TOSHIBA

Realising Scalable QKD Networks


TOSHIBA
TOSHIBA

01

Introduction

Toshiba Europe Limited conducts research, development, commercialisation and deployment of a range of quantum technologies. We have been at the forefront of QKD R&D for decades and have demonstrated a number of global firsts in QKD.

Our unique QKD technology provides superior performance leading to better business outcomes, and our ongoing R&D activities are helping us to enable global and pervasive quantum secure networking.

In this paper, we cover how we work to realise and validate scalable, quantum-secured networks in which our quantum key distribution technology is integrated into conventional telecoms networks, accessible by multiple users.

Relentless progress in quantum computing threatens to severely weaken much of the cryptography used today. In particular, all widely-used forms of public key cryptography rely on the difficulty of certain mathematically-hard problems, which can be solved efficiently on a large-scale quantum computer. To protect future network communications, it is imperative to develop new “quantum-safe” technologies resistant to attack in the quantum era.

The problem lies not just in the future. Today’s data is also susceptible to “harvest now, decrypt later” attacks, where an adversary can store encrypted messages today, to later decrypt when a large-scale quantum processor becomes available. This is particularly problematic for information with a long-term value, such as financial records, medical data, corporate IPR or details of a nation’s critical infrastructure.

Quantum cryptography provides a suite of protocols, the security of which can be proven from first principles. In particular, quantum key distribution (QKD) allows secret keys to be shared on optical networks. Unlike algorithmic-based techniques, QKD will be not vulnerable to attack by powerful computers, not even a quantum processor, in the future.

Although QKD protocols can be Information Theoretic Secure (ITS), real-world security requires a careful implementation.[1] There has been considerable effort in recent years to understand attacks and countermeasures on QKD systems and work to create a security certification framework is underway.[2]

There have been several impressive demonstrations of QKD networks to date.[3-7] However, most of these have been conducted using dark fibre or with equipment hosted in a lab. This work will review recent progress to embed quantum security devices, along with quantum resistant algorithms, in operational telecom networks, as well as the technological advances and innovations which have made it possible.

02

QKD Technology

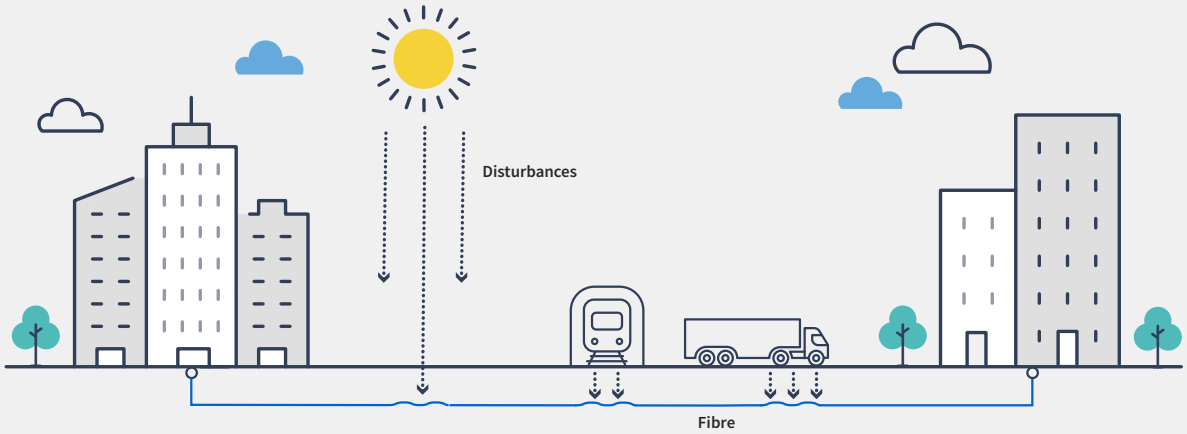
Our QKD systems[8] use laser pulses attenuated to the single photon level as carriers. These inevitably sometimes contain two or more photons, but by sending weaker ‘decoy’ pulses randomly interspersed with the signals, it is possible to eliminate potential information leakage due to these multi-photon pulses.[9]

The qubits are encoded as a phase difference between two paths in an asymmetric Mach-Zehnder interferometer in the transmitter and read out using a matched interferometer in the receiver.[10] Such fibre interferometers are typically very sensitive to ambient fluctuations in temperature. However, active stabilisation of the path lengths allows to operate the system continuously with minimal fluctuation in key rate.

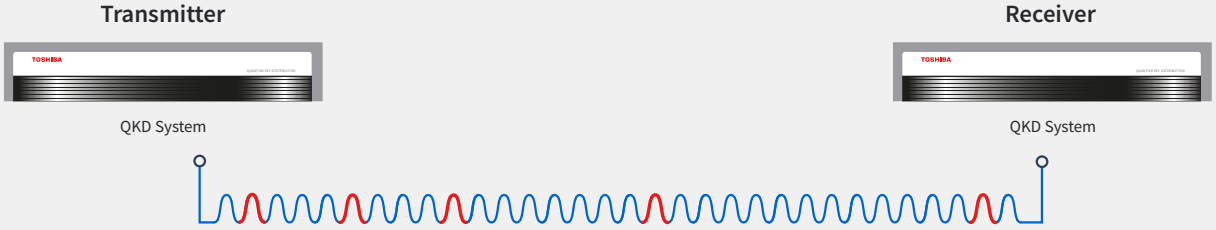
Secret keys are formed by implementing the BB84 protocol with decoy states, which has a complete security proof under the most general types of attack, and ITS authentication. Its security analysis takes account that a key formation session lasts a finite length of time, with a finite number of measurements, and so results in statistical uncertainty in the measured values. Consequently, keys can be guaranteed secure within a certain confidence bound. The probability of obtaining a compromised key (failure probability, ε) can be set very low, in our case $\varepsilon < 10^{-10}$, corresponding a frequency of less than one in tens of thousands of years.[9]

We’ve pioneered active stabilisation technology that allows our QKD systems to distribute key material continuously, in challenging operating conditions, without any user intervention. By embedding stabilisation pulses into the signal, we are able to avoid the need for recalibration of the system due to temperature-induced changes in the fibre lengths.

The realities of a commercial fibre network

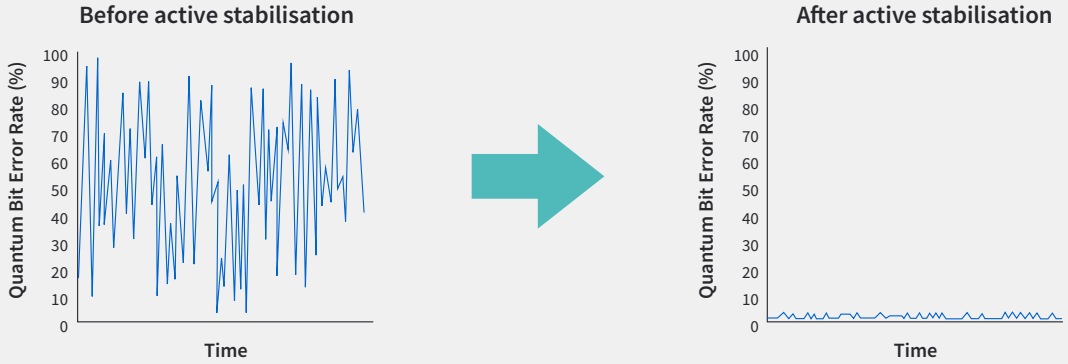


Toshiba's proprietary active stabilisation technology mitigates the impact of disturbances



Dedicated stabilisation pulses are embedded into the transmitted signals, providing a reference for fast automatic self-correction algorithms.

The result: dramatically increased stability and reliability



03

Long Distance QKD

Toshiba's QKD has market leading range on optical fibre due to its proprietary 'self-differencing' technology for single photon detection. This allows singe photons to be detected at GHz clock rates with minimal afterpulse noise. As a result, the Long Distance QKD system can operate over distances up to 184km of fibre and with secret key rates of ~ 800 kbit/s at 10 dB channel loss.

To achieve the longest possible fibre range, the quantum channel is provisioned on a DWDM channel near 1550nm, where photon loss in the fibre is minimal. Figure 1 plots the key rate measured for the Long Distance (LD) QKD system for different lengths of standard fibre, with an attenuation of 0.2 dB/km at 1550 nm, along with a simulation. Notice the key rate reduces exponentially with fibre length due to fibre loss and drops rapidly to zero when the detected photon rate becomes comparable to the noise rate.

An important aspect in ensuring optimum performance (maximum secret bit rate and range) is to utilise high frequency (1 GHz) gated rates whilst reducing system noise. Toshiba utilise a self-differencing technique for our Avalanche Photodiode Detectors to provide reduced noise and increased detection efficiency.[11]

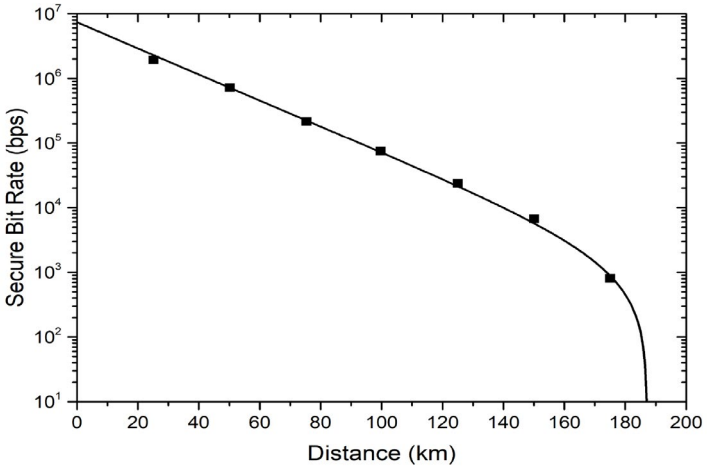
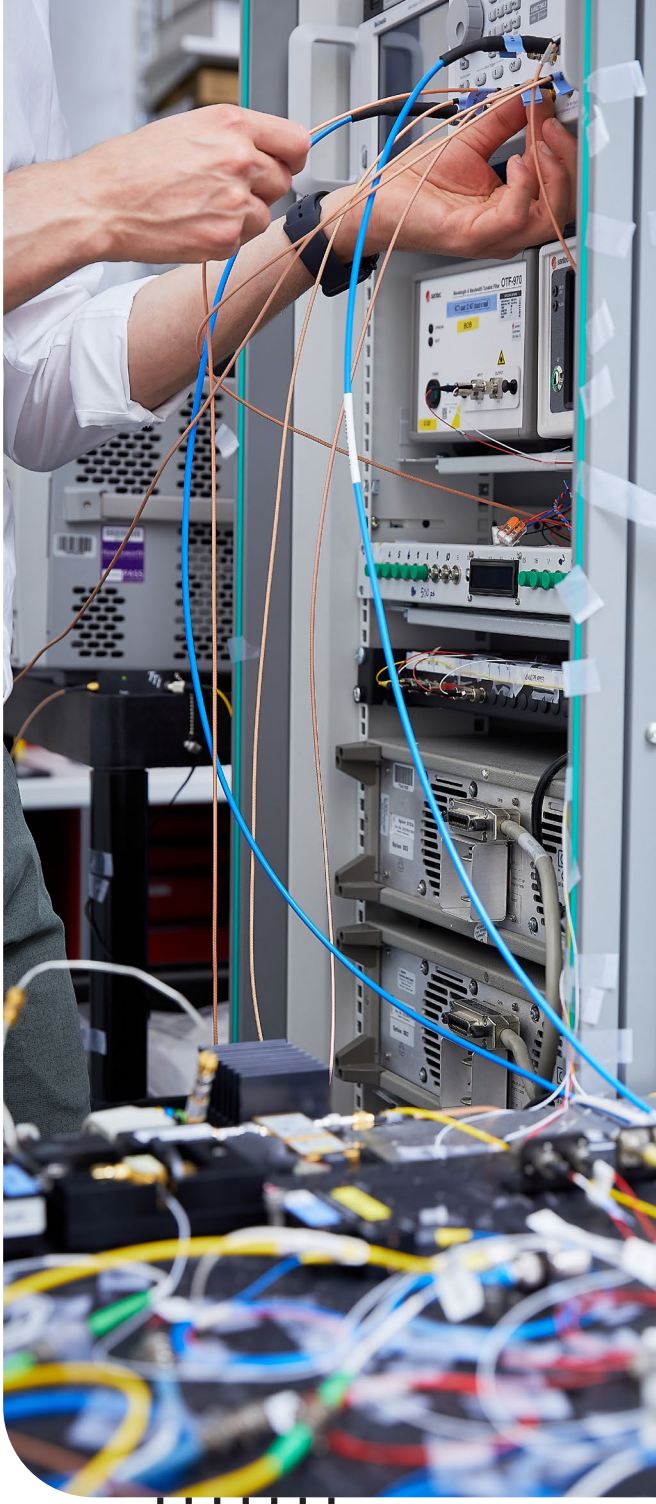


Fig. 1: Secure key rate vs fibre length measured (symbols) on the Toshiba LD QKD system, along with the calculated dependence (solid line).

It can be seen in Fig. 1 that the secure key rate (SKR) is typically ~ 800 kb/s at 50 km fibre length (10 dB loss), sufficient for >3,000 AES-256 keys per second. High key rates are important, especially in the backbone links of the network, which will provide key material simultaneously to thousands of users and applications.

The key rate rolls off around 187 km in Fig.1, corresponding to a maximum loss budget of 37 dB. This value can be extended by cooling the detector to reduce its dark count noise, allowing operation with lower rate quantum signals. In previous work we have demonstrated QKD over 240 km by thermo-electrically cooling to -60°C.[12]

The LD system can support a limited number of data channels launched concurrently on vacant DWDM channels in the C-band. The data channels create Raman scattered photons over a broad spectrum. As the launch power, or the number of data channels is increased, the Raman noise increases and eventually swamps the quantum signal, rendering QKD impossible. However, by carefully filtering the Raman noise in the receiver, co-existence of QKD and data channels with a combined launch power of a few dBm is possible for the LD QKD system.



04

Multiplexed QKD

Much higher data launch powers can be tolerated if we shift the quantum channel to the O-band (1310 nm), where the Raman noise is much lower. This configuration is used in the Multiplexed (MU) QKD system, to enable operation with a large number of co-propagating DWDM channels. This is highly advantageous in situations where dark fibre is not available, or prohibitively expensive, and the QKD channels must therefore be provisioned on data-carrying fibres.

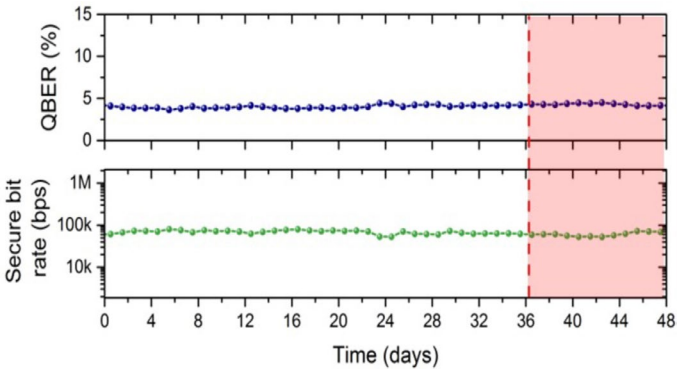


Fig. 2: QBER and SKR recorded on a 28.6 km installed fibre. After day 36, 31 DWDM channels were multiplexed onto the fibre to co-propagate with the quantum channel

Figure 2 plots the quantum bit error rate (QBER) and SKR measured on a 28.7 km installed fibre (16 dB loss) in BT Group's network over a forty day duration. The first 36 days of the trial were performed with only QKD signals propagating on the fibre. Remarkably, we see no change in the quantum bit error rate or secure key rate when (on day 36) 31 DWDM channels in the C-band (between 1530 and 1560 nm) are multiplexed onto the same fibre. These measurements were limited by the number of wavelengths available, but by increasing the laser power we observed that >20dBm of launch power could be supported in the presence of QKD, equivalent to 100 channels with 0 dBm launch power.

In addition to enabling high optical launch power and multiple data channel multiplexing, our MU system provides further performance and deployment benefits. We perform the multiplexing / demultiplexing of the user's classical data channels inline within our QKD appliances – this reduces costs along with the space needed for external multiplexing equipment. We also utilise ultra narrow temporal filtering for ~ 10 times improvement in fibre optic noise rejection.

The capability to multiplex QKD onto existing data carrying fibres presents significant benefits in terms of reduced fibre utilisation. We can, if required, further reduce the fibre requirement for QKD by deploying our MU product alongside classical data channels using only a single fibre strand (single fibre working).

05

QKD and high-speed data co-existence

Following detailed testing, Orange recently reported multiplexing of 60 x 100G data channels with the MU QKD system over 50km of fibre.[13] Along with the high number of data channels deployed, a high optical launch power (~17dBm) was used and high secret key rates were observed, as shown in figure 3.

These results highlight that the MU QKD system can be operated on fibres carrying high data bandwidths, thereby removing the requirement for dark fibre and allowing significantly lower operating costs.

In other work, JP Morgan Chase and Ciena have demonstrated MU QKD with 800G data channels (total bandwidth 2.4 Tb/s) over a 100 km fibre.[14]

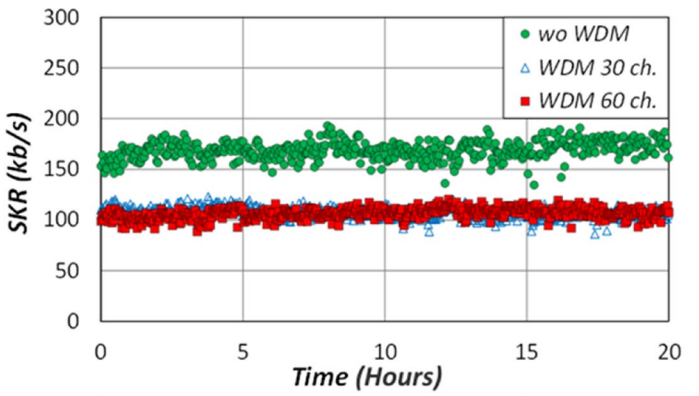
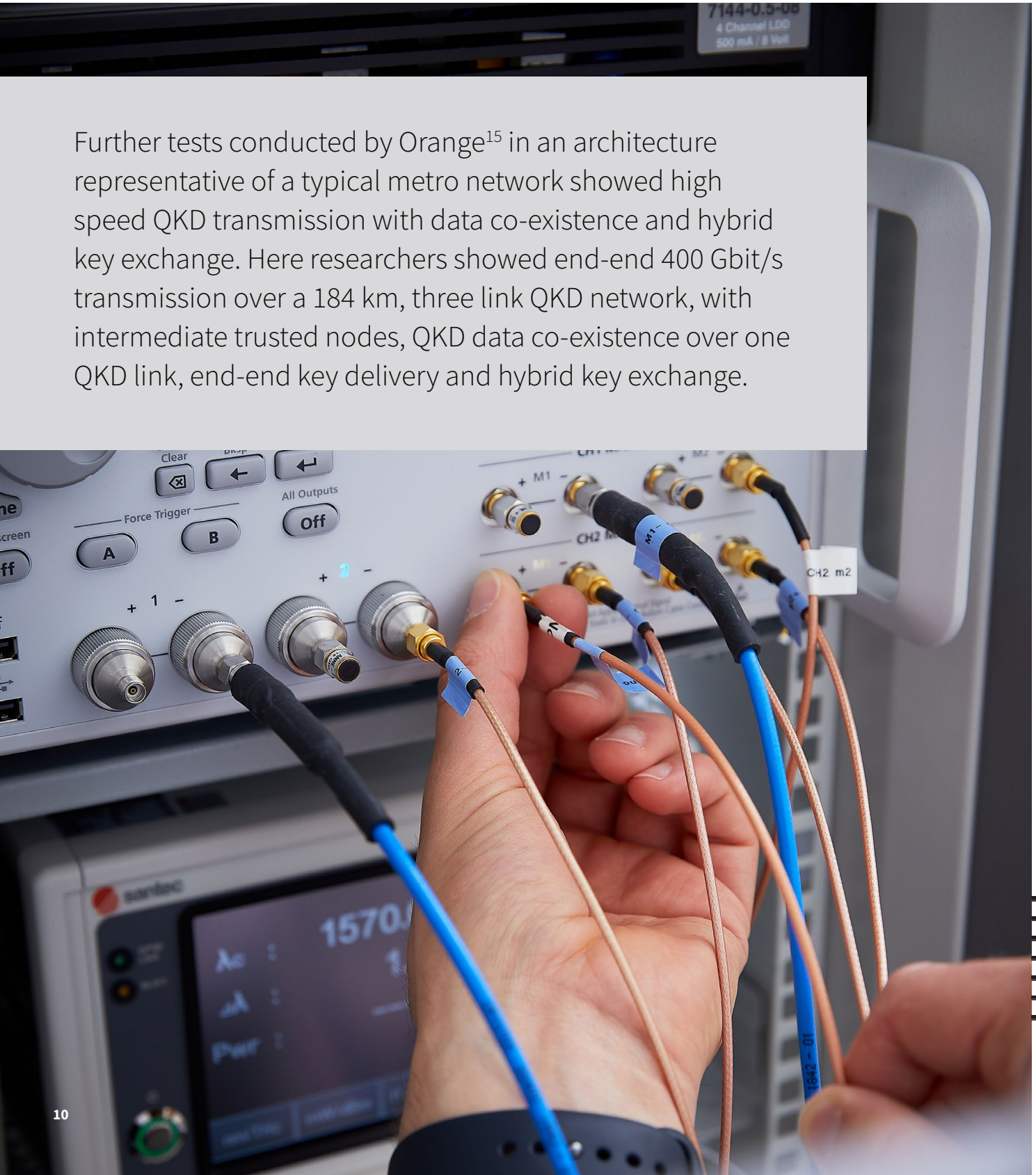


Fig. 3: Orange multiplexing results, SKR vs Time for 0, 30 and 60 WDM data channel multiplexing with QKD

06

QKD performance and co-existence in Metro network architectures

Further tests conducted by Orange[15] in an architecture representative of a typical metro network showed high speed QKD transmission with data co-existence and hybrid key exchange. Here researchers showed end-end 400 Gbit/s transmission over a 184 km, three link QKD network, with intermediate trusted nodes, QKD data co-existence over one QKD link, end-end key delivery and hybrid key exchange.



07

Key Management System

QKD can be implemented in a networked scenario using our Key Management System (KMS)[16] to facilitate delivery of symmetric keys between any two points connected to the network, as shown in Figure 4. Applications can request key material using a REST-based API, which has been standardised by ETSI.[17]

Deployments by multiple users demonstrate that our QKD technology is pragmatically and practically deployable for today's networking architectures, multiplexing schemes and data transmission requirements.

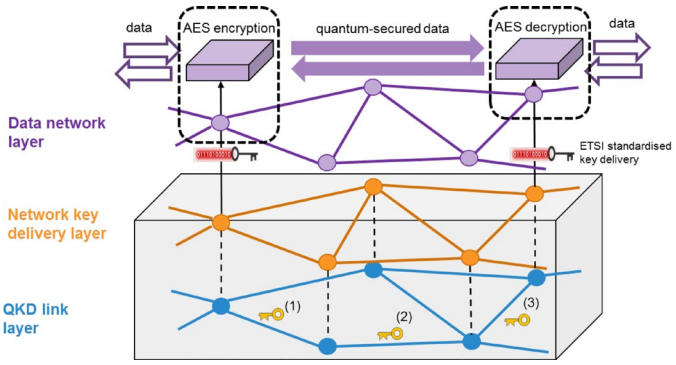


Fig. 4: Schematic of a Key Management System supplying keys for AES encryption of data.

We abstract the network into a physical QKD link layer, responsible for producing the local keys. These local keys are supplied to a network key delivery layer, which is responsible for routing a network key to the desired destination. The network key is protected in transit, using one-time-pad encryption with the corresponding local key, across each hop in the network.

The keys served by the KMS can be used in a variety of ways. For example, for one-time pad encryption of data, with information theoretic security, leveraging QKD's ability to deliver high volumes of key material. More commonly, however, the symmetric keys are used for bulk encryption of data between two sites using AES encryption, which is also quantum safe. A number of vendors of AES encryption hardware and software, operating in different layers of the OSI stack, have implemented the ETSI QKD-014 interface,[15] allowing compatibility with Toshiba QKD systems.

08

London Quantum-Secured Metro Network

Figure 5 shows a schematic of the London Quantum-Secured Metro Network. It consists of three core nodes located in secure locations in BT Group exchanges in London. These were chosen to be in central London, the East/ Docklands financial district and the West/M4 Corridor region, with the latter providing access to major datacentres to the west of London.

Fig. 5: Schematic of the London Quantum Secured Metro Network.

QKD systems were installed on the core links to provide a constant stream of key material between the core nodes, with both Toshiba's LD and MU systems deployed. Customers connect to the core network via an access tail from their premise to the nearest core nodes provided by OpenReach. The access tails use the Optical Filter Connect (OFC) product[18] which provides use of 8 DWDM wavelengths in the C-band.

Three of these channels are used for the quantum, classical and synchronisation channels of the QKD system, while the remaining wavelengths are available for encrypted customer data. OFC is specified to operate over links up to 40 km, although the QKD technology can span a much greater radius around each node. The KMS orchestrates delivery of key material to multiple customers connected to the network simultaneously.

09

Towards Global Networks

QKD performance is now sufficient to allow national/continental scale quantum-secured networks based solely on fibre. As discussed above the LD QKD system offers a maximum loss budget of 37 dB, sufficient to directly connect the core nodes of a national network, located in the main population centres. The link loss can be further extended by using lower noise detectors.

Such high loss tolerance is a significant advance, as it eliminates the requirements for trusted nodes in intermediate sites, such as communication huts located between cities, thus reducing the cost of both the hardware in the network and its secure deployment.

The most promising approach for longer distances in the near term is to use low Earth orbit satellites, as shown in Figure 6. These can form a QKD link between the satellite and fibre networks in different regions, thereby forming a global network.

In order to enable practical (real time, large quantum key generation in a single overpass) and scalable (small telescope apertures and communication with a large number of ground nodes) satellite QKD transmission there are several considerations and challenges to overcome.

Toshiba researchers[19] have recently emulated an LEO satellite QKD overpass showing real time, free space, GHz QKD transmission which shows favourable QKD key distillation of large keys in a single overpass

With several missions planned to launch in the coming few years, rapid progress towards a global quantum-secured network can be expected.

In the longer term, quantum repeaters may become viable for all fibre, global quantum networks. Recently there has been promising progress. Practical techniques for Twin-Field QKD,[20] which has similar scaling to a 1-stage quantum repeater, have been demonstrated[21].

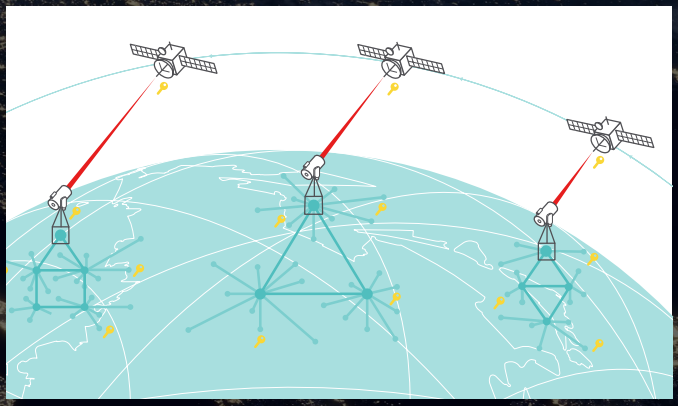


Fig. 6: Schematic of a global Quantum Secured Network, in which large-area fibre QKD networks are linked by Satellite QKD links.

To find out more about Toshiba QKD, please visit **toshiba.eu/quantum**

or contact us at **quantum@toshiba.eu**

References

[1] Implementation Security of Quantum Cryptography, ETSI White Paper No. 27, https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf

[2] Common Criteria Protection Profile – Pair of Prepare and Measure Quantum Key Distribution Modules, ETSI GS QKD 016 https://www.etsi.org/committee/qkd

[3] The SECOQC quantum key distribution network in Vienna, M Peev et al, New J. Phys. 11 075001 (2009)

[4] Field test of quantum key distribution in the Tokyo QKD network, Optics Express 19, 10387 (2011)

[5] Cambridge Quantum Network J.F. Dynes et al. npj Quantum Inf 5, 101 (2019)

[6] Implementation of a 46-node quantum metropolitan area network, T. Y. Chen, npj Quantum Inf 7, 134 (2021)

[7] OpenQKD: https://openqkd.eu/

[8] https://www.toshiba.eu/quantum

[9] Efficient decoy-state quantum key distribution with quantified security, M. Lucamarini, K.A. Patel, J.F. Dynes, B. Fröhlich, A.W. Sharpe, A.R. Dixon, Z.L. Yuan, R.V. Penty & A.J. Shields, Optics Express. 21, 24550 (2013)

[10] 10-Mb/s Quantum Key Distribution, Z. L. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato and A. J. Shields, J. Lightwave Technol. 36, 3427 (2018)

[11] High speed single photon detection in the near infrared Z L Yuan et al Appl. Phys. Lett. 91, 041114 (2007)

[12] Long-distance quantum key distribution secure against coherent attacks, B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. L. Yuan and A. J. Shields, Optica 4, no 1, (2017)

[13] Co-propagation of 6 Tb/s (60x100Gb/s) DWDM & QKD channels with ~17 dBm aggregated WDM power over 50 km standard single mode fiber, P. Gavignet, F. Mondain, E. Pincemin, A. J. Grant, L. Johnson, R. I. Woodward, J. F. Dynes, A. J. Shields, arXiv:2305.13742 (2023)

[14] Paving the Way towards 800 Gbps Quantum-Secured Optical Channel Deployment in Mission-Critical Environments, F. Toudeh-Fallah, M. Pistoia, Y. Kawakura, N. Moazzami, D. H. Kramer, R. I. Woodward, G. Sysak, B. John, O. Amer, A. O. Polychroniadou, J. Lyon, S. Shetty, T. D. Movva, S. Upadhyay, M. R. Behera, J. A. Dolphin, P. A. Haigh, J. F. Dynes and A. J. Shields, arXiv:2202.07764 (2022)

[15] Co-propagation of QKD & 6 Tb/s (60 × 100G) DWDM Channels with ~17 dBm Total WDM Power in Single and Multi-Span Configurations, P. Gavignet, E. Pincemin, F. Herviou, Y. Loussouarn, F. Mondain, A. J. Grant, L. Johnson, R. I. Woodward, J. F. Dynes, B. Summers, A. J. Shields, K. Taira, H. Sato, R. Zink, V. Grempka, V. Castay, and J. Zo u. https://arxiv.org/ftp/arxiv/papers/2312/2312.11924.pdf

[16] A high-speed key management method for quantum key distribution network, R. Takahashi et al. 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN) 437-442 (2019)

[17] Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API, ETSI GS QKD014, https://www.etsi.org/committee/qkd

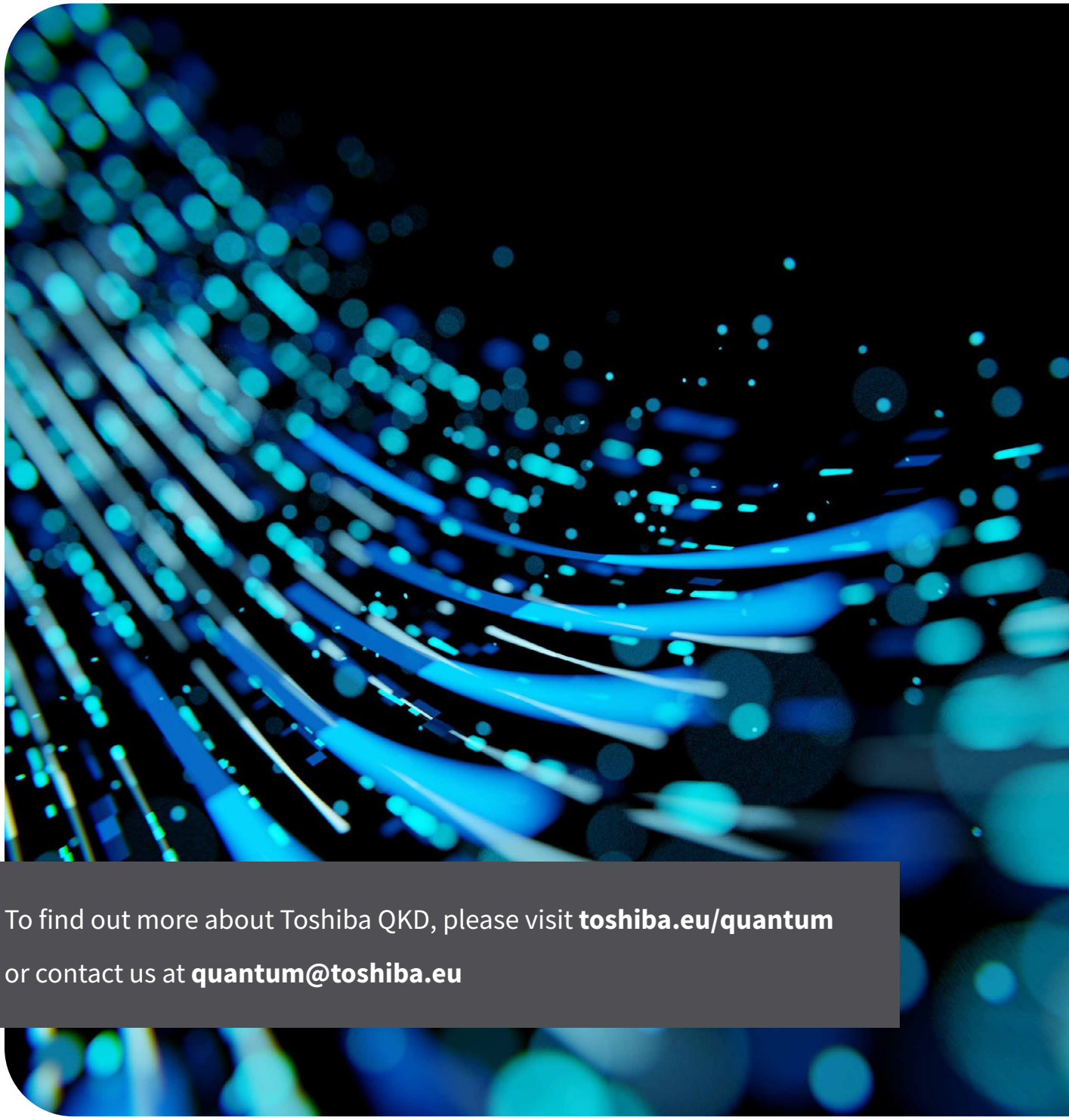
[18] https://www.openreach.co.uk/cpportal/products/optical/optical-spectrum-access(OSA)

[19] Real-time gigahertz free-space quantum key distribution within an emulated satellite overpass, Thomas Roger et al., Sci. Adv.9, eadj5873(2023).DOI:10.1126/sciadv.adj5873

[20] 600-km repeater-like quantum communications with dual-band stabilization, M Pittaluga, M Minder, M Lucamarini, M Sanzaro, R I Woodward, M-J Li, Z Yuan & A J Shields Nature Photonics 15, 530 (2021).

[21] Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, M. Lucamarini, Z. L. Yuan, J. F. Dynes & A. J. Shields, Nature 557, 400 (2018).

TOSHIBA



To find out more about Toshiba QKD, please visit **toshiba.eu/quantum**

or contact us at **quantum@toshiba.eu**

Toshiba Europe Limited, 406 Cambridge Science Park Milton Road, Cambridge CB4 0WW, UK