Efficient heralding of photonic qubits with applications to device-independent quantum key distribution

David Pitkanen,[1] Xiongfeng Ma,[1] Ricardo Wickert,[2] Peter van Loock,[2] and Norbert Lütkenhaus[1]

[1]*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, N2L 3G1 Waterloo, Ontario, Canada*

[2]*Max Planck Institute for the Science of Light and Universität Erlangen-Nürnberg, D-91058 Erlangen, Germany*

(Received 25 May 2011; published 19 August 2011)

We present an efficient way of heralding photonic qubit signals using linear optics devices. First, we show that one can obtain asymptotically perfect heralding and unit success probability with growing resources. Second, we show that even using finite resources, we can improve qualitatively and quantitatively over earlier heralding results. In the latter scenario, we can obtain perfect heralded photonic qubits while maintaining a finite success probability. We demonstrate the advantage of our heralding scheme by predicting key rates for device-independent quantum key distribution, taking imperfections of sources and detectors into account.

DOI: 10.1103/PhysRevA.84.022325 PACS number(s): 03.67.Dd, 03.65.Ud, 42.50.−p

I. INTRODUCTION

Applications such as the verification of entanglement for quantum communication, and the establishment of security proofs in device-independent quantum key distribution (DIQKD) [1] have generated increasing interest in violations of Bell's inequalities over long distances. A violation of Bell's inequality is supposed to be a test for a nonlocal correlation between the outcomes of pairs of events; however, it is difficult to design an experiment that rigorously shows this nonlocality, as imperfections in the experimental equipment can open loopholes, which allow for a local hidden variable (HV) explanation of the measured data. For example, signal loss in optical implementations generates the so-called detection efficiency loophole [2].

In experiments, with growing distance the transmission loss increases. Consequently, the resulting low total detection probabilities make violations of Bell's inequality virtually impossible. To overcome this issue, the use of heralding devices [3,4] has been suggested. Such an apparatus performs a measurement that resembles a quantum nondemolition (QND) measurement, raising a flag to indicate whenever the desired signal successfully traverses the channel. The state generated by conditioning on this flag can then be employed in a Bell test. This procedure does not lead to a detection loophole as long as the flagging is independent of the measurement choice.

Gisin *et al.* [3] have considered an implementation of a heralding device in a DIQKD scheme employing realistic sources, linear optical components, and photon-number resolving detectors. The proposed scheme uses the transmissivity of one of its beam splitters as an adjustable parameter to regulate the ratio between vacuum and single photons in the conditional output state at the expense of the probability of successful heralding. With input signals consisting only of vacuum and single-photon states, increasing the single-photon component to unity in the conditional state can only be achieved in the limit of vanishing success probability. If the input also contains multiphoton signals, then the fraction of single-photon signals in the conditional states cannot reach unity.

In the present work we investigate improvements on this scheme to overcome its limitations. We begin by reviewing the known results on heralding in Sec. II. Then in Sec. III, we investigate fundamental limits with unlimited resources, staying within the linear optics toolbox. In this regime, we can employ large ancilla states to realize a Knill-Laflamme-Milburn–like (KLM-like) teleportation procedure [5] and demonstrate that we can perform the desired QND measurement perfectly, although nondeterministically. Shifting our focus to practical schemes that allow only limited resources, we then revisit in Sec. IV the original proposal. Motivated by our general scheme and the Hong-Ou-Mandel effect [6], we suggest a modification that significantly improves the heralding device. The modification is done by adding two beam splitters to the initial linear optics circuit while maintaining the original simple ancilla states.

Since the original amplifier was proposed for use in DIQKD, we analyze the performance of our amplifier in Sec. V and demonstrate that the improvement of the heralding device translates into an enhanced key rate.

II. PHOTONIC AND QUBIT AMPLIFIER

We begin by revisiting the noiseless linear photonic amplifier proposal of Ralph and Lund [4] (see Fig. 1). A single-photon state passes through a beam splitter of transmissivity t to create an entangled state of two modes involving vacuum and single photons. One of the modes will be the output of the device, while the other is mixed with the input mode, ρ_{in}, on a 50:50 beam splitter. Both output modes of the 50:50 beam splitter are measured on photon detectors and the observation of exactly one photon in the measured modes is taken as the successful heralding flag.

Depending on which of the two detectors is triggering the flag, an optical phase correction has to be applied at the output of the device. This feed-forward mechanism is not essential to our discussions, and we incorporate it directly into the description of the device. In practice one will have to do this feed forward, unless the action of the phase correction can be combined with a subsequent measurement in such a way that, instead of active feed forward, just a reinterpretation of the measurement results takes place.

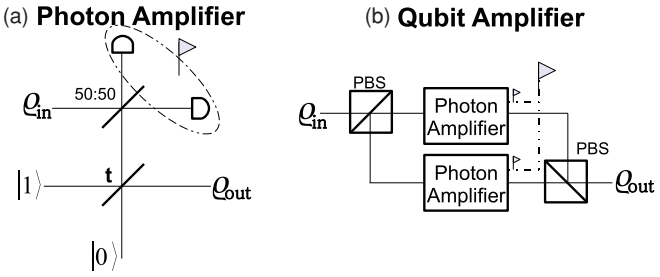

FIG. 1. (Color online) (a) The Ralph-Lund noiseless linear amplifier scheme: An input mode ρ_{in} interacts with an ancilla state through a 50:50 beam splitter. Conditioned on a successful detection pattern, which raises the heralding flag, the output ρ_{out} is shifted toward the single-photon state. The parameter t is the transmissivity of the beam splitter. (b) The Gisin-Pironio-Sangouard qubit heralding device: Two amplifiers are combined to amplify states in the horizontal-vertical (h-v) basis; the flag is only raised if both of the amplifiers are successful. The input state ρ_{in}, encoded in the polarization basis (h-v), is sent through a polarizing beam splitter (PBS) to spatially separate its modes so that the different amplifiers may be applied. A second PBS is used to combine the different spatial modes of the output into the h-v basis. In both schemes the feed-forward mechanism has been omitted.

For $t = \frac{1}{2}$, this scheme amounts to standard probabilistic quantum teleportation; however, for $t > \frac{1}{2}$, the vacuum component $|0\rangle$ of the outgoing mode ρ_{out} is reduced and the single-photon term $|1\rangle$ emerges enhanced relative to the vacuum component. This corresponds to a mapping induced by a Kraus operator A,

$$A\,(c_0|0\rangle + c_1|1\rangle) = \sqrt{1-t}c_0|0\rangle + \sqrt{t}c_1|1\rangle, \tag{1}$$

which has the important property that, as $t \to 1$, this circuit approaches a projection onto the single-photon state, $|1\rangle$. We use non-normalized states in our description, so that the success probability of the heralding device is given by the norm of the conditional output state and it is naturally dependent of the input state.

The two-dimensional Hilbert space of exactly one excitation in two optical modes is known as a photonic or dual-rail qubit [7]. It is the central idea of the work by Gisin *et al.* [3] to use two Ralph-Lund amplifiers [4] in parallel on the two modes to herald such a photonic qubit. A successfully heralded event is defined as the joint success of both amplifiers. The action is then represented as

$$\begin{aligned} &A \otimes A\,(c_{00}|00\rangle + c_{10}|10\rangle + c_{01}|01\rangle) \\ &\quad = (1-t)c_{00}|00\rangle + \sqrt{t(1-t)}\,(c_{10}|10\rangle + c_{01}|01\rangle)\,. \end{aligned} \tag{2}$$

The circuit for this qubit amplifier is shown in Fig. 1, where the dual-rail qubit is encoded in the polarization. The weight of the dual-rail qubit component in this conditional state can reach unity in the limit $t \to 1$. In this limit the probability of successful heralding vanishes independently of the input state. If the input state also contains a multiphoton component, $c_{11}|11\rangle$, then the weight of the dual-rail qubit in the output state can no longer reach unity, as the output will also contain the component $tc_{11}|11\rangle$. In that case, the choice $\frac{t}{1-t} = \frac{|c_{00}|}{|c_{11}|}$ optimizes the qubit fraction of the output. This optimal qubit fraction in the heralded signals is then given by

$$\frac{|c_{10}|^2 + |c_{01}|^2}{2|c_{11}||c_{00}| + |c_{10}|^2 + |c_{01}|^2}. \tag{3}$$

Although we have only considered the case of a pure state input, this bound also applies to mixed states if $\sqrt{\langle ij|\rho_{in}|ij\rangle}$ is used instead of $|c_{ij}|$.

III. KNILL-LAFLAMME-MILBURN PROCEDURE

Before proposing a scheme to overcome the limitations of the heralding setup by Gisin *et al.*, let us take a more fundamental point of view. We remain restricted to the linear optics toolbox, but allow for the use of more complicated sources for the ancilla states, and show that, in this context, the heralding measurement for dual-rail qubits can be performed asymptotically perfectly. Our approach is based on the KLM framework [5] and the procedure introduced therein, which successfully accomplishes the teleportation of an arbitrary state of the form $c_0|0\rangle + c_1|1\rangle$ with a probability that can be brought asymptotically close to 1.

The implementation of such procedure relies on the use of an ancilla state

$$|t_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{i=0}^{n} |s_{n,i}\rangle, \tag{4}$$

where $|s_{n,i}\rangle = |1\rangle^i|0\rangle^{n-i}|0\rangle^i|1\rangle^{n-i}$. Here the notation $|1\rangle^i$ refers to the i-fold tensor product $|1\rangle^{\otimes i}$. We refer to the first n modes of this state as the teleporting modes, while the second n modes are referred to as output modes. In order to perform the teleportation, an $(n+1)$-mode Fourier transform is performed on the teleporting modes of the ancilla $|t_n\rangle$ and the input, followed by a photon-counting measurement on these modes. The Fourier transform is responsible for making the result of the photon measurements indistinguishable independently of which modes the photons have originated from. As a result, if k photons are detected, the remaining unmeasured output modes are left in the state

$$c_0|0\rangle^k|1\rangle^{n-k} + e^{-i\phi_k}c_1|0\rangle^{k-1}|1\rangle^{n-k+1}. \tag{5}$$

The phase ϕ_k depends on the number of counted photons, k, and the observed detection pattern, and can be corrected with an appropriately adjusted phase shifter. As in the case of the linear photonic amplifier, we will incorporate this correction automatically into our description. Overall, the input state will then be found in the kth mode of the above state.

This approach can also be adapted to perform a nondemolition measurement onto the single-photon input space of two modes. To do this, we will consider the auxiliary state

$$|\tilde{t}_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{i=0}^{n} |s_{n,i}\rangle|s_{n,n-i}\rangle, \tag{6}$$

which corresponds to those terms in $|t_n\rangle \otimes |t_n\rangle$ containing exactly n photons in the two sets of teleporting modes in the $|s_{n,i}\rangle$ states. We now show that the application of the KLM-type procedure, employing the alternative state above, realizes a QND measurement onto the total photon-number space of the input modes. To verify this, we first note that this procedure effectively measures the photon number in the

input: As the total number of photons in the two pairs of teleporting auxiliary modes is known to be n, the observed photon number on the input and these $2n$ modes tells us how many photons have entered the heralding device. In a second step, we need to verify that the output state corresponds to that of a QND measurement: If the two Fourier measurements acting each on one input mode and one set of teleporting modes yield the observation of i and $n-i+1$ photons respectively, giving exactly $n+1$ photons in total, and these individual photon numbers are neither 0 nor $n+1$, then the corresponding conditional state of the remaining $2n$ output modes is

$$c_{01}|0\rangle^{i}|1\rangle^{n-i}|0\rangle^{n-i}|1\rangle^{i}+c_{10}|0\rangle^{i-1}|1\rangle^{n-i+1}|0\rangle^{n-i+1}|1\rangle^{i-1}. \tag{7}$$

This means that the input state has been teleported into the mode pair with indices $(i,2n-i+1)$ of the above state. The probability of failure of this scheme, just as in the original KLM proposal, is connected to occurrence of 0 or $n+1$ photons in the individual Fourier measurements, and is given by $\frac{1}{n+1}$. Thus, one can perform a probabilistic perfect heralding measurement and the probability of success can be made arbitrarily close to unity.

IV. MODIFIED AMPLIFIER CIRCUIT

An obvious strength of the scheme proposed in [3] lies in the relative simplicity of its ancilla states, which can be generated with a single-photon source and vacuum states. Here we take a practical approach, keeping the same ancilla states, and look for simple modifications we can make to the amplifier to improve its performance. We focus on modifying the amplifier so that a vacuum input will no longer trigger the heralding flag at all. We begin by examining the original scheme, which consists of two separate Ralph-Lund amplifiers, each with their own auxiliary single-photon states.

In order for the signal to be heralded by the qubit amplifier, both of the flags on the separate Ralph-Lund amplifiers need to be raised by detecting exactly one photon respectively, after each of the 50:50 beam splitters. This setup can lead to false flagging for a vacuum input. These false heralding flags occur if both of the auxiliary photons from the separate amplifiers travel upward in our diagram toward the heralding detectors behind the 50:50 beam splitters.

We suppress this component by adding another 50:50 beam splitter between these upward directed modes; the Hong-Ou-Mandel effect [6] ensures that the component with two photons in each mode will now bunch to either of the outgoing modes of the beam splitter. This means that the heralding detectors of one of the Ralph-Lund amplifiers will see zero photons, while the other will see two, and therefore, the heralding condition of the qubit amplifier will no longer be met. A second 50:50 beam splitter is added to the output modes of the qubit amplifier, so that the transformation effected by the amplifier to the single-photon input does not change. On the other hand, the action of the second beam splitter corresponds to a change of polarization basis on the single-photon subspace, and can be absorbed into the action of any device that is acting on the output of the heralding device. With these two additional beam splitters (see Fig. 2), we find that the successful heralding is

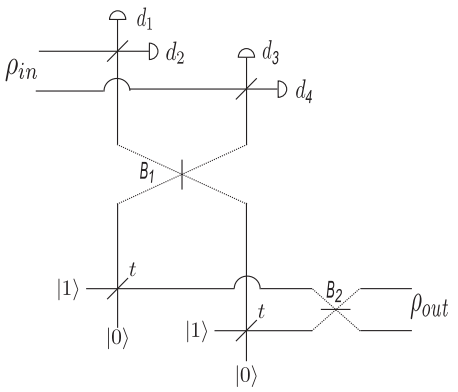

FIG. 2. The proposed circuit for the improved qubit amplifier. Without the two 50:50 beam splitters, marked B_1 and B_2, it corresponds exactly to the amplifier suggested by Gisin *et al*. The circuit's inputs are the two modes of ρ_{in}. The amplifier is only meant to output a signal, ρ_{out}, when a single photon is measured in each of the detector sets (d_1,d_2) and (d_3,d_4). The required feed-forward mechanism to correct optical phases is omitted.

connected to the Kraus operator A_{mod} given by

$$\begin{aligned}&A_{\text{mod}}\left(c_{00}|00\rangle+c_{10}|10\rangle+c_{01}|01\rangle+c_{11}|11\rangle\right)\\&\quad=\sqrt{t(1-t)}\left(c_{01}|01\rangle+c_{10}|10\rangle\right)+t\frac{1}{\sqrt{2}}c_{11}\left(|20\rangle+|02\rangle\right).\end{aligned} \tag{8}$$

This Kraus operator already accounts for the required phase correction that depends on the exact pattern of single-photon detection after each of the two 50:50 beam splitters.

The transformation overcomes both of the problems discussed in Sec. II: First, assuming only vacuum and single-photon input signals ($c_{11}=0$), this amplifier can perform a perfect, heralded projection onto the dual-rail component. Second, even if multiple photons are present in the input ($c_{11}\neq 0$), the single-photon fraction in the output can still be made arbitrarily close to unity in the limit of vanishing success probability ($t\longrightarrow 0$).

V. APPLICATION TO DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

The security of device-independent quantum key distribution (DIQKD) is based on a set of assumptions that is reduced compared to that of traditional QKD, the most remarkable difference being that for DIQKD the communicating users of an entanglement-based scheme can be ignorant of the precise characterization of their measuring devices without compromising the security of the protocol. The privacy of the resulting key depends on the users being able to perform measurements that violate Bell's inequality. This approach first appeared with Einstein-Podolsky-Rosen–based (EPR-based) QKD [8]. Related work has been done under the headline of self-testing devices [9–11]. Here we refer to the formulation by Acin *et al*. [12].

To bound information of an eavesdropper in DIQKD, Alice and Bob both randomly and independently select two measurements that are designed to verify the violation of Bell's inequality by evaluating a Bell parameter S. To generate the

key, the receiver also makes use of a third measurement, σ_z, which is designed to obtain highly correlated data with the sender. These data serve as the raw key from which the final key will be distilled. On these data, we expect to find binary error rates Q.

In the proposal for the original qubit heralding device, a DIQKD simulation was performed to demonstrate how heralding overcomes transmission losses. The simulation included imperfect sources and detectors. We perform analogous simulations to demonstrate the improvement that our heralding device offers. For this comparison, we consider three main scenarios. The first one is motivated by the simulation reported in Gisin *et al.* [3], where the authors introduced a theoretical framework to deal with inconclusive outputs due to imperfect devices. In this framework restrictions on the eavesdropping strategies are assumed; we therefore refer to this framework in our simulations as the restricted device-independent theory, in Sec. V A 1. In addition we also run simulations that deal with the inconclusive results by randomly assigning them a conclusive binary value, thereby allowing us to apply the usual unrestricted device-independent theory, in Sec. V A 2. As a third framework, we explore the so-called detection device-independent theory, in Sec. V A 3, where knowledge of the source is assumed, but one can remain ignorant about the measurement device of one of the parties. The assumed knowledge of the source, in this framework, makes it useful not only for entanglement-based setups, but also for prepare-and-measure schemes.

A. Experimental Setup

We now describe the proposed experimental setup for DIQKD. To mediate the communication, a spontaneous parametric down-conversion (EPR-SPDC) source is used which generates entangled photons. The (unnormalized) state obtained through this process is given by

$$\rho_{\text{source}} = |0\rangle\langle 0| + p|\phi^+\rangle\langle\phi^+| + p^2|\phi^{+2}\rangle\langle\phi^{+2}| + O(p^3), \tag{9}$$

where $|\phi^+\rangle$ is an EPR pair, $|1010\rangle + |0101\rangle$ and $|\phi^{+2}\rangle = |2020\rangle + |1111\rangle + |0202\rangle$, up to a normalization. The parameter p is related to the pumping power. This EPR-SPDC source is located near one of the parties, Alice, and the two-mode signal that is received by the more distant party, Bob, is subject to transmission loss η_t. The loss which results from using imperfect detectors and coupling into fibers is taken into account with efficiency parameters η_d and η_c respectively. In our simulations we assume that all the detectors have the same efficiency so we model the detectors as perfect and include the detector loss in the coupling efficiency $\eta_{\text{cd}} = \eta_c\eta_d$. The photons employed in the auxiliary states of the amplifiers are generated from a heralded SPDC process that outputs the state [13]

$$\begin{aligned}\rho_{\text{aux}} = {} & p'\eta_{\text{cd}}|1\rangle\langle 1| + 2(1-\eta_{\text{cd}})\eta_{\text{cd}}p'^2|2\rangle\langle 2| \\ & + 3(1-\eta_{\text{cd}})^2\eta_{\text{cd}}p'^3|3\rangle\langle 3| + O(p'^4),\end{aligned} \tag{10}$$

where p' is again the pumping power. The amplifier therefore acts on the state

$$\rho_{\text{total}} = \rho_{\text{source}} \otimes \rho_{\text{aux}}^{\otimes 2} \otimes |0\rangle\langle 0|^{\otimes 2} \tag{11}$$

which includes both components of the source states: the one that remains at Alice's site, and that which enters the amplifier. The whole setup is depicted in Fig. 3 to indicate where coupling and detection efficiencies are included. Note that we include coupling efficiencies for the heralding detectors. Omitting these reproduces for the original heralding device the simulation shown in [3]. The source is on Alice's side of the setup. Therefore, transmission loss affects only the signal traveling from the source to the amplifier, which is located in Bob's site.

In order to maximize the key rate, an optimization is performed over the pump parameter p and over the transmissivity t of the beam splitter used in the heralding device. The range of the parameters p and p' are restricted to $0 \leqslant p, p' \leqslant 10^{-2}$, as we use a perturbative approach in our simulations. This constraint, however, affects only the simulations of the detection device-independent scenario.

Our simulations are done as perturbative approximations in the pump parameters p and p'. To bound the error in this approximation, we also provide lower bounds on the expected key rates by calculating the total weight of the neglected terms,

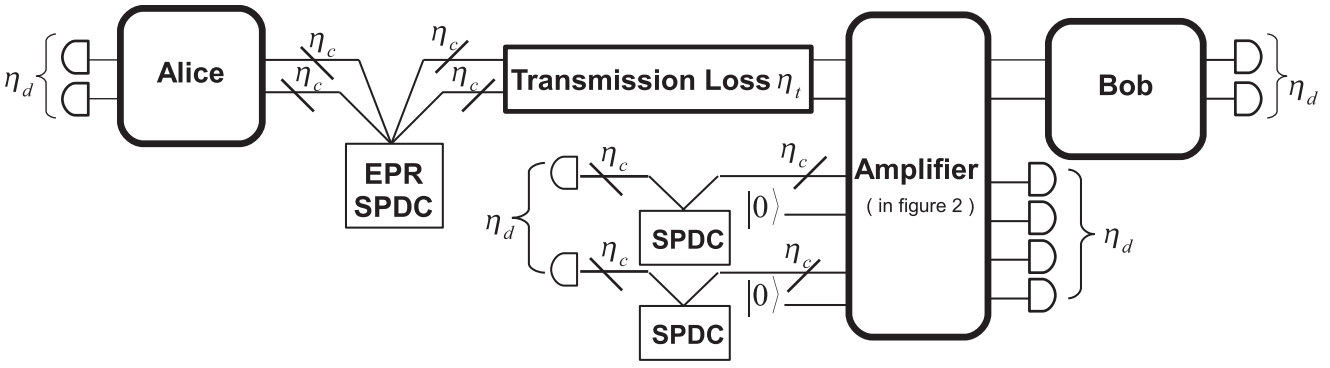

FIG. 3. Experimental setup for the amplifier in the DIQKD simulations we consider. An EPR-SPDC source is used to generate photons that are sent to the two distant parties. Two additional SPDC sources are used as heralded single photon sources for the amplifier. Each wire in this diagram represents a separate optical mode (i.e., we use two wires to represent a single spatial mode if we are using both of the polarization, horizontal (h) and vertical (v), degrees of freedom). The signal received by Bob is only processed if the right detection pattern appears on the amplifier.

and by using this weight in independent worst-case values for the Bell parameters S and quantum bit error rates Q.

For simulation purposes, we follow the choices made in [3]. This includes modeling our detectors with photon-number resolving capabilities, neglecting dark counts, assuming a detection efficiency as high as 95% and running the sources at a repetition rate of 10 GHz. Dark counts can be neglected if the total dark count rate is negligible compared to the total rate of heralded events.

Superconducting nanowire single-photon detectors and transition-edge superconducting detectors have shown these properties, although not in a single device [14,15]. Transition-edge superconducting detectors are photon-number resolving detectors and have also been demonstrated to work at an efficiency of 95%. However the repetition rate of the sources we use, 10 GHz, is several orders of magnitude higher then the optimal clock rate of these detectors, which run at 1000 counts per second. Alternatively, superconducting nanowire single-photon detectors are capable of working at the clock rates we consider in our simulations. These detectors are not photon-number resolving, however, a cascade of single-photon detectors may be used to approximate a number resolving detector. However, the nanowire detectors work at efficiencies that are much lower than what we have assumed in our simulations, typically the efficiency is 20% [14].

1. *Restricted device-independent theory*

The framework proposed by Gisin *et al.* follows the standard device-independent protocol [16], but augments it by an analysis that makes an additional assumption about the eavesdropping strategies. Thanks to this assumption, all of the inconclusive results can be discarded during postprocessing, though the rate of inconclusive results affects the resulting key rate. The key rate, which is given by

$$K \geqslant \mu_{\mathrm{cc}}\Bigg\{1 - h[Q_{\mathrm{cc}}] - \left[\left(1 - \frac{\mu_c}{\mu_{\mathrm{cc}}}\right)\chi\left(\frac{\mu_{\mathrm{cc}}S_{\mathrm{cc}} - 4\mu_c}{\mu_{\mathrm{cc}} + \mu_c}\right) + \frac{\mu_c}{\mu_{\mathrm{cc}}}\right]\Bigg\}, \quad (12)$$

with

$$h[x] = -x\log_2[x] - (1-x)\log_2[1-x] \quad \text{and} \quad (13)$$

$$\chi[x] = \begin{cases} h\left[\frac{1+\sqrt{(x/2)^2-1}}{2}\right] & \text{if} \quad x > 2 \\ 1 & \text{otherwise} \end{cases}. \quad (14)$$

Here, μ_{cc} is the probability that both parties obtain a conclusive result. Within this set of conclusive data, S_{cc} is the measured Bell parameter, and Q_{cc} is the error rate. The probability that only one of the parties obtains a conclusive result is denoted by μ_c. The results are shown in Fig. 4. We find that our heralding device improves the distance and rate significantly.

2. *Unrestricted device-independent theory*

The scheme utilizing the unrestricted device-independent theory differs solely from the setting in the previous section in its data postprocessing stage. Any inconclusive measurement result on either side has binary outcomes assigned at random. Knowledge of the placements of such inconclusive results is later used in the error correction step [17]. For this reason, the key rate includes quantities that reflect the fraction of conclusive results. The resulting key rate is

$$K = \mu_{-c}\,(1 - h[Q_{-c}]) - \chi[S]. \quad (15)$$

Here, μ_{-c} is the probability of Bob obtaining a conclusive result and Q_{-c} is the error rate within Bob's conclusive measurement results. Finally, $h[x]$ and $\chi[x]$ are the same as in Eqs. (13) and (14). The Bell parameter S is evaluated using the data from all of the measurement results, including the random assignments of inconclusive results.

From Eq. (15), we can see that the parties need nonclassical correlations with at least $S > 2$ to generate a positive key, since $\chi[S] = 1$ otherwise. With our chosen postprocessing strategy, we randomly assign binary outcomes to inconclusive measurement results, so that only the subset of measurements that yield conclusive outcomes on both sides make nonzero contributions to the Bell parameter, S. As quantum mechanics bounds the Bell parameter in any subset to $2\sqrt{2}$ the requirement that $S > 2$ leads to the bound $\mu_{\mathrm{cc}} > \frac{1}{\sqrt{2}} \sim 0.707$, on the probability of conclusive-conclusive measurement outcomes. However, if we use a SPDC source to generate the signals, we find from Eq. (3) that the qubit fraction after heralding is bounded by $\mu_{\mathrm{cc}} < 3/5$ when using the original heralding device, even when using ideal detectors and single-photon sources. Therefore, such an amplifier cannot be employed to generate positive key rates in this framework, unless a different source is used to generate the entangled photons. Note that other assignments of inconclusive results are possible [1], which may allow the extraction of a secret key with the original heralding device. The discussion requires more detailed analysis, as it depends on the exact configuration of the setup. It is omitted here, as these studies go beyond the scope of the current research. However, some discussion of this question can be found in the work by Moroder and Curty [18].

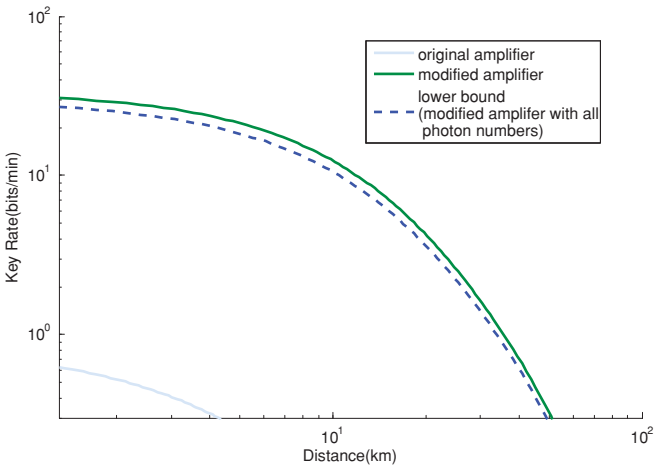

FIG. 4. (Color online) Key rate vs distance, plotted for both the original [3] and the modified amplifier. The simulations are done using the restricted device-independent theory framework. The key rate is calculated from Eq. (12), multiplied by the repetition rate of the source and the probability that the amplifier successfully heralds the signal. The efficiency parameters are chosen as $\eta_d = 0.95$ and $\eta_c = 0.90$, resulting in an overall efficiency of $\eta_{\mathrm{cd}} = 0.855$.

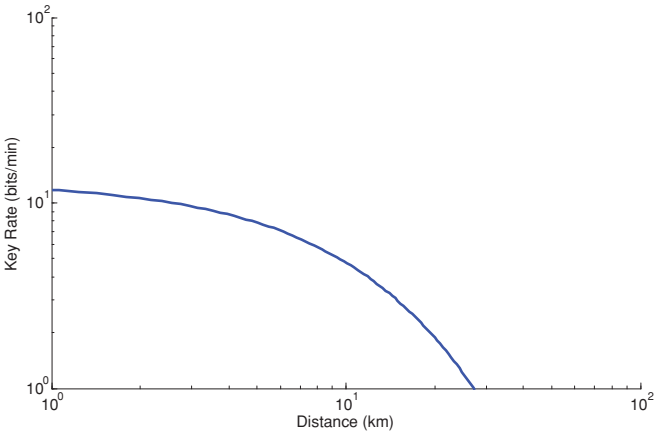

FIG. 5. (Color online) Key rate vs distance, plotted on a logarithmic scale for our proposed amplifier using the unrestricted device-independent theory framework. We calculate the key rate from Eq. (15), multiplied by the repetition rate of the source, 10 GHz, and the probability that the amplifier successfully heralds the signal. The efficiency parameter is $\eta_{\mathrm{cd}} = 0.95$. The bound for the influence of the higher photon terms is not included in this plot since the bound differed negligibly from the perturbative calculation.

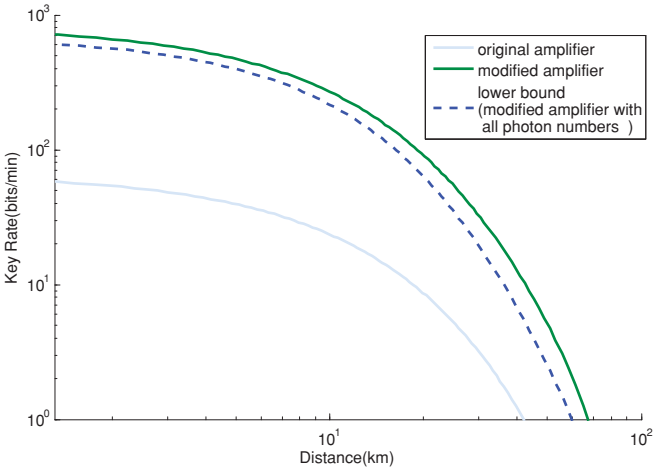

FIG. 6. (Color online) Key rate vs distance, plotted for both the original and the modified amplifier using the detection device-independent theory framework. We calculate our key rate from Eq. (16), multiplied by the repetition rate of the source, 10 GHz, and the probability that the amplifier successfully heralds the signal. The efficiency parameter is $\eta_{\mathrm{cd}} = 0.75$.

Due to the above, the simulations for the unrestricted device-independent theory are performed only for our proposed amplifier (see Fig. 5). This framework is the most demanding on coupling and detection efficiencies that need to be used in order to generate a positive key: In our simulations, we use a total loss term $\eta_{\mathrm{cd}} = 0.93$.

3. *Detector device-independent theory*

The final framework we consider is not fully device independent and, as a result, the security does not require a loophole-free violation of Bell's inequality. Here, the standard Bennett-Brassard 1984 (BB84) protocol is used [19] and we trust the source on Alice's side only. Bob's detectors remain uncharacterized. This scenario has been considered by Mayers [20], and later also by Koashi [21]. The scenario makes random assignment of inconclusive results on Bob's side necessary and therefore places a constraint on the detection probability that is required in order to generate a secure key [17]. Again we use the fact that the position of events with random assignment are known to Bob, who can utilize this knowledge in the later error correction step. The security proof [17] is therefore a variation of corresponding proofs of Koashi [21]. This scenario is more tolerant to transmission loss. For example, with perfect photon pair sources and detection devices, this scenario tolerates a total efficiency accounting for transmission, coupling, and detection loss of 64.5% without heralding [17]. The key rate for this scheme is given by [17]

$$K \geqslant \mu_{-c}\,(1 - h[Q_{-c}]) - h[\delta_b]. \tag{16}$$

Here, $\delta_b = \mu_{-c} Q_{-c} + (1 - \mu_{-c})\frac{1}{2}$ is an effective phase error rate, μ_{-c} is the probability of Bob obtaining a conclusive result [as in Eq. (15)], and Q_{-c} is the error rate when Bob's measurement is conclusive. This framework is the least demanding on the coupling and detector efficiencies.

The simulations' results are shown in Fig. 6. In this case the pump parameters are larger compared to the other two scenarios. Therefore, the gap between the approximated rates and the lower bounds is more pronounced.

VI. CONCLUSIONS

Heralding devices can play an important role in quantum key distribution. In principle, they allow to overcome the limitation posed by transmission losses to device-independent quantum key distribution. In addition, other areas of quantum communication can benefit from such heralding devices. For example, some quantum memory approaches do not provide intrinsic heralding devices. Using external heralding, as proposed in this paper, will allow the use of such memories in quantum repeater technologies [22].

In this regard, we have explored the KLM framework and employed it in the implementation of a conceptually optimal heralding strategy that, in the limit of asymptotic resources, achieves a perfect QND-like measurement onto the desired signal subspace with success probability approaching unity.

Departing from the conceptual scenario, we discussed a simple and experimentally viable improvement on the original work by Gisin *et al.* [3], enhancing the performance of the heralding device. Specifically, we were able to overcome the undesired relation between how reliably the device works in heralding its input, and the success probability of the heralding process. Our device allows, in an idealistic implementation, perfect operation on the important input subspace containing at most one photon in each of the optical modes that define the dual-rail qubit.

This improvement not only increases the achievable key rates, in the context of a restricted device-independent theory, by roughly one order of magnitude in distance and rate as compared to the scheme in [3], but also allows us to enter the domain of fully unrestricted device-independent theory. Our simulations show that, under similar assumptions as those made in [3], we can obtain positive key rates in this desirable

scenario. Note, however, that the requirements on detection and coupling efficiency are more demanding.

Finally, we showed that, for detector device-independent theories with a well characterized source but uncharacterized detection devices, a secret key can be generated with relaxed requirements on the detection and coupling efficiencies, pushing these scenarios now into the domain where experimental realization can be attempted.

ACKNOWLEDGMENTS

D.P., X.F.M., and N.L. have been supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) under its Discovery Program, NSERC and the National Research Agency (ANR) of France with the Strategic Project Grant (SPG) FREQUENCY, and the Innovation Platform Quantum Works. Further support has been received by the Ontario Centres of Excellence. P.v.L and R.W. were supported by the German Research Foundation (Deutsche Forschungsgemeinschaft) through its Emmy Noether Program. Portions of this work were carried out while R.W. was visiting the Institute for Quantum Computing in Waterloo, Canada. He is thankful for the hospitality of the Optical Quantum Communication Theory group and acknowledges financial support through the Collaborative Student Training in Quantum Information Processing program.

[1] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[2] P. M. Pearle, Phys. Rev. D **2**, 1418 (1970).
[3] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[4] T. C. Ralph and A. P. Lund, in *Proceedings of 9th International Conference on Quantum Measurement and Computing* (AIP, New York, 2009), pp. 155–160.
[5] E. Knill, R. Laflamme, and G. Milburn, Nature (London) **409**, 46 (2001).
[6] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[7] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 797 (2007).
[8] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[9] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, FOCS '98* (IEEE, Palo Alto, 1998).
[10] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).
[11] M. McKague and M. Mosca, in *Proceedings of the 5th Conference on Theory of Quantum Computation, Communication, and Cryptography* (Springer-Verlag, Berlin, 2011), pp. 113–130.
[12] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[13] T. Pittman, B. Jacobs, and J. Franson, Opt. Commun. **246**, 545 (2005).
[14] G. N. Gol'sman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, Appl. Phys. Lett. **705**, 79 (2001).
[15] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).
[16] A. Acin, S. Massar, and S. Pironio, New J. Phys. **8**, 126 (2006).
[17] X. Ma and N. Lütkenhaus (unpublished).
[18] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304(R) (2011).
[19] 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.
[20] D. Mayers, JACM **48**, 351 (2001).
[21] M. Koashi, New J. Phys. **11**, 045018 (2009).
[22] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).