Stable Polarization Entanglement based Quantum Key Distribution over Metropolitan Fibre Network

Yicheng Shi¹, Soe Moe Thar¹, Hou Shun Poh¹, James A. Grieve¹,
Christian Kurtsiefer¹,², Alexander Ling¹,²

¹ Centre for Quantum Technologies, 3 Science Drive 2, National University of Singapore, 117543 Singapore
² Department of Physics, National University of Singapore, Blk S12, 2 Science Drive 3, 117551 Singapore
cqtsy@nus.edu.sg

Abstract: Quantum key distribution with O-band polarization-entangled photons over deployed telecom fiber network is demonstrated. Liquid-crystal retarders are used to compensate for fiber birefringence induced errors and ensure stable operation. © 2020 The Author(s)

1. Introduction
Quantum Key Distribution (QKD) enables two parties to share random encryption keys without placing assumptions on an eavesdropper’s capabilities [1]. In particular, entanglement based QKD protocols take a step further by eliminating the need of a random number generator, reducing the security risk due to untrusted devices [2]. Existing telecom fibre networks are ideal candidates for distributing entangled photons over shorter distances covering metropolitan areas [3]. In this work we report an entanglement-based QKD system implemented over a deployed fibre using the BBM92 protocol [4], with a total system loss of -30 dB.

Fig. 1: Location map (a) and Optical Time-Domain Reflectometer (OTDR) trace (b) of the deployed fibre under test. Setup of the entanglement based QKD system using BBM92 protocol is shown in (c). InGaAs single photon detectors (10% average detection efficiency) are used in the receivers.

2. Field Implementation
The setup of the QKD system is shown in Fig.1(c). Our photon pair source is based on Type-0 spontaneous parametric down-conversion in a periodically-poled crystal of potassium titanyl phosphate pumped by a grating stabilized laser diode at 658 nm [5]. The photon pairs are degenerate at 1316 nm (telecom O-band), avoiding interference from other telecom windows. They also potentially benefit from non-local dispersion compensation which help to preserve photon timing correlations over large distances [6].

The photon pairs are prepared in $|\Phi^{+}\rangle$ state and are sent to the two receivers named Alice and Bob via optical fibres. The fibre connecting the source and Alice’s receiver is a 10km link deployed by Singapore Telecommuni-
Each receiver setup comprises of 4 InGaAs single photon detectors to measure photon polarization in both horizontal/vertical (H/V) and diagonal/anti-diagonal (+/-) basis. The arrival time of single photons at each detector is recorded and the timestamp information is exchanged between Alice and Bob for coincidence identification and key sifting \[^7\]. To compensate for polarization state error induced by fibre birefringence, a set of Liquid Crystal Variable Retarders (LCVRs) are placed before Bob’s receiver setup. These voltage controlled LCVRs actively compensate the polarization state error to minimize the Quantum Bit Error Rate (QBER) measured between the two parties.

We estimate a total system loss of -30 dB in our setup. The deployed 10-km fibre and the optical coupling of receivers contributes -7 dB and -3 dB respectively. The main loss contributions are from the single photon detectors which yields -20 dB in total (10% average detection efficiency on both sides).

![Graph](image)

Fig. 2: Quantum bit error rate (a), and final key rate (b) logged over 6 hours of continuous operation. The measurement stops due to a technical interrupt in the time-stamping device and is not a fundamental limiting factor for longer operation time.

We recorded about 6 hours of continuous operation in Fig. 2. The system achieved an average quantum bit error rate of 6.4%, and a final key rate of 109 bits/s after error correction and privacy amplification. While this key rate may not be sufficient for a one-time pad application, it can be used to seed encryption devices over classical channels. For example, one can afford to refresh the keys of a AES-256 encryption every 2.4 seconds with the current key rate. We expect a minimum performance improvement of 64 folds in key rate by utilizing superconducting nanowire detectors (~80% detection efficiency) \[^8\]. This implementation can also modified to accommodate other entanglement based protocols.

**References**

1. C. H. Bennett, & G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179, 1984.
2. I. Marcikic, A. Lamas-Linares, & C. Kurtsiefer, *Free-space quantum key distribution with entangled photons*, Appl. Phys. Lett. 89, 101122 (2006).
3. N. Gisin, G. Ribordy, W. Tittel, & H. Zbinden, *Quantum cryptography*, Rev. Mod. Phys. 74, 145 (2002).
4. C. H. Bennett, G. Brassard, & N. D. Mermin, *Quantum cryptography without Bell’s theorem*, Phys. Rev. Lett. 68, 557, (1992).
5. A. Lohrmann, C. Perumangatt, A. Villar, & A. Ling, *Towards detecting Gigacount rates from a polarization entangled photon-pair source*, arXiv:1908.09568 [quant-ph] (2019).
6. J. Grieve, Y. Shi, H. Poh, C. Kurtsiefer, & A. Ling *Characterizing nonlocal dispersion compensation in deployed telecommunications fiber*, Appl. Phys. Lett. 114:13 (2019).
7. C. Ho, A. Lamas-Linares, & C. Kurtsiefer, *Clock synchronization by remote detection of correlated photon pairs*, New J. Physics, 11, 1–14 (2009).
8. V. B. Verma, B. Korzh, F. Bussières, R. D. Horansky, A. E. Lita, F. Marsili, M. D. Shaw, H. Zbinden, R. P. Mirin, and S. W. Nam, *High-efficiency WSi superconducting nanowire single-photon detectors operating at 2.5K*, Appl. Phys. Lett. 105, 122601 (2014).