Hyperentangled Time-bin and Polarization QKD for Space Applications

J. Chapman[1], C. C. W. Lim[2], C. Zeitler[1], and P. G. Kwiat[1]
[1]Dept. of Physics, University of Illinois at Urbana Champaign,
[2] Dept. of Elec. and Comp. Eng., National University of Singapore

Implementing quantum key distribution (QKD) or other quantum communication protocols over long distances is a major goal and challenge. To lay dedicated fiber over long distances is expensive and non-reconfigurable, and, without quantum repeaters, such a link has very low transmission. It has been proposed to instead use space-based links where there are quantum channels between a ground station and an orbiting platform [1]. This channel has much lower loss than fiber over the same distance, allowing much more efficient protocol execution over comparable distances; for example, the recent achievement of entanglement distribution from a satellite to two ground stations realized a loss reduction of some 12 orders of magnitude [2], though the detection rate and signal-to-noise ratio was far too low for secure QKD.

With the goal of making a versatile, space-deployable quantum communication system, we are investigating a source and measurement system that can execute multiple quantum communication protocols with minimal changes. Our system consists of a source of photons hyperentangled in the polarization and time-bin degrees of freedom, resulting in pairs of entangled ququarts, and two state characterization and detection systems. With this system, we have previously shown that efficient Superdense Teleportation is achievable [3]. By changing various waveplate settings, polarization BB84 QKD, as well as a hyperentangled quantum key distribution protocol (HEQKD) with two mutually unbiased bases and four measurement outcomes per basis can be implemented. HEQKD is interesting since, it is theoretically possible to achieve greater than 1 bit per photon of raw key. Also for the same number of detection events, the finite key analysis is more favorable for HEQKD when compared to BB84, which would be advantageous in a low transmission channel. Currently, we have demonstrated Polarization BB84 with error rates below 1%. For HEQKD, we have measured preliminarily error rates of 1.5% in one of the bases and 10% in the other basis; because of the quantum interference in the latter basis, it is more important to have matched path and detection efficiencies between the various measurement outcomes, as unbalances result in errors. Work is ongoing to reduce errors in the latter basis.

Additionally, using results from [4-7], we have conducted a finite-key security analysis of our system that includes errors from multiple-pair events and different channel losses between Alice and Bob. The analysis shows that it should be possible to generate a secure key between the International Space Station and a ground station in a single overhead pass if the error rates are below 5% and the channel loss is below 25 db, which is not practically unreasonable.

References

[1] R. J. Hughes et al., *IEEE Aerospace Conf. Proc*. (2000).
[2] Yin, J. et al., *Science*, **35**, 6343 (2017).
[3] J. C. Chapman, T. Graham, F. Marsili, M. Shaw, C. Zeitler, and P. G. Kwiat, *Proc. of OSA Conf. on Lasers and Electro-Optics* (2017).
[4] M. Tomamichel, C. C. W. Lim, N. Gisin and R. Renner, Nature Commun., **3**, 634 (2012).
[5] J. Mueller-Quade & R. Renner, *New Journal of Physics*, **11**, 085006 (2009).
[6] M. Tomamichel & M. Hayashi, *IEEE Transactions on Information Theory*, **59,** 7693-7710 (2013).
[7] R. Koenig, R. Renner & C. Schaffner, *IEEE Transactions on Information Theory*, **55**, 4337-4347 (2009).