Measurement-device-independent quantum key distribution with quantum memories

Silvestre Abruzzo, Hermann Kampermann, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, Universitätsstrasse 1, 40225 Düsseldorf, Germany
(Received 26 June 2013; published 2 January 2014)

We generalize measurement-device-independent quantum key distribution [Lo, Curty, and Qi, Phys. Rev. Lett. **108**, 130503 (2012)] to the scenario where the Bell-state measurement station contains also heralded quantum memories. We find analytical formulas, in terms of device imperfections, for all quantities entering in the secret key rates, i.e., the quantum bit error rate and the repeater rate. We assume either single-photon sources or weak coherent pulse sources plus decoy states. We show that it is possible to significantly outperform the original proposal, even in presence of decoherence of the quantum memory. Our protocol may represent the first natural step for implementing a two-segment quantum repeater.

DOI: 10.1103/PhysRevA.89.012301 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum communication has been developed in the past thirty years. One prominent communication protocol is quantum key distribution (QKD), which aims at distributing a secret key between two distant parties. Suitable quantum systems for quantum communication are photons as they have very low decoherence and can be easily generated, distributed, and detected with standard technology. However, due to absorption in optical fibers (or free space), QKD with reasonable rates is only possible up to ca. 150 km [1]. To overcome this problem, quantum repeaters have been developed [2]. The idea is to divide the distance between Alice and Bob in segments, to create entanglement in each segment, and then to enlarge the distance using entanglement swapping. Nowadays, the constituent parts of a quantum repeater have been realized and small networks have been implemented in a laboratory setup [3]. However, a complete quantum repeater (even with two segments) that will outperform direct transmission has not been realized yet [4].

Recently, measurement-device-independent QKD (MDI-QKD-RELAY) has been proposed [5,6]. The protocol, described in Ref. [5], is based on the principle of a quantum relay [7] and uses weak coherent pulse (WCP) sources. Briefly speaking, two parties, Alice and Bob, each equipped with a WCP source, send photon pulses to a station which performs a Bell-state measurement (BSM) and communicates the result to Alice and Bob. Then Alice sends Bob information regarding the used basis such that if necessary Bob can implement a bit flip. This protocol is measurement device independent because Alice and Bob do not need to measure anything and therefore the protocol is immune to detector attacks [8,9]. The MDI-QKD-RELAY has already been implemented experimentally, both in a laboratory environment and in a real-world environment [10–12]. Moreover, more efficient protocols have already been proposed [13–15] and finite-size corrections have been analyzed [15–18].

In this paper we extend the original MDI-QKD-RELAY protocol [5], introducing quantum memories in the BSM station. The first consequence is that heralding, provided by quantum memories, permits improvement of the rate at a given distance where MDI-QKD can be used. The advantage of our protocol over other quantum repeater protocols is that it does not need entanglement sources but only commercial off-the-shelf weak coherent pulse sources. Quantum memories have not reached the commercial market yet but they are under active development. With our protocol we show that it is possible to use quantum memories with low coherence time.

The manuscript is organized as follows. In Sec. II we present a generalization of measurement-device-independent QKD with single-photon sources to the scenario with quantum memories. We derive the formula for the secret key rate and we study its dependency on the decoherence of the quantum memories. Finally, we compare the secret key rate obtained with our protocol with the one obtained with the quantum relay proposed in Ref. [5]. In Sec. III we generalize the whole analysis to WCP sources. In order to calculate the secret key rate we consider QKD with decoy states [19,20]. In Sec. IV we give our conclusions.

II. SCHEME WITH SINGLE-PHOTON STATES

In this section we extend the MDI-QKD-RELAY protocol presented in Ref. [5], introducing quantum memories (QM) and using single-photon sources (SPS), which would be the ideal type of source for this protocol. Therefore, although SPSs are still not practical they will permit us to establish upper bounds on the achievable secret key rate; i.e., sources emitting multiphoton pulses or with additional imperfections will lead to worse secret key rates. We denote the protocol considered in this section as MDI-QKD-REPEATER-SPS.

A. The protocol

In the following we give the steps of the protocol, which is a generalization of the one proposed in Ref. [5] (see Fig. 1):

(1) Alice and Bob prepare randomly and independently one of the four qubit states $|\psi\rangle \in \{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, where $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$. We refer to the set $\{|0\rangle,|1\rangle\}$ as the Z basis (or rectilinear basis) and the set $\{|+\rangle,|-\rangle\}$ as the X basis (or diagonal basis). The states are sent through the quantum channel to the repeater station. The information related to the created states is stored by Alice and Bob locally. This process is repeated continuously by Alice and Bob with frequency ν_s, which is the repetition frequency of the source.

(2) When both quantum memories are filled up, the quantum memories are read and a Bell-state measurement

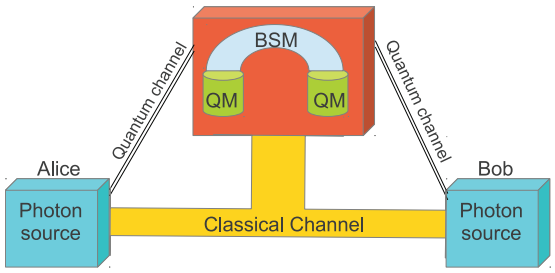

FIG. 1. (Color online) Scheme of a measurement-device-independent quantum repeater. The difference with regard to MDI-QKD-RELAY is that quantum memories are used. QM, quantum memories; BSM, Bell-state measurement. The two sources produce single-photon states or weak coherent pulses.

(BSM) is performed. The result of the BSM, the fact that the measurement was successful, and the time bin of the measured quantum states are sent to both Alice and Bob.

(3) Sources and stations are time synchronized; i.e., Alice, Bob, and the station have information about the time bin of a photon and a measurement. Using the received information, Alice and Bob discard classical information related to photons absorbed by the channel. Moreover, if the measurement was successful Alice and Bob will keep their stored information about the arrived photons and if needed one of the two parties will perform a bit flip. If the measurement was not successful then Alice and Bob will remove the classical information about the measured photons from their stored pool of data.

(4) After creating sufficiently many bits Alice and Bob do the usual QKD postprocessing, which consists of sifting, parameter estimation, error correction, and privacy amplification [1].

The second step is different from the original MDI-QKD-RELAY protocol. Here quantum memories are used for increasing the entanglement swapping success probability. As a result the total secret key rate will be higher than for the case without quantum memories. The second difference is about the exchanged classical information, which now also includes the value of the arrival times of the photons.

B. The secret key rate

Concerning the security, the protocol is equivalent to the entanglement-based repeater protocol[1] [5,21,22]. In this paper we consider the asymptotic secret key rate, which gives an upper bound on the achievable secret key rate. Finite-size corrections can be included using the analysis done in Refs. [16,17]. Moreover, we assume that sources produce perfectly the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. If this is not the case our analysis can be easily modified by considering the overlap between the basis X and Y as done in Ref. [23]. The formula for the asymptotic secret key rate considered in this manuscript is given in Refs. [1,5]

$$r_\infty^{\mathrm{REP}} := \frac{1}{\langle T\rangle}[1 - h(e_Z) - h(e_X)], \tag{1}$$

where $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy, $e_X(e_Z)$ is the quantum bit error rate (QBER) in the X basis (Z basis) and $\frac{1}{\langle T\rangle}$ is the raw key rate.[2] The QBER represents the fraction of discordant bits in the raw key, which is the collection of bits stored by Alice and Bob before the postprocessing.

We give now an analytical expression for the raw key rate. We denote by P_0 the probability that the quantum state sent by Alice (Bob) is stored in the quantum memory.[3] This probability includes the loss probability of the quantum channel and the writing efficiency of the quantum memory. One knows that photons have been stored because quantum memories are supposed to be heralded. In the following we measure the time in units of $\Delta t := \nu_s^{-1}$, which represents the time that the quantum memory has to wait between two attempts. We introduce the probability $P(k_A,k_B)$ that the photons of Alice AND Bob are stored at time bin k_A and k_B and they were not stored before, i.e.,

$$P(k_A,k_B) := P_0^2(1-P_0)^{k_A-1}(1-P_0)^{k_B-1}. \tag{2}$$

The average number of attempts by the source necessary for generating one bit of the raw key is given by

$$\begin{aligned}\langle K\rangle := \sum_{\substack{s=0\\k=1}}^{\infty} ks\Big\{&[P_{\mathrm{BSM}}(k|k,k)(1-P_{\mathrm{BSM}}(k|k,k)]^s P(k,k)\\ &+\sum_{i=1}^{k-1} P_{\mathrm{BSM}}(k|k,i)[1-P_{\mathrm{BSM}}(k|k,i)]^s P(k,i)\\ &+\sum_{i=1}^{k-1} P_{\mathrm{BSM}}(k|i,k)[1-P_{\mathrm{BSM}}(k|i,k)]^s P(i,k))\Big\},\end{aligned} \tag{3}$$

where $P_{\mathrm{BSM}}(k|k_A,k_B)$ is the probability that the BSM was successful at time $k = \max(k_A,k_B)$ when the two involved photons were stored at times k_A and k_B. Note that if we consider only the first line containing $P(k,k)$ then we recover the expression for the rate of the relay. The second (third) line

[1]The equivalence is seen by the following arguments: Consider an entanglement-based repeater protocol where Alice and Bob each produce the state $|\phi^+\rangle_{\mathrm{AC}} = |\phi^+\rangle_{\mathrm{DB}} := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The subsystems C and D are sent to the channel and subjected to a BSM. On the other hand, subsystems A and B remain in Alice's and Bob's laboratory and are measured in basis X or Z. For the case where both Alice and Bob have chosen basis Z, the measurement is described by two projectors $\{\Pi^{(0)} := |0\rangle\langle 0|, \Pi^{(1)} := |1\rangle\langle 1|\}$. The resulting state is given by $((\Pi_A^i \otimes \Pi_B^j)\otimes \mathcal{E}_{\mathrm{CD}})(|\phi^+\rangle_{\mathrm{AC}} \otimes |\phi^+\rangle_{\mathrm{DB}})$ with $i,j = 0,1$. The QKD measurement and BSM act on different Hilbert spaces and therefore they can be interchanged leading to $(\mathcal{E}_{\mathrm{CD}} \otimes (\Pi_{\mathrm{A}}^i \otimes Pi_B^j))(|\phi^+\rangle_{\mathrm{AC}} \otimes |\phi^+\rangle_{\mathrm{DB}}) = \mathcal{E}_{\mathrm{CD}}(|i\rangle_C \otimes |j\rangle_D)$, where the state $|i\rangle_C \otimes |j\rangle_D$ represents two single photons prepared in the Z basis with polarization i and j. The case of the X basis is analogous.

[2]The sifting rate does not appear because we employ an asymmetric protocol where Alice and Bob produce with probability almost one a state in base X and the remaining times a state in base Z [24].

[3]Here, we consider a completely symmetric setup which implies that the success probability is the same on Alice's and Bob's side. However, in case that Alice and Bob have different probabilities, it is easy to repeat the analysis keeping these two probabilities different.

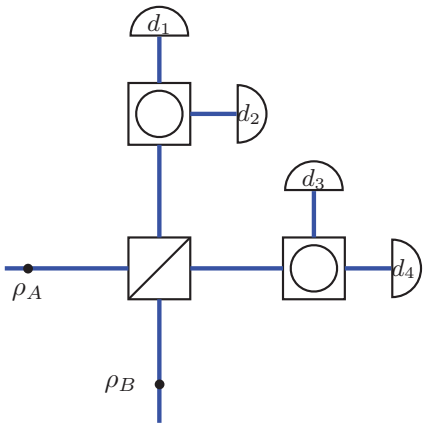

FIG. 2. (Color online) (Adapted from Ref. [26]) Scheme for entanglement swapping with linear optics [3,25]. The square with a diagonal line is a polarizing beam splitter in the rectilinear basis and the squares with circles inside are polarizing beam splitters in the diagonal basis. Entanglement swapping is successful if d_1 and d_3 click (or d_1 and d_4 or d_2 and d_3 or d_2 and d_4). The state $\rho_A(\rho_B)$ is produced by Alice (Bob).

accounts for the case that a photon sent by Bob (Alice) has been stored at a certain time $i < k$ and the photon sent by Alice (Bob) has been stored at time k. The average time becomes $\langle T\rangle := \Delta t\langle K\rangle$.

In order to obtain a closed formula we consider a specific implementation of the BSM [3,25] where the photons are first retrieved from the quantum memories and then measured with linear optics (see Fig. 2). This method is probabilistic and when implemented with perfect quantum memories and detectors leads to a maximal success probability of $\frac{1}{2}$ [27]. The BSM is successful when a particular two-fold detection happens. We consider practical threshold detectors with detection efficiency η_D and dark count probability p_D. We denote by η_M the retrieval probability of a photon from the quantum memory. The BSM success probability for the scheme given in Fig. 2 as a function of $\eta_{\mathrm{MD}} := \eta_M\eta_D$ is then given by [28]

$$P_{\mathrm{BSM}}(\eta_{\mathrm{MD}}) := \tfrac{1}{2}(1-p_D)^2\big[\eta_{\mathrm{MD}}^2 + 2(4-3\eta_{\mathrm{MD}})\eta_{\mathrm{MD}}p_D + 8(1-\eta_{\mathrm{MD}})^2p_D^2\big]. \tag{4}$$

For $p_D = 0$ as we expect $P_{\mathrm{BSM}} = \frac{\eta_{\mathrm{MD}}^2}{2}$. Assuming that η_M does not depend on the time, a simple expression for the average number of attempts in Eq. (3) was derived in Refs. [29,30],

$$\langle K\rangle := \frac{1}{P_{\mathrm{BSM}}(\eta_{\mathrm{MD}})}\frac{3-2P_0}{(2-P_0)P_0}. \tag{5}$$

In the case of absence of quantum memories we get $\langle K\rangle_{\mathrm{relay}} := [P_{\mathrm{BSM}}(P_0\eta_D)]^{-1}$. For small P_0 the rate of the repeater scales as P_0^{-1} while the rate for the relay scales as P_0^{-2}. Moreover for the repeater, dark counts do not play a role as typically $p_D \ll \eta_{\mathrm{MD}}$. The equivalent condition for the relay would be $p_D \ll \eta_D P_0$, which is much more difficult to ensure. For the quantum repeater η_M plays the role of P_0 for the relay.

With the same formalism we calculate the QBER, which enters in the formula of the secret key rate. Let $e_j(k|k_A,k_B)$ be the QBER in the basis $j \in \{X,Z\}$ when the BSM has been performed at time k and the two photons were stored at times k_A and k_B, respectively. Then the average QBER in the basis j is given by

$$e_j = \sum_{k=1}^{\infty}\Bigg[e_j(k|k,k)P(k,k) + \sum_{i=1}^{k-1}e_j(k|k,i)P(k,i) + \sum_{i=1}^{k-1}e_j(k|i,k)P(i,k)\Bigg], \tag{6}$$

where the first line gives the QBER for the case of a quantum relay, i.e., when both photons arrive at the same time. The second and third lines include the contribution to the QBER given by the measurements where one photon arrived at $i < k$ and the second arrives at time k.

Here, we consider a simple model of decoherence where the quantum memory stores perfectly a quantum state for a certain time τ and then it transforms the quantum state to the identity for $t > \tau$ [29]. We call τ the coherence time and measure it in units of Δt. This model is valid in quantum memories where the fidelity remains approximately constant for a certain time and then it drops very fast. Formally, we have

$$e_j(k|k_A,k_B) := e_j(\infty)\Theta[\tau-(k-k_A)]\Theta[\tau-(k-k_B)] + \tfrac{1}{2}\{1-\Theta[\tau-(k-k_A)]\Theta[\tau-(k-k_B)]\}, \tag{7}$$

where $\Theta[t]$ is the Heaviside step function [31] such that $\Theta[t] = 1$ for $t \geqslant 0$ and $\Theta[t] = 0$ for $t < 0$ and $e_j(\infty)$ is the QBER that would be obtained if the memory does not decohere ($\tau \to \infty$) and it is given by [32]

$$e_X(\infty) = e_Z(\infty) = \frac{2p_D(2(\eta_{\mathrm{MD}}-1)^2p_D - (\eta_{\mathrm{MD}}-2)\eta_{\mathrm{MD}})}{\eta_{\mathrm{MD}}^2 + 8(\eta_{\mathrm{MD}}-1)^2p_D^2 + 2(4-3\eta_{\mathrm{MD}})\eta_{\mathrm{MD}}p_D}. \tag{8}$$

By inserting Eqs. (2), (7), and (8) into Eq. (6) we obtain a closed formula for the average QBER:

$$e_j = e_j(\infty) + 2\frac{\big[\frac{1}{2}-e_j(\infty)\big](1-P_0)^{1+\tau}}{2-P_0}. \tag{9}$$

It is easy to verify $e_j(\infty) \leqslant e_j \leqslant \frac{1}{2}$ and moreover $\lim_{\tau\to\infty} e_j = e_j(\infty)$ and $\lim_{P_0\to 0} e_j = \frac{1}{2}$. Note that due to our specific setup $e_X = e_Z$.

If the QBER is too high it is not possible to extract a secret key as the secret key rate in Eq. (1) becomes nonpositive. When $e_X = e_Z$ the maximal QBER for a nonzero secret key rate is given by $e^{\mathrm{MAX}} := 0.11$. A critical parameter is therefore $\tau_{\mathrm{SPS}}^{\mathrm{MIN}}$, which represents the minimal τ permitting us to extract a secret key and can be obtained from Eq. (9) by requiring that $e_X = e^{\mathrm{MAX}}$. The minimal allowed coherence time is given by

$$\tau_{\mathrm{SPS}}^{\mathrm{MIN}} = \frac{\ln\left(\frac{(P_0-2)[e_X(\infty)-e^{\mathrm{MAX}}]}{(P_0-1)[2e_X(\infty)-1]}\right)}{\ln(1-P_0)}. \tag{10}$$

In the following section we provide numbers for the minimal coherence time and the secret key rate in a realistic scenario.

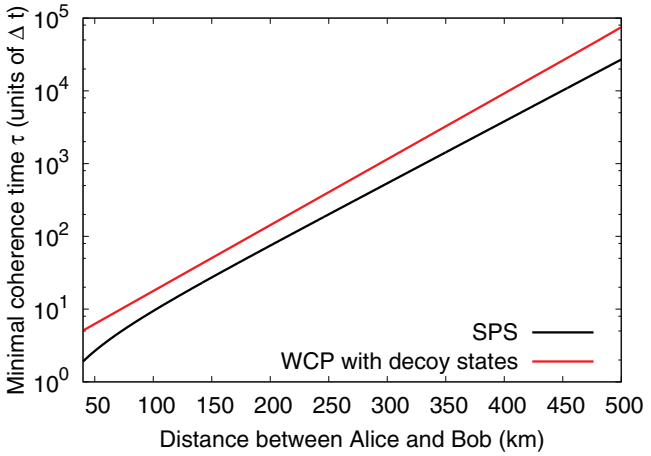

FIG. 3. (Color online) Minimal coherence time τ^{MIN} in units of Δt such that the secret key rate is non zero. Black solid line: SPS protocol [see Eq. (10)]. Red (gray) solid line: WCP protocol [derived by calculating the zero of Eq. (11)]. Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 10^{-6}$, $\alpha = 0.17$ dB/km.

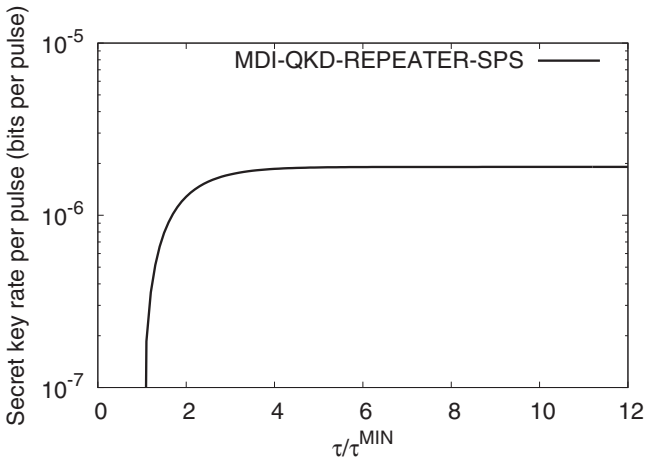

FIG. 4. Secret key rate per pulse as function of $\tau/\tau^{\mathrm{MIN}}_{\mathrm{SPS}}$. The secret key rate increases as the ratio $\tau/\tau^{\mathrm{MIN}}_{\mathrm{SPS}}$ increases. However, after $\tau/\tau^{\mathrm{MIN}}_{\mathrm{SPS}} > 5$ the secret key rate is almost constant and therefore it is not advantageous to use better quantum memories. Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 10^{-6}$, $\alpha = 0.17$ dB/km, $L = 400$ km.

C. Performance

We discuss now the performance of the protocol as a function of the imperfections of the set up. Then we analyze the relation with the original MDI-QKD-RELAY with single-photon states. We consider an implementation where photons are transmitted through optical fibers. Therefore $P_0 := \eta_T$, where $\eta_T := 10^{-\frac{\alpha L}{2\cdot 10}}$ is the probability that a photon has not been absorbed after traveling for a distance $\frac{L}{2}$ and α is the absorption coefficient. Throughout the whole paper we consider $\alpha = 0.17$ dB/km, which is the lowest attenuation in common optical fibers. In the following analysis we consider detectors with detection efficiency $\eta_D = 0.2$ and dark count probability $p_D = 10^{-6}$. Such detectors are considered optimistic but not unrealistic [1]. Regarding quantum memories, we use $\eta_M = 0.6$, which is a value already achieved experimentally [3].

In Fig. 3 we show $\tau^{\mathrm{MIN}}_{\mathrm{SPS}}$ versus the distance between Alice and Bob. For $L = 400$ km we get $\tau^{\mathrm{MIN}} \approx 4 \times 10^4$, which can be transformed in seconds multiplying by Δt. For an hypothetical source at 100 MHz this would correspond to a coherence time of the order of 400 ms. This value of coherence time can be already reached nowadays with room-temperature quantum memories [33]. Note that single-photon sources at such a speed do not yet exist. We reconsider this number in the next section when we consider WCP sources. By increasing the repetition frequency it is possible to use quantum memories with lower coherence times. This is different from standard quantum repeater protocols, where the coherence time depends also on the communication time. We see that the curve of τ^{MIN} is tightly upper bounded by the average maximal time that is necessary to wait before both quantum memories are filled up. This can be understood by observing that for $P_0 \ll 1$ and $e_X \approx 0$ we have $\langle K \rangle P_{\mathrm{BSM}} \approx \frac{3}{2P_0}$ and $\tau^{\mathrm{MIN}} \approx \frac{\ln(2e^{\mathrm{MAX}})}{-P_0} \approx \frac{1.51}{P_0}$.

In Fig. 4 we show the secret key rate as a function of $\tau/\tau^{\mathrm{MIN}}_{\mathrm{SPS}}$ for a fixed distance between Alice and Bob ($L = 400$ km). We see that a flat region is reached for $\tau \approx 5\tau^{\mathrm{MIN}}_{\mathrm{SPS}}$. The same behavior is found also for other values of the distance between Alice and Bob.

Finally, we discuss the secret key rate as a function of the distance and compare it to a setup without quantum memories. As shown in Fig. 5, the setup with quantum memories permits us to increase significantly the secret key rate with respect to a setup without quantum memories. For $\eta_{\mathrm{D}} = 0.2$, $\eta_M = 0.6$ and $p_D = 10^{-6}$ the crossover distance is around 100 km. Moreover, we see that the difference between $\tau = 2\tau^{\mathrm{MIN}}$ and $\tau = \infty$ is very small. This result suggests that the protocol is not very susceptible to decoherence of

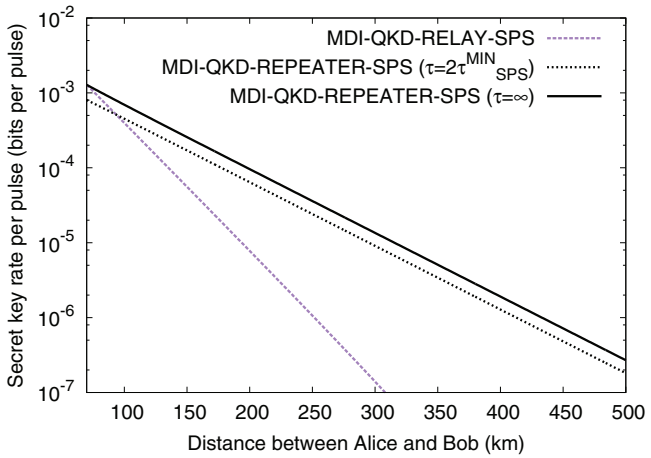

FIG. 5. (Color online) Secret key rate per pulse vs distance between Alice and Bob. Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 10^{-6}$, $\alpha = 0.17$ dB/km. In the region $L < 50$ km the quantum relay performs better than the quantum repeater. This is due to the fact that in this region the quantum memory efficiency plays a major role. Moreover, in this region there are already efficient and practical QKD protocols which do not require an additional measurement station [1]. For $L > 500$ km the secret key rate is already so low that it is not convenient to use the proposed setup.

quantum memories: Perfect quantum memories are not needed as coherence times slightly bigger than τ^{MIN} permit us to achieve the maximal secret key rate obtainable with perfect quantum memories. Moreover, we have performed numerical simulations for quantum memories where the decoherence model is depolarization,[4] and we found that this result does not change qualitatively.

Concluding this section, we have proven that by using single-photon sources and imperfect quantum memories it is possible to essentially double the distance with respect to MDI-QKD-RELAY when implemented with single-photon sources.

III. SCHEME WITH WEAK COHERENT PULSE SOURCES

A critical assumption of the previous section was that Alice and Bob have on-demand single-photon sources at their disposal. In this section we consider sources of weak coherent pulses which offer a very high repetition frequency with current technology even in the order of gigahertz [34]. On the other hand, this type of source requires a more complicated security analysis due to the fact that multiphoton pulses are susceptible to the photon-number-splitting (PNS) attacks [35]. In order to detect this attack it is possible to use decoy states [19,20]. In the scheme with decoy states Alice and Bob prepare phase randomized weak coherent pulses of the form $\rho = \sum_{n=0}^{\infty} p(n) |n\rangle \langle n|$ with $p(n) := e^{-\mu} \frac{\mu^n}{n!}$. The parameter μ is the intensity (average photon number) of the pulse.

The QKD protocol with decoy states [19,20] which we employ here is analogous to the one described in Sec. II, apart from the following differences:

(1) When Alice and Bob prepare the state, they also choose at random and independently its intensity μ, which is a continuous parameter with $0 \leqslant \mu < \infty$. One particular intensity $\overline{\mu}$ is chosen with probability of almost one.

(2) The measurements for pulses with intensity $\overline{\mu}$ are used for extracting a secret key, whereas the others are used for detecting Eve's PNS attack.

The formula for the secret key rate is analogous to Eq. (1) with the modifications due to the fact that Eve can perform PNS attacks. It is given by [5]

$$r_\infty := \max_{\mu>0} \left(\frac{1}{\langle T \rangle} \left\{ f_{11} \left[1 - h\left(e_X^{11}\right) \right] - h(e_Z) \right\} \right), \tag{11}$$

where f_{11} is the fraction of bits in the raw key which are generated when Alice and Bob send single-photon states and e_X^{11} is the QBER of these bits. The QBER e_X^{11} is accessible due to the fact that we use decoy states [5]. The QBER e_Z is determined using all data. All quantities entering in the formula of the secret key rate in Eq. (11) depend on a generic intensity μ. This intensity is used as free parameter for the optimization of the secret key rate. The optimal intensity is denoted by $\overline{\mu}$ (see above). In the following we derive analytical expressions for these parameters as function of the imperfections of the setup. We assume that detectors have no dark counts. This will permit closed formulas, which allow to understand the role of each parameter. Dark counts do not play a crucial role as long as $\eta_{\mathrm{MD}} \gg p_D$. For realistic choice of parameters this condition is easily satisfied.

Given a pulse of n photons, the probability that at least one photon is stored into the quantum memory is given by $[1-(1-\eta_T)^n]$, where η_T is the probability that one photon has not been absorbed by the quantum channel. In general, the probability P_0 that a state has been stored into the quantum memory is given by

$$P_0 := \sum_{n=1}^{\infty} p(n)[1-(1-\eta_T)^n] = 1 - e^{-\mu\eta_T}, \tag{12}$$

which for $\mu\eta_T \ll 1$ reduces to $P_0 = \mu\eta_T$ as expected.

The BSM success probability depends on the probability to store a state with n photons given that the source has generated a state of m photons with $m \geqslant n$. Formally,

$$P(n) := \sum_{m=n}^{\infty} p(m) \binom{m}{n} \eta_T^n (1-\eta_T)^{m-n} = \frac{(\eta_T \mu)^n}{n!} e^{-\eta_T \mu}. \tag{13}$$

The quantity $\binom{m}{n}\eta_T^n(1-\eta_T)^{m-n}$ is the probability that n photons survive from a state with m photons after the transmission through the channel. The probability that the BSM is successful given that one quantum memory contains n_a photons and the other n_b photons is given by (see the appendix for our derivation)

$$P_{\mathrm{BSM}}(n_a,n_b) = \left[\left(1 - \frac{\eta_{\mathrm{MD}}}{2}\right)^{n_a} - (1-\eta_{\mathrm{MD}})^{n_a} \right] \times \left[\left(1 - \frac{\eta_{\mathrm{MD}}}{2}\right)^{n_b} - (1-\eta_{\mathrm{MD}})^{n_b} \right]. \tag{14}$$

For $n_a = n_b = 1$ we obtain $P_{\mathrm{BSM}}(1,1) = \frac{1}{2}\eta_{\mathrm{MD}}^2$ in accordance with Eq. (4). Thus, the BSM success probability is given by

$$P_{\mathrm{BSM}} := 2 \frac{\sum_{n_a=1}^{\infty} \sum_{n_b=1}^{\infty} P(n_a) P(n_b) P_{\mathrm{BSM}}(n_a,n_b)}{\sum_{n_a=1}^{\infty} \sum_{n_b=1}^{\infty} P(n_a) P(n_b)} \tag{15a}$$

$$= 2 \frac{e^{-2\mu\eta_T(\eta_{\mathrm{MD}}-1)} (e^{\frac{1}{2}\mu\eta_{\mathrm{MD}}\eta_T} - 1)^2}{(e^{\mu\eta_T} - 1)^2}. \tag{15b}$$

The denominator in Eq. (15a) gives the probability that two photons are stored in the quantum memories, which is equal to P_0^2. The numerator is the total probability of all events in which the BSM is successful when one quantum memory contains n_a photons and the other one contains n_b photons. The factor 2 comes from the fact that the BSM with linear optics can distinguish only two Bell states. For the limiting case $\mu\eta_T \ll 1$ we obtain $P_{\mathrm{BSM}} = P_{\mathrm{BSM}}(1,1)$.

Under the assumption that an infinite number of decoy states is used, the fraction of measurements coming from single

[4] The model we have considered is $D(\rho) := e^{-\frac{t}{\tau}}\rho + \frac{1-e^{-\frac{t}{\tau}}}{2}\mathbb{1}$, where τ is the coherence time.

photons is denoted as f_{11} and given by

$$f_{11} = \frac{P(1)^2 P_{\mathrm{BSM}}(1,1)}{\sum_{n_a=1}^{\infty}\sum_{n_b=1}^{\infty} P(n_a)P(n_b)} \tag{16a}$$

$$= \frac{\mu^2\eta_{\mathrm{MD}}^2\eta_T^2 e^{\mu\eta_{\mathrm{MD}}\eta_T - 2\mu}}{4\left(e^{\frac{1}{2}\mu\eta_{\mathrm{MD}}\eta_T} - 1\right)^2}, \tag{16b}$$

which in the limit $\mu\eta_T \ll 1$ becomes $f_{11} = 1$ as in this limit all measurements come from single-photon states. The numerator of Eq. (16a) represents the probability that the sources of Alice and Bob produce single photons which are stored in the quantum memories and which lead to successful BSM. The denominator is the total probability to obtain a state which does not contain the vacuum.

Regarding the QBER we observe that if there are no dark counts then both e_X^{11} and e_Z are zero. This property of the protocol has been discussed also in Ref. [5]. Therefore, errors will arise only due to decoherence. The calculation is analogous to the one for single-photon sources of Eq. (6). We assume the same decoherence model. The only difference comes from the fact that now P_0 is different; in particular, we have

$$e_X^{11} = e_X^{11}(\infty) + \frac{1}{2}\frac{\left[\frac{1}{2} - e_X^{11}(\infty)\right]\left(1 - P_0^{11}\right)^{1+\tau}}{2 - P_0^{11}}, \tag{17}$$

$$e_Z = e_Z(\infty) + \frac{1}{2}\frac{\left[\frac{1}{2} - e_Z(\infty)\right](1 - P_0)^{1+\tau}}{2 - P_0}, \tag{18}$$

with $P_0^{11} = p(1)\eta_T$ the probability to store single-photon states in one quantum memory.

We have thus derived all quantities present in the formula of the secret key rate, and we can now evaluate and characterize the protocol.

In Fig. 6 we show the comparison between MDI-QKD-REPEATER-WCP and MDI-QKD-RELAY-WCP. As we see, quantum memories permit us to increase significantly the secret key rate or the distance where it is possible to perform QKD.

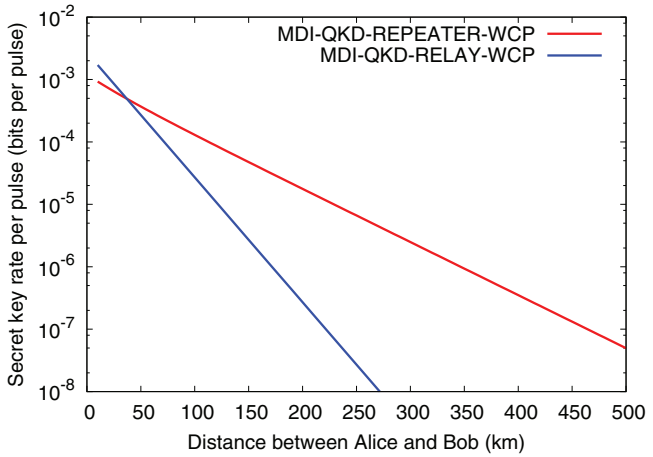

FIG. 6. (Color online) Secret key rate vs distance between Alice and Bob. Comparison between relay [5] (blue [gray]) and repeater [see Eq. (11)] (red [gray]). Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 0$, $\alpha = 0.17$ dB/km, $\tau = \infty$.

As shown in Fig. 3, the minimally allowed coherence time $\tau_{\mathrm{WCP}}^{\mathrm{MIN}}$ is larger then $\tau_{\mathrm{SPS}}^{\mathrm{MIN}}$. The reason is that now the produced state contains also a vacuum that reduces the probability that a photon arrives to the quantum memory. However, the difference is less than one order of magnitude. Moreover, analogously to the case of SPS the flat region($\tau \to \infty$) of the secret key rate is reached already with $\tau = 5\tau_{\mathrm{WCP}}^{\mathrm{MIN}}$.

In practical cases, only a finite number of different decoy states is used. In order to adapt our result to this case it is enough to use the results of Ref. [13]. Moreover, finite-size corrections are necessary for giving realistic estimates. This can be done by adopting the formalism developed in Refs. [15–17].

IV. CONCLUSIONS

In this paper we have explored the possibility to enable long-distance QKD without entanglement sources. We have shown that when quantum memories are used it is possible to improve the distance where measurement-device-independent quantum key distribution can be implemented. Moreover, we have shown that the protocol we consider in this paper is robust against common device imperfections such as detector efficiency, quantum memory retrieval efficiency, and finite decoherence time. Moreover, the robustness of measurement-device-independent QKD has been also investigated under the effect of additional imperfections in the quantum channel, in the detectors and in the quantum memories in Ref. [36]. We believe that our result could be used as a first step in the development of long-distance quantum key distribution. It requires weak coherent pulse sources, which are already available commercially, and heralded quantum memories, which are under current development.

ACKNOWLEDGMENTS

We thank Sylvia Bratzik, Tobias Moroder, and Mohsen Razavi for valuable and enlightening discussions. We thank the referees for providing constructive comments and help in improving the contents of this paper. We acknowledge financial support by the German Federal Ministry of Education and Research (BMBF, Project QuOReP).

APPENDIX

We prove Eq. (14) when the Bell-state measurement is done between two WCP states in the computational basis. The proof for the case of the diagonal basis is analogous.

We define

$$G_{i_1 i_2 i_3 i_4}\left(\rho_A^{(n_a)}, \rho_B^{(n_b)}\right) := \mathrm{tr}\left(\Pi_{d_{i_1}}^{(1)}\Pi_{d_{i_2}}^{(0)}\Pi_{d_{i_3}}^{(1)}\Pi_{d_{i_4}}^{(0)}\mathcal{E}\left(\rho_A^{(n_a)} \otimes \rho_B^{(n_b)}\right)\right), \tag{A1}$$

where $\mathcal{E}$ represents the action of the partial BSM and is given by the following mapping (see Fig. 2):

$$b_H \to \frac{d_3 + d_4}{2}, \quad b_V \to \frac{d_1 - d_2}{2}, \tag{A2}$$

$$a_H \to \frac{d_1 + d_2}{2}, \quad a_V \to \frac{d_3 - d_4}{2}, \tag{A3}$$

where a_H, a_V are the modes of ρ_A and b_H, b_V are the modes of ρ_B. The positive-operator valued measure (POVM) elements of threshold detectors are given by

$$\Pi^{(0)} := \sum_{i=0}^{\infty} (1-\eta_D)^i \left|i\right\rangle \left\langle i\right|, \Pi^{(1)} := \sum_{i=0}^{\infty} (1-(1-\eta_D)^i) \left|i\right\rangle \left\langle i\right|. \tag{A4}$$

The success probability of a BSM is given by

$$P_{\mathrm{BSM}}(n_a, n_b) := \frac{1}{4} \sum_{i_1 i_2 i_3 i_4 \in \mathcal{A}} \sum_{\phi \in \mathcal{B}} G_{i_1 i_2 i_3 i_4}(\phi^{\otimes n_a}, \phi^{\otimes n_b}), \tag{A5}$$

where $\mathcal{A} = \{1234, 1243, 2134, 2143\}$ is the set containing the combinations of two-fold detection leading to a successful entanglement swapping and $\mathcal{B} = \{\left|HH\right\rangle \left\langle HH\right|, \left|VV\right\rangle \left\langle VV\right|\}$ is a set containing the quantum states produced by the two sources of Alice and Bob when they choose the computational basis. The set $\mathcal{B}$ does not contain the cross-terms like $\sigma := \left|HH\right\rangle \left\langle VV\right|$ because $G_{i_1 i_2 i_3 i_4}(\sigma^{\otimes n_a}, \sigma^{\otimes n_b}) = 0$. Due to the symmetries of the map $\mathcal{E}$ we find that the function G is equal for all combinations of indices in $\mathcal{A}$ and quantum states in $\mathcal{B}$, and therefore

$$P_{\mathrm{BSM}}(n_a, n_b) = \frac{4 \cdot 2}{4} G_{1234}(\left|HH\right\rangle\left\langle HH\right|^{\otimes n_a}, \left|HH\right\rangle\left\langle HH\right|^{\otimes n_b}). \tag{A6}$$

We use the fact that $\left|HH\right\rangle := a_H^\dagger b_H^\dagger \left|0\right\rangle$ and, using the definition of $\mathcal{E}$, it is straightforward but lengthly to calculate G and finally to find the result in Eq. (14).

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[3] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

[4] N. Sangouard, Nat. Photon. **6**, 722 (2012).

[5] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[6] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[7] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, Phys. Rev. Lett. **92**, 047904 (2004).

[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).

[9] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).

[10] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, arXiv:1204.0738 [quant-ph].

[11] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[12] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).

[13] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).

[14] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).

[15] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007, (2013).

[16] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, Phys. Rev. A **86**, 022332 (2012).

[17] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).

[18] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, arXiv:1307.1081 [quant-ph].

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

[20] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[21] C. Bennett, G. Brassard *et al.*, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175 (Bangalore, India, 1984).

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

[23] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).

[24] H. K. Lo, H. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).

[25] H. Weinfurter, Europhys. Lett. **25**, 559 (1994).

[26] J. C. V. Minář, H. de Riedmatten, and N. Sangouard, Phys. Rev. A **85**, 032313 (2012).

[27] J. Calsamiglia and N. Lütkenhaus, Appl. Phys. B **72**, 67 (2001).

[28] P. Kok and B. W. Lovett, *Introduction to Optical Quantum Information Processing* (Cambridge University Press, Cambridge, 2010).

[29] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, Phys. Rev. Lett. **98**, 060502 (2007).

[30] N. K. Bernardes, L. Praxmeyer, and P. van Loock, Phys. Rev. A **83**, 012323 (2011).

[31] M. E. Abramowitz *et al.*, *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*, Vol. 55 (Courier Dover, Washington DC, 1964).

[32] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Phys. Rev. A **87**, 052315 (2013).

[33] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup, and R. J. Young, Eur. Phys. J. D **58**, 1 (2010).

[34] M. Jofre, A. Gardelein, G. Anzolin, G. Molina-Terriza, J. P. Torres, M. W. Mitchell, and V. Pruneri, J. Lightwave Technol. **28**, 2572 (2010).

[35] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[36] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, arXiv:1309.3406 [quant-ph].