Practical Long-Distance Quantum Key Distribution Using Concatenated Entanglement Swapping

Aeysha Khalique[1,2] and Barry C. Sanders[2,3,4]

[1]*School of Natural Sciences, National University of Sciences and Technology, H-12 Islamabad, Pakistan*

[2]*Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[3]*Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*

[4]*Program in Quantum Information Science, Canadian Institute for Advanced Research, Toronto, Ontario M5G 1Z8, Canada*

We present our model for long-distance communication using concatenated entanglement swapping (CES) [1, 2]. Our theory takes into account practical resources considering various losses. We suggest a quantum key distribution protocol based on this CES setup [3]. The results show that the distance to which secure key can be distributed extends to about 850 km with three concatenated swappings but the secret key generation rate is unimaginably low. This necessitates the use of quantum memory in the setup. Our model provides a framework to model the realistic setup with memories.

Entanglement swapping creates entanglement between two parties, which have never interacted in past. The communication protocols, which rely on entanglement between two parties to establish secure communication, like the 1992 Bennett-Brassard-Mermin (BBM92) protocol [4], can then be applied for key distribution [5]. We have proposed key distribution protocol based on concatenation of entanglement swappings, which constitutes a relay as shown in Fig. 1 to connect two distant parties A and B. Here two parametric down-conversion (PDC) sources and one measurement station comprises entanglement swapping setup. Two adjacent swapping setups are connected by another measurement station. The measurement station consists of beam splitters and polarizing beam splitter to split the incoming beam into two spatial modes for each polarization component and then to be detected on one of the four detectors. Under ideal situation with perfect resources, entanglement is established between the photons in two extreme ends when all the measurements are successful. B also has constructs a record of measurement events obtained by A, by all measurement stations, and by himself. The coincidence of counts on the detectors at all measurement stations ensures entanglement between A and B. This makes the setup for

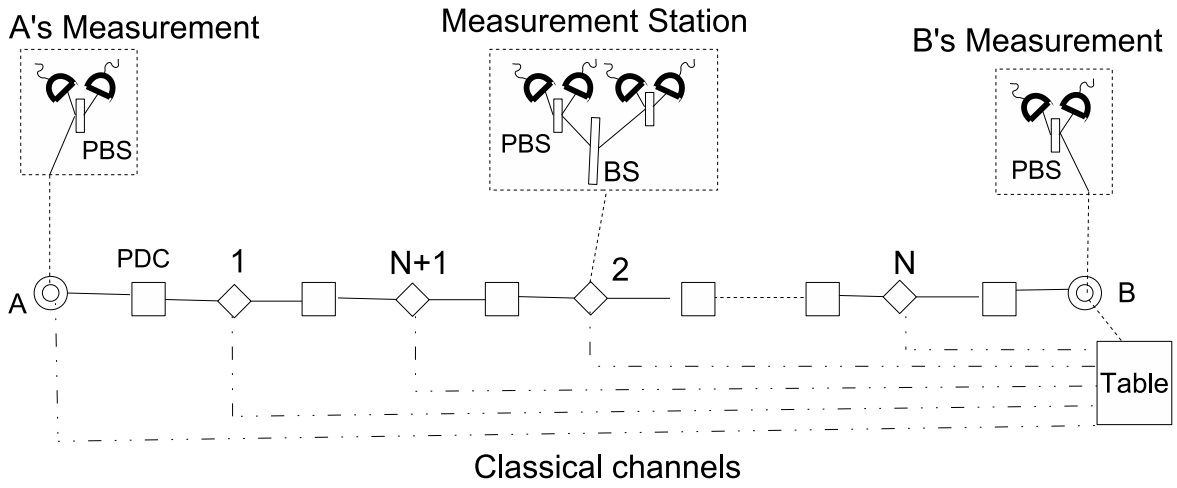

FIG. 1: The PDC-CES-BBM92 protocol: Two distant parties A and B, are connected by two channels: one quantum and the other classical. Two PDC sources □ and one measurement station ⋄ comprise an entanglement swapping setup. A and B each have a polarizing beam splitters (PBS) Each measurement station comprises a beam splitter (BS), two PBSs, and four threshold photon counters. Figure taken from Fig. 1 in [3].

PDC-CES-BBM92 protocol for key distribution. In principle, communication can be extended to arbitrarily large distance. In realistic scenario, the resources are imperfect and in this case, we use visibility between the coincidences of photons to measure the extent of entanglement between the two parties at two ends [1, 6].

We have analyzed the above mentioned protocol by taking into account the practical resources. The entangled photon pair sources are PDC sources, which are probabilistic and generate multi-photon pairs in addition to single photon pairs and vacuum pulses. In addition inefficient threshold detectors with non-zero dark counts and quantum channels exhibiting exponential loss are taken into account. The calculation of the visibility relies on the coincidence of clicks on various detectors. We provide a closed form solution for the coincidence probability for any number of concatenated entanglement swapping and hence the visibility. We have been able to numerically analyze the visibility for concatenation of up to three swap stations.

We have further analyzed this setup for PDC-CES-BBM92 protocol [3]. Our results show that high sifted-key rate needs large pair production rate from the PDC source. However this leads to small visibility and hence high quantum bit error rate, which in turn gives small key-generation rate after error correction and privacy amplification. For small pair production rate the dark counts become more prominent and thus detector efficiency needs to be kept small. We have

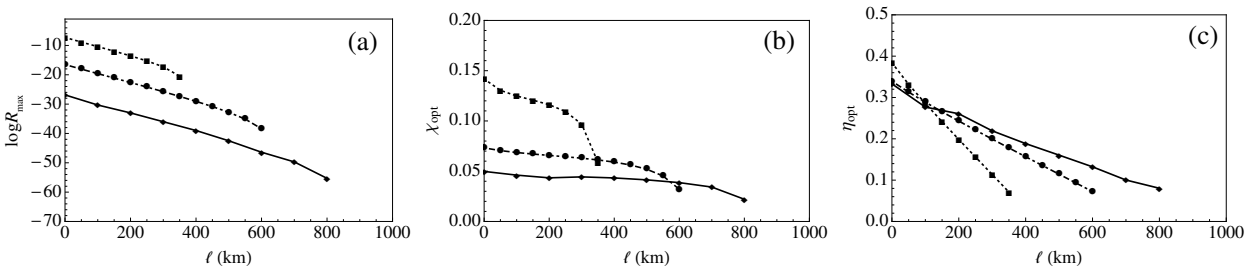

FIG. 2: Plot of (a) $\log R_{\max}$, log of maximum key generation rate (b) χ_{opt}, optimum pair production rate and (c) η_{opt}, optimum efficiency vs distance ℓ up to maximum $\ell_{\max}$ for $N = 1$ (dotted), $N = 2$ (dot-dashed) and $N = 3$ (solid) for channel loss $\alpha = 0.25$ dB/km and constant loss $\alpha_0 = 4$ dB. Symbols ■, • and ♦ represent numerically determined data points, which are connected by straight lines. Figure taken from Fig. 3 in [3].

optimized these parameters to maximize the key generation rate in Fig. 2. The optimal value of pair production rate is very low which in turn increases the experiment run time unrealistically. Thus a trade off is needed between experiment run time and key-generation rate. Although the achievable distance increases to about 850 km, the key-generation rate becomes atrociously low as the number of concatenations increases.

The key generation rate obtained from PDC-CES-BBM92 protocol is lower than yet very close to the Takeoka-Guha-Wilde bound [7], which is the upper bound for non-repeater based key generation protocols. Thus in order to further increase the key generation rate quantum memories are essential. Quantum memory can synchronize the photons and increase the key-generation rate in the entanglement swapping based quantum key distribution protocol. Our model will provide a framework to model the key generation protocol with quantum memory.

[1] A. Khalique, W. Tittel, and B. C. Sanders, Phys. Rev. A **88**, 022336 (2013).

[2] A. Khalique and B. C. Sanders, Phys. Rev. A **90**, 032304 (2014).

[3] A. Khalique and B. C. Sanders, J. Opt. Soc. Am. B **32**, 2382 (2015).

[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[5] A. Scherer, B. C. Sanders, and W. Tittel, Opt. Express **19**, 3004 (2011).

[6] A. Scherer, R. B. Howard, B. C. Sanders, and W. Tittel, Phys. Rev. A **80**, 062310 (2009).

[7] M. Takeoka, S. Guha, and M. M. Wilde, Nat Commun **5** (2014).