

Quantum key distribution over multicore fiber

J. F. Dynes,¹ S. J. Kindness,^{1,2} S. W.-B. Tam,¹ A. Plews,¹ A. W. Sharpe,¹
M. Lucamarini,¹ B. Fröhlich,¹ Z. L. Yuan,^{1,*} R. V. Pentyl² and A. J. Shields¹

¹Toshiba Research Europe Ltd, Cambridge Research Laboratory,
208 Cambridge Science Park, Cambridge CB4 0GZ, UK

²Cambridge University Engineering Department, 9 JJ Thomson Ave, Cambridge, CB3 0FA, UK
*zhiliang.yuan@crl.toshiba.co.uk

Abstract: We present the first quantum key distribution (QKD) experiment over multicore fiber. With space division multiplexing, we demonstrate that weak QKD signals can coexist with classical data signals launched at full power in a 53 km 7-core fiber, while showing negligible degradation in performance. Based on a characterization of intercore crosstalk, we perform additional simulations highlighting that classical data bandwidths beyond 1Tb/s can be supported with high speed QKD on the same fiber.

©2016 Optical Society of America

OCIS codes: (060.5565) Quantum communications; (270.5568) Quantum cryptography; (060.2330) Fiber optics communications.

References and links

1. C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. Comput. Syst. Signal Process. **175**, 175–179 (2014).
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301 (2009).
3. 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. Nauerth, 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-Brouiri, 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," New J. Phys. **11**, 075001 (2009).
4. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD network," Opt. Express **19**, 10387-10409 (2011).
5. A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki and A. J. Shields, "High speed prototype quantum key distribution system and long term field trial," Opt. Express **23**, 7583-7592 (2015).
6. T. Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W. Q. Cai, L. Ju, L. K. Chen, L. J. Wang, Y. Gao, K. Chen, C. Z. Peng, Z. B. Chen, and J.-W. Pan "Metropolitan all-pass and inter-city quantum communication network," Opt. Express **18**, 27217–27225 (2010).
7. S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express **22**, 21739–21756 (2014).
8. I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, H. Griesser, M. Eiselt, C. Chunnillall, G. Lepert, A. Sinclair, J. P. Elbers, A. Lord and A. J. Shields, "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," Opt. Express **22**, 23121-23128 (2014).
9. R.-J. Essiambre, G. Kramer, P. J. Winzer, G. J. Foschini and B. Goebel, "Capacity limits of optical fiber networks," J. Lightwave Technol. **28**, 662-701 (2010).
10. D. Qian, M. Huang, E. Ip, Y. Huang, Y. Shao, J. Hu, and T. Wang, "101.7-Tb/s (370×294-Gb/s) PDM-128 QAM-OFDM Transmission over 3×55-km SSMF using pilot-based phase noise mitigation," OFC 2011, paper PDPB5 (2011).

11. K. Saitoh and S. Matsuo, "Multicore fibers for large capacity transmission," *Nanophotonics* **2**, 441-454 (2013).
12. D. J. Richardson, J. M. Fini and L. E. Nelson, "Space-division multiplexing in optical fibres," *Nat. Photonics* **7**, 354-362 (2013).
13. P. J. Winzer, "Making spatial multiplexing a reality," *Nat. Photonics* **8**, 345-348 (2014).
14. B. Zhu, T. F. Taunay, M. F. Yan, J. M. Fini, M. Fishteyn, E. M. Monberg, and F. V. Dimarcello, "Seven-core multicore fiber transmissions for passive optical network," *Opt. Express* **18**, 11117-11122 (2010).
15. H. Takara, A. Sano, T. Kobayashi, H. Kubota, H. Kawakami, A. Matsuura, Y. Miyamoto, Y. Abe, H. Ono, K. Shikama, Y. Goto, K. Tsujikawa, Y. Sasaki, I. Ishida, K. Tokenaga, S. Matsuo, K. Saitoh, M. Koshiba, and T. Morioka, "1.01 Pb/s (12 SDM/222 WDM/456 Gb/s) crosstalk-managed transmission with 91.4-b/s/Hz aggregate spectral efficiency," ECOC Postdeadline paper, Th.3.C.1 (2012).
16. D. Qian, E. Ip, M. Huang, M. Li, A. Dogariu, S. Zhang, Y. Shao, Y. Huang, Y. Zhang, X. Cheng, Y. Tian, P. Ji, A. Collier, Y. Geng, J. Linares, C. Montero, V. Moreno, X. Prieto, and T. Wang, "1.05Pb/s Transmission with 109b/s/Hz Spectral Efficiency using Hybrid Single- and Few-Mode Cores," in *Frontiers in Optics 2012/Laser Science XXVIII, OSA Technical Digest (online)* (Optical Society of America, 2012), paper FW6C.3.
17. B. J. Puttnam, R. S. Luis, W. Klaus, J. Sakaguchi, J.-M. Delgado Mendinueta, Y. Awaji, N. Wada, Y. Tamura, T. Hayashi, M. Hirano and J. Marcianite, "2.15 Pb/s Transmission using a 22 core homogeneous single-mode multi-core fibre and wideband optical comb," in *Proc. ECOC2015, PDP.3.1*.
18. K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty and A. J. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X* **2**, 041010 (2012).
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 and K P McCabe, "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New J. Phys.* **11**, 045012 (2009).
20. P. Eraerds, N. Walenta, M. Legre, N. Gisin and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New J. Phys.* **12**, 063027 (2010).
21. K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty and A. J. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.* **104**, 051123 (2014).
22. R. Kumar, H. Qin and R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," *New J. Phys.* **17**, 043027 (2015).
23. I. Choi, R. J. Young and P. D. Townsend, "Quantum information to the home," *New J. Phys.* **13**, 063039 (2013).
24. A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martin, "Quantum metropolitan optical network based on wavelength division multiplexing," *Opt. Express* **22**, 1576-1593 (2014).
25. B. Fröhlich, J. F. Dynes, M. Lucamarini, A.W. Sharpe, S. W.-B. Tam, Z. Yuan and A. J. Shields, "Quantum secured gigabit optical access networks," *Sci. Rep.* **5**, 18121 (2015).
26. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express* **21**, 24550-24565 (2013).
27. 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**, 041114 (2007).
28. G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," *Lect. Notes Comput. Sci.* **765**, 410-423 (1993).
29. <https://www.alcatel-lucent.com/products/1625-lambdaxtreme-transport>.

1. Introduction

Quantum key distribution (QKD) is emerging as a powerful technique for secure distribution of encryption keys between remote parties [1-4]. It guarantees the security of the distributed keys using the fundamental constraints of quantum mechanics as well as providing the ability to detect an eavesdropper. Underpinned by many new developments, including the establishment of a quantified security level [2], QKD technology has matured considerably in the last decade. Furthermore the technology is making the transition from the laboratory to successful field trials [3-8].

As the bandwidth demands on data communication increases, multiplexing over different degrees of freedom in conventional single-core single-mode fiber (SSMF), including wavelength, phase, time and polarization multiplexing, is being utilized to circumvent the future information capacity crunch [9]. With help of advanced coding formats, these multiplexing techniques have allowed a channel capacity of up to 100 Tb/s per SSMF [10]. To prevent future saturation, space division multiplexing (SDM) was proposed to further increase the data bandwidth [11-14]. SDM can now be effectively realized by fabricating fibers with multiple single or few mode cores possessing low loss and crosstalk. These could replace

standard SSMFs in telecoms systems to improve the bandwidth to the Pb/s regime [15-17].

Novel multicore fibers (MCF's) are also an excellent opportunity for QKD. Previously, operation of QKD systems usually required dedicated SSMFs, which are not only expensive but might even be unavailable. Multiplexing QKD into data-populated SSMF has been explored, but it constrains either the communication distance or the launched data laser power and maximum bandwidth [8, 18-25]. These constraints are a consequence of signal contamination to the quantum channel by the Raman photons generated by the strong data signals in the same fiber. Future MCF deployment could allocate one core for quantum signals only, therefore permitting simultaneous transmission of QKD and data signals through the same fiber without severe restriction on the data launch power or bandwidth. This opportunity has not been explored to date, however.

In this paper we report the first QKD experiment over MCF. After a careful characterization of crosstalk of a 7-core MCF of 53-km length, we run QKD continuously for a duration of 24 hours in the presence of spatially multiplexed bi-directional 10 Gb/s data signals launched at 0 dBm power. We compare the MCF results with a dual SSMF setup and find no performance penalty associated with the use of MCF. Moreover, a simulation based on the measured parameters shows that MCF can support a simultaneous transmission of QKD and Tb/s data in the same fiber.

2. Multicore fiber characterization

The MCF selected for the experiment is 53 km in length, and has a cladding diameter of 185 μm and 7 cores with a core-to-core distance of 47 μm , see Fig. 1(a). Each core supports a single optical mode, and has similar transmission characteristics as a standard telecom SSMF. For example, the central core of the MCF is measured to have an attenuation of 0.23 dB/km at 1550 nm, which is only slightly higher than the SSMF which has a typical loss rate of 0.20 dB/km. It is noteworthy that the MCF's diameter is only a factor of 1.5 larger than that of a standard SSMF. At the same time, the MCF displays a 7-fold increase in achievable bandwidth due to the increased spatial capacity. This highlights MCF's potential to increase the communication bandwidth when incorporating into current telecoms systems [15-17].

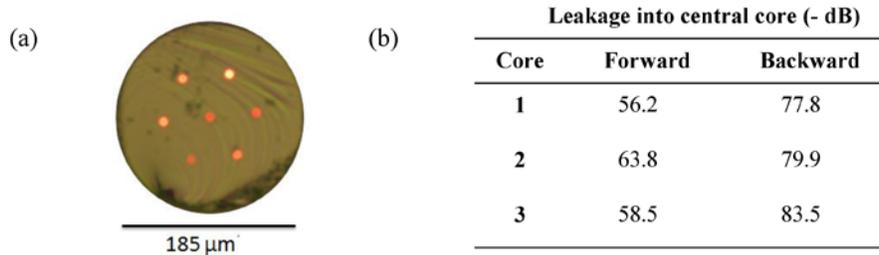


Fig. 1. (a) Optical microscope images showing cross-sections of the multicore fiber (MCF); The MCF was manufactured by OFS Labs. (b) Power leakage into the central core measured in decibels from 3 outer cores. A 1550 nm laser is used in this measurement.

Optical crosstalk between MCF cores must be carefully characterized, because of its possible impact on the quantum channel which operates in the single photon regime. We consider two types of crosstalk. First, photons transmitted in one core can transfer into adjacent cores through evanescent field coupling. We term this type as *leakage*, and the leaked photons have the same wavelength as the launched signal. The second type is *Raman crosstalk*, scattered from neighboring cores where strong data signals are present. To characterize these two types of crosstalk, we assign the central core of the MCF as the quantum channel and the outer cores for classical signals. This configuration allows all classical signals to impact the quantum channel equally, and thus is the most suitable to evaluate the MCF's applicability to QKD. A laser power of 0 dBm (1 mW) is launched into

one of the outer cores at a time, and we then measure the optical power exiting from the central one at either the launch end (i.e.: backward scattered signal) or the receive end of the MCF fiber (i.e.: forward scattered).

We measure the leakage signal from different outer cores with results summarized in Fig. 1(b). Here, the leakage value is calculated as the ratio of the optical power exiting from the central core to the launch power into the outer one. The forward and backward leakage signals are around 60 and 80 dB weaker than the launched signal, respectively. The latter is lower because Rayleigh backscattering is required in addition to intercore evanescent field coupling. At the given data launch power of 0 dBm, the forward leakage level shown in Fig. 1(b) corresponds to a noise intensity on the order of 10 photons/ns, which is about 100 times stronger than the received quantum signal expected for a weak-pulse QKD system. This level of contamination therefore necessitates applying noise rejection techniques. Thankfully, the leakage signals have well-defined wavelength, which is the same as that of the data laser, so they can be effectively removed spectrally by a standard DWDM filter in the quantum receiver. It has been previously shown [21] that even 0 dBm data signal within the same fiber core can be effectively filtered.

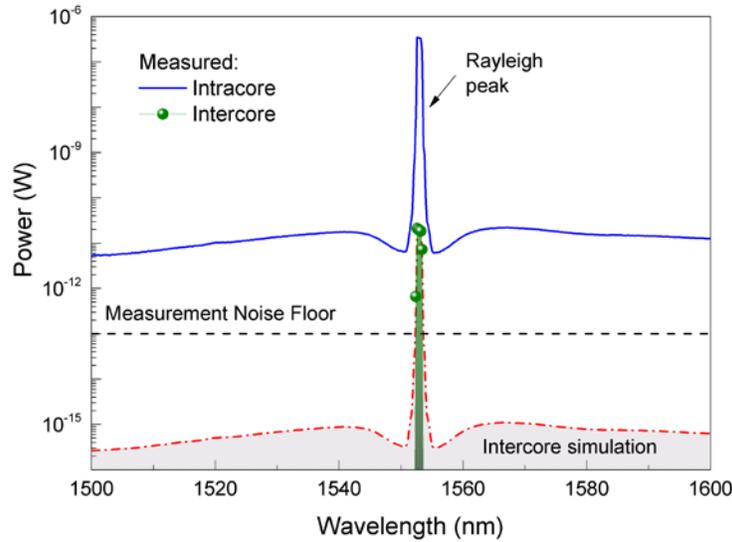


Fig. 2. Spectra of backscattered signals into the same outer core (intracore, blue line) or the central core (intercore, green dots) in the presence of a 0 dBm power of a 1552-nm laser launched into an outer core. The dashed line shows the noise floor of the optical spectrum analyzer used in the measurement. The dash-dotted line shows the simulated Raman crosstalk.

We attempt to measure the Raman crosstalk in the backward configuration only. This is because we expect backward scattering to be stronger than forwards scattering as the backscattered signal is attenuated less by the fiber. We use an optical spectrum analyzer (OSA) to spectrally resolve the signal scattered into the central core. However, this intercore Raman signal is below the noise floor of the OSA and too weak to be measured. As shown in Fig. 2, we resolve only a sharp peak (green dots), caused by the backward leakage, at the same wavelength as the launch laser. To deduce the Raman crosstalk, we instead measure the backward Raman signal exiting from the same outer core. As shown in Fig. 2, the intracore spectrum is essentially identical to that of a SSMF [18]. The Raman signal distributes over a wide spectrum exceeding 100 nm, and its peak intensity is about 40 dB lower than the Rayleigh peak. To quantify the Raman crosstalk we assume that it has the same spectral shape as for intercore scattering, however, with a 40 dB lower intensity as suggested by the difference of inter- and intracore Rayleigh peak. The Raman crosstalk is below 1 fW over the entire spectral range. This level of noise is negligible relative to the quantum channel power and is expected not to affect the operation of QKD.

3. QKD/data spatial multiplexing setup

Figure 3 shows our experimental setup. The 53-km, 7-core MCF spool forms the optical channels between two communicating parties, Alice and Bob. At each end of the fiber, all transmitters or receivers are terminated with SSMF's. Optical coupling between SSMF's and MCF is realized through two 1×7 fanouts featuring a coupling loss in the range of 1.0 – 4.6dB.

We use a QKD system operating with a clock rate of 1 GHz and using the T12 decoy-state protocol [26]. The photons are detected with InGaAs avalanche photodiodes operating in Geiger mode and with self-differencing [27] electronics. While crucial for noise rejection in SSMF multiplexing [18], the temporal filtering capability offered by the detectors is less important in the present spatial multiplexing setup. Optical crosstalk from other channels (cores) is much less than in the SSMF case since space division gives >40dB isolation. The QKD system utilises a fully automatic FPGA control for stabilising the photon count rate and quantum bit error rate (QBER) through feedback control of the polarization controller, fiber phase delay and system delay. Error correction is accomplished using Cascade [28] and a number theoretic transform approach to execute efficient matrix multiplication is utilized for privacy amplification.

The QKD system requires a quantum channel and auxiliary classical channels for clock synchronization and key reconciliation. We assign two cores of the MCF for these signals: the central core is to carry the weak quantum signal while one of the outer cores for the QKD auxiliary classical signals. The spare 5 outer cores are free to use for intense classical data communication signals. The quantum signal is transmitted on the DWDM grid with a wavelength of 1547.72 nm while all classical signals are transmitted at other wavelengths. This arrangement allows rejection of the intercore leakage into the quantum channel using a standard DWDM filter of 0.4 nm passband located in the quantum receiver. A pair of 10 Gb/s data channels, with 0 dBm power each launched into separate cores from opposite directions, are assigned at the wavelength of 1552.72 nm.

The quantum channel has a total loss of 14.1 dB, consisting of 12.4 dB due to the MCF, 1.1 dB loss at the optical fanout and 0.6 dB at the DWDM filter.

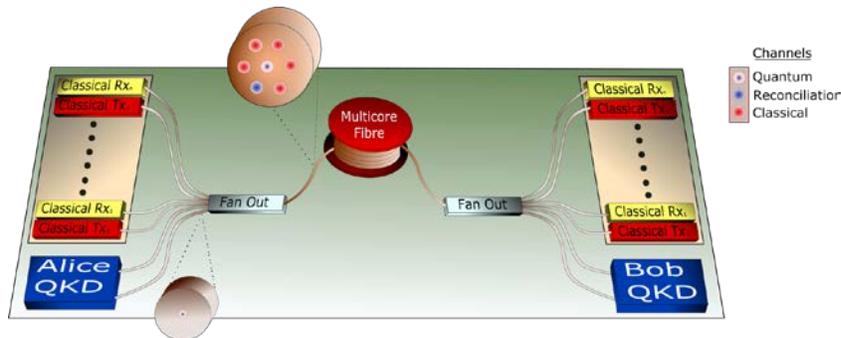


Fig. 3. QKD over MCF experimental setup.

4. Results and discussion

We operate the QKD system over the central core of the MCF while bi-directional 10Gb/s classical signals are transmitted simultaneously through two of the six outer cores. A bit-error tester is used to monitor the data communication. It typically does not record a single error during the experiments. Figure 4 plots the secure key rate and quantum bit error rate (QBER) over a 24 hour period. These values are obtained through real-time data-processing, including error correction and privacy amplification, on a sifted block size of 1×10^8 bits. The block size is sufficiently large to achieve 85% of the asymptotic secure key rate [26]. Each data block is collected over a session time of about 36 seconds with a sifted bit rate of ~ 2.7 Mb/s. Over the

entire measurement, the QBER displays a very small fluctuation around its average value of 3.36% with a standard deviation of 0.54%. The secure bit rate fluctuates more visibly, because of its sensitivity to the QBER with an average secure key rate of 605 ± 18 kb/s. This result represents the first QKD operation over MCF, and also the first demonstration of spatial mode multiplexing of data and QKD over the same fiber.

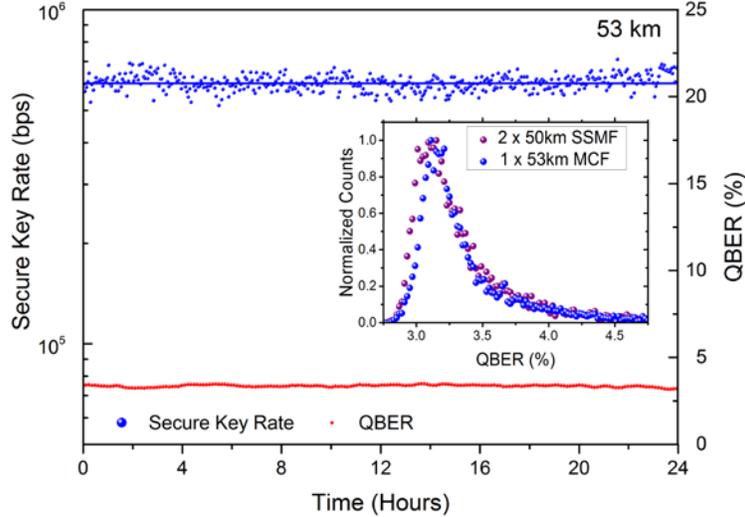


Fig. 4. QKD results over 53 km of MCF in the presence of 10 Gb/s bi directional classical traffic launched at 0 dBm in outer cores. The solid blue line indicates the average value of the secure bit rate. Inset: Comparison of the histograms of instantaneous QBERs obtained with MCF and standard SSMF's.

We compare the above MCF result with a control experiment over standard SSMF's. We use two 50-km SSMF spools to replace the MCF. Quantum signals are transmitted through one spool, while all classical signals are transmitted through the other. The physical separation of these signals ensures zero crosstalk. Extra attenuation is added to the quantum channel to be consistent with the MCF experiment. All other experimental parameters remain identical to the MCF case. QKD over the SSMF's yields a secure bit rate of 619 kb/s and a QBER of 3.36% averaged over a duration of four hours. Within statistical error, there is no significant impairment in performance using the MCF compared to two SSMFs. This demonstrates that neither the MCF, nor the intense 10G data signals on the same MCF cause a performance penalty, except for the higher attenuation of the MCF which may be improved with better quality fiber and coupling in the future. The inset of Fig. 4 compares the distributions of instantaneous QBERs recorded with a ~ 0.5 second sampling time, to detect difference in the disturbance to the quantum signal by different fibers. Nearly identical distributions suggest that the MCF has a very similar optical characteristics to standard telecom SSMF.

We simulate the impact of higher power data signals on the QKD performance assuming equal-power bidirectional data launched into the separate outer cores. As the Raman coefficient is wavelength dependent, we choose a worst-case scenario in which both forward and backward data channels produce the maximum Raman scattering to the quantum channel. The scattering coefficient is obtained from the intracore scattering measurement corrected by the amplitude difference in Rayleigh peaks (Fig. 2). Parameters for the QKD system are taken directly from experimental values, including clock frequency, channel attenuation, detector efficiency and dark count rate.

Figure 5 shows the simulation results. In the absence of data channels, our simulation gives a theoretical secure key rate of 627 kb/s and a QBER of 3.36%. These values do not degrade noticeably for an increasing combined power of data channels of up to 100 mW, or 20 mW

per core. Accounting for the optical crosstalk into the quantum channel, this power level is well below the point at which non-linear effects are expected in DWDM transport systems [19]. Moreover, they are in excellent agreement with measured values in both MCF (2×1 mW) and SSMF (crosstalk free) experiments. Further increasing the data launch power causes a gradual increase of QBER and hence a reduction in the secure key rate. Nevertheless, the simulation still predicts the co-existence of QKD with more than 1 W of data laser power in each direction. This highlights the potential of the MCF spatial multiplexing technique to support QKD along with high bandwidth data transport. DWDM systems containing 128 channels are now commercially available [29] and if a full-power 10Gb/s per channel system was deployed in each of the 5 spare outer cores, this would correspond to a combined power of only 320 mW in each direction and a total of 6.4 Tb/s of bidirectional classical information simultaneously transmitted with a high rate QKD channel.

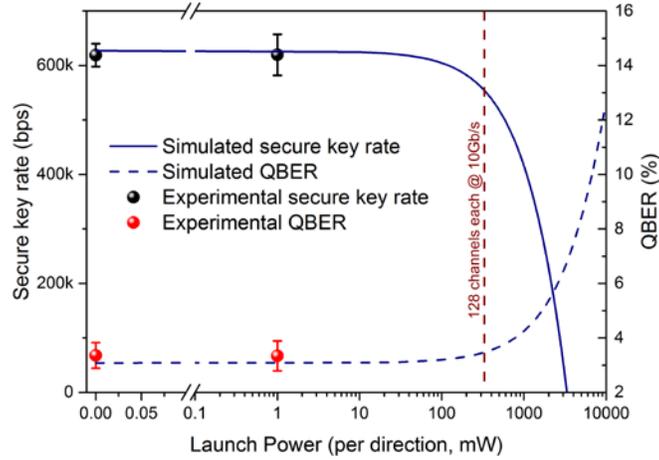


Fig. 5. Simulation of QKD performance over the 53 km MCF in the presence of bidirectional data communication, using the worst-case scenario of Raman crosstalk into the quantum channel. Also shown is the total launch power of 1 mW, 128×10 Gb/s channels (brown dashed line).

5. Conclusion

In this paper, QKD has been successfully demonstrated through MCF for the first time. Our experiment demonstrates that standard 10 Gb/s bi-directional traffic can be spatially multiplexed onto the same MCF without detrimental effect on the performance of the QKD. Secure key rates averaging at 605 kb/s are successfully transmitted over 53 km of MCF continuously for a 24 hour period. Furthermore, our calculation suggests that QKD can potentially coexist with Tb/s bidirectional data traffic on the same fiber.

Acknowledgment

S.J.K. acknowledges support from the EPSRC CDT in Photonic Systems Development.