Field Trial of Continuous Variable Quantum Key Distribution on Trackside Fibre

Rupesh Kumar[1], Bimal Nayar[2], Tim Lane[2], and Tim Spiller[1]

[1]School of Physics, Engineering and Technology and York Centre for Quantum Technologies, University of York, York, YO10 5DD, UK
[2]Network Rail, The Quadrant:MK, Elder Gate, Milton Keynes, MK9 1EN, UK

ABSTRACT

We report the field trial of a Gaussian Modulated Coherent State (GMCS) Continuous Variable Quantum Key Distribution (CVQKD) system over 49.82km of railway trackside fibre. We have examined the effect of a moving train on the QKD system and implemented compensation methods, mainly for polarisation stabilization. The system generated 4kbps secure key, in the asymptotic limit, under the collective attacks. The CVQKD transmitter and receiver were deployed at the Rail Innovation and Development Centre (RIDC) at Melton Mowbray, UK, and remotely monitored and operated from the University of York, at York, UK.

Keywords: Continuous variable quantum key distribution, trackside fibre

1. INTRODUCTION

Continuous Variable Quantum Key Distribution (CVQKD) exploits the Heisenberg Uncertainty principle, in the measurement of highly attenuated coherent signals, for generating unconditionally secured cryptographic keys[1,2]. Amplitude and phase of the modulated quantum coherent signal holds the information for the users—Alice and Bob—to convert into secure keys. The quantum coherent signals are either continuously[1] or discretely modulated[3] in their amplitude and/or phase, according to the protocol. In this paper, we consider the Gaussian Modulated Coherent State (GMCS) protocol[1], in which the quadratures of the coherent states are normally distributed. The modulation variance is generally optimized for the transmission distance, in order to extract maximal amount of secure key. At Bob, shot-noise limited measurement is performed either randomly on one of the quadratures (referred to as homodyne detection[2]), or simultaneously on both quadratures (referred to as heterodyne detection[4]). The quadrature measurements are performed against a strong reference pulse called Local Oscillator (LO). One of the advantages of homodyne/heterodyne detection is that the LO acts like a strong filter for photons which are not coherent with the LO. This noise rejection property of the detection makes CVQKD highly resistance to background noise in Dense Wavelength Division Multiplexed (DWDM) fibre networksREF. The LO is either sent by Alice with each signal—referred to as Transmitted LO (TLO)[5]—or locally generated at Bob—referred to as Local LO (LLO)[6]. In this work, we use a TLO-based CVQKD system with homodyne detection.

In a TLO configuration, the LO also serves the purpose of clock distribution from Alice to Bob, whereas in a LLO setup a separate clock channel is necessary. This is due to the limited pulse intensity of the reference signal, which serves as the phase reference for both Alice and Bob. Our setup is a fibre-based TLO configuration, in which each LO pulse is time and polarisation multiplexed with the signal, before being fed into the fibre channel that connects Alice and Bob. The time and polarisation multiplexing are not only to avoid the cross-talk from an intense LO pulse to the signal, but also to enable Bob to separate the signal and LO into separate channels for homodyne detection, when these are received in a single fibre channel. The time multiplexing also acts to provide timing information to generate a clock for data acquisition. The polarisation and time demultiplexing are performed sequentially at Bob. A portion of LO pulse is used for clock generation, prior to polarisation demultiplexing, in order to avoid the impact of polarisation on the clock generation at Bob. Once separated

Further author information: (Send correspondence to Rupesh Kumar)
E-mail: rupesh.kumar@york.ac.uk

and time and polarisation modes are matched, the signal and LO interfere at the beam-splitter of the homodyne detector. The output of this homodyne detector is acquired on the rising or falling edge of the clock. The quadrature data values are then digitally processed, in order to generate the secure keys.

In this work, we have used 49.98km of trackside fibre as the quantum channel. The Alice and Bob CVQKD transmitter and receiver were hosted at the testing room at the Railway Innovation and Development Centre (RIDC), Asfordby, and remotely operated from the Univerity of York's laboratory. Alice's signal and LO outputs were connected to the termination rack of the trackside fibre and sent to the termination point of the trackside fibre at Syston railway station. The signal and LO then returned to the Asfordby testing room over a separate fibre channel. However,both inward and outward fibre were a situated in a 24-core ruggedised fibre cable. The track side fibre cables are contained within surface concrete troughing route near the railway tracks. This proceedings article is arranged in the following way. In section 2, we outline the channel parameters and secure key rate of the CVQKD system. In section 3, we discuss the effects of the fibre channel on the secure key rate. We detail the polarisation drift measurement and effect of vibrations from trains on the trackside fibre in section 4, and provide the experimental setup and results in section 5.

2. CHANNEL PARAMETERS AND SECURE KEY RATE OF CVQKD

Since the signal and LO pass through different fibre lines inside Alice and Bob, the phase reference, i.e. the relative phase between the LO and the signal, changes continuously and randomly. This is referred to as phase drift in TLO CVQKD. Once the phase drift is compensated, Alice and Bob can establish correlated quadrature data sets, from which they can estimate the channel parameters: transmittance T and excess noise ξ, of the CVQKD setup, from the following equations.

$$T = \frac{(< X_A X_B >)^2}{\eta_B (V_A)^2} \tag{1}$$

$$\xi = \frac{V_B - \eta_B T V_A - N_0 - v_{ele}}{\eta_B T} \ . \tag{2}$$

Here, X_A and X_B are the X-quadratures of the coherent state $\mid \alpha\rangle = X + iP$, prepared by Alice and detected by Bob, with variances V_A and V_B, respectively. η_B and v_{ele} are the detection efficiency and electronic noise of Bob's homodyne detector and N_0 is the shot noise variance. Eqs. (1) and (2) also hold for the P quadratures. The secure key rate under collective attacks in the asymptotic limit is given by:

$$k = f\{\beta I_{AB} - \chi_{BE}\} \ , \tag{3}$$

where f is the fraction of the samples that contribute to the key generation, β is the reconciliation efficiency and $I_{AB} = \log\left(\frac{V+\chi_{tot}}{1+\chi_{tot}}\right)$ is the mutual information between Alice and Bob. Here, the total noise $\chi_{tot} = \chi_{line} + \frac{\chi_{hom}}{T}$, in which $\chi_{line} = \frac{1}{T} - 1 + \xi$ and $\chi_{hom} = (1 + v_{ele} - \eta)/\eta$. v_{ele} is the electronic noise and η is the efficiency of Bob's homodyne detection. $\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=2}^{5} G\left(\frac{\lambda_i - 1}{2}\right)$ is the Holevo bound for Eve's information, in reverse reconciliation, with $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, $\lambda^2_{1,2} = \frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right)$, $\lambda^2_{3,4} = \frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right)$ and $\lambda_5 = 1$. Here, $A = V^2(1-2T) + 2T + T^2(V + \chi_{line})^2$, $B = T^2(V\chi_{line} + 1)^2$, $C = \frac{1}{(T(V+\chi_{tot})^2}\left[A\chi^2_{hom} + B + 1 + \chi_{hom}(V\sqrt{B} + T(V + \chi_{line})) + 2T(V^2 - 1)\right]$ and $D = \frac{V + \sqrt{B}\chi_{hom}}{T(V+\chi_{tot})}$.

3. EFFECTS OF THE FIBRE CHANNEL ON THE SECURE KEY RATE

It is assumed that the channel parameters are controlled by the eavesdropper. From a practical perspective, here we examine how the fibre channel contributes to the estimation of the channel parameters. The actual physical value of channel transmittance is the property of single mode silica fibre (SMF). This is considered as static loss, due to the intrinsic losses such as absorption and scattering and the extrinsic losses such as bending and coupling loss. Both the CVQKD signal and LO naturally experience the above mentioned physical losses. For a typical SMF, this loss is about 0.2dB/km at a wavelength of 1550nm. The channel transmittance that accounts for the

secure key is not measured directly, but estimated from the correlation between the detected and transmitted quadratures, from Eq.(1). Hence any fluctuations in the signal, due to the channel, affect the correlation and thus the estimation of the channel transmittance, T. Therefore, the dynamics of the channel properties that affect the signal strength have a direct impact on the secure key rate. We refer to this as dynamic loss.

Imperfect polarisation demultiplexing is the general cause of dynamic loss in CVQKD. At Alice's output, the LO and signal are aligned along the fast and slow axes of the polarisation maintaining (PM) fibre. The single mode fibre channel that couples to the PM fibre does not preserve the polarisation and adds random drift to the polarisation. However, it does preserve the orthogonality of the signal and LO polarisations. At Bob, a dynamic polarisation controller (DPC) is used to compensate the polarisation drift and align the LO and signal polarisations to the fast and slow axes of the input PM fibre. A polarisation beam-splitter separates the LO from the signal and then a fibre delay line time demultiplexes these, ready for homodyne detection. Improper polarisation demultiplexing leaks signal to the LO path and creates a loss. Variations in the birefringence along the fibre channel cause the polarisation rotation in single mode fibre. This polarisation rotation is affected by any thermal drift and physical oscillations, such as vibrations, imposed on the fibre.

4. POLARISATION DRIFT MEASUREMENT

We have monitored the polarisation drift in the trackside fibre, using the setup given in the Fig.1(a). Continuous wave (CW) laser light was injected to the trackside fibre in a loop back configuration. The polarisation states of the received light were measured in the horizontal (H)/vertical (V) basis and also in the diagonal (+45)/anti-diagonal (-45) basis, using a 50/50 beam-splitter (BS), polarisation beam-splitters (PBS) and a half-wave polarisation rotator ($\lambda/2$), as shown in the Fig..1 (a). A data acquisition module logged the photo-diode outputs, as shown in the Fig..1(b). We have observed that the movements of the trains cause small spikes in the states of the polarisation. However, these are negligible in comparison to the slow polarisation drifts caused by the temperature changes in the fibre. Therefore, we infer that the movements of the trains have a negligible effect on the polarisation, as the fibre cables are securely positioned in concrete cable route, typically 1m-2m away from the railway tracks.

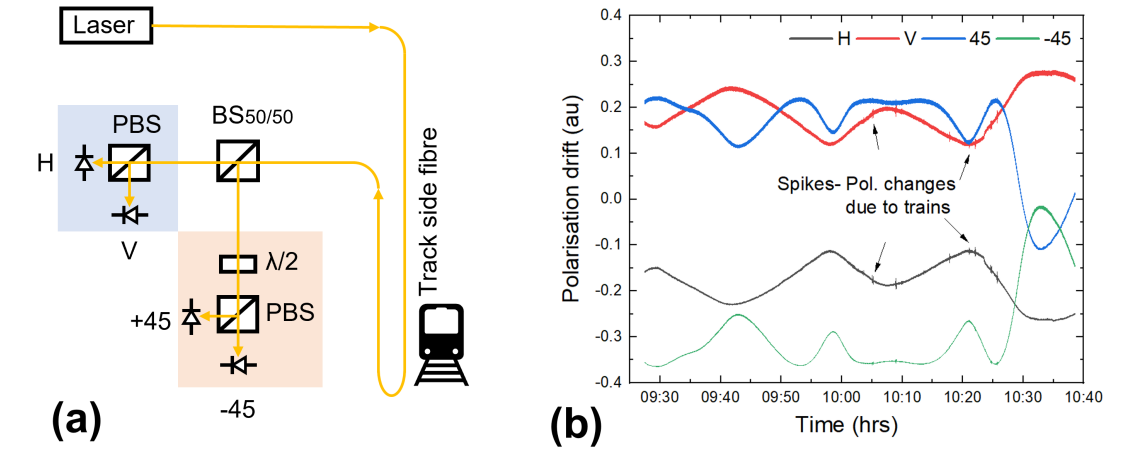

Figure 1. (a) Setup for monitoring the polarisation drift in trackside fibre. (b) Polarisation drift over a period of time.

5. CVQKD FIELD DEPLOYMENT OVER TRACKSIDE FIBRE

Following the polarisation test, we have performed the CVQKD field trial over the trackside fibre. The CVQKD Alice was connected to Bob over a 49.82km fibre channel that runs between RIDC, at Asfordby and Syston railway station, in a loop back configuration (12.9dB total transmission loss, including patching losses at trackside cabinets), as shown in Fig.2(b). Fig.2(a) shows the CVQKD optical setup. In our CVQKD system, Alice

generated 100ns, 1550nm wavelength, laser pulses at 1MHz repetition rate. A weak portion of the pulse was amplitude and phase modulated for the GMCS protocol and attenuated to signal variance, $V_A = 13N_0$. The signal and intense local oscillators(LO) were polarisation and time multiplexed at Alice and demultiplexed at Bob. Bob measured one of the quadratures of the coherent state sent by Alice, using a shot-noise limited homodyne detector. A portion of the LO was used to generate a clock, for homodyne detection data acquisition. We applied a gradient descent algorithm for correcting the polarisation drift, by using a DPC. The CVQKD run initialized with the calibration of the electronic noise, followed by the DPC maximising the quadrature correlation between Alice and Bob. The shot-noise variance was estimated in real time, by Bob measuring the homodyne output in the absence of signal from Alice. The channel parameters were estimated from Eq.(1) and Eq.(2) and if the

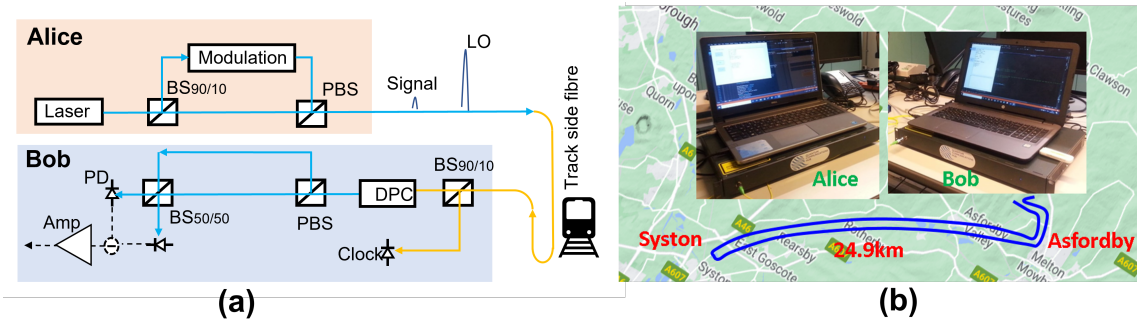

Figure 2. (a) Optical setup of the CVQKD system. (b) Field demonstration of CVQKD over the trackside fibre

excess noise, ξ, was below the null key threshold, the secure key rate was estimated. However, if the excess noise exceeded the null key threshold, the DPC routine was actioned, to maximise the quadrature correlation. We used binary slice mapping for digitising the quadrature data, and CASCADE error correction and Toeplitz-based privacy amplification for generation of the final secure key, at 4kbps, over 49.82km of fibre. The classical data processing was effected over the Ethernet cables directly connected between the two PCs representing Alice and Bob. These PCs were remotely accessed over the virtual network for CVQKD initialisation, monitoring and trouble-shooting purposes. In conclusion, we have identified that the effect of trains on the trackside fibre has negligible impact on the performance of the CVQKD. We have demonstrated that the CVQKD can be made to work across the existing railway trackside fibre network, in the UK.

ACKNOWLEDGMENTS

The authors acknowledge funding support from the Univerity of York's EPSRC impact accelerator account (grant number EP/R51181X/1) and the EPSRC Quantum Communications Hub (Grant number EP/T001011/1).

REFERENCES

[1] Grosshans, F. and Grangier, P., "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.* **88**, 057902 (2002).

[2] Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N. J., and Grangier, P., "Quantum key distribution using gaussian-modulated coherent states," *Nature* **421**, 238–241 (Jan. 2003).

[3] Leverrier, A. and Grangier, P., "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Phys. Rev. Lett.* **102**, 180504 (May 2009).

[4] Weedbrook, C., Lance, A. M., Bowen, W. P., Symul, T., Ralph, T. C., and Lam, P. K., "Quantum cryptography without switching," *Phys. Rev. Lett.* **93**, 170504 (Oct 2004).

[5] Jouguet, P., Kunz-Jacques, S., Debuisschert, T., Fossier, S., Diamanti, E., Alléaume, R., Tualle-Brouri, R., Grangier, P., Leverrier, A., Pache, P., and Painchault, P., "Field test of classical symmetric encryption with continuous variables quantum key distribution," *Opt. Express* **20**(13), 14030–14041 (2012).

[6] Qi, B., Lougovski, P., Pooser, R., Grice, W., and Bobrek, M., "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," *Phys. Rev. X* **5**, 041009 (Oct 2015).