Quantum Information to the Home

Iris Choi, Robert J. Young and Paul D. Townsend
Photonic Systems Group. Tyndall National Institute and Department of Physics, University College Cork, Ireland
Email: paul.townsend@tyndall.ie

Abstract: A novel Raman-noise suppression scheme has enabled the first quantum key distribution (QKD) over a Gigabit-Ethernet PON carrying realistic data traffic. The DPSK-QKD system produced a sifted-key rate of 84kb/s with a Quantum-BER of 4%.

OCIS codes: (270.5568) Quantum Cryptography, (270.5565) Quantum Communications

1. Introduction
Fibre-to-the-premises (FTTP) networks offer the ultimate in bandwidth provision for end-users. However, because of the shared nature of these networks, information is physically accessible by all the users and hence encryption is required to maintain privacy. An intriguing possibility would be to exploit the quantum mechanics-based security guarantees offered by quantum key distribution [1, 2], to protect the data. However, in real FTTP networks, the spontaneous Raman scattering [3] from the conventional high power upstream (1260nm-1360nm band) and downstream (1490nm-1560nm band) channels in the optical fibre induces crosstalk with the single photon QKD channel, such that the latter is unable to operate securely. The reasons for this can be seen from figure 1a, which shows the optical spectrum measured at the input to the central office/local exchange in a realistically-emulated Gigabit-Ethernet Passive Optical Network (GE-PON) FTTP scheme (details given in section 3). The inelastic Raman process exhibits equal scattering cross-sections in both the forward and reverse directions and is sufficiently broadband that photons from the conventional channels are transferred into new frequency bands spread across the full fibre transparency window. This background induces high error rates on the quantum channel which can only be reduced sufficiently by using sub-nanometer optical filtering [4-6]. However, this is not practical in an FTTP context, as the necessary filters and wavelength-locked sources are prohibitively expensive. Here, we propose and demonstrate for the first time a novel technique, which enables QKD to be employed for security provision on practical FTTP networks. The new scheme involves synchronous interleaving of QKD channel photons with Raman scattered photons from the classical channels such that the instantaneous cross-talk is periodically minimised to <0.3% of its peak value, thus enabling secure QKD. We demonstrate the technique on a laboratory emulated GE-PON to show the scheme working under practical conditions.

2. Principles of novel Raman noise suppression scheme
Our proposed solution results from an analysis of the temporal characteristics of the back- and forward-Raman scattered photons generated by conventional on-off modulated data streams under different fibre chromatic dispersion conditions. We begin by considering an arbitrary sequence of on-off modulated classical data pulses 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, the 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 (figure 1b left). This occurs because the pulse propagation times (ms, for multi-kilometer fibre lengths) are significantly longer than the characteristic timescales of the
intensity modulation on the generating channel (~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. Of course the chromatic dispersion in real optical fibres is only non-zero at one specific wavelength (1309nm for the standard single mode fibres used here), at other wavelengths the Raman gaps will eventually fill due to two processes; the temporal ‘walk-off’ 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 1300nm and 1500nm 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 (figure 1b, right).

3. Experimental setup

Our experimental system (figure 2) emulates a GE-PON, which is a widely deployed FTTP architecture, combined with a 10GHz Return-to-Zero, Differential Phase Shifted Keyed (RZ-DPSK) QKD system [7].

The classical channels are provided by DFB lasers, which are on-off modulated with 2^-1 bit pseudo-random-bit-sequences (PRBS) to emulate a GE-PON where bidirectional downstream (1550nm) and upstream (1310nm) data traffic at 1.25Gb/s is present (wavelength choice determined by laser availability). Users are linked to the central office via a 2km drop fibre, a 1×16 power splitter and an 8km feeder fibre. Downstream and upstream conventional channels were launched at >−3dBm to represent typical launch powers in real networks. This ensures the Raman crosstalk is not under-estimated. Low cost CWDM filters and wideband 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 >120dB and >60dB respectively, sufficient to render direct inter-channel crosstalk negligible. The quantum channel is a 10GHz, RZ DPSK system. The quantum channel source is a tunable external cavity laser which is data encoded by a phase modulator (PM) driven by 10Gb/s 2^-1 NRZ PRBS to generate a sequence of 0 and π phase shifts in a DPSK QKD scheme. The PM output is pulse-carved by a Mach-Zehnder Modulator (MZM) driven by the 10GHz clock from the PPG to generate a sequence of 45ps duration, return-to-zero (RZ) pulses. Prior to transmission, the QKD source is attenuated to the single photon level, with a mean photon number of 0.2 photons/pulse. The channel loss is ≈23dB. The QKD signal is detected by a pair of superconducting single-photon detectors with effective mean detection efficiencies of 5%. Time correlation analysis of the photocount is carried out by a time-interval analyser, which is triggered by a 78.1MHz clock recovered and divided from the 1.25Gb/s upstream data. This provides accurate timing information to ensure the quantum channel is synchronised with the classical channels. As the Raman anti-Stokes lines are weaker than the Stokes lines, the quantum channel is placed at 1290nm, the adjacent channel on the shorter wavelength side of the 1310nm upstream classical channel to minimise crosstalk. In this configuration, the upstream and (Rayleigh-backscattered) downstream channels lie outside the quantum channel filter pass-band and hence are blocked from reaching the QKD receiver, as are the un-modulated, backward Raman-scattered photons from the downstream channel (as shown by figure 1a). 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. Since the GE-PON upstream channel operates in burst mode, with only one user transmitting at a time, only the Raman generated by a given user will impair that same user’s QKD exchange. Consequently, individual users can be “upgraded” for QKD without need for changes to the terminal equipment of other users.
4. Results and discussion

In the experiments, the upstream channel laser bias was adjusted so that the ‘0’ level current was 20% below the 30mA threshold, giving a mean on-off extinction ratio of 26dB. 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, which are associated with below threshold biasing. BER curves were taken for both upstream and downstream channels to confirm that they were both operating error-free (BER ≤ 10^{-10}). In operation, the classical system had >5dB power margin with upstream received power of ~−21.3dB, and downstream received power of ~−22dBm, showing adequate margin for aging effects (figure 3a). The quantum channel performance is illustrated by Figure 3b, which shows a time-resolved photo-count histogram measured at the ‘1’ (constructive interference for π-phase shift) port of the DPSK demodulator. Highly modulated Raman crosstalk was observed in the 1290nm quantum channel. The large peaks correspond to ‘1’s in the upstream data while the ‘0’s were observed as Raman gaps and were used to embed quantum signals. Significant inter-symbol interference (ISI) can be inferred from the relatively shallow minima observed between consecutive ones on the quantum channel, which resulted from the limited instrumental response time of the single photon detection system. The latter was dominated by ~35ps timing jitter of the detectors, which is a significant fraction of the 100ps bit period. Errors due to ISI were significantly reduced by employing a windowing technique rejecting counts occurring outside of the central 40ps of each quantum bit. The mean value for the QBER obtained under these conditions with the quantum channel only 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 (figure 3b). We attribute this 0.8% rise in QBER to residual Raman counts. The mean QBER value is comparable to the value achieved in [7] for a 200km point-to-point DPSK QKD system with no classical channels. The total measured count rate was 3.8MHz which was dominated by Raman counts. Upon removing the Raman peaks and using appropriate temporal windowing technique [6], the sifted key distribution rate was determined to be 84kb/s when the central 400ps of data within the Raman gaps were analysed. This results in a predicted key generation rate of 1.3kb/s per user after error correction and privacy amplification [8].

5. Conclusion

We have introduced a novel protocol to allow classical and quantum information to co-exist on standardised, mass-deployed FTTP networks. Using the scheme we demonstrated the first secure quantum communication on a practical network containing realistic levels of classical data. A sifted key rate of 84kb/s with QBER of 4% (1.3kb/s secure key rate) was achieved in the presence of FTTP channels. Furthermore, the technique is QKD protocol-independent. In a complete system the keys distributed using the scheme could be used to encrypt the conventional communication channels and hence provide communications privacy for all of the users sharing the network.

Acknowledgements: this work was funded by Science Foundation Ireland (06/IN/269), Enterprise Ireland (TD/2008/312) & the Irish HEA ‘INSPIRE’ initiative. R. J. Young’s present address is: Department of Physics, Lancaster University, Lancaster, UK.

References

[1] C. H. Bennett and G. Brassard, Proc. of the IEEE Intl Conf on Computers, Systems & Signal Processing, India, (1984), pp. 175-179
[2] P. D. Townsend, Nature 385 47-49 (1997)
[3] D. Subacius et al., Appl. Phys. Lett. 86, 011103 (2005)
[4] N. Peters et al., New Journal of Physics, 2009. 11: p. 045012.
[5] T. Xia et al., paper OThA7, OFC/2006).
[6] I. Choi et al. Optics Express 18 (9) pp. 9600-9612 (2010)
[7] H. Takesue at al. Nature Photon. 1, 343-348 (2007)
[8] Zhang Q et al. New J. Phys. 11 045010 (2009)