Performance Analysis on Co-existence of COW-QKD and Classical DWDM Channels Transmission in UK National Quantum Networks

Xiao Duan, Joseph Pearse, Adrian Wonfor, Catherine White, Arash Bahrami, Andrew Straw, Tim Edwards, Richard Penty, Andrew Lord, Rupesh Kumar, Tim Spiller

***Abstract*—To analyse and evaluate the physical layer performance of a UK national quantum network (UKQNtel) utilising COW-QKD, in O band, integrated with 500 Gb/s encrypted data, in C band, over 121 km between BT Labs and the University of Cambridge, a theoretical model encompassing COW-QKD and Raman scattering noise is developed and fitted with real-world experimental data. Different physical mechanisms underpinning the link performance are identified and discussed. The model developed in this work also provides a preliminary technical guidance for future UKQNtel upgrade and expansion, as well as potentially useful insights for quantum-secured networks design prior to practical deployment.**

***Index Terms*—Quantum cryptography, quantum key distribution, network security, optical networks.**

I. INTRODUCTION

QUANTUM key distribution (QKD) [1-3], based on the laws of quantum physics, is a promising cryptographic technique that can provide information theoretic long-term security for data communication links. QKD is perceived to be resilient to attacks from quantum computers as its security does not depend on computational assumptions.

To facilitate commercial utilisation of QKD, it is imperative that QKD can be seamlessly integrated into existing telecommunication network infrastructures [4-7]. From a cost-effectiveness perspective, QKD and classical data needs to be transmitted over the same fibre. A number of field-trials have been previously conducted based on discrete variable (DV) QKD [8-16]. Recently, a new QKD protocol which belongs to the class of distributed phase reference (DPR) QKD, named coherent one way (COW) [17, 18], has been proposed. The main advantage of COW protocol is its simplicity and easy implementation using standard telecom components. Several laboratory-based experiments and field tests relevant to COW QKD have also been performed [19, 20].

Recently, a QKD link between BT Labs in Adastral Park and University of Cambridge over 121km installed fibre and intermediate exchanges, named UKQNtel, has been launched [21]. The link is the world-first field trial of a COW QKD system integrated with commercial-grade encrypted classical DWDM transmission system coexisting on the same fibre. It is also connected to the Cambridge quantum network [22] and they are both part of the UK quantum network (UKQN). More recently, 5G network slicing provisioned by software-defined networking (SDN) orchestration is also demonstrated on UKQNtel [23]. In this paper, based on our previous studies in [21], we focus on the performance analysis of the physical layer of UKQNtel by using a theoretical model which is developed and fitted with the experimentally measured link performance.

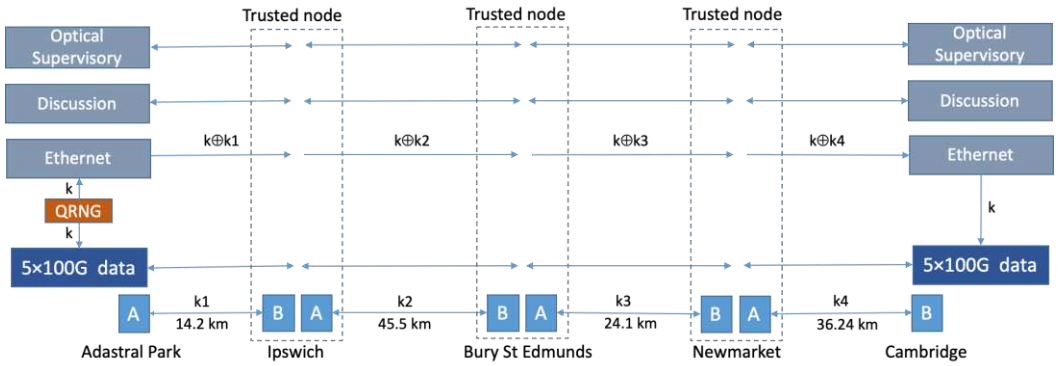

Fig. 1. UKQNtel link diagram (after [21]).

This work was supported by Innovate UK through the Knowledge Transfer Partnerships (KTP) programme under Grant 510820), EPSRC through the UK Quantum Technology Hub for Quantum Communications Technologies under (EP/M013472/1), Quantum Technology Capital: UKQNtel - Bringing the Telecoms Industry to the UK Quantum Network (EP/N015207/1) and The EPSRC Quantum Communications Hub (EP/T001011/1), Corresponding author: rupesh.kumar@york.ac.uk. X. Duan was with University of York and also with ADVA. He is now with Fraunhofer Singapore, and also with Nanyang Technological University, Singapore 639798 (e-mail: xiao.duan@ntu.edu.sg).

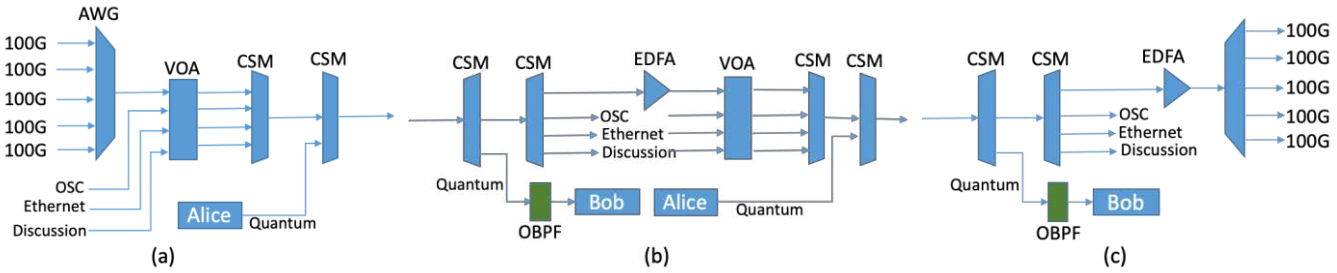

Fig. 2. Optical components in the nodes (after [21]). (a) start node, (b) intermediate nodes, (c) end node. Please see text for details.

II. UKQNTEL DESCRIPTION

In UKQNtel, there are 5 nodes with 3 intermediate trusted nodes, as seen in Fig. 1. Two end nodes are linked via three intermediate trusted nodes, spanning total 121 km. Intermediate nodes are equipped with QKD Alice and Bob for two consecutive links respectively while end nodes use either of the QKD system. The classical data transmission is bi-directional with each direction's transmission on a separate fibre, whilst the QKD signal flow is in one direction from Adastral Park to Cambridge, co-propagating with the classical data on one fibre. Optical supervisory channel is used for

TABLE I
SYSTEM PARAMETERS

Channel	Wavelength (nm)
5×100G data	1558.17, 1558.98, 1559.79, 1560.61, 1561.42
Optical supervisory (OSC)	1510
Discussion	1530
Key management (Ethernet)	1531
Quantum	1310

remote software update and network management information. Discussion channel contains reconciliation information and timing signals for QKD system. Ethernet channel is used for passing end-to-end keys (k) along the whole link. These keys are one-time-pad (OTP) encrypted by local quantum keys (k_1, k_2, k_3, k_4) shared in each span respectively. All the above-mentioned channels are multiplexed and transmitted on a single fibre in each span. The detailed channel assignment is in table 1.

The optical components in each end and intermediate nodes are illustrated in Fig. 2. The AWG (arrayed waveguide) and CSM (channel splitter multiplexer) are used to multiplex/demultiplex different optical channels. The VOA (variable optical attenuator) and the EDFA (erbium doped fibre amplifiers) are employed to control the classical optical power levels. To mitigate the filter leakage from ADVA 1310 CSM, an additional OBPF (optical band-pass filter) is applied after ADVA 1310 CSM to further filter out Raman noise into Bob for quantum detection and make the system works.

A commercial COW-QKD system developed by ID

TABLE II
MEASURED AND REFERENCE (FIXED) PARAMETERS

Parameter	Value
N_d	2
μ	0.5
t_B	0.9 [17]
η	0.1
α	0.35
c_{AP}	0.008
t_{dead}	50 μs
f_{rep}	1.25 GHz
f	0.1 [17]
Δf	700 GHz
Δt	0.8 ns
L_s	5.5 dB
V (Ipswich-Bury)	0.95
V (Bury-Newmarket)	0.8

Quantique [24], Clavis 3, is used as the quantum channel in UKQNtel. The operating principle of COW-QKD protocol is described in the next section. Placing the quantum channel at 1310 nm in O-band can lower the noise (primarily anti-Stokes Raman scattering noise) from co-propagating classical channels in the C-band. Fibre loss in O-band (0.35 dB/km) is larger than that in C-band (0.2 dB/km), therefore there is a trade-off between choosing O-band and C-band. Furthermore, there are several determining factors in the choice of OBPF bandwidth: 1) increasing OBPF bandwidth leads to larger Raman noise and thus decreasing the secure key rate (SKR); 2) decreasing OBPF bandwidth possibly leads to increased optical loss in the filter thus decreasing SKR; 3) importantly the emission wavelength of the 1310 nm laser is not defined as precisely as the ITU channels in the C band. A very narrow 1310 nm filter might be misaligned with the QKD wavelength. However, for this system, the Raman scattering is the most significant factor, hence, O-band is selected for the quantum channel in this work.

The classical data transmission employs 5 pairs of ADVA 100G AES line cards operating DP-QPSK (Dual-polarization quadrature phase shift keying)-modulated signal on the ITU DWDM grid in the FSP 3000 optical transport platform [25].

III. UKQNTEL PHYSICAL LAYER MODEL

In order to analyse the physical layer performance of UKQNtel, we first create a theoretical model of the COW protocol, then develop a Raman scattering noise model to

simulate the interference from classical channels to the quantum channel.

Raman scattering is one of the major nonlinear effects in optical fibres. It is generated by photons changing their wavelength as a result of photon-phonon interaction. Raman scattering occurs at wavelengths below (anti-Stokes) and above (Stokes) the initial pump wavelength. Thus, it can be characterised by the wavelength-dependent effective Raman scattering cross-section.

In UKQNtel, the quantum channel is placed below the wavelength of classical channels, therefore the Spontaneous Anti-Stokes Raman Scattering (SASRS) generated by classical channel is the dominant noise to the quantum channel. Note that other noise sources including Amplified Spontaneous Emissions (ASE) of the EDFA, leakage of photons from classical channels due to the finite isolation of the de-multiplexer and Four-Wave Mixing (FWM) are all neglected with respect to SASRS in this work. Details of COW-QKD and SASRS noise models are presented in the following sections.

A. COW-QKD system model

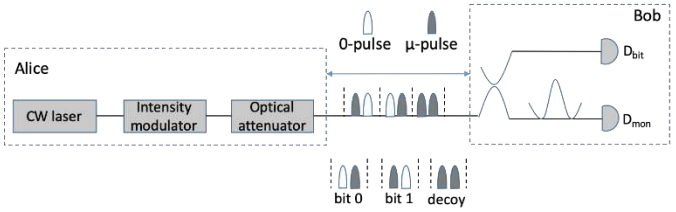

Fig. 3. COW-QKD system diagram (after [24]). CW: continuous wave. 0-pulse: empty pulse. μ-pulse: a pulse with mean photon number μ. D_{bit}: data-line detector for raw key generation. D_{mon}: monitor-line detector for eavesdropping check.

As Fig. 3 shows, in COW-QKD, logical bits are encoded in time. The transmitter, Alice, contains a laser which emits a CW beam. The beam is subsequently modulated and then attenuated producing either an empty pulse or a pulse with a mean photon number, μ ($0<\mu<1$). The logical bit is encoded in two consecutive pulses, namely, 0-μ for 0 and μ-0 for 1. In addition, decoy sequences (μ-μ) are produced to eliminate PNS (photon number splitting) attacks. These pulses travel from the transmitter over the quantum channel. In the receiver, Bob, there are two detection schemes after the pulses pass through a beamsplitter: one for key generation and the other for a security check. The beamsplitter provides passive but random path selection, so that some of the pulses reach the detector D_{bit} where they generate the raw key by using the time-of-arrival measurement, whilst other pulses go through the monitoring interferometer and reach detector D_{mon} for monitoring eavesdropping. Such monitoring works as follows: There is a definite phase between any successive non-empty pulses because of the coherence of a laser. These successive non-empty pulses occur in any 0-1 bit sequence (0-μ-μ-0 pulse sequence) and also in any decoy sequence, i.e. (μ-μ, μ-μ-μ-0 and 0-μ-μ-μ pulse sequences). It should be noted that a detailed security analysis for various attacks is beyond the scope of this paper, but can be found in [26-29].

To estimate the quantum bit error rate (QBER) and secure key rate (SKR) of the COW QKD system, we need to calculate the raw detection rate, which can be determined from the detectors' clicks due to quantum signals, detector dark counts, after-pulses and clicks due to noise photons (mainly Raman noise from the classical channel in this case). The raw key rate can be written as [30]:

$$R_{raw} = (p_\mu + N_d p_{dc} + p_{AP} + p_{ram}) f_{rep} \eta_{dead} \quad (1)$$

f_{rep} is the pulse repetition frequency of the QKD system, N_d is the number of quantum detectors in Bob, and p_x denotes different detection probabilities per pulse duration time (as the system is in free-running mode): p_μ quantum signal, p_{dc} dark count, p_{AP} after-pulse, p_{ram} Raman noise photon. η_{dead} is the detector dead time coefficient.

The quantum signal detection probability is:

$$p_\mu = \mu T t_B \eta \quad (2)$$

μ is the average photon number per pulse, t_B is the beam-splitter transmission coefficient in Bob, η is the quantum detector efficiency, T is the fibre transmission given by:

TABLE III
FITTED PARAMETERS

Parameter	Value
p_{dc} (Ipswich-Bury)	8.5×10^{-6}
p_{dc} (Bury-Newmarket)	3.2×10^{-5}
β	1.2×10^{-11} km^{-1}nm^{-1}
η_{ec}	1.68

$$T = 10^{-\frac{\alpha L + L_S}{10}} \quad (3)$$

with α the fibre attenuation coefficient, L the fibre length and L_s the extra loss between Alice and Bob.

The after-pulse detection probability is approximated by:

$$p_{AP} = c_{AP}(p_\mu + N_d p_{dc} + p_{ram}) \quad (4)$$

c_{AP} is the fractional coefficient of after-pulse probability to the total detection probability.

The quantum detector dead time coefficient is defined as:

$$\eta_{dead} = \frac{1}{1 + t_{dead} f_{rep} (p_\mu + N_d p_{dc} + p_{AP} + p_{ram})} \quad (5)$$

with t_{dead} being the dead time of the quantum detector after each detection.

A certain fraction of R_{raw} is discarded after sifting so the sifted key rate is:

$$R_{sift} = \frac{1}{2}(p_\mu + N_d p_{dc} + p_{AP} + p_{ram}) f_{rep} \eta_{dead} (1 - f) \quad (6)$$

f is the probability that Alice sends the decoy sequence.

The SKR after error correction and privacy amplification is:

$$R_{sec} = R_{sift}(I_{AB} - I_{AE}) \quad (7)$$

I_{AB} and I_{AE} are the mutual information per bit between Alice and Bob, and between Alice and a potential eavesdropper, respectively.

I_{AB} is given by [30]:

$$I_{AB} = 1 - \eta_{ec} H(QBER) \quad (8)$$

with $H(p)$ the Shannon entropy function for a given $QBER$ related to the minimum fraction of bits lost due to error correction defined as:

$$H(p) = -p log_2 p - (1 - p) log_2 (1 - p) \quad (9)$$

and η_{ec} denotes the error correction [31] efficiency. I_{AE} is estimated after [17, 24]:

$$I_{AE} = \mu(1 - T) + (1 - V)\frac{1 + e^{-\mu T}}{2e^{-\mu T}} \quad (10)$$

The first term corresponds to PNS attacks and second to intercept-resend attacks. V is the monitoring interferometer's visibility.

Finally, the QBER is defined as the ratio between the number of error detections and total detections in the sifted key:

$$QBER = \frac{1}{2}\frac{p_{dc}+p_{AP}+p_{ram}}{p_{\mu}+N_d p_{dc}+p_{AP}+p_{ram}} \quad (11)$$

B. SASRS noise model

The SASRS noise power within a bandwidth of $\Delta\lambda$ is [32]:

$$P_{SASRS} = P_{in} e^{-\alpha L} \beta L \Delta\lambda \quad (12)$$

in which P_{in} is the total launch optical power of the classical channel (data, supervisory, Ethernet, discussion), α is the fibre attenuation coefficient, β is the effective Raman scattering cross-section coefficient, L is the fibre length.

Given that the total mode number in a bandwidth of $\Delta\lambda$ and a time window of Δt is:

$$N_{mode} = |\Delta f \Delta t| = \frac{c}{\lambda^2}\Delta\lambda \quad (13)$$

The SASRS photon number per spatiotemporal mode is:

$$N_{SASRS} = \frac{P_{SASRS}}{hf N_{mode}}\eta_{drop} = \frac{\lambda^3}{hc^2} P_{in} e^{-\alpha L} \beta L \eta_{loss} \quad (14)$$

η_{drop} includes the insertion loss of the 1310nm add/drop optical filter, low-bandwidth filter before Bob and various connection loss.

Therefore p_{ram} in equation 1 can be calculated as:

$$p_{ram} = N_{SASRS} \Delta f \Delta t \eta \quad (15)$$

Δf is the bandwidth of the optical filter inserted before Bob as this filter is adopted to reduce the Raman noise.

As an example, Fig. 4 shows the number of SASRS photons per ns time window versus fibre length under different optical launch powers P_{in}. The maximum Raman noise photon number occurs at approximately 21km fibre length.

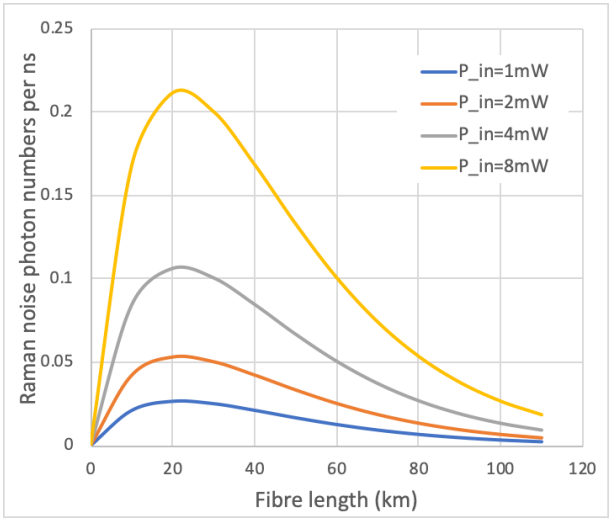

Fig. 4. Simulated SASRS photon numbers per ns against fibre length under different launch optical power

IV. UKQNTEL LINK PERFORMANCE ANALYSIS

For simplicity but without loss of generality, performance analysis is focused on the two spans of the UKQNtel link between Ipswich and Newmarket. All the simulation parameters in section 3 are listed in table 2 and table 3. Table 2 lists the referenced and experimentally measured parameter values whilst table 3 lists the fitted ones.

Fig. 5 shows the QBERs of the above two spans against different classical channel powers in C-band indicated in Table 1. The fitting of simulation result with experimental measurement from [21] is performed at a given classical optical power level (-8 dBm and -7 dBm in this case). We adjust dark count probability p_{dc} until the measured QBER value is fitted. Then we fit the slope of the simulated QBER curve by tuning the Raman coefficient β.

These two fitted parameter values are listed in Table 3. It is encouraging to see from Fig. 5 that there is a good agreement between the results generated by the model and measured in the link, which supports the validity of the model. It is also clear to see that the QBER of the Bury-Newmarket span is much lower than that of the Ipswich-Bury span. This corresponds to the fact that the fibre transmission length of Bury-Newmarket span is only about half of Ipswich-Bury span, resulting in lower fibre loss. The QBER trend is similar between two spans as they both use G.652 single mode fibre (SMF) with the same Raman coefficient.

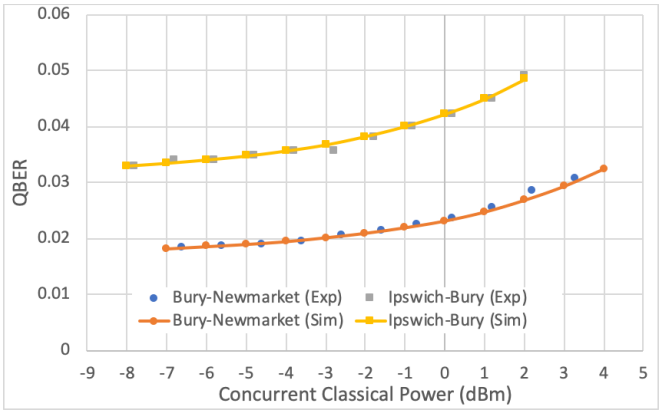

Fig. 5. Measured and simulated QBER against classical optical power in Ipswich-Bury and Bury-Newmarket spans. Exp: experiment. Sim: simulation

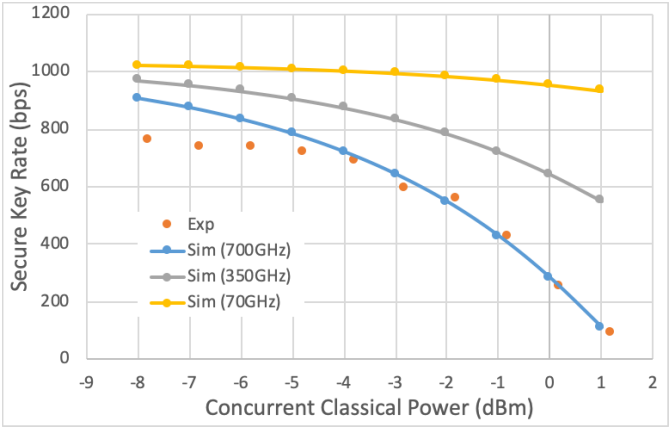

Fig. 6. Measured and simulated SKR against classical optical power in Ipswich-Bury span. Exp: experiment. Sim: simulation

Fig. 6 presents the SKR with different classical powers in the Ipswich-Bury span. Using the dark count probability p_{dc} and Raman coefficient β that we have already fitted for this link, here the fitting of the SKR is achieved by modifying the

efficiency of error correction η_{ec} in equation 8. At high concurrent classical power, where Raman noise is significant, the fitted ideal curve for SKR reproduces the observed SKR well; we can see from Fig. 6 that when the classical power varies from -4 dBm to 1 dBm, the simulated and measured results are consistent. However, when the classical power is lower than -4dBm, the experimentally measured SKR values are lower than expected and the simulated curve cannot be well fitted to them. This behaviour suggests that when the signal to noise ratio (SNR) of the quantum signal is high, the implementation of post processing (error correction and privacy amplification) in the practical QKD system is likely to be the major factor limiting SKR. The above discussions imply that SKR could be increased by enhancing error correction and privacy amplification algorithms.

Moreover, Fig. 6 also shows SKRs with different OBPF's bandwidth but similar insertion loss values. It can be seen that, when using OBPF of narrower bandwidth the SKR will be improved especially in the high classical power region. This evidently suggests that a more optimised OBPF is another key to achieve better physical layer performance in UKQNtel. The OBPF (which may in practice comprise two or more OBPFs in series) usually provides a choice of passband width, stopband attenuation and insertion loss, often with a trade-off between these parameters, however these parameter values generally depend on the technology on which the filter is based, so it is not possible to establish a generalised mathematical model for this trade-off within the scope of the paper. However, high values of stopband attenuation, optimum passband width to match the quantum channel source, and low insertion loss, will significantly improve QKD performance when co-propagating classical channels.

V. Conclusion

In this paper, a theoretical model has been built and fitted to obtain insights into the physical layer performance of a UK national quantum network (UKQNtel) utilising COW-QKD integrated with 500Gb/s encrypted data over 121km between BT Labs and the University of Cambridge. Different physical factors underlying the link performance are calibrated and examined. The model is sufficient to explain the observed QBER. Future work could be useful to understand the dependence on the fitted Raman coefficient on the placement of the channels.

References

[1] S. Weisner, "Conjugate Coding", *SIGACT News*, vol. 15, no. 1, pp. 78-88, 1983.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: public-key distribution and coin tossing", in Proceedings of *IEEE International Conference on Computers Systems and Signal Processing*, Bangalore, pp. 175-179, 1984.

[3] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography", *J. Cryptology*, vol. 5, no. 1, pp. 3-28, 1992.

[4] P. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing", *Electron. Lett*., vol. 33, no. 3, pp. 188–190, 1997.

[5] T. Chapuran, "Optical networking for quantum key distribution and quantum communications", *New J. Phys*. 11, 105001, 2009.

[6] Y. Mao, B., X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, et al., "Integrating quantum key distribution with classical communications in backbone fiber network", *Opt. Express*, vol. 26, no. 5, pp. 6010-6020, 2018.

[7] A. Lord, C. White, E. Hugues-Salas, "Quantum Key Distribution (QKD) and the Quantum Internet: The challenges facing this new technology", in *Optical Fiber Communications Conference and Exhibition (OFC)*, San Francisco, 2021, paper Th2A.1.

[8] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh. "Current status of the DARPA Quantum Network", *Quantum Information and Computation III*, pp. 138-149, 2005.

[9] M. Peev *et al*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys*. 11, 075001, 2009.

[10] S. Wang *et al*, "Field test of wavelength-saving quantum key distribution network", *Opt. Lett.*, vol. 35, no. 14, pp. 2454-2456, 2010.

[11] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.* 13, 123001, 2011.

[12] M. Sasaki *et al*, "Field test of quantum key distribution in the tokyo qkd network", *Opt. Express*, vol. 19, no. 11, pp. 10387-10409, 2011.

[13] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, et al., "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," *Opt. Express*, vol. 22, no. 19, pp. 23121-23128, 2014.

[14] R. Tessinari, A. Bravalheri, E. Hugues-Salas, R. Collins, D. Aktas, R. Guimaraes, O. Alia, J. Rarity, G. Kanellos, R. Nejabati, D. Simeonidou, "Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the Bristol city 5GUK Test Network", in *European Conference on Optical Communications (ECOC)*, Dublin, 2019.

[15] A. Gatto, M. Brunero, M. Ferrari, A. Tarable, D. Bodanapu, J. P. Brito, R. B. Mendez, R. J. Vicente, F. Bianchi, M. Frittelli, V. Martin, P. Comi, and P. Martelli, "A BB84 QKD Field-Trial in the Turin Metropolitan Area," in *Photonics in Switching and Computing*, Washington DC, 2021.

[16] Y. Yang, P. Li, S. Ma, X. Qian, K. Zhang, L. Wang, W. Zhang, F. Zhou, S. Tang, J. Wang, Y. Yu, Q. Zhang, and J. Pan, "All optical metropolitan quantum key distribution network with post-quantum cryptography authentication," *Opt. Express*, vol. 29, no. 16, pp. 25859-25867, 2021.

[17] D. Stucki, N. Brunner, N. Gisin, V. Scarani and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett*., vol. 87, 194108, 2005.

[18] D. Stucki, C. Barreiro, S. Fasel et al., 'Continuous high-speed coherent one-way quantum key distribution', *Opt. Express*, vol. 17, no. 16, pp. 13326-13334, Aug. 2009.

[19] N. Walenta *et al.*, "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," *New J. Phys*., vol. 16, 013047, 2014.

[20] B. Korzh *et al*., 'Provably secure and practical quantum key distribution over 307 km of optical fibre', *Nature Photonics*, vol. 9, no. 3, pp. 163–168, Mar. 2015.

[21] A. Wonfor, C. White, A. Bahrami, J. Pearse, G. Duan, T. Edwards, A. Straw, T. Spiller, R. Penty, and A. Lord, "Field Trial of Multi-Node Coherent-One-Way Quantum Key Distribution with Encrypted 5x100G DWDM System", in *European Conference on Optical Communications (ECOC)*, Dublin, 2019, paper Th.1.A.1.

[22] J.F. Dynes, A. Wonfor, W.W.S. Tam *et al.*, "Cambridge quantum network", *npj Quantum Inf*, vol. 5, no. 101, 2019.

[23] P. Wright, C. White, R. Parker, J-S. Pegon, M. Menchetti, J. Pearse, A. Bahrami, A. Moroz, A. Wonfor, R. Penty, T. Spiller, and A. Lord, "5G network slicing with QKD and quantum-safe security," *Journal of Opt. Comm and Netw*. vol. 13, no. 3, Jan. 2021.

[24] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long distance quantum key distribution over 250 km of ultra low loss fibres," *New J. Phys*. 11, 075003, 2009.

[25] 'FSP3000AgileConnect™'.https://www.advaoptical.com/en/products/scalable-optical-transport/fsp-3000-agileconnect

[26] C. Branciard, N. Gisin and V. Scarani, "Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography," *New J. Phys*., vol. 10, 013031, 2008.

[27] T. Moroder, M. Curty, C. Lim, L. Thinh, H. Zbinden, and N. Gisin, *Phys. Rev. Lett.,* vol. 109, 260501, 2012.
[28] J. González-Payo, R. Trényi, W. Wang, and M. Curty, *Phys. Rev. Lett.,* vol. 125, 260510, 2020.
[29] R. Trényi and M. Curty, "Zero-error attack against coherent-one-way quantum key distribution," *New J. Phys*., vol. 23, 093005, 2021.
[30] 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.
[31] G. Brassard, L. Salvail, "Secret-Key Reconciliation by Public Discussion", *Eurocrypt'93*, *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, vol. 765, pp. 410-423, 1993.
[32] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New J. Phys*., vol. 12, 103042, 2010.