Article:
Piparo, NL, Razavi, M and Panayi, C (2015) Measurement-device-independent quantum key distribution with ensemble-based memories. IEEE Journal of Selected Topics in Quantum Electronics, 21 (3). 6601010. - . ISSN 1077-260X

https://doi.org/10.1109/JSTQE.2014.2377651

Measurement-device-independent quantum key distribution with ensemble-based memories

Nicoló Lo Piparo,[1] Mohsen Razavi,[1] and Christiana Panayi[1]

[1]*School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK*

Abstract

Quantum memories are enabling devices for extending the reach of quantum key distribution (QKD) systems. The required specifications for memories are, however, often considered too demanding for available technologies. One can change this mindset by introducing memory-assisted measurement-device-independent QKD (MDI-QKD), which imposes less stringent conditions on the memory modules. It has been shown that, in the case of *fast* single-qubit memories, we can reach rates and distances not attainable by single no-memory QKD links. Single-qubit memories, such as single atoms or ions, have, currently, too slow of an access time to offer an advantage in practice. Here, we relax that assumption, and consider ensemble-based memories, which satisfy the main two requirements of having short access times and large storage-bandwidth products. Our results, however, suggest that the multiple-excitation effects in such memories can be so detrimental that they may wash away the scaling improvement offered by memory-equipped systems. We then propose an alternative setup that can in principle remedy the above problem. As a prelude to our main problem, we also obtain secret key generation rates for MDI-QKD systems that rely on imperfect single-photon sources with nonzero probabilities of emitting two photons.

I. INTRODUCTION

Future quantum communication networks may well rely on quantum repeater links for distributing entanglement between different nodes. Such entangled states can then be used for various applications including quantum key distribution (QKD). While progress toward building repeater systems is underway, one can think of intermediary steps that can be implemented in a nearer future. On the one hand, they ease the way for future generations of quantum networks [1, 2], and, on the other, they offer services over a range of distances not currently available by conventional direct QKD links. Memory-assisted measurement-device-independent QKD (MDI-QKD) has recently been proposed with the above objectives in mind [3, 4]. Such systems will resemble a single-node quantum repeater link with quantum memories (QMs) in the middle node. There is, however, no QMs at the users' ends and they are only equipped with encoder/source modules. Instead of distributing entanglement over elementary links, users send BB84-encoded states toward the memories, and once both memories are loaded with relevant states, an entanglement swapping operation is performed on the memories. In a recent work [4], it has been shown that if one uses fast memories with large storage-bandwidth products, it would be possible to beat existing no-memory QKD systems in a practical range of interest using memories mostly attainable with current technologies. Among different developing technologies for QMs, ensemble-based memories have a good chance to satisfy both required conditions. Writing times as short as 300 ps and bandwidths on the order of GHz have been reported for such memories [5, 6]. They are however inflicted by multiple-excitation effects, which may cause errors in QKD setups relying on such QMs. Here, we show how sensitive the performance of memory-assisted MDI-QKD can be to this type of errors and propose a modified setup resilient to multiple-excitation effects.

MDI-QKD offers a key exchange approach resilient to detector attacks [7]. In this system, Alice and Bob send their encoded signals to a middle station, at which a Bell-state measurement (BSM) is performed. This BSM effectively performs an entanglement swapping operation, similar to that of quantum repeaters, on the incoming photons, based on whose result Alice and Bob can infer certain correlations between their transmitted bits. Because of relying on the reverse-EPR protocol [8], the middle party does not need to be trusted, nor does he need to perform a perfect BSM. In the memory-assisted MDI-QKD, we

add two QMs before the middle BSM module; see Fig. 1(a). The objective is to obtain a better rate-versus-distance behavior as now the two photons sent by Alice and Bob do not need to arrive at the BSM module in the same round. This way, we expect to get the same improvement as in single-node quantum repeaters.

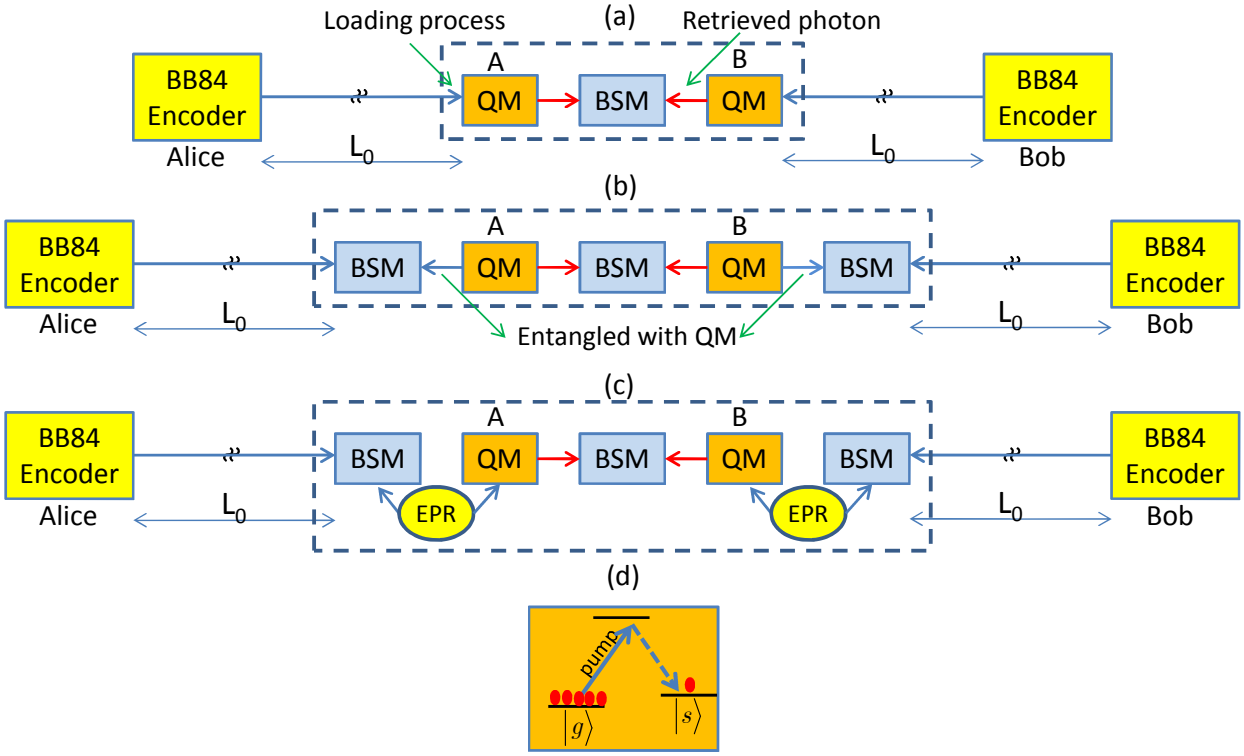

FIG. 1. Different setups for memory-assisted MDI-QKD. (a) MDI-QKD with directly heralding quantum memories [4]. (b) MDI-QKD with indirectly heralding quantum memories [4]. At each round, an entangling process is applied to each QM, generating a photon entangled with the QM. These photons interfere at the side BSM modules next to the QMs with incoming pulses from the encoders. (c) Similar to (b), but the entanglement between the QM and a photon is achieved by generating a pair of entangled photons by the EPR source, and storing one of the photons in the QM. (d) A possible energy-level configuration for an ensemble-based QM suitable for phase encoding.

The required specifications for the QMs in Fig. 1 can be milder than that of a quantum repeater [4]. In a single-node quantum repeater, with two legs of length L_0 and one BSM module in the middle, we have to distribute entanglement between memories in each leg before being able to perform the BSM. For single-mode memories, the entanglement distri-

bution scheme can only be applied once every $T_0 = L_0/c$, where c is the speed of light in the channel [9]. The required coherence time for the QMs is then proportional to T_0 as well. In the memory-assisted MDI-QKD of Fig. 1(a), the repetition rate is dictated by the writing time into QMs. If, therefore, a *heralding* mechanism is available, and if the QMs have short access times, we can run the MDI-QKD protocol faster than that of a quantum repeater, and, correspondingly, the required coherence time could also be lower [4].

The required heralding mechanism, by which we can tell if the QMs have been loaded with the corresponding state to that sent by the users, can be implemented in several ways. In Fig. 1(a), we rely on a direct heralding mechanism in which we attempt to store the transmitted photons into the memories and non-destructively verify whether the writing procedure has been successful. This mechanism is only applicable to a limited number of QMs, such as trapped single atoms/ions, and it is often very slow [10]. In [4], the authors have analyzed an indirect heralding mechanism as in Fig. 1(b) in the single-excitation regime, that is, when QMs can only store a qubit. In this scheme, a photon is first entangled with the QM, and then immediately a side BSM is performed on this photon and the signal sent by the user. A successful side BSM, declared by two detector clicks, ideally teleports the user's state onto the QM and heralds a successful loading event. In order to outperform no-QM QKD systems, the setup of Fig. 1(b) must be equipped with memories with large storage-bandwidth products as well as short access and entangling times. It turns out that the state of the art for single-qubit memories, e.g., single atoms [11] or ions [10], is not yet sufficiently advanced to meet the requirements of practical memory-assisted protocols. In particular, we need faster memories for the practical ranges of interest.

Here we extend the analysis in [4] to the case of *ensemble-based* memories, which often offer very large bandwidths, or, equivalently, very short access times, suitable for the memory-assisted scheme. Such memories, however, suffer from multiple-excitation effects, which we carefully look into in this paper. In fact, when multiple-excitations are present, a seemingly successful side BSM may have been resulted from two photons originating from the QM in Fig. 1(b), in which case the final measurement results have no correlation with the transmitted signal by the user. Our results show that such effects can be so detrimental that we cannot beat no-memory QKD systems within practical ranges of interest. We then look at an alternative indirect heralding mechanism, see Fig. 1(c), and show that, in principle, we can avoid multiple-excitation errors if a proper entangled-photon (EPR) source is

used [12].

The rest of this paper is organized as follows. As the first step toward the analysis of the MDI-QKD system of Fig. 1(b) with non-qubit memories, in Sec. II, we study a no-QM MDI-QKD link that uses imperfect sources, that is, the ones which have a nonzero probability for generating more than one photon. This is a good approximation to the state of the field entangled with an ensemble-based QM. We then extend our results, in Sec. III, to the memory-assisted system in Fig. 1(b) and study the system performance in the presence of multiple excitations in the QMs. We then propose a modified setup that can handle multiple-excitation errors. We conclude the paper in Sec. IV commenting on the practicality of each scheme.

II. MDI-QKD WITH IMPERFECT SOURCES

Regardless of the type of material used, an ensemble-based memory can be modeled as a non-interacting ensemble of quantum systems. Here, for simplicity, but without loss of generality, we assume our QM is an ensemble of neutral atoms with the Λ-level configuration shown in Fig. 1(d). One possible way to entangle a photon with such a QM is to pump all the atoms in the ensemble to be initially in their ground states $|g\rangle$; we then excite the ensemble by a short pulse in such a way that the probability, p, of driving an off-resonant Raman transition in the ensemble is kept well below one. In that case, the joint state of the released Raman optical field and the ensemble follows that of a two-mode squeezed state given by [13]

$$|\psi\rangle_{AP} = \sum_{n=0}^{\#\text{atoms}} \sqrt{(1-p)p^n}|n\rangle_A|n\rangle_P, \tag{1}$$

where $|n\rangle_P$ is the Fock state for n photons and $|n\rangle_A$ is the symmetric collective state to have n atoms in their $|s\rangle$ states; see Fig. 1(d). Assuming $p \ll 1$, we can truncate the above state at $n = 2$ without losing much accuracy. Furthermore, assuming that there is a post-selection mechanism by which the state $|0\rangle_A|0\rangle_P$ is selected out, the effective state for the photonic system P is given by

$$\rho_P(p) = (1-p)|1\rangle_{PP}\langle 1| + p|2\rangle_{PP}\langle 2|, \tag{2}$$

which resembles an imperfect single-photon source with a nonzero probability p for emitting two photons. This is the type of state that one would get for the photons entangled with

the QMs in Fig. 1(b). That is, each leg of the system, can be modeled as an asymmetric MDI-QKD link, where the source on one side generates photons in the form of (2). The source on the user's end could be the same, or one may use decoy coherent states for practical purposes. The latter case will be investigated in a separate publication [14]. Note that the type of states as in (1) do not represent maximally entangled states. One can, however, combine two such states and obtain an effective entangled states after post-selection [15].

In this section, we study an MDI-QKD link with imperfect sources as in (2). Although we digress a bit from the main problem, it gives us some insight into the analysis of the setup in Fig. 1(b), and, more generally, when MDI-QKD links are connected to quantum repeater setups [14]. The type of memory considered here best fits into phase-encoded QKD setups as we will consider next [16].

A. Phase-encoded MDI-QKD

In this section we describe phase-encoded MDI-QKD as proposed in [16]. For the sake of convenience, we analyze the dual-rail setup in Fig. 2, but, for practical purposes, it is possible to implement the same scheme via time multiplexing, by using only one physical channel [16]. Here, states sent by Alice and Bob are encoded either in the z or the x basis. Encoding the states in the z basis is achieved by sending horizontally or vertically polarized pulses to a polarizing beam splitter (PBS) to, respectively, generate a signal in the r or in the s mode (corresponding to bits 0 or 1) in Fig. 2. To implement the x-basis encoding, +45-polarized pulses are prepared at the source and two relative phases, $\{0, \pi\}$ corresponding to bits $\{0, 1\}$, are used at the phase modulator. In this case, the PBS splits the signal into r and s modes, and photons will be in a superposition of these modes.

The procedure to establish a secret key is as follows. Alice and Bob, who are separated by a distance $L = L_A + L_B$, choose randomly a basis from $\{x, z\}$ and a bit from $\{0, 1\}$ and send a pulse to a middle site, where a BSM is performed by an untrusted party, Charlie. We make photons indistinguishable through the filters represented by empty boxes in Fig. 2. A click in exactly one of the r detectors, in Fig. 2, and exactly one of the s detectors will correspond to a successful event. When the users both choose the z basis, a successful event corresponds to complementary bits on the two ends. When they both choose the x basis, instead, a different bit assignment will follow. If they pick the same phase then the state

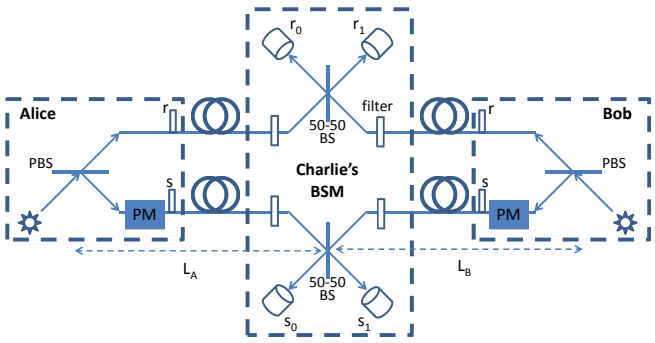

FIG. 2. Schematic diagram for the MDI-QKD protocol with phase encoding [16]. Here BS stands for beam splitter, PBS for polarizing BS, and PM for phase modulator.

will be correlated and r_0 and s_0 or r_1 and s_1 will ideally click. We will refer to this detection event as type I. If they pick different phase values then the state will be anti-correlated and r_0 and s_1 or r_1 and s_0 will ideally click. The latter pattern of clicks is referred to as type II. In either case, Charlie announces her BSM results to Alice and Bob. Alice and Bob will compare the bases used for all transmissions. They keep the results if they have chosen the same basis and discard the rest.

B. Key rate analysis

In this section, the secret key generation rate for the MDI-QKD scheme of Fig. 2 is calculated. Here, we assume that Alice and Bob each have an imperfect single-photon source that can emit two photons with probability $p \ll 1$ as in (2); hence, in our following analysis, we neglect $O\left(p^2\right)$ terms corresponding to the simultaneous emission of two photons by both sources. We assume Alice and Bob are located at, respectively, distances L_A and L_B from the BSM module, and the total path loss for a channel with length l is given by $\eta_{\rm ch}(l) = \exp\left(-l/L_{\rm att}\right)$, with $L_{\rm att} = 25$ km for an optical fiber channel. The secret key generation rate is then lower bounded by [16, 17]

$$R_{ss} \geq Q_{11}^z \left(1 - h\left(e_{11}^x\right)\right) - Q_{pp}^z f\, h\left(E_{pp}^z\right), \tag{3}$$

where $Q_{11}^z = (1-p)^2 Y_{11}^z$, with Y_{11}^z being the probability of a successful click pattern, in the z basis, when Alice and Bob send exactly one photon each; e_{11}^x is the quantum bit error rate (QBER), in the x basis, when Alice and Bob send exactly one photon each; Q_{pp}^z and E_{pp}^z are, respectively, the gain and the QBER, in the z basis, when Alice and Bob send the states as

in (2); f is the error correction inefficiency; and, $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the Shannon's binary entropy function. In (3), we have assumed that the efficient QKD protocol is used, in which the z basis is used much more often than the x basis [18].

In Appendix A, we derive each term in (3) under the normal mode of operation when no eavesdropper is present. This will simulate the parties' estimate of relevant parameters in the limit of infinitely long keys. We consider the dark count noise of photodetectors and possible misalignment errors in the setup. The latter will model our deviation from the indistinguishibility condition required for the BSM operation. The key tool in calculating the key rate parameters in (3) is an asymmetric butterfly operation as shown in Fig. 3. By modeling the path loss in each channel as well as photodetector efficiencies, η_d, by fictitious beam splitters, each (upper or lower) arm in Fig. 2 can be modeled as in Fig. 3(a), in which the photodetectors have unity quantum efficiencies. This can be simplified to the butterfly module in Fig. 3(b), where $\eta_a = \eta_{\rm ch}(L_A)\eta_d$ and $\eta_b = \eta_{\rm ch}(L_B)\eta_d$. In Appendix A, we find the input-output relationship for all relevant input states to a general butterfly module, from which the joint state of photons sent by Alice and Bob right before photodetection can be calculated. By applying proper measurement operators on this state, we find the post-measurement state corresponding to each of the relevant click patterns. For instance, a click on the non-resolving detector r_0, and no click on r_1, can be modeled by the following measurement operator [19]

$$M_{r_0} = (1-d_c)\left[(I_{r_0} - |0\rangle_{r_0r_0}\langle 0|)\otimes|0\rangle_{r_1r_1}\langle 0| + d_c|0\rangle_{r_0r_0}\langle 0|\otimes|0\rangle_{r_1r_1}\langle 0|\right], \tag{4}$$

where I_{r_0} denotes the identity operator for the mode entering the r_0 detector, and d_c is the dark-count rate per gate width per detector. The measurement operator for the event that only detectors r_0 and s_0 click would then be given by $M_{r_0}\otimes M_{s_0}$, and similarly for other combinations.

Figure 4 shows the secret key generation rate per transmitted pulse for the setup of Fig. 2 versus the double-photon probability. We have used a nominal set of values, listed in Table I, for all relevant parameters. The near-ideal nominal values for quantum efficiency and dark count have been achieved in [20]. We have considered two scenarios. The first is a symmetric setup, when the BSM module is located in the middle of the link, i.e., $L_A = L_B$. The other scenario is for when the BSM module is next to the Bob's apparatus, similar to the situation that we have in the side-BSM of Fig. 1(b). In both cases, there seems to be

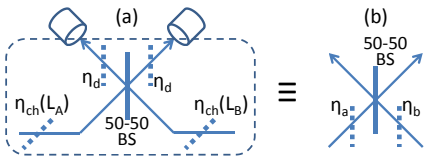

FIG. 3. (a) The simplified module for the upper or lower arms in the setup of Fig. 2. (b) An asymmetric butterfly module with parameters η_a and η_b.

Quantum efficiency, η_d	0.93
Memory reading efficiency, η_{r0}	0.87
Dark count per pulse, d_c	10^{-9}
Attenuation length, L_{att}	25 km
Misalignment, e_d	0

TABLE I. Nominal values used in our numerical results

little effect on the key rate as a result of introducing double-photons. The key reason for this behavior is the fact that the only error term in (3) that depends on p is E^z_{pp}. An error in the z basis arises from the cases where Alice and Bob are both sending the same bits, let's say both send a signal in their respective r modes, but one r detector and one s detector clicks in Fig. 2. The click on the s detectors should then be because of dark counts and is not affected by the double photon states in the r modes. Double photons slightly change the rate, as we disregard double-click cases, and that is the reason for lower key rates once p increases.

III. MDI-QKD WITH ENSEMBLE-BASED MEMORIES

In this section, we analyze the effect of multiple excitations in (1) on the key rate of the memory-assisted MDI-QKD link of Fig. 1(b). We again use the phase-encoding scheme described in Sec. II A and combine it with four ensemble-based memories as described below. In contrast to the previous section, where double-photon terms had little effect on system performance, it turns out that, within the setup of Fig. 1(b), multiple excitations in memories would adversely affect the achievable key rate. We then look at the scheme of Fig. 1(c) and show, how, in principle, we can remedy this problem.

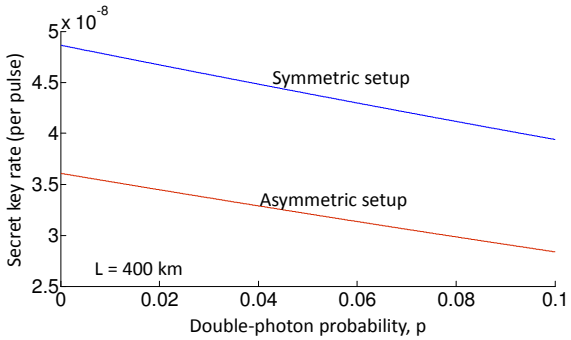

FIG. 4. Secret key generation rate per transmitted pulse versus the double-photon probability, p. In all curves $L = 400$ km and all other parameters are taken from Table I. In the symmetric case, $L_A = L_B$, whereas in the asymmetric case, $L_A = L$ and $L_B = 0$.

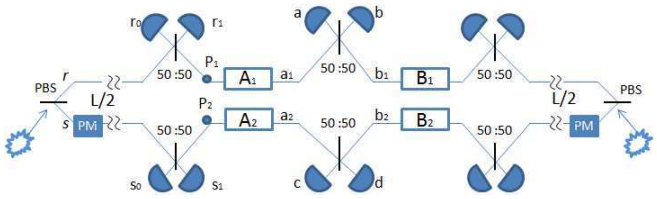

FIG. 5. Schematic diagram for the MDI-QKD setup with ensemble-based memories, represented by A_1, A_2, B_1, and B_2.

A. Setup description

Figure 5 shows the phase-encoding variant of the memory-assisted MDI-QKD system of Fig. 1(b). Here, in order to focus on the memory effects, we assume Alice and Bob are using perfect single-photon sources. For each photon encoded and sent by the users, we pump the corresponding memories A_1, A_2, B_1, and B_2 in order to generate a joint photonic-atomic state as in (1). The state sent by the user is indirectly loaded to the memories by the side-BSM modules in Fig. 5. For instance, on the Alice side, we perform a BSM on the single-photon state sent by Alice and P_1 and P_2 states using the same BSM module as in Fig. 2. A successful side BSM, with the same definition for success as in Sec. II A, would ideally load the memory with a state corresponding to what the users have sent. For instance, if Alice uses the z basis, and sends a signal in the r mode, a successful BSM on her side, would imply that the memories A_1-A_2 are ideally in the $|01\rangle_{A_1A_2}$ state. Of course, considering the dark current and double-photon terms, we will deviate from this ideal case,

Basis	Alice BSM	Bob BSM	Middle BSM	Bit assignment
z	type I/II	type I/II	type I/II	Bob flips his bit
x	type I (II)	type I (II)	type I	Bob keeps his bit
x	type I (II)	type I (II)	type II	Bob flips his bit
x	type I (II)	type II (I)	type I	Bob flips his bit
x	type I (II)	type II (I)	type II	Bob keeps his bit

TABLE II. Bit assignment protocol as a function of the results of the three BSMs in Fig. 5. Here, Alice (Bob) BSM refers to the side BSM on the left (right).

and that is what we are going to study in this paper. Alice and Bob attempt repeatedly to load their memories until they succeed, at which point they wait for the other party to complete this task. Once both sets of memories are loaded, we read out all four memories and proceed with the middle BSM. Once the results of all three BSMs as well as the bases used are communicated to users, Alice and Bob can distill with a sifted key bit. Table II shows what bits Alice and Bob assign to their sifted keys depending on the results of the three BSM operations.

B. Key rate analysis

In this section, the key rate for the setup of Fig. 5 is obtained under the normal operation condition when no eavesdropper is present. Using the efficient QKD protocol, where the z basis is used more often than the x basis, the secret key rate per transmitted pulse is lower bounded by

$$R_{\mathrm{QM}} \geq Y_{11}^{\mathrm{QM}} \left[1 - h\left(e_{11;x}^{\mathrm{QM}}\right) - h\left(e_{11;z}^{\mathrm{QM}}\right)\right], \tag{5}$$

where $e_{11;x}^{\mathrm{QM}}$ and $e_{11;z}^{\mathrm{QM}}$, respectively, represent the QBER between Alice and Bob in the x and z basis, when single photons are sent, and Y_{11}^{QM} represents the probability that, in the z basis, both sets of memories A and B are loaded *and* the middle BSM is successful. In Appendix B, we derive all above terms assuming that memories may undergo amplitude decay according to an exponential law. That is, if the recall/reading efficiency, right after a successful writing procedure, is denoted by η_{r0}, the reading efficiency after a time t is given by $\eta_r(t) = \eta_{r0}\exp(-t/T_1)$, where T_1 is the amplitude decay time constant.

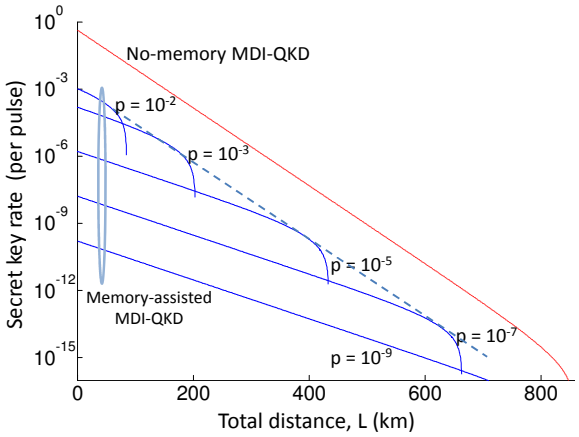

FIG. 6. Secret key generation rate per transmitted pulse versus distance for the MDI-QKD scheme in Fig. 5 with QMs (blue curves) and that of Fig. 2 without QMs (red curves) for different values of the excitation probability p. Nominal values are used as in Table I with $T_1 = \infty$. For the no-memory curve, $L_A = L_B$ and $p = 0$.

In the absence of dark counts, memory decay, and source imperfections, the major source of noise in the setup of Fig. 5 is the multiple-excitation terms in (1). Even if the users send exactly one photon, the state loaded to the QMs may contain more than one excitation overall. These additional excited atoms will cause errors in the middle BSM setup. The errors in the latter stage are partly similar to what we studied in the previous section, when we considered imperfect single-photon sources. These cases correspond to loading states like $|20\rangle_{A_1A_2}$ into A_1-A_2 memories, or similar states for B_1-B_2. There are, however, other terms that must be considered, such as $|11\rangle_{A_1A_2}$, and they turn out to give a much larger contribution to the noise terms in (5). Our analysis in this section, considers up to two excitations in each memory module.

Figure 6 shows the effect of multiple excitations in the scheme of Fig. 5 and compares it with a symmetric no-memory setup as in Fig. 2. Assuming no decay or misalignment in the setup and with a negligible amount of dark count as in Table I, Fig. 6 shows that the memory-assisted system of Fig. 5 cannot outperform the no-memory system within a reasonable range of rates and/or distances. Here, we have considered different values of p. As we decrease the value of p, the chance of entangling a photon with the memories becomes lower, and that is why the initial key generation rate drops. However, lower values of p will make the generation of multiple-excitation states less likely and that is why the

cut-off security distance becomes longer. The rate, however, remains below the no-QM curve even for very small values of p.

In order to understand the above behavior, we need to look more closely at the dynamics of different terms in (5). The term $Y_{11}^{\rm QM}$ is proportional to the loading probability, i.e., the success probability in each of the side BSMs of Fig. 5. In order to have a successful BSM we need to get two clicks, one on the upper arm, and one in the lower one. For short distances, the two clicks are typically caused by the photon sent by the user and a photon entangled with the two memories on each side. The loading probability, in this limit, is then on the order of $p\exp[-(L/2)/L_{\rm att}]$, where p is the probability that one of the two ensembles on each side has one excitation, and $\exp[-(L/2)/L_{\rm att}]$ is the channel efficiency for the transmitted photon by the user. The initial slope of the curves in Fig. 6 corresponds to the above scaling with distance, similar to that of quantum repeaters. As the distance becomes longer and longer, the chance of receiving the photon sent by the user becomes slimmer and slimmer. In this limit, a successful BSM is often caused by photons originating from memories, in particular, terms like $|11\rangle_{A_1A_2}|11\rangle_{P_1P_2}$. Such successful BSMs do not imply any correlations between the states of memories and that of Alice or Bob, and will simply result in random errors and the eventual decline of the key rate to zero. Given that the probability of generating a two-photon state is on the order of p^2, the transition from the first region to the cut-off region roughly occurs at a distance L_c, where $p\exp[-(L_c/2)/L_{\rm att}]\approx p^2$, or equivalently, when $\exp[-(L_c/2)/L_{\rm att}]\approx p$. This implies that the total rate would then scale as $p\exp[-(L_c/2)/L_{\rm att}]\approx\exp[-L_c/L_{\rm att}]$, which is similar to a no-QM system. This is evident in Fig. 6 by the envelop (dashed line) of QM-assisted curves, which is parallel to the no-QM curve. Considering the additional inefficiencies in the memory-assisted system as compared to the no-QM one, for the range of values used in our calculations, it becomes practically impossible to beat the no-QM system if we use ensemble-based memories in the setup of Fig. 5. Note that the performance would further degrade if memory decay effects are also included.

C. Modified Setup

The results of the previous subsection imply that ensemble-based memories barely offer any advantages over no-QM systems within the setup of Fig. 5. The key reason is the

generation of multiple excitation terms in the memory once a photonic state is entangled with it via driving off-resonant Raman transitions. In the scheme of Fig. 1(b), we use the entanglement between the memory and the photon to effectively *teleport*, via the side BSM, the user's state onto the memories. This task can be done in a different way as shown in Fig. 1(c). In this setup, we use an EPR source to generate entangled photons. If we store one of the photons into the memory, we would have effectively achieved the same required entanglement between the memory and the other photon in the EPR pair, and the rest of the protocol can proceed as before. Note that this scheme is not fully heralding, because we cannot tell if the photon has actually been stored in the QM, but considering that entangled photons are generated locally, the required writing procedure can be very efficient [21].

The main advantage that the setup of Fig. 1(c) offers is its in-principle resilience to multi-photon terms. If the employed EPR sources do not include multi-photon terms, we only generate at most one excited atom in the respective ensembles. That implies that once we read the memories, there will only be one photon from each side and we will not deal with the types of errors that exist in the setup of Fig. 5.

Another advantage of the setup of Fig. 1(c) is that we are not, in this setup, restricted by the writing time of the memories. The writing time specifies the repetition rate for the setup of Figs. 1(b) and 5. If we need to repeatedly write into a memory, the writing time will be restricted by the time it takes for possible cooling operations or when we need to pump the QM to a special initial state. This will in essence reduce the key generation rate per unit of time. In Fig. 1(c), we can avoid sequential writing into the QMs if we use a delay line and a fast optical switch for the photon that must be stored into the memory. We will only attempt to write into the memory once there is a successful side BSM. In this way, the overhead time for preparing the memory will become almost irrelevant, and the repetition rate is determined by the EPR source entanglement generation rate. Note that the delay time required in the above scheme is typically much shorter than the required storage time in the memory. One can, however, study the system performance when an optical memory (delay line), rather than a QM, is in use. Alternatively, one may drive a large number of these fully optical systems to asymptotically get the same rate improvement as obtained here [22]. In either case, a single memory-assisted system is expected to outperform a single all-optical system over a certain range.

The choice of the EPR source is very important in the scheme of Fig 1(c). In particular,

it is important to note that the existing sources of entangled photons based on parametric down-conversion are not suitable for this scheme. In fact, they have exactly the same multi-photon statistics as given by (1) for the number of photons in their idler and signal beams [23], hence would give the same kind of performance as in Fig. 6. Quantum-dot based sources, on the other hand, offer high generation rates of entangled states with negligible two-photon components [24, 25]. They need, nevertheless, to improve their fidelity of generated entangled photons [26]. The performance of MDI-QKD systems relying on such imperfect sources will be investigated in a separate publication.

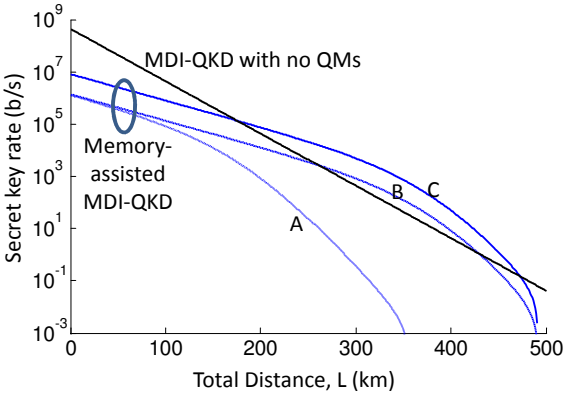

FIG. 7. Secret key generation rate for the scheme in Fig. 1(c) using ensemble-based QMs. Ideal EPR sources with 12% efficiency are used. Curve A assumes $T_1 = T_2 = 1.5$ μs, where T_2 is the dephasing time constant, and the initial retrieval efficiency is $\eta_{r0} = 0.3$; curve B assumes $T_1 = T_2 = 150$ μs and $\eta_{r0} = 0.3$; and curve C assumes $T_1 = T_2 = 150$ μs and $\eta_{r0} = 0.73$. In all curves, reading and writing times are 300 ps, the repetition rate is 1 GHz, channel loss is 0.2 dB/km, and detector parameters are as in Table I.

In this section, we use the results reported in [4] to find the key rate for the setup of Fig. 1(c) assuming that the EPR source generates a maximally entangled state. Figure 7 shows the achievable key rates for the scheme of Fig. 1(c), when it is driven by an EPR source with 12% efficiency [25]. We have neglected the double-photon emissions and have assumed that each generated photon can be loaded into the memory with unity efficiency. In Fig. 7, curve A is based on realistic parameter values as reported in [5]. The achievable key rate can clearly not beat the no-QM system. By improving the coherence time of the QMs by two orders of magnitude, as in curve B, we can now outperform the no-memory system over a certain range. This range becomes wider and more practical, as shown in curve C, if our

initial retrieval efficiency is increased from 0.3 to 0.73. Both required improvements in curve C are potentially achievable within our current technology as they have been obtained in other similar setups [27] for cold atomic ensembles. This promises an imminent exploitation of QMs in real systems with clear advantages over no-memory systems.

IV. CONCLUSION

In this paper, we provided a full analysis of the MDI-QKD systems that use ensemble-based memories. Memory-assisted MDI-QKD is expected to beat conventional no-memory QKD links in rate and distance. This is to be achieved without requiring much demanding technology for quantum memories, which hinders the progress of quantum repeaters. In memory-assisted MDI-QKD, memories are required to be fast and to demonstrate sufficiently long coherence times as compared to their access times. Both these conditions have been met for certain memories that rely on atomic ensembles or atomic frequency combs. In both cases, the memories, when driven by coherent pulses, suffer from multiple excitation effects. In this paper, we showed that these multiple excitations deteriorate the performance of certain memory-assisted MDI-QKD systems to the extent that they could no longer beat their no-memory counterparts. We showed that in order to revive the promised advantage of beating no-memory systems, using ensemble-based memories, one needed to be equipped with almost ideal entangled-photon sources. In other words, our memory problem would be converted into a source problem. The prospect of developing memory-assisted QKD systems is, nevertheless, still bright. In particular, sources based on quantum dot structures have shown to have very little multi-photon components, and can be run at GHz rates. Further progress in that ground put together with the slight improvements that we need on the memory side would enable us to devise the first generation of memory-assisted systems that offer realistic advantages in practice.

Appendix A: MDI-QKD with imperfect sources

In this Appendix we will derive the terms in (3) for the setup of Fig. 2, considering path loss, quantum efficiency η_d, dark count rates d_c, double-photon probability p, and misalignment probability e_d assuming that no eavesdropper is present. This provides us

with an estimate of how well the system performs under normal conditions. In (3), Y_{11}^z and e_{11}^x have already been calculated in [16]. Here, we will derive the other two terms Q_{pp}^z and E_{pp}^z. In the z basis, a successful click event at the BSM module corresponds to different key bits at Alice's and Bob's ends. We can therefore separate the input states that result in correct inference of bits versus those causing errors. The input states that result in correct inference of bits are those that correspond to sending different bits by Alice and Bob given by

$$\rho_C^{(\text{in})} = [\rho_{r_A}(p) \otimes \rho_{s_B}(p) + \rho_{s_A}(p) \otimes \rho_{r_B}(p)]/2, \tag{A1}$$

whereas

$$\rho_E^{(\text{in})} = [\rho_{r_A}(p) \otimes \rho_{r_B}(p) + \rho_{s_A}(p) \otimes \rho_{s_B}(p)]/2 \tag{A2}$$

results in erroneous decisions. In above equations, $r_{A(B)}$ and $s_{A(B)}$ subscripts, respectively, refer to the r and s optical modes of Alice (Bob) in Fig. 2. Note that terms corresponding to $O\left(p^2\right)$ are neglected in (A1) and (A2). Each of the above states undergoes a state transformation according to the butterfly module in Fig. 3(b). We denote this transformation by B_{η_a,η_b}^{xy}, where x and y refer to the input modes to the module. The input-output relationships for this butterfly operation are given in Table III for a range of input states of interest. The output states in Fig. 3(b), for the input states as in (A1) and (A2), are then given by

$$\rho_K^{(\text{out})} = B_{\eta_a,\eta_b}^{r_A r_B} \otimes B_{\eta_a,\eta_b}^{s_A s_B}(\rho_K^{(\text{in})}), \quad K = C, E, \tag{A3}$$

where $\eta_a = \eta_{\text{ch}}(L_A)\eta_d$ and $\eta_b = \eta_{\text{ch}}(L_B)\eta_d$.

With the above output states in hand, one just needs to apply the relevant measurement operators to find all probabilities of interest. In particular, by denoting the probability that detectors r_i and s_j, $i, j = 0, 1$, click by

$$P_{r_i s_j}^{(K)} = \text{tr}(\rho_K^{(\text{out})} M_{r_i} M_{s_j}), \quad K = C, E, \tag{A4}$$

the probability that an acceptable click pattern occurs in the z basis, Q_{pp}^z, is given by

$$Q_{pp}^z = Q_C^z + Q_E^z \tag{A5}$$

where

$$Q_K^z = \left(P_{r_0 s_0}^{(K)} + P_{r_1 s_1}^{(K)} + P_{r_0 s_1}^{(K)} + P_{r_1 s_0}^{(K)}\right)/2, \quad K = C, E. \tag{A6}$$

Finally, E_{pp}^z is given by

$$E_{pp}^z = \frac{Q_{EE}^z}{Q_{pp}^z} \tag{A7}$$

ρ_{AB}	$B^{AB}_{\eta_a,\eta_b}(\rho_{AB})$
$\|10\rangle\langle 10\|$	$\frac{\eta_a}{2}\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_a)\|00\rangle\langle 00\|$
$\|01\rangle\langle 01\|$	$\frac{\eta_b}{2}\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_b)\|00\rangle\langle 00\|$
$\|11\rangle\langle 11\|$	$\frac{1}{2}\left(\eta_a+\eta_b-2\eta_a\eta_b\right)\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_a)(1-\eta_b)\|00\rangle\langle 00\| + \frac{\eta_a\eta_b}{2}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$
$\|20\rangle\langle 20\|$	$\eta_a(1-\eta_a)\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_a)^2\|00\rangle\langle 00\| + \frac{\eta_a^2}{4}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$
$\|02\rangle\langle 02\|$	$\eta_b(1-\eta_b)\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_b)^2\|00\rangle\langle 00\| + \frac{\eta_b^2}{4}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$
$\|21\rangle\langle 21\|$	$\eta_c(1-\eta_a)\left[\eta_a(1-\eta_b)+\frac{\eta_b}{2}(1-\eta_a)\right]\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_a)^2(1-\eta_b)\|00\rangle\langle 00\|$ $+\eta_a\left[\frac{\eta_a}{4}(1-\eta_b)+\eta_b(1-\eta_a)\right]\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right) + \frac{3}{8}\eta_a^2\eta_b\left(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|\right)$
$\|12\rangle\langle 12\|$	$(1-\eta_b)\left[\eta_b(1-\eta_a)+\frac{\eta_a}{2}(1-\eta_b)\right]\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_b)^2(1-\eta_a)\|00\rangle\langle 00\|$ $+\eta_b\left[\frac{\eta_b}{4}(1-\eta_a)+\eta_a(1-\eta_b)\right]\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right) + \frac{3}{8}\eta_a\eta_b^2\left(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|\right)$
$\|10\rangle\langle 01\|$	$\frac{1}{2}\sqrt{\eta_a\eta_b}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right)$
$\|01\rangle\langle 10\|$	$\frac{1}{2}\sqrt{\eta_a\eta_b}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right)$
$\|11\rangle\langle 20\|$	$(1-\eta_a)\sqrt{\frac{\eta_a\eta_b}{2}}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right) + \frac{\eta_a\sqrt{\eta_a\eta_b}}{2\sqrt{2}}\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|11\rangle\langle 02\|$	$(1-\eta_a\eta_c)\sqrt{\frac{\eta_a\eta_b}{2}}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right) + \frac{\eta_a\sqrt{\eta_a\eta_b}}{2\sqrt{2}}\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|20\rangle\langle 11\|$	$(1-\eta_a)\sqrt{\frac{\eta_a\eta_b}{2}}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right) + \frac{\eta_a\sqrt{\eta_a\eta_b}}{2\sqrt{2}}\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|02\rangle\langle 11\|$	$(1-\eta_a)\sqrt{\frac{\eta_a\eta_b}{2}}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right) + \frac{\eta_a\sqrt{\eta_a\eta_b}}{2\sqrt{2}}\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|20\rangle\langle 02\|$	$\frac{\eta_a\eta_b}{4}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$
$\|02\rangle\langle 20\|$	$\frac{\eta_a\eta_b}{4}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$
$\|22\rangle\langle 22\|$	$(1-\eta_a)^2(1-\eta_b)^2\|00\rangle\langle 00\| +$ $(1-\eta_a)(1-\eta_b)\left[\eta_a(1-\eta_b)+\eta_b(1-\eta_a)\right]\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) +$ $\frac{3}{4}\eta_a\eta_b\left[\eta_a(1-\eta_b)+\eta_b(1-\eta_a)\right]\left(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|\right) +$ $\frac{1}{4}\left[\eta_a^2(1-\eta_b)^2+\eta_b^2(1-\eta_a)^2\right]\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right) + \frac{3}{8}\eta_a^2\eta_b^2\left(\|40\rangle\langle 40\| + \|04\rangle\langle 04\|\right)\|$

TABLE III. The input-output relationship for the asymmetric butterfly module of Fig. 3(b). For the sake of brevity, here, we have only included the terms that provide us with nonzero values after applying the measurement operation. More specifically, we have removed all *asymmetric* density matrix terms, such as $|10\rangle\langle 01|$ or $|01\rangle\langle 10|$, for which the bra state is different from the ket state, from the output state.

where $Q^z_{EE} = e_d Q^z_C + (1 - e_d) Q^z_E$.

More generally, for any input state $\rho^{(\text{in})} = \rho_{r_A r_B s_A s_B}$, and for total transmissivities η_A and η_B for, respectively, Alice's and Bob's photons, we can define a gain parameter $Q^\beta(\eta_A, \eta_B; \rho_{r_A r_B s_A s_B})$ to represent the success probability, in basis $\beta = x, z$, for the BSM operation in Fig. 2. For any such input state, the probabilities of getting a click on detectors r_i and s_j, $i, j = 0, 1$, is given by

$$P_{r_i s_j}(\rho^{(\text{in})}) = \text{tr}(\rho^{(\text{out})} M_{r_i} M_{s_j}), \tag{A8}$$

where

$$\rho^{(\text{out})} = B^{r_A r_B}_{\eta_A, \eta_B} \otimes B^{s_A s_B}_{\eta_A, \eta_B}(\rho^{(\text{in})}). \tag{A9}$$

With the above notation, we obtain

$$\begin{aligned} Q^\beta(\eta_A, \eta_B; \rho^{(\text{in})}) = P_{r_0 s_0}(\rho^{(\text{in})}) + P_{r_1 s_1}(\rho^{(\text{in})}) \\ + P_{r_0 s_1}(\rho^{(\text{in})}) + P_{r_1 s_0}(\rho^{(\text{in})}). \end{aligned} \tag{A10}$$

The total gain for the basis $\beta = x, z$ is then given by

$$Q^\beta(\eta_A, \eta_B) = \sum_{\text{all input states } \rho} Q^\beta(\eta_A, \eta_B; \rho) \Pr(\rho) \tag{A11}$$

Similarly, we also define $Q^\beta_C(\eta_A, \eta_B)$ to be the probability to get a successful BSM *and* Alice and Bob end up with correct inference of their bits:

$$Q^\beta_C(\eta_A, \eta_B) = \sum_{\text{all input states } \rho} \sum_{\substack{\text{all correct detection} \\ \text{pairs } (r_i, s_j) \text{ for input } \rho}} P_{r_i s_j}(\rho) \Pr(\rho). \tag{A12}$$

Likewise, $Q^\beta_E(\eta_A, \eta_B) = Q^\beta(\eta_A, \eta_B) - Q^\beta_C(\eta_A, \eta_B)$ denotes the probability to get a successful BSM and Alice and Bob end up with incorrect inference of their bits. Finally, error terms can be defined as $e^\beta Q^\beta = Q^\beta_E$ calculated at the point (η_A, η_B). We use the above relationships in the next Appendix.

Appendix B: MDI-QKD with imperfect memories

In this Appendix we will derive the terms in (5) for the setup of Fig. 5, considering path loss, quantum efficiency η_d, dark count rates d_c, excitation probability p of the memories, and memories' amplitude decay assuming that no eavesdropper is present. We will follow the

same procedure as in Appendix A to separate the terms that result in error versus correct key bits. The general idea is to find the post-measurement density matrix of memories for any relevant input state upon a successful side-BSM event. Once both sets of memories are loaded, we apply the middle BSM operation and find relevant probabilities of interest.

The setup of Fig. 5 can be thought of three asymmetric MDI-QKD setups, where memories link them together. The first and second systems are those that are involved with the loading process. They include the photons entangled with memories, e.g. P_1 and P_2 on Alice side, with those sent by the users. The third one is centered around the middle BSM and the photons retrieved from the memories. Here we use the general notation introduced in (A8)-(A12) to calculate the relevant gain and error parameters. In order to do so, we need to first find the input state for the final stage of BSM. For any input state $\rho_A^{(\text{in})}$ sent by Alice, we can find the post-measurement state $\rho_A^{(\text{pm})}(r_i, s_j; \rho_A^{(\text{in})})$ of the memories A_1 and A_2 upon a click on detectors r_i and s_j, for $i, j = 0, 1$, as follows

$$\rho_A^{(\text{pm})}(r_i, s_j; \rho_A^{(\text{in})}) = \frac{\text{tr}_{P_1,P_2,r_A,s_A}(\rho_A^{(\text{out})} M_{r_i} M_{s_j})}{\text{tr}(\rho_A^{(\text{out})} M_{r_i} M_{s_j})}, \tag{B1}$$

where

$$\rho_A^{(\text{out})} = B_{\eta_a,\eta_d}^{r_A P_1} \otimes B_{\eta_a,\eta_d}^{s_A P_2}(\rho_A^{(\text{in})} \otimes \rho_{A_1 P_1} \rho_{A_2 P_2}), \tag{B2}$$

where $\rho_{A_i P_i} = |\psi\rangle_{A_i P_i}\langle\psi|$, for $i = 1, 2$. Similarly, one can find the post-measurement state for B_1-B_2 memories and denote it by $\rho_B^{(\text{pm})}(r_m, s_n; \rho_B^{(\text{in})})$ once detectors r_m and s_n, for $m, n = 0, 1$, click on the side BSM of Bob. The final parameter we need from the loading stage is the loading probability, i.e., the probability to get a successful side BSM on Alice's ($K = A$) or Bob's ($K = B$) side given by

$$P_K = Q^z(\eta_{\text{ch}}(L_K)\eta_d, \eta_d; |10\rangle_{r_K s_K}\langle 10| \otimes \rho_{P_1} \rho_{P_2}). \tag{B3}$$

In order to apply the middle BSM on the post-measurement states $\rho_A^{(\text{pm})}$ and $\rho_B^{(\text{pm})}$, One must consider the random nature of the loading process. Given that one set of the memories can be loaded earlier than the other, the former will undergo some amplitude decay before being read for the final BSM. That would result in an imbalanced middle BSM, where the reading efficiency for one memory could be lower than that of the other. To fully capture this random storage time, following the analysis and notations used in [4], let us consider two geometric random variables N_A and N_B corresponding to the number of attempts until

Alice memories (A_1, A_2) and Bob memories (B_1, B_2) are, respectively, loaded. Therefore, the number of rounds needed to load both sets of memories will be given by $max\left\{N_A,\, N_B\right\}$. The effective reading efficiency for memories $K = A, B$ will then be given by

$$\eta_{rK} = \begin{cases} \eta_{r0}, & \text{if memory K is late} \\ \eta_r\left(t = |N_A - N_B|T\right), & \text{if memory K is early} \end{cases}, \tag{B4}$$

where T is the repetition period for the protocol, determined by the writing time into memories.

With all above considerations in mind, we obtain

$$Y_{11}^{\mathrm{QM}} = \frac{1}{N_L(P_A, P_B) + N_r}\mathrm{E}\left\{Q^z\left(\eta_{rA}\eta_d,\, \eta_{rB}\eta_d\right)\right\} \tag{B5}$$

where $\mathrm{E}\left\{\cdot\right\}$ is the expectation value operator with respect to N_A and N_B; Q^z is the total gain in (A11), where the input states ρ in the sum cover all possible post-measurement states that can be obtained for different states sent by Alice and Bob; and $N_L = \mathrm{E}\left\{max\left(N_A, N_B\right)\right\}$ and N_r are obtained in [4].

Similarly, the QBER terms in (5) can be obtained from the following

$$e_{11;\beta}^{\mathrm{QM}}\mathrm{E}\left\{Q^\beta\left(\eta_{rA}\eta_d,\, \eta_{rB}\eta_d\right)\right\} = \mathrm{E}\left\{Q_E^\beta\left(\eta_{rA}\eta_d,\, \eta_{rB}\eta_d\right)\right\}, \tag{B6}$$

where, again, the sum in (A12) are taken over all possible post-measurement states obtained from (B1) and $\beta = x, z$.

Finally, to calculate the expected value terms in the above equations, one needs to use the following relationships:

$$\begin{aligned} S_{A<B}(\delta) &= \frac{P_A P_B(1-P_B)e^{-\delta}}{\left[1-(1-P_A)(1-P_B)\right]\left[1-(1-P_B)e^{-\delta}\right]} \\ S_{B<A}(\delta) &= \frac{P_A P_B(1-P_A)e^{-\delta}}{\left[1-(1-P_A)(1-P_B)\right]\left[1-(1-P_A)e^{-\delta}\right]} \\ \mathrm{E}\left\{\eta_{rA}\right\} &= \eta_{r0}[\frac{P_B}{1-(1-P_A)(1-P_B)} + S_{A<B}(T/T_1)] \\ \mathrm{E}\left\{\eta_{rB}\right\} &= \eta_{r0}[\frac{P_A}{1-(1-P_A)(1-P_B)} + S_{B<A}(T/T_1)] \end{aligned}$$

$$
\begin{aligned}
\mathrm{E}\left\{\eta_{rA}\eta_{rB}\right\} &= \eta_{r0}^2 P_0[\frac{1}{1-(1-P_A)e^{-T/T_1}} \\
&+ \frac{1}{1-(1-P_B)e^{-T/T_1}} - 1] \\
\mathrm{E}\left\{\eta_{rA}^2\right\} &= \eta_{r0}^2[\frac{P_B}{1-(1-P_A)(1-P_B)} + S_{A<B}(2T/T_1)] \\
\mathrm{E}\left\{\eta_{rB}^2\right\} &= \eta_{r0}[\frac{P_A}{1-(1-P_A)(1-P_B)} + S_{B<A}(2T/T_1)] \\
\mathrm{E}\left\{\eta_{rA}^2\eta_{rB}\right\} &= \eta_{r0}^3[P_0 + S_{B<A}(T/T_1) + S_{A<B}(2T/T_1)] \\
\mathrm{E}\left\{\eta_{rA}\eta_{rB}^2\right\} &= \eta_{r0}^3[P_0 + S_{A<B}(T/T_1) + S_{B<A}(2T/T_1)] \\
\mathrm{E}\left\{\eta_{rA}^2\eta_{rB}^2\right\} &= \eta_{r0}^4 P_0[\frac{1}{1-(1-P_A)e^{-T/T_1}} \\
&+ \frac{1}{1-(1-P_B)e^{-T/T_1}} - 1],
\end{aligned}
\tag{B7}
$$

where P_A (P_B) is the loading probability for Alice (Bob).

---

[1] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, Nature Photon. **6**, 771 (2012).

[2] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).

[3] S. Abruzzo, H. Kampermann, and D. Bruß, Phys. Rev. A **89**, 012301 (2014).

[4] C. Panayi, M. Razavi, X. Ma, and N. Lï¿œtkenhaus, New Journal of Physics **16**, 043005 (2014).

[5] K. F. Reim, P. Michelberger, K. C. Lee, J. Nunn, N. K. Langford, and I. A. Walmsley, Phys. Rev. Lett. **107**, 053603 (2011).

[6] E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussiéres, M. George, R. Ricken, W. Sohler, and W. Tittel, Nature **469**, 512 (2011).

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

[8] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).

[9] M. Razavi, M. Piani, and N. Lütkenhaus, Phys. Rev. A **80**, 032301 (2009).

[10] A. Stute, B. Casabone, P. Schindler, T. Monz, P. O. Schmidt, B. Brandstätter, T. E. Northup, and R. Blatt, Nature **485**, 482 (2012).

[11] S. Ritter, C. Nölleke, C. Hahn, A. Reiserer, A. Neuzner, M. Uphoff, M. Mücke, E. Figueroa,

J. Bochmann, and G. Rempe, Nature **484**, 195 (2012).

[12] M. Razavi, N. Lo Piparo, C. Panayi, X. Ma, and N. Lütkenhaus, in *Research in Optical Science*, edited by p. Q. OSA Technical Digest (online) (Optical Society of America, 2014) (2014).

[13] M. Razavi and J. H. Shapiro, Phys. Rev. A **73**, 042303 (2006).

[14] N. Lo Piparo and M. Razavi, to appear in IEEE J. Sel. Top. Quant.; e-print arXiv: 1407.8025.

[15] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).

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

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

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

[19] N. Lo Piparo and M. Razavi, Phys. Rev. A **88**, 012332 (2013).

[20] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Nat. Photon. **7**, 210 (2013).

[21] Y.-H. Chen, M.-J. Lee, I.-C. Wang, S. Du, Y.-F. Chen, Y.-C. Chen, and I. A. Yu, Phys. Rev. Lett. **110**, 083601 (2013).

[22] K. Azuma, K. Tamaki, and W. J. Munro, e-print arXiv: 1408.2884.

[23] E. Bocquillon, C. Couteau, M. Razavi, R. Laflamme, and G. Weihs, Phys. Rev. A **79**, 035801 (2009).

[24] M. Müller, S. Bounouar, K. D. Jöns, M. Glässl, and P. Michler, Nature Photon. **8**, 224 (2014).

[25] A. Dousse, J. Suffczyński, A. Beveratos, O. Krebs, A. Lemaître, I. Sagnes, J. Bloch, P. Voisin, and P. Senellart, Nature **466**, 217 (2010).

[26] A. J. Hudson, R. M. Stevenson, A. J. Bennett, R. J. Young, C. A. Nicoll, P. Atkinson, K. Cooper, D. A. Ritchie, and A. J. Shields, Phys. Rev. Lett. **99**, 266802 (2007).

[27] X.-H. Bao, A. Reingruber, P. Dietrich, J. Rui, A. Dück, T. Strassel, L. Li, N.-L. Liu, B. Zhao, and J.-W. Pan, Nat. Phys. **8**, 517 (2012).