Realistic parameter regimes for a single sequential quantum repeater node

F. Rozpędek, K. Goodenough, J. Ribeiro, V. Caprara Vivoli, A. Reiserer, D. Elkouss, and S. Wehner
QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands

The goal of a quantum repeater is to be able to communicate more efficiently than it is possible *without* a quantum repeater. Since quantum key distribution will be of one the main tasks for a quantum network, it is natural to compare the rate at which one can generate secret key with an implementation of a quantum repeater and the theoretical maximum rate *without* a quantum repeater. We propose a series of benchmarks that can be used to assess the performance of a quantum repeater, as opposed to direct communication. These benchmarks are based on finite-energy considerations, and to what one considers as losses in the setup.

We analyze a realistic model of a quantum repeater setup that can be implemented with current technologies. In particular, we analyze a single sequential quantum repeater node, used together with either the BB84 or six-state protocol. Sequentiality implies that the entanglement generation is split into two phases, necessitating the storage of quantum states over time. The effects of decoherence during storage can be reduced by implementing a *cut-off* on the allowed storage time.

Here, we analyze the advantages of a cut-off for the performance of a single sequential quantum repeater node implementation. We show that this cut-off can, without any experimental difficulties, dramatically increase the performance of such setups. Finally, we find realistic parameters for which it is possible to achieve rates greater than certain benchmarks, guiding the way towards implementing quantum repeaters.

I. INTRODUCTION

A quantum repeater will represent an important step towards building the first long-distance quantum networks. Unfortunately, current implementations of quantum repeaters are not good enough; that is, no experimental system has shown an advantage over direct transmission. It is thus of great practical importance to build and test proof-of-concept quantum repeater implementations.

Here, we analyze a realistic model of a quantum repeater and find explicit parameter trade-offs where such an implementation would repeat. In the analyzed model, two parties Alice and Bob are separated by a single sequential quantum repeater node [5]. That is, the quantum repeater cannot be addressed at the same time by Alice and Bob. This is the case for example with a setup using nitrogen-vacancy centers in diamond. The quantum repeater (QR) is composed of two quantum memories (QM) where each QM can be entangled with a single photon, see FIG. 1.

The protocol consists of a number of *rounds* and *trials*. In each trial, Alice tries to receive a photon from the QR that is entangled with the QM_1, after which she measures in a BB84 or six-state basis [1–3]. Subsequently, the same procedure is applied between Bob and the QM_2. Afterwards, a Bell state measurement is performed on the two QMs at the QR, concluding one round. With suitable classical post-processing, Alice and Bob can generate secret bits.

In a sequential protocol, a quantum state needs to be stored during the time that Bob tries to receive a photon from the QR. If Bob has to try many times to receive a photon, the state stored in the quantum memory will have decohered too much to use for secret-key generation.

As we show here, this challenge can be overcome by implementing a *cut-off* on the maximum amount of time/trials the state should be stored in the quantum memory. That is, when Bob has unsuccessfully tried $n^\star$ times to generate entanglement, Alice and Bob will start a new round. This prevents the state in the memory from decohering too much, albeit increasing the trials that Alice and Bob need to generate a certain amount of bits.

II. MODEL OF A SINGLE SEQUENTIAL QUANTUM REPEATER NODE

The raw key distribution part of the protocol can be seen in algorithm 1. The protocol and QR setup are, besides the cut-off, identical to the one in [5].

Algorithm 1 Quantum repeater protocol

Initialize:
  $N_A \leftarrow 0,\ N_B \leftarrow 0$
loop ▷ Start of round
  repeat ▷ Start of trial on Alice's side
    $N_A \leftarrow N_A + 1$
    Generate entangled photon-QM_1 pair at QR
    Send entangled photon through fiber towards Alice
  until Alice receives photon
  Alice measures in BB84/six-state basis, stores result
  repeat ▷ Start of trial on Bob's side
    $N_B \leftarrow N_B + 1$
    Generate entangled photon-QM_2 pair at QR
    Send entangled photon through fiber towards Bob
  until Bob receives photon or $N_B = n^\star$
  if Bob received photon **then**
    Bob measures in BB84/six-state basis, stores result
    Measurement on memories, communicate result
    Store $\max(N_A, N_B)$ ▷ Store channel uses
    $N_A \leftarrow 0,\ N_B \leftarrow 0$ ▷ Reset channel uses
  return

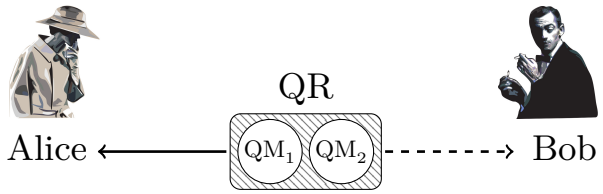

FIG. 1. The QR will send one photon after another entangled with the QM_1 to Alice. After receiving one photon she will measure it in a BB84 or six-state basis. Due to the sequential nature of the QR, only after Alice has measured a photon, can the QR try and send an entangled photon to Bob. If Bob does not receive a photon within some pre-defined amount of times (cut-off), the QR will restart the protocol. This is to prevent the state in the QM_1 from decohering too much. If Bob does succeed, the QR performs a Bell state measurement on the two QMs.

III. ASSESSING QUANTUM REPEATERS

To assess the performance of a QR implementation, we compare the efficiency of the implemented QR with the theoretical maximum *without* a QR. The secret-key capacity of a channel is, informally speaking, a quantification of the maximum rate of secret bits that Alice and Bob could generate per channel use without a QR.

Transmission of photons through fibers is generally modeled as a pure-loss channel, where only a fraction η of the input photons reach the end of the channel on average. The secret-key capacity per mode of such a channel is [6]

$$-\log_2(1-\eta) \ . \tag{1}$$

There is also an upper bound on the secret-key capacity per mode if the mean photon number on the input is restricted to be less than some number P [9]. The corresponding finite energy bound per mode is given by

$$g\left((1+\eta)P/2\right) - g\left((1-\eta)P/2\right) \ , \tag{2}$$

where $g(x) := (x+1)\log_2(x+1) - x\log_2 x$. The finite energy restriction comes from the fact that for qubit encoding only one photon is used, and that the average photon number then satisfies $P = p_{\text{em}}$. This gives rise to two different sets of benchmarks, one with and one without a finite-energy restriction.

We can further distinguish possible benchmarks by considering what to include into the transmittivity η in equations (1) and (2), since it is not clear where the channel begins and ends. We consider three cases,

1. Fiber losses only, $\eta = \eta_{\text{f}} = \eta_A\eta_B$.
2. Inclusion of post-selection, e.g. frequency-filtering probability p_{ps}, $\eta = \eta_{\text{f}}p_{\text{ps}}$.
3. Inclusion of post-selection and emission-probability p_{em} of photon $\eta = \eta_{\text{f}}p_{\text{ps}}p_{\text{em}}$.

This gives us a set of benchmarks that define the limits of direct transmission,

	Infinite	Finite
η_{f}	1a	1b
$\eta_{\text{f}}p_{\text{ps}}$	2a	2b
$\eta_{\text{f}}p_{\text{ps}}p_{\text{em}}$	3a	–

TABLE I. Labels of the benchmarks that we use to assess the performance of a quantum repeater. The left column indicates what is included into the channel while the top row indicates the possible energy constraint.

Note that although in the experimental implementation p_{ps} and p_{em} will appear twice, the benchmarks which include them in the channel do so only once, since we are comparing with the scenario without a QR. We do not consider the finite energy version for $\eta = \eta_{\text{f}}p_{\text{ps}}p_{\text{em}}$, since p_{em} is already included in the channel.

IV. ANALYSIS OF A SINGLE SEQUENTIAL QUANTUM REPEATER NODE

The average secret-key rate of a single sequential QR node can be calculated by finding the average number of channel uses needed to generate one secret bit of key. To this end, we calculate the average number of channel uses needed for Alice and Bob to share one (entangled) state and the average amount of such states that they would have to share to generate one secret bit of key.

These two concepts are captured in the yield Y and the secret-key fraction r, respectively. The secret-key rate per mode achieved is then $R = \frac{Y}{2}r$, where the factor of a half is due to the fact that two modes are needed when encoding in qubits.

A. Yield/channel uses

The yield Y is defined as p_{bsm} times the inverse of the counted channel uses, where p_{bsm} is the probability of success for the Bell state measurement. With a single sequential quantum repeater node it is not obvious how to count the number of channel uses. As in [5], we count the *maximum* of the two channel uses N_A and N_B on Alice and Bob respectively,

$$Y = \frac{p_{\text{bsm}}}{\mathbb{E}\left[N\right]} = \frac{p_{\text{bsm}}}{\mathbb{E}\left[\max(N_A, N_B)\right]} \ . \tag{3}$$

A closed-form expression of the average amount of channel uses has currently not yet been found. We approximate the channel uses by performing a Monte Carlo simulation of algorithm 1. In the regime where $\frac{1}{p_A} \gg n^\star$, the average channel uses can be approximated by

$$\langle N\rangle \approx \left(p_A\left(1-(1-p_B)^{n^\star}\right)\right)^{-1} \ , \tag{4}$$

where p_A and p_B are the total probabilities that a photon will reach Alice or Bob in a single trial, respectively.

B. Secret-key fraction

The secret-key fraction will depend on the error processes that occur in the setup. All error processes are modeled as being either depolarizing or dephasing noise. Any time-independent errors are modeled as depolarizing and dephasing channels, with parameters equal to F_{gm} and F_{prep}, respectively. The time-dependent depolarizing and dephasing decoherence is modeled by an exponential decay in the number of trials n. That is, $F_{\text{mem1}} = e^{-\frac{n}{T_1}}$ for depolarizing and $F_{\text{mem2}} = \frac{1+(2F_{\text{prep}}-1)e^{-\frac{n}{T_2}}}{2}$ for dephasing. Here T_1 and T_2 are two parameters that allow to quantify the coherence times.
With this we find that the average errors in the X, Y and Z basis equal

$$\langle e_X \rangle = \langle e_Y \rangle = \tfrac{1}{2} - \tfrac{1}{2} F_{\text{gm}} \left(2F_{\text{prep}} - 1\right)^2 \left\langle e^{-\left(\frac{1}{T_1}+\frac{1}{T_2}\right)n} \right\rangle \quad (5)$$

$$\langle e_Z \rangle = \tfrac{1}{2} - \tfrac{1}{2} F_{\text{gm}} \langle e^{-\frac{n}{T_1}} \rangle \, . \quad (6)$$

Here $\langle e^{-cn} \rangle$ is the average of the exponential e^{-cn} over a geometric distribution over $n^\star$ trials. From equations (5) and (6) it is possible to calculate the asymptotic secret-key rate for both the BB84 and six-state protocol [8].

V. RESULTS

With the approximated yield and the average errors in hand it is possible to estimate the secret-key rate $R = \frac{Y}{2} r$. We first analyze the effects of the cut-off on the secret-key rate. Here we use parameters from a typical setup using a nitrogen-vacancy center in diamond [4, 7] together with $T_2 = 2000$ trials, $T_1 = 5000$ trials and $\eta_A = \eta_B = 0.001$. In FIG 2, we plot the secret-key rate as a function of the cut-off $n^\star$ for several scenarios with increased parameters for BB84.

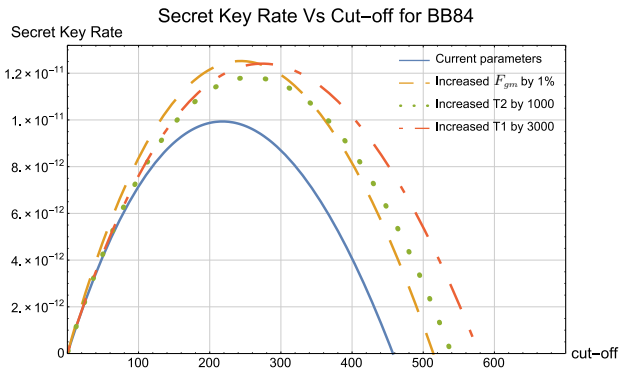

FIG. 2. Secret-key rate as a function of $n^\star$. The blue solid line corresponds to the parameters from [4, 7], with $T_2 = 2000$ trials and $T_1 = 5000$ trials. We see that the cut-off is crucial to being able to generate key.

It is now possible to optimize over the cut-off $n^\star$ and study the effect of changing certain parameters. We show in FIG 3 the regions for which it is possible to beat the benchmarks in Table I as a function of p_{ps} and p_{em}.

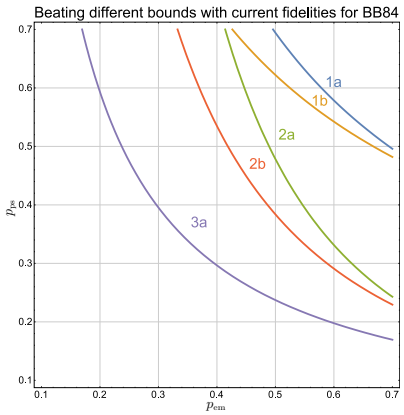

FIG. 3. Regions of p_{ps} versus p_{em} where the benchmarks listed in Table I can be surpassed.

We follow a similar approach in FIG. 4, where we now compare F_{gm} and p_{em}.

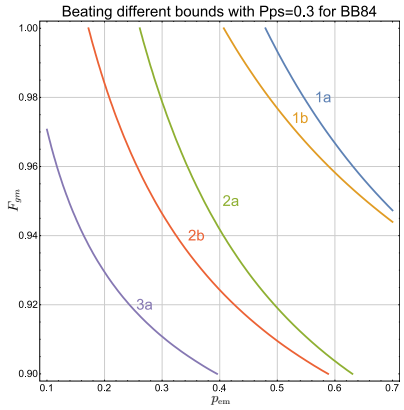

FIG. 4. Regions of F_{gm} versus p_{em} where the benchmarks listed in Table I can be surpassed.

VI. CONCLUSION

In this work, we have analyzed realistic quantum repeater implementations. We have introduced the concept of a cut-off, allowing for a trade-off between the channel uses required and the secret-key fraction. By optimizing over the cut-off, we have found realistic parameter regions where one beats the considered benchmarks. These benchmarks are relevant milestones towards claiming a quantum repeater, and thus form an important step in the creation of the first large-scale quantum networks.

VII. ACKNOWLEDGEMENTS

The authors would like to thank Norbert Kalb for helpful discussions and Dmytro Vasylyev for the illustrations of Alice and Bob.

[1] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*, 59(6):4238, 1999.

[2] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[3] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.

[4] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau. Repeated quantum error correction on a continuously encoded qubit by real-time feedback. *arXiv preprint arXiv:1508.01388*, 2015.

[5] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus. Overcoming lossy channel bounds using a single quantum repeater node. *arXiv preprint arXiv:1508.02811*, 2015.

[6] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. 10 2015.

[7] A. Reiserer, N. Kalb, M. S. Blok, K. J. van Bemmelen, D. J. Twitchen, M. Markham, T. H. Taminiau, and R. Hanson. Robust quantum-network memory using decoherence-protected subspaces of nuclear spins. *arXiv preprint arXiv:1603.01602*, 2016.

[8] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[9] M. Takeoka, S. Guha, and M. M. Wilde. The squashed entanglement of a quantum channel. *Information Theory, IEEE Transactions on*, 60(8):4987–4998, 2014.