

Quantum key distribution on a 10Gb/s WDM-PON

Iris Choi*, Robert J. Young and Paul D. Townsend

Photonic Systems Group, Tyndall National Institute and Department of Physics,
University College Cork, Cork, Ireland
*iris.choi@tyndall.ie

Abstract: We present the first demonstration of quantum key distribution (QKD) on a multi-user wavelength division multiplexed passive optical network (WDM-PON) with simultaneous, bidirectional 10Gb/s classical channel transmission. The C-Band QKD system operates at a clock rate of 10GHz and employs differential phase shift keying (DPSK). A dual feeder fiber and band filtering scheme is used to suppress classical to quantum channel cross-talk generated by spontaneous Raman scattering, which would otherwise prevent secure key distribution. Quantum keys were distributed to 4 users with negligible Raman cross-talk penalties. The mean QBER value for 4 users was 3.5% with a mean raw key distribution rate of 1.3Mb/s, which decreased to 696kb/s after temporal windowing to reduce inter-symbol interference due to single photon detector timing jitter.

©2010 Optical Society of America

OCIS codes: (270.5568) Quantum Cryptography; (060.0060) Quantum Communications.

References and links

1. C. H. Bennett, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, (IEEE New York), pp. 175–179 (1984)
2. C. Marand, and P. D. Townsend, "Quantum key distribution over distances as long as 30km," *Opt. Lett.* **20**(16), 1695–1697 (1995).
3. P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electron. Lett.* **33**(3), 188–190 (1997).
4. C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.* **84**(19), 3762–3764 (2004).
5. R. J. Hughes, and J. E. Nordholt, D. Derkacs and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *N. J. Phys.* **4**(43), 1–14 (2002).
6. D. Stucki, N. Gisin, and O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *N. J. Phys.* **4**(41), 1–8 (2002).
7. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Phys. Rev. Lett.* **98**(1), 010504 (2007).
8. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nat. Phys.* **3**(7), 481–486 (2007).
9. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nat. Photonics* **1**(6), 343–348 (2007).
10. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauwerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," *N. J. Phys.* **11**(7), 075001 (2009).

11. P. D. Townsend, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, "Design of quantum cryptography systems for passive optical networks," *Electron. Lett.* **30**(22), 1875–1876 (1994).
12. P. D. Townsend, "Quantum cryptography on multi-user optical fibre networks," *Nature* **385**(6611), 47–49 (1997).
13. V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, "Passive Optical Network Approach to Gigahertz-Clocked Multiuser Quantum Key Distribution," *IEEE J. Quantum Electron.* **43**(2), 130–138 (2007).
14. P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of Four Multi-User Quantum Key Distribution Schemes Over Passive Optical Networks," *J. Lightwave Technol.* **23**(1), 268–276 (2005).
15. D. Subacius, A. Zavriyev, and A. Trifonov, "Backscattering limitation for fiber-optic quantum key distribution systems," *Appl. Phys. Lett.* **86**(1), 011103 (2005).
16. P. Toliver, R. J. Runser, T. E. Chapuran, S. McNown, M. S. Goodman, J. Jackel, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallman, "Impact of Spontaneous Anti-Stokes Raman Scattering on QKD+DWDM Networking," in *Proceedings of Lasers and Electro-Optics Society (LEOS)*, vol. **2**, pp. 491–492 (2004).
17. N. I. Nweke, P. Toliver, R. J. Runser, S. R. McNown, T. E. Chapuran, M. S. Goodman, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann, "Experimental Characterisation of Wavelength Separation for 'QKD+WDM' Co-existence," in *Proceedings of Conference on Lasers and Electro-Optics (CLEO)*, vol. **2**, pp.1503–1505 (2005), paper CW06.
18. T. J. Xia, D. Z. Chen, G. Wellbrock, and A. Zavriyev, A. Beal and K. M. Lee, "In-Band Quantum Key Distribution (QKD) on Fiber Populated by High-Speed Classical Data Channels," in *Optical Fiber Communication Conference and Exposition and The National Fiber Optic Engineers Conference*, Technical Digest (Optical Society of America, 2006), paper OTuJ7.
19. N. A. Peters, P. Toliver, T. E. Chapuran, R. J. Runser, S. R. McNown, C. G. Peterson, D. Rosenberg, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, and K. T. Tyagi, "Dense Wavelength multiplexing of 1550nm QKD with strong classical channels in reconfigurable networking environments," *N. J. Phys.* **11**(4), 045012 (2009).
20. ITU Standard G.694.1 (06/02), "Spectral grids for WDM applications: DWDM frequency grid," International Telecommunication Union (2002).

1. Introduction

Quantum cryptography, or quantum key distribution (QKD), offers the potential for secure cryptographic key distribution with secrecy guaranteed by quantum mechanics [1]. This opens the intriguing possibility of communication systems that rely solely on fundamental physical laws for security provision without recourse to the (often unproven) principles of mathematical complexity that underpin much of today's cryptographic technology. Much of the research on practical QKD systems has focused on extending the transmission distance of both point-to-point optical fiber and free-space optical links, with the goal of establishing national- or global-scale networks for secure key exchange and management [2–10]. Up to now, comparatively less attention has been given to the problem of developing QKD for the access networks that would be required to link end-users to these secure network infrastructures. In principle, a wide range of access network topologies are feasible for QKD [11–14], but it is highly likely that standardized schemes developed primarily with the needs of conventional high speed communications will ultimately provide the lowest cost and hence most practical solutions. In this paper we focus on one leading topology, which is known as the wavelength division multiplexed passive optical network (WDM-PON). As illustrated in Fig. 1, these virtual point-to-point networks enable the connection of end-users to central network nodes using a purely passive fiber and filter plant with no intervening electronic switches or routers. Each user is allocated a pair of dedicated wavelengths; one for upstream (US) communications (from the user) and one for downstream (DS) communications (to the user). Arrayed waveguide grating (AWG) routers are used to multiplex/demultiplex signals entering the feeder fiber, and the AWG in the remote node has a cyclic property that enables each output port to pass multiple wavelengths corresponding to the different diffraction orders of the device. Consequently, only a single drop fiber needs to be connected to each user to support US and DS communications, which reduces cost. The WDM-PON has the advantage over other architectures, such as power splitter PONs, of offering substantial, uncontended bandwidth per user. Here we propose a new type of ultra-secure WDM-PON in which the

cyclic property of the AWG is further exploited in order to add an additional QKD wavelength channel for each user for encryption purposes.

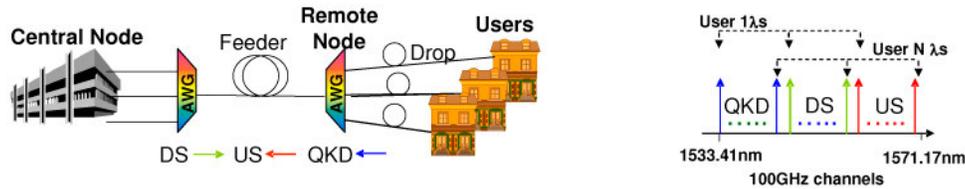


Fig. 1. WDM-PON access architecture and cyclic wavelength plan supporting N users.

The major challenge with the proposed scheme is how to achieve co-existence of the high power classical channels and low power quantum channels with sufficiently low cross-talk that the QKD system can operate securely at low error rate (typically a few percent in practice). In a standard WDM-PON, the classical channels operate at power levels of around 1mW per channel, or approximately 10^6 photons/bit at 10Gbit/s. This is nearly 7 orders of magnitude higher than the 0.2 photons/bit typically employed for a weak coherent pulse QKD scheme. As will be demonstrated, it is possible to reduce cross-talk due to filter leakage to negligible levels using standard AWGs and filters. However, some of the photons in the conventional channels will undergo spontaneous inelastic Raman scattering, which is generated symmetrically in both the forward and reverse directions over a spectral width of $>240\text{nm}$ [15]. Unless suitable mitigation schemes are employed the resulting Raman cross-talk will prevent QKD. Detailed studies on the impact of spontaneous Raman scattering on QKD systems can be found in [15,16]. A number of solutions that enable the interworking of QKD with C-band (1530nm-1565nm) Dense Wavelength Division Multiplexed (DWDM) point-to-point systems have been demonstrated to date. These include placement of the QKD channel in the O-Band region around 1300nm [17], which is outside of the Raman spectrum generated by C-band classical channels, and the use of non-standard, or additional, narrow-band filters with a high out-of-band blocking ratio to reduce Raman cross-talk for QKD channels located in the C-band [16–19]. These solutions are not ideal for WDM-PONs where infrastructure costs are shared across a relatively small number of users. In this case it is imperative to reduce costs by using standardized telecom components and multiplexing schemes if possible (for example, the DWDM grid adopted by the International Telecommunication Union [20] is not defined in the O-Band). Here we introduce a simple, but highly effective scheme which uses a second shared feeder fiber to significantly reduce the effects of Raman. The scheme has enabled the first demonstration of QKD on a high speed (10Gb/s) WDM-PON.

2. Spontaneous Raman scattering theory

The main factor preventing the coexistence of quantum and classical channels in DWDM systems is spontaneous Raman scattering. In order to understand the effects of Raman we first consider the propagation of a single classical channel in a fiber link, and then generalize to the case of a WDM-PON, which supports the bidirectional propagation of multiple classical channels. Figure 2 shows the back-scattering spectrum measured from a 25km length of standard single mode transmission fiber (SMF) using a 1540nm-wavelength, distributed feedback laser (DFB). The DFB launch power was set to 1mW (0dBm) to represent the typical launch power in conventional short-haul systems, which is more than an order of magnitude below the threshold for stimulated Raman scattering. The spontaneous, inelastic scattering process converts photons from the conventional classical channel into a broad band of wavelengths approximately 240nm wide, which covers the entire C band and is centered on the classical channel. The spectrum consists of stronger Stokes- and weaker Anti-Stokes-lines

with structures characteristic of the Raman-active optical phonon-modes in amorphous Silica glass fiber [15].

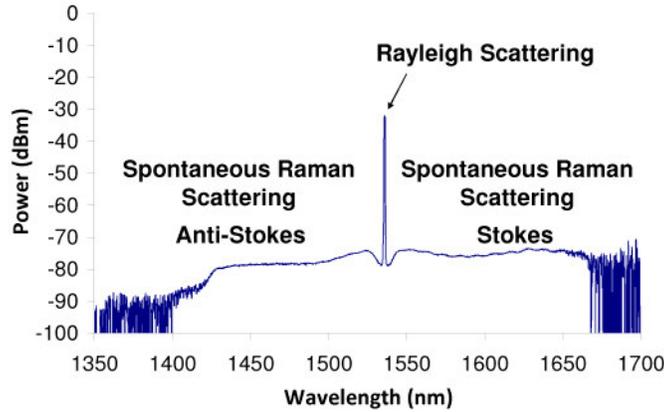


Fig. 2. Back- scattering spectrum taken with 25km of standard single mode transmission fiber with a resolution of 1nm. Discrete Rayleigh peak and broad spontaneous Raman bands were observed.

Spontaneous Raman scattering occurs in both the forward and backward directions. The back-scattered Raman power generated by a single classical channel in a transmission fiber can be obtained by integrating the contribution of each small length element over the fiber length, L , to give Eq. (1) [15]:

$$P_{RB} = \frac{P_C \beta(\lambda, \Delta\lambda)}{2\alpha} (1 - e^{-2\alpha L}), \quad (1)$$

where P_C is the classical channel launch power, α is the fiber attenuation coefficient, $\beta(\lambda, \Delta\lambda)$ is the linear spontaneous Raman scattering coefficient, which is dependent on wavelength (λ) and the measurement bandwidth ($\Delta\lambda$). Similarly, the forward-scattered Raman power can be described by Eq. (2) [19]:

$$P_{RF} = P_C e^{-\alpha L} L \beta(\lambda, \Delta\lambda) \quad (2)$$

As can be seen from Fig. 2, the Raman scattering coefficient $\beta(\lambda, \Delta\lambda)$ varies with wavelength and filter bandwidth, in particular, is smaller on the short wavelength side of the classical channel. Taking typical values of $\alpha=0.046 \text{ km}^{-1}$ (0.2dB km^{-1}) and $\beta=2.1 \times 10^{-9} \text{ km}^{-1}$ (see below) and assuming a value of $P_C=1\text{mW}$ (a typical practical value for WDM-PON applications) we calculate back- and forward-scattered powers as a function of fiber length. As we shall be concerned with the level of cross-talk noise that the Raman scattering generates in a given quantum channel, the results shown in Fig. 3 are represented in the form of a count rate, modelled by assuming an AWG measurement filter and a single photon detector with the same characteristics as those used in the experiments detailed later in this paper. For distances up to approximately 10km, which are relevant for WDM-PON applications, the backward and forward Raman levels are essentially identical. However for longer distances the backward Raman shows saturation behaviour, whilst the forward reaches a maximum value at $1/\alpha$ ($\sim 21.7\text{km}$) then decreases exponentially as the fiber attenuation reduces the scattered signal more quickly than it can be replenished by the classical channel [19].

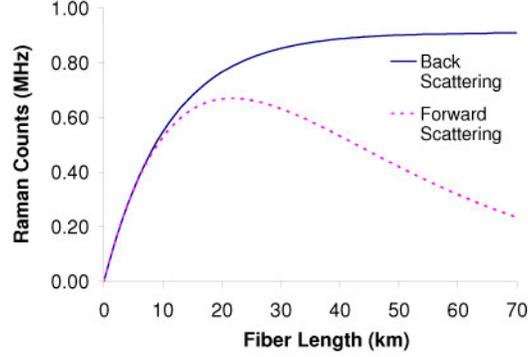


Fig. 3. Modelled fiber length dependence for Back- and Forward- Spontaneous Raman Scattering in single transmission fiber

Turning now to the case of a WDM-PON of the type shown schematically in Fig. 1, we calculate the Raman power generated by the multiple upstream (US) and downstream (DS) classical channels that fall within each quantum channel AWG pass-band. As will be explained further in section 3, the quantum channels were chosen to co-propagate with the US channels since this configuration employs the filtering effect of an AWG to only allow Raman photons within the AWG channel bandwidth of 0.4nm to pass, hence giving the lowest levels of Raman cross-talk. We amend Eqs. (1) and (2) to take into account the multiple classical channels (US and DS), the separate contributions of the feeder and drop fibers and explicitly include the loss and Gaussian filtering effects of the AWGs at the central and remote nodes.

The expression for the Raman power at the output port of the i^{th} quantum channel in the central node AWG due to back-scattering from the DS channels is given by Eq. (3):

$$P_{RBi} = P_{DS} \frac{\sum_{j=1}^N \beta_{ij}(\lambda, \Delta\lambda)}{2\alpha} (1 - e^{-2\alpha L_F}) A + P_{DS} e^{-2\alpha L_F} \frac{\beta_{ij(j=i)}(\lambda, \Delta\lambda)}{2\alpha} (1 - e^{-2\alpha L_D}) A^3 F, \quad (3)$$

where N is the total number of DS channels (one per user), P_{DS} is the DS channel launch power into the feeder fiber after the AWG in central node (assumed to be equal for all channels), L_F and L_D are, respectively, the feeder and drop fiber lengths, A is the AWG insertion loss and F is the additional loss arising for broadband light double passing the AWG filter. The latter is assumed to be Gaussian with full width half maximum (FWHM) equal to $\Delta\lambda$. For the 100GHz channel spacing AWGs used in the experiments $\Delta\lambda = 0.4\text{nm}$, $F = 0.7527$ and $A = -4\text{dB}$.

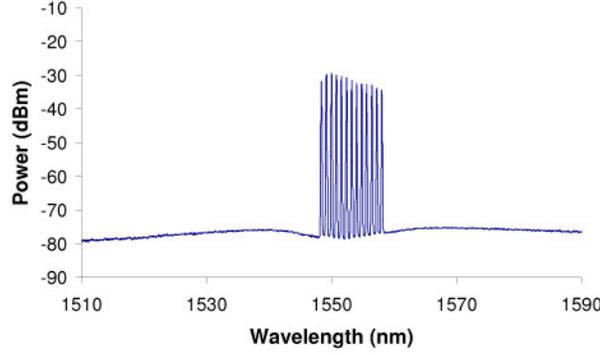


Fig. 4. Experimental spontaneous Raman spectrum taken with resolution of 0.1nm, for 13DS lasers in a WDM-PON with 8km feeder fibre

Two main assumptions are used in deriving Eq. (3). Firstly, the Raman spectrum is approximately flat over the AWG pass-band so a single-valued parameter $\beta_{ij}(\lambda, \Delta\lambda)$ can be used to describe the scattering from the j^{th} classical channel into the i^{th} quantum channel. This assumption is supported by Fig. 4 where a Raman spectrum from 13 DS lasers in a WDM-PON configuration is shown. Evidently, across the AWG channel passband of 0.4nm, the accumulated Raman is relatively featureless and constant. Secondly, the AWG out-of-band crosstalk is negligible so that only Raman generated within the wavelength pass-band of the i^{th} quantum channel contributes noise to the i^{th} quantum channel receiver. These approximations are well-satisfied in practice. Equation (3) consists of two terms. The first term describes Raman generated in the feeder fiber, which is filtered once by the central node AWG. The second term describes the Raman generated in the drop fiber, which is doubly filtered; firstly by the remote node AWG and secondly by the central node AWG. It is evident from Eq. (3) that the dominant contribution to the back-scattered Raman comes from the feeder fiber, since all N DS channels contribute to this term. In contrast, the drop term contains a contribution from only one DS channel, because only Raman from the i^{th} user's drop fibre will reach the i^{th} quantum channel receiver due to the filtering action of the remote node AWG. The drop term is also further attenuated with respect to the feeder term by the loss of the remote node AWG and transmission loss of the feeder fiber.

Similarly, the expression for the Raman power at the output port of the i^{th} quantum channel due to forward-scattering from the US channels is given by Eq. (4):

$$P_{RFi} = P_{US} e^{-\alpha(L_f + L_D)} L_D \beta_{ik(k=i)}(\lambda, \Delta\lambda) A^2 F + P_{US} e^{-\alpha(L_D + L_f)} L_F \sum_{k=1}^N \beta_{ik}(\lambda, \Delta\lambda) A^2, \quad (4)$$

where P_{US} is the US channel launch power and the other parameters are as defined above, with $\beta_{ik}(\lambda, \Delta\lambda)$ describing the scattering from the k^{th} US classical channel into the i^{th} quantum channel (note $i=j=k=1$ for user 1 and so on). The first term describes the Raman contribution from the drop fiber while the second term describes Raman from the feeder fiber. As is the case for Eq. (3), the feeder term is dominant since it contains contributions from all N US channels. This suggests that if the feeder fiber scattering can be suppressed, a significant reduction in Raman cross-talk from both US and DS channels is feasible. In the following sections we quantify the level of Raman cross-talk in a practical WDM-PON, show that such noise suppression is required for QKD and introduce a dual feeder fiber and band filtering scheme that allows it to be achieved.

3. Experimental set-up

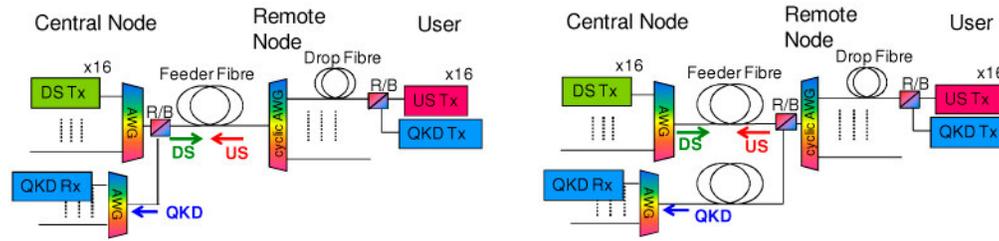


Fig. 5. Schematic for single feeder fiber (left) and dual feeder fiber (right) architecture

Two experimental configurations were used; a conventional single feeder scheme and the dual feeder design as illustrated in Fig. 5. For clarity, DS and US receivers (Rx) are not shown in the schematics. Both WDM-PON architectures comprised of: user, remote node, central node, feeder and drop sections. The total system span could be varied over the range 4-12km using different lengths of standard SMF fiber in order to represent typical access network transmission distances. The wavelength plan was based on a 1×16 , 100GHz channel spacing, cyclic AWG with a free spectral range of $\sim 13\text{nm}$, which was located at the remote node position. Hence, the network could potentially support up to 16 users ($i=1-16$), with each assigned 3 wavelengths, one each for US, DS and QKD: $\lambda_{\text{US}i}$ (1559.03nm-1571.17nm), $\lambda_{\text{DS}i}$ (1546.11nm-1558.16nm), and $\lambda_{\text{QKD}i}$ (1533.41nm-1545.36nm). As the anti-Stokes lines are weaker than the Stokes lines the quantum channels were placed on the shorter wavelength side of the DS or US channels to minimize Raman crosstalk [16,19]. At various points in the network low cost C-band splitting red/blue (R/B) filters were used to multiplex/demultiplex the QKD channel band with the US+DS channel bands. The R/B filters provided isolations of $>35\text{dB}$, directivities of $>60\text{dB}$ and had polarization dependent losses of $<0.5\text{dB}$. However, due to the finite width ($\sim 20\text{nm}$) of the red passband (long wavelength cut-off at 1563nm), it was not possible to accommodate all 16 DS and 16 US channels in the current experiment. This limited the maximum number of users supplied with all 3 wavelengths in the experiment to 4. Nevertheless, with optimized filters the network could be fully populated. At the user end, a R/B filter was used to multiplex the US and QKD channels into the drop fiber and also to suppress ($>35\text{dB}$) the Amplified Spontaneous Emission (ASE) from the US laser at $\lambda_{\text{QKD}i}$. A further dual stage R/B filter was used at the remote node to direct the QKD channels through the lower feeder fiber shown in Fig. 5, whilst the US and DS channels were carried by the upper feeder fiber. In the conventional single feeder configuration, this R/B filter was moved to the central node. At the central node, standard $40 \times 100\text{GHz}$ channel spacing Gaussian pass-band, AWGs were used to multiplex/demultiplex the US, DS and QKD channels. The AWG filters used in experiments had channel isolations of $>45\text{dB}$ between the QKD and the DS and US channels and polarization dependent losses $<0.5\text{dB}$. For the dual feeder scheme as shown in Fig. 5, for example, this gives a total isolation figure of $>105\text{dB}$ for DS and $>115\text{dB}$ for US, which is large enough to ensure that leakage from the DS or US channels into the QKD channels, either directly or via Rayleigh backscattering, is negligible ($<0.1\%$ of expected QKD counts) All AWGs were temperature controlled to maintain wavelength channel alignments.

Figure 6 shows a detailed diagram of the dual feeder setup. Tunable external cavity lasers (ECLs) were used as sources for the US channels, one of which was externally modulated by an Electroabsorption Modulator (EAM) driven by a 10Gb/s 2^7-1 non-return-to-zero (NRZ) pseudo-random bit sequence (PRBS) generated by a pulse pattern generator (PPG). The US signal was detected by a PIN receiver (Rx) and a 10GHz clock recovery circuit. The DS channels were emulated by a bank of DFBs (13 were available), which were externally modulated using a Lithium Niobate Mach-Zehnder Modulator (MZM) driven by a 10Gb/s NRZ $2^{31}-1$ PRBS. The DS signal was detected at the user via a circulator and PIN Rx. The

mean US and DS fiber launch powers were set to typical practical values of 0dBm per channel to ensure realistic levels of Raman cross-talk.

The quantum channel source was a tunable ECL, which was data encoded by a phase modulator (PM) driven by 10Gb/s 2^7-1 NRZ PRBS to generate a sequence of 0 and π phase shifts in a differential phase shift keyed (DPSK) QKD scheme [9]. Although a short PRBS was used for test purposes in the experiments, a fully-implemented QKD system would require a truly random bit sequence [1]. The PM output was then pulse-carved by a MZM driven by the 10GHz clock from the PPG to generate a sequence of ~ 45 ps duration, return-to-zero (RZ) pulses. Prior to transmission, the QKD source was attenuated to the single photon level, with mean photon numbers μ of 0.2 photons/pulse. At the central node, a one-bit-delay Asymmetric Mach-Zehnder Interferometer (AMZI) (~ 2 dB insertion loss) and a pair of superconducting single photon detectors (SSPDs) with mean detection efficiencies of 1.2% and dark count rates of less than 150Hz were used to detect the DPSK QKD signals. Analysis of the output photocount sequence was performed by a Time Interval Analyzer (TIA), which was synchronized to the QKD transmitter via the divided clock (78.1MHz) recovered from the 10Gb/s US channel.

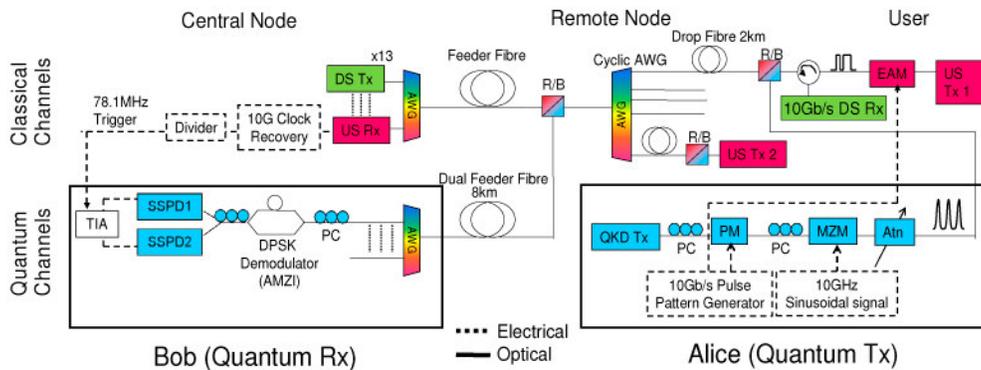


Fig. 6. Experimental set-up (dual feeder case)

4. Experimental results and discussion

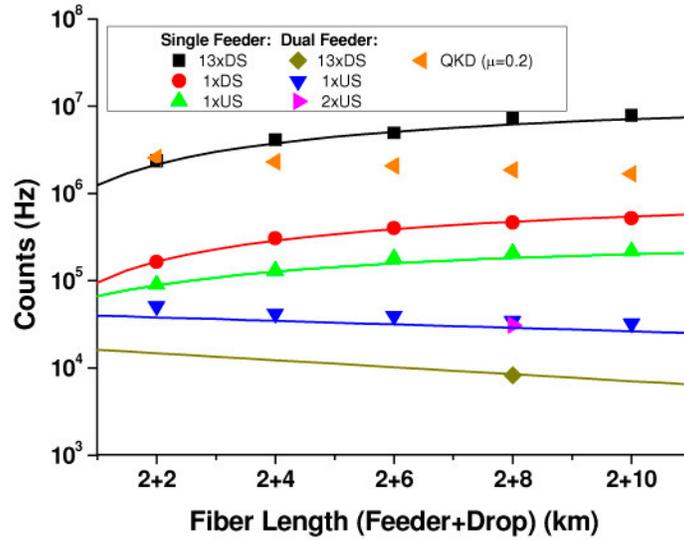


Fig. 7. Measured Raman & predicted QKD counts in single feeder and dual feeder configurations referenced to QKD Rx input shown as a function of total (feeder + drop) fiber length. The solid lines represent the length variation predicted by Eqs. (3) and (4).

Figure 7 shows the results of experiments that quantify the Raman cross-talk for the single and dual feeder fiber configurations via the count rate measured at the input to the DPSK demodulator using one of the SSPDs. The results are shown as a function of drop+feeder fiber length, and the US and DS channel contributions were evaluated separately. In order to gain a full understanding of the phenomena, the Raman was measured (at a QKD channel wavelength of 1535.79nm) for several different cases; including a single DS channel (1555.75nm), a single US channel (1559.79nm) and 13 DS channels (centered at 1553.33nm as shown in Fig. 4). The results for the single and dual feeder cases are quite distinct. In the single feeder case the Raman count is comparable to, or larger than, the predicted QKD channel count rate and increases with increasing feeder fiber length. For the dual feeder case, the Raman is significantly smaller than the QKD count rate and decreases with increasing feeder fiber length. These observations are consistent with the predictions of Eqs. (3) and (4) as shown by the solid lines in Fig. 7 (only the drop terms are used in the dual feeder case). Raman scattering coefficients $\beta_{ij}(\lambda, \Delta\lambda)$ in the range $1.8 - 2.2 \times 10^{-10} \text{ km}^{-1}$ (depending on channel wavelength) were found to give excellent fits to the observed data for the single feeder fiber case. In the dual feeder case, the $\beta_{ij}(\lambda, \Delta\lambda)$ values obtained for the single feeder experiment were used with the drop terms in Eqs. (3) and (4) to simulate the curves shown by the lower two solid lines in Fig. 7. Again excellent agreement is obtained with the measured data. Other parameter values were as given above, but with the fiber loss α set to 0.23dB/km to represent the mean measured value including connector and splice losses.

For the single feeder case, the largest contribution to the cross-talk comes from the back-scattered Raman generated by the DS channels. As expected from Eq. (3), this increases approximately linearly with channel count and is 4.8 times larger than the predicted QKD channel photocount at the maximum transmission distance (2+10km) when all 13 DS channels are on. For a fully populated system with all 16 US and DS channels the total Raman count would be greater than the QKD count for all distances investigated, which clearly demonstrates that low quantum bit error rates (QBERs) would not be achievable in the single feeder system.

In contrast, in the dual feeder case, the back-scattered Raman generated by the DS channels and the forward-scattered Raman generated by the US channels, both in the upper feeder fiber, do not enter the lower feeder fiber. Hence, since there is no physical path available for these Raman components to reach the QKD Rx, they do not lead to cross-talk. Similarly, the forward-scattered Raman generated by the DS channels and the backward-scattered Raman generated by US channels in the feeder fibre are also blocked from entering the second feeder fiber by the high directivity of the R/B filter (>60dB) at the Remote Node. However, the back-scattered Raman generated by DS channels in the drop fiber does enter QKD Rx and its effect is described by the second term in Eq. (3). This contribution is negligible (<0.4% of expected QKD count rate, with only half of these counts on average leading to errors) as shown by the 13xDS data point for the 2+8km dual feeder fiber case in Fig. 7.. As a result, the forward-scattered Raman from the US in the drop fiber becomes the dominant contribution (described by the first term in Eq. (4)). This leads to a substantial reduction in total Raman count to a maximum of 2% of the expected QKD count rate, which should result in a small QBER penalty of ~1% (as on average only half of Raman counts lead to errors). The reduction is due partly to the fact that the drop fiber is generally shorter than the feeder and partly due to the fact that Raman originating in the drop fibre is attenuated by the loss of the Cyclic AWG at the remote node (4dB). However, the main difference arises from the filtering action of the latter, which ensures that for the i^{th} user, only the slice (FWHM ~0.4nm) of Raman centered at λ_{QKDi} generated by the user's US channel and drop fiber can pass through the assigned cyclic AWG port and reach the QKD Rx; Raman from all other users' US channels is blocked. Hence the addition of more users to the network does not increase the Raman cross-talk for any individual user. This conclusion is confirmed by the experimental point obtained with 2 US channels (users), which is the same as for the single US case within experimental error. The scheme retains the cost benefits of single fiber connections to end users and adds only a cost-shared element - the second feeder fiber - to the system.

The Quantum Bit Error Rate (QBER) is of central importance in a practical QKD system as it quantifies the efficiency with which the system can establish secret information. QBER is defined as the ratio of number of incorrect bits detected and the total number of bits received. In general, this quantity will be non-zero, even in the absence of an eavesdropper, due to a variety of imperfections that generate background errors in the system. For secure operation, QBER must be minimized. In this system, 3 factors contribute to QBER: optical imperfections, dark counts and Raman counts, as shown in Eq. (5):

$$QBER_{\text{Total}} = QBER_{\text{Opt}} + QBER_{\text{Darkcount}} + QBER_{\text{Raman}} \quad (5)$$

The dominant optical imperfections are associated with the DPSK modulation system at the QKD Tx and the Asymmetric Mach-Zehnder interferometer (AMZI) at the QKD Rx. As the interference visibility, V , of the AMZI is less than unity (>0.98 specified value) there is a finite probability that any given photon will be detected at the incorrect AMZI output port, leading to an error. This error probability, $QBER_{\text{opt}}$, can be represented by the quantity $\kappa=(1/2)(1-V)$, which shows that, with ideal phase modulation, the error contribution due to finite interference visibility should be less than 1%. However, in practice the optical system is further degraded by imperfect phase modulation, which arises from noise and distortion introduced by the 10Gb/s data generator, electrical drive amplifier and phase modulator. We include this contribution by means of an effective κ value, κ_{eff} , which represents the performance of the complete interferometric system under dynamic modulation conditions. The quantity κ_{eff} can be estimated from the DPSK data eye contrast ratio, $C=1/\kappa_{\text{eff}}$, measured at the QKD Tx before attenuation (Fig. 8). This results in a value of $C = 40(16\text{dB})$ corresponding to a mean κ_{eff} value and hence $QBER_{\text{opt}} = 2.5\%$. The second error contribution comes from the combined SSPD dark count rate, D . On average only half of the dark counts

generate errors. For this experiment, $D \sim 200$ counts per second, which is approximately 4 orders of magnitude smaller than the quantum channel photocount rate. As a result, $QBER_{\text{Dark}}$ gives a negligible contribution to the total QBER. The final error contribution comes from Raman counts. On average, only half of the Raman counts contribute to errors. From Fig. 7, $QBER_{\text{Raman}}$ is estimated to be $\sim 1\%$. Hence, $QBER_{\text{Total}}$ is expected to be $\sim 3.5\%$.

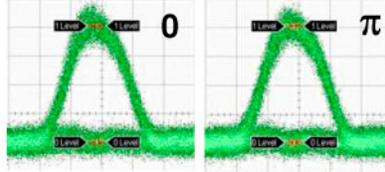


Fig. 8. DPSK eyes at QKD Rx outputs, both showing at least 16dB contrast ratio. (horizontal scale: 20ps per division)

For completeness, we show the detailed contributions to each error term in Eq. (6). The total photocount is given by $\eta\mu BR$, where η is the quantum efficiency of the SSPDs used, μ is the mean photon number, B is the total system loss and R is the QKD system clock rate (10GHz). Raman counts are generated by the combined contribution of back- and forward- scattered Raman. The total received Raman power for the dual feeder case can be calculated by adding P_{RBI} and P_{RFI} for all channels from the drop terms from Eqs. (3) and (4). To obtain the Raman count rate, the summed power should be divided by the photon energies for the given quantum channel, E_i . All other parameters are as defined above.

$$QBER_{\text{TOTAL}} = \frac{\kappa_{\text{eff}}\eta\mu BR + \frac{1}{2}\left[D + \frac{\eta(P_{\text{RBI}} + P_{\text{RFI}})}{E_i}\right]}{\eta\mu BR + D + \frac{\eta(P_{\text{RBI}} + P_{\text{RFI}})}{E_i}} \quad (6)$$

Following Raman evaluation, the set-up was configured as shown in Fig. 6 with 8km feeder and 2km drop fibers and QKD experiments were performed. Results were obtained for emulated users 1-4 with QKD wavelengths of 1535.79nm, 1536.58nm, 1537.38nm and 1538.18nm, respectively. Figure 9 shows a typical example of a photocount histogram measured at the one (constructive interference for π phase shift) port of the DPSK demodulator over 78.7×10^6 PRBS pattern repetitions. The contrast between the maxima (one) and deepest minima (zero) levels is high indicating the potential for low QBER transmission. However, significant Inter-Symbol Interference (ISI) can be inferred from the relatively shallow minima observed between consecutive ones. This arises from the limited instrumental response time of the single photon detection system. The latter is dominated by ~ 40 ps timing jitter of the SSPDs, which is a significant fraction of the 100ps bit period. To reduce the errors due to ISI, a windowing technique was used that rejected any counts occurring outside of the central τ ps of each bit period [9]. The QBER values for 1s long bursts of quantum data were then evaluated for different values of window width, τ , as shown by the results obtained for user 4 in Fig. 10. As τ decreases the QBER falls due to the reduction in ISI, which is lower in the central part of the data eye. Little improvement in QBER is obtained for τ values lower than 40ps so this window width was used for subsequent QKD experiments. The QBER results for emulated users 1-4 were: 2.9%, 3.7%, 3.9% and 3.6%, respectively. The resulting mean QBER value of 3.5% is in agreement with the expected value from the QBER analysis above. The QBER is mainly dominated by the dynamic interference contrast ratio in the system (2.5% contribution), with only $\sim 1\%$ arising from residual Raman generated mainly by the US channel. The mean QBER value is similar to the value of 4% achieved in [9] for a 200km a point-to-point DPSK QKD system with no DWDM classical channels. Our result demonstrates the effectiveness of the dual feeder scheme in reducing Raman cross-talk in the

system. For reference, the raw key distribution rate for user 1 was 1.3Mb/s, which decreased to 696kb/s following 40ps windowing.

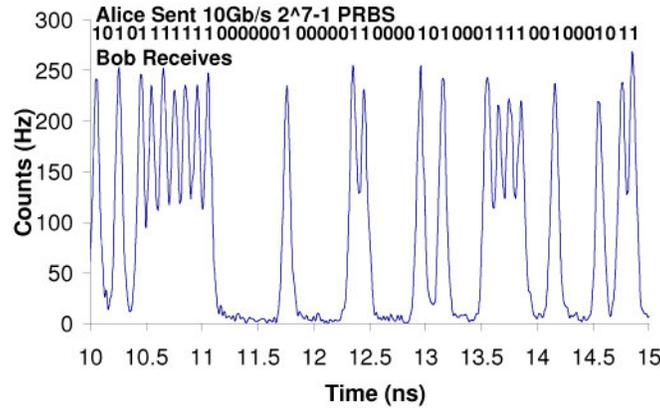


Fig. 9. Photocount histogram showing QKD data segment ($\mu = 0.2$). Quantum channel is coded with a 10Gbit/s 2^7 -1 PRBS pattern with 78.7M repetitions

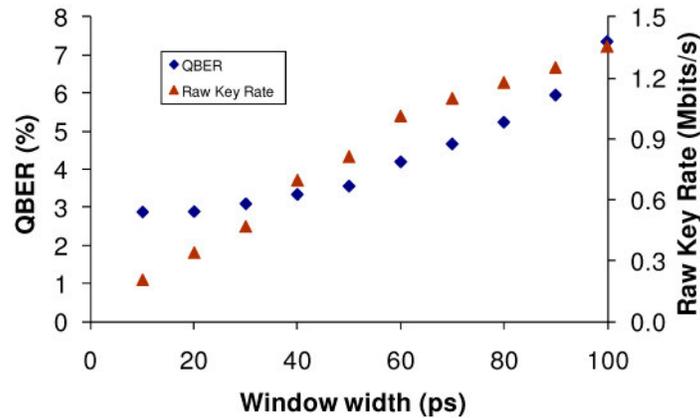


Fig. 10. QBER and raw key rate as a function of window width for user 4

To confirm correct operation of the classical channels, BER curves were taken for each of the 4 users in the back-to-back (B2B) case (without transmission fiber) and with 2+8km drop+feeder fibers. Figure 11(a) shows the BER measurements for the US channels while Fig. 11(b) shows those for the DS channels. A 10Gb/s PIN receiver with a relatively poor sensitivity of -15dBm (at $\text{BER}=10^{-10}$) was used to show the potential for low cost operation of the system. Relatively low power penalties of $\leq 1\text{dB}$ were observed and all channels were capable of error-free operation (defined as $\text{BER}<10^{-10}$). The minimum received power was -9.9dBm for both US and DS and the measured system margins were $>4\text{dB}$ and $>5\text{dB}$ for US and DS channels respectively. This indicates that the US and DS channel launch powers are sufficient for error-free operation of the classical part of the system with adequate margin for aging effects, and hence, that the Raman levels were not underestimated in the experiments.

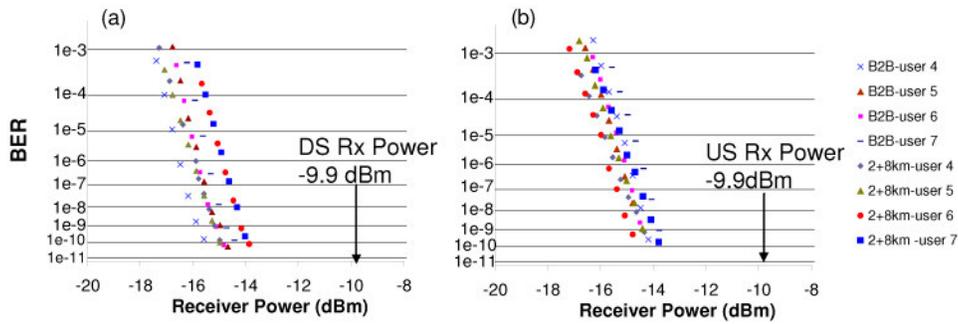


Fig. 11. (a). and (b). BER curves for DS and US, both showing error free operation

5. Summary and conclusion

We have presented a novel dual feeder fiber technique to mitigate the effects of spontaneous Raman crosstalk during simultaneous transmission of classical and QKD optical communication channels. This technique has enabled the first demonstration of 10GHz-clock rate, C-band-based DPSK QKD on a WDM-PON with negligible cross-talk penalties. We identified spontaneous Raman scattering as the main noise mechanism that degrades the performance of the quantum channels, preventing secure operation of a standard single feeder network. We have briefly described the characteristic of spontaneous Raman spectrum and presented a model to quantify the impact of spontaneous Raman noise in a WDM-PON. With bi-directional 10Gb/s US and DS conventional data traffic running error free, QKD transmission was demonstrated for 4 users. The mean QBER value was 3.5% with a mean raw key distribution rate of 1.3Mb/s, which decreased to 696kb/s after temporal windowing to reduce inter-symbol interference due to single photon detector timing jitter. The mitigation scheme is protocol transparent and hence is also applicable to other QKD protocols such as BB84 [1].

Acknowledgements

This work was funded by Science Foundation Ireland under Grant 06/IN/I969, the Embark Initiative, Inspire and Enterprise Ireland under Grant CFTD/2008/312 The authors would like to thank Dr. Emanuele Pelucchi for the loan of the superconducting single photon detectors used in this work and help with their set-up.