Exact analysis and numerical evaluation of QKD over a practical repeater chain*

Saikat Guha, Hari Krovi, Christopher A. Fuchs, Zachary Dutton
Quantum Information Processing group, Raytheon BBN Technologies, 10 Moulton Street, Cambridge, MA USA 02138

Joshua A. Slater, Christoph Simon, Wolfgang Tittel
Institute for Quantum Information Science, University of Calgary, Alberta T2N 1N4

INTRODUCTION

Shared entanglement underlies many quantum information protocols such as quantum key distribution (QKD) [1], teleportation [2] and dense coding [3], and is a fundamental information resource that can boost reliable classical and quantum communication rates over noisy quantum channels [4, 5]. Optical photons are arguably the only candidate for distributing entanglement across long distances. They however are susceptible to loss and noise in the channel, which is the bane of practical realizations of long-distance quantum communication. In order to generate entanglement over long distances at high rates, intermediate nodes equipped with quantum processing power must be interspersed along the lossy channel. *Quantum repeaters* are one example of such nodes that can help circumvent the linear rate-transmittance fall-off of the unassisted lossy channel also known as the TGW bound [7]. However, *not* all quantum devices, for example quantum-limited phase-sensitive amplifiers, can serve as effective intermediate nodes for improved quantum communication performance over the unassisted pure-loss channel [8].

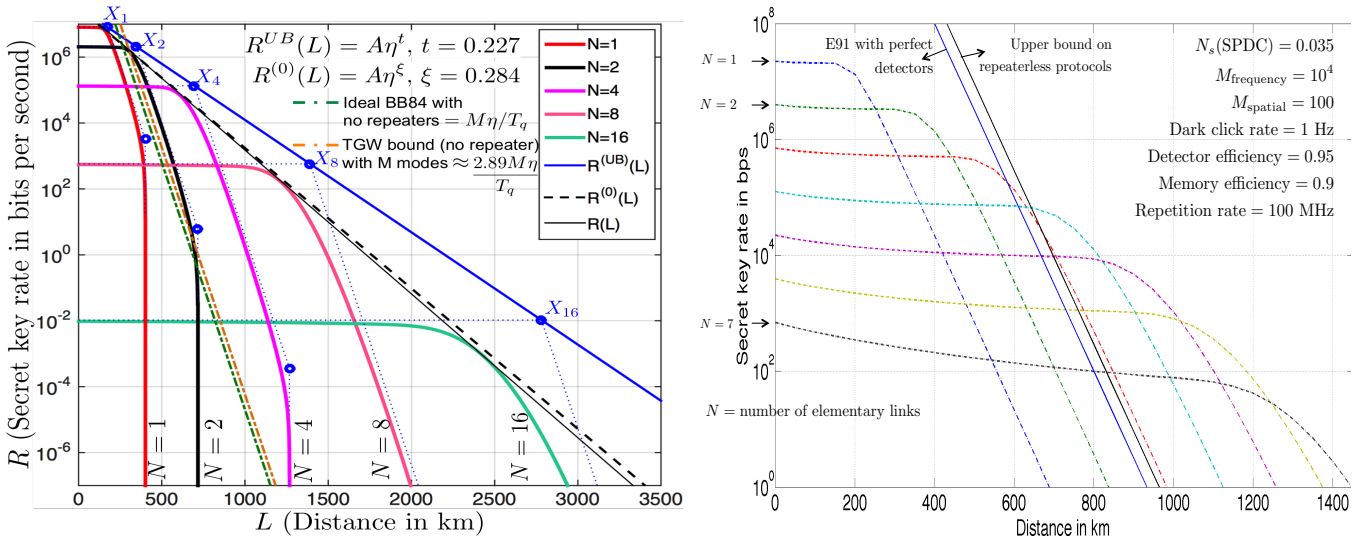
Several quantum repeater protocols have been proposed, most of which use entanglement swapping by Bell-state measurements, and quantum memories, of some form (see [9] for a recent review). The basic quantum repeater protocol probabilistically connects a string of imperfect entangled qubit pairs by using a nested entanglement swapping and purification protocol, thereby creating a single distant pair of high fidelity [10]. If used for QKD, those final distant entangled pairs are measured by Alice and Bob in randomly-chosen mutually-unbiased bases, followed by sifting, error-correction and privacy amplification over a two-way authenticated classical channel, to generate a shared secret. An alternative (the DLCZ) repeater protocol [11] uses a chain of elementary links between pairs of atomic memories prepared with single-photon entangled states, followed by a distant heralded interferometric conversion of two copies of such entangled states into a two-photon entangled state. Repeater protocols usually rely on purifying multiple long-distance imperfect shared entangled pairs (into fewer pairs of high fidelity)—a procedure known as *entanglement distillation*. As an alternative to entanglement distillation, several forward-quantum-error-corrected protocols have been proposed and analyzed [12, 13], which can afford a better rate performance at the expense of more frequent memory-based repeaters capable of universal quantum logic. Some of the more recently proposed forward-coded protocols do not even need any matter quantum memories [14, 15], but come at the expense of fast universal quantum logic and feedforward at all-optical center stations, which is challenging.

In [16], a repeater architecture was proposed that uses photon-pair sources, spectral-multiplexing, multi-mode quantum memories, linear-optic Bell-state measurements [17, 18], and classical-only error correction. This protocol does not rely on purification, and does not require hierarchical connection of the elementary links (i.e., multiple connections can proceed simultaneously), and thus the memory coherence time requirements and the system's clock speed are not driven by long-distance classical communication delays. The protocol allows the fidelity (of the end-to-end shared entangled state) to deteriorate as the chain lengthens, and finally uses classical error correction on a long sifted sequence of correlated pairs of classical data generated by measurements by Alice and Bob, to extract quantum-secure shared secret keys.

The work summarized in this abstract is part of two papers [19, 20]. In [19], we have a rigorous calculation of its achievable rate-vs.-loss performance—both entanglement-distillation and secret-key generation rates—in the presence of various loss and noise detriments, and show that it can fundamentally outperform the TGW bound [7]. To our knowledge, we provide one of the first explicit calculations of the rate-vs.-loss function of any quantum repeater protocol with lossy and noisy components. Although, we analyze the scheme proposed in [16], our method can be carried over to other repeater schemes as well. All of our analysis assumes that the sources are perfect (i.e., have no two or higher photon pair terms). We also perform numerical simulation of the key rates for sources with non-zero higher photon pair terms. All the simulations and analytic results assume that the detectors are single photon detectors (i.e., they have no photon number resolution).

---

* This work is described in two papers. The first one [19] can be found on the arxiv (1404.7183). The second paper [20] is attached along with this abstract and will be posted to the arxiv soon.



(a) Deterministic sources with single photon detectors

(b) SPDC sources with PNR detectors

Figure 1: Rate vs. loss in the case of deterministic (ideal) and SPDC (non-ideal) sources.

In [20], we investigate the effect of having photon number resolving (PNR) detectors. The results in this paper are entirely numerical with the realistic device parameters of loss and noise as in [19]. In this paper, the focus is on finding a practical repeater scheme by assuming that the sources are not deterministic (since deterministic sources are hard to produce). In particular, we consider the issue of realizing quantum repeaters with down-conversion sources and two-photon interference, and we show that this approach can in fact lead to impressive quantum repeater performance, provided that there are two additional elements, namely highly multi-mode quantum memories and photon-number resolving detectors. Multi-mode memories help to compensate for the requirement of working with low pair emission probability, and photon-number resolving detectors make it possible to greatly suppress the remaining errors due to multi-pair emissions. Both highly multi-mode memories and photon-number resolving detectors are under very active development at this point. The main conclusion from our study in [20] is therefore that truly practical quantum repeaters may be within reach. Our results also show that in designing quantum repeater architectures there are interesting trade-offs between the performance and capabilities of the different components, i.e. in the present case, pair sources, memories, and detectors.

ANALYTIC RESULTS

We present a complete analytical characterization of the evolution of the end-to-end shared-entangled state in a concatenated quantum repeater chain and evaluate its performance for QKD. We account for several common device non-idealities except for sources, which we assume are ideal.

- We analyze QKD using the aforesaid repeater chain as an example application, and obtain an exact expression for the secret key rate as a function of loss, number of swap stages, and various loss-and-noise parameters of the channel and detectors. We account for fiber loss, detector dark counts, detector inefficiency, multi-pair emission rates of the entanglement sources, and loss in loading (readout) into (from) the quantum memories.

- We find a compact scaling law for how the quantum bit error rate (QBER)—the probability that Alice and Bob obtain a mismatched sifted key bit despite measuring their halves of the entangled state in the same bases—scales up with increasing number of swap levels. This analytical scaling has practical importance, since an experimentally measured QBER on a single elementary link can be used to predict the QBER (and hence the key rates) practically obtainable over a long-distance channel that is constructed with multiple elementary links made with identical imperfect devices. Our calculation involves a detailed analysis of the Bell-swap operations by modeling imperfect single-photon detectors with appropriate positive-operator-valued-measure (POVM) elements, and solving a variant of the *logistic map*, a non-linear difference equation whose solutions are known to be chaotic in general [25].

- Our calculations show that the aforesaid repeater chain, even if built using lossy and noisy devices, attains an overall rate-loss scaling for QKD that outperforms the TGW bound—the best performance achievable by any QKD

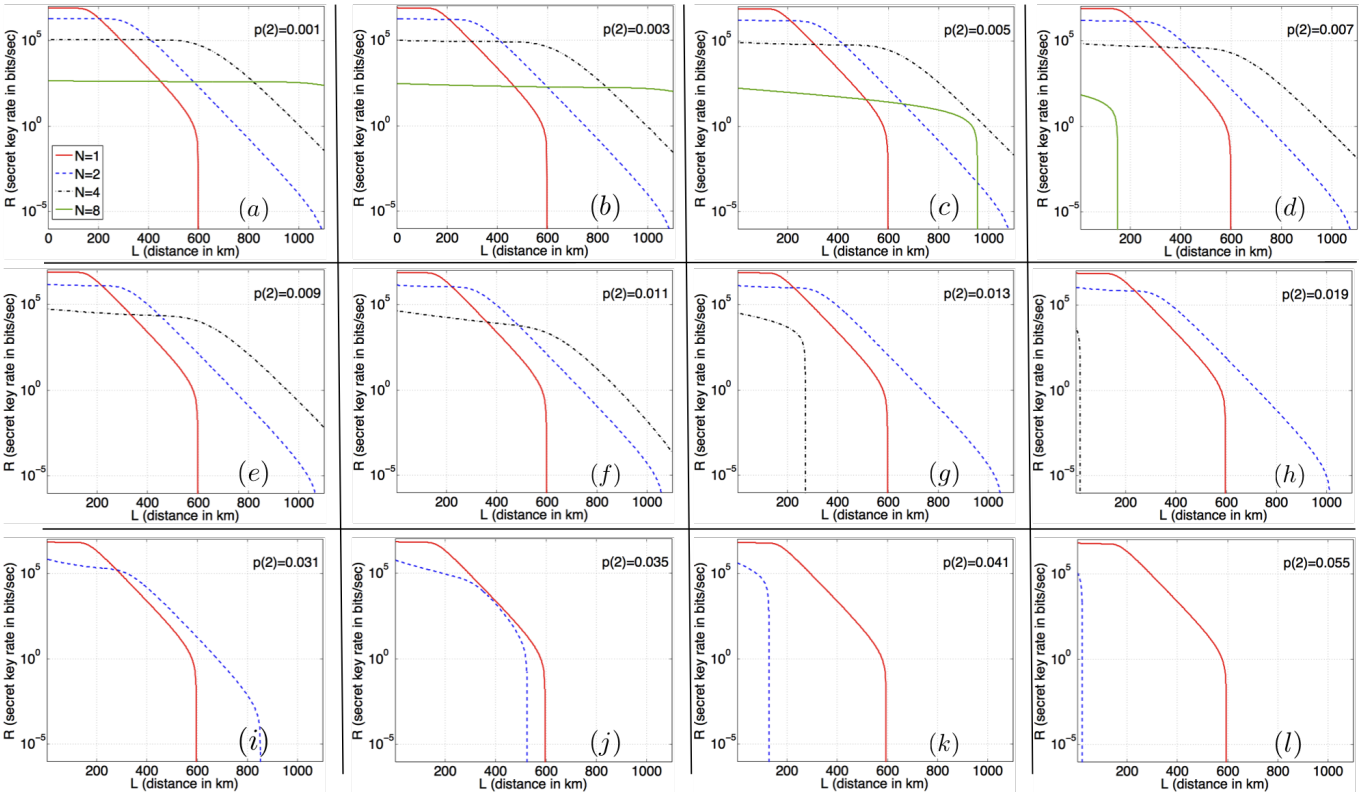


Figure 2: Secret key rate vs. distance for different values of $p(2)$.

protocol that does not employ quantum repeaters. To be precise, if $\eta \in (0, 1]$ is the end-to-end transmittance of the Alice-to-Bob channel, we show that by dividing up the channel into an optimum number of repeater nodes, the secret key rate achieved by the repeater chain, $R = A\eta^{\xi}$. The pre-factor A and the power-law exponent ξ, $0 < \xi < 1$ are constants that are functions of various loss and noise parameters of the system (Fig. 1a).

- Furthermore, since we calculate the exact quantum state after every swap stage, our results can be used to calculate any other quantity of interest, such as fidelity, for other applications of long-distance shared entanglement.

NUMERICAL RESULTS

In our analytical results, while we take into account several different device imperfections, we assume that the sources are deterministic. In order to take into account non-zero $p(2)$, we set up a detailed numerical simulation of the repeater architecture. We obtain the following results.

- When single photon detectors (i.e., non number resolving detectors) are used, even a small amount of $p(2)$ has a very detrimental effect on the secret key rates. This is shown in Fig. 2. This figure depicts the rapid deterioration as $p(2)$ is increased with all the other parameters kept constant.

- Even for sources with $p(2) > 0$, our analytical prediction of QBER propagation through the repeater chain is shown to hold, albeit with a $p(2)$-dependent modification to a pre-factor. Using the above phenomenological model of QBER propagation, we show that positive two-pair probability $p(2)$ is shown to deteriorate the rate-distance function in a particular way described in more detail in [19].

- We investigate the performance when single photon detectors are replaced by photon number resolving (PNR) detectors. We find that the performance is enhanced tremendously even in the presence of non-zero $p(2)$. In fact, as explained in [20], we find that using parametric down-convertor sources (SPDC), which have two pair and higher pair terms as well, with PNR detectors seems to be a feasible experimental goal for the near future. We find that the rate-loss envelope of the plots for different numbers of repeaters beats the TGW bound and, in fact, comes close to the scaling for deterministic sources and single photon detectors (although the multiplexing needed for SPDC sources is higher). This is shown in Fig. 1b.

[1] A. Ekert, Phys. Rev. Lett. **67**, 6 (1991).
[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895–1899 (1993).
[3] C. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[4] M. M. Wilde and M.-H. Hsieh, Quantum Information Processing **11**, 6, 1431–1463 (2012).
[5] M. M. Wilde, P. Hayden, and S. Guha, Phys. Rev. Lett. **108**, 140501 (2012).
[6] S. Guha, J. H. Shapiro, and B. I. Erkmen, "Capacity of the Bosonic Wiretap Channel and the Entropy Photon-Number Inequality", Proc. of the IEEE International Symposium on Information Theory (ISIT), (2008).
[7] M. Takeoka, S. Guha, and M. M. Wilde, Nature Communications **5**, 5235 (2014).
[8] R. Namiki, O. Gittsovich, S. Guha, and Norbert Lütkenhaus, Phys. Rev. A **90**, 062316 (2014).
[9] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).
[10] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[11] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413–418, 22 November (2001).
[12] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Phys. Rev. A **79**, 032325 (2009).
[13] S. Bratzik, H. Kampermann, and D. Bruß, Phys. Rev. A **89**, 032335 (2014).
[14] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and Kae Nemoto, Nature Photonics **6**, 777–781 (2012).
[15] K. Azuma, K. Tamaki, and H.-K. Lo, arXiv:1309.7207 [quant-ph] (2013).
[16] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, and W. Tittel, Phys. Rev. Lett., **113**, 053603 (2014).
[17] S. L. Braunstein, and A. Mann, Phys. Rev. A *Rapid Communications* **51**, 3 (1995).
[18] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).
[19] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, W. Tittel, arXiv:1404.7183.
[20] H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon, W. Tittel, Manuscript attached.
[21] A. Dousse *et al.*, Nature **466**, 217 (2010).
[22] Y. Huang and P. Kumar, Phys. Rev. Lett. **108**, 030502 (2012).
[23] A. Khalique, W. Tittel, and B. C. Sanders, Phys. Rev. A **88**, 022336 (2013).
[24] M. Razavi, H. Farmanbar, and N. Lütkenhaus, Optical Fiber Communication (OFC) Conference, San Diego, California, United States, February 24-28 (2008).
[25] E. Schröder, "Über iterierte Funktionen", Math. Ann. 3 (2): 296–322, doi:10.1007/BF01443992 (1870).
[26] E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussières, M. George, R. Ricken, W. Sohler, and W. Tittel, Nature **469**, 512 (2011).
[27] M. Afzelius, C. Simon, H. de Riedmatten, and N. Gisin, Phys. Rev. A **79**, 052329 (2009).
[28] P. Shor and J. Preskill, Phys. Rev. Lett **85**, 441–444, (2000).
[29] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[30] A. Ferenczi and N. Lütkenhaus, Phys. Rev. A **85**, 052310 (2012).
[31] Z.-X. Xiong, H.-D. Shi, Y.-N. Wang, L. Jing, J. Lei, L.-Z. Mu, and H. Fan, Phys. Rev. A **85**, 012334 (2012).
[32] Scarani *et al.*, Rev. Mod. Phys., **81**, No. 3, July-September (2009).
[33] W. P. Grice, Phys. Rev. A **84**, 042331 (2011).
[34] H. A. Zaidi and P. van Loock, Phys. Rev. Lett. **110**, 260501 (2013).
[35] F. Ewert and P. van Loock, Phys. Rev. Lett. **113**, 140403 (2014).
[36] C. Śliwa and K. Banaszek, Phys. Rev. A **67**, 030101(R) (2003).
[37] G. A. Durkin, C. Simon, and D. Bouwmeester, Phys. Rev. Lett. **88**, 187902 (2002).
[38] H. Krovi, Z. Dutton, S. Guha, C. A. Fuchs, W. Tittel, C. Simon, J. A. Slater, K. Heshami, M. P. Hedges, G. S. Kanter, Y.-P. Huang, and C. Thiel, Proc. Conf. on Lasers and Electro-Optics (CLEO), San Jose, CA, (2014).
[39] H. Krovi, S. Guha, Z. Dutton, C. A. Fuchs, J. Slater, C. Simon, and W. Tittel, *in preparation*, (2014).
[40] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207–235 (2005).

Practical Quantum Repeaters with Parametric Down-Conversion Sources

Hari Krovi, Saikat Guha, Zachary Dutton
Quantum Information Processing group, Raytheon BBN Technologies, 10 Moulton Street, Cambridge, MA USA 02138

Joshua A. Slater, Christoph Simon, Wolfgang Tittel
Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4

Conventional wisdom suggests that realistic quantum repeaters will require quasi-deterministic sources of entangled photon pairs. In contrast, we here study a quantum repeater architecture that uses simple parametric down-conversion sources, as well as frequency-multiplexed multimode quantum memories and photon-number resolving detectors. We show that this approach can significantly extend quantum communication distances compared to direct transmission. This shows that significant trade-offs are possible between the different components of quantum repeater architectures.

I. INTRODUCTION

The distribution of quantum states over long distances is essential for applications such as quantum key distribution [1] and a future "quantum internet" [2]. The distances that are accessible by direct transmission are limited by photon loss. Some form of quantum repeater [3] architecture will be required to overcome this barrier. On the one hand, approaches based on quantum error correction [4] or satellite links [5] promise quantum communication over global distances in the long term, but have significant resource requirements. On the other hand, there is also a lot of interest in simpler approaches, where the focus is on significantly outperforming direct transmission in the short or medium term [6].

The first concrete proposal for a quantum communication architecture with relatively modest resource requirements was the well-known DLCZ protocol [7], which is based on atomic ensembles that serve as photon sources and quantum memories. This proposal stimulated a lot of experimental work [8], but it was soon recognized that the achievable repeater rates were still too low. A potential solution was put forward in [9], which proposed to implement a multiplexed version of the DLCZ protocol combining parametric down-conversion sources (which are comparatively simple to implement) and multimode quantum memories. Such memories are now being developed very intensively, in particular in rare-earth doped crystals [10, 11].

Unfortunately, the protocol of [9] (just as the DLCZ protocol) relies on single-photon interference to create entanglement in the elementary repeater links, and thus requires interferometric stability over long distances, which is a major practical challenge. This difficulty can be avoided by designing repeater protocols where the elementary entanglement creation is based on two-photon interference [12, 13].

However, in the present context, relying on two-photon interference also means relying on simultaneous single photon pair emissions from two different sources, so that one photon from each pair can interfere. It is then challenging to work with parametric down-conversion sources because they can always emit multiple pairs, which typically causes errors. Some of these errors can be eliminated by working with small emission probabilities, but this has a large negative impact on the achievable rates. Other types of errors cannot be eliminated at all in this way.

Past proposals therefore focused on quasi-deterministic sources of entangled photon pairs, which can in principle be realized using individual emitters such as atoms or quantum dots [14], more indirectly by using non-ideal sources in combination with quantum memories, or by combining parametric down-conversion with strong nonlinearities [15]. While many of these approaches seem promising in the longer term, they all pose significant practical challenges in the short and medium term.

Here we adopt a different approach. We reconsider the issue of realizing quantum repeaters with down-conversion sources and two-photon interference, and we show that this approach can in fact lead to impressive quantum repeater performance, provided that there are two additional elements, namely highly multi-mode quantum memories and photon-number resolving detectors. Multi-mode memories help to compensate for the requirement of working with low pair emission probability, and photon-number resolving detectors make it possible to greatly suppress the remaining errors due to multi-pair emissions. Both highly multi-mode memories and photon-number resolving detectors are under very active development at this point. The main conclusion from our study is therefore that truly practical quantum repeaters may be within reach. Our results also show that in designing quantum repeater architectures there are interesting trade-offs between the performance and capabilities of the different components, i.e. in the present case, pair sources, memories, and detectors.

II. REPEATER ARCHITECTURE

A. Description of the Scheme

The architecture that we consider is similar to that proposed in [13] and analyzed in detail in [16], but with

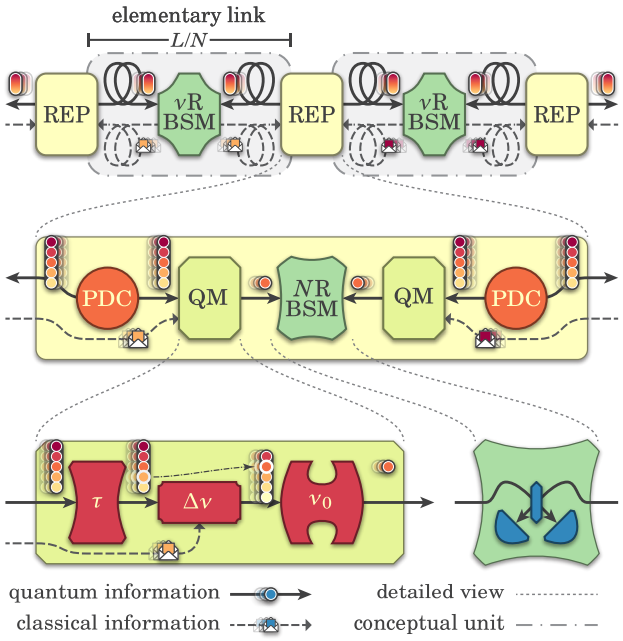


Figure 1. Schematic of quantum repeater architecture [13]. Top Level: The channel is divided into N elementary links, each with a spectrally-resolving BSM (νRBSM) at its center, and with Repeater Nodes (REP) connecting each pair of links. Middle Level: Detailed view of Repeater Node. Each REP contains two PDC sources of frequency-multiplexed bipartite entanglement, two quantum memory units (QM) and a number-resolving BSM (NRBSM). Bottom Level: Detailed view of QM and NRBSM. Each QM unit contains a multi-mode atomic quantum storage device (τ), a frequency-shifting unit ($\Delta\nu$) and a frequency filter (ν_0), while each NRBSM contains a simple linear-optics circuit followed by two single-photon detectors. See main text for a detailed description of the functioning of the architecture

the key difference that we consider parametric down-conversion sources and photon-number resolving detectors, instead of close to ideal pair sources and non-number resolving detectors.

The architecture is depicted schematically in Fig. 1. The total distance between Alice to Bob is divided into N elementary links. At either side of the elementary link is a repeater node (REP) containing a parametric down-conversion source (PDC), which sends one half of an entangled state to the center of the elementary link through a fiber. At every time step entangled states are created in a large number of modes M. We envision M of the order 10^5, which can be achieved mainly by using many distinct frequency modes, although a moderate degree of spatial multiplexing may also be beneficial. The entanglement in each mode can be in polarization or temporal/time-bin degree of freedom, as our discussion applies equally to either encoding. At the center of each elementary link, a frequency-resolving linear-optic Bell-state measurement (νRBSM) [17] is performed on the state comprising of the halves of the two entangled pairs coming from each side. This creates an entangled state across the elementary link by entanglement swapping. The νRBSM consists of a simple linear optical circuit followed by a spectrally-resolved detector array, which can detect across a range of frequencies. Note that the efficiency of a linear optical BSM can at most be 50% for each mode [18].

The other half of each of the entangled states produced by the sources is locally loaded into a multi-mode atomic quantum memory (QM) [13]. For realistic link lengths, most of the photons produced by the sources will be lost in transit. However, if one chooses a large number of modes M, then a successful swap for at least one of them occurs with a high probability. At this point, this frequency information (i.e. the successful frequencies) is transmitted to the memories on either side of the elementary link (dashed lines and envelopes in Fig. 1). Now, each repeater node (REP) receives a pair of which-frequency information from the two elementary links on either side. It uses this information to translate the frequency of the modes (device labelled $\Delta\nu$) on either side to a pre-determined common frequency and filter away all other modes (device labelled ν_0) [13], and thereafter performs a linear-optic BSM (with number-resolving detectors, see below) to do entanglement swapping (νRBSM). If this BSM is successful, the states across two elementary links are connected to create an entangled state across both of them. This process is continued until we obtain an entangled state across Alice and Bob. Alice and Bob can now use this entanglement for tasks such as quantum key distribution or quantum teleportation. For the case of quantum key distribution, secret key rates can be determined following the approach of [16].

B. Parametric Down-Conversion Sources

We now describe the entangled state generated by the parametric down-conversion sources in more detail. For each of the M (frequency) modes discussed above, each source generates a multi-photon entangled state of the form $|\psi\rangle = e^{-iHt}|vac\rangle$, where

$$H = ig(a_0^\dagger b_1^\dagger - a_1^\dagger b_0^\dagger) + h.c., \tag{1}$$

where the coupling constant g is proportional to the pump laser amplitude and nonlinear coefficient of the crystal, the creation operators a_i and b_i refer to the two "halves" of the entangled state discussed above, and the index $i = 0, 1$ refers to the degree of freedom in which the entanglement is prepared, i.e. either polarization or time bins. Each "mode" in our above terminology therefore really corresponds to four physical modes a_0, a_1, b_0, b_1. One can show that [19]

$$|\psi\rangle = \sum_{n=0}^{\infty} \frac{\sqrt{n+1}\tanh^n gt}{\cosh^2 gt}|\psi_n\rangle, \tag{2}$$

with

$$|\psi_n\rangle = \frac{1}{n!\sqrt{n+1}}(a_0^\dagger b_1^\dagger - a_1^\dagger b_0^\dagger)^n |vac\rangle = \sum_{m=0}^{n}(-1)^m |n-m, m; m, n-m\rangle, \quad (3)$$

where $|n-m, m; m, n-m\rangle$ signifies a state with $n-m$ photons in mode a_0, m photons in mode a_1, m photons in mode b_0 and $n-m$ photons in mode b_1.

In the context of the quantum repeater protocol described above, only the term with $n = 1$, corresponding to the emission of a single entangled photon pair, is desired. The case $n = 0$ means that no photons were emitted at all, whereas the terms with $n \geq 2$ correspond to multi-pair emissions, which a priori introduce errors. We now discuss how these errors can be greatly suppressed using photon-number resolving detectors.

C. Suppression of Multi-photon Errors using photon-number resolving detectors

[16] analyzed multi-pair errors in the context of the repeater protocol of [13] (i.e. for much more ideal sources than parametric down-conversion) and found that they severely limit its performance. This analysis was done for ordinary single-photon detectors, which do not count the number of photons. However, photon-number resolving (PNR) detectors are being developed and have reached impressive performance levels [20]. We now show that the use of such detectors allows one to greatly alleviate the problems associated with multi-pair emission by down-conversion sources. In fact, we show that ideal PNR detectors would allow one to eliminate the associated multi-photon terms completely in this repeater architecture.

The improved performance with the use of PNR detectors can best be understood by first considering perfect PNR detectors (i.e. 100% efficiency and no noise). We argue that by post-selecting the outcomes corresponding to single pair terms at the repeaters as well as by Alice and Bob, one can completely eliminate the multi-photon errors, *provided* that the repeater stations (and Alice and Bob) have PNR detectors with no dark clicks. At the center of each elementary link one can use either ordinary single photon detectors or PNR detectors as long as there are no dark clicks in them. With this setup, one can post-select the outcomes corresponding to single pair terms at Alice's and Bob's ends. This means that Alice and Bob wait for a single click in their detectors (which are PNR) and so they know for sure that they have a single photon. This, in turn, means that the entanglement source closest to them has produced the correct state. For simplicity, let us focus on the case when there are two elementary links with a repeater in the center i.e., one elementary link between Alice and the repeater and one between Bob and the repeater. In this case, the center of the elementary link has the right

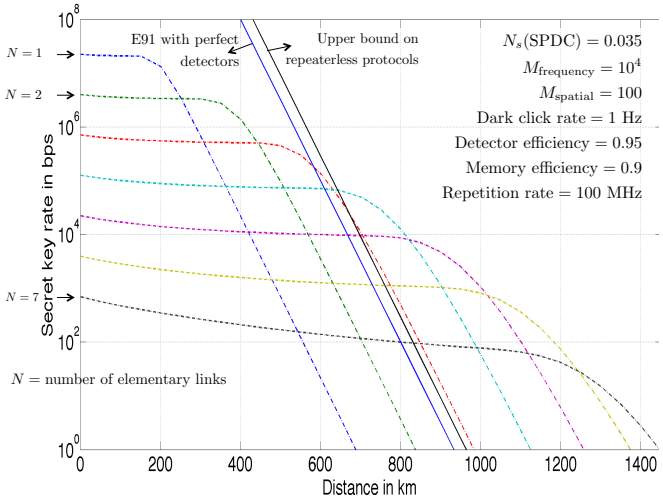


Figure 2. Secret key rate vs. distance for SPDC sources with PNR detectors. The solid black line is the TGW bound and the solid blue line is the achievable rate using E91 protocol and perfect detectors.

state on one side. If the Bell swap results in two detector clicks, this means that the other side of the elementary link must have had one or more photons. Now reasoning similarly from Bob's side, we arrive at the fact that at the repeater station, the two sources on either side have produced one or more photons. But since the repeater has perfect PNR detectors and we post-select the two photon outcome, we can be sure that the two sources on either side have produced a single pair (i.e., the correct state). Finally, this implies that Alice and Bob share a perfect entangled state. This analysis can be extended to any number of elementary links under the same conditions i.e., the repeaters (and Alice and Bob) have perfect PNR detectors and the elementary links have detectors with no dark clicks. This shows that by post-selecting on the single click outcomes by Alice and Bob and the two click outcomes for the repeaters, we can obtain a good entangled state across Alice and Bob. In the presence of detector imperfections such as non-unit efficiency and dark counts, the generated state is no longer perfect, but the fidelity can still be high. In the next section we show what secret key rates should be achievable under realistic conditions with this approach.

III. RESULTS ON REPEATER RATES

To quantify the performance of this protocol we utilized our previously developed MATLAB code which can evaluate entanglement generation and secret key rates across a chain of repeater nodes, accounting for multiple sources of imperfections including detector inefficiency and dark counts, multi-pair emission in the sources, memory lifetime and read/write inefficiency, mode mismatches in Bell measurements, and photon loss in optical

components. Our analysis propagates the density matrix state present in a single (frequency) mode, initializing with the entangled states created at the sources given in Eq.(4) and then transforming directly through lossy fiber and then beam-splitters and other components to perform Bell-state measurements at the center of each elementary link. The total Hilbert space we track includes states with up to 4 total photons. When a state comes upon a detector a two outcome POVM is applied, corresponding to a "click" or "no click" event, as described in Appendix A of [16]. The POVM properly accounts for the detector inefficiency and dark counts. The remaining (undetected) modes continue to propagate through the remainder of the system. Any instance in which the number or pattern of clicks does not correspond to the ideal case is discarded as an successful attempt and the calculation reveals the probability of a successful attempt for each mode P_{s0}. Since we assume large-scale multiplexing M (via frequency and spatial modes) on each elementary link, we then calculate the much higher probability of at least one successful event $P_s(1) - 1 - (1 - P_{s0})^M$ at a particular elementary link before continuing. We then calculate the propagation through the Bell measurements at each repeater node. When N is a power of two, one can take advantage of symmetry and explicitly calculate a case where the Bell-state measurements are done in a binary tree fashion, with the entanglement distance doubling at each stage. However, our calculation and code are for general cases which do not contain a number of elementary links corresponding to a power of two (see for example Fig. 2). Again, the probability of a successful click pattern is calculated and unsuccessful patterns can be discarded. For any successful click pattern, the density matrix can then be used to calculate the total error Q of mis-matched bit values measured at Alice and Bob. The obtainable rate of secret key generation is related to this error rate via $R(Q) - 1 - h_2(Q)$ where $h_2(x) = -x \log_x(x) - (1-x) \log_2(1-x)$ is the binary entropy function. This rate is non-zero when $Q \leq 0.1104$. Note that in [16] we performed this same calculation analytically for the case of perfect entangled photon pair sources and also numerically for the more general source case.

In Figure 3, we present a comparison of the SPDC sources with PNR detectors and perfect sources (i.e., sources with no multi-photon terms). We find that in order for the SPDC-PNR architecture to have a performance comparable to perfect sources, one needs a high level of multiplexing. The number of frequency modes used for perfect sources was 1000, while for the SPDC-PNR architecture we used 10^7 (dot-dashed lines) and 10^8 (dashed lines). The multiplexing needed for the SPDC-PNR architecture can be intuitively predicted by noting that in the SPDC source, one obtains the correct state, i.e., the one with a single pair of photons, with probability $1/N_s^2$. Therefore, the level of multiplexing needed for SPDC sources to perform comparable to perfect sources should be about M/N_s^2, where M is the number of frequency modes used for the perfect sources. With this high level of multiplexing, one can obtain an envelope (over different numbers of repeaters) that is comparable to the envelope obtained from perfect sources. If one wants to improve over repeaterless QKD instead, then a more modest level of multiplexing would suffice. This figure shows that by merely increasing the number of frequency modes, one can obtain a performance that improves over repeater based QKD with perfect entanglement sources. From a practical point of view, this is extremely interesting since improving the level of frequency multiplexing is easier than producing deterministic entanglement sources.

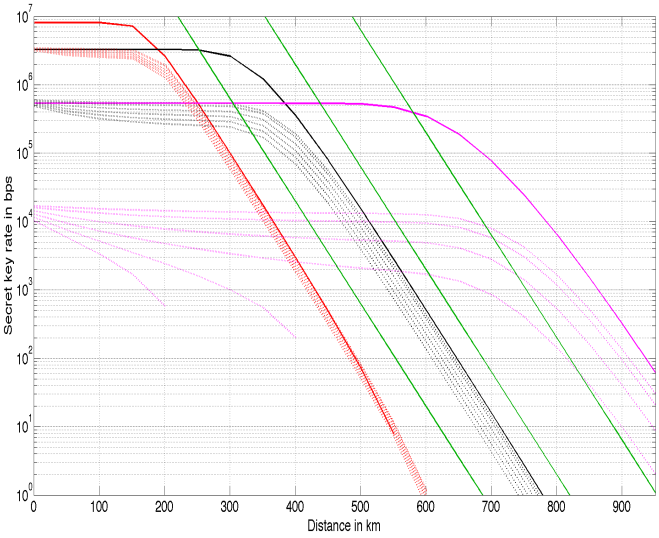


Figure 3. Comparison of the performance of SPDC source (dashed lines) for $N_s = 0.01, 0.02, \ldots 0.1$ and perfect sources (solid lines) with PNR detectors. The number of frequency modes used in the SPDC sources is $10^3/N_s^2$ and for perfect sources is 1000. The three different colors (red, black and magenta) are $1, 2$ and 4 elementary links. The three green lines correspond to repeaterless E91 rates with $10^3, 10^5$ and 10^7 frequency modes.

Modeling of sources: The state can be written as follows.

$$|\psi\rangle = \sqrt{p(0)}\,|00,00\rangle + \sqrt{p(1)/2}\,(|10,01\rangle + |01,10\rangle + \sqrt{p(2)/3}\,(|20,02\rangle - |11,11\rangle + |02,20\rangle)\,. \quad (4)$$

Here we assume that the amplitudes are $p(0) = 1/(N_s + 1)$, $p(1) = N_s/(N_s + 1)^2$ and $p(2) = 1 - N_s/(N_s + 1)^2 - 1/(N_s + 1)$. We compare the performance of this source with a perfect source, i.e., sources that produce an entangled pair deterministically with no higher photon terms. The output of a perfect source is the maximally entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|10,01\rangle + |01,10\rangle)\,. \quad (5)$$

IV. IMPLEMENTATION

A. Photon-number resolving Detectors

Highly efficient (up to 95%) photon number resolving detectors have already been demonstrated (superconducting transition edge sensors) [20] and intrinsic dark counts in these detectors are extremely low. Dark counts are dominated by background light and with appropriate filtering rates as low as 1 Hz should be achievable [21].

B. Multi-mode Memories

Frequency multiplexed quantum memories can be realized based on rare-earth doped crystals. Optical transitions in these systems can have very large ratios of inhomogeneous (100s of GHz) to homogeneous linewidths (kHz), making a great number of frequency channels available (potentially millions) [10]. The proposed repeater architecture does not require readout on demand in time, i.e. it requires only a low-loss delay, followed by appropriate frequency shifts. Such a delay can be realized based on the atomic frequency comb (AFC) memory protocol [11]. For a delay one needs no control pulses, no additional ground state level. One very promising material is Tm:YGG [22]. Storage time of order 1 ms should be possible. (This determines the possible elementary link length.) Memory efficiency can be made very high by using (low-finesse) cavities [23].

V. CONCLUSIONS AND OUTLOOK

In this paper, we argued that SPDC sources along with PNR detectors are a viable alternative to deterministic entanglement sources for repeater based QKD. We showed, numerically, that the performance of the SPDC-PNR architecture is comparable to that of perfect sources when one increases the level of frequency multiplexing. In order to demonstrate an improvement over reapeaterless QKD, one can use a smaller number frequency modes. We have presented a combinatorial argument to show that perfect PNR detectors at the repeater stations and Alice and Bob's ends can completely eliminate the multi-pair errors. We would like to also emphasize the modularity of this architecture. Since the architecture can in principle be used for any sources, if better sources become available, we need not modify anything else in the architecture.

[1] N Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] J. Kimble, Nature **253**, 1023 (2008).
[3] W. Dr, H.- J. Briegel, J. I. Cirac, P. Zoller, Phys. Rev. A **59**, 169 (1999).
[4] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, M. D. Lukin, Phys. Rev. A **79**, 032325 (2009).
[5] K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, C. Simon, arXiv:14010.5384.
[6] N. Sangouard, C. Simon, H. de Riedmatten, N. Gisin, Rev. Mod. Phys, **83**, 33 (2011).
[7] LM. Duan, M. Lukin, I. Cirac, P. Zoller, Nature **414**, 413 (2001).
[8] C. W. Chou, J. Laurat, H. Deng, K. S. Choi, H. de Riedmatten, D. Felinto and H. J. Kimble, Science **316**, 1316 (2007).
[9] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, N. Gisin, Phys. Rev. Lett.**98**, 190503 (2007).
[10] W. Tittel, M. Afzelius, T. Thaneliere, R.L. Cone, S. Kroll, S.A. Moiseev, and M. Sellars, Laser and Photonic Review **4**, 244 (2010).
[11] H. De Riedmatten M. Afzelius, M.U. Staudt, C. Simon, and N. Gisin, Nature **456**, 733 (2008).
[12] N. Sangouard, C. Simon, B. Zhao, Y.-A. Chen, H. de Riedmatten, J.-W. Pan, N. Gisin, Phys. Rev. A **77**, 062301 (2008).
[13] Sinclair *et al.*, Phys. Rev. Lett. **113**, 053603 (2014).
[14] A. Dousse, *et al.*, Nature **466**, 217 (2010).
[15] Y.-P. Huang, P. Kumar, Phys. Rev. Lett. **108**, 030502 (2012).
[16] S. Guha, *et al.*, arXiv:1404.7183.
[17] S. L. Braunstein and A Mann, Phys. Rev. A **51**, R1727-R1730 (1995).
[18] J. Calsamiglia and N. Lutkenhaus, Appl. Phys. B **72**, 67 (2001).
[19] P. Kok and S.L. Braunstein, Phys. Rev. A **61**, 042304 (2000).
[20] A.E. Lita, A. Miller, S.W. Nam, Opt. Exp. **16**, 3032 (2008).
[21] F. Marsili, *et al.*, Nat. Phot. **7**, 210 (2013).
[22] C.W. Thiel, N. Sinclair, W. Tittle, and R.L. Cone, Phys. Rev. Lett. **113**, 160501 (2014).
[23] M. Afzelius and C. Simon, Phys. Rev. A **82** 022310 (2010).