Overcoming lossy channel bounds by a single quantum repeater node

David Luong,[1] Liang Jiang,[2] Jungsang Kim,[3] and Norbert Lütkenhaus[1]

[1] *Department of Physics and Astronomy and Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

[2] *Department of Applied Physics, Yale University, New Haven, CT 06511 USA*

[3] *Electrical and Computer Engineering Department, Duke University, Durham, NC 27708, USA*

(Dated: June 26, 2015)

One of the problems that plague the experimental implementation of quantum key distribution (QKD) is the problem of reaching long distances. The transmittance of optical fiber decreases exponentially with length, which puts a severe constraint on the amount of secret key that can be generated over long distances. Specifically, Takeoka, Guha, and Wilde have found that, for any pure-loss bosonic channel with transmittivity η, the key rate is upper bounded by $\log_2[(1+\eta)/(1-\eta)]$ per mode [1]; this is approximately 2.88η for small η. One way to surpass this bound, which we will call the TGW bound, is by using quantum repeaters. First described in [2], they are auxiliary quantum devices placed along the channel between the communicating parties Alice and Bob, dividing their channel into multiple low-loss channels. There are fast repeater schemes that promise very high performance, but they often contain many intermediate stations with multiple qubits in each. These requirements are too onerous for an experimental realization of such a scheme at present, when no experiment has even been performed that beats the TGW bound over any distance.

We propose a simple scheme which still retains the possibility of beating the TGW bound over some distances (Fig. 1), but does not directly scale up to multiple repeater stations. It consists of a central station, placed between Alice and Bob, containing two quantum memories which can each be entangled with single photons. One memory sends entangled photons to Alice, who makes BB84 measurements until she successfully detects a photon. The same thing happens on Bob's side. Once both Alice and Bob successfully detect photons, a Bell state measurement (BSM) is performed on the memories, entangling them. Our scheme is similar in spirit to that of [3], except that in our protocol, photons are emitted from the QMs instead of being sent towards them.

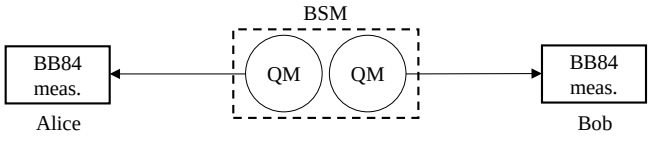

FIG. 1. Schematic of the proposed protocol. One QM sends entangled photons to Alice, the other to Bob. Once both parties successfully measure photons using BB84 measurements, they are entangled by a BSM on the QMs.

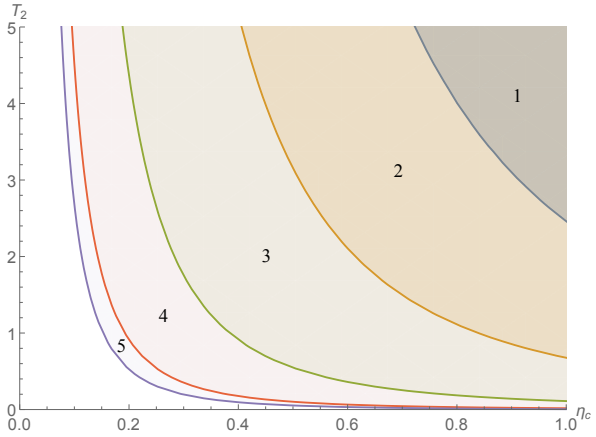

FIG. 2. Values of the memory-channel coupling efficiency η_c and dephasing times T_2 for which our protocol beats (1) the TGW bound, (2) ideal BB84, (3) BB84 with a realistic detector setup, (4) decoy-state BB84, and (5) BB84 using a QM as a single-photon source, given that other experimental parameters are held constant.

In our analysis, we determine whether it is possible for our protocol to beat the TGW bound in practice by taking into account a number of experimental imperfections such as memory dephasing, channel loss, dark counts, and errors in the BSM, envisioning a trapped-ion implementation. We also compare the protocol to a number of other benchmarks, such as ideal BB84 and decoy-state BB84, and find parameter regimes in which our protocol beats them. Fig. 2, for example, shows combinations of dephasing times and coupling efficiencies for which our protocol beats the direct transmission benchmarks (given that other experimental parameters are held constant). Our results suggest that beating the TGW bound in experiment is possible using currently available technology.

[1] M. Takeoka, S. Guha, and M. M. Wilde, IEEE Transactions on Information Theory **60**, 4987 (2014).

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

[3] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, New Journal of Physics **16**, 043005 (2014).