Quantum information to the home

2011 New J. Phys. 13 063039

(http://iopscience.iop.org/1367-2630/13/6/063039)

New Journal of Physics
The open-access journal for physics

Quantum information to the home

Iris Choi, Robert J Young[1] and Paul D Townsend[2]
Photonic Systems Group, Tyndall National Institute and Department of Physics, University College Cork, Cork, Ireland
E-mail: paul.townsend@tyndall.ie

New Journal of Physics **13** (2011) 063039 (13pp)
Received 4 March 2011
Published 23 June 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/6/063039

Abstract. Information encoded on individual quanta will play an important role in our future lives, much as classically encoded digital information does today. Combining quantum information carried by single photons with classical signals encoded on strong laser pulses in modern fibre-to-the-home (FTTH) networks is a significant challenge, the solution to which will facilitate the global distribution of quantum information to the home and with it a quantum internet [1]. In real-world networks, spontaneous Raman scattering in the optical fibre would induce crosstalk between the high-power classical channels and a single-photon quantum channel, such that the latter is unable to operate. Here, we show that the integration of quantum and classical information on an FTTH network is possible by performing quantum key distribution (QKD) on a network while simultaneously transferring realistic levels of classical data. Our novel scheme involves synchronously interleaving a channel of quantum data with the Raman scattered photons from a classical channel, exploiting the periodic minima in the instantaneous crosstalk and thereby enabling secure QKD to be performed.

[1] Current address: Department of Physics, Lancaster University, Lancaster, UK.
[2] Author to whom any correspondence should be addressed.

Contents

1. Introduction

To date, the technology most widely deployed to distribute classical data to the home via fibre optics is the Gigabit Ethernet Passive Optical Network (GE-PON), as illustrated in figure 1 [2]; its architecture consists of a tree-network with a passive splitter to link a large number of end users, homes and businesses to a telecommunications local exchange. Wavelength is used to separate communications from the user (upstream) with communications destined for the user (downstream). The 1300 nm wavelength band is chosen for the former and the 1500 nm band for the latter, for cost reasons. The wavelength plan for GE-PON is optimized for low-cost operation; 1300 nm Fabry–Pérot lasers are relatively cheap and are supplied to users, the 1500 nm band distributed feedback (DFB) laser is more expensive and only one is used, located in the local exchange.

The upstream traffic operates in burst mode, employing a time-division-multiple-access scheme to share the available bandwidth, which is typically 1.25 Gbit s^{-1} in today's systems, between the various users on the network. Downstream data traffic from the local exchange to homes operates continuously in broadcast mode using addresses to identify data intended for a particular user. Any party with physical access to the network can eavesdrop on its traffic making encryption essential for privacy. One exciting possibility on such a network is to co-propagate quantum information with the classical data, and to base the security of the network on qubits distributed using this new channel. When properly implemented [3], quantum key distribution (QKD) promises security guaranteed by the fundamental laws of physics [4–19], rather than the current practice of relying on unproven principles of mathematical complexity. The feasibility of transferring qubits on modern fibre-to-the-home (FTTH) networks has been demonstrated [20], but its operation under real traffic was not considered. Practical networks are based on standards that have been designed to minimize costs; the addition of a quantum channel to such networks should therefore be achieved by modifying the protocols used to implement it,

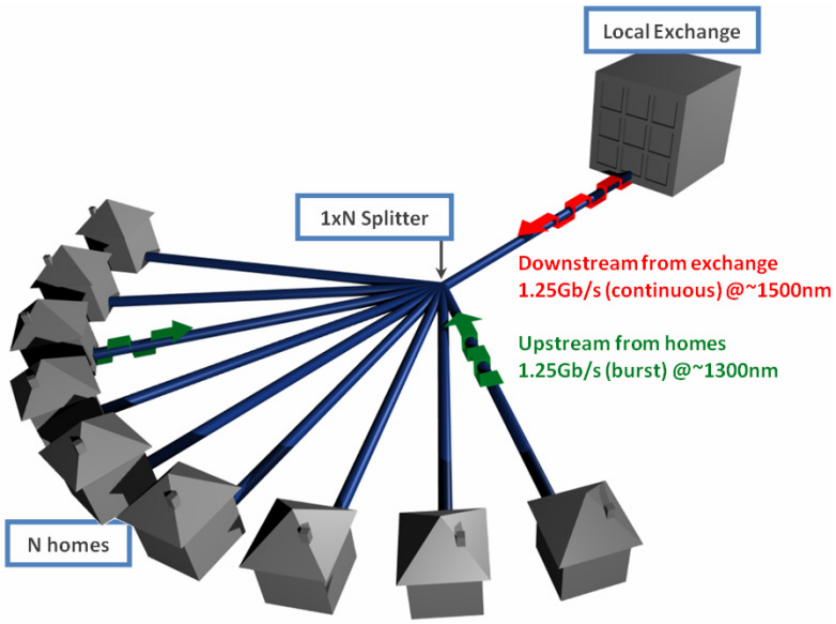

Figure 1. The most widely deployed FTTH network architecture to date: the GE-PON. The GE-PON operates at 1.25 Gb s^{-1}; it links the telecommunication local exchange with the customers using a tree-like passive power splitter.

rather than adapting existing networks, if it is to have any realistic hope of being deployed. Detailed consideration of the problem of integrating quantum and classical information on networks leads to a complete re-design of the operating procedure of the quantum channel, with keys distributed from, instead of to, individual users, and with transmission taking place in bursts, rather than being continuous. Critically, a novel time- and wavelength-multiplexing scheme is also required to send the quantum data during 'quiet periods' between the bursts of noise generated by Raman scattering from the conventional data pulses propagating in the system.

2. Challenges for quantum key distribution (QKD) implementations with existing fibre-to-the-home (FTTH) architectures

The barrier to implementing a single-photon quantum channel on an FTTH network is illustrated in figure 2, which shows the optical spectrum measured at the input to the local exchange in a realistically emulated network. The spectra were measured at the local exchange input in the FTTH system. Two strong peaks are generated by the upstream channel and Rayleigh back-scattering from the downstream channel, respectively. In addition, a broad background is observed, arising from spontaneous Raman scattering in the silica glass of the fibre. This inelastic process exhibits equal scattering cross-sections in both the forward and reverse directions, thus transferring photons from the conventional channels into new frequency bands spread across the full fibre transparency window [21, 22]. The QKD system used here has a nominal launch power level of −65 dBm and the FTTH network has a transmission loss of approximately 23 dB, resulting in a receive power of the quantum channel of around −88 dBm.

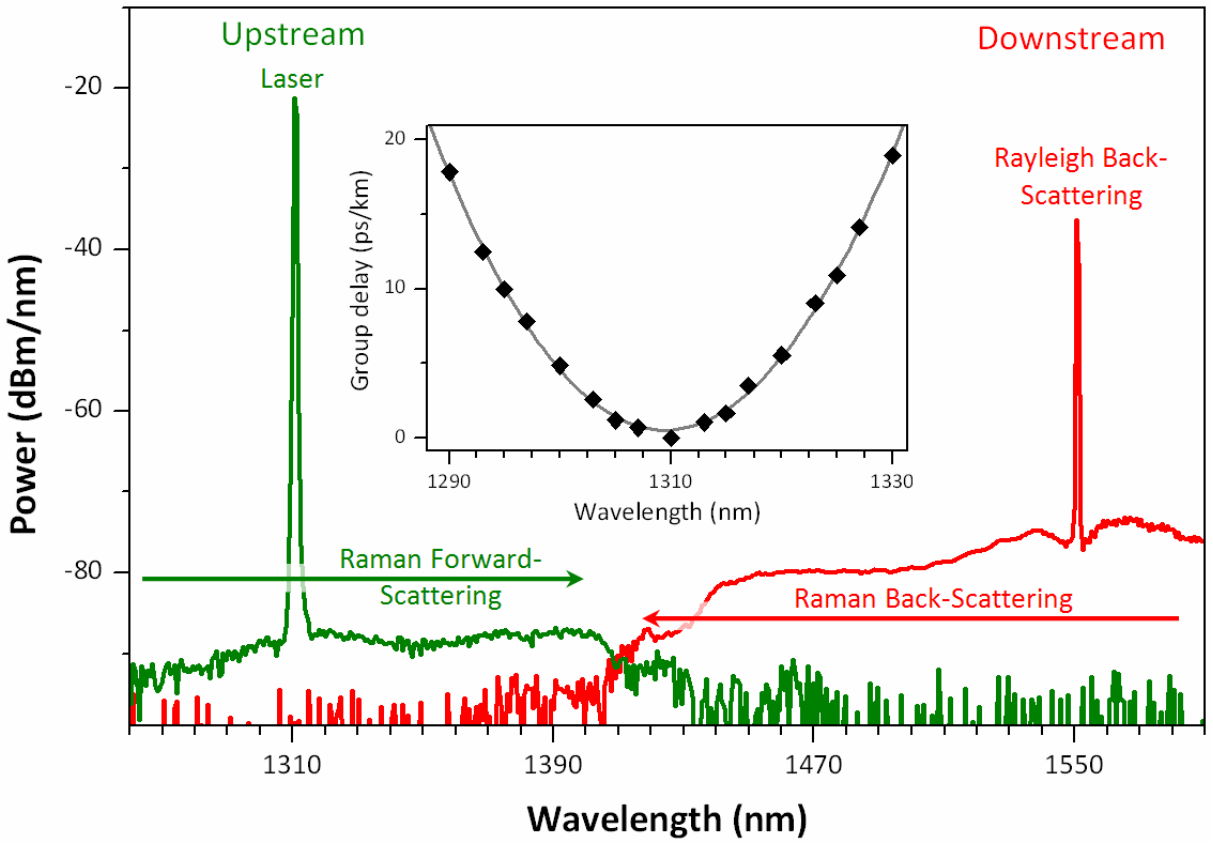

Figure 2. Spontaneous Raman spectra from an FTTH network. The spectra show no available Raman noise-free window in which a quantum channel could be added. The inset shows the dispersion curve of the 10 km transmission fibre used in our experiment. The data are fitted with a three-term Sellmeier equation $D = a + bx^2 + cx^{-2}$, where D is the group delay and x is the wavelength. The dispersion minimum is extracted to be at 1309.6 nm.

The minimal spontaneous Raman scattering is $-95\,\mathrm{dBm\,nm^{-1}}$. Typical, low-cost, spectral filters have widths >10 nm, leading to the Raman noise power falling within the quantum channel wavelength band being greater than the power of the quantum signal. This gives rise to large ($\sim$50%) error rates, preventing secure quantum communication. Research groups have succeeded in implementing QKD systems over wavelength division multiplexed (WDM) networks by reducing this Raman noise level using sub-nanometre optical filtering [23, 24]. However, this is not practical in an FTTH context, as the necessary filters and wavelength-locked sources are prohibitively expensive.

3. Novel Raman noise suppression scheme

The proposed solution results from an analysis of the temporal characteristics of the back- and forward-Raman scattered photons generated by on–off intensity-modulated conventional data streams under different fibre chromatic dispersion conditions. An arbitrary sequence of on–off

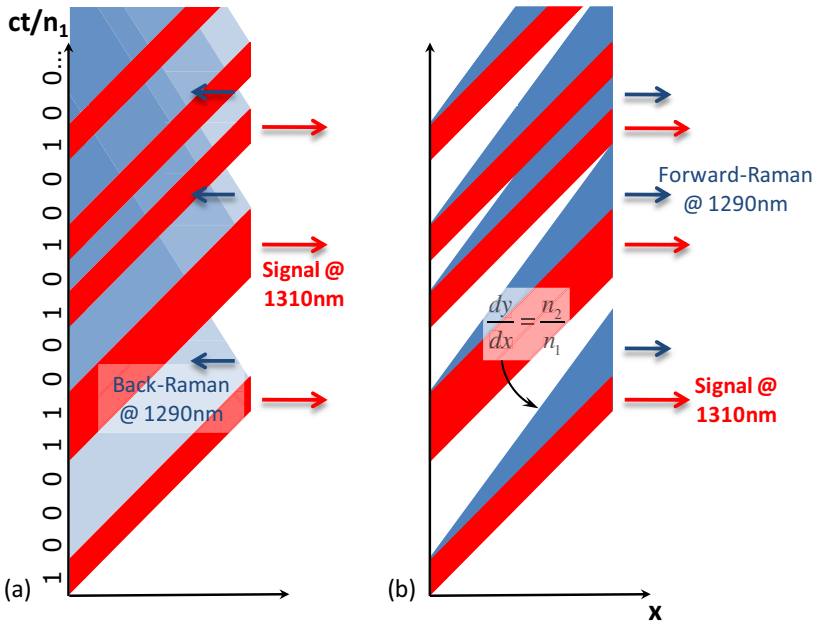

Figure 3. Minkowski diagrams to independently illustrate the problem of (a) back- and (b) forward-scattered Raman photons. (a) Backscattering leads to a time-average Raman background. (b) Dispersive forward-scattering leads to a temporal broadening of '1' pulses, ultimately resulting in a strong background signal throughout '0' events. As illustrated, for short lengths of fibre the background signal can contain Raman-free gaps in the '0' events. n_1 (n_2) is the group refractive index of silica fibre at 1310 nm (1290 nm).

modulated classical data pulses is first considered, propagating in an ideal, dispersion-free fibre. As the Raman scattering is distributed in nature, the instantaneous intensity of the scattered light at the fibre input or output will contain contributions from all of the microscopic length elements that make up the full length of the fibre. Consequently, in the backward direction, scattering contributions generated along the length of the fibre by a given classical data pulse will arrive out of step, leading to a Raman signal that is approximately continuous in time as illustrated in figure 3(a). This occurs because the pulse propagation times (ms, for multi-kilometre fibre lengths) are significantly longer than the characteristic timescales of the intensity modulation on the generating channel (of the order of ns). Conversely, in the forward direction, with no group velocity dispersion, the frequency-shifted Raman photons will propagate in-step with each generating data pulse and hence will build-up along the length of the fibre to give a Raman pulse train with the same temporal characteristics as the generating data sequence. Critically, this implies that in the forward direction, the instantaneous Raman scattering is low for 'zero' positions in the data sequence and, in principle, can be reduced to an arbitrarily small value simply by increasing the modulation depth of the conventional channel laser source. However, as can be seen in figure 2, the chromatic dispersion in real optical fibres is non-zero, apart from that at one specific wavelength (∼1309 nm) where the waveguide and material contributions cancel. At other wavelengths the non-zero dispersion causes the Raman gaps to eventually fill, as illustrated in figure 3(b). This is due to two processes: the temporal 'walk-off'

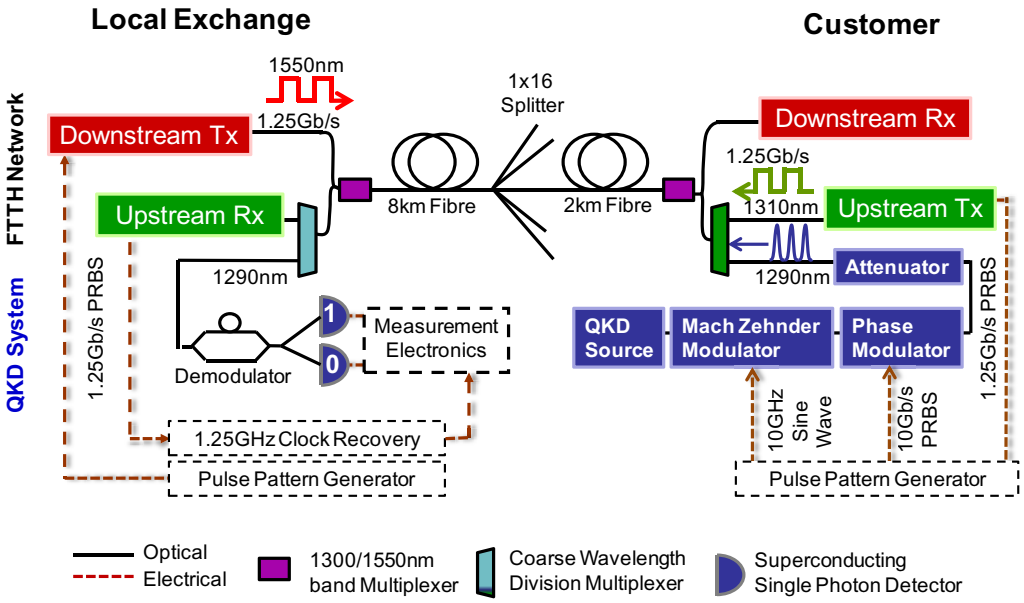

Figure 4. Experimental setup for the QKD system implementation over a realistic FTTH architecture. The classical channels emulate a GE-PON with bidirectional downstream (1550 nm) and upstream (1310 nm) data traffic at 1.25 Gb s^{-1}.

between the generating pulses and the Raman pulses and the dispersive spreading of the Raman pulses themselves. The situation on a real network is further complicated by the presence of separate counter-propagating upstream and downstream data channels in the 1300 and 1500 nm wavelength bands, which means that whichever direction is chosen for quantum communication it must operate in the presence of both forward (modulated) and backward (continuous) Raman. The relative contributions of each will depend on the direction and wavelength of the quantum channel with respect to the upstream and downstream channels. Nevertheless, if the quantum channel is chosen to operate in the upstream direction, at a wavelength close to the upstream channel wavelength, the Raman gaps can be maintained and exploited to perform QKD.

4. Experimental setup

4.1. Classical channels

The experimental system, as shown in figure 4, emulates a GE-PON, combined with a 10 GHz return-to-zero, differential phase shifted keyed (RZ-DPSK) QKD system [16, 25]. Customers are linked to the local exchange via a 2 km drop fibre, a 1×16 power splitter and an 8 km feeder fibre. Bidirectional downstream (1550 nm) and upstream (1310 nm) channels are used to emulate real Ethernet data traffic. These conventional channels are generated by DFB lasers, which are on–off (non-return-to-zero) modulated at 1.25 Gb s^{-1} using $2^7 - 1$ bit pseudo-random-bit-sequences (PRBS) produced by a pair of pulse pattern generators (PPGs). The downstream and upstream launch powers are 0 and −2.7 dBm, respectively, which are typical

values used in real networks and sufficiently high to ensure that the Raman crosstalk is not underestimated. Low-cost coarse wavelength division multiplexing (CWDM) filters and wideband 1300/1550 nm WDM filters are used to combine the QKD channel with the GE-PON. They provide high channel isolations, which suppress leakage of downstream and upstream signals into the quantum channel by >120 and >60 dB, respectively, sufficient to render direct inter-channel crosstalk negligible. In operation, the classical system has >5 dB power margin with an upstream received power of −21.3 dB and a downstream received power of −22 dBm, showing adequate margin for aging effects.

4.2. Quantum channel setup and allocation

The quantum channel is multiplexed/de-multiplexed with the classical upstream channel using low-cost CWDM filters, based on the standard 20 nm grid spacing. As the Raman anti-Stokes lines are weaker than the Stokes lines, the quantum channel is placed at 1290 nm, the adjacent channel on the shorter wavelength side of the 1310 nm upstream classical channel to minimize crosstalk. In this configuration, the upstream and (Rayleigh-backscattered) downstream channels lie outside the quantum channel filter passband and hence are blocked from reaching the QKD receiver, as are the unmodulated, backward Raman-scattered photons from the downstream channel (as shown by figure 2). Hence, only a spectral slice of forward Raman-scattered light generated by the upstream channel is passed by the filter. The latter experiences low dispersion due to the proximity of the fibre dispersion zero and is therefore strongly modulated and contains gaps in which quantum communications can exist. The fact that the Raman crosstalk is then solely determined by the upstream channel has important consequences in terms of network deployment and upgrade. Specifically, since the GE-PON upstream channel operates in burst mode, with only one user transmitting at a time (time-division multiple access), only the forward Raman generated by a given user can impair the same user's quantum key exchange. This means that individual users can be upgraded for QKD operation without the need for changes to the terminal equipment of other users.

The quantum channel is a 10 GHz clock rate, RZ DPSK system. The quantum channel source is a tuneable external cavity laser. The continuous laser output is then pulse-carved by a Mach–Zehnder modulator (MZM) driven by the 10 GHz clock from the PPGs to generate a sequence of 45 ps duration, return-to-zero (RZ) pulses. Next, data are encoded by a phase modulator (PM) driven by 10 Gb s^{-1} $2^7 - 1$ NRZ PRBS to generate a sequence of 0 and π phase shifts in a DPSK QKD scheme. Prior to transmission, the QKD source is attenuated to the single-photon level, with mean photon numbers of 0.2 photon per pulse. The channel loss is ∼23 dB, which includes 13.5 dB loss from the 1 × 16 power splitter, CWDM filter loss (∼1 dB each), 1310 nm/1550 nm WDM (de)multiplexer loss of ∼0.6 dB each, 3 dB loss from 10 km transmission fibre in total, 2 dB loss from the DPSK demodulator and ∼1 dB connector loss. The QKD signal is detected by a pair of superconducting single photon detectors (SSPDs) with effective mean detection efficiencies of 5%, dark count rate of <10 counts per second and maximum count rate of 70 MHz. Time correlation analysis of the photocount is carried out by a time interval analyser (TIA), which is triggered by a 78.1 MHz clock recovered and divided from the 1.25 Gb s^{-1} upstream data. This provides accurate timing information to ensure that the quantum channel is synchronized with the classical channels. The TIA has a specified dead time of less than 95 ns, which is the dominant source of dead time in the experiment.

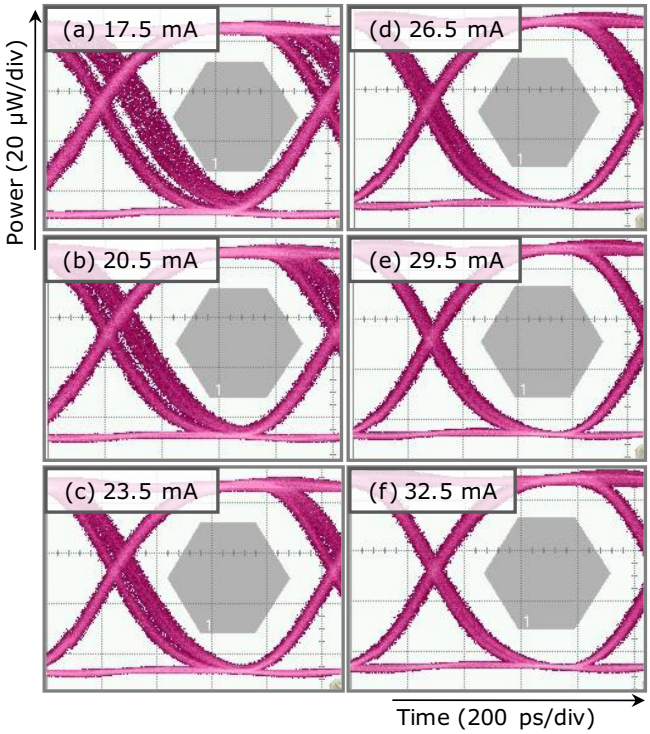

Figure 5. Data eye mask test results for the upstream channel for various '0' level drive current values, (a)–(f), as labelled.

5. Results

5.1. Classical channel results

In the experiments, the upstream laser bias was set such that the drive current for the 'zero' levels was 23.5 mA, which was approximately 20% below the laser threshold level, giving an on-off extinction ratio of ∼26 dB. This gave a good compromise between maximizing the depth of the Raman gaps, and minimizing the timing jitter caused by pattern-dependent turn-on times and gain-switching transients that are associated with below threshold biasing. The chosen operating conditions were carefully tested via a series of data eye mask tests (figure 5), and bit error rate (BER) tests, figure 6). The performance of the upstream channel was not degraded. BER curves were taken for both upstream and downstream channels to confirm that they were both operating error-free (i.e. BER $\leqslant 10^{-10}$).

5.2. Quantum channel results

An example time-resolved photocount histogram measured at the 'one' (constructive interference for π-phase shift) port of the DPSK demodulator is shown in figure 7. Strongly modulated Raman crosstalk is observed in the 1290 nm quantum channel. The large peaks correspond to the Raman counts generated whenever a 'one' is transmitted on the upstream channel. The crosstalk in these temporal regions is sufficiently high that secure QKD is impossible. However, in the data 'zero' positions the Raman crosstalk is negligible and is observed as Raman gaps where QKD data can be embedded and transmitted with high fidelity.

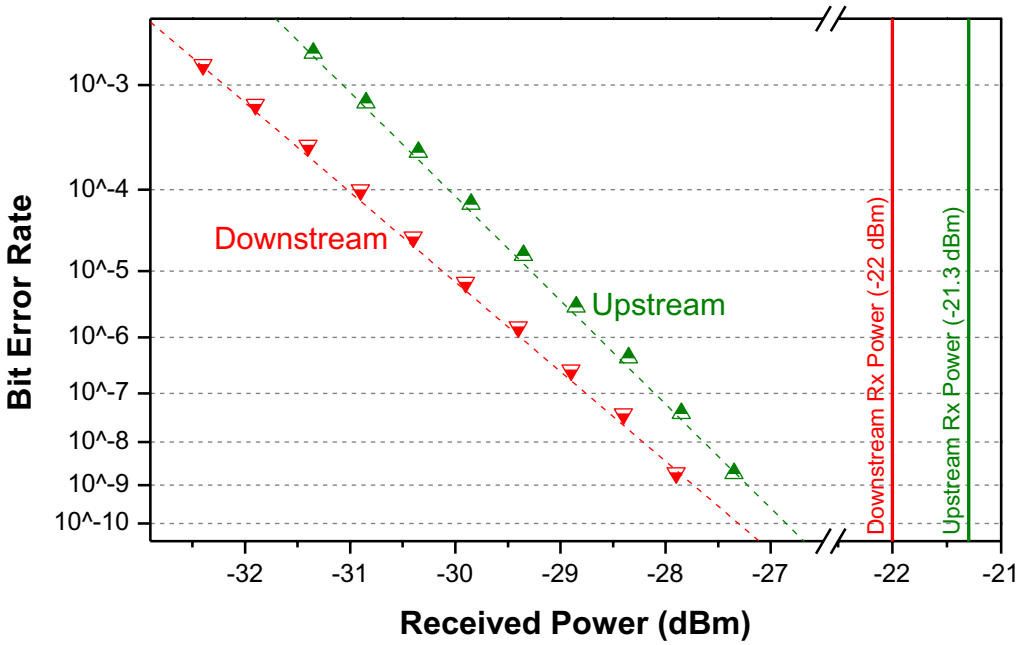

Figure 6. BER tests for downstream and upstream channels. Dashed lines represent fits to the data with the form $\log[\log(y)] = mx + c$ to illustrate their linear dependence with the chosen scale mappings.

As shown in figures 7(b) and (c), significant inter-symbol interference (ISI) can be inferred from the relatively shallow minima observed between consecutive ones on the quantum channel, which arises from the limited instrumental response time of the single-photon detection system. The latter is dominated by ∼35 ps timing jitter of the detectors, which is a significant fraction of the 100 ps bit period. Errors due to ISI were significantly reduced by employing a windowing technique rejecting counts occurring outside of the central 32 ps of each quantum bit (leading to approximately 60% bit-loss) [16].

The mean value for the QBER obtained under these conditions with the quantum channel alone was 3.2% (1.9% from ISI and 1.3% from finite DPSK interference visibility), which only rises to 4% with the full FTTH system turned on. The 0.8% rise in QBER is attributed to residual Raman counts. The mean QBER value is comparable to the value achieved in [16] for a 200 km point-to-point DPSK QKD system with no classical channels. The total measured count rate was 3.8 MHz, which was dominated by Raman counts. Upon removing the Raman peaks and appropriate temporal windowing, the sifted key distribution rate was determined to be 84 kb s^{-1} when the central 400 ps of data within the Raman gaps were analysed. This results in a predicted key generation rate of 1.3 kb s^{-1} after error correction and privacy amplification [25–27].

5.3. Security analysis

The efficiency of the DPSK QKD protocol in the case of general collective attacks (including photon number splitting) is characterized by

$$R_{\text{Secure}} = R_{\text{Sift}}\{\tau + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\}, \tag{1}$$

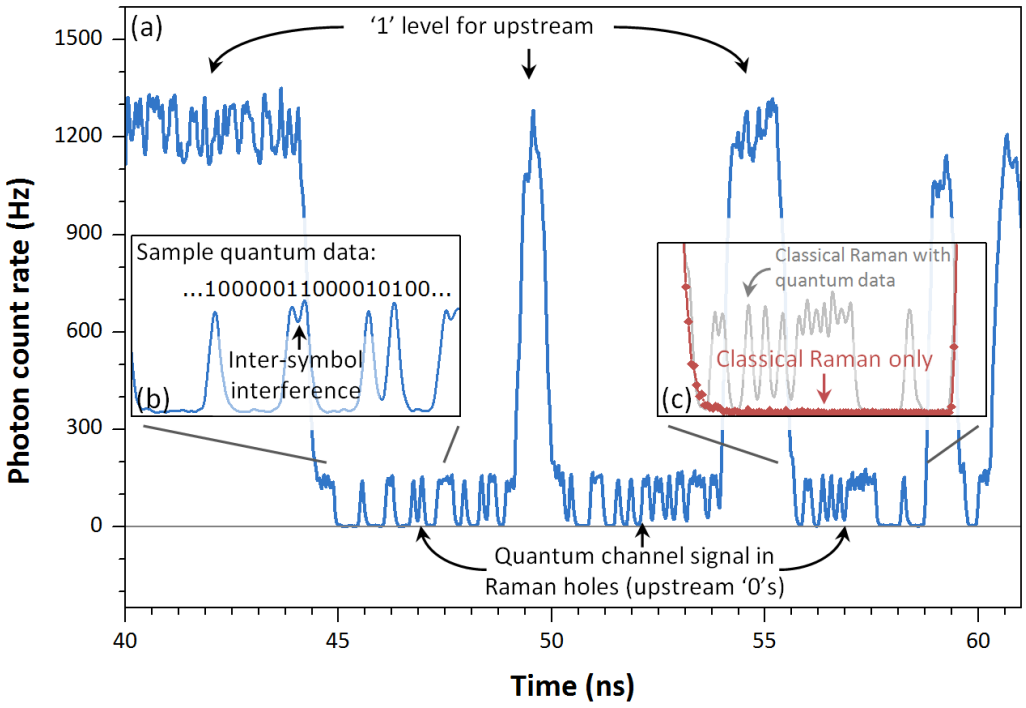

Figure 7. Time-resolved photocount histograms corresponding to 1 s of integration, approximately 8×10^7 repetitions of the QKD data pattern. (a) The histogram shows the highly modulated Raman crosstalk observed in the 1290 nm quantum channel, generated by a segment of the classical data pattern corresponding to a 11111000000100000110000101 bit sequence. Quantum signals are embedded in the Raman gaps. (b, c) Significant ISI can be inferred from the relatively shallow minima observed between consecutive ones on the quantum channel. On removal of the error counts using a 32 ps window, the mean value for the QBER obtained with the quantum channel alone was 3.2%, which only rises to 4% with the full FTTH system turned on.

where R_{Secure} is the final secure key distribution rate after error correction and privacy amplification, R_{Sift} is the experimentally determined sifted key rate, $f(e)$ is a function that characterizes how far above the Shannon limit the error correction algorithm is performing, e is the background QBER in the system and τ is the compression factor due to privacy amplification [7], [25–27]. The parameter values for the experimental system described here are $R_{\text{Sift}} = 84\,\text{kb}\,\text{s}^{-1}$, $\tau = 0.296$, $f(e) = 1.16$, $e = 0.04$ and $R_{\text{Secure}} = 1.3\,\text{kb}\,\text{s}^{-1}$. Here, we assume the same privacy amplification methods as in [27] and hence the same compression factor.

6. Simulations

As the experimental setup employed for the proof of principle experiments discussed above is based on available components and fibres, potential optimization of the chosen wavelength plan and the scheme's robustness to the variations in fibre parameters expected in real systems is considered. This is undertaken using a numerical model to predict the Raman output pulse

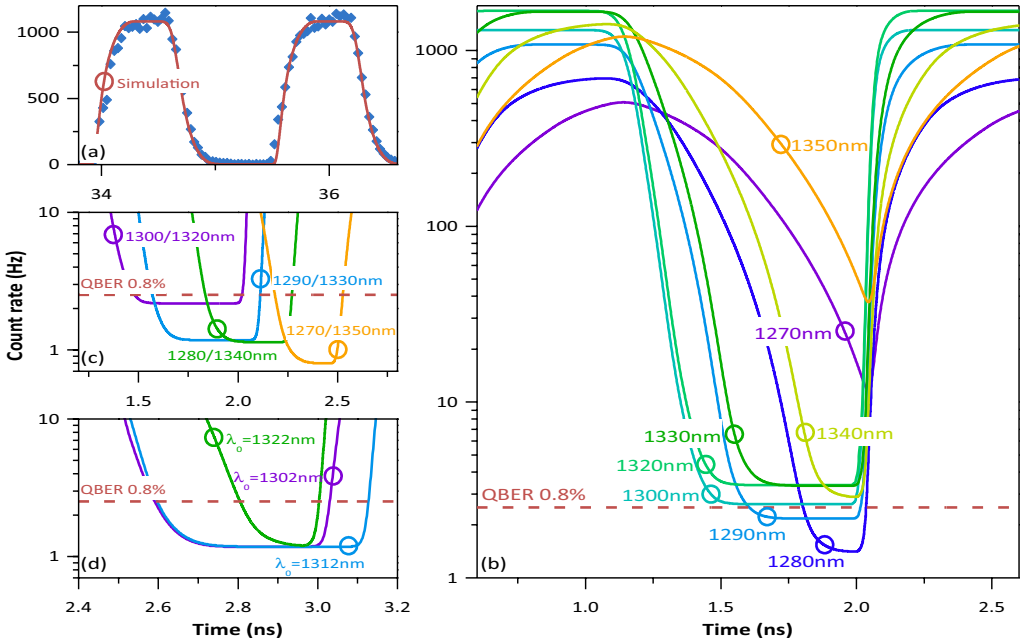

Figure 8. Simulation data. (a) Experimental upstream pulse shapes for a '101' data segment together with the numerical fit used for Raman gap simulations. (b) Fixed classical upstream wavelength of 1310 nm and various quantum channel wavelengths. (c) Classical and quantum channel wavelengths spaced approximately symmetrically about the dispersion zero. (d) Effect of variation in fibre dispersion minimum.

shape using the experimentally measured upstream pulse and fibre group delay characteristics (figure 2, inset). We model a segment of the upstream data sequence, which contains a single isolated zero as this generates the smallest possible gap.

The numerical dispersion model uses the experimentally measured Raman spectrum, upstream pulse shape ('101' data segment, with 40 ps/100 ps 10–90% rise/fall times and 690 ps pulse width at half-maximum) and group delay curve to calculate the composite Raman pulse generated at the output of the fibre by scattering from multiple fibre segments of length Δx. This composite pulse has a total spectral width of 17 nm (defined by the CWDM filter) and is made up of multiple spectral slices of width $\Delta\lambda$, with relative amplitudes and delays determined by the measured wavelength-dependent scattering amplitude and fibre group delay, respectively. The model assumes a square CWDM filter response, an instantaneous Raman response and no dispersive broadening of the upstream pulse due to its (relatively) narrow spectral width. All of these approximations are well satisfied in practice. The group delay values were obtained from the Sellmeier expression given with figure 2 using fitted values of $a = -38.34\,\mathrm{ps\,nm^{-1}}$, $b = 1.12 \times 10^{-5}\,\mathrm{ps\,nm^{-3}}$ and $c = 3.287 \times 10^{7}\,\mathrm{ps\,nm^{-1}}$. Simulations were performed using the values of $\Delta x = 0.1$ km and $\Delta\lambda = 0.1$ nm, which were found to give negligible quantization errors.

Figure 8(a) shows the experimentally measured upstream pulse shapes for a '101' data segment together with the numerical fit used for the subsequent simulations. Figure 8(b) shows modelled Raman gaps for various quantum channel wavelengths with the classical upstream wavelength fixed at 1310 nm for a 10 km fibre link. The 1290 nm curve exhibits a gap equivalent

to four quantum bits and a minimum Raman count rate that corresponds to a QBER contribution of 0.7%, which is close to the experimental value of 0.8% (dashed horizontal line). At 1280 nm, the Raman level is reduced further, but the gap narrows significantly to approximately two quantum bits due to increased dispersive broadening. In figure 8(c), the Raman gap is further optimized through minimization of the walk-off between the classical and quantum channels, by placing the two channels approximately symmetrically about the dispersion zero. In this case, the optimum performance (QBER ∼0.4%, 5 bit gap) is obtained for quantum and upstream channel wavelengths of 1290 and 1330 nm, respectively, symmetrically about the fibre dispersion zero. This gives the best trade-off between the need to minimize Raman scattering amplitude (favours large wavelength separation) and the need to minimize dispersive broadening of the Raman pulse (favours wavelengths close to the dispersion zero). Finally, for this optimum configuration, the impact of varying the fibre dispersion zero from 1302 nm to 1322 nm, as commercially specified for standard single-mode transmission fibre [28], is investigated. Figure 8(d) confirms that in this case (quantum and classical channels at 1290 and 1330 nm, respectively) the Raman gap is maintained over the full range of possible dispersion zero values found in commercial fibres.

7. Conclusions

A novel protocol that allows classical and quantum information to co-exist on standardized, mass-deployed FTTH networks has been introduced. The scheme was employed to demonstrate secure quantum communication on a practical network containing realistic levels of classical data. The technique uses a novel time- and wavelength-multiplexing scheme to send secure quantum key data during the 'quiet periods' between the bursts of noise generated by Raman scattering from the conventional data pulses propagating in the system. Although demonstrated here using the DPSK QKD scheme, the approach is completely protocol independent and could also be used with alternative QKD schemes such as BB84, for example. In a fully implemented system, the keys distributed using the scheme can be used to encrypt the conventional communication channels and hence provide communications privacy for all of the users sharing the network.

Acknowledgments

We gratefully acknowledge financial support from Science Foundation Ireland under grant no. 06/IN/1969, Enterprise Ireland under grant no. CFTD/2008/312 and the HEA under the INSPIRE initiative. IC acknowledges the IRCSET-Embark Initiative for the award of a PhD scholarship. We also thank Dr E Pelucchi for expert advice and assistance regarding the SSPDs used in the experiments.

References

[1] Kimble H 2008 The quantum internet *Nature* **453** 1023–30
[2] Twist K 2007 Driving fibre closer to the home *Nat. Photonics* **1** 149–50
[3] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Hacking commercial quantum cryptography systems by tailored bright illumination *Nat. Photonics* **4** 686–9
[4] Bennett C and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Int. Conf. on Computers, Systems and Signal Processing* (*Bangalore, India*) pp 175–9

[5] Bennett C, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography *J. Cryptol.* **5** 3–28
[6] Marand C and Townsend P 1995 Quantum key distribution over distances as long as 30 km *Opt. Lett.* **20** 1695
[7] Lütkenhaus N 2000 Security against individual attacks for realistic quantum key distribution *Phys. Rev.* A **61** 52304
[8] Shor P and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441–4
[9] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95
[10] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 Quantum key distribution over 67 km with a plug&play system *New J. Phys.* **4** 41
[11] Hughes R, Nordholt J, Derkacs D and Peterson C 2002 Practical free-space quantum key distribution over 10 km in daylight and at night *New J. Phys.* **4** 43
[12] Gobby C, Yuan Z and Shields A 2004 Quantum key distribution over 122 km of standard telecom fiber *Appl. Phys. Lett.* **84** 3762
[13] Gottesman D, Lo H, Lutkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices *Proc. Int. Symp. on Information Theory (Chicago, IL, June 27–July 2 2004)* p 136
[14] Zhao Y, Qi B, Ma X, Lo H and Qian L 2006 Experimental quantum key distribution with decoy states *Phys. Rev. Lett.* **96** 70502
[15] Ursin R *et al* 2007 Entanglement-based quantum communication over 144 km *Nat. Phys.* **3** 481–486
[16] Takesue H *et al* 2007 Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors *Nat. Photonics* **1** 343–8
[17] Fernandez V, Collins R, Gordon K, Townsend P and Buller G 2007 Passive optical network approach to gigahertz-clocked multiuser quantum key distribution *IEEE J. Quantum Electron.* **43** 130–8
[18] Peev M *et al* 2009 The SECOQC quantum key distribution network in Vienna *New J. Phys.* **11** 075001
[19] Choi I, Young R J and Townsend P D 2010 Quantum key distribution on a 10 Gb/s WDM-PON *Opt. Express* **18** 9600–12
[20] Townsend P 1997 Quantum cryptography on multiuser optical fibre networks *Nature* **385** 47–9
[21] Subacius D, Zavriyev A and Trifonov A 2005 Backscattering limitation for fiber-optic quantum key distribution systems *Appl. Phys. Lett.* **86** 011103
[22] Toliver P 2004 Impact of spontaneous anti-Stokes Raman scattering on QKD + DWDM networking *Proc. of Lasers and Electro-Optics Society* (*LEOS*) vol 2, pp 491–2
[23] Xia T 2006 In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels *Proc. of Optical Fiber Communication Conf. and the National Fiber Optic Engineers Conf.* (*OFC/NFOEC*) Paper OTuJ7
[24] Peters N *et al* 2009 Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments *New J. Phys.* **11** 045012
[25] Inoue K, Waks E and Yamamoto Y 2002 Differential-phase-shift quantum key distribution *Phys. Rev. Lett.* **89** 037902
[26] Waks E, Takesue H and Yamamoto Y 2006 Security of differential-phase-shift quantum key distribution against individual attacks *Phys. Rev* A **73** 012344
[27] Zhang Q *et al* 2009 Megabits secure key rate quantum key distribution *New J. Phys.* **11** 045010
[28] Corning commercial single-mode fibre datasheet: http://www.corning.com/assets/0/433/573/583/09573389-147D-4CBC-B55F-18C817D5F800.pdf