
# Quantum Cryptography

## Securing the future of a digital society

By adopting Quantum Key Distribution, organizations can **protect their communication infrastructure** from today's vast array of cyber-threats, as well as those of tomorrow. Already, hackers are using techniques such as harvest and decrypt, where data is scraped and stored today with the aim of decrypting it once they have the capability to do so through advances with supercomputers, the realisation of a **quantum computer**, or the discovery of new techniques for cryptanalysis. With QKD, any data which requires **long-term protection** is not only secure in today's IT landscape, but also **future-proofed** to remain protected in the impending **quantum age**.

Robust levels of security are required in many sectors. In **healthcare**, the technology has been applied to ensure the secure transmission of genome data in Japan. Within the **public sector** QKD is used to provide government with secure communications, in the **finance industry** to **protect banking network infrastructure** and in **aerospace** and **pharmaceuticals** to protect high-value long-life **Intellectual Property**. Equally, in the age of IoT and smart cities, the necessity for a robust, **tamper-proof** and **ultra-sensitive infrastructure** is essential to ensure day-to-day life operates without disruption both now and in the future.

Toshiba is the world leader in high-speed quantum cryptographic systems. Based on decades of scientific research, we have taken on the challenges of this unexplored field and have pioneered the path to practical use.

### Long range

Toshiba QKD enables long range deployments. Toshiba was the first to demonstrate QKD over 100 km of fibre in 2004 and have demonstrated, in lab conditions, the Twin-Field QKD protocol capable of operating over 500 km of fibre

### High key rates

Toshiba QKD offers market leading secure key rates. In fact we were the first to demonstrate continuous secure key rates exceeding 1 Mb/s (in 2008) and 10 Mb/s (in 2017).

### Data co-existence

Toshiba's Multiplexed QKD solution allows QKD to be operated on fibre carrying multiple 10 Gb/s or 100 Gb/s data channels, eliminating the need for dark fibre and reducing the cost of deployment.

### Fully automated operation with plug & play setup

Automated start-up and system optimisation in real time, delivered through active stabilization technology, that allows the system to distribute key material continuously without any user intervention in even the most challenging operating conditions.

### Easy-to-use graphical user interface

A simple web-browser-based interface provides access to both real-time and historical performance data.

### Integrated key delivery interface

An integrated key delivery interface is provided for secure key delivery. This is compatible with leading encryptors, and other applications using ETSI industry standards.

# Product details

Two variants are available: a **Multiplexed QKD System** with O-band quantum channel, which removes the need for dark fibre when operating on a 'lit' optical fibre; and a **Long-Distance QKD System** with C-band quantum channel for the longest possible range.

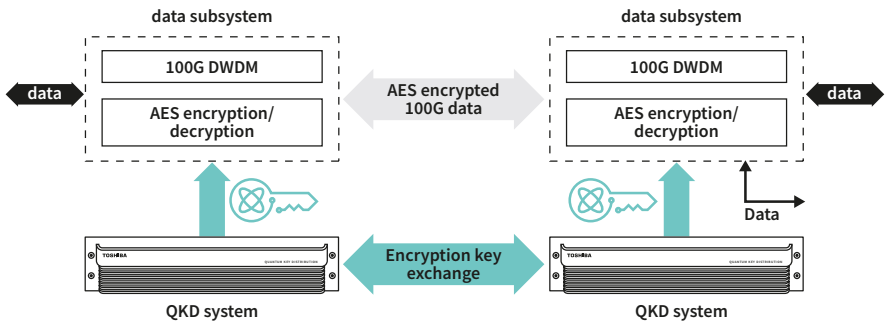
| | Multiplexed QKD System | Long-Distance QKD System |
|---|---|---|
| **Key Exchange Protocol** | Toshiba T12 protocol (efficient BB84 protocol with decoy states and phase encoding) | |
| **Quantum Wavelength** | 1310 nm | 1550 nm |
| **Fibre Requirement** | Single fibre pair or single bidirectional fibre | Two fibres required |
| **Multiplexing Compatibility** | Option to multiplex multi-channel C-band DWDM customer data with up to +20 dBm[1] total launch power | Limited-bandwidth multiplexing supported |
| **Secure Key Rate** | 300 kb/s at 10dB channel loss | 300 kb/s at 10 dB channel loss |
| **Maximum Loss (using ideal SM fibre)** | 30 dB (1310 nm) specified | 30 dB (1550 nm) specified |
| **Detection Technology** | Proprietary self-differencing semiconductor detectors | |
| **Security Parameter** | Key failure probability $< 10^{-10}$, corresponding to less than once in 30,000 years | |
| **Monitoring functions** | SNMP v2 & v3, GUI, CLI | |
| **Key Delivery Interface** | Integrated Key Delivery Interface to provide keys to encryptors and other applications supporting ETSI GS QKD 014 industry standard key delivery API | |
| **Standards** | **CE, UKCA:** BSI EN 55032, BSI EN 55035, BSI EN 61000-3-2, BSI EN 61000-3-3, BSI EN 63000, BSI EN IEC 62368-1, BSI EN IEC 60825-1, BSI EN IEC 60825-2<br>**FCC:** 47 CFR, Part 15 **FDA:** 21 CFR, Part J | |
| **Dimensions** | Standard 19'' rack mount (3U height) | |

[1] Operators should ensure all system deployments adhere to current laser safety limits

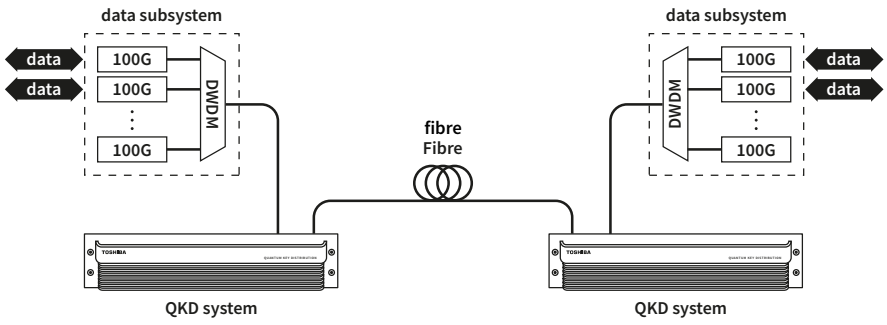
# Network Integration

Toshiba's Multiplexed QKD systems include add/drop filters for simple integration into existing fibre networks: all C-band user traffic can be passed through the unit without requiring additional multiplexing hardware.

The schematic (right) shows an example use case, with an AES encryptor obtaining keys from a Multiplexed QKD system to secure high-bandwidth data streams.




**Key distribution and encryption**




**Physical layer**


TOSHIBA

Toshiba Europe Limited, 406 Cambridge Science Park
Milton Road, Cambridge CB4 0WW, UK | **Tel: +44 1223 659730**

https://www.toshiba.eu/quantum
quantum@toshiba.eu