

Entanglement Based Quantum Key Distribution With Two Free Space Optical Links

C. Erven (1), C. Couteau (2), R. Laflamme (3), G. Weihs (4)

1: IQC, University of Waterloo, 200 University Ave W, Waterloo, ON, N2L 3G1, cerven@iqc.ca

2: IQC, ccouteau@iqc.ca

3: IQC, Perimeter Institute, laflamme@iqc.ca

4: IQC, weihs@iqc.ca

Abstract

We report on the first real-time implementation of an entanglement based quantum key distribution (QKD) system which uses polarization entangled photon pairs that are sent over two free-space optical telescope links to distribute the key. The two free-space links are 430 m and 1,325 m long respectively, yielding a total separation of 1,575 m between the two receivers. The system performs the complete QKD protocol including all error correction and privacy amplification algorithms. Over the course of approximately 6.5 hours of communication during the night an average raw key rate of 565 bits/sec with an average quantum bit error rate (QBER) of 4.92% was observed; this resulted in a final key rate of 85 bits/sec.

Introduction

From the initial ideas of uncloneable quantum money by Wiesner in the 1970's [1] to the first concrete quantum key distribution (QKD) protocol by Bennett and Brassard in 1984 [2], QKD has rapidly become one of the first technologies to mature out of the new field of quantum information processing. Many demonstrations of different QKD protocols have been performed both over optical fibre and free-space optical links with two of the most recent free-space experiments being performed by Ursin *et. al.* [3] and Marcikic *et. al.* [4] (for a more complete review of the subject and various experimental implementations please refer to [5]).

Motivation

There have been many demonstrations of fibre based QKD systems to date, but far fewer demonstrations of free-space systems. To that end, we set out to construct the first real-time entanglement based two free-space link QKD system. The main motivation behind this was to expand the experimental knowledge for such systems with an eye to contributing to possible future long distance experiments with ground-to-satellite QKD links which would use the same three location setup as in our experiment. Indeed, there have been a number of feasibility studies [6] for quantum communication with satellites and there is now a proposal in front of the European Space Agency (ESA) to perform both decoy state and entanglement based QKD experiments using the International Space Station (ISS) and two earth bound observatories [7].

Experimental Setup

Our system performs the BBM92 [8] entanglement based QKD protocol discovered by Bennett *et. al.* in 1992. Entangled photon pairs are generated via a

compact type-II spontaneous parametric down-conversion (SPDC) source [9] with a local detection rate of 18,000 pairs/sec. The photons are carried to rooftop telescopes with singlemode fibre where they are collimated into a 76 mm beam and sent through free-space to the two receiving locations located 435 m and 1,325 m away. This produces a total separation of 1,575 m between the two receiving locations. Custom designed electronic and mechanical alignment hardware allows the two free-space links to be aligned with the source remotely from the receiving locations.

The photons are measured with passive polarization detector boxes which consist of: a filter to reject background light, a 50/50 non-polarizing beamsplitter (BS) to perform the basis choice, a polarizing beamsplitter in the reflected arm of the BS to separate horizontally and vertically polarized photons, and a half waveplate and PBS in the transmitted arm of the BS to separate photons polarized at $+45^\circ$ and -45° . Avalanche photodiode single photon detectors convert the photons into an electronic signal which is stamped with the polarization measured and a highly accurate time of arrival. This information is then transferred to a laptop at each location and custom written software then performs the rest of the BBM92 protocol including sifting, error correction with the cascade algorithm [10], and privacy amplification with a 2-universal hash function [11].

Security for the system is assured with the security proof by Ma *et. al.* [12] neglecting the need for authenticated classical communication, the loopholes opened from detector efficiency mismatch and double clicks, finite key statistics, and some simplifying assumptions made in the proof such as bit and phase errors being equal and active polarization detection. For more details about the system including more in depth discussion about the security assumptions, the optical and electronic hardware used, and the custom

software please refer to the following articles [13,14,15].

Main achievements

During experiments with the full two link system performed from 11:55 pm to 6:15 am we observed an average raw key rate of 565 pairs/sec with a corresponding average quantum bit error rate (QBER) of 4.92%. This was well under the 11% threshold necessary to prevent against coherent attacks [16] and thus allowed us to generate key in an information theoretic secure manner. After sifting, error correction, and privacy amplification we observed an average final secure key rate of 85 bits/sec. Over the course of the night we were able to generate a total raw key of 10.8 Mbits and a total final key of 1.6Mbits. Figure 1 shows the rates for our system over the course of the night, with each data point representing two seconds worth of data. The top graph shows the QBER in blue, while the bottom graph shows the raw key rate in blue, the sifted key rate in red, the optimum final key rate possible with an error correction algorithm operating at the Shannon limit in green, and the actual final key rate observed in magenta.

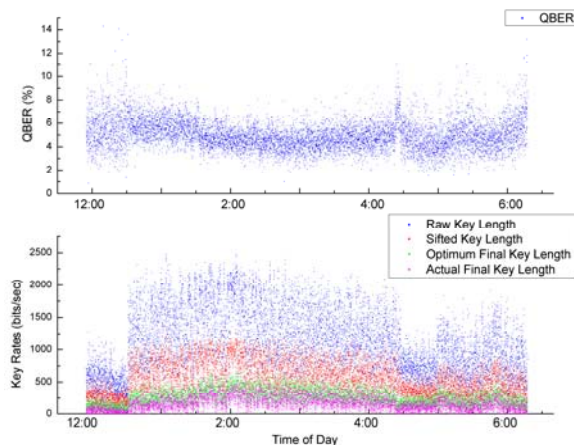


Figure 1: QBER (top) and key rates (bottom) over the course of the experiment. In the top graph the QBER is shown in blue, while on the bottom graph the raw key rate is shown in blue, the sifted key rate is shown in red, the optimum final key rate is shown in green, and the actual final key rate is shown in magenta.

We also performed a quick and admittedly crude Bell inequality violation experiment observing an average Bell parameter of 2.51 ± 0.11 over the course of about 45 minutes just prior to the QKD experiment described above. Lastly, we performed experiments with a variety of free-space setups including: local

detection, one short link and local detection, two short links, one long link and local detection, and multiple nights of the full two link system. This allowed us to observe the dependence of the key rate on the free-space transmission of the photons and the observed QBER.

Conclusions

In conclusion, we have demonstrated the first real-time two free-space link entanglement based QKD system including: entangled photon generation, free-space transmission, polarization detection, error correction and privacy amplification. Over the course of approximately 6.5 hours of communication during the night we observed an average raw key rate of 565 bits/sec with a corresponding QBER of 4.92%. This produced an average final key rate of 85 bits/sec.

Support for this work by NSERC, QuantumWorks, CIFAR, CFI, CIPI, and the Bell family fund is gratefully acknowledged.

References

1. S. Wiesner, Sigact News, 15 (1983), 78
2. C. Bennett *et al.*, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, New York (1984), 175
3. R. Ursin *et al.*, Nature Physics, 3 (2007), 481
4. L. Marcikic *et al.*, Appl. Phys. Lett., 89 (2006), 101122
5. V. Scarani *et al.*, arXiv:quant-ph/0802.4155 (2008)
6. P. Villoresi *et al.*, arXiv:quant-ph/0408067 (2004)
7. J. Perdigues *et al.*, 58th International Astronautical Congress, Hyderabad, India (2007)
8. C. Bennett *et al.*, Phys. Rev. Lett., 68 (1992), 557
9. P. Kwiat *et al.*, Phys. Rev. Lett., 75 (1995), 4337
10. G. Brassard *et al.*, Lect. Notes Comput. Sci., 765 (1994), 410
11. J. Carter *et al.*, Journal of Computer and System Sciences, 18 (1979), 143
12. X. Ma *et al.*, arXiv :quant-ph/0703122 (2007)
13. C. Erven, Master's Thesis, University of Waterloo (2007)
14. G. Weihs *et al.*, Proceedings of SPIE – Quantum Communications Realized, 6780 (2007), 1
15. C. Erven *et al.*, in preparation (2008)
16. N. Gisin *et al.*, Rev. Mod. Phys., 74 (2002), 145