High Speed Quantum Key Distribution for Smart City Distances with Data Multiplexing

Ketaki A. Patel[1,3], Iris Choi[1], James F. Dynes[1,2], Andrew W. Sharpe[1], Alexander R. Dixon[1,2], Zhi L. Yuan[1,2], Richard V. Penty[3] and Andrew J. Shields[1,2]

1. *Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, UK*
2. *Corporate Research & Development Center, Toshiba Corporation, 1 Komukai-Toshiba-Cho, Saiwai-ku, Kawasaki 212-8582, Japan*
3. *Cambridge University Engineering Department, 9 JJ Thomson Ave, Cambridge, CB3 0FA, United Kingdom*

iris.choi@crl.toshiba.co.uk

1. Introduction

To maintain a sustainable urban development, many metropolitan areas have adopted the 'Smart City' model [1]. It is a strategic concept where a city provides its inhabitants the availability of knowledge communication by means of Information and Communication Technologies (ICTs). Infrastructures and services such as transport, waste management, power distribution and utilities can be monitored by the ICTs and efficiently distributed to each inhabitant to minimise waste of manpower and resources (Figure 1). As the Smart City model relies heavily on information transfer, information security is of utmost importance. Quantum Key Distribution (QKD) [2,3] is an unique technology for providing encryption keys between remote parties with a directly quantifiable security [4]; therefore it would be highly desirable to combine QKD with classical information transfer in a Smart community. QKD in the presence of classical data traffic has been demonstrated by [5-8], however the secure key rates and transfer distances are far too low for broadband applications over Smart City distances (typically ranging from 30km to 80km [1]). For example, a conferencing video would usually require 256kbit/s secure key for one time pad encryption. The low quantum key transfer rate is primarily limited by the low single photon detection rate. With the novel self-differencing (SD) technique [9], GHz gating of the single photon detectors is possible, therefore allowing high speed quantum keys to be created for high bandwidth applications. Here in this paper, we present the first QKD system demonstration with sufficient secure key rate for one time pad encryption of video conferencing applications over metropolitan fibre distances. Secure keys in presence of error free classical data are demonstrated for distances up to 90km. This demonstration is the first step towards enabling utmost secure data exchange for Smart City distances. We anticipate such demonstration will increase the level of confidence towards ICT infrastructures.

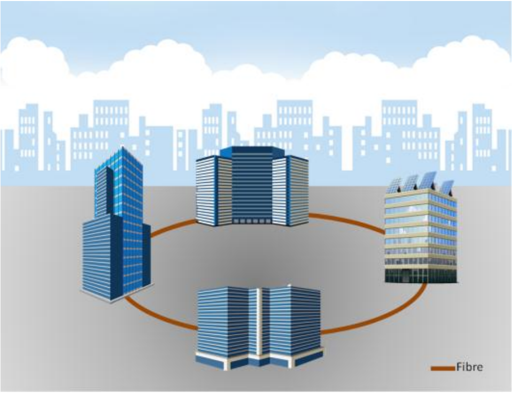

Figure 1: Information transfer in a Smart City secured by quantum key distribution

2. Challenges

To lower the operational cost, the QKD channels should share the same fibre architecture as used by the conventional channels. In practice this is challenging to realise owing to the large intensity contrast between the QKD channels and the conventional data channels. In conventional Gb/s data communication, millions of photons are present in each optical pulse. On the other hand, QKD channels use optical pulses in the single photon regime. When significant light is injected into optical fibre eg. for conventional data transmission, various scattering mechanisms occur. These can strongly scatter into the QKD channels increasing the QKD channel noise. Spontaneous Raman scattering is an inelastic process where single wavelength incoming photons interact with the optical phonons of silica glass fibre to generate new photons at different energies (hence wavelength). As an amorphous material, silica glass has a large number of phonon modes available for scattering, and therefore the scattered photons have a wide range of energies. Figure 2a shows a typical Raman scattered spectrum, covering over 200nm of spectral window.

Figure 2b shows the length dependence of Raman scattering. Signals at 1570nm, 1590nm and 1610nm are launched into SMF-28 fibre. Their relative scattered strength can be deduced from the spectral shape of the

Raman spectrum as shown in Figure 2a. Spontaneous Raman scattering exhibits different fibre length dependences in the forward and backward directions. In the forward direction, the Raman power increases initially with fibre length and gradually decreases as the signal power is attenuated by accumulated fibre loss. In the backward direction, the Raman power increases initially and reaches a plateau. When viewing in the backward direction, the strongest Raman power is generated by the first section (~30km) of the optical fibre. Fibre sections that are far from the beginning of the fibre contribute negligibly as all back-scattered Raman photons are attenuated as they travel towards the beginning of the fibre to be detected.

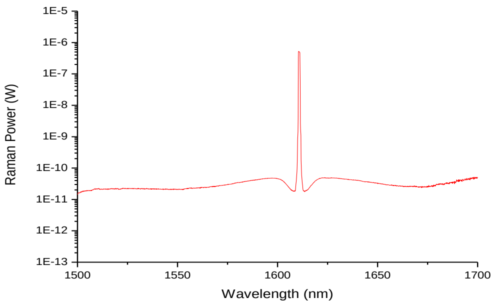

Figure 2a: Spontaneous Raman spectrum from a 0dBm 1610nm signal

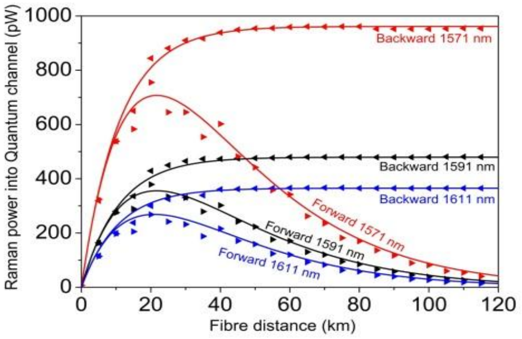

Figure 2b: Length dependence on spontaneous Raman spectrum. (Symbols represent measured data and lines represents calculations)

3. Experimental Set-up

Our GHz QKD system is of the decoyed BB84 type employing phase encoding which has been reported previously [10]. Figure 3 shows a simplified schematic of the experimental arrangement.

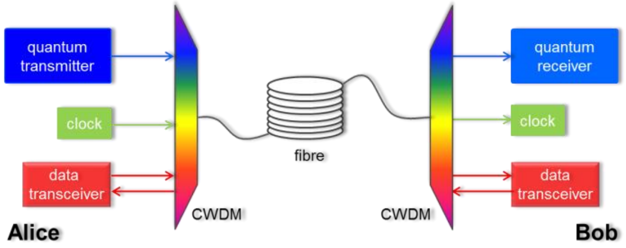

Figure 3: Experimental Setup

The classical signal which includes an optical synchronisation clock and two data channels is transmitted simultaneously over the same fibre as the quantum channel. Coarse Wavelength Division Multiplexing (CWDM) was chosen for data multiplexing. With the large filter spacing (20nm) and passband (13nm), the CWDM technology is designed to cope with the wide wavelength drift with temperature associated with cheap, uncooled lasers, where power-consuming thermo-electric cooling circuitry is not required.

Standard CWDM channels at 1571nm, 1591nm and 1611nm are used for optical synchronisation and data communication. The optical synchronisation clock signal is transmitted from Alice to Bob. A photo-receiver at Bob recovers this clock to synchronize his optics and electronics. In addition, to simulate Smart City applications, two classical data channels are implemented for bidirectional 1.25Gbit/s Ethernet transmission. The two data channels are provided by commercially available small form-factor pluggable (SFP) transceivers.

4. Results and Discussions

To mitigate the effect of Raman scattering, the launch powers of data transmitters are minimised while maintaining error-free classical communication. For example, at 80 km, the launching power was set at −19dBm for the 1611nm data signal. The bit error rate is measured to be $<10^{-11}$ (Fig. 4a). Furthermore, a narrow bandpass filter is inserted in the quantum channel after the CWDM for further rejection of the Raman photons, see Fig. 4(b).

Figure 5 shows the fibre length dependence of the QKD raw and secure key rates, and the quantum bit error ratio (QBER). Theoretical simulation, which includes the effect of the classical signals, is also shown. The measured QBER agrees well with the simulation. The presence of the classical signals does not deteriorate the

QBER strongly for the distances studied. Here, the measured QBER at 50km is dominated by modulation errors, afterpulses and dark counts at 50km. At 80km, the Raman scattering starts to impact the QKD transmission.

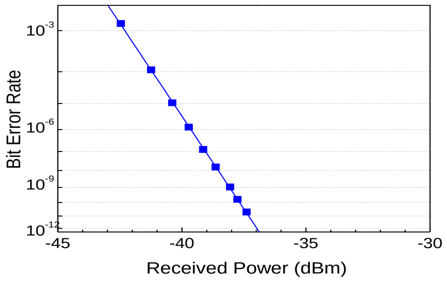

Figure 4a: Bit error rate measurement for the 1611nm data channel.

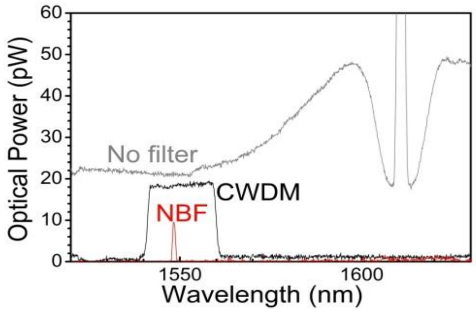

Figure 4b: Raman spectrum measured with various filters. (NBF= Narrow Bandpass Filter)

The measured key rates are in excellent agreement with the theoretical simulation. We have obtained a secure key rate of 507k, 68k and 7.6kbit/s for 50, 80 and 90 km transmission respectively. The key rates demonstrated here are orders of magnitude higher than previously reported for QKD systems multiplexed with classical communication [6,7].

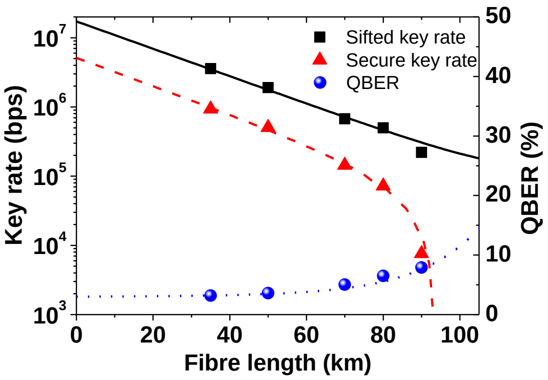

Figure 5: QKD raw key rate, secure key rate and QBER as a function of fibre distance. Symbols are measured values while lines are theoretical simulation.

5. Summary

We report the operation of a gigahertz clocked quantum key distribution system, with three classical channels using coarse wavelength division multiplexing over a fibre distance up to 90km. A secure key rate of 507kbit/s and 7.6kbit/s is achieved in presence of classical communication channels over 50km and 90km respectively. This secure key rate is sufficient to support high bandwidth encryption applications, such as conferencing video (typically 256kbit/s), over a metropolitan distance of 50km. This result shows the potential of using QKD to enable utmost security over 'Smart City' applications.

References

1. Canada: http://stratfordsmartcity.ca/2012/01/fibre-comes-home/; USA : http://chattanoogagig.com/; http://www.wired.com/epicenter/2011/01/internet-meets-smart-grid/
2. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing*, Bangalore India, 175-179 (1984).
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," Rev. Mod. Phys. **74**(1), 145-195 (2002).
4. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. N. Lütkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," Rev. Mod. Phys. **81**(3), 1301-1350 (2009).
5. P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength division multiplexing", Electron. Lett. 33, 188-190, (1997).
6. N. A. Peters *et al.*, "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments", New J. Phys. **11**, 045012 (2009).
7. P. Eraerds *et al.*, "Quantum key distribution and 1 Gbps data encryption over a single fibre", New J. Phys. **12**, 063027 (2010).
8. I. Choi, R. J. Young and P. D. Townsend, ''Quantum Information to the Home'', N. J. Phys. **13** 063039 (2011)
9. Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, '"High speed single photon detection in the near infrared," Appl. Phys. Lett. **91**(4), 041114/1-3 (2007)
10. A. R. Dixon *et al.*, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate", Opt. Express **16**, 18790 (2008).