consider direct communication [extension of $\rho_{AB}(e)$ to two copies of system B] or reverse reconciliation [extension of $\rho_{AB}(e)$ to two copies of system A]. The quantum bit error rate (QBER), i.e., the fraction of signals where Alice and Bob's measurements results differ, is given by QBER $= e$.

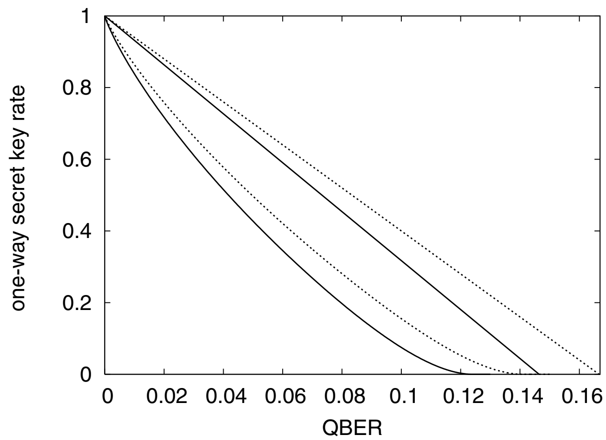

FIG. 1. Upper bound on the one-way secret key rate $K_{\rightarrow}$ given by Eq. (24) for the four-state (solid) and the six-state (dotted) QKD protocols in comparison to known lower bounds on the secret key rate given in Ref. [19]. The equivalence class of states $\mathcal{S}$ is fixed by the observed data p_{ij}, which are generated via measurements onto the state $\rho_{AB}(e)=(1-2e)|\psi^{+}\rangle_{AB}\langle\psi^{+}|+e/2\mathbb{1}_{AB}$. The quantum bit error rate is given by QBER$=e$. Here we assume an asymmetric basis choice to suppress the sifting effect [44].

The resulting upper bounds on $K_{\rightarrow}$ are illustrated in Fig. 1. These results do not include the sifting factor of 1/2 for the four-state protocol (1/3 for the six-state protocol), since this effect can be avoided by an asymmetric basis choice for Alice and Bob [44]. In Fig. 1 we include as well *lower* bounds for the secret key rate obtained in Ref. [19].

Let us consider in more detail the cutoff points for $K_{\rightarrow}$, i.e., the values of QBER for which the secret key rate drops down to zero in Fig. 1. We find that in the four-state protocol (six-state protocol) one-way secret key distillation might only be possible for a QBER<14.6 (QBER$<1/6$). These results reproduce the well-known upper bounds on both protocols from Refs. [20–22]. More recently, a new threshold point for the six-state protocol was obtained in Refs. [18,19], QBER$\lessapprox 16.3$. This result indicates that the upper bound given by Eq. (24) is not tight, since it fails to reproduce this last value.

One could think that this example from Refs. [18,19] concludes that Observation 1 might be only a necessary but not sufficient condition for one-way secret key distillation: there exist bipartite states which are nonextendible, nevertheless no secret key can be obtained from them via one-way postprocessing. However, the example does not include the possibility for Alice and Bob to perform arbitrary one-way LOCC operations onto the quantum state. Therefore the complete characterization of useful quantum states for one-way QKD is still an open problem.

V. CONCLUSION

In this paper we address the fundamental question of how much secret key can be obtained from the classical data that become available once the first phase of QKD is completed. In particular, we restrict ourselves to one-way public communication protocols between the legitimate users. This question has been extensively studied in the literature and analytic expressions for upper and lower bounds on the one-way secret key rate are already known. Unfortunately, to evaluate these expressions for particular QKD protocols is, in general, a nontrivial task. It demands to solve difficult optimization problems for which no general solution is known so far.

Here we provide a simple method to obtain an upper bound on the one-way secret key rate for QKD. It is based on a necessary precondition for one-way secret key distillation: The legitimate users need to prove that there exists no quantum state having a symmetric extension that is compatible with the available measurements results. The main advantage of the method is that it is straightforward to calculate, since it can be formulated as a semidefinite program. Such instances of convex optimization problems can be solved very efficiently. More importantly, the method applies both to prepare and measure schemes and to entanglement based schemes, and it can reproduce most of the already known cutoff points for particular QKD protocols. It is so far unclear whether the precondition that no symmetric extension exists is also sufficient.

ACKNOWLEDGMENTS

The authors wish to thank R. Renner, A. Winter, M. Koashi, J. I. Cirac, D. Bruß, J. M. Renes, W. Mauerer, J. Rigas, H. Häseler, and V. Scholz for very useful discussions, and especially G. O. Myhr for very interesting discussions about Appendix A. This work was supported by the DFG under the Emmy Noether programme, and the European Commission (Integrated Project SECOQC).

APPENDIX A: QKD WITH MIXED SIGNAL STATES

In this appendix we describe very briefly the case of QKD based on mixed quantum states instead of pure states. In particular, we analyze PM schemes, since in EB schemes it is clear that Eve can always distribute mixed states to Alice and Bob, and this situation is already contained in the results included in the preceding sections. More specifically, we translate the necessary precondition for secret key generation by unidirectional communication to the PM mixed state scenario.

In the most general PM scheme, Alice prepares mixed signal states ρ_B^i following a given probability distribution p_i and sends them to Bob. Equivalently, we can think of the preparation process as follows. Suppose that the spectral decomposition of the signal state ρ_B^i is given by $\rho_B^i=\sum_j\lambda_j^i|\varphi_j^i\rangle_B\langle\varphi_j^i|$. This can be interpreted as producing with probability λ_j^i the pure state $|\varphi_j^i\rangle$. Alternatively, ρ_B^i can as well originate from a pure state in a higher dimensional Hilbert space. That is, from a possible purification $|\phi_i\rangle_{A'B}$ of the state ρ_B^i in the composite Hilbert space $\mathcal{H}_{A'}\otimes\mathcal{H}_B$ which reads as

$$|\phi^i\rangle_{A'B}=\sum_j\sqrt{\lambda_j^i}|j\rangle_{A'}|\varphi_j^i\rangle_B. \quad (A1)$$

Now we can use the same formalism as the one for PM schemes based on pure signal states. We can assume that first Alice prepares the tripartite quantum state

$$|\psi_{\text{source}}\rangle_{AA'B} = \sum_{ij} \sqrt{p_i\lambda_j^i}|i\rangle_A|j\rangle_{A'}|\varphi_j^i\rangle_B. \quad \text{(A2)}$$

Afterwards, in order to produce the actual signal state in system B, Alice performs a measurement onto the standard basis of system A only, and completely ignores system A'. Her measurement operators are given by $A_i=|i\rangle_A\langle i|\otimes\mathbb{1}_{A'}$. The produced signal states are sent to Bob who measures them by means of the POVM $\{B_j\}$. Since Eve can only interact with system B, the reduced density matrix of $\rho_{AA'}=\text{Tr}_B(|\psi_{\text{source}}\rangle_{AA'B}\langle\psi_{\text{source}}|)$ is fixed by the actual preparation scheme. This information can be included in the measurement process by adding to the observables measured by Alice and Bob other observables $\{C_{k,AA'}\otimes\mathbb{1}_B\}$ such that they provide complete information on the bipartite Hilbert space of Alice $\mathcal{H}_{AA'}=\mathcal{H}_A\otimes\mathcal{H}_{A'}$. (See also [45].)

The relevant equivalence class of quantum states $\mathcal{S}_{AA'B}$ contains all tripartite quantum states $\rho_{AA'B}$ consistent with the available information during the measurement process. Obviously, Eve can always access every purification $|\Psi_{AA'BE}\rangle$ of a state in $\mathcal{S}_{AA'B}$. Note that the situation is completely equivalent to the case of pure signal states [6].

Now we are ready to rephrase the necessary precondition for one-way secret key distillation for the case of QKD based on mixed states. For direct communication we need to search for symmetric extensions to two copies of system B. That is, if we denote with $\bar{A}$ the bipartite system on Alice's side $\bar{A}\equiv AA'$, we must search for quantum states in the equivalence class $\mathcal{S}_{AA'B}=\mathcal{S}_{\bar{A}B}$ which are extendible to $\rho_{\bar{A}BB'}$. In the case of reverse reconciliation, Eve needs to possess only a copy of system A. Note that the final key is created only from measurements onto this system. Therefore, in order to determine the cutoff points for the key distillation process, one must examine the question whether a four-partite quantum state $\rho_{AA'BE}$ with $\text{Tr}_E(\rho_{AA'BE})\in\mathcal{S}_{AA'B}$ exists such that $\text{Tr}_{A'}(\rho_{AA'BE})$ is exactly the desired symmetric extension to two copies of system A.

APPENDIX B: SEMIDEFINITE PROGRAMS AND SEARCHING FOR $\lambda_{\max}^{\mathcal{S}}$ AND ρ_{ne}

In this appendix we provide a method to obtain the parameter $\lambda_{\max}^{\mathcal{S}}$ and the corresponding nonextendible state ρ_{ne}. In particular, we show how one can cast this problem as a convex optimization problem known as semidefinite programming. Such instances of convex optimization problems appear frequently in quantum information theory and they can be solved very efficiently. There are freely available input tools like, for instance, YALMIP [46], and standard semidefinite programming solvers, see SeDuMi [47] and SDPT3-3.02 [48].

A typical semidefinite problem, also known as primal problem, has the following form:

$$\begin{aligned} &\text{minimize} \quad c^T\mathbf{x}, \\ &\text{subject to} \quad F(\mathbf{x}) = F_0 + \sum_i x_iF_i \geq 0, \end{aligned} \quad \text{(B1)}$$

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 the matrices F_0 and F_i are Hermitian matrices. The goal is to minimize the linear objective function $c^T\mathbf{x}$ subject to a linear matrix inequality constraint $F(\mathbf{x})\geq 0$ [23,24]. (See also [54].)

Any bounded Hermitian operator $\rho_A=\rho_A^\dagger$ acting on a n-dimensional Hilbert space $\mathcal{S}$ can be written in terms of an operator basis, which we shall denote by $\{S_k\}$, satisfying the following three conditions: $\text{Tr}(S_j)=n\delta_{j1}$, $S_j=S_j^\dagger$, and $\text{Tr}(S_jS_{j'})=n\delta_{jj'}$. A possible choice is given by the SU(n) generators. Using this representation, a general bipartite state ρ_{AB} in a d_{AB}-dimensional Hilbert space can be written as

$$\rho_{AB} = \frac{1}{d_{AB}}\sum_{kl} r_{kl}S_k^AS_l^B, \quad \text{(B2)}$$

where the coefficients r_{kl} are given by $r_{kl}=\text{Tr}(S_k^AS_l^B\rho_{AB})$. Note that in order to simplicity the notation, in this appendix we omit the tensor product signs $\otimes$ between the operators. The representation given by Eq. (B2) allows us to describe any bipartite density operator in terms of a fixed number of parameters r_{kl} which can serve as the free parameters in the program.

The knowledge of the Alice and Bob POVMs $\{A_i\}$ and $\{B_j\}$, respectively, and the observed probability distribution p_{ij} determines the equivalence class of compatible states $\mathcal{S}$. Since every POVM element is a Hermitian operator itself, every element can as well be expanded in the appropriate operator basis $A_i=\Sigma_m a_{im}S_m^A$ and $B_j=\Sigma_n b_{jn}S_n^B$.

An arbitrary operator $\rho_{AB}=1/d_{AB}\Sigma r_{kl}S_k^AS_j^B$ belongs to the equivalence class $\mathcal{S}$ if and only if it fulfills the following constraints: In order to guarantee that the operator ρ_{AB} represents a valid quantum state, it must be normalized $\text{Tr}(\rho_{AB})=r_{11}=1$, and it must be a semidefinite positive operator $\rho_{AB}\geq 0$. In addition, it must reproduce the observed data of Alice and Bob. This last requirement imposes the following constraints:

$$\Pr(a_i,b_j) = \sum_{kl} a_{ik}b_{jl}r_{kl} = p_{ij} \quad \forall \ i,j, \quad \text{(B3)}$$

which are linear on the state coefficients r_{kl}. Note that every equality constraint $\Pr(a_i,b_j)=p_{ij}$ can be represented by two inequality constraints as $\Pr(a_i,b_j)-p_{ij}\geq 0$ and $-[\Pr(a_i,b_j)-p_{ij}]\geq 0$.

In order to find the decomposition of a given state $\rho_{AB}=1/d_{AB}\Sigma_{kl}r_{kl}S_k^AS_l^B$ into an extendible part σ_{ext} and a nonextendible part ρ_{ne}, with maximum weight $\lambda_{\max}(\rho_{AB})$ of extendibility, we can proceed as follows. First we rewrite the problem in terms of unnormalized states $\tilde{\sigma}_{\text{ext}}\equiv\lambda\sigma_{\text{ext}}$ and $\tilde{\rho}_{\text{ne}}\equiv(1-\lambda)\rho_{\text{ne}}$ as

$$\rho_{AB} = \min_{\text{Tr}(\tilde{\rho}_{\text{ne}})} \tilde{\sigma}_{\text{ext}} + \tilde{\rho}_{\text{ne}}. \quad \text{(B4)}$$

Now assume that the unnormalized, extendible state is written as $\tilde{\sigma}_{\text{ext}}=1/d_{AB}\Sigma\tilde{e}_{kl}S_k^AS_l^B$, which must form a semidefinite positive operator $\tilde{\sigma}_{\text{ext}}\geq 0$. In the case of direct communication we must impose that $\tilde{\sigma}_{\text{ext}}$ has a symmetric extension $\chi_{ABB'}$ to two copies of system B. That is, $\chi_{ABB'}$ remains invariant under permutation of the systems B and B'. This is only possible if the state $\chi_{ABB'}$ can be written as

$$\chi_{ABB'} = \frac{1}{d_{ABB'}} \sum_{\substack{k \\ l>m}} f_{klm}(S_k^A S_l^B S_m^{B'} + S_k^A S_m^B S_l^{B'}) + \sum_{kl} f_{kll} S_k^A S_l^B S_l^{B'} \tag{B5}$$

with appropriate state coefficients $f_{klm} \forall k$, $\forall l \geq m$. The extension must as well reproduce the original state $\mathrm{Tr}_{B'}(\chi_{ABB'}) = \tilde{\sigma}_{\mathrm{ext}}$, which implies that the state coefficients of $\tilde{\sigma}_{\mathrm{ext}}$ and $\chi_{ABB'}$ are related by

$$f_{kl1} = \tilde{e}_{kl} \quad \forall \ k,l. \tag{B6}$$

Hence, some of the state parameters of $\chi_{ABB'}$ are already fixed by the coefficients of $\tilde{\sigma}_{\mathrm{ext}}$. In addition, the coefficients f_{klm} must form a semidefinite positive operator $\chi_{ABB'} \geq 0$.

Once the states $\rho_{AB} = \Sigma r_{kl} S_k^A S_l^B$ and the unnormalized extendible part $\tilde{\sigma}_{\mathrm{ext}} = \Sigma \tilde{e}_{kl} S_k^A S_l^B$ are fixed, the remaining nonextendible state $\tilde{\rho}_{\mathrm{ne}}$ is determined by the decomposition given by Eq. (B4), and is equal to

$$\tilde{\rho}_{\mathrm{ne}} = \sum (r_{kl} - \tilde{e}_{kl}) S_k^A S_l^B. \tag{B7}$$

This operator must be semidefinite positive $\tilde{\rho}_{\mathrm{ne}} \geq 0$.

In total, the state coefficients of the states in the equivalence class ρ_{AB}, the unnormalized, extendible part in the best extendibility decomposition $\tilde{\sigma}_{\mathrm{ext}}$ and the symmetric extension itself $\chi_{ABB'}$ will constitute the objective variables of the SDP program

$$\mathbf{x} = (r_{kl}, \tilde{e}_{kl}, f_{klm})^T. \tag{B8}$$

This requires a fixed ordering of the set of coefficients. The function to be minimized is the weight on the unnormalized, nonextendible part, $\mathrm{Tr}(\tilde{\rho}_{\mathrm{ne}}) = r_{11} - \tilde{e}_{11}$. Hence the vector c is given by

$$c^T = (\underbrace{1}_{r_{11}}, 0, \ldots, \underbrace{-1}_{\tilde{e}_{11}}, 0, \ldots). \tag{B9}$$

All the semidefinite constraints introduced previously on the state coefficients can be collected into a single linear matrix inequality constraint given by Eq. (B1). The final $F(\mathbf{x})$ collects all these constraints as block matrices on the diagonal.

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[3] G. S. Vernam, J. Am. Inst. Electr. Eng. **45**, 295 (1926).
[4] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[5] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[6] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[7] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. A **71**, 022306 (2005).
[8] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[9] D. Mayers, in *Advances in Cryptology—Proceedings of Crypto '96* (Springer, Berlin, 1996), pp. 343–357.
[10] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[11] H. K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[12] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[13] N. Lütkenhaus, Appl. Phys. B: Lasers Opt. **69**, 395 (1999).
[14] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[15] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).
[16] M. Curty and N. Lütkenhaus, Phys. Rev. A **69**, 042321 (2004).
[17] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).
[18] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[19] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[20] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[21] I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
[22] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[23] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).
[24] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, 2004).
[25] J. I. Cirac and A. Winter (private communication). The idea originates from entanglement distillation by one-way communication [49,40].
[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] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[30] The derivation of the upper bound presented in Refs. [18,19] does not follow a simple optimization procedure according to the description in this paper. Rather, a very elegant technique is used: the authors are able to derive a set of condition on a function such that this function, if it fulfills these conditions, necessarily represents an upper bound on the secret one way key rate.
[31] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[32] T. Holenstein and R. Renner, in *Advances in Cryptology—CRYPTO '05*, edited by V. Shoup (Springer-Verlag, Berlin, 2005), Lecture Notes in Computer Science, pp. 478–493.
[33] U. Maurer and S. Wolf, IEEE Trans. Inf. Theory **45**, 499 (1999).
[34] The equivalence class $\mathcal{S}$ reduces to the trivial one, i.e., it contains only one element up to a global phase, when the measurements realized by Alice and Bob provide complete tomog-

raphic information about ρ_{AB}. This is the case, for instance, in the six-state QKD protocol [29]. Otherwise, $\mathcal{S}$ contains always more than one quantum state.

[35] T. Moroder, M. Curty, and N. Lütkenhaus, Phys. Rev. A **73**, 012311 (2006).

[36] Note that this improvement still does not represent the most general case, since it forces Eve to measure directly her state before the public-discussion phase. In principle, Eve might also use eavesdropping strategies where no measure on her system is performed until the public-discussion phase is completed, or she could even wait to attack the final cryptosystem, that uses the generated key, with her quantum probe. This last scenario is related with the idea of composability [50–52].

[37] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1997).

[38] S. Karnas and M. Lewenstein, J. Phys. A **34**, 6919 (2001).

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

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

[41] From now on, the term extension will always stand for a symmetric extension to two copies of system A or B. We will not make any further distinction between the different types of extension and we simply call the state extendible. The extension to two copies of system A corresponds to reverse reconciliation, and extensions to two copies of system B corresponds to the direct communication case.

[42] If the best extendibility approximation of the state ρ_{AB} is not unique, Eve simply takes one particular decomposition of the possible set of them.

[43] In order to verify only whether the parameter $\lambda_{\max}^{\mathcal{S}}$ is one or not, one can use as well entanglement witnesses of a particular form [53].

[44] H. K. Lo, H. F. C. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).

[45] Note that the preparation scheme is not unique. There are many different ways to actually purify all the signal states ρ_B^i together. For example, every signal state can be purified to the same auxiliary system A', alternatively each signal can as well be purified to a special separated system, say A_i', so that the overall purified system $A'=A_1'\cdots A_n'$ is higher dimensional. This will lead to different reduced density matrices $\rho_{AA'}$. Note however that the exact form of the reduced density matrix $\rho_{AA'}$ has no physical meaning, except for the *a priori* probabilities of the signals on the diagonal.

[46] J. Löfberg, *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004, pp. 284–289, available from http://control.ee.ethz.ch/~joloef/yalmip.php

[47] J. F. Sturm, Optim. Methods Software **10-11**, 625 (1999); also available at http://fewcal.kub.nl/sturm/software/sedumi.html

[48] K. C. Toh, R. H. Tutuncu, and M. J. Todd, Optim. Methods Software **11**, 545 (1999); also available at http://www.math.nus.edu.sg/~mattohkc/sdpt3.html

[49] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[50] R. Renner and R. Koenig, in *Second Theory of Cryptography Conference, TCC 2005*, edited by J. Kilian (Springer, New York, 2005), Vol. 3378 of LNCS, pp. 407–425.

[51] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Second Theory of Cryptography Conference, TCC 2005*, edited by J. Kilian (Springer, New York, 2005), Vol. 3378 of LNCS, pp. 386–406.

[52] M. Ben-Or and D. Mayers, e-print quant-ph/0409062.

[53] T. Moroder, Diploma thesis, University Erlangen-Nuremberg, 2005.

[54] Note that two (or even more) linear matrix inequalities constraints $\tilde{F}(\mathbf{x})\geq 0,\bar{F}(\mathbf{x})\geq 0$, can be combined into a single new linear matrix inequality constraint as $F(\mathbf{x})=\begin{pmatrix}\tilde{F}(\mathbf{x}) & 0\\ 0 & \bar{F}(\mathbf{x})\end{pmatrix}\equiv\tilde{F}(\mathbf{x})\oplus\bar{F}(\mathbf{x})\geq 0$.