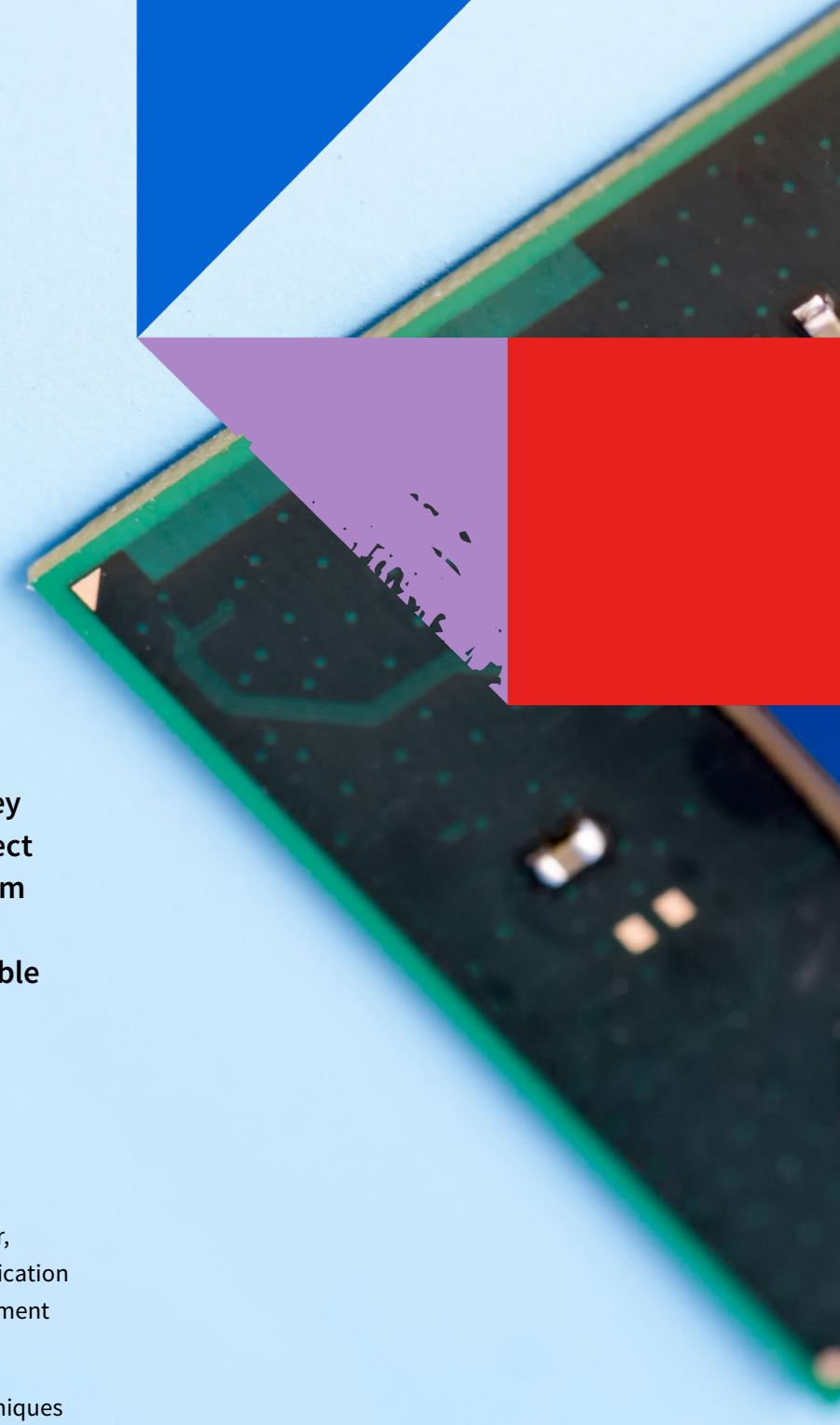
TOSHIBA

Transforming telecoms

EASING YOUR TRANSITION TO A QUANTUM-SAFE NETWORK

Easily integrate quantum-safe technologies into your existing telecoms infrastructure without dedicated fibres

Summary



Quantum computing technology is advancing rapidly, with ever larger quantum circuits becoming available. A large-scale quantum computer will reduce the time taken to break public key encryption – the techniques which protect much of our internet activity today – from trillions of years to mere seconds[1]. For telecommunications providers responsible for the protection of global or local networks, there's an urgent need to act ahead of that reality.

Quantum Key Distribution (QKD) technology offers a powerful way to securely transmit data without risk of decryption, even by quantum computers. However, integrating the technology into existing telecommunication networks has posed problems that challenge deployment and compromise performance – until now.

Toshiba has developed pioneering multiplexing techniques that enable the easy integration of QKD technology with commercial and public network infrastructure, allowing quantum and conventional data channels to co-exist in a single deployed optical fibre. Toshiba's multiplexed QKD technology offers a number of unique features which, combined, ensure telecoms providers can now more easily upgrade and future-proof their existing infrastructure, ready to provide the backbone of the quantum-secure network.

[1]https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/?sh=747ad06b7d3f

Introduction

Across the globe, vast amounts of data are transmitted and shared through optical fibre networks every day. While cyber security attacks have boomed in the past decade alone, public key cryptography has provided an effective barrier, keeping bad actors from accessing valuable data. All that changes with the arrival of quantum computing.

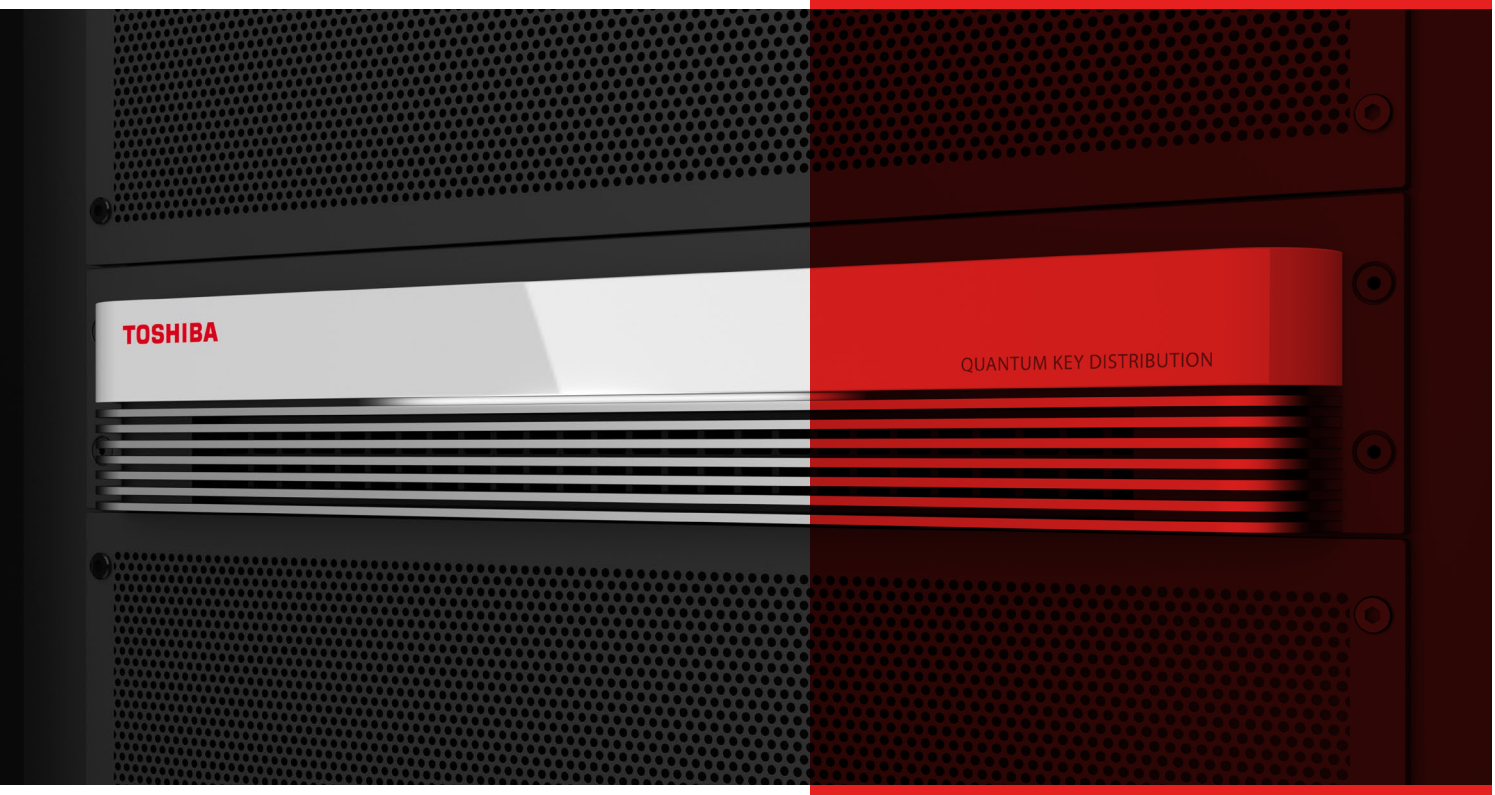
“Harvest now and decrypt later” attacks have been in the public awareness for some time, but have presented more of an abstract threat than a tangible one. But as the availability and reliability of quantum computers increases, these kinds of attacks will come to fruition. Attackers who previously recorded and stored encrypted data in transit will soon be able to easily crack commonly used security protocols such as public key encryption.

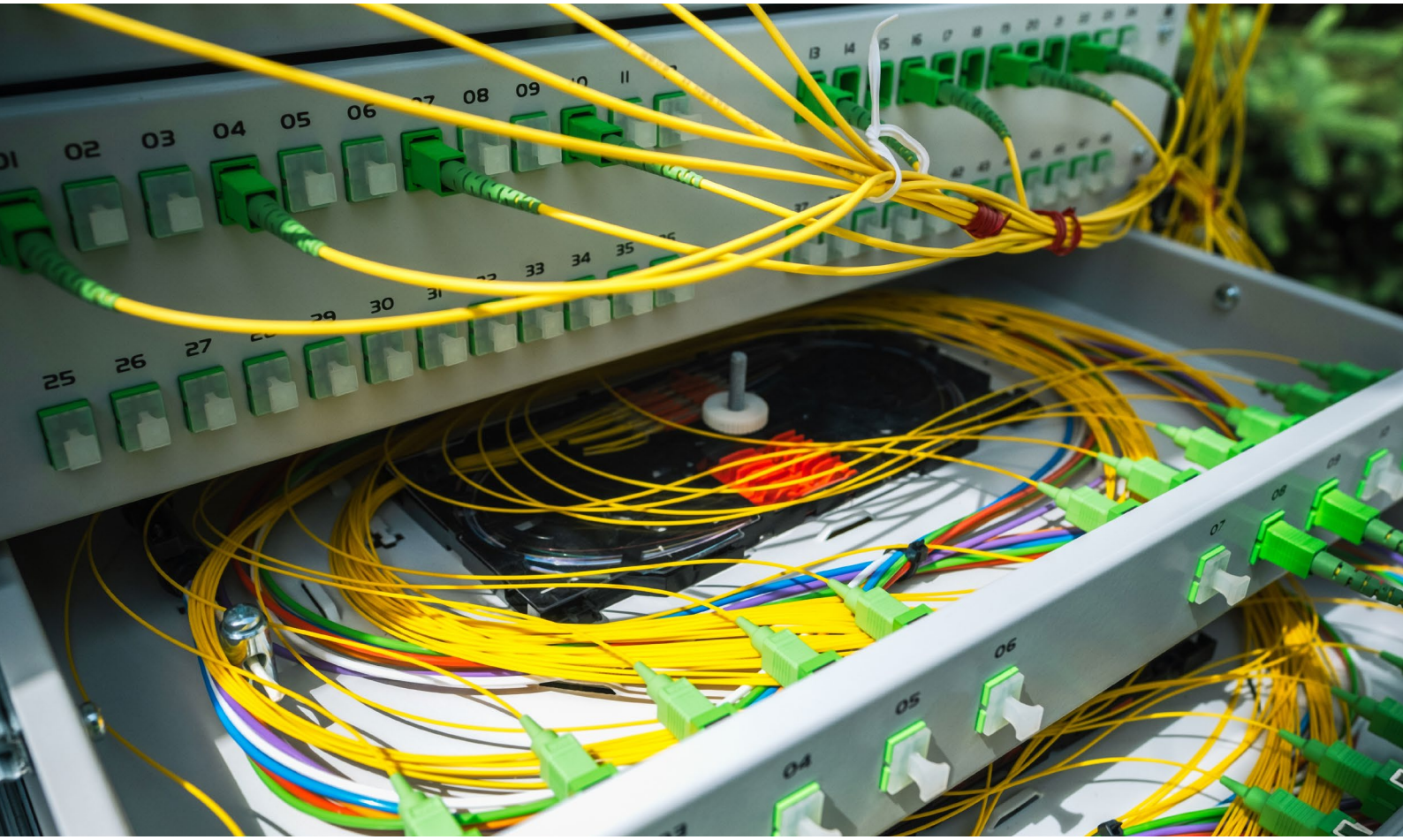
QKD technology offers a solution. Once it is built into telecommunication networks, it will protect data against decryption, now and in the future.

What is QKD?

Quantum Key Distribution (QKD) technology takes advantage of the laws of quantum physics to ensure that bad actors cannot decrypt data in transit. QKD-protected data is resilient to attack by a quantum computer, or indeed any other powerful computing resource. This guarantees protection against all current attack methods, and crucially provides resistance against future developments in high-performance or quantum computing.

QKD is an optical technology which works by transmitting individual photons between two parties, enabling them to communicate and agree on the same shared secret encryption key to safeguard their data. It can also detect whether a third party is attempting to eavesdrop on their key agreement protocol and mitigate against this.





As a telecoms provider, QKD technology offers you a way to protect your customers from current and future cyber security threats. However, integrating QKD into existing networks has traditionally presented complications, including the need to introduce dedicated dark fibre cables alongside your original infrastructure to carry the QKD signal.

With respect to longer distance requirements (for example, core transmission networks or long-haul links between key sites), the dark fibre approach can work effectively. Toshiba provides a Long Distance QKD system, operating on dark fibre, specifically for this purpose.

For other parts of your network, it may be logistically and commercially impractical to use dedicated dark fibres – for example, in your metro networks, either connecting central offices in a city area, or the access tail connections from the central office to customers.

Challenges of QKD delivered solely via dedicated dark fibres

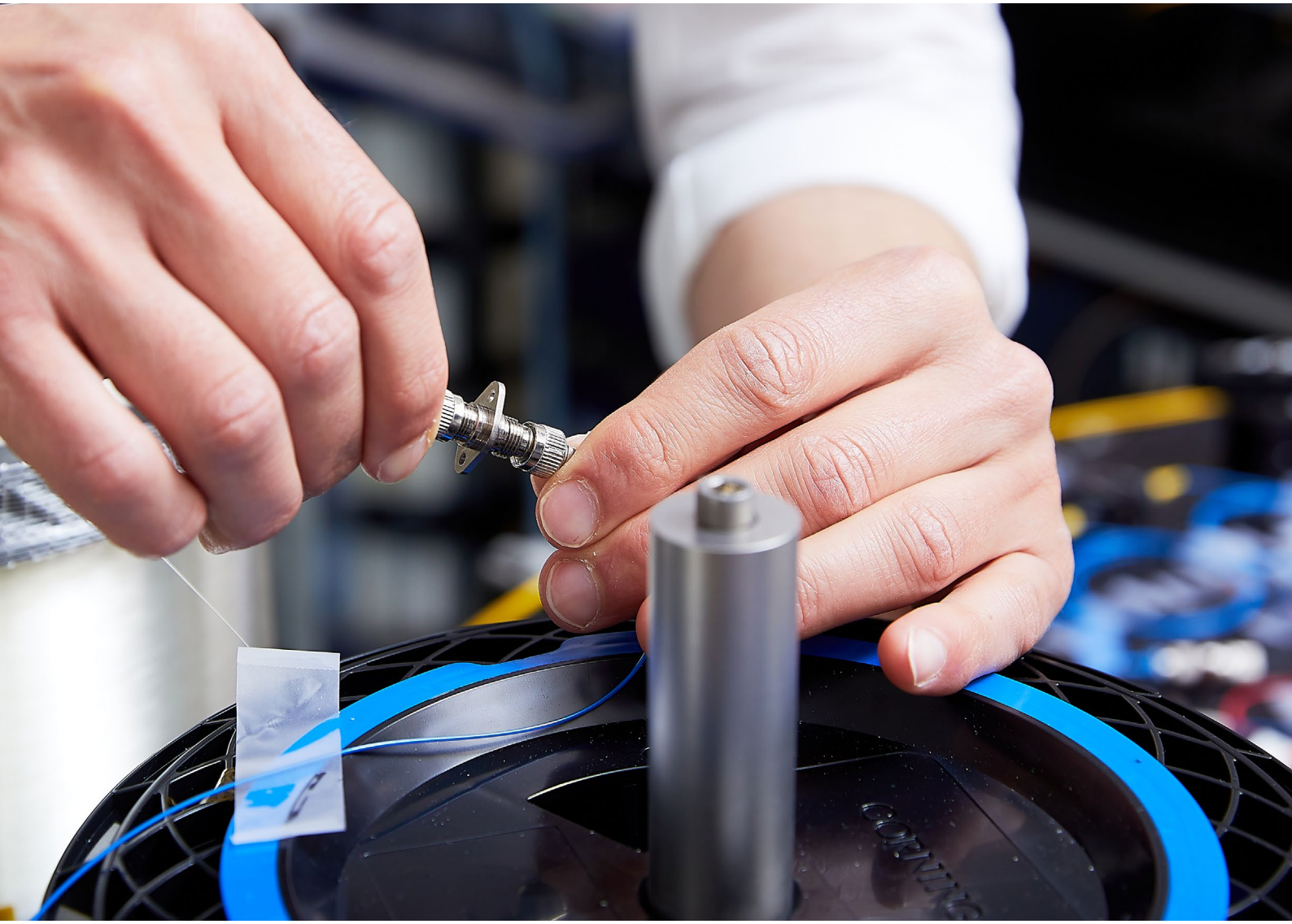
- **High cost:** It would be expensive and logistically challenging to install an additional dark fibre for every QKD link across your network, especially for metro connections in built-up areas.
- **Increased resource usage:** Dark fibres are often a scarce and valuable resource which are better deployed for other customer services.
- **Limited redundancy:** There is limited redundancy/back up with a dedicated dark fibre in the event of failure or performance reduction.

Multiplexed QKD Systems

Wavelength division multiplexing (WDM) is a common technique to increase a fibre's data carrying capacity, launching multiple data channels which use different optical wavelengths on the same fibre.

In the most commonly used form, called Dense Wavelength Division Multiplexing (DWDM), channels are arranged in the telecom C-band spanning 1530 to 1565nm, with a channel spacing of approximately 0.4nm. The channel count can be further increased using the L-band extending from 1565 to 1625nm.

WDM – or simply '**multiplexing**', as we will refer to it from now – is the simplest way to integrate QKD in situations which would normally be prohibitively expensive as it eradicates the need for dedicated fibres for QKD. Instead, QKD is integrated onto the existing fibre, with the secret encryption keys being transmitted on the same fibres that are carrying conventional telecoms data services.



Typical challenges with multiplexed QKD

QKD signals are typically 100 million times weaker than those used to carry conventional data. It's therefore unsurprising that it's challenging to preserve the very faint quantum signal in the presence of multiple conventional data channels.

In particular, scattering effects due to multiple, high power conventional data channels can create noise photons over a broad wavelength band, which can be hundreds of nanometres wide. These photons can easily dominate the weak quantum signals, making quantum key distribution impossible.

The Toshiba multiplexed QKD solution

Multiplexing without compromise

Toshiba has pioneered techniques to overcome these challenges and allow QKD to be operated on data-carrying fibre. We have achieved an industry-leading performance with our unique multiplexed QKD system, which places the quantum channel in the O-Band at 1310nm, spectrally distant from the data channels in the C and/or L-Bands. This separation reduces the effect of the scattered photons and enables more effective noise filtering.

As a result, it becomes possible to send QKD signals on fibres carrying multiple, conventional data signals. Using this technique, your existing network can be easily and incrementally upgraded to support QKD.

As you'll see in Figure 1, operator data channels in the 1550nm window are presented to the Toshiba transmitter. Then, inside the appliance, the operator data channels are multiplexed onto a fibre along with the quantum channel within the 1310nm window.

For situations in which customers cannot use the O-band – for regulation reasons or otherwise – Toshiba offers an alternative solution in which the quantum channel is transmitted on one of the DWDM wavelengths in the C-band.

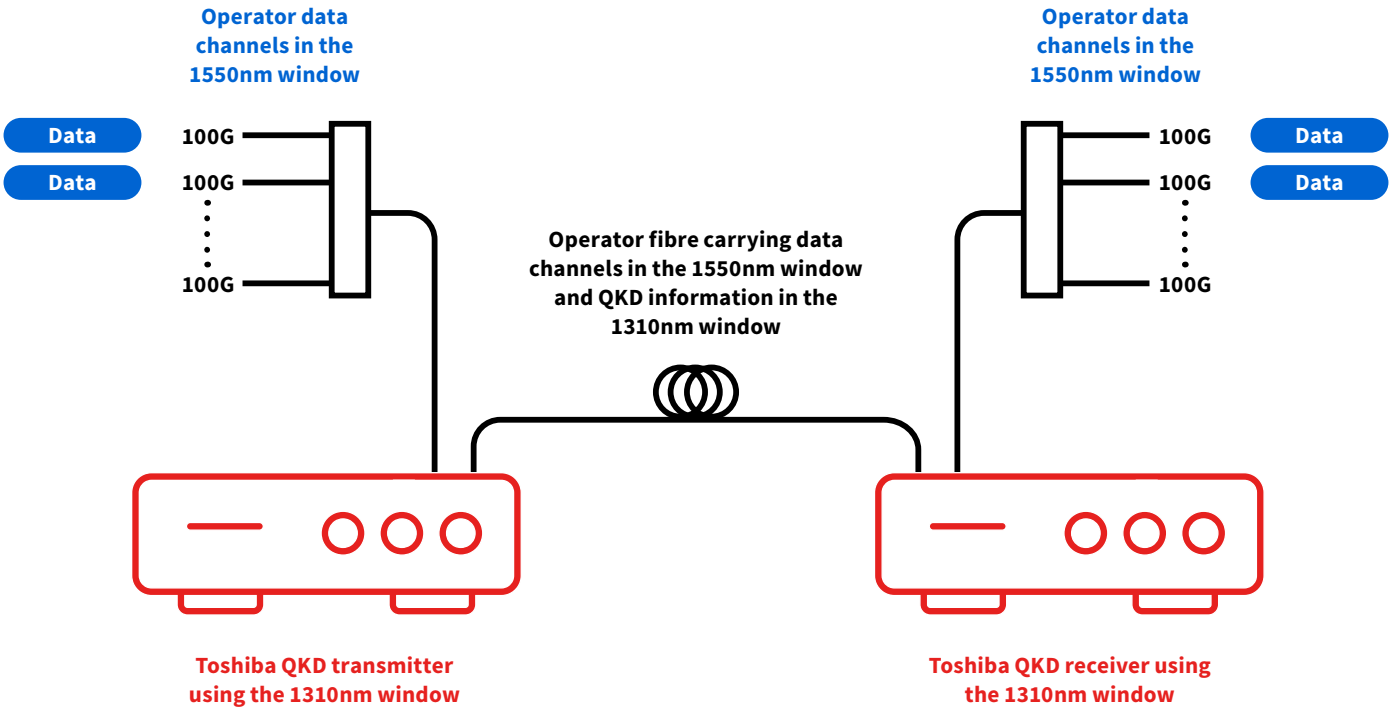


Figure 1: Overview of Toshiba's multiplexed QKD system

Toshiba's "MU" QKD multiplexing technology

Performance

For telecoms providers, multiplexing data with QKD information on the same fibre typically involves making trade-offs on a number of factors: the number of data channels multiplexed, the total optical launch power into the fibre, the QKD secret key rate and the overall fibre transmission distance.

The Toshiba-patented technology within our QKD systems overcomes these challenges and achieves optimum QKD system performance.

The Toshiba MU Multiplexed QKD system is able to support multiple co-propagating data channels. In Figure 2 we show the results of tests with up to 24 DWDM data channels. In these tests we set the launch power of each DWDM channel to be 0dBm (1mW), a value typical of that used in the metro network.

Figure 2 demonstrates the measured secret key rate as the number of co-propagating DWDM channels is increased from 0 to 24. For a 50km fibre link – typical of the range required in most metro networks – the QKD-only secret key rate is ~245kb/s, corresponding to >90 AES-256 keys per second. In the presence of 24 data channels, the key rate declines only fractionally to 220kb/s, demonstrating that there is minimal key rate degradation, even when introducing many multiplexed data channels.

Extending the fibre distance to 70km, we find the multiplexed QKD system can still tolerate multiple co-propagating data channels. Fig.3 illustrates the co-propagation of 24 data channels with QKD at a key rate of 31kb/s. Even for a fibre distance of 100km (not shown in Fig. 2), we find the system is able to support QKD and several co-propagating, full power data channels.

Toshiba's multiplexed QKD systems are also highly resilient. Thanks to a combination of unique stabilisation techniques and dynamic auto-alignment processes, it is possible to add or drop data channels without impacting the performance of data or quantum channels, or having to restart the system – meaning zero-downtime adjustment of the data channels.

With this resilience, it's easier for you to scale your operations by introducing additional data channels without impacting the performance of either data or quantum channels.

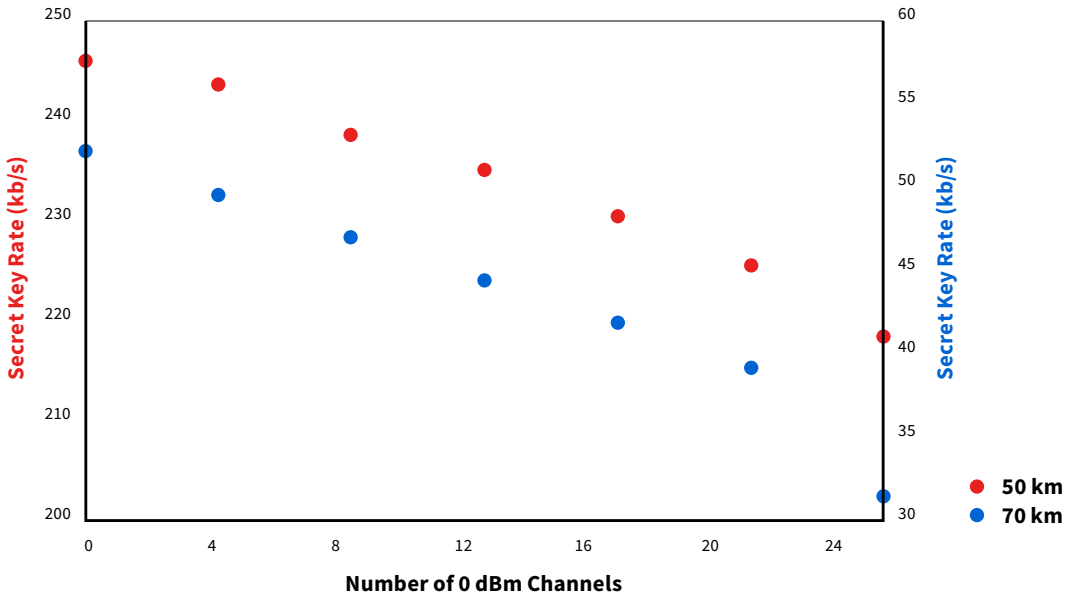


Figure 2: Impact of the number of 0dBm data channels on Toshiba's multiplexed QKD system. Illustrated at 50km (red markers, left y-axis) and 70km (blue markers, right y-axis

Key benefits

Multiplexing onto an existing fibre typically means making compromises. But with our MU system, customers can achieve a uniquely high performance across multiple factors at once. This removes many of the barriers to adoption which previously existed and allows telecoms providers to implement the technology into their existing infrastructure.

- **Supports a high number of data channels**
- **Supports high secret key rates**
- **Supports high transmission distances**
- **Supports high optical launch power**
- **Resilience while you scale**

Toshiba's Multiplexed QKD in action

Toshiba's QKD systems are already being used by customers to drive business success.

We collaborated with JP Morgan Chase and Ciena on applications in the banking sector. Using the Toshiba MU QKD system, JPMC demonstrated co-existence of the quantum channel with two 800Gb/s and eight 100Gb/s channels over a 70km fibre link, with a key rate able to support up to 258 AES-256 encrypted channels at a key refresh rate of 1 key/sec. Operation of QKD and the ten high-bandwidth channels was also verified for fibre lengths up to 100km.

Working with BT, we demonstrated co-existence of QKD and 31 DWDM channels over installed fibre. In these tests, the installed fibre had a length of 28.7km and an optical loss of 16dB. The QKD system operated with a secure key rate of 66kb/s, which was unaffected by the co-propagating data. Our multiplexed QKD system has subsequently been deployed in the London Quantum Secured Metro Network, launched by BT and Toshiba as the world's first trial of a commercial QKD network.

Conclusion

Toshiba has led innovation in QKD systems for nearly 30 years and has consistently demonstrated world-leading systems that push the boundaries of the technology.

Toshiba's world firsts:

2003

First company to demonstrate QKD over 100km of fibre.

2008

First QKD network in Europe and first company to show QKD continuous secret key rates > 1Mbps.

2017

First company to show QKD secret key rates > 10Mbps.

2021

Demonstrating twin-field QKD over a distance of 600km; making QKD possible between cities for the first time.

2022

JP Morgan Chase, Ciena and Toshiba demonstrate multiplexing of QKD and 2.4Tb/s of data over a 100km fibre link.

April 2022

Joint launch of the world's first trial of a commercially available Quantum Secure Metro Network with BT in London.

Dedicated-fibre QKD may still play a role in some instances. However, for many applications a dedicated fibre will not be realistic or necessary. To make QKD a practical route for telecoms providers, a QKD system was needed which could be integrated with 1550nm band traffic.

That's exactly what we achieved. By enabling co-existence of a quantum channel and a high number of classical data channels within a single optical fibre, Toshiba has overcome a long-established limit to QKD systems. This in turn has created a practical way for telecoms providers to future-proof their networks against the threat posed by quantum computing.

Contact Lee Johnson, QKD Business Development Manager, to discover how multiplexing can help integrate QKD into your networks.

Lee.johnson@crl.toshiba.co.uk

TOSHIBA