Upper bounds for the secure key rate of decoy state quantum key distribution

Marcos Curty[1], Tobias Moroder[2,3], Xiongfeng Ma[2], Hoi-Kwong Lo[4] and Norbert Lütkenhaus[2,3]
[1] *ETSI Telecomunicación, Department of Signal Theory and Communications,*
University of Vigo, Campus Universitario, E-36310 Vigo (Pontevedra), Spain
[2] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada*
[3] *Quantum Information Theory Group, Institut für Theoretische Physik I,*
and Max-Planck Research Group, Institute of Optics, Information and Photonics,
University of Erlangen-Nürnberg, 91058 Erlangen, Germany
[4] *Center for Quantum Information and Quantum Control (CQIQC),*
Department of Electrical & Computer Engineering and Department of Physics,
University of Toronto, Toronto, ON, M5S 3G4, Canada

The use of decoy states in quantum key distribution (QKD) has provided a method for substantially increasing the secret key rate and distance that can be covered by QKD protocols with practical signals. The security analysis of these schemes, however, leaves open the possibility that the development of better proof techniques, or better classical post-processing methods, might further improve their performance in realistic scenarios. In this paper, we derive upper bounds on the secure key rate for decoy state QKD. These bounds are based basically only on the classical correlations established by the legitimate users during the quantum communication phase of the protocol. The only assumption about the possible post-processing methods is that double click events are randomly assigned to single click events. Further we consider only secure key rates based on the uncalibrated device scenario which assigns imperfections such as detection inefficiency to the eavesdropper. Our analysis relies on two preconditions for secure two-way and one-way QKD: 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. Both criteria have been previously applied to evaluate single-photon implementations of QKD. Here we use them to investigate a realistic source of weak coherent pulses. The resulting upper bounds can be formulated as a convex optimization problem known as a semidefinite program which can be efficiently solved. For the standard four-state QKD protocol, they are quite close to known lower bounds, thus showing that there are clear limits to the further improvement of classical post-processing techniques in decoy state QKD.

PACS numbers:

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. Together with the Vernam cipher [3], QKD can be used to provide information-theoretic secure communications.

Practical QKD systems can differ in many important aspects from their original theoretical proposal, since these proposals typically demand technologies that are beyond our present experimental capability. Especially, the signals emitted by the source, instead of being single photons, are usually weak coherent pulses (WCP) with typical average photon numbers of 0.1 or higher. The quantum channel introduces errors and considerable attenuation (about 0.2 dB/km) that affect the signals even when Eve is not present. Besides, for telecom wavelengths, standard InGaAs single-photon detectors can have a detection efficiency below 15% and are noisy due to dark counts. All these modifications jeopardize the security of the protocols, and lead to limitations of rate and distance that can be covered by these techniques [4].

A main security threat of practical QKD schemes based on WCP arises from the fact that some signals contain more than one photon prepared in the same polarization state. Now Eve is no longer limited by the no-cloning theorem [5] since in these events the signal itself provides her with perfect copies of the signal photon. She can perform, for instance, the so-called *photon number splitting* (PNS) attack on the multi-photon pulses [4]. This attack gives Eve full information about the part of the key generated with the multi-photon signals, without causing any disturbance in the signal polarization. As a result, it turns out that the standard BB84 protocol [6] with WCP can deliver a key generation rate of order $O(\eta^2)$, where η denotes the transmission efficiency of the quantum channel [7, 8].

To achieve higher secure key rates over longer distances, different QKD schemes, that are robust against the PNS attack, have been proposed in recent years [9, 10, 11, 12, 13]. One of these schemes is the so-called decoy state QKD [9, 10, 11] where Alice varies, independently and at random, the mean photon number of each signal state that she sends to Bob by employing different intensity settings. Eve does not know a priori the mean photon number of each signal state sent by Alice. This means that her eavesdropping strategy can only depend on the photon number of these signals, but not on the particular intensity setting used to generate them.

From the measurement results corresponding to different intensity settings, the legitimate users can estimate the classical joint probability distribution describing their outcomes for each photon number state. This provides them with a better estimation of the behaviour of the quantum channel, and it translates into an enhancement of the achievable secret key rate and distance. This technique has been successfully implemented in several recent experiments [14], and it can give a key generation rate of order $O(\eta)$ [9, 10, 11].

While the security analysis of decoy state QKD included in Refs. [9, 10, 11] is relevant from a practical point of view, it also leaves open the possibility that the development of better proof techniques, or better classical post-processing protocols, might further improve the performance of these schemes in realistic scenarios. For instance, it is known that two-way classical post-processing protocols can tolerate a higher error rate than one-way communication techniques [15, 16], or that by modifying the public announcements of the standard BB84 protocol it is possible to generate a secret key even from multi-photon signals [12]. Also, the use of local randomization [17] and degenerate codes [18] can as well improve the error rate thresholds of the protocols.

In this paper we consider the uncalibrated device scenario [2] and we assume the typical initial post-processing step where double click events are not discarded by Bob, but they are randomly assigned to single click events [19]. In this scenario, we derive simple upper bounds on the secret key rate and distance that can be covered by decoy state QKD based exclusively on the classical correlations established by the legitimate users during the quantum communication phase of the protocol. Our analysis relies on two preconditions for secure two-way and one-way QKD. In particular, Alice and Bob need to prove that there exists no separable state (in the case of two-way QKD) [20, 21], or that there exists no quantum state having a symmetric extension (one-way QKD) [22], that is compatible with the available measurements results. Both criteria have been already applied to evaluate single-photon implementations of QKD [20, 21, 22, 23, 24]. Here we employ them for the first time to investigate practical realizations of QKD based on the distribution of WCP.

We show that both preconditions for secure two-way and one-way QKD can be formulated as a convex optimization problem known as a semidefinite program (SDP) [25]. Such instances of convex optimization problems appear frequently in quantum information theory and can be solved with arbitrary accuracy in polynomial time, for example, by the interior-point methods [25]. As a result, we obtain ultimate upper bounds on the performance of decoy state QKD when this typical initial post-processing of the double clicks is performed. These upper bounds hold for any possible classical communication technique that the legitimate users can employ in this scenario afterwards like, for example, the SARG04 protocol [12], adding noise protocols [17], degenerate codes protocols [18] and two-way classical post-processing protocols [15, 16]. The analysis presented in this manuscript can as well be straightforwardly adapted to evaluate other implementations of the BB84 protocol with practical signals as, for instance, those experimental demonstrations based on WCP without decoy states or on entangled signals coming from a parametric down conversion source.

The paper is organized as follows. In Sec. II we describe in detail a WCP implementation of the BB84 protocol based on decoy states. Next, in Sec. III we apply two criteria for secure two-way and one-way QKD to this scenario. Here we derive upper bounds on the secret key rate and distance that can be achieved with decoy state QKD as a function of the observed quantum bit error rate (QBER) and the losses in the quantum channel. Moreover, we show how to cast both upper bounds as SDPs. These results are then illustrated in Sec. IV for the case of a typical behaviour of the quantum channel, *i.e.*, in the absence of eavesdropping. Finally, Sec. V concludes the paper with a summary.

II. DECOY STATE QKD

In decoy state QKD with WCP Alice prepares phase-randomized coherent states with Poissonian photon number distribution. The mean photon number (intensity) of this distribution is chosen at random for each signal from a set of possible values μ_l. In the case of the BB84 protocol, and assuming Alice chooses a decoy intensity setting l, such states can be described as

$$\rho_B^k(\mu_l) = e^{-\mu_l} \sum_{n=0}^{\infty} \frac{\mu_l^n}{n!} |n_k\rangle_B \langle n_k|, \qquad (1)$$

where the signals $|n_k\rangle_B$ denote Fock states with n photons in one of the four possible polarization states of the BB84 scheme, which are labeled with the index $k \in \{0, \ldots, 3\}$. On the receiving side, we consider that Bob employs an active basis choice measurement setup. This device splits the incoming light by means of a polarizing beam-splitter and then sends it to threshold detectors that cannot resolve the number of photons by which they are triggered. The polarizing beam-splitter can be oriented along any of the two possible polarization basis used in the BB84 protocol. This detection setup is characterized by one *positive operator value measure* (POVM) that we shall denote as $\{B_j\}$.

In an entanglement-based view, the signal preparation process described above can be modeled as follows: Alice produces first bipartite states of the form

$$|\Psi_{\text{source}}\rangle_{AB} = \sum_{k=0}^{3} \sum_{l=0}^{\infty} \sqrt{q_k p_l} |k\rangle_{A_1} |l\rangle_{A_2} |\phi_{kl}\rangle_{A_3 B}, \qquad (2)$$

where system A is the composition of systems A_1, A_2, and A_3, and the orthogonal states $|k\rangle_{A_1}$ and $|l\rangle_{A_2}$ record, respectively, the polarization state and decoy intensity setting selected by Alice. The parameters q_k and p_l represent the a priori probabilities of these signals. For instance, in the standard BB84 scheme the four possible polarization states are chosen with equal a priori probabilities and $q_k = 1/4$ for all k. The signal $|\phi_{kl}\rangle_{A_3B}$ that appears in Eq. (2) denotes a purification of the state $\rho_B^k(\mu_l)$ and can be written as

$$|\phi_{kl}\rangle_{A_3B} = e^{-\mu_l/2} \sum_{n=0}^{\infty} \frac{\sqrt{\mu_l}^n}{\sqrt{n!}} |n\rangle_{A_3} |n_k\rangle_B, \qquad (3)$$

where system A_3 acts as a shield, in the sense of Ref. [26] and records the photon number information of the signals prepared by the source. This system is typically inaccessible to all the parties. One could also select as $|\phi_{kl}\rangle_{A_3B}$ any other purification of the state $\rho_B^k(\mu_l)$. However, as we will show in Sec. III, the one given by Eq. (3) is particularly suited for the calculations that we present in that section.

Afterwards, Alice measures systems A_1 and A_2 in the orthogonal basis $|k\rangle_{A_1}$ and $|l\rangle_{A_2}$, corresponding to the measurement operators $A_{kl} = |k\rangle_{A_1}\langle k| \otimes |l\rangle_{A_2}\langle l|$. This action generates the signal states $\rho_B^k(\mu_l)$ with a priori probabilities $q_k p_l$. The reduced density matrix $\rho_A = \text{Tr}_B(\rho_{AB})$, with $\rho_{AB} = |\Psi_{\text{source}}\rangle_{AB}\langle\Psi_{\text{source}}|$, is fixed by the actual preparation scheme and cannot be modified by Eve. In order to include this information in the measurement process, one can add to the observables $\{A_{kl}\otimes B_j\}$, measured by Alice and Bob, other observables $\{C_i \otimes \mathbb{1}_B\}$ such that $\{C_i\}$ form a complete tomographic set of Alice's Hilbert space $\mathcal{H}_A$ [21]. In order to simplify our notation, from now on we shall consider that the observed data $p_{klj} = \text{Tr}(A_{kl} \otimes B_j \ \rho_{AB})$ and the POVM $\{A_{kl} \otimes B_j\}$ contain also the observables $\{C_i \otimes \mathbb{1}_B\}$. That is, every time we refer to $\{A_{kl}\otimes B_j\}$ we assume that these operators include as well the observables $\{C_i \otimes \mathbb{1}_B\}$.

III. UPPER BOUNDS ON DECOY STATE QKD

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

$$\mathcal{S} = \big\{\sigma_{AB} \mid \text{Tr}(A_{kl} \otimes B_j \ \sigma_{AB}) = p_{klj} \ \forall k, l, j\big\}. \qquad (4)$$

A. Two-way classical post-processing

Let us begin by considering two-way classical post-processing of the data p_{klj}. It was shown in Ref. [21] that a necessary precondition to distill a secret key in this scenario is that the equivalence class $\mathcal{S}$ does not contain any separable state. That is, we need to find quantum-mechanical correlations in p_{klj}, otherwise the secret key rate, that we shall denote as K, vanishes [27]. As it is, this precondition answers only partially the important question of how much secret key Alice and Bob can obtain from their correlated data. It just tells if the secret key rate is zero or it may be positive. However, this criterion can be used as a benchmark to evaluate any upper bound on K. If $\mathcal{S}$ contains a separable state then the upper bound must vanish. One upper bound which satisfies this condition is that given by the regularized relative entropy of entanglement [28]. Unfortunately, to calculate this quantity for a given quantum state is, in general, a quite difficult task, and analytical expressions are only available for some particular cases [29]. Besides, this upper bound depends exclusively on the quantum states shared by Alice and Bob and, therefore, it does not include the effect of imperfect devices like, for instance, the low detection efficiency or the noise in the form of dark counts introduced by current detectors [23]. Another possible approach is that based on the best separable approximation (BSA) of a quantum state σ_{AB} [30]. This is the decomposition of σ_{AB} into a separable state σ_{sep} and an entangled state ρ_{ent}, while maximizing the weight of the separable part. That is, any quantum state σ_{AB} can always be written as

$$\sigma_{AB} = \lambda(\sigma_{AB})\sigma_{sep} + [1 - \lambda(\sigma_{AB})]\rho_{ent}, \qquad (5)$$

where the real parameter $\lambda(\sigma_{AB}) \geq 0$ is maximal.

Given an equivalence class $\mathcal{S}$ of quantum states, one can define the maximum weight of separability within the class, $\lambda_{BSA}^{\mathcal{S}}$, as

$$\lambda_{BSA}^{\mathcal{S}} = \max\{\lambda(\sigma_{AB}) \mid \sigma_{AB} \in \mathcal{S}\}. \qquad (6)$$

Note that the correlations p_{klj} can originate from a separable state if and only if $\lambda_{BSA}^{\mathcal{S}} = 1$. Let $\mathcal{S}_{BSA}^{ent}$ denote the equivalence class of quantum states given by

$$\mathcal{S}_{BSA}^{ent} = \{\rho_{ent} \mid \sigma_{AB} \in \mathcal{S} \text{ and } \lambda(\sigma_{AB}) = \lambda_{BSA}^{\mathcal{S}}\}, \qquad (7)$$

where ρ_{ent} represents again the entangled part in the BSA of the state σ_{AB}. Then, it was proven in Ref. [23] that the secret key rate K always satisfies

$$K \leq (1 - \lambda_{BSA}^{\mathcal{S}}) I^{ent}(A; B), \qquad (8)$$

where $I^{ent}(A;B)$ represents the Shannon mutual information calculated on the joint probability distribution $q_{klj} = \text{Tr}(A_{kl} \otimes B_j \ \rho_{ent})$. As it is, this upper bound can be applied to any QKD scheme [23], although the calculation of the parameters $\lambda_{BSA}^{\mathcal{S}}$ and ρ_{ent} might be a challenge. Next, we consider the particular case of decoy state QKD.

Upper bound on two-way decoy state QKD

The signal states $\rho_B^k(\mu_l)$ that Alice sends to Bob are mixtures of Fock states with different Poissonian photon number distributions of mean μ_l. This means, in particular, that Eve can always perform a *quantum non-demolition* (QND) measurement of the total number of photons contained in each of these signals without introducing any errors. The justification for this is that the total photon number information via the QND measurement "comes free", since the execution of this measurement does not change the signals $\rho_B^k(\mu_l)$. That is, the realization of this measurement cannot make Eve's eavesdropping capabilities weaker [31]. If Eve performs such a QND measurement, then the signals $\rho_{AB} = |\Psi_{\text{source}}\rangle_{AB}\langle\Psi_{\text{source}}|$ are transformed as

$$\rho_{AB} \mapsto \gamma_{AB} = \sum_{n=0}^{\infty} r_n |\varphi_n\rangle_{A_1B}\langle\varphi_n| \otimes |\mu_n\rangle_{A_2}\langle\mu_n| \otimes |n\rangle_{A_3}\langle n|, \tag{9}$$

where the probabilities r_n are given by

$$r_n = \sum_{l=0}^{\infty} p_l \frac{e^{-\mu_l}\mu_l^n}{n!}, \tag{10}$$

the signals $|\varphi_n\rangle_{A_1B}$ have the form

$$|\varphi_n\rangle_{A_1B} = \sum_{k=0}^{3} \sqrt{q_k}|k\rangle_{A_1}|n_k\rangle_B, \tag{11}$$

and the normalized states $|\mu_n\rangle_{A_2}$ only depend on the signals $|l\rangle_{A_2}$ and the photon number n.

From the tensor product structure of γ_{AB} we learn that the signals γ_{AB} can only contain quantum correlations between systems A_1 and B. Therefore, without loss of generality, we can always restrict ourselves to only search for quantum correlations between these two systems. Additionally, in decoy state QKD Alice and Bob have always access to the conditional joint probability distribution describing their outcomes given that Alice emitted an n-photon state. This means that the search for quantum correlations in $\mathcal{S}$ can be done independently for each n-photon signal. That is, the legitimate users can define an equivalence class of signal states for each possible Fock state sent by Alice.

A further simplification arises when one considers the typical initial post-processing step where double click events are not discarded by Bob, but they are randomly assigned to single click events [19]. In the case of the BB84 protocol, this action allows Alice and Bob to always explain their observed data as coming from a single-photon signal where Bob performs a single-photon measurement $\{T_j\}$ [32]. This measurement is characterized by a set of POVM operators which are projectors onto the eigenvectors of the two Pauli operators σ_x and σ_z, together with a projection onto the vacuum state $|vac\rangle$ which models the losses in the quantum channel,

$$\begin{aligned} T_0 &= \frac{1}{2}|0\rangle_B\langle 0|, \qquad T_1 = \frac{1}{2}|1\rangle_B\langle 1|, \\ T_\pm &= \frac{1}{2}|\pm\rangle_B\langle\pm|, \qquad T_{vac} = |vac\rangle_B\langle vac|, \end{aligned} \tag{12}$$

with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and where $\sum_j T_j = \mathbb{1}_B$ [32]. In particular, let p_{kj}^n denote the conditional joint probability distribution obtained by Alice and Bob after their measurements $\{A_k \otimes T_j\}$, with $A_k = |k\rangle_{A_1}\langle k|$, given that Alice emitted an n-photon state. That is, p_{kj}^n includes the random assignment of double clicks to single click events. As before, we consider that the observables $\{A_k \otimes T_j\}$ contain as well other observables $\{C_i \otimes \mathbb{1}_B\}$ that form a tomographic complete set of Alice's Hilbert space $\mathcal{H}_{A_1}$. We define the equivalence class $\mathcal{S}^n$ of quantum states that are compatible with p_{kj}^n as

$$\mathcal{S}^n = \{\sigma_{A_1B}^n \mid \text{Tr}(A_k \otimes T_j\ \sigma_{A_1B}^n) = p_{kj}^n,\ \forall k, j\}. \tag{13}$$

Then, the secret key rate K can be upper bounded as

$$K \leq \sum_{n\geq 1} r_n (1 - \lambda_{BSA}^{\mathcal{S}^n}) I_n^{ent}(A;B), \tag{14}$$

where $\lambda_{BSA}^{\mathcal{S}^n}$ denotes the maximum weight of separability within the equivalence class $\mathcal{S}^n$, and $I_n^{ent}(A;B)$ represents the Shannon mutual information calculated on $q_{kj}^n = \text{Tr}(A_k \otimes T_j\ \rho_{ent}^n)$, with ρ_{ent}^n being the entangled part in the BSA of a state $\sigma_{A_1B}^n \in \mathcal{S}^n$ and whose weight of separability is maximum.

The main difficulty when evaluating the upper bound given by Eq. (14) still relies on obtaining the parameters $\lambda_{BSA}^{\mathcal{S}^n}$ and ρ_{ent}^n. Next, we show how to solve this problem by means of a semidefinite program (SDP) [25]. For that, we need to prove first the following observation.

Observation: Within the equivalence classes $\mathcal{S}^n$ of quantum signals given by Eq. (13) Alice and Bob can only detect the presence of negative partial transposed (NPT) entangled states [33].

Proof. The signals $\sigma_{A_1B}^n \in \mathcal{S}^n$ can always be decomposed as

$$\sigma_{A_1B}^n = p\tilde{\rho}_{A_1B}^n + (1-p)\tilde{\rho}_{A_1}^n \otimes |vac\rangle_B\langle vac|, \tag{15}$$

for some probability $p \in [0,1]$, and where $\tilde{\rho}_{A_1B}^n \in \mathcal{H}_{A_1} \otimes \mathcal{H}_2$, and $\tilde{\rho}_{A_1}^n \in \mathcal{H}_{A_1}$. That is, the state $\sigma_{A_1B}^n$ can only be entangled if $\tilde{\rho}_{A_1B}^n$ is also entangled. In order to detect entanglement in the latter one, Bob projects it onto the eigenvectors of the two Pauli operators σ_x and σ_z. This means, in particular, that the class of *accessible* entanglement witness operators W that can be constructed from the available measurements results satisfy $W = W^\Gamma$. Here Γ denotes transposition with respect to Bob's system. We have, therefore, that $\text{Tr}(W\tilde{\rho}_{A_1B}^n) = \text{Tr}(W\Omega)$, with $\Omega = \frac{1}{2}[\tilde{\rho}_{A_1B}^n + \tilde{\rho}_{A_1B}^{n\ \Gamma}]$. For the given dimensionalities, it was proven in Ref. [34] that whenever Ω is nonnegative it represents a separable state, *i.e.*, $\text{Tr}(W\Omega) \geq 0$. This means that Alice and Bob can only detect entangled states $\tilde{\rho}_{A_1B}^n$ that satisfy $\Omega \ngeq 0$. Since $\tilde{\rho}_{A_1B}^n \geq 0$, the previous condition is only possible when $\tilde{\rho}_{A_1B}^{n\ \Gamma} \ngeq 0$. ■

Let us now write the search of $\lambda_{BSA}^{\mathcal{S}^n}$ and ρ_{ent}^n as a SDP. This is a convex optimisation problem of the following form [25]:

$$\begin{aligned} &\text{minimize} && c^T\mathbf{x} \\ &\text{subject to} && F(\mathbf{x}) = F_0 + \sum_i x_i F_i \geq 0, \end{aligned} \tag{16}$$

where the vector $\mathbf{x}$ represents the objective variable, the vector c is fixed by the particular optimisation problem, and 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 $F(\mathbf{x}) \geq 0$. The SDP that we need to solve has the form [35]:

$$\begin{aligned} &\text{minimize} && 1 - \mathrm{Tr}[\sigma^n_{sep}(\mathbf{x})] \\ &\text{subject to} && \sigma^n_{A_1B}(\mathbf{x}) \geq 0, \\ & && \mathrm{Tr}[\sigma^n_{A_1B}(\mathbf{x})] = 1, \\ & && \mathrm{Tr}[A_k \otimes T_j \ \sigma^n_{A_1B}(\mathbf{x})] = p^n_{kj}, \ \forall k, j, \\ & && \sigma^n_{sep}(\mathbf{x}) \geq 0, \\ & && \sigma^{n\ \Gamma}_{sep}(\mathbf{x}) \geq 0, \\ & && \sigma^n_{A_1B}(\mathbf{x}) - \sigma^n_{sep}(\mathbf{x}) \geq 0, \end{aligned} \tag{17}$$

where the objective variable $\mathbf{x}$ is used to parametrise the density operators σ^n_{sep} and $\sigma^n_{A_1B}$. For that, we employ the method introduced in Refs. [23, 24]. The state σ^n_{sep} which appears in Eq. (17) is not normalized, *i.e.*, it also includes the parameter $\lambda(\sigma^n_{A_1B})$. The first three constraints in Eq. (17) guarantee that $\sigma^n_{A_1B}$ is a valid normalized density operator that belongs to the equivalence class $\mathcal{S}^n$, the following two constraints impose σ^n_{sep} to be a separable state, while the last one implies that the entangled part of $\sigma^n_{A_1B}$ is a valid but not normalized density operator. Its normalization factor is given by $1 - \lambda(\sigma^n_{A_1B})$. If $\mathbf{x}_{sol}$ denotes a solution to the SDP given by Eq. (17) then

$$\lambda^{\mathcal{S}^n}_{BSA} = \mathrm{Tr}[\sigma^n_{sep}(\mathbf{x}_{sol})], \tag{18}$$

and the state ρ^n_{ent} is given by

$$\rho^n_{ent} = \frac{\sigma^n_{A_1B}(\mathbf{x}_{sol}) - \sigma^n_{sep}(\mathbf{x}_{sol})}{1 - \lambda^{\mathcal{S}^n}_{BSA}}. \tag{19}$$

B. One-way classical post-processing

The classical post-processing of the observed data can be restricted to one-way communication [36]. Depending on the allowed direction of communication, two different cases can be considered: *Direct reconciliation* (DR) refers to communication from Alice to Bob, *reverse reconciliation* (RR) permits only communication from Bob to Alice [37]. In this section, we will only consider the case of DR. Expressions for the opposite scenario, *i.e.*, RR, can be obtained in a similar way. In Ref. [22] it was shown that a necessary precondition for secure QKD by means of DR (RR) is that the equivalence class $\mathcal{S}$ given by Eq. (4) does not contain any state having a symmetric extension to two copies of system B (system A).

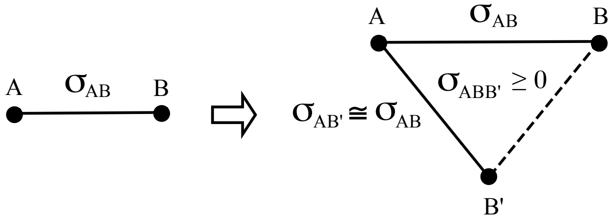

FIG. 1: Graphical illustration of a quantum state σ_{AB} which has a symmetric extension to two copies of system B.

A state σ_{AB} is said to have a symmetric extension to two copies of system B if and only if there exists a tripartite state $\sigma_{ABB'} \geq 0$, with $\mathrm{Tr}(\sigma_{ABB'}) = 1$, and where $\mathcal{H}_B \cong \mathcal{H}_{B'}$, which fulfills the following two properties [38]:

$$\mathrm{Tr}_{B'}(\sigma_{ABB'}) = \sigma_{AB}, \tag{20}$$

$$P\sigma_{ABB'}P = \sigma_{ABB'}, \tag{21}$$

where the swap operator P satisfies $P|ijk\rangle_{ABB'} = |ikj\rangle_{ABB'}$. A graphical illustration of a state σ_{AB} which has a symmetric extension to two copies of system B is given in Fig. 1. This definition can be easily extended to cover also the case of symmetric extensions of σ_{AB} to two copies of system A, and also of extensions of σ_{AB} to more than two copies of system A or of system B.

The best extendible approximation (BEA) of a given state σ_{AB} is the decomposition of σ_{AB} into a state with a symmetric extension, that we denote as σ_{ext}, and a state without symmetric extension ρ_{ne}, while maximizing the weight of the extendible part, *i.e.*,

$$\sigma_{AB} = \lambda(\sigma_{AB})\sigma_{ext} + [1 - \lambda(\sigma_{AB})]\rho_{ne}, \tag{22}$$

where the real parameter $\lambda(\sigma_{AB}) \geq 0$ is maximal [22, 39]. Note that this parameter is well defined since the set of extendible states is compact.

Equation (22) follows the same spirit like the BSA given by Eq. (5). Now, one can define analogous parameters and equivalence classes as in Sec. III A. In particular, the maximum weight of extendibility within an equivalence class $\mathcal{S}$ is defined as $\lambda^{\mathcal{S}}_{BEA} = \max\{\lambda(\sigma_{AB}) \mid \sigma_{AB} \in \mathcal{S}\}$. That is, the correlations $p_{klj} = \mathrm{Tr}(A_{kl} \otimes B_j \ \sigma_{AB})$ can originate from an extendible state if and only if $\lambda^{\mathcal{S}}_{BEA} = 1$. Finally, one defines $\mathcal{S}^{ne}_{BEA}$ as the equivalence class of quantum states given by $\mathcal{S}^{ne}_{BEA} = \{\rho_{ne} \mid \sigma_{AB} \in \mathcal{S}$ and $\lambda(\sigma_{AB}) = \lambda^{\mathcal{S}}_{BEA}\}$, where ρ_{ne} denotes the nonextendible part in the BEA of the state σ_{AB}. Then, it was proven in Ref. [22] that the one-way secret key rate $K_{\rightarrow}$ satisfies

$$K_{\rightarrow} \leq (1 - \lambda^{\mathcal{S}}_{BEA}) I^{ne}(A; B), \tag{23}$$

where $I^{ne}(A; B)$ represents the Shannon mutual information now calculated on the joint probability distribution $q_{klj} = \mathrm{Tr}(A_{kl} \otimes B_j \ \rho_{ne})$ with $\rho_{ne} \in \mathcal{S}^{ne}_{BEA}$.

The analysis contained in Sec. III A to derive Eq. (14) from Eq. (8) also applies to this scenario and we omit it here for simplicity. We obtain

$$K_{\rightarrow} \leq \sum_{n\geq 1} r_n (1-\lambda_{BEA}^{\mathcal{S}^n}) I_n^{ne}(A;B). \tag{24}$$

where $\lambda_{BEA}^{\mathcal{S}^n}$ denotes the maximum weight of extendibility within the equivalence class $\mathcal{S}^n$ given by Eq. (13), and $I_n^{ne}(A;B)$ represents the Shannon mutual information calculated on $q_{kj}^n = \mathrm{Tr}(A_k \otimes T_j \ \rho_{ne}^n)$, with ρ_{ne}^n being the nonextendible part in the BEA of a state $\sigma_{A_1B}^n \in \mathcal{S}^n$ and whose weight of extendibility is maximum.

The parameter $\lambda_{BEA}^{\mathcal{S}^n}$ and the nonextendible state ρ_{ne}^n can directly be obtained by solving the following SDP:

$$\begin{aligned} \text{minimize} \quad & 1 - \mathrm{Tr}[\sigma_{ext}^n(\mathbf{x})] \qquad (25) \\ \text{subject to} \quad & \sigma_{A_1B}^n(\mathbf{x}) \geq 0, \\ & \mathrm{Tr}[\sigma_{A_1B}^n(\mathbf{x})] = 1, \\ & \mathrm{Tr}[A_k \otimes T_j \ \sigma_{A_1B}^n(\mathbf{x})] = p_{kj}^n, \ \forall k,j, \\ & \rho_{A_1BB'}^n(\mathbf{x}) \geq 0, \\ & P\rho_{A_1BB'}^n(\mathbf{x})P = \rho_{A_1BB'}^n(\mathbf{x}), \\ & \mathrm{Tr}_{B'}[\rho_{A_1BB'}^n(\mathbf{x})] = \sigma_{ext}^n(\mathbf{x}), \\ & \sigma_{A_1B}^n(\mathbf{x}) - \sigma_{ext}^n(\mathbf{x}) \geq 0, \end{aligned}$$

where the state σ_{ext}^n is not normalized, *i.e.*, it also includes the parameter $\lambda(\sigma_{A_1B}^n)$. The first three constraints coincide with those of Eq. (17). They just guarantee that $\sigma_{A_1B}^n \in \mathcal{S}^n$. The following three constraints impose σ_{ext}^n to have a symmetric extension to two copies of system B, while the last one implies that the nonextendible part of $\sigma_{A_1B}^n$ is a valid but not normalized density operator. Its normalization factor is $1-\lambda(\sigma_{A_1B}^n)$. This SDP does not include the constraint $\sigma_{ext}^n \geq 0$ because non-negativity of the extension $\rho_{A_1BB'}^n$, together with the condition $\mathrm{Tr}_{B'}(\rho_{A_1BB'}^n) = \sigma_{ext}^n$, already implies non-negativity of σ_{ext}^n. If $\mathbf{x}_{sol}$ represents a solution to the SDP given by Eq. (25) then we have that

$$\lambda_{BEA}^{\mathcal{S}^n} = \mathrm{Tr}[\sigma_{ext}^n(\mathbf{x}_{sol})], \tag{26}$$

and the state ρ_{ne}^n is given by

$$\rho_{ne}^n = \frac{\sigma_{A_1B}^n(\mathbf{x}_{sol}) - \sigma_{ext}^n(\mathbf{x}_{sol})}{1-\lambda_{BEA}^{\mathcal{S}^n}}. \tag{27}$$

IV. EVALUATION

In this section we evaluate the upper bounds on the secret key rate both for two-way and one-way decoy state QKD given by Eq. (14) and Eq. (24). Moreover, we compare our results with known lower bounds for the same scenarios. The numerical simulations are performed with the freely available SDP solver SDPT3-3.02 [40], together with the parser YALMIP [41].

p_{kj}^n	$T_{j=0}$	$T_{j=1}$	$T_{j=+}$	$T_{j=-}$	$T_{j=vac}$
$k=0$	$\frac{Y_n(1-e_n)}{8}$	$\frac{Y_n e_n}{8}$	$\frac{Y_n}{16}$	$\frac{Y_n}{16}$	$\frac{1-Y_n}{4}$
$k=1$	$\frac{Y_n e_n}{8}$	$\frac{Y_n(1-e_n)}{8}$	$\frac{Y_n}{16}$	$\frac{Y_n}{16}$	$\frac{1-Y_n}{4}$
$k=2$	$\frac{Y_n}{16}$	$\frac{Y_n}{16}$	$\frac{Y_n(1-e_n)}{8}$	$\frac{Y_n e_n}{8}$	$\frac{1-Y_n}{4}$
$k=3$	$\frac{Y_n}{16}$	$\frac{Y_n}{16}$	$\frac{Y_n e_n}{8}$	$\frac{Y_n(1-e_n)}{8}$	$\frac{1-Y_n}{4}$

TABLE I: Conditional joint probability distribution $p_{kj}^n = \mathrm{Tr}(A_k \otimes T_j \ \sigma_{A_1B}^n)$, where the index $k \in \{0,\ldots,3\}$ labels, respectively, the four possible polarization states of the BB84 protocol $(0,1,+,-)$, and the operators T_j are given by Eq. (12). It satisfies $\sum_{k,j} p_{kj}^n = 1$.

A. Channel model

To generate the observed data, we consider the channel model used in Ref. [10, 42]. This model reproduces a normal behaviour of the quantum channel, *i.e.*, in the absence of eavesdropping. Note, however, that our analysis can as well be straightforwardly applied to other quantum channels, as it only depends on the probability distribution p_{kj}^n that characterizes the results of Alice's and Bob's measurements. This probability distribution is given in Tab. I, where the conditional yields Y_n have the form

$$Y_n = Y_0 + [1-(1-\eta)^n], \tag{28}$$

with Y_0 being the background detection event rate of the system, and where η represents the overall transmittance, including the transmission efficiency of the quantum channel and the detection efficiency. The parameter e_n denotes the quantum bit error rate of an n-photon signal. It is given by

$$e_n = \frac{e_{det}[1-(1-\eta)^n] + \frac{1}{2}Y_0}{Y_n}, \tag{29}$$

where e_{det} represents the probability that a photon hits the wrong detector due to the misalignment in the quantum channel and in the detection apparatus.

The parameter η can be related with a transmission distance l measured in km for the given QKD scheme as $\eta = 10^{-\frac{\alpha l}{10}}$, where α represents the loss coefficient of the optical fiber measured in dB/km. The total dB loss of the channel is given by αl.

B. Illustration of the upper bounds

As discussed in Sec. III, the reduced density matrix of Alice, that we shall denote as $\rho_{A_1}^n$, is fixed and cannot be modified by Eve. This state has the form $\rho_{A_1}^n = \mathrm{Tr}_B(|\varphi_n\rangle_{A_1B}\langle\varphi_n|) = \sum_{k,k'=0}^{3}\sqrt{q_k q_{k'}}\langle n_{k'}|n_k\rangle|k\rangle_{A_1}\langle k'|$, where $|\varphi_n\rangle_{A_1B}$ is given by Eq. (11). In the standard BB84 protocol the probabilities q_k satisfy $q_k = 1/4$. We obtain, therefore, that $\rho^n_{A_1}$ can be expressed as

$$\rho^n_{A_1} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 2^{-n/2} & 2^{-n/2} \\ 0 & 1 & 2^{-n/2} & (-1)^n 2^{-n/2} \\ 2^{-n/2} & 2^{-n/2} & 1 & 0 \\ 2^{-n/2} & (-1)^n 2^{-n/2} & 0 & 1 \end{pmatrix}. \tag{30}$$

To include this information in the measurement process, we consider that Alice and Bob have also access to the results of a set of observables $\{C_i \otimes \mathbb{1}_B\}$ that form a tomographic complete set of Alice's Hilbert space $\mathcal{H}_{A_1}$. In particular, we use a Hermitian operator basis $\{C_1, \ldots, C_{16}\}$. These Hermitian operators satisfy $\mathrm{Tr}(C_i) = 4\delta_{i1}$ and have a Hilbert-Schmidt scalar product $\mathrm{Tr}(C_i C_j) = 4\delta_{ij}$. The probabilities $\mathrm{Tr}(C_i \otimes \mathbb{1}_B\ \sigma^n_{A_1B}) = \mathrm{Tr}(C_i\ \rho^n_{A_1})$, with $\rho^n_{A_1}$ given by Eq. (30).

The resulting upper bounds on the two-way and one-way secret key rate are illustrated, respectively, in Fig. 2 and Fig. 3. They state that no secret key can be distilled from the correlations established by the legitimate users above the curves, *i.e.*, the secret key rate in that region is zero. These figures include as well *lower* bounds for the secret key rate obtained in Refs. [8, 10, 16]. Note, however, the security proofs included in Refs. [8, 10] implicitly assume that Alice and Bob can make public announcements using two-way communication, and only the error correction and privacy amplification steps of the protocol are assumed to be realized by means of one-way communication. We consider the uncalibrated device scenario and we study two different situations in each case: (1) no errors in the quantum channel, *i.e.*, $Y_0 = 0$, $e_{det} = 0$, and (2) $Y_0 = 1.7 \times 10^{-6}$ and $e_{det} = 0.033$. This last scenario corresponds to the experimental parameters reported by Gobby-Yuan-Shields (GYS) in Ref. [43]. Figure 2 and Fig. 3 do not include the sifting factor of 1/2 for the BB84 protocol, since this effect can be avoided by an asymmetric basis choice for Alice and Bob [44]. Moreover, we consider that in the asymptotic limit of a large number of transmitted signals most of them represent signal states of mean photon number μ_0. That is, the proportion of decoy states used to test the behaviour of the quantum channel within the total number of signals sent by Alice is neglected. This means that p_0 in Eq. (10) satisfies $p_0 \approx 1$ and

$$r_n = \frac{e^{-\mu_0}\mu_0^n}{n!}. \tag{31}$$

C. Discussion

In the case of no errors in the quantum channel (Case (1) above) the lower bounds for two-way and one-way QKD derived in Refs. [8, 10, 16] coincide. Furthermore, for low values of the total dB loss, the upper bounds shown in the figures present a small bump which is specially visible in this last case. The origin of this bump is the potential contribution of the multi-photon pulses to the key rate.

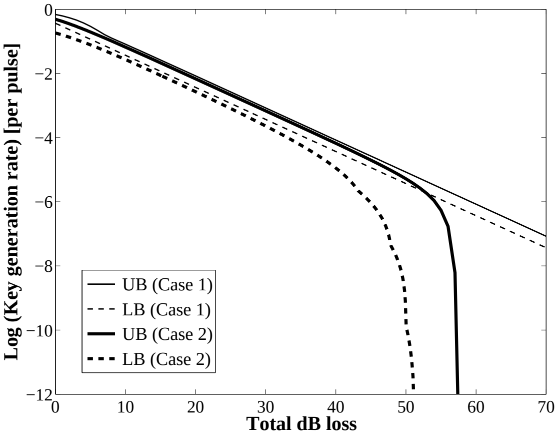

FIG. 2: Upper bounds on the two-way secret key rate K given by Eq. (14) in logarithmic scale in comparison to known lower bounds for the same scenario given in Ref. [16]. The figure includes two cases. (1) No errors in the quantum channel, *i.e.*, $Y_0 = 0$ and $e_{det} = 0$. In this case, the upper bound (UB) is represented by a thin solid line, while the lower bound (LB) is represented by a thin dashed line. (2) $Y_0 = 1.7 \times 10^{-6}$ and $e_{det} = 0.033$, which correspond to the GYS experiment reported in Ref. [43]. In this case, the upper bound (UB) is represented by a thick solid line, while the lower bound (LB) after 3 B steps is represented by a thick dashed line. We assume asymmetric basis choice to suppress the sifting effect [44].

Let us now consider the cutoff points for decoy state QKD in the case of errors in the quantum channel (Case (2) above). These are the values of the total dB loss for which the secret key rate drops down to zero in Fig. 2 and Fig. 3. We find that they are given, respectively, by: ≈ 51.1 dB (lower bound two-way after 3 B steps), ≈ 57.4 dB (upper bound two-way), ≈ 44.9 dB (lower bound one-way), and ≈ 53.5 dB (upper bound one-way with RR). These quantities can be related with the following transmission distances: 179.2 km, 209.2 km, 149.6 km and 190.6 km. Here we have used $\alpha = 0.21$ dB/km and the efficiency of Bob's detectors is 4.5% [43]. It is interesting to compare the two-way cutoff point of 209.2 km with a similar distance upper bound of 208 km provided in Ref. [16] for the same values of the experimental parameters. Note, however, that the upper bound derived in Ref. [16] relies on the assumption that a secure key can only be extracted from single photon states. That is, it implicitly assumes the standard BB84 protocol. If this assumption is removed and one also includes in the analysis the potential contribution of the multi-photon signals to the key rate (due, for instance, to the SARG04 protocol [12]), then the cutoff point provided in Ref. [16] transforms from 208 km to 222 km, which is above the 209.2 km presented here.

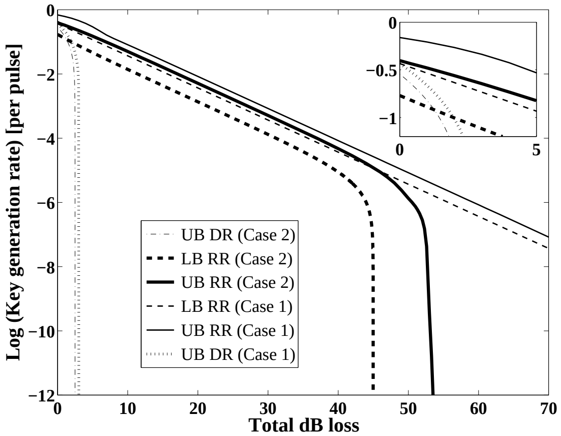

FIG. 3: Upper bounds on the one-way secret key rate $K_{\rightarrow}$ given by Eq. (24) in logarithmic scale in comparison to known lower bounds for the same scenario given in Refs. [8, 10]. The figure includes two cases. (1) No errors in the quantum channel, *i.e.*, $Y_0 = 0$ and $e_{det} = 0$. In this case, the upper bound (UB) RR is represented by a thin solid line, while the lower bound (LB) is represented by a thin dashed line. (2) $Y_0 = 1.7 \times 10^{-6}$ and $e_{det} = 0.033$, which correspond to the GYS experiment reported in Ref. [43]. In this case, the upper bound (UB) RR is represented by a thick solid line, while the lower bound (LB) is represented by a thick dashed line. The two lines on the left hand side of the graphic represent upper bounds for the case of DR (case (1) short dashed line, case (2) dash-dotted line). The inset figure shows an enlarged view of the upper bounds for a total dB loss ranging from 0 to 5 dB. We assume asymmetric basis choice to suppress the sifting effect [44].

Figure 3 shows a significant difference between the behaviour of the upper bounds for one-way classical post-processing with RR and DR. Most importantly, the upper bounds on $K_{\rightarrow}$ for the case of DR can be below the lower bounds on the secret key rate derived in Refs. [8, 10]. Note, however, that the scenario considered here is slightly different from the one assumed in the security proofs of Refs. [8, 10]. In particular, the analysis contained in Sec. III B for the case of DR does not allow *any* communication from Bob to Alice once the conditional probabilities p_{kj}^n are determined. This means, for instance, that Bob cannot even declare in which particular events his detection apparatus produced a “click”. However, as mentioned previously, Refs. [8, 10] implicitly assume that only the error correction and privacy amplification steps of the protocol are performed with one-way communication. If the analysis performed in Sec. III B is modified such that Bob is now allowed to inform Alice which signal states he actually detected, then it turns out that the resulting upper bounds in this modified scenario coincide with those derived for the case of RR. To include this initial communication step from Bob to Alice in the analysis, one can use the following procedure. Let the projector Π_{A_1B} be defined as

$$\Pi_{A_1B} = \mathbb{1}_{A_1} \otimes (\mathbb{1}_B - |vac\rangle_B\langle vac|). \tag{32}$$

Then, one can add to Eq. (25) one extra constraint

$$\sigma_{A_1B}^{n\ post}(\mathbf{x}) = \frac{\Pi_{A_1B}\sigma_{A_1B}^n(\mathbf{x})\Pi_{A_1B}}{Y_n}, \tag{33}$$

and substitute the condition $\sigma_{A_1B}^n(\mathbf{x}) - \sigma_{ext}^n(\mathbf{x}) \geq 0$ by

$$\sigma_{A_1B}^{n\ post}(\mathbf{x}) - \sigma_{ext}^n(\mathbf{x}) \geq 0. \tag{34}$$

Equation (33) refers to the normalized state that is postselected by Alice and Bob once Bob declares which signals he detected. Equation (34) indicates that the BEA has to be applied to this postselected state. Finally, each term in the summation given by Eq. (24) has to be multiplied by the yield Y_n, *i.e.*, the probability that Bob obtains a “click” conditioned on the fact that Alice sent an n-photon state.

Our numerical results indicate that the upper bounds given by Eq. (14) and Eq. (24) are close to the known lower bounds available in the scientific literature for the same scenarios. However, one might expect that these upper bounds can be further tightened in different ways. For instance, by substituting in Eq. (14) and Eq. (24) the Shannon mutual information with any other tighter upper bound on the secret key rate that can be extracted from a classical tripartite probability distribution measured on a purification of the state ρ_{ent}^n (in the case of two-way QKD) or of the state ρ_{ne}^n (one-way QKD). Moreover, as they are, Eq. (14) and Eq. (24) implicitly assume that the legitimate users know precisely the number of photons contained in each signal emitted. However, in decoy state QKD Alice and Bob have only access to the conditional joint probability distribution describing their outcomes given that Alice emitted an n-photon state, but they do not have single shot photon number resolution of each signal state sent.

As a side remark, we would like to emphasize that to calculate the upper bounds given by Eq. (14) and Eq. (24) it is typically sufficient to consider only a finite number of terms in the summations. This result arises from the limit imposed by the unambiguous state discrimination (USD) attack [31]. This attack does not introduce any errors in Alice's and Bob's signal states. Moreover, it corresponds to an entanglement-breaking channel [45] and, therefore, it cannot lead to a secure key both for the case of two-way and one-way QKD [20, 22]. The maximum probability of unambiguously discriminating an n-photon state sent by Alice is given by [31]

$$P_D^n = \begin{cases} 0 & n \leq 2 \\ 1 - 2^{1-n/2} & n \text{ even} \\ 1 - 2^{(1-n)/2} & n \text{ odd.} \end{cases} \tag{35}$$

For typical observations this quantity can be related with a transmission efficiency η_n of the quantum channel, *i.e.*, an η_n that provides an expected click rate at Bob's side equal to P_D^n. This last condition can be written as

$$\eta_n = 1 - (1 - P_D^n)^{1/n}. \tag{36}$$

Whenever the overall transmission probability of each photon satisfies $\eta \leq \eta_n$, then any pulse containing n or more photons is insecure against the USD attack. After a short calculation, we obtain that the total number of n-photon signals that need to be considered in the summations of Eq. (14) and Eq. (24) can be upper bounded as

$$n \leq \begin{cases} \left\lfloor \frac{1}{\log_2[\sqrt{2}(1-\eta)]} \right\rfloor & n \text{ even} \\ \left\lfloor \frac{1}{2\log_2[\sqrt{2}(1-\eta)]} \right\rfloor & n \text{ odd.} \end{cases} \tag{37}$$

V. CONCLUSION

In this paper we have derived upper bounds on the secret key rate and distance that can be covered by two-way and one-way decoy state quantum key distribution (QKD). Our analysis considers the uncalibrated device scenario and we have assumed the typical initial post-processing step where double click events are randomly assigned to single click events. We have used two preconditions for secure two-way and one-way QKD. 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. Both criteria have been previously employed in the scientific literature to evaluate single-photon implementations of QKD. Here we have applied them to investigate a realistic source of weak coherent pulses, and we have shown that they can be formulated as a convex optimization problem known as a semidefinite program (SDP). Such instances of convex optimization problems can be solved efficiently, for example by means of the interior-point methods.

As a result, we have obtained fundamental limitations on the performance of decoy state QKD when this initial post-processing of the double clicks is performed. These upper bounds cannot be overcome by any classical communication technique (including, for example, SARG04 protocol, adding noise protocols, degenerate codes and two-way classical post-processing protocols) that the legitimate users may employ to process their correlated data afterwards. Moreover, our results seem to be already close to well known lower bounds for the same scenarios, thus showing that there are clear limits to the further improvement of classical post-processing techniques in decoy state QKD.

The analysis presented in this paper could as well be straightforwardly adapted to evaluate other implementations of the BB84 protocol with practical signals like, for example, those experimental demonstrations based on WCP without decoy states or on entangled signals coming from a parametric down conversion source.

VI. ACKNOWLEDGEMENTS

M.C. especially thanks H.-K. Lo and N. Lütkenhaus for hospitality and support during his stay at the University of Toronto and at the Institute for Quantum Computing (University of Waterloo) where this manuscript was finished. This work was supported by the European Projects SECOQC and QAP, NSERC, Quantum Works, CSEC, CFI, CIPI, CIFAR, the CRC program, MITACS, OIT, OCE, by Xunta de Galicia (Spain, Grant No. INCITE08PXIB322257PR), and by University of Vigo (Program "Axudas á mobilidade dos investigadores").

[1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); M. Dušek, N. Lütkenhaus and M. Hendrych, Progress in Optics **49**, Edt. E. Wolf (Elsevier), 381 (2006).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, Preprint quant-ph/0802.4155, accepted for publication in Rev. Mod. Phys.

[3] G. S. Vernam, J. Am. Inst. Electr. Eng. **XLV**, 109 (1926).

[4] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[5] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[6] C. H. Bennett and G. Brassard, Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE Press, New York, 175 (1984).

[7] H. Inamori, N. Lütkenhaus and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[8] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quant. Inf. Comput. **4**, 325 (2004).

[9] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[10] H.-K. Lo, X. Ma and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[11] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); X. Ma, B. Qi, Y. Zhao and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005); X.-B. Wang, Phys. Rev. A **72**, 012322 (2005); X.-B. Wang, Phys. Rev. A **72**, 049908 (E) (2005).

[12] V. Scarani, A. Acín, G. Ribordy and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[13] M. Koashi, Phys. Rev. Lett. **93**, 120501(2004); K. Tamaki, N. Lütkenhaus, M. Koashi and J. Batuwantudawe, Preprint quant-ph/0607082; K. Inoue, E. Waks and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).

[14] Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006); Y. Zhao, B. Qi, X. Ma, H.-K. Lo and L. Qian, Proc. of IEEE International Symposium on Information Theory (ISIT'06), 2094 (2006); C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang and J.-W. Pan,

Phys. Rev. Lett. **98**, 010505 (2007); D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007); T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007); Z. L. Yuan, A. W. Sharpe and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007); Z.-Q. Yin, Z.-F. Han, W. Chen, F.-X. Xu, Q.-L. Wu and G.-C. Guo, Chin. Phys. Lett **25**, 3547 (2008); J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka and A. Tomita, Preprint quant-ph/0705.3081; J. F. Dynes, Z. L. Yuan, A. W. Sharpe and A. J. Shields, Optics Express **15**, 8465 (2007).

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

[16] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki and H.-K. Lo, Phys. Rev. A **74**, 032330 (2006).

[17] B. Kraus, N. Gisin and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005); R. Renner, N. Gisin and B. Kraus, Phys. Rev. A **72**, 012332 (2005); J. M. Renes and Graeme Smith, Phys. Rev. Lett. **98**, 020502 (2007).

[18] P. W. Shor and J. A. Smolin, Preprint quant-ph/9604006v2; D. P. DiVincenzo, P. W. Shor and J. A. Smolin, Phys. Rev. A **57**, 830 (1998); G. Smith and J. A. Smolin, Phys. Rev. Lett. **98**, 030501 (2007); H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001); G. Smith, J. M. Renes and J. A. Smolin, Phys. Rev. Lett. **100**, 170502 (2008); O. Kern and J. M. Renes, Quantum Inf. Comput. **8**, 756 (2008).

[19] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999); N. Lütkenhaus, Appl. Phys. B: Lasers Opt. **69**, 395 (1999); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

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

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

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

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

[24] M. Curty and T. Moroder, Phys. Rev. A **75**, 052336 (2007).

[25] L. Vandenberghe and S. Boyd, SIAM Review **38**, 49 (1996); S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, England, 2004).

[26] K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim, Preprint arXiv:quant-ph/0506189.

[27] Here we define quantum correlations as those correlations that cannot be explained by means of an intercept-resend attack [20, 21].

[28] K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005); V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[29] K. Audenaert, J. Eisert, E. Jané, M. B. Plenio, S. Virmani and B. De Moor, Phys. Rev. Lett. **87**, 217902 (2001).

[30] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1997); S. Karnas and M. Lewenstein, J. Phys. A **34**, 6919 (2001).

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

[32] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008); N. Beaudry, T. Moroder and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

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

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

[35] Note that every equality constraint of the form $f(\mathbf{x}) = g(\mathbf{x})$, for any functions f and g, can always be represented by two inequality constraints $f(\mathbf{x}) - g(\mathbf{x}) \geq 0$ and $-[f(\mathbf{x}) - g(\mathbf{x})] \geq 0$. Moreover, two (or even more) LMI constraints $F_0(\mathbf{x}) \geq 0, F_1(\mathbf{x}) \geq 0$, can always be combined into a single new LMI constraint as

$$F(\mathbf{x}) = \begin{pmatrix} F_0(\mathbf{x}) & 0 \\ 0 & F_1(\mathbf{x}) \end{pmatrix} \equiv F_0(\mathbf{x}) \oplus F_1(\mathbf{x}) \geq 0.$$

[36] Before restricting Alice and Bob to only communicate one-way, one typically allows them to realize an initial two-way communication step to estimate the joint probability distribution describing their measurements outcomes. This is the approach that we follow in this paper. In decoy state QKD this is also important in order to distinguish between signal and decoy pulses and to estimate the conditional probabilities p_{kj}^n.

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

[38] A. C. Doherty, P. A. Parrilo and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002); A. C. Doherty, P. A. Parrilo and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004); A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **71**, 032333 (2005).

[39] 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 B corresponds to DR, and extensions to two copies of system A corresponds to RR.

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

[41] J. Löfberg, in *Proceedings of the CACSD Conference*, Taipei, Taiwan, p. 284 (2004).

[42] X. Ma, Ph.D. thesis, University of Toronto, 2008.

[43] C. Gobby, Z. L. Yuan and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

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

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