# Crosstalk Limitations on Reconfigurable QKD Networks

**X. Tang[1], A. Wonfor[1], R. Kumar[1,2], S. Ren[1], R. V. Penty[1], and I. H. White[1]**
*[1]Centre for Photonic Systems, University of Cambridge, 9 JJ Thomson Avenue, Cambridge, CB3 0FA, United Kingdom*
*[2]Quantum Communication Hub, University of York, UK*
*Author e-mail address: xt217@cam.ac.uk*

Abstract

Quantum key distribution (QKD) has been widely demonstrated to enable two authenticated parties to share unconditionally secure messages over optical channels. The secure key rate achievable in such systems is very sensitive to channel loss and noise as the key is transmitted using single photons. Since the first complete QKD protocol (BB84) was proposed in 1984 [1], and the first experimental demonstration of a QKD system in 1992 [2], significant progress has been achieved in the performance of QKD links between two users. The transmission distance has been extended from a few tens of centimetres to over a hundred kilometres in recent years and the secure bit rate achievable has reached megabits per second [3,4]. However, nearly all current systems are based on point-to-point transmission. For cost-effectively extending the scope of QKD systems to provide secure reconfigurable network communications between multiple parties, optical switching techniques may be applied between QKD end-points, reducing the amount of deployed hardware.

In this work, we study the feasibility of a basic reconfigurable multi-user QKD system, using amendments to current protocols enabling rapid switching between end-points. We examine the QKD performance with additional loss and crosstalk an optical switching element would introduce, which could be critical in building reconfigurable multiuser QKD systems using optical switches. The performance in terms of quantum bit error rate (QBER) of QKD paths (based on the BB84 protocol) through optical switches is predicted using simulation and a series of proof-of-principle experiments featuring additional emulated switch losses and crosstalk from an interferer. Experiments and simulations show that -21dB of crosstalk introduce negligible penalty, but a -9dB crosstalk level adds 5% QBER and reduces the key rate from 11kbit/s to 6kbit/s for back to back signals. For a channel loss of 10dB, -21dB crosstalk reduces the key rate by 250bit/s whereas -9dB crosstalk reduces the key rate to 0bit/s.

[1] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp.175-179, 1984.
[2] C. H. Bennett, et.al., “Experimental quantum cryptography,” J. Cryptology, 5, 3–28, 1992.
[3] L. C. Comandar, et.al., "Room temperature single-photon detectors for high bit rate quantum key distribution", Appl. Phys. Lett., 104, 021101, 2014.
[4] D. Huang, et.al., "Continuous-variable quantum key distribution with 1 Mbps secure key rate," Opt. Express, 23, 17511-17519, 2015.