

# Quantum Cryptography

## Toshiba Long Distance and Multiplexed QKD systems

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.



### Fully automated operation with plug & play setup

Automated start-up and system optimization in real time, delivered through active

stabilization technology that allows the system to distribute key material continuously, in even the most challenging operating conditions, without any user intervention.



### Easy-to-use graphical user interface

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

performance data, as well as reporting any tamper attempts, providing perfect security and peace of mind.



### Integrated key management / delivery system

Toshiba's Key Management System is

included with QKD systems for key storage / delivery. This is compatible with many leading encryptor vendors, using ETSI industry standards.



### Long range

Toshiba QKD offers the longest range on fibre available commercially today, and were first to demonstrate QKD over 100km of fibre in 2004, and have demonstrated in lab conditions the Twin-Field QKD protocol capable of operating over 500km of fibre



### High key rates

Toshiba QKD offers the highest 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.

## Product details

The Toshiba **Multiplexed QKD System** uses an O-band quantum channel, which removes the need for dark fibre when operating on a 'lit' existing optical fibre; the **Long-Distance QKD System** uses a C-band quantum channel for the longest possible range

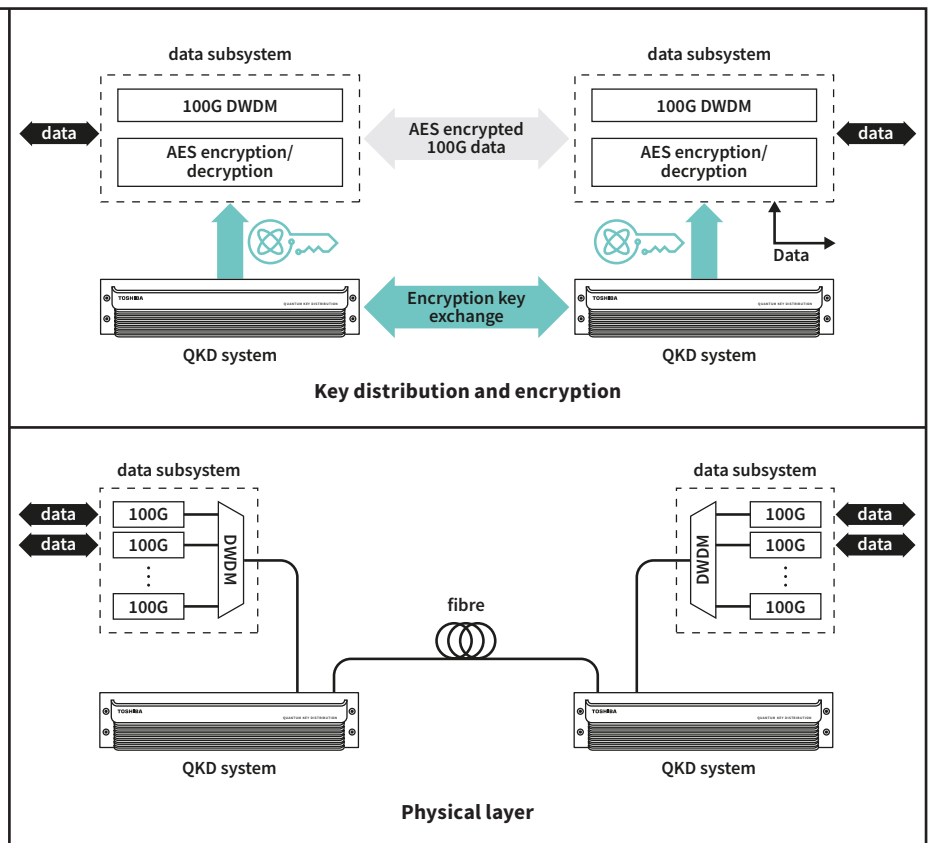


	Multiplexed QKD System	Long-Distance QKD System
Key Exchange Protocol	Toshiba T12 protocol (efficient BB84 protocol with decoy states and phase encoding)	
Quantum Wavelength	1310 nm	1550 nm
Fibre Requirement	Two fibres, or single bi-directional fibre	Two fibres required
Multiplexing Compatibility	Option to multiplex C band high bandwidth customer data (with up to +20dBm 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 (ideal SM fibre)	30dB specified loss budget	30dB specified loss budget
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 Management	Key Management (key generation, key storage, proactive/on-demand key delivery). System supporting ETSI GS QKD 014 industry standard key delivery API	
Standards	CE, UKCA: EN 55032:2015+A11, EN 55035:2017+A11, EN 61000-3-2:2014, EN 61000-3-3:2013, EN 63000:2018. IEC 62638-1:2014, IEC 62638-1:2020, BS EN 60825-1:2014, IEC 60825-2:2010, FCC: 47 CFR, Part 15, FDA: 21 CFR, Part J	
Dimensions	Standard 19" rack mount (3U height)	

## Network Integration

Toshiba's 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.



## TOSHIBA