QKD secured networks in the UK

A. Wonfor

R. Nejabati[2], C. White[3], J.F. Dynes[4] and R.V. Penty[1]

1 University of Cambridge, Cambridge, UK

2 University of Bristol, Bristol, UK

3 BT Labs, Adastral Park, Ipswich, UK

4 Toshiba Research Europe Ltd., Cambridge Research Laboratory, Cambridge, UK

Acknowledgements: UK EPSRC

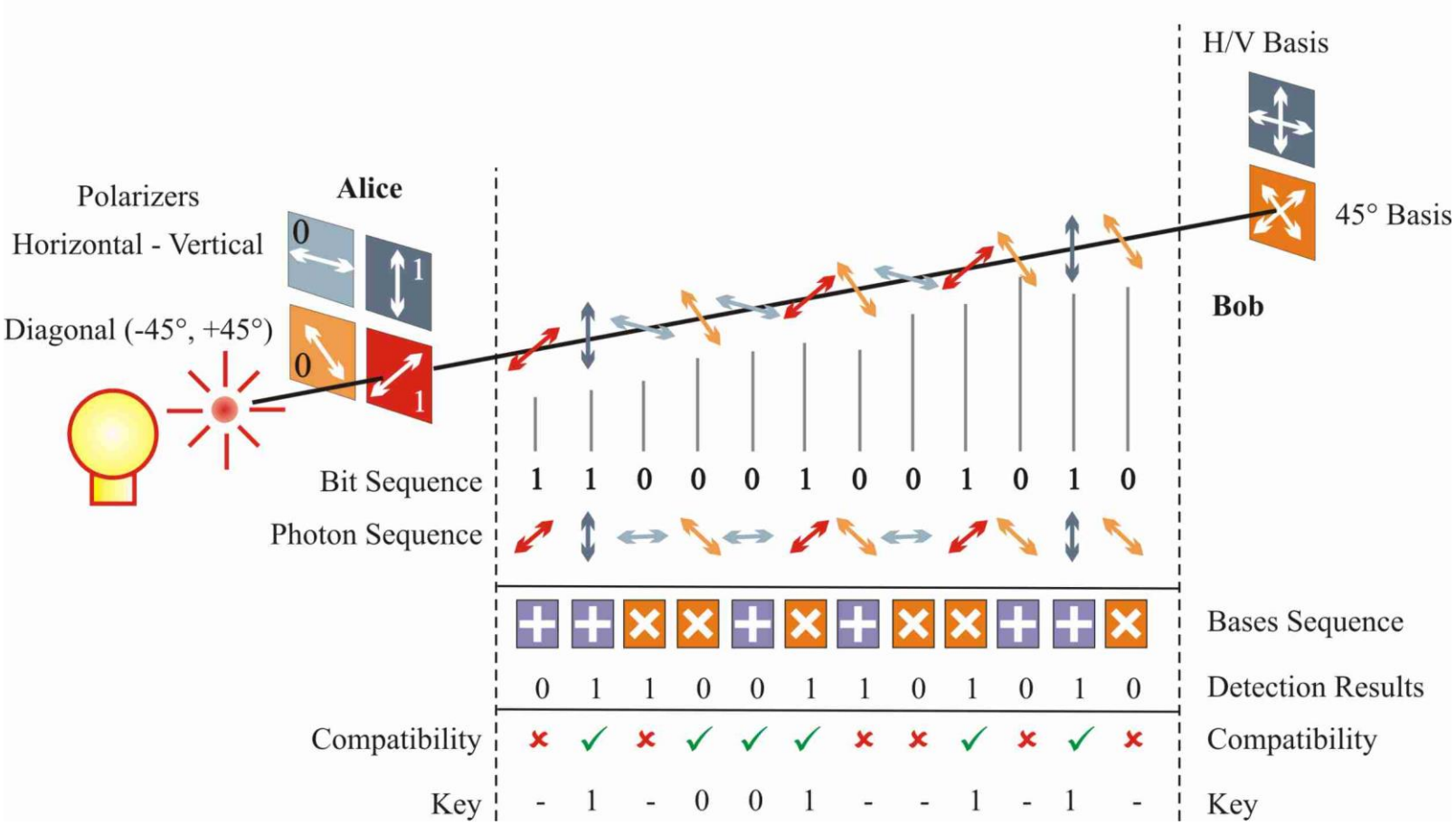
The EPSRC Quantum Communications Hub grant EP/T001011/1

UK Quantum Technology Hub for Quantum Communications Technologies EP/M013472/1

QKD?

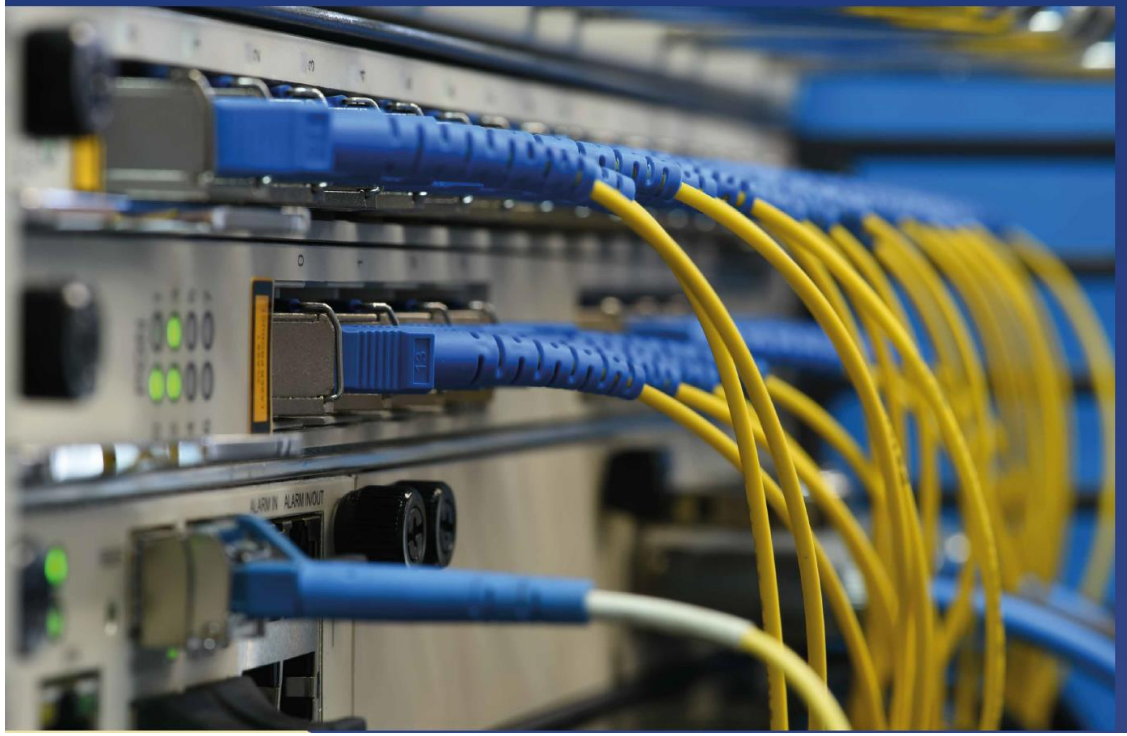
- Threat to current PKI encryption from Quantum Computers
  - RSA, Diffie-Hellman, Elliptic curve…
  - Shor's algorithm – Quantum Fourier Transform (has factored 21)
- Countermeasures
  - Make RSA keys longer
  - Post Quantum Cryptography
    - Latest from NIST competition 5 July 2022
    - Public-key Encryption and Key-establishment Algorithms : CRYSTALS-KYBER
    - Digital Signature Algorithms : CRYSTALS-DILITHIUM, FALCON, SPHINCS+
  - All rely on computational complexity for security
- Quantum Key Distribution
  - Information theoretically secure – uses quantum mechanical principles
  - Requires infrastructure on network

QKD BB84 Protocol



NDFF
EPSRC National Dark Fibre Facility

The National Dark Fibre Facility
supporting research into **new communications technologies** for the future internet



NDFF provides:

- a network of over 750km of single-mode optical fibre, together with control and monitoring systems (provided through the Jisc Janet Network).
- access to a dedicated dark fibre network at the physical layer, through access points at four universities and major internet exchanges.
- access for researchers throughout the UK via Layer-2 connections, equipment hosted at access points and remotely.
- a reliable, ultra-high-bandwidth network that can be configured remotely and dynamically.

UCL · University of Bristol · University of Cambridge · University of Southampton

CONTACT NDFF ndff@ee.ucl.ac.uk www.ndff.ac.uk

The National Dark Fibre Facility is an EPSRC National Research Facility

UKRI Engineering and Physical Sciences Research Council

In Partnership with Jisc

UK Long Distance Quantum Network

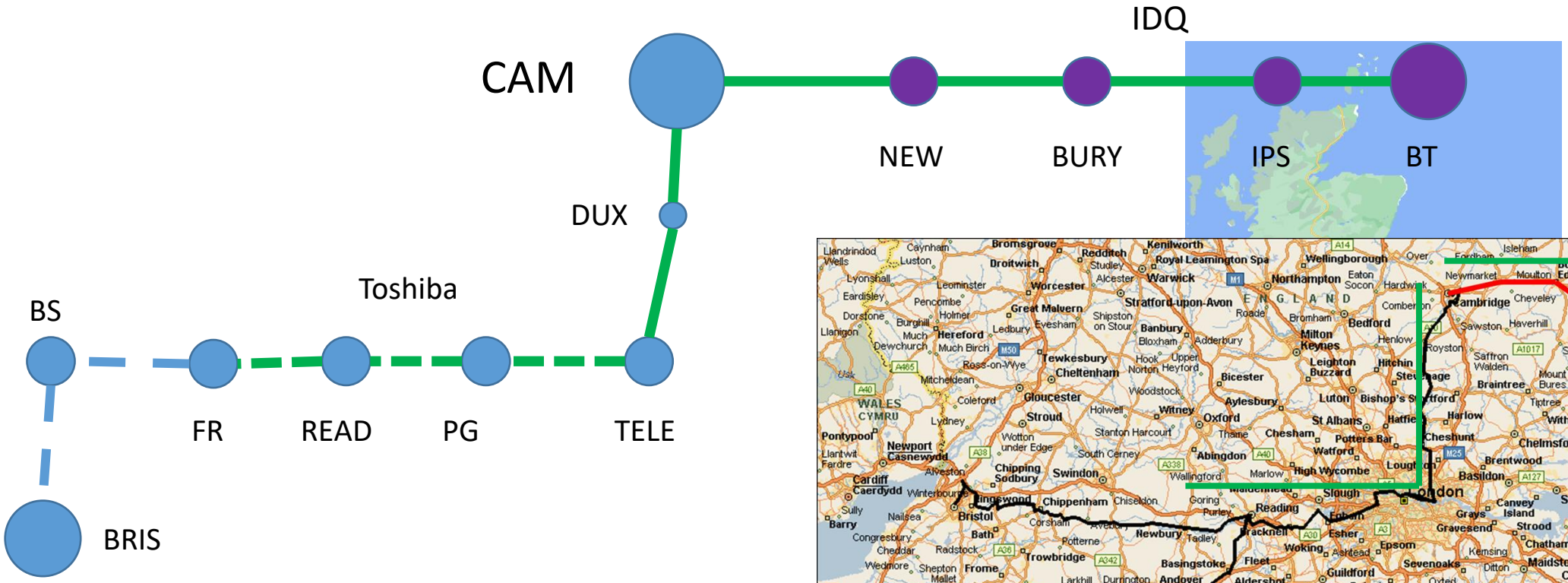


Image Credit: Google maps

- UKQN – linking Cambridge and Bristol – over the NDFF
- UKQNTel – linking Cambridge with BT Adastral Park

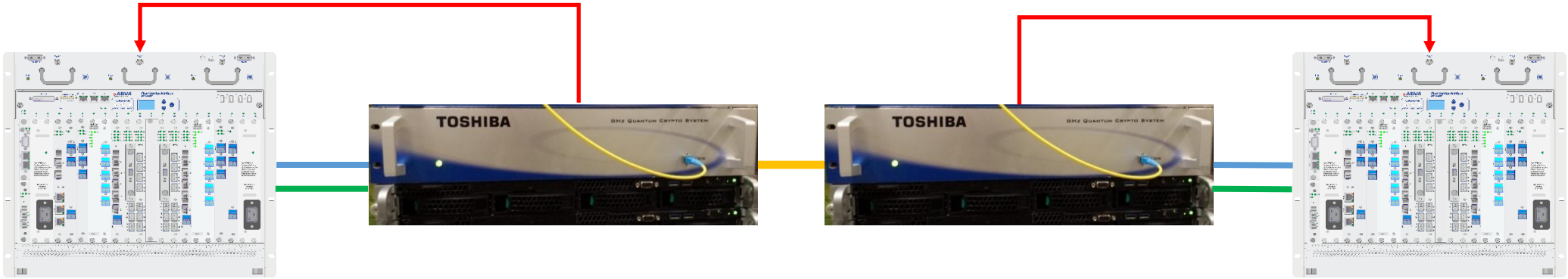
NDFF
EPSRC National Dark Fibre Facility

www.ndff.ac.uk

Electrical Engineering CAMBRIDGE
PHOTONICS AND QUANTUM TECHNOLOGIES

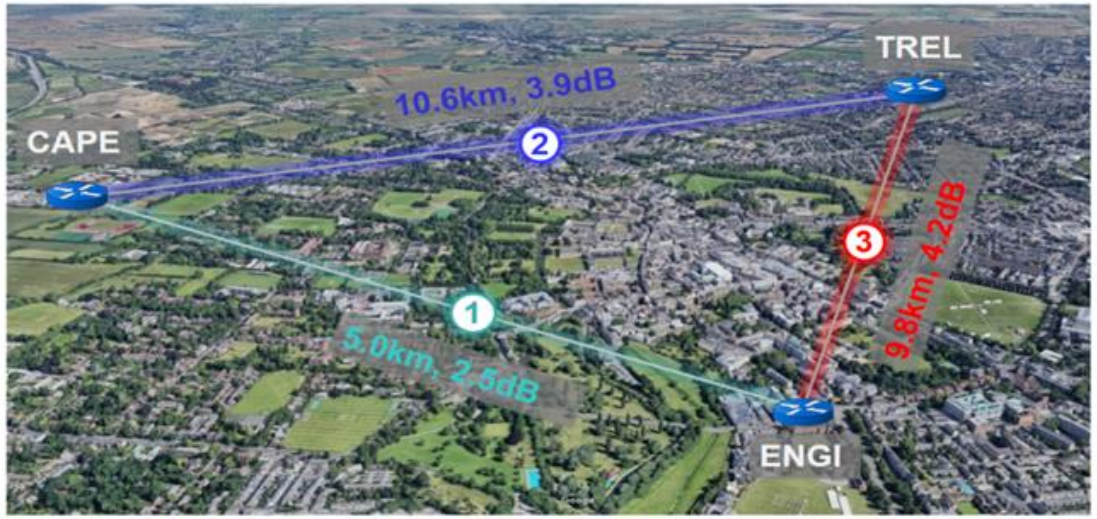
UNIVERSITY OF CAMBRIDGE

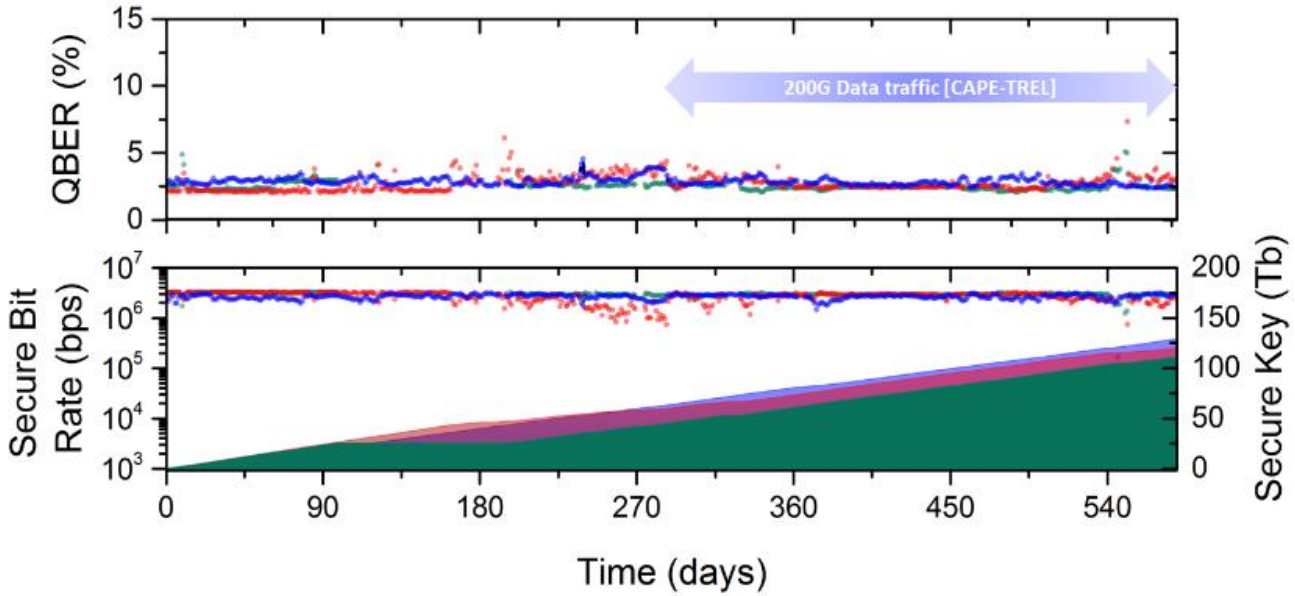
Secure high data rate transmission with QKD



- Classical traffic is fed through QKD system, which adds quantum and control wavelengths
- Quantum Keys are extracted from QKD system to drive the ADVA encrypted line-cards
- Line-cards adapted to take QKD keys rather than using conventional Diffie-Hellman key generation
- 2 x 100Gb/s line cards secured by QKD keys.

Cambridge Quantum Network – long term performance



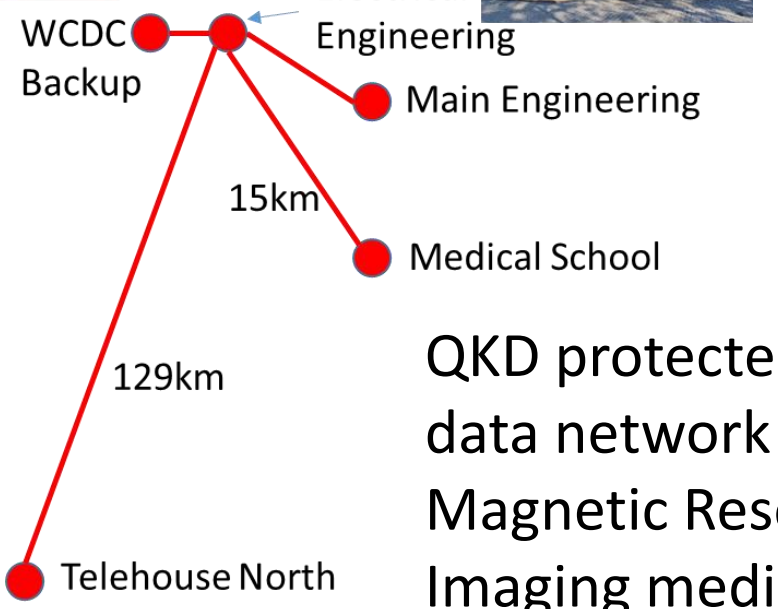


- Secure key rates on all links consistently above 1Mb/s
- Concurrent 100Gb/s traffic over all links
- Well over 100Tb of secure key transferred

Dynes, J.F., Wonfor, A., Tam, W.W.-. *et al.* Cambridge quantum network. *npj Quantum Inf* **5,** 101 (2019). https://doi.org/10.1038/s41534-019-0221-4

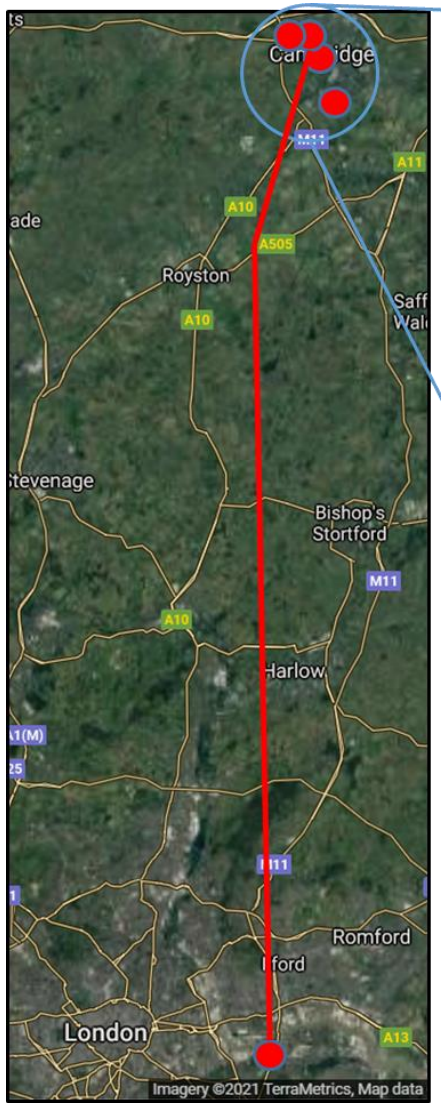
Multi-homed backup network – Medical and Research

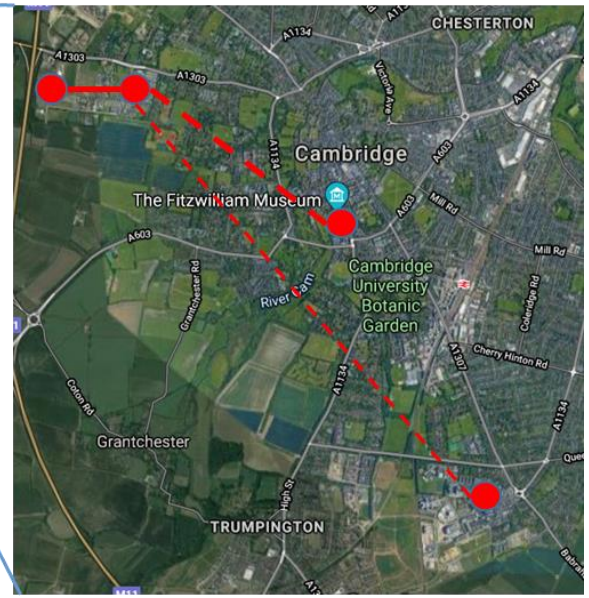
Electrical Engineering
CAMBRIDGE
PHOTONICS AND QUANTUM TECHNOLOGIES

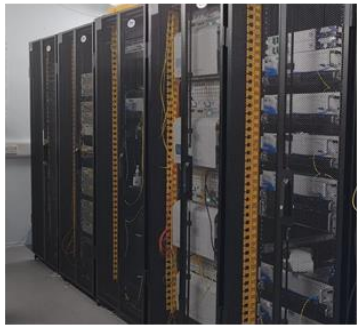


External view of Telehouse

QKD protected classical data network backs up real Magnetic Resonance Imaging medical data from Medical School to West Cambridge Data Centre and remote node at Telehouse North in London







Electrical Engineering QKD nodes

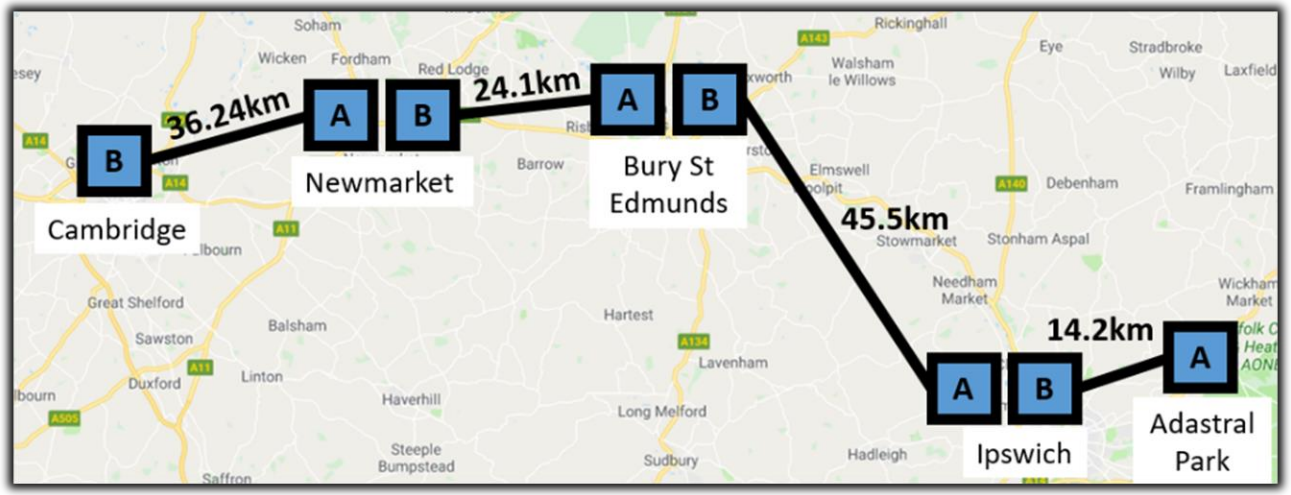
OPEN QKD

TOSHIBA
Leading Innovation

UNIVERSITY OF CAMBRIDGE

UKQNTel

Centre for Advanced Photonics and Electronics, Cambridge

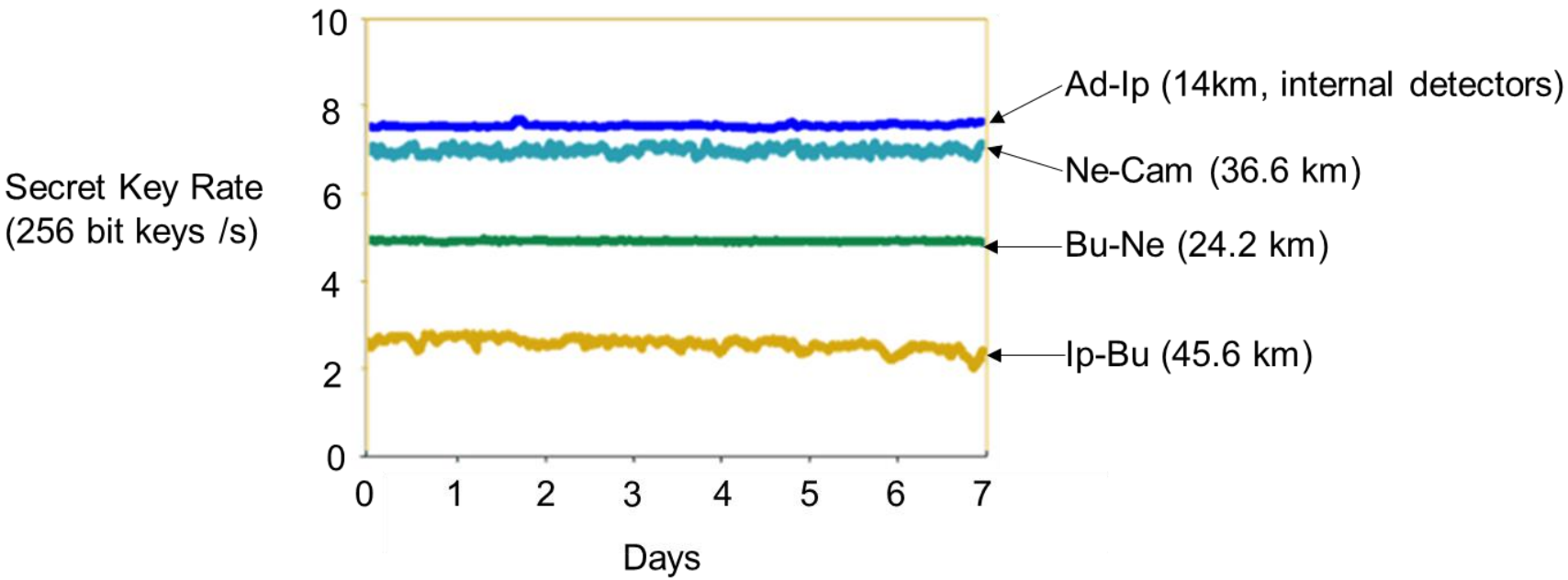


BT Adastral Park

- Encrypted traffic between University of Cambridge and Adastral Park, via 3 trusted nodes at BT Exchanges.
- Standard optical fibre pair (G.652) between each site, 120km total span
- Purposes
- Integration of QKD into real world network
- Test and optimise performance and resilience
- Develop strategies for large scale deployment

Field trial – steady state performance

- IDQuantique Clavis 3 QKD in O band
  COW protocol
- Secure key rates between 0.8 and 2.0 kb/s
- 5 x 100Gb/s ADVA classical channels (pre FEC BER 10^{-4})



Link length, loss at 1310nm, secure key rate

14.2km, 4.7dB, 2.0kb/s

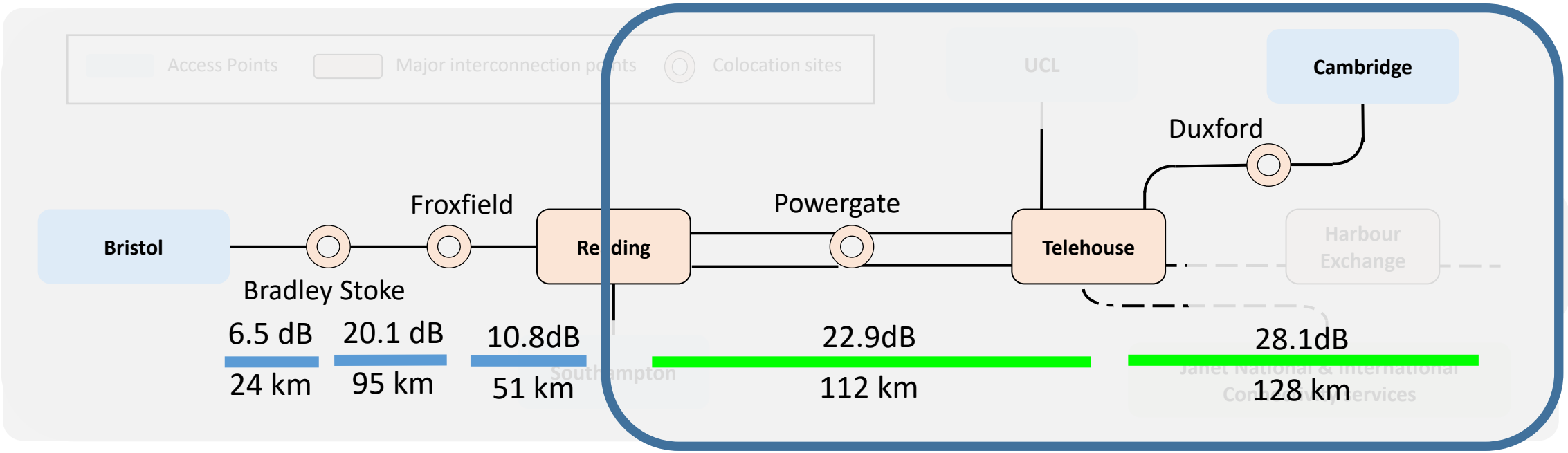
36.6km, 16.6dB, 1.9kb/s

24.2km, 10.2dB, 1.3kb/s

45.6km, 18.7dB, 0.8kb/s

A. Wonfor, C. White, A. Bahrami, J. Pearse, G. Duan, A. Straw, T. Edwards, T. Spiller, R.V. Penty, A. Lord, 'Field trial of multi-node, coherent-one-way Quantum Key Distribution with encrypted 5×100G DWDM transmission system', in *45th European Conference on Optical Communication (ECOC 2019)*, Sep. 2019, pp. 1–4. doi: 10.1049/cp.2019.0962

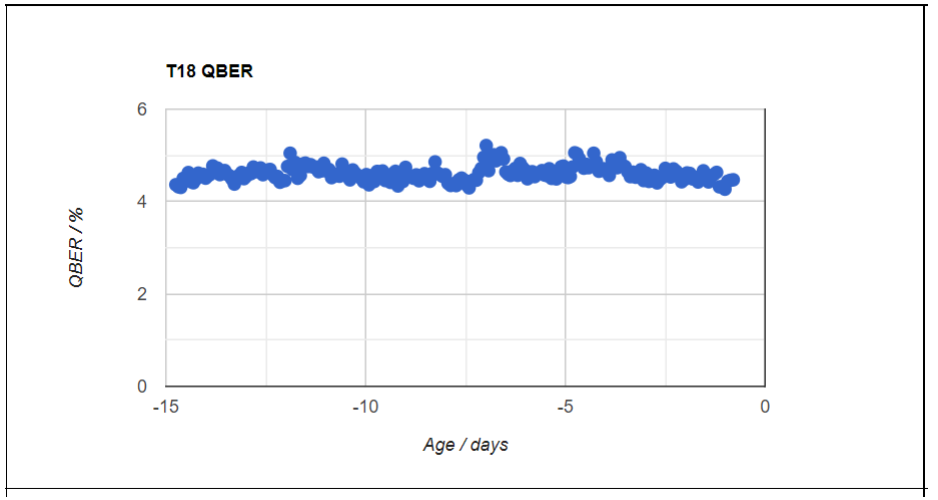
UK Quantum Network – Long Haul

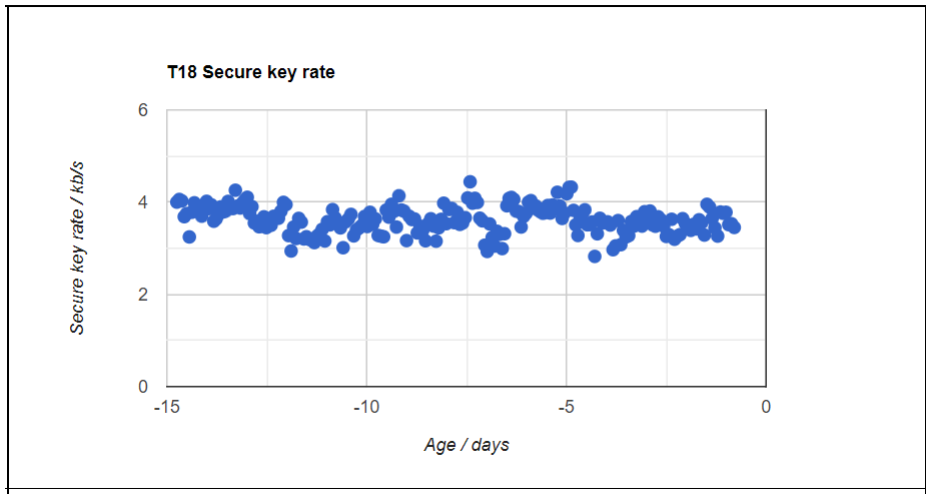


- Four Long Haul QKD systems
- Cambridge – London installed and working
  - Long distance – need physical patches at ends and intermediate point
- Others lower loss, can use installed fibre switches in installed plant
  - Will allow easier time sharing of NDFF

Operational performance

- Performance data – last 28 days
- QBER 4.6 ± 0.2 %
- Secure Key Rate 3.6 ± 0.3 kb/s
- 28 dB loss link
- QKD channel co-exists with classical reconciliation, timing and sync channels
- Pre-standards QKD system being upgraded to use ETSI 014 standard.
- Imminent deployment of standards compliant ADVA classical 100Gb/s classical system.





Captured 06:00 2022-04-11

DV-QKD Coexistence Over Single Mode Fiber

- Dynamic DV-QKD Networking in Trusted-node-free Software-Defined Optical Networks.
- A QKD-aware centralised Software-defined networking (SDN) controller is utilised to provide dynamicity in switching and rerouting for QKD links.
- Coexistence over field-deployed in the same optical band (C-band) is experimentally explored.
- The coexistence of a DV-QKD channel and 4x100 Gbps classical channel was successfully demonstrated over multiple links with the ability to switch between the links using a centralised SDN controller

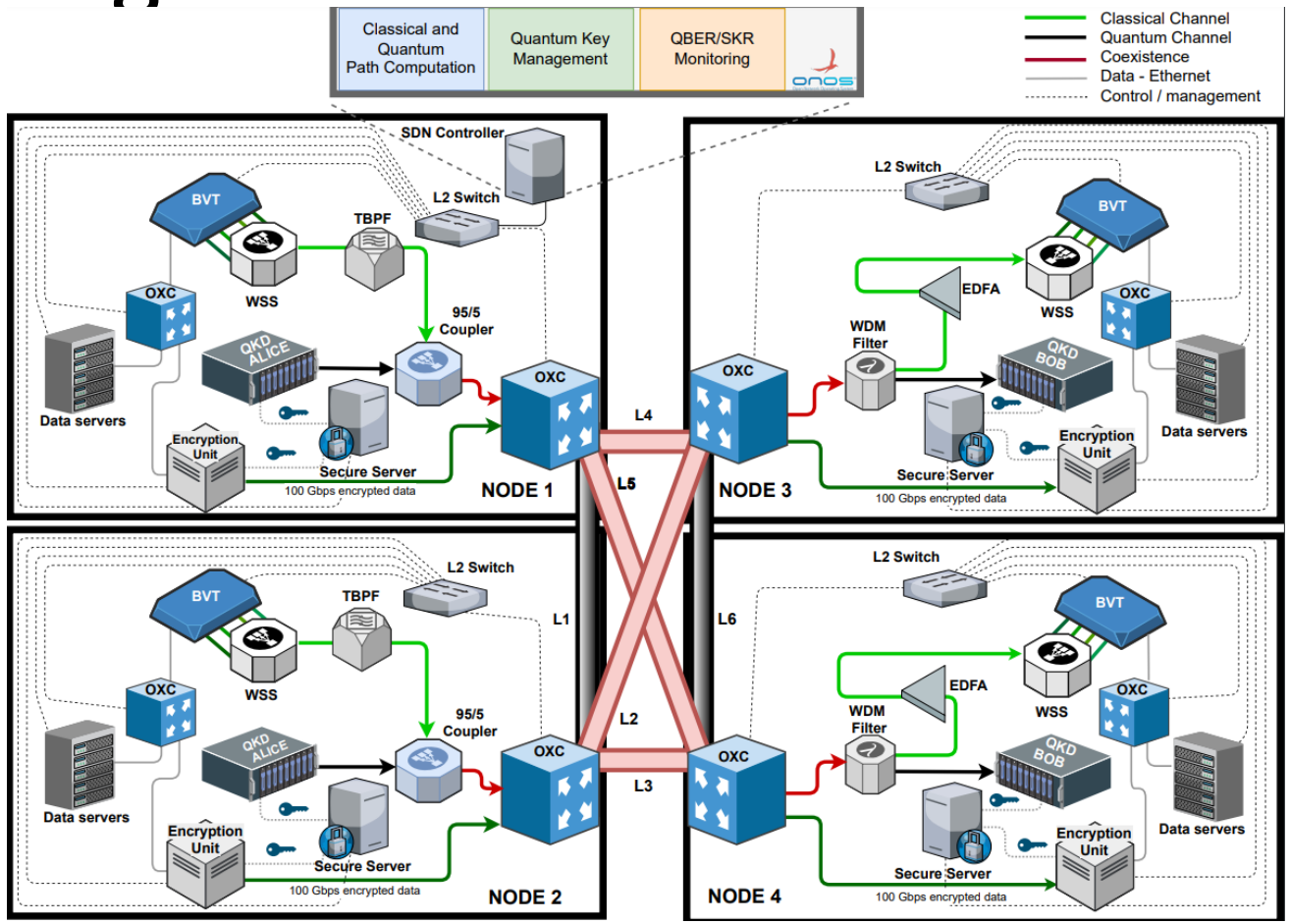


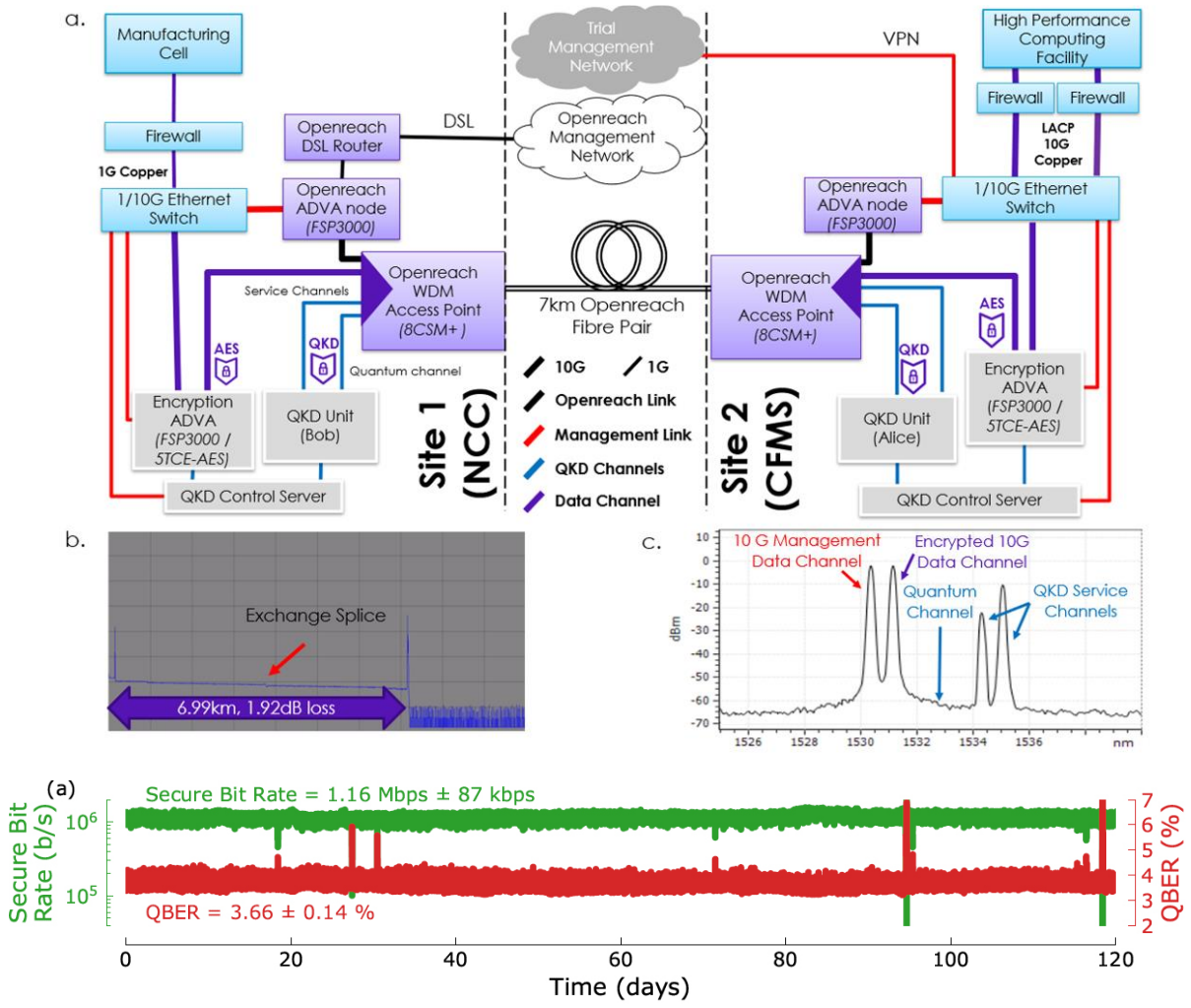
Fig.3: Trusted-node-free Dynamic QKD Network configuration two testbed. Red link: Fibre with QKD communication, Black link: Fibre without QKD communication.

R. S. Tessinari, et al., "Field trial of dynamic dv-qkd networking in the sdn-controlled fully-meshed optical metro network of the bristolcity 5guk test network," in 45th European Conference on Optical Communication (ECOC 2019). IET, 2019, pp. 1–4.

O. Alia , et al., "Dynamic DV-QKD Networking in Fully-Meshed Software-Defined Optical Networks," arXiv. https://arxiv.org/abs/2108.11145. Submitted to JLT

Industrial QKD trial

- Connecting the National Composites Centre (NCC) and the Centre for Modelling & Simulation (CFMS) in Bristol
- 7km link provided by Openreach ‘Optical Filter Connect’
- Over 120 day operation
  QBER of 3.6 ± 0.1%
  1.2 ± 0.09 Mb/s secure bit rate



R. I. Woodward, J. F. Dynes, P. Wright, C. White, R. C. Parker, A. Wonfor, Z. L. Yuan, A. Lord, and A. J. Shields, ‘Quantum Key Secured Communications Field Trial for Industry 4.0’, in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, Jun. 2021, pp. 1–3.

Summary

- Cambridge Quantum Network running successfully for several years
  - Mb/s secure key rates in the presence of 100Gb/s classical data
- Many metro scale networks in Cambridge and Bristol
- The highest long term key rates demonstrated in a field trial
- Long term operation of the longest single span QKD field trial
  - 128 km and 28dB loss operating for months with 3.6kb/s key rate
- Industrial demonstration of QKD

Acknowledgements: UK EPSRC

The EPSRC Quantum Communications Hub grant EP/T001011/1

UK Quantum Technology Hub for Quantum Communications Technologies EP/M013472/1