



UNIVERSITY OF LEEDS

This is a repository copy of *Repeat-until-success quantum repeaters*.

White Rose Research Online URL for this paper:

<http://eprints.whiterose.ac.uk/81754/>

Article:

Bruschi, DE, Barlow, TM, Razavi, M et al. (1 more author) (2014) Repeat-until-success quantum repeaters. *Physical Review A: Atomic, Molecular and Optical Physics*, 90 (3). ARTN 032306. ISSN 1050-2947

<https://doi.org/10.1103/PhysRevA.90.032306>

Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.



eprints@whiterose.ac.uk
<https://eprints.whiterose.ac.uk/>

Repeat-until-success quantum repeaters

David Edward Bruschi,^{1,*} Thomas M. Barlow,² Mohsen Razavi,¹ and Almut Beige²

¹*School of Electronic and Electrical Engineering,
University of Leeds, Leeds LS2 9JT, United Kingdom*

²*School of Physics and Astronomy, University of Leeds, Leeds LS2 9JT, United Kingdom*

(Dated: July 15, 2014)

We propose a repeat-until-success protocol to improve the performance of probabilistic quantum repeaters. Quantum repeaters rely on passive static linear optics elements and photodetectors to perform Bell-state measurements (BSMs). Conventionally, the success rate of these BSMs cannot exceed 50%, which is an impediment for entanglement swapping between distant quantum memories. Every time that a BSM fails, entanglement needs to be re-distributed between the corresponding memories in the repeater link. The key ingredient in our scheme is a repeatable BSM. Although it too relies only on linear optics and photo-detection, it ideally allows us to repeat every BSM until it succeeds. This, in principle, can turn a probabilistic quantum repeater into a deterministic one. Under realistic conditions, where our measurement devices are lossy, our repeatable BSMs may also fail. However, we show that by using additional threshold detectors, we can improve the entanglement generation rate between one and two orders of magnitude as compared to the probabilistic repeater systems that rely on conventional BSMs. This improvement is sufficient to make the performance of probabilistic quantum repeaters comparable with some of existing proposals for deterministic quantum repeaters.

PACS numbers: 03.67.Bg, 03.67.Dd, 03.67.Hk, 42.50.Ex

I. INTRODUCTION

The quest for long-distance quantum communications has resulted in various schemes for quantum repeaters [1–7]. Such systems ideally enable two users, at an arbitrarily long distance, to share entangled states, which can consequently be used in applications such as quantum key distribution (QKD) [8, 9], teleportation [10], and quantum networking [11]. While there have been successful demonstrations over short distances [12, 13], all proposed techniques for quantum repeaters face certain technological challenges for their full implementation. In the originally proposed quantum repeaters [1, 2], quantum memories as well as highly efficient deterministic quantum gates are required. These gates enable the Bell-state measurement (BSM) required for entanglement swapping as well as the controlled-NOT operation required for the purification of entangled states [14, 15]. In the latest proposals for quantum repeaters [6, 7], the need for quantum memories, as storage devices, has been eliminated, but high-fidelity quantum processing is still required for the proper operation of such systems. There is also another class of quantum repeaters, known as probabilistic quantum repeaters, which are proposed to alleviate the need for high-fidelity operations by relying on probabilistic gates [3–5, 16–18]. By restricting the total channel length to a moderate distance up to around 1000 km, probabilistic repeaters are expected to be the first generation of working quantum repeaters, before deterministic

or no-memory repeaters come to reality. In this paper, we build on the existing techniques in quantum computing [19, 20], to devise a repeatable technique for BSMs, thereby improving the rate one can achieve for probabilistic quantum repeaters to a level comparable with deterministic ones [21].

Probabilistic quantum repeaters rely on quantum memories for entanglement storage, and linear optics and photodetection for entanglement swapping [3–5, 16–18]. In such systems, the entire channel is split into multiple shorter segments with quantum memories at the two ends of each segment. Entanglement must be initially established over these segments and stored in the corresponding memories. This process is often probabilistic, as it typically relies on single-photon communications [3], hence requires several repetitions until it succeeds. Once initial entanglement distribution over two neighboring segments is done, entanglement can be extended to farther distances by performing BSMs on the intermittent memories.

In the case of non-interacting memories often used in probabilistic repeaters, a direct BSM on quantum memories is not possible. In this case, one conventionally reads out the memory state, i.e., transfers the memory state to a photonic one, and then performs the BSM over the retrieved photons. The latter measurement can be implemented by using passive static linear optics and photodetection, but, for that matter, is an incomplete measurement with a success rate limited to 50% [22]. This is because that, even if our measurement module is loss free, we can only measure two, out of four, Bell states by such devices. By accounting for the loss in the BSM module, the chance of success would further go down. In the event of a BSM failure, the initial states of the mem-

*Current affiliation: Racah Institute of Physics and Quantum Information Science Centre, the Hebrew University of Jerusalem, Jerusalem 91904, Israel

ories cannot be recovered, hence entanglement must be distributed again between the corresponding memories, and the whole process must be repeated. The total rate of entanglement generation may then end up to be low in probabilistic repeaters.

There have been several proposals to improve the BSM success rates on photonic states [23, 24]. The main idea is to avoid some of the conditions in the no-go theorem of [22], which enable them to distinguish between more than two Bell states. Auxiliary entangled photons can be used to boost the performance of the BSM (see [23]). Under ideal conditions, and using photon-number resolving detectors (PNRDs), it is shown that by the addition of $2^N - 2$ entangled photons, the success rate can reach $1 - 1/2^N$. Conditional feed-forward techniques, relying on a concatenation of linear-optics module, have also been attempted but to no avail [25]. A more recent proposal used squeezers to make the four Bell states partially distinguishable, which allows for a success rate that exceeds 60%, under ideal conditions and by using PNRDs. Further proposals rely on nonlinear optics, although these are more challenging to implement [26].

In this work we propose a repeat-until-success (RUS) protocol that can improve the chance of success of the BSMs required for entanglement swapping, therefore improving the performance of probabilistic quantum repeaters. Our protocol relies on passive linear optics and photodetection for performing a BSM. Unlike previously proposed photonic BSMs, our RUS scheme actively incorporates the quantum memories on which the BSM is performed. Instead of simply reading the quantum memory, our scheme uses an entangling procedure between the memory and a photon, known as double encoding [19]. The use of entanglement is reminiscent of the technique used in [23], but without requiring external entangled photon sources. We can then suitably choose measurements of the photon state in such a way that the initial entangled states are not destroyed in case of measurement failure. As we shall see below, using mutually unbiased measurements [19], we can ideally retain the initial entangled states of the memories, if the swap operation is unsuccessful, and repeat the process until success. Under ideal conditions, this makes our probabilistic BSM a deterministic one with unity efficiency, thereby significantly improving the performance of our quantum repeaters.

In the presence of loss, our RUS scheme, too, becomes probabilistic. We can nevertheless achieve higher BSM success rates especially if photon number resolving detectors are available. Without resolving detectors, it is still possible, by accepting some errors, to perform BSMs, at an improved success rate, by only using typical threshold detectors. By using additional threshold detectors, we would be able to simulate the required photon number resolution property, by which, without loss of the fidelity, the total entanglement generation rate in a probabilistic quantum repeater can be improved by one to two orders of magnitude. That would make the probabilistic approaches to quantum repeaters comparable with those

that rely on deterministic, but optimistically realistic, measurement operations [21].

This work is organised as follows. In Section II, we introduce the basic tools for the practical implementation of the proposed RUS quantum repeater scheme. These include the double-encoding of quantum information in stationary and flying qubits, the implementation of BSMs, and the realization of gate operations between non-interacting quantum memories. Section III describes a basic RUS quantum repeater link and analyzes its performance under ideal and realistic conditions. In Section IV, we introduce two modified RUS schemes, which do not rely on resolving detectors. In Section V, we calculate the generation rate of entangled states in a multiple-memory repeater setup using RUS entanglement swapping. Finally, we summarize our findings in Section VI.

II. BASIC TOOLS

In this section, we summarize the building blocks of an RUS quantum repeater. Since our scheme employs the same resources as other proposed probabilistic repeater schemes [3, 4, 16–18], there are many similarities. Nevertheless, there would be differences in terms of how the state of quantum memories are double-encoded with that of photons, and how the released photons are measured. Moreover, this section introduces a relatively straightforward scheme for the implementation of four different unitary operations, U_1 to U_4 , between two non-interacting quantum memories.

A. Double-encoding of quantum information

Double-encoding is an entangling process by which the state of a memory is entangled with the state of a single photon. In particular, suppose our memory A is initially in a qubit state $\alpha|0\rangle_A + \beta|1\rangle_A$, where α and β are complex numbers that satisfy $|\alpha|^2 + |\beta|^2 = 1$, and $|0\rangle_A$ and $|1\rangle_A$ represent the corresponding basis vectors of the memory. The state of the memory can then be double-encoded by a single photon a according to the following mapping

$$\alpha|0\rangle_A + \beta|1\rangle_A \rightarrow \alpha|0V\rangle_{Aa} + \beta|1H\rangle_{Aa}, \quad (1)$$

where $|H\rangle_a$ and $|V\rangle_a$ represent orthogonal polarization states of the single photon a . As a result of this double-encoding, a photon entangled with the memory would be released, which will be later used for measurement. The above mapping is called double-encoding, as the quantum information content of the initial state has now been encoded into two subsystems.

One way of implementing the mapping of Eq. (1) is illustrated in Fig. 1. This figure shows an atomic system in the double- Λ configuration, where the qubit states $|0\rangle$ and $|1\rangle$ could represent certain hyperfine states. Here we assume that each quantum memory is placed inside an

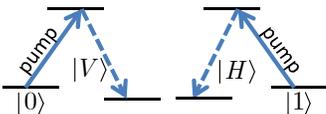


FIG. 1: Double- Λ atomic structure for the realization of the double encoding scheme described in Eq. (1). This requires a so-called stimulated Raman adiabatic passage (STIRAP) process, which results in a vertically polarized photon, if the source is initially in $|0\rangle$ and a horizontally polarized photon, if the source is initially in $|1\rangle$.

optical cavity, where a stimulated Raman adiabatic passage (STIRAP) for the generation of a single photon on demand can be induced [27]. Two laser pulses are applied such that a qubit initially in $|0\rangle$ creates a vertically polarized photon and a qubit in $|1\rangle$ creates a horizontally polarized photon inside the resonator. The photon subsequently leaks out of the cavity and can be used for further processing. Eventually, the atomic state needs to return into its initial state. This can be done, even when the initial state of the quantum memory is not known.

There are, of course, alternative encoding schemes. For example, depending on the level structure of the respective quantum memories, it might be easier to replace the above polarization encoding with time-bin encoding and to generate photons subsequently. The required BSM will again rely on linear optics elements and photodetectors. Although we focus in the following on polarization encoding, all the operations described below can be implemented analogously with time-bin encoding.

B. An incomplete photonic BSM

Passive, static linear optics elements and photodetectors, with infinitely many ancillary vacuum modes, do not allow for the discrimination of four maximally entangled states of two photonic qubits [22]. At most, two maximally entangled Bell states and two product states can be distinguished. For example, using the setup of Fig. 2, it is possible, in the ideal scenario, to distinguish the following photon pair states

$$\begin{aligned} |\Phi_1\rangle &= |\text{HH}\rangle, & |\Phi_2\rangle &= |\text{VV}\rangle, \\ |\Phi_{3,4}\rangle &= |\text{HV} \pm \text{VH}\rangle, \end{aligned} \quad (2)$$

where, for brevity and throughout this paper, we use a simplified notation which is intuitive and allows us to neglect normalization factors.

In Fig. 2, the two modes of light enter the measurement module via the two input ports of the beam splitter. The setup is such that photons in either $|\Phi_1\rangle$ or $|\Phi_2\rangle$ cause clicks at the same detector. More concretely, in the ideal scenario when there is no overall loss, the two input photons, because of quantum interference, would choose the same path at the beam splitter. There will then be clicks on D_2 or D_4 , if $|\Phi_1\rangle$ is at the input, and

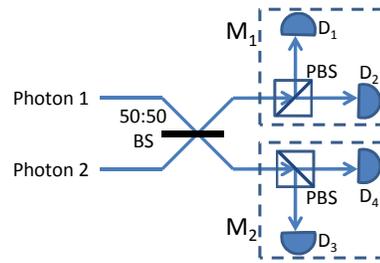


FIG. 2: Experimental setup for the implementation of the incomplete photonic BSM described by Eq. (2) consisting of a 50-50 beamsplitter (BS), two polarising beam splitters (PBS's), and four photodetectors (D_1 to D_4). In the text, we assume that the PBS's change the path of vertically polarised photons but do not affect horizontally polarised photons.

clicks on D_1 or D_3 , if $|\Phi_2\rangle$ is at the input. If we have photon-number resolving detectors, we should be able to count exactly two photons in each case. The two maximally entangled states $|\Phi_3\rangle$ and $|\Phi_4\rangle$ are measured when two different detectors click. Clicks on D_1 and D_2 or on D_3 and D_4 occur, if the photons are in $|\Phi_3\rangle$. Clicks on D_1 and D_4 or on D_2 and D_3 indicate a measurement of $|\Phi_4\rangle$, as summarized in Table I.

C. An incomplete photonic BSM in a mutually unbiased basis

Let us assume that a single qubit rotation is performed before photons 1 and 2 enter the measurement device shown in Fig. 2. As shown in Fig. 3, we denote the single-qubit rotation performed on photon j by R_j . In the following we assume that

$$R_j^\dagger = |x_j\rangle\langle\text{H}| + |y_j\rangle\langle\text{V}| \quad (3)$$

with $j = 1, 2$ and with the x and y -states

$$\begin{aligned} |x_j\rangle &\equiv |\text{H} + \text{V}\rangle, \\ |y_j\rangle &\equiv i^{j-1}|\text{H} - \text{V}\rangle. \end{aligned} \quad (4)$$

Notice that R_1 and R_2 differ only by the factor i in the definition of $|y_2\rangle$. Given that $\langle x_j|y_j\rangle = 0$, the operations in Eq. (3) are indeed unitary. Both operations, R_1 and R_2 , can be implemented using linear optical elements.

Incoming photons	Measurement outcomes	
	Possibility 1	Possibility 2
$ \Phi_1\rangle$ (or $ \chi_1\rangle$)	2 clicks at D_2	2 clicks at D_4
$ \Phi_2\rangle$ (or $ \chi_2\rangle$)	2 clicks at D_1	2 clicks at D_3
$ \Phi_3\rangle$ (or $ \chi_3\rangle$)	D_1 and D_2 clicks	D_3 and D_4 clicks
$ \Phi_4\rangle$ (or $ \chi_4\rangle$)	D_1 and D_4 clicks	D_2 and D_3 clicks

TABLE I: Overview of the possible measurement outcomes for the photon pair states $|\Phi_i\rangle$, $i = 1, \dots, 4$, considered in Eq. (2) and the photon pair states $|\chi_i\rangle$ considered in Eq. (6).

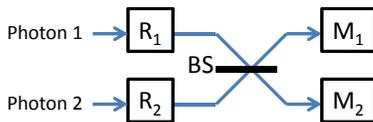


FIG. 3: Experimental setup for the measurement of the states given in Eq. (6), which are the basis vectors of a mutually unbiased basis. Measurement modules M_1 and M_2 are the same as those in Fig. 2.

Proceeding as in the previous subsection, one can show that Fig. 3 now realizes the four projections $|\chi_i\rangle\langle\chi_i|$ with the states $|\chi_i\rangle$ defined as

$$|\chi_i\rangle = R_1^\dagger R_2^\dagger |\Phi_i\rangle, \quad i = 1, \dots, 4. \quad (5)$$

Using Eqs. (2)–(5), we can show that these states are given by

$$\begin{aligned} |\chi_1\rangle &= |(\mathbf{H} + \mathbf{V})(\mathbf{H} + \mathbf{V})\rangle, \\ |\chi_2\rangle &= i|(\mathbf{H} - \mathbf{V})(\mathbf{H} - \mathbf{V})\rangle, \\ |\chi_3\rangle &= |\mathbf{H}(\mathbf{H} - i\mathbf{V}) + \mathbf{V}(i\mathbf{H} - \mathbf{V})\rangle, \\ |\chi_4\rangle &= |\mathbf{H}(i\mathbf{H} - \mathbf{V}) + \mathbf{V}(\mathbf{H} - i\mathbf{V})\rangle \end{aligned} \quad (6)$$

up to an overall phase factor. This implies that two photons arriving at the same detector now indicate a measurement of the product states $|\chi_1\rangle$ or $|\chi_2\rangle$. Analogously, we find that clicks on two different detectors now indicate a measurement of the states $|\chi_3\rangle$ or $|\chi_4\rangle$. More details on this measurement scheme are given in Table I. Similar to $|\Phi_3\rangle$ and $|\Phi_4\rangle$, both states $|\chi_3\rangle$ and $|\chi_4\rangle$ are maximally entangled states.

D. Unitary operations between quantum memories

Notice that the photon states in Eq. (6) are all equal superpositions of the polarisation states $|\mathbf{HH}\rangle$, $|\mathbf{HV}\rangle$, $|\mathbf{VH}\rangle$, and $|\mathbf{VV}\rangle$. Hence they form a so-called mutually unbiased basis [28]. Similarly, if one measures the polarization states $|\mathbf{HH}\rangle$, $|\mathbf{HV}\rangle$, $|\mathbf{VH}\rangle$, and $|\mathbf{VV}\rangle$ in the mutually unbiased basis, the outcome could be any of $|\chi_i\rangle$, $i = 1, \dots, 4$ with the same probability. This means that measuring in the χ -basis does not reveal any information about the polarization of the photons. As we shall see below, this plays an important role in our RUS quantum repeater scheme.

The above measurement, when combined with the double encoding in Section II A, can be used to implement unitary operations on quantum memories. Suppose the quantum memories A' and B' are initially in a state of the form

$$|\psi_{\text{in}}\rangle = |\alpha 00 + \beta 01 + \gamma 10 + \delta 11\rangle_{A'B'}, \quad (7)$$

where the Greek letters denote complex coefficients. The mapping in Eq. (1) transforms the state of quantum

memories and the two generated photons a and b into the state

$$|\psi_{\text{de}}\rangle = |\alpha 00\mathbf{V}\mathbf{V} + \beta 01\mathbf{V}\mathbf{H} + \gamma 10\mathbf{H}\mathbf{V} + \delta 11\mathbf{H}\mathbf{H}\rangle_{A'B'ab}. \quad (8)$$

Finding the photons a and b subsequently in one of the four states $|\chi_i\rangle$ in Eq. (6) prepares the quantum memories A' and B' in the following state

$$|\psi_{\text{mem}}(i)\rangle = \langle\chi_i|\psi_{\text{de}}\rangle. \quad (9)$$

More concretely, using the above equations, we find that the states $|\Psi_{\text{mem}}(i)\rangle$ can also be written as

$$|\psi_{\text{mem}}(i)\rangle = U_i |\psi_{\text{in}}\rangle, \quad (10)$$

where, up to an overall phase factor, the operators U_i are unitary operators given by

$$\begin{aligned} U_1 &= \text{diag}(1, 1, 1, 1), \\ U_2 &= \text{diag}(1, -1, -1, 1), \\ U_3 &= \text{diag}(-1, -i, i, 1), \\ U_4 &= \text{diag}(1, -i, i, -1) \end{aligned} \quad (11)$$

with respect to the computational basis states $|00\rangle_{A'B'}$, $|01\rangle_{A'B'}$, $|10\rangle_{A'B'}$, and $|11\rangle_{A'B'}$. While U_1 is the identity operator and preserves the initial state of the quantum memory, U_2 adds a minus sign when exactly one of the memories is in $|1\rangle$. In contrast to this, one can show that the quantum gates U_3 and U_4 are maximally entangling. They rotate maximally entangled states onto product states.

III. SINGLE-NODE RUS QUANTUM REPEATERS

One of the fundamental challenges for the realization of commercial QKD is the limited distance over which secure keys can be exchanged [29]. Quantum repeaters are a possible solution to this problem. As mentioned in Sec. I, each repeater link consists of a series of nodes. Every intermediary node, in the simplest scenario, is equipped with two quantum memories. We first entangle memories in adjacent nodes. Afterwards, entanglement swapping at the nodes is employed to extend entanglement over larger and larger distances, while destroying the initially generated entangled states between intermediary nodes. The final aim is to create a maximally entangled state shared between the users, which enables them to generate a secret bit of a cryptographic key among other applications.

In this section, we consider the basic building block of quantum repeaters, which is a repeater link with a single middle node. This link is composed of a quantum memory A held by Alice and a quantum memory B held by Bob, respectively, entangled with memories A' and

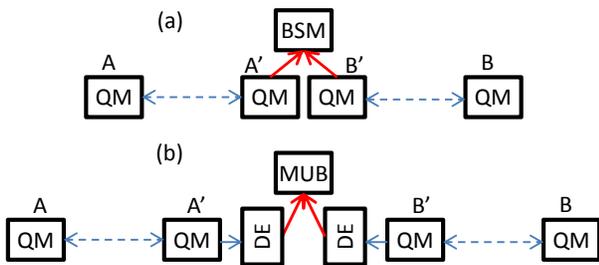


FIG. 4: (a) The main building block of a quantum repeater system. Entanglement is first distributed between pairs of quantum memories (QMs) on the left and right sides of the network. A successful BSM on the middle-node QMs can then extend entanglement between remote parties A and B. (b) An RUS quantum repeater link. Instead of directly measuring the retrieved photons from QMs A' and B' , we first double encode (DE) their states with photons, and then use the module in Fig. 3 to perform a measurement in the mutually unbiased basis (MUB box).

B' held at the middle node (service provider). In conventional probabilistic quantum repeaters, the BSM on A' and B' is performed by first reading the states of the memories, that is by transferring the state of each memory to a single photon, and then performing the BSM optically on the released photons by the measurement module in Fig. 2. Figure 4(a) shows such a link's setup. In this setup, obtaining states $|\Phi_1\rangle$ or $|\Phi_2\rangle$ in Eq. (2) would leave memories A and B in separable states, while the initial entanglement between A and A' as well as that of B and B' are both irreversibly broken. The BSM in Fig. 4(a) at best has a 50% chance of success.

In this section we propose a new *repeatable* BSM scheme as shown in Fig. 4(b). Under ideal conditions, our RUS repeater protocol runs as follows:

- (i) The provider initializes the pairs of memories A, A' and B, B' in the maximally entangled state

$$|\Psi_{\text{in}}\rangle = |01 + 10\rangle_{AA'} \otimes |01 + 10\rangle_{BB'} \quad (12)$$

using standard techniques [4].

- (ii) The provider employs the double-encoding scheme, which we described in section II A, to entangle memory A' with a newly generated photon a and memory B' with a newly generated photon b . The result of this operation is the following state

$$|\Psi_{\text{de}}\rangle = |0101\text{HH} + 0110\text{HV} + 1001\text{VH} + 1010\text{VV}\rangle_{AA'BB'ab}. \quad (13)$$

The memories A, A' and photon a now share a tripartite entangled state, so do the memories B, B' and photon b .

- (iii) The provider measures the double encoded photons in the mutually unbiased basis. If a suitable measurement outcome is obtained, the four memories

A, A', B', B share a multipartite entangled state. Otherwise, after possibly some local operations, we go back to step (ii).

- (iv) The provider separately measures the states of A' and B' to project the state of the memories A and B into a maximally entangled state. Note that these are single-qubit measurements, which can more easily be done with high precision.

In the following we describe our scheme in more detail and find its performance under ideal and realistic conditions. Under ideal conditions, we show that the success rate in our scheme approaches one if photon number resolving detectors (PNRDs) are used. In the next section, we then propose two practical RUS schemes, which do not rely on PNRDs.

A. RUS entanglement swapping under ideal conditions

In this section, we show how our scheme of Fig. 4(b) works in the ideal case when there are no inefficiencies in the measurement procedure, all operations are error free, and we are equipped with PNRDs. To model step (iii) in our protocol, we use the results we obtained in Sec. II D. There we showed that the mutually unbiased measurement on photons a and b can be modelled as a unitary operation U_i on quantum memories A' and B' . More concretely, using Eq. (11), one can show that detection of $|\chi_i\rangle$ in the measurement module of Fig. 4(b), projects the initial state $|\Psi_{\text{in}}\rangle$ in Eq. (12) onto

$$|\Psi_{\text{mem}}(i)\rangle = U_i |\Psi_{\text{in}}\rangle \quad i = 1, \dots, 4, \quad (14)$$

where, using Eq. (11), we have

$$\begin{aligned} |\Psi_{\text{mem}}(1)\rangle &= |01 + 10\rangle_{AA'} \otimes |01 + 10\rangle_{BB'}, \\ |\Psi_{\text{mem}}(2)\rangle &= |01 - 10\rangle_{AA'} \otimes |01 - 10\rangle_{BB'}, \\ |\Psi_{\text{mem}}(3)\rangle &= |01(01 + i10) - i10(01 - i10)\rangle_{AA'BB'}, \\ |\Psi_{\text{mem}}(4)\rangle &= |01(01 - i10) + i10(01 + i10)\rangle_{AA'BB'}, \end{aligned} \quad (15)$$

up to an overall phase factor. An interesting point in the above equation is that the local unitary operations U_1 and U_2 do not erase the entanglement between the quantum memories A and A' and between B and B' . Finding photons in $|\chi_1\rangle$ or $|\chi_2\rangle$ is not a desired measurement outcome. However, the provider no longer needs to return to step (i). He/she only needs to repeat step (ii) until observing either $|\chi_3\rangle$ or $|\chi_4\rangle$. This is a great advantage because the initial entanglement distribution part in step (i) is inefficient and costly.

There is a fundamental difference between our approach to BSM enhancement as compared to those proposed in [23, 24]. In the latter, the focus is on finding a mechanism by which all four Bell states can be distinguished to some extent. In our approach we are still

limited to distinguishing only two Bell states out of four, but our mechanism allows us to repeat the measurement if a product state (which overlaps with one of the two indistinguishable Bell states) is observed. This has become possible by incorporating the quantum memories into our photon pair measurement scheme. Notice that the quantum memories are only indirectly measured, since we use a double-encoding technique.

Measuring the photons in $|\chi_3\rangle$ or $|\chi_4\rangle$ is equivalent to the application of a maximally entangling gate to qubits A' and B' . In order to complete step (iv) and to disentangle the network node from the quantum memories A and B , the provider individually measures the states of the quantum memories A' and B' in the $|0\pm 1\rangle$ basis. For instance, if all four memories are initially in $|\Psi_{\text{mem}}(3)\rangle$ and the measurement outcome of the provider is

$$|\Psi_{\text{node}}\rangle = |0+1\rangle_{A'} \otimes |0+1\rangle_{B'}. \quad (16)$$

In this case, the memories A and B are left in

$$|\Psi_{\text{final}}(3)\rangle = |0(0+i1) - i1(0-i1)\rangle_{AB}, \quad (17)$$

which is a maximally entangled state between quantum memories A and B . Proceeding analogously, one can show that measuring A' and B' in the $|0\pm 1\rangle$ basis, always prepares the remaining quantum memories in a maximally entangled state between the two communicating parties, thereby completing step (iv) of our protocol up to local rotations. This state can now be used to extract one bit of the cryptographic key by performing a local measurement in an appropriately chosen basis.

B. RUS entanglement swapping under realistic conditions

Under ideal conditions, repeat-until-success entanglement swapping saves time and resources compared to entanglement swapping with an incomplete BSM. As we have seen above, the memories A and A' and the memories B and B' need to be entangled only once during the repeater protocol. However, by having a closer look at Table 1, we notice that photon losses would also affect our proposed RUS quantum repeater scheme. As soon as one of the two photons, entangled with memories A' and B' , is lost, the measurement outcome becomes ambiguous. For example, a single click at detector D_1 might be caused by a photon pair initially prepared in $|\chi_2\rangle$ or in $|\chi_3\rangle$. Moreover, without photon number resolving detectors, it is not possible to distinguish two clicks at the same detector from the case, where two photons arrived at different detectors but only one of them caused a click. In this subsection, we have a closer look at the possible imperfections of the measurement module in Fig. 3 and modify step (iii) in our protocol to come up with a basic RUS BSM protocol that works under non-ideal conditions. We calculate the success rate for our basic RUS BSM scheme.

The main source of imperfection we consider in our analysis is the efficiency of our measurement module. We denote the measurement efficiency of our module by η . We assume this factor includes the quantum efficiency of our detectors as well as the efficiencies of our double-encoding scheme and any other coupling or path loss in the measurement module. We assume the measurement module is symmetric and we model the measurement efficiency by adding virtual beam splitters with transmissivity η before photodetectors. All other elements in the measurement module are then assumed to be loss free. We also introduce a unifying notation for the efficiencies of resolving and non-resolving modules. In our work, $\eta\mu$ denotes the probability of distinguishing two photons, when two photons simultaneously arrive at the same detector. For PNRDs, both photons are equally likely to be detected and $\mu = \eta$. In the case of non-resolving threshold detectors, we have $\mu = 0$. In general, μ can be thought to be between zero and η . For simplicity, we neglect dark count effects and assume that all single-qubit rotations and measurements can be performed without introducing additional errors.

Step (iii) of our RUS entanglement swapping protocol now has *four* possible outcomes. In the first case, two different photodetectors click. Taking into account that every one of the operations U_i occurs with the same probability, one can show that the probability P_{1+1} of this happening, for the initial state as in Eq. (12), is given by

$$P_{1+1} = \frac{1}{2}\eta^2. \quad (18)$$

The second scenario is when two photons arrive at the same detector and the detector registers them both, that is it declares the detection of exactly two photons. The probability P_{2+0} for this to happen is given by

$$P_{2+0} = \frac{1}{2}\eta\mu. \quad (19)$$

Another scenario is the registration of only one click at any of the detectors. This occurs with probability

$$P_{1+0} = P_{1+0}(1) + P_{1+0}(2) \quad (20)$$

with $P_{1+0}(1)$ and $P_{1+0}(2)$ given by

$$\begin{aligned} P_{1+0}(1) &= \frac{1}{2}\eta(1-\mu) + \frac{1}{2}(1-\eta)\eta, \\ P_{1+0}(2) &= \eta(1-\eta). \end{aligned} \quad (21)$$

Here $P_{1+0}(1)$ accounts for the cases, where the two initial photons are heading to the same detector, while $P_{1+0}(2)$ accounts for the cases where the two photons are heading towards different detectors. In either case, only one detectors has clicked, either because our detectors are non-resolving, or, in the case of PNRDs, because one of the photons has been lost. The final scenario is when no detector clicks. The probability for this to happen is given by

$$P_{0+0} = (1-\eta)^2. \quad (22)$$

One can easily check that the above probabilities add up to one, as they should. Moreover, it is easy to see that the probability of detecting no photon P_{0+0} is much smaller than all other probabilities, if η is relatively close to one. For example, for $\eta = 0.9$, we have P_{0+0} as small as 0.01. Later, we will take advantage of this fact.

When including loss and inefficiencies in our model, step (iii) in our protocol has four possible outcomes, where only two of which with certainty specify the output state. In other cases, the post-measurement state can be in a mixture of several states. For instance, suppose, in the setup of Fig. 4(b), detector D_2 clicks (see Fig. 2 for the notation). In this case, we know that the photons a and b are in one of the states $|\chi_1\rangle$, $|\chi_3\rangle$, and $|\chi_4\rangle$ but we cannot say which one. In order to avoid any errors in the final state of the quantum memories A and B , in our *basic* protocol, we ignore all cases where none, or only a single detector clicks. That is if we register only one photon, or no photon at all, we consider that as a failure, and go back to step (i). The cases where two different detectors click result in a successful entanglement swapping. These cases correspond to the measurement of either $|\chi_3\rangle$ or $|\chi_4\rangle$. Moreover, two clicks at the same detector indicate a measurement of $|\chi_1\rangle$ or $|\chi_2\rangle$, respectively. In this case, the entanglement between neighboring quantum memories is preserved and the attempted swap operation can be repeated. The total success probability P_{succ} for our basic RUS entanglement swapping scheme hence obeys the relation

$$P_{\text{succ}} = P_{1+1} + P_{2+0} \cdot P_{\text{succ}}. \quad (23)$$

Taking this and the above probabilities into account, we find that

$$\begin{aligned} P_{\text{succ}} &= \frac{P_{1+1}}{1 - P_{2+0}} \\ &= \frac{\eta^2}{2 - \eta\mu}. \end{aligned} \quad (24)$$

For PNRDs, and for $\eta > \sqrt{2/3} = 0.816$, the success rate is above 50%, which beats the maximum that can be achieved by passive static linear optics modules. With existing technology for resolving detectors at efficiencies exceeding 88% [30], this is certainly a promising approach for efficient entanglement swapping.

For non-resolving detectors, i.e., for $\mu = 0$, the success rate of the above scheme equals

$$P_{\text{succ}} = \frac{1}{2}\eta^2. \quad (25)$$

This is exactly the same as the success rate of entanglement swapping schemes based on conventional BSMs as in Fig. 2. In order to achieve an improvement, the photodetectors need to be able to distinguish one and two photons at least to some extent ($\mu \neq 0$) or advantage needs to be taken of cases where only one photodetector registers a photon. In the following section, we introduce two protocols that do not rely on PNRDs.

IV. RUS ENTANGLEMENT SWAPPING WITH NON-RESOLVING DETECTORS

Our basic RUS entanglement swapping scheme can only beat the 50% limit if PNRDs are used. Although the technology for superconducting detectors with high efficiency and resolving capabilities is on the rise [30], it would be more practical if our RUS scheme could work with threshold non-resolving single-photon detectors as well. In this section, we propose two modified RUS BSM schemes, which do not rely on PNRDs. In the first approach, we use the same setup as in Fig. 3 with non-resolving detectors, but allow for errors in the final state. In our second scheme, we create resolving capability by concatenated splitting followed by an array of threshold detectors.

A. Modified RUS BSM with possible errors

One way of improving the success rate in our basic protocol is to not abort the protocol if only one detector clicks. Note that in this section we assume all detectors are non-resolving, i.e., $\mu = 0$. In this case, a single click might be because of two photons heading toward the same detector with a click probability $P_{1+0}(1)$, or two photons heading toward different detectors with a click probability $P_{1+0}(2)$. For values of η near 1, the former case is much more likely than the latter. That is because, after including loss, in the former, both one-photon and two-photon components can make a click, whereas in the latter only one-photon terms can generate only one click. Therefore by accepting some errors, in step (iii) of our basic protocol, we can interpret the detection of only one photon as a measurement of either $|\chi_1\rangle$ or $|\chi_2\rangle$. Instead of aborting the protocol, when only one of the photodetectors clicks, we now continue until either none or two detectors click. We now only abort the entanglement swapping, if no detector clicks, which is relatively unlikely to occur (cf. Eq. (22)).

A closer look at Table 1 shows, for example, that a click on the non-resolving detector D_2 prepares the quantum memories in the following statistical mixture

$$\begin{aligned} \rho_{\text{mem}}(1) &= \frac{1}{P_{1+0}} \\ &\times [(P_{1+0}(1)) |\Psi_{\text{mem}}(1)\rangle\langle\Psi_{\text{mem}}(1)| \\ &+ \frac{1}{2}P_{1+0}(2) |\Psi_{\text{mem}}(3)\rangle\langle\Psi_{\text{mem}}(3)| \\ &+ \frac{1}{2}P_{1+0}(2) |\Psi_{\text{mem}}(4)\rangle\langle\Psi_{\text{mem}}(4)|]. \end{aligned} \quad (26)$$

Alternatively, this density matrix can be written as

$$\begin{aligned} \rho_{\text{mem}}(1) &= (1 - P_{\text{error}}) |\Psi_{\text{mem}}(1)\rangle\langle\Psi_{\text{mem}}(1)| \\ &+ \frac{1}{2}P_{\text{error}} |\Psi_{\text{mem}}(3)\rangle\langle\Psi_{\text{mem}}(3)| \\ &+ \frac{1}{2}P_{\text{error}} |\Psi_{\text{mem}}(4)\rangle\langle\Psi_{\text{mem}}(4)|, \end{aligned} \quad (27)$$

memories in other nodes. In this case, in the limit of a large number of memories, the rate at which we can entangle memories over a distance $L = 2^n L_0$ per logical memory used is given by [5]

$$R_{\text{ent}} = \frac{P_S(P_{\text{succ}})^n}{2L/c}, \quad (34)$$

where n is the nesting level of the repeater setup and P_{succ} is the BSM success probability, here, assumed to be the same for all nesting levels. In our case, P_{succ} can be obtained from Eqs. (24) and (33).

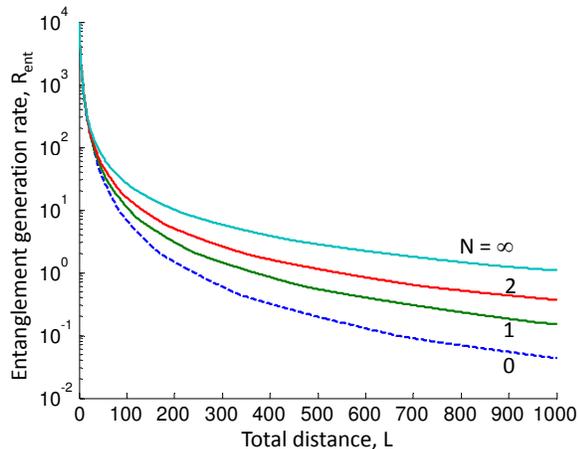


FIG. 8: Entanglement distribution rate (1/s) over a distance L for different branching levels N . The dashed line represent the case of a non-RUS scheme, whereas $N = \infty$ corresponds to the case when resolving detectors are used. In all curves, and, at each point, the optimum value of n is used. We assume $\eta = 0.93$, $c = 2 \times 10^5$ km/s, and $P_S = 0.1 \exp(-L_0/L_{\text{att}})$, where $L_{\text{att}} = 25$ km.

Figure 8 shows the number of entangled pairs per memory per second that can be generated for the quantum repeater network of Fig. 7 at a distance L . We have considered the non-RUS scheme (dashed line) that uses the BSM module in Fig. 2 for its entanglement swapping, and those of RUS schemes with different levels of branching. In each curve, we have plotted the rate at the optimum value of the nesting level n . Given that the RUS entanglement swapping is more efficient than the non-RUS one, the optimum nesting level for the former is typically higher than that of the latter. For instance, at $L = 1000$ km, the optimum value of n for the non-RUS

scheme is 5, whereas for the RUS scheme, with $N = 1, 2$, it is 6, and eventually 7 as $N \rightarrow \infty$. From Fig. 8, it can be seen that, by using our proposed RUS scheme for entanglement swapping, we can achieve one to two orders of magnitude improvement in the entanglement generation rate per memory used. This would translate in either requiring proportionally fewer number of memories, or achieving higher secret generation rates once this setup is used for QKD applications.

VI. CONCLUSIONS

Entanglement swapping is a key operation for quantum repeater networks. Most conventional approaches to entanglement swapping rely on passive static linear-optics modules, which cannot perform a full BSM. That is, in over 50% of the time, an inconclusive result is obtained, which requires the repetition of time consuming initialization steps in quantum repeaters. In our work, we used the repeat-until-success protocol to improve the success rate for such modules once used in a repeater setup. Quantum repeaters rely on quantum memories and entanglement swapping between these memories. Our protocol relied on an entangling procedure between memory states and photons followed by an optical measurement in mutually unbiased bases. The combination of these two allowed us to repeat the required BSM in some cases of failure, thereby achieving higher than 50% success rates. The success rate will approach one in the ideal case and when resolving photodetectors are used. Photon number resolution could be achieved by sequential splitting of photons and detection with an array of non-resolving detectors. In the latter case, a few stages of splitting was sufficient to improve the entanglement generation rate by over one order of magnitude at a nominal distance of 1000 km as compared to non-RUS schemes.

Acknowledgments

DEB and MR acknowledge financial support in part by the UK Engineering and Physical Sciences Research Council Grant No. EP/J005762/1 and the European Community's Seventh Framework Programme under Grant Agreement 277110. TMB receives funding from a UK White Rose Studentship Network on Optimising Quantum Processes and Quantum Devices for future Digital Economy.

-
- [1] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).
 - [2] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, *Phys. Rev. A* **59**, 169 (1999).
 - [3] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature* **414**, 413 (2001).
 - [4] N. Sangouard, C. Simon, H. de Riedmatten, and

- N. Gisin, *Rev. Mod. Phys.* **83**, 33 (2011).
- [5] M. Razavi, M. Piani, and N. Lütkenhaus, *Phys. Rev. A* **80**, 032301 (2009).
- [6] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, *Nat. Photon.* **6**, 771 (2012).
- [7] K. Azuma, K. Tamaki, and H.-K. Lo, arXiv:1309.7207 [quant-ph] (2013).

- [8] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [9] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
- [10] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [11] H. J. Kimble, Nature **453**, 1023 (2008).
- [12] C.-W. Chou, J. Laurat, H. Deng, K. S. Choi, H. de Riedmatten, D. Felinto, and H. J. Kimble, Science **316**, 1316 (2007).
- [13] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan, Nature **454**, 1098 (2008).
- [14] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
- [15] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
- [16] M. Razavi and J. H. Shapiro, Phys. Rev. A **73**, 042303 (2006).
- [17] J. Amirloo, M. Razavi, and A. H. Majedi, Phys. Rev. A **82**, 032304 (2010).
- [18] N. Lo Piparo and M. Razavi, Phys. Rev. A **88**, 012332 (2013).
- [19] Y. L. Lim, A. Beige, and L. C. Kwek, Phys. Rev. Lett. **95**, 030505 (2005).
- [20] Y. L. Lim, S. D. Barrett, A. Beige, P. Kok, and L. C. Kwek, Phys. Rev. A **73**, 012304 (2006).
- [21] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Phys. Rev. A **87**, 052315 (2013).
- [22] J. Calsamiglia and N. Lütkenhaus, Applied Physics B **72**, 67 (2001), ISSN 0946-2171.
- [23] W. P. Grice, Phys. Rev. A **84**, 042331 (2011).
- [24] H. A. Zaidi and P. van Loock, Phys. Rev. Lett. **110**, 260501 (2013).
- [25] M. Pavičić, Phys. Rev. Lett. **109**, 079902 (2012).
- [26] Y.-H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).
- [27] G. S. Vasilev, A. Kuhn, and N. V. Vitanov, Phys. Rev. A **80**, 013417 (2009).
- [28] W. K. Wootters and B. D. Fields, Annals of Physics **191**, 363 (1989), ISSN 0003-4916.
- [29] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).
- [30] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, Phys. Rev. A **71**, 061803 (2005).
- [31] 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, et al., Nat. Photon. **7**, 210 (2013).
- [32] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, New J. Phys. **11**, 045019 (2009).
- [33] 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).