Quantum networks in the UK

Adrian Wonfor*[a], Catherine White[b], Andrew Lord[b], Reza Nejabati[c], Timothy P. Spiller[d], James F. Dynes[e], Andrew J. Shields[e] and Richard V. Penty[a]
[a]Department of Engineering, University of Cambridge, Cambridge, UK, [b]BT Labs, Adastral Park, Ipswich, UK, [c]Department of Electrical Engineering, University of Bristol, Bristol, UK, [d]Department of Physics, University of York, York, UK , [e]Toshiba Research Europe Ltd., Cambridge Research Laboratory, Cambridge, UK.

ABSTRACT

We describe recent progress in quantum secured optical networks in the UK. The Cambridge Quantum Network has been operating for several years with 3 nodes separated by between 5-10 km of installed fibre. All links are secured by QKD systems operating with secure key rates in excess of 1 Mb/s, the highest recorded long term key rates in a deployed network. The network operates in the presence of 100Gb/s classical traffic with no significant reduction of secure key generation rate. In addition, the Bristol Quantum Network has four nodes 1-3km apart connected in a mesh protected by two pairs of QKD systems. The network is designed to be very dynamic, switching both QKD and WDM classical traffic to enable rapid reconfiguration and is used as a testbed for QKD protected dynamic applications. The two metropolitan networks are being connected by a 410 km QKD link, with 4 spans, the longest of which operates over 129km of fibre with an attenuation of 28dB achieving secure key rates of 2.7kb/s, the longest and highest loss QKD field trial to date. A 120km extension of the UK quantum network from Cambridge to BT Labs, Adastral Park operates with fully commercially available components and is an important testbed comprising 3 intermediate nodes and operates with 5 x 100Gb/s classical channels. This helps determine how to proceed with a large-scale commercial deployment of QKD.

Keywords: Quantum Key Distribution, Quantum secured networks, Quantum Networks, co-existing quantum and classical transmission, Quantum Cryptography, Optical Communications.

1. INTRODUCTION

It is clear that the need to secure network infrastructure is becoming ever more pressing[1], and with the advent of ever more capable quantum computers[2], using Shor's algorithm[3], the long term security of public key cryptography[4,5] is increasingly in doubt. While quantum resistant algorithms show promise, especially with the work of NIST in securing good candidates[6], they still rely on computational complexity and have the potential to be compromised in the future.

Quantum cryptography[7–9] brings the capability of robustly securing data transmissions across optical networks, relying on the laws of quantum mechanics, rather than computational complexity. This security does come at a cost however, as the information in quantum cryptography is carried by a quantum state, frequently by a single photon, which makes simultaneous transmission of both quantum keys and classical data challenging. Indeed early quantum networks used an additional dark fibre[10–14] for the quantum channel, separated from classical data traffic.

There have been many laboratory demonstrations of point-to-point Quantum secured links in which both the the quantum and classical channels are transmitted down the same fibre using both single photon 'discrete variable'[15–20] and coherent state 'continuous variable'[21,22] forms of QKD. These point-to-point laboratory experiments have advanced to field trials[23,24] and then on to multiple node network demonstrations, both in the laboratory[25,26] and field demonstrations[27–32]. It is convenient to summarise QKD link and network demonstrations in table 1. We can see that the Cambridge Quantum Network has operated reliably with consistently high secure key rates for periods exceeding a year.

*aw300@cam.ac.uk

Table 1. Comparison of QKD link and network trials

	Tokyo QKD network[13]	Geneva QKD network[14]	Hefei-Wuhan QKD network[31]	Zhucheng-Huanshang QKD link[23]	Cambridge quantum network[32]
Node number	6	3	9	2	3
Longest link length (loss)	45km (14.5dB)	14.4km (5.6dB)	85km (18.4dB)	66km (13dB)	10.6km (3.9dB)
Data multiplexing	No	No	No	Yes	Yes
Continuous operation	1 day	600 days	212 days	180 mins	580 days
Secure key rate	300 kb/s	2.4 kb/s	16.2 kb/s	6 kb/s	2.5 Mb/s

In this paper, we will report on quantum networks in the UK, both metropolitan networks in Cambridge and Bristol and also longer distance networks linking them and BT research labs in Ipswich. The geographical layout of these locations and the interconnecting QKD links are shown in figure 1. It should be noted that owing to the geography of the UK, extremely long and impressive QKD networks such as that between Beijing and Shaghai[33] are impractical, so we try to incorporate the key elements on a smaller ~500km scale

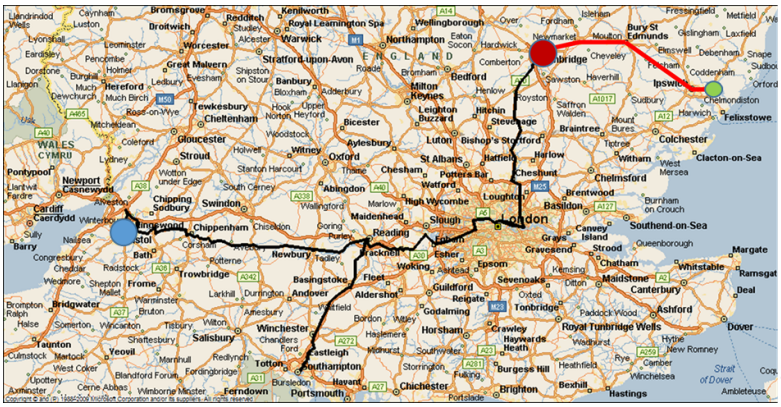


Figure 1. The UK Quantum network, connecting Cambridge (red circle) with Bristol (blue circle) and BT labs (green circle). Credit Google maps.

2. METROPOLITAN QKD NETWORKS

2.1 Cambridge quantum network

The Cambridge Quantum Network was initially constructed with three nodes, each separated by between 5.0 and 10.6 km of standard fibre within the network infrastructure operated by the University of Cambridge. The network connects the Electrical Engineering dept., the main Engineering dept. and Toshiba Research Europe's Cambridge Research Lab, as shown in figure 2. Additional nodes are being added to bring additional connectivity to the University's data centre and biomedical campus, but are not reported here.

The network operates with QKD systems on each leg of the network, this creating a high speed 3 node metropolitan ring network. The QKD infrastructure is produced by Toshiba[34] with the quantum channel operating at 1550nm. This system is capable of producing secure key rates in excess of 3Mb/s, this providing a rapid supply of quantum keys to the ADVA FSP 3000 classical data encryption systems used to provide 2 x 100Gb/s of secured data transport at 1530nm within the

network. These classical data systems have been modified so that their AES encryptors accept QKD keys, rather than using conventional Diffie-Hellman key exchange.

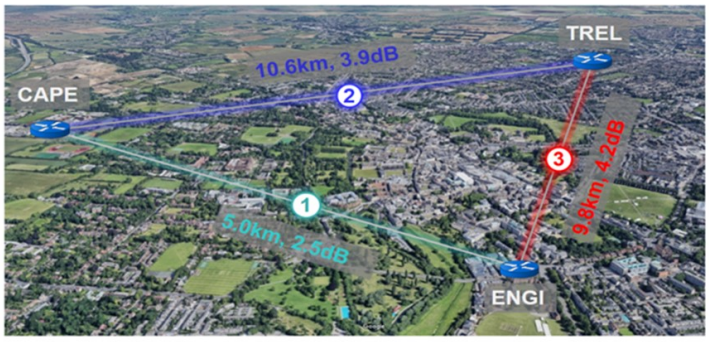


Figure 2. The Cambridge quantum network, connecting the University of Cambridge's Electrical Engineering building (CAPE), Engineering dept (ENGI) and Toshiba Research Europe (TREL). Fibre lengths range from 5.0 to 10.6km, with losses between 2.5 and 4.2dB. Credit Dynes et al[32].

Each leg of the network produces its own secure keys, which are consumed by a network key delivery layer[32,35] which serves keys to applications within the network, such as the 100Gb/s data encryption cards used to secure the classical traffic.

As with all QKD networks carrying classical data, an optimization of the classical channel optical powers is required. Most high bandwidth optical transmission systems are designed to operate at powers of the order of 0dBm, but this can prove to be problematic for QKD systems which typically operate at powers below -70dBm, as leakage through optical filters as well as Raman scattering in the optical fibres can add noise to the quantum channel. These issues can be mitigated by a modest reduction of the launch power of the classical data channels. Figure 3 shows a simulation[18,32] of the effect of classical optical power at the receiver on the Quantum bit error rate (QBER) as well as the pre forward error correction (FEC) bit error rate (BER) on the classical channel. It can be seen that operating the classical channel at powers of -7dBm has negligible effect on the QBER, while keeping the pre FEC BER better than 10^{-4}.

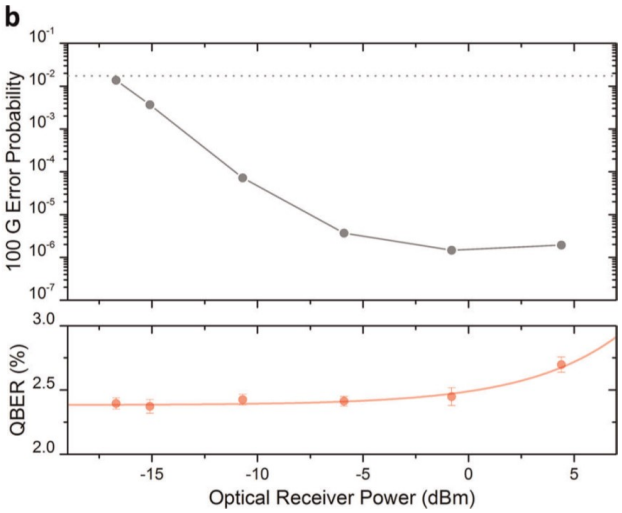


Figure 3. The effect of received optical power of the high data-rate classical channel on both the pre FEC BER of the classical channel and the QBER of the quantum channel. Credit Dynes et al[32].

Successful operation of the quantum network over extended periods of greater than 1 year has been achieved with 2 x 100Gb/s of traffic on link 2 of figure 2 and also with 100Gb/s on all links, configurations being constrained by the availability of 100Gb/s line cards. Typical secure key rates and QBERs for the network are shown in figure 4. It can be noted that the long term stability of the network was excellent, with QBERs below 5% and secure key rates in excess of 100Gb/s in the presence of 100Gb/s classical traffic.

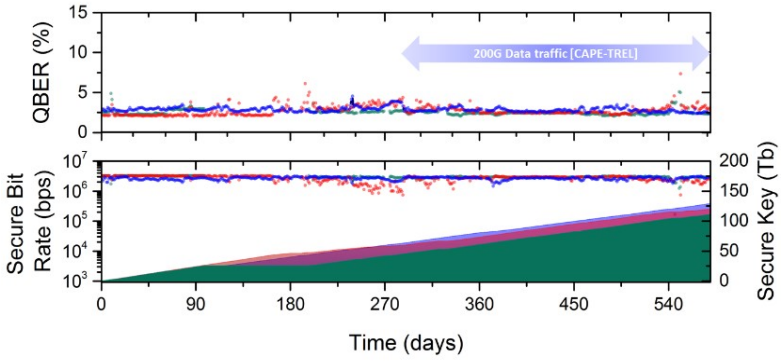
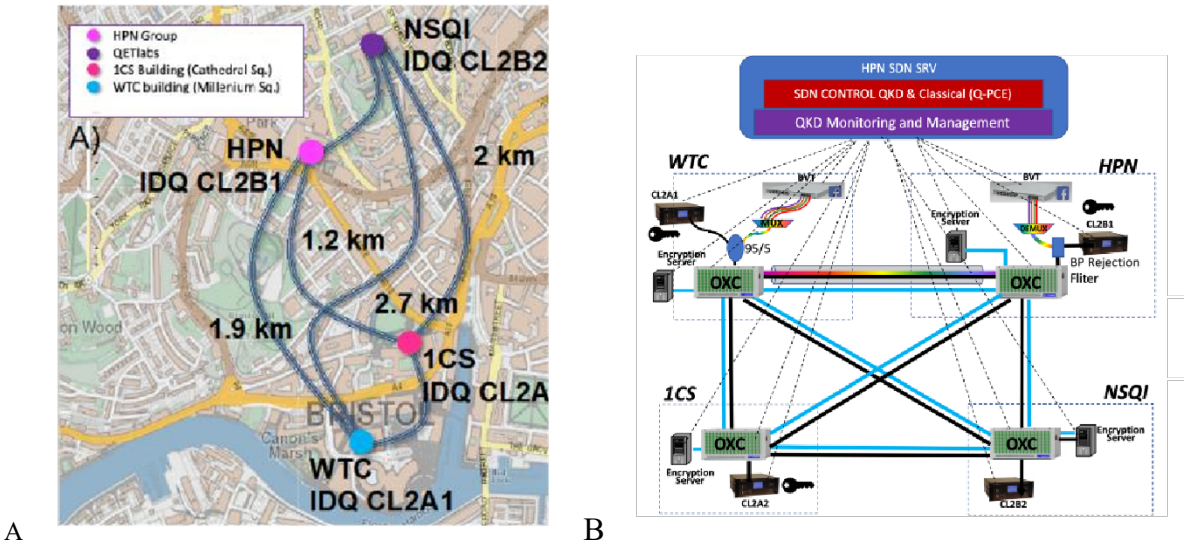


Figure 4. QBER, secure key rate and total key volume of 580 days operation of the Cambridge Quantum Network. Data in blue represent the CAPE-TREL segment, red the TREL-ENGI and green the ENGI-CAPE segments, as shown in figure 2. Credit Dynes et al[32].

2.2 Bristol QKD network

The Bristol QKD network[36], as shown in figure 5a, comprises four nodes at the University of Bristol and locations in the city, connected by six fibre pairs which are between 1.2 and 2.7km long forming a mesh network. The primary aim of this network is to enable research into dynamically switched software defined networks protected by QKD[37,38]. In order to accomplish this the nodes use two pairs of Clavis 2 QKD systems from ID Quantique. Figure 5b shows that each node comprises an optical cross connect, enabling the QKD signal to be re-routed dynamically between paths and wavelength division multiplexed optical channels to be arbitrarily routed around the network, coping with fibre breakages or changes in demand.



A B

Figure 5a. Bristol QKD network, with four nodes and two pairs of ID Quantique Clavis 2 QKD systems. Figure 5b shows schematically the network configuration, including optical cross connects and high bandwidth WDM classical channels. Credit Kanellos et al[36].

3. LONG DISTANCE QKD NETWORKS

The UK Quantum network, part of the EPSRC Quantum Communications Hub[39], is designed to encompass and connect both the quantum networks in Cambridge and Bristol and further connect to BT Labs at Adastral Park Ipswich. This has two major components, the connection between Cambridge and Bristol and also the extension from Cambridge to

Adastral Park. The latter is designed to use only commercially available sub-systems, providing a test-network to learn the challenges involved in large scale commercial deployments of quantum secured networks.

3.1 The UK Quantum network between Cambridge and Bristol

The linking of the two research centres at Cambridge and Bristol is facilitated by the UK National Dark Fibre Facility[40] (NDFF). The 410 km dark fibre link is available on a time-shared basis to connect both sites via a number of intermediate locations, some of which are quite widely spaced, providing a challenge for QKD.

Initial tests on the long haul quantum links were carried out by launching from Cambridge and looping back at the first node on the NDFF, 33km away at Duxford. This then provided a 66km round trip field trial over installed fibre with 17dB attenuation. The field trial over this link was conducted in a similar way to the setup of the Cambridge Quantum Network, but with both the QKD transmitter and receivers co-located in the Cambridge Electrical Engineering building. Figure 6 shows the configuration of the initial field trial performed on the first part of the NDFF, An ADVA FSP 3000 shelf comprising two 100Gb/s encrypted line cards (10TCE muxponder cards, with 10 x 10Gbls tributaries and 1 x 100Gb/s output) is connected to the Toshiba QKD transmitter (blue and green lines). The output from the QKD transmitter comprising the classical and quantum channels (orange line) is launched down the 66km of field trial fibre. Upon its return the optical signal is injected into the QKD receiver, which outputs the classical wavelengths to the other ADVA shelf. Each of the QKD systems inject the distilled secure QKD key to the ADVA shelves, which use them as keys for the 100Gb/s AES encrypted transceivers.

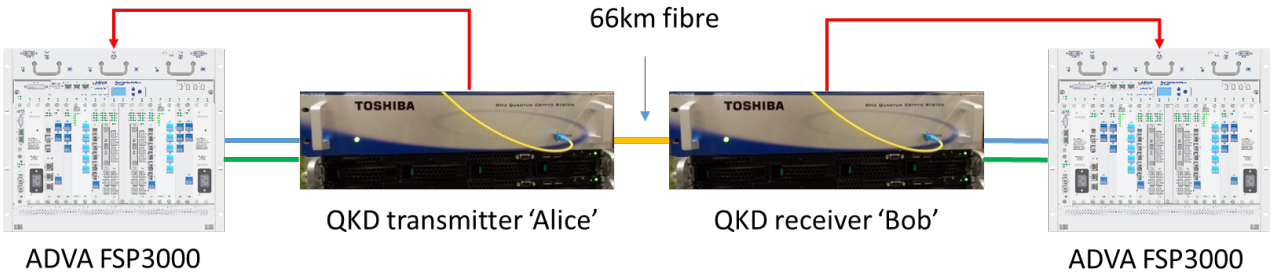


Figure 6. shows the configuration of the initial field trial performed on the first part of the NDFF, with ADVA classical transponders and QKD transmitter and receiver co-located in Cambridge, connected by the 66km field trial fibre.

The physical location for the fibre in the field trial is shown in figure 7a, with typical QBERs and secure key rates achieved over the link shown in figure 7b. Over a three-week trial, a QBER of 6.6 ± 0.5% was achieved, with a secure key rate of 80 ± 28kb/s. This represents the highest sustained secure key rate for a long distance field trial in the presence of classical traffic.

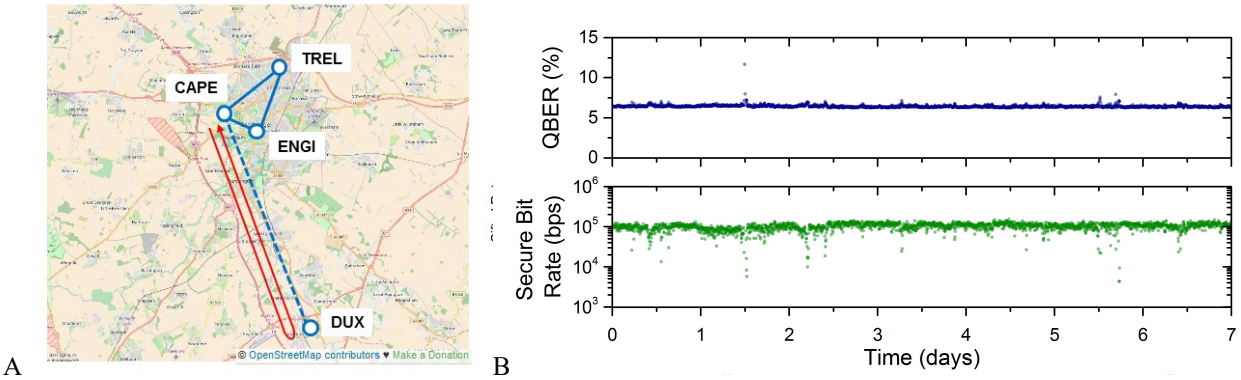


Figure 7a shows the layout of the initial field trial, with the 66km loop back from Cambridge to Duxford and back to Cambridge. Figure 7b shows both the QBER and secure key rate for this link, in the presence of 200 Gb/s of classical data. Credit Dynes et al[32]

Successful operation of the mini field–trial paved the way to using the NDFF to connect Cambridge to Bristol. Figure 8 shows a schematic of the fibre plant within the NDFF. The first part of this link is much the most challenging, having the

first link connecting Cambridge to Telehouse (the principal London internet exchange). The first node is bypassed at Duxford by connecting the two fibre pairs together producing a single span of 129km, with 28dB of loss. Subsequent spans are not as challenging as the distances and losses between nodes are lower.

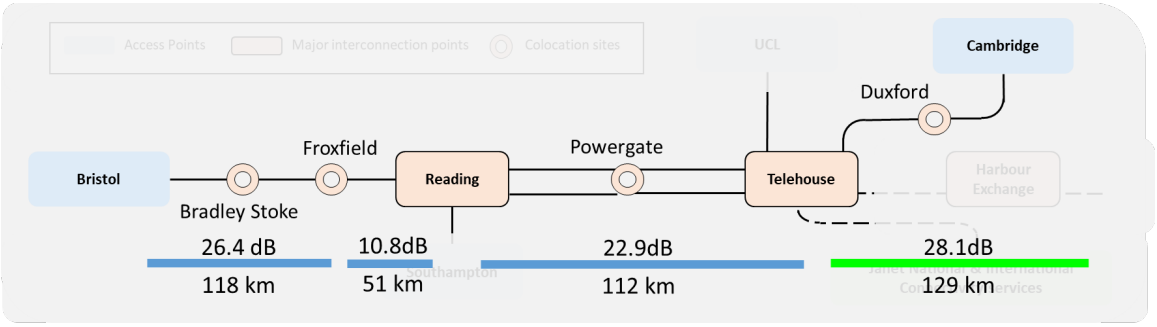
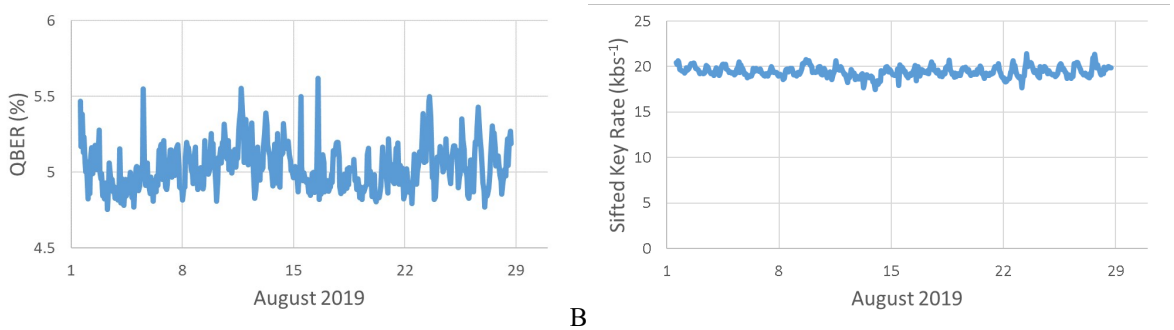


Figure 8 shows the layout of the UK quantum network between Cambridge and Bristol. The first span is both the longest and highest loss at 129km with 28dB loss. The other three spans are lower loss and therefore more straightforward.

The first span of the UKQN from Cambridge to Telehouse London was deployed in 2019. Optimised QKD systems were used, with optical amplification at the receiver for classical discussion and synchronization channels, enabling operation with up to 30dB loss. This link (shown in green in figure 8) performed very well with 3 months of continuous operation in the period when we were given the fibre. Figure 9a shows the QBER, of 5.0 ± 0.1 % whilst figure 9b shows the sifted key rate of 19.4 ± 0.6 kb/s for a sample week's operation. Figure 10 shows the secure key rate of 2.7 ± 0.3 kb/s, which remained stable over the 3 month trial, until the link was surrendered in November 2019. This is believed to be the longest, highest loss single fibre span field trial yet reported.



A B

Figure 9a QBER and 9b sifted key rate for the long distance link in the UKQN.

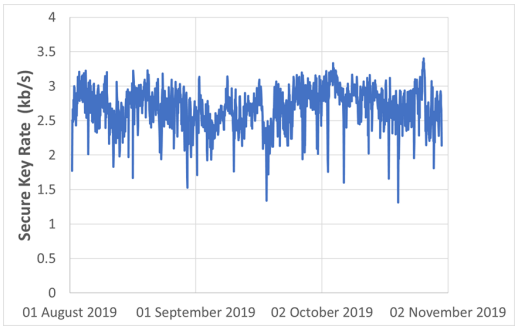


Figure 10 Secure key rate for the long distance link in the UKQN over a period of three months.

It was anticipated to complete the UKQN, using the other 3 links (shown in blue in figure 8) in 2020. Unfortunately, restrictions in research operations off site have been imposed owing to the COVID-19 outbreak in the UK, which prevent access to the network locations within the NDFF. At the time of writing it is anticipated that restrictions will be eased soon enabling the completion of this link in 2021. All three systems remaining to be deployed have been tested in the laboratory and are predicted to function well.

3.2 The UK Quantum network Telecom extension (UKQNTel) between Cambridge and BT Labs

In addition to the UKQN from Cambridge to Bristol, another QKD secured link has been deployed between Cambridge and BT Labs at Adastral Park, near Ipswich, this is shown for context as the red section in figure 1. This link comprises 120km of fibre with three intermediate nodes, as shown in figure 11. The purpose of the UKQNTel is to test the ease of integration of QKD into real world network and develop use cases and procedures for widespread deployment of QKD secured networks in commercial optical networks

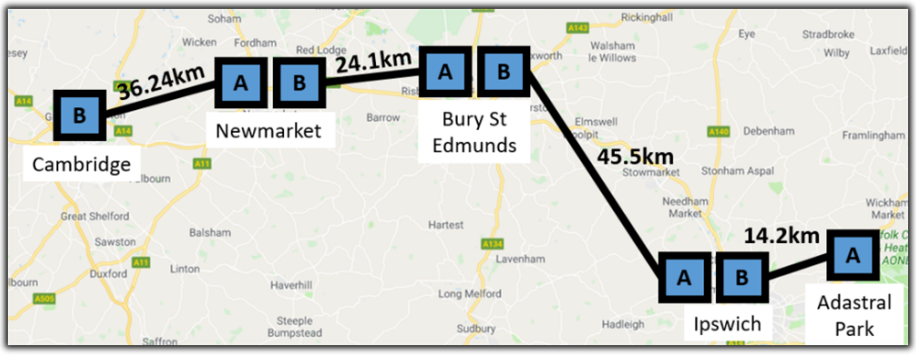


Figure 11 Schematic of the layout of the UKQNTel addition to the UK .

Figure 12 shows the principal design elements of the UKQNTel[41] which has an end-to-end classical data path, comprising 5 x 100Gb/s data channels in the c band at 1550nm, these classical channels are amplified at each of the intermediate nodes. The QKD systems are modified Clavis 3 systems from ID Quantique, with the quantum channel at 1310nm. At the transmitter node the classical channels are multiplexed and then optimized in power and then combined with the signal from the quantum transmitter at the final stage. At each intermediate node the quantum signal is dropped first to go immediately to the quantum receiver (this minimizes both optical noise and loss). The classical signal is amplified and the power of all non-quantum channels is optimized for onward transmission. At the final stage the next quantum transmitter is multiplexed back on to the channel. At the receive end of the link the quantum channel is dropped to the quantum receiver and classical channels are amplified and demuxed to their respective transponders.

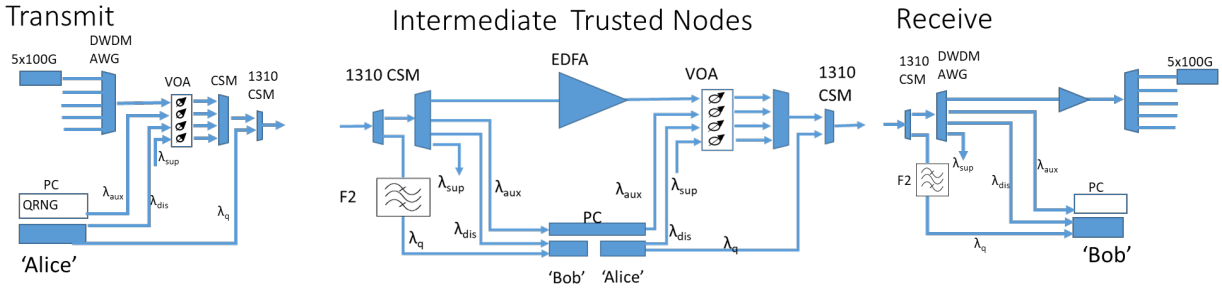


Figure 12 Schematic of the layout of the UKQNTel addition to the UKQN. λ_q :quantum channel 1310nm, λ_{dis} :discussion channel 1530nm, λ_{aux} :QKD management and key management traffic channel 1529nm, λ_{sup} :Adva FSP-3000 supervisory channel 1510nm, F2 :Additional narrow bandwidth 1310nm bandpass filter

Figure 13 shows the long term performance of the UKQNTel with the secure key rates of all of the links within the network. It can be seen that the longest link has the lowest secure key rate of 763 b/s was achieved over the 45.6 km span, with a loss of 18.8dB at 1310nm. This is the limiting rate for the entire link, as the keys are passed from one end of the network to the other using trusted nodes at each intermediate point. These perform an XOR operation between a random number produced by a quantum random number generator at the transmitter and with keys derived from each span. At each intermediate span the random key generated at the beginning is XOR'd with the received key from the incoming span and also XOR'd with the key of the outgoing span. A final XOR operation at the final receiver recovers the random number originally sent. Thus, the lowest rate span is the limiting step for the entire network.

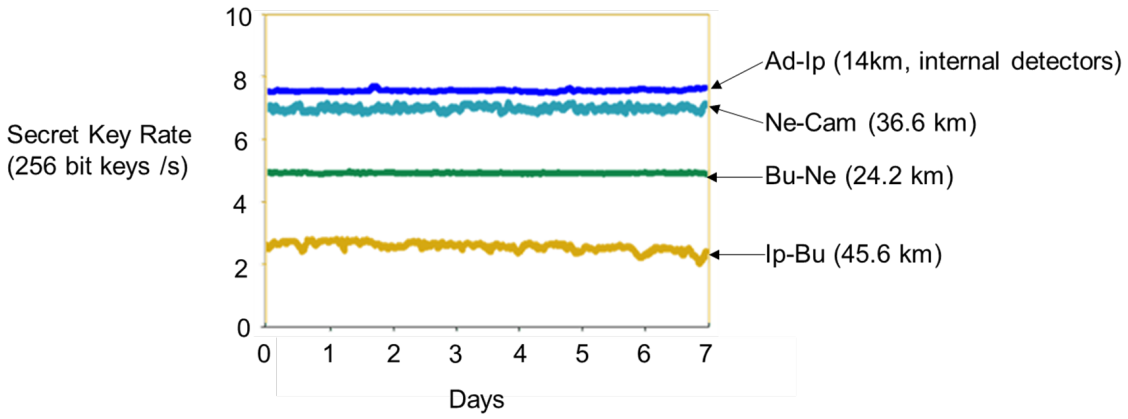


Figure 13 Secure key rates generated by each span within the UKQNTel.

4. CONCLUSIONS

There are a number of quantum communication networks within the UK, performing several different roles, yet unified by the UK Quantum Communications hub. A metropolitan network in Cambridge has sought to optimize the performance of QKD systems in the presence of 100Gb/s classical traffic encrypted with AES using quantum derived keys, reaching secure key rates in excess of 1 Mb/s over several years operation. Efficient key management has also enabled significant excess key material to be collected and made available for other network applications, such as ultra-secure one-time pad based transmission. This has proved to be the highest secure key rate field deployed network operating successfully for extended times.

In addition the Bristol quantum network has shown the capabilities of dynamic QKD networks for software defined networking and network function virtualization, in particular in the context of rapidly reconfigurable QKD protected 5G networks.

Longer haul networks, such as the 410 km UK Quantum Network from Cambridge to Bristol is nearing completion, delayed only by COVID-19 restrictions. The most challenging part of this network has been completed, with a single span of 129km and 28dB loss producing secure keys at a rate of 2.7 kb/s of many months. This is the longest and highest loss QKD link yet deployed.

Finally, the UKQNTel extension to the Cambridge Quantum Network, connecting Cambridge and BT labs has shown how to deploy commercial QKD equipment together with high data rate classical communications equipment in the challenging environment of deployed fibre networks, with nodes within active exchanges. This has proved to be an extremely valuable tool for understanding the challenges involved in large-scale commercial deployment of QKD secured communications.

5. ACKNOWLEDGEMENTS

This work has been funded by the UK EPSRC under the UK Quantum Technology Hub for Quantum Communications Technologies EP/M013472/1 and the EPSRC Quantum Communications Hub EP/T001011/1. The authors would like to acknowledge the EPSRC EP/S028854/1 National Dark Fibre Facility.

REFERENCES

[1] Ziegeldorf, J. H., Morchon, O. G. and Wehrle, K., “Privacy in the Internet of Things: threats and challenges,” Security and Communication Networks **7**(12), 2728–2742 (2014).

[2] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E.,

Foxen, B., et al., “Quantum supremacy using a programmable superconducting processor,” 7779, Nature **574**(7779), 505–510 (2019).
[3] Shor, P. W., “Algorithms for quantum computation: discrete logarithms and factoring,” Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134, IEEE Computer Society, Santa Fe, New Mexico (1994).
[4] Diffie, W. and Hellman, M., “New directions in cryptography,” IEEE Transactions on Information Theory **22**(6), 644–654 (1976).
[5] Rivest, R. L., Shamir, A. and Adleman, L., “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM **21**(2), 120–126 (1978).
[6] Computer Security Division, I. T. L., “Round 3 Submissions - Post-Quantum Cryptography | CSRC | CSRC,” CSRC | NIST, 3 January 2017, <https://content.csrc.e1c.nist.gov/Projects/post-quantum-cryptography/round-3-submissions> (25 February 2021).
[7] Bennett, C. H. and Brassard, G., “Quantum cryptography: Public key distribution and coin tossing,” Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, 175–179, Institute of Electrical and Electronics Engineers, New York, Bangalore, India (1984).
[8] Bennett, C. H. and Brassard, G., “Quantum cryptography: Public key distribution and coin tossing,” Theoretical Computer Science **560**, 7–11 (2014).
[9] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., “Quantum cryptography,” Rev. Mod. Phys. **74**(1), 145–195 (2002).
[10] Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J. and Yeh, H., “Current status of the DARPA quantum network,” Quantum Information and Computation III **5815**, 138–149, International Society for Optics and Photonics (2005).
[11] Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J. F., Fasel, S., Fossier, S., Fürst, M., Gautier, J.-D., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y., et al., “The SECOQC quantum key distribution network in Vienna,” New J. Phys. **11**(7), 075001 (2009).
[12] Mirza, A. and Petruccione, F., “Realizing long-term quantum cryptography,” J. Opt. Soc. Am. B, JOSAB **27**(6), A185–A188 (2010).
[13] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., et al., “Field test of quantum key distribution in the Tokyo QKD Network,” Opt. Express, OE **19**(11), 10387–10409 (2011).
[14] Stucki, D., Legré, M., Buntschu, F., Clausen, B., Felber, N., Gisin, N., Henzen, L., Junod, P., Litzistorf, G., Monbaron, P., Monat, L., Page, J.-B., Perroud, D., Ribordy, G., Rochas, A., Robyr, S., Tavares, J., Thew, R., Trinkler, P., et al., “Long-term performance of the SwissQuantum quantum key distribution network in a field environment,” New J. Phys. **13**(12), 123001 (2011).
[15] Townsend, P. D., “Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing,” Electronics Letters **33**(3), 188–190 (1997).
[16] Chapuran, T. E., Toliver, P., Peters, N. A., Jackel, J., Goodman, M. S., Runser, R. J., McNown, S. R., Dallmann, N., Hughes, R. J., McCabe, K. P., Nordholt, J. E., Peterson, C. G., Tyagi, K. T., Mercer, L. and Dardy, H., “Optical networking for quantum key distribution and quantum communications,” New J. Phys. **11**(10), 105001 (2009).
[17] Eraerds, P., Walenta, N., Legré, M., Gisin, N. and Zbinden, H., “Quantum key distribution and 1 Gbps data encryption over a single fibre,” New J. Phys. **12**(6), 063027 (2010).
[18] Patel, K. A., Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V. and Shields, A. J., “Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber,” Phys. Rev. X **2**(4), 041010 (2012).
[19] Patel, K. A., Dynes, J. F., Lucamarini, M., Choi, I., Sharpe, A. W., Yuan, Z. L., Penty, R. V. and Shields, A. J., “Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks,” Appl. Phys. Lett. **104**(5), 051123 (2014).
[20] Wang, L.-J., Zou, K.-H., Sun, W., Mao, Y., Zhu, Y.-X., Yin, H.-L., Chen, Q., Zhao, Y., Zhang, F., Chen, T.-Y. and Pan, J.-W., “Long-distance copropagation of quantum key distribution and terabit classical optical data channels,” Phys. Rev. A **95**(1), 012301 (2017).

[21] Kumar, R., Qin, H. and Alléaume, R., "Coexistence of continuous variable QKD with intense DWDM classical channels," New J. Phys. **17**(4), 043027 (2015).
[22] Huang, D., Lin, D., Wang, C., Liu, W., Fang, S., Peng, J., Huang, P. and Zeng, G., "Continuous-variable quantum key distribution with 1 Mbps secure key rate," Opt. Express, OE **23**(13), 17511–17519 (2015).
[23] Mao, Y., Wang, B.-X., Zhao, C., Wang, G., Wang, R., Wang, H., Zhou, F., Nie, J., Chen, Q., Zhao, Y., Zhang, Q., Zhang, J., Chen, T.-Y. and Pan, J.-W., "Integrating quantum key distribution with classical communications in backbone fiber network," Opt. Express, OE **26**(5), 6010–6020 (2018).
[24] Choi, I., Zhou, Y. R., Dynes, J. F., Yuan, Z., Klar, A., Sharpe, A., Plews, A., Lucamarini, M., Radig, C., Neubert, J., Griesser, H., Eiselt, M., Chunnilall, C., Lepert, G., Sinclair, A., Elbers, J.-P., Lord, A. and Shields, A., "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," Opt. Express, OE **22**(19), 23121–23128 (2014).
[25] Ciurana, A., Martínez-Mateo, J., Peev, M., Poppe, A., Walenta, N., Zbinden, H. and Martín, V., "Quantum metropolitan optical network based on wavelength division multiplexing," Opt. Express, OE **22**(2), 1576–1593 (2014).
[26] Wang, L.-J., Chen, L.-K., Ju, L., Xu, M.-L., Zhao, Y., Chen, K., Chen, Z.-B., Chen, T.-Y. and Pan, J.-W., "Experimental multiplexing of quantum key distribution with classical optical communication," Appl. Phys. Lett. **106**(8), 081108 (2015).
[27] Chen, T.-Y., Liang, H., Liu, Y., Cai, W.-Q., Ju, L., Liu, W.-Y., Wang, J., Yin, H., Chen, K., Chen, Z.-B., Peng, C.-Z. and Pan, J.-W., "Field test of a practical secure communication network with decoy-state quantum cryptography," Opt. Express, OE **17**(8), 6540–6549 (2009).
[28] Chen, W., Han, Z.-F., Zhang, T., Wen, H., Yin, Z.-Q., Xu, F.-X., Wu, Q.-L., Liu, Y., Zhang, Y., Mo, X.-F., Gui, Y.-Z., Wei, G. and Guo, G.-C., "Field Experiment on a 'Star Type' Metropolitan Quantum Key Distribution Network," IEEE Photonics Technology Letters **21**(9), 575–577 (2009).
[29] Wang, S., Chen, W., Yin, Z.-Q., Zhang, Y., Zhang, T., Li, H.-W., Xu, F.-X., Zhou, Z., Yang, Y., Huang, D.-J., Zhang, L.-J., Li, F.-Y., Liu, D., Wang, Y.-G., Guo, G.-C. and Han, Z.-F., "Field test of wavelength-saving quantum key distribution network," Opt. Lett., OL **35**(14), 2454–2456 (2010).
[30] Chen, T.-Y., Wang, J., Liang, H., Liu, W.-Y., Liu, Y., Jiang, X., Wang, Y., Wan, X., Cai, W.-Q., Ju, L., Chen, L.-K., Wang, L.-J., Gao, Y., Chen, K., Peng, C.-Z., Chen, Z.-B. and Pan, J.-W., "Metropolitan all-pass and inter-city quantum communication network," Opt. Express, OE **18**(26), 27217–27225 (2010).
[31] Wang, S., Chen, W., Yin, Z.-Q., Li, H.-W., He, D.-Y., Li, Y.-H., Zhou, Z., Song, X.-T., Li, F.-Y., Wang, D., Chen, H., Han, Y.-G., Huang, J.-Z., Guo, J.-F., Hao, P.-L., Li, M., Zhang, C.-M., Liu, D., Liang, W.-Y., et al., "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express, OE **22**(18), 21739–21756 (2014).
[32] Dynes, J. F., Wonfor, A., Tam, W. W.-S., Sharpe, A. W., Takahashi, R., Lucamarini, M., Plews, A., Yuan, Z. L., Dixon, A. R., Cho, J., Tanizawa, Y., Elbers, J.-P., Greißer, H., White, I. H., Penty, R. V. and Shields, A. J., "Cambridge quantum network," 1, npj Quantum Information **5**(1), 1–8 (2019).
[33] Chen, Y.-A., Zhang, Q., Chen, T.-Y., Cai, W.-Q., Liao, S.-K., Zhang, J., Chen, K., Yin, J., Ren, J.-G., Chen, Z., Han, S.-L., Yu, Q., Liang, K., Zhou, F., Yuan, X., Zhao, M.-S., Wang, T.-Y., Jiang, X., Zhang, L., et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," 7841, Nature **589**(7841), 214–219 (2021).
[34] Lucamarini, M., Patel, K. A., Dynes, J. F., Fröhlich, B., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V. and Shields, A. J., "Efficient decoy-state quantum key distribution with quantified security," Opt. Express, OE **21**(21), 24550–24565 (2013).
[35] Tanizawa, Y., Takahashi, R., Sato, H. and Dixon, A. R., "An approach to integrate quantum key distribution technology into standard secure communication applications," 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), 880–886 (2017).
[36] Kanellos, G., Alia, O., Hugues-Salas, E., Tessinari, R. S., Wang, R., Nejabati, R. and Simeonidou, D., "Dynamic optical interconnects for quantum secure distributed nodes and quantum processing," 2020 IEEE Photonics Conference (IPC), 1–2 (2020).
[37] Tessinari, R. S., Bravalheri, A., Hugues-Salas, E., Collins, R., Aktas, D., Guimaraes, R. S., Alia, O., Rarity, J., Kanellos, G. T., Nejabati, R. and Simeonidou, D., "Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the Bristol city 5GUK Test Network," 45th European Conference on Optical Communication (ECOC 2019), 1–4 (2019).

[38] Nejabati, R., Wang, R., Bravalheri, A., Muqaddas, A., Uniyal, N., Diallo, T., Tessinari, R., Guimaraes, R. S., Moazzeni, S., Hugues-Salas, E., Kanellos, G. T. and Simeonidou, D., "First Demonstration of Quantum-Secured, Inter-Domain 5G Service Orchestration and On-Demand NFV Chaining Over Flexi-WDM Optical Networks," 2019 Optical Fiber Communications Conference and Exhibition (OFC), 1–3 (2019).
[39] "Quantum Communcations Hub.", Quantum Communcations Hub, <https://www.quantumcommshub.net/> (25 February 2021).
[40] "Welcome to NDFF.", NDFF, <https://www.ndff.ac.uk> (25 February 2021).
[41] Wonfor, A., White, C., Bahrami, A., Pearse, J., Duan, G., Straw, A., Edwards, T., Spiller, T., Penty, R. and Lord, A., "Field trial of multi-node, coherent-one-way Quantum Key Distribution with encrypted 5×100G DWDM transmission system," 45th European Conference on Optical Communication (ECOC 2019), 1–4 (2019).