Toshiba Solutions for Quantum-Safe Communications

TOSHIBA

June 2025

Shin Takashima
Toshiba Europe Ltd

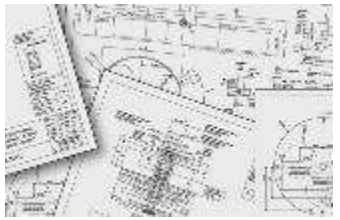
Confidential

Long-term Information Security

Many types of information must stay **confidential for several years**…

Financial


Medical


Corporate


Critical Infrastructure

- However, long-term confidentiality is threatened by **harvest and decrypt** attacks
- It is **easy to collect and store encrypted data**
- Decrypt later when more **powerful computers** are available


IBM researchers have already installed the mounting hardware for a jumbo cryostat big enough to hold a quantum computer with 1 million qubits. CONNIE ZHOU/IBM

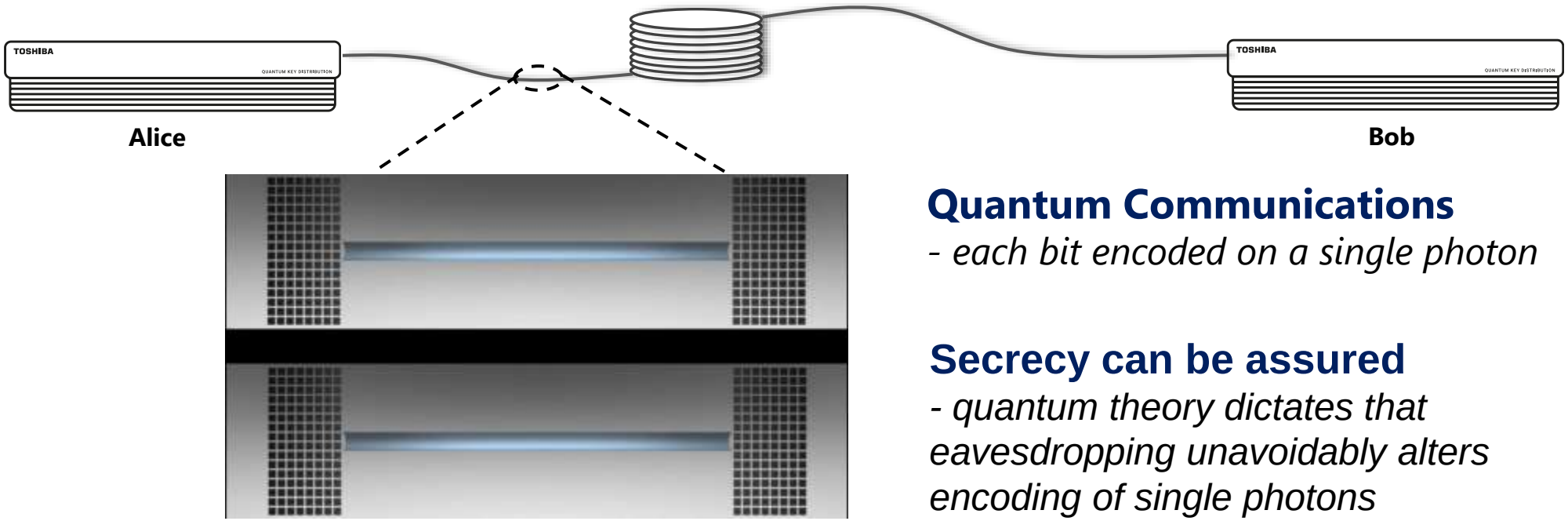
IBM promises 1000-qubit quantum computer—a milestone—by 2023

By Adrian Cho | Sep. 15, 2020 , 5:45 PM

https://www.science.org/content/article/ibm-promises-1000-qubit-quantum-computer-milestone-2023

New techniques needed <u>today</u> for long-term data confidentiality

Quantum Key Distribution (QKD)



Quantum Communications

- each bit encoded on a single photon

Secrecy can be assured

- quantum theory dictates that eavesdropping unavoidably alters encoding of single photons

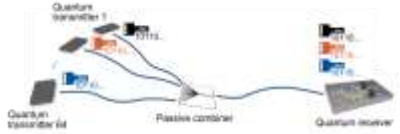
Distribute secret keys which are secure from all future advances in cryptanalysis, computing and quantum computing

Toshiba's Contribution to Quantum Communications

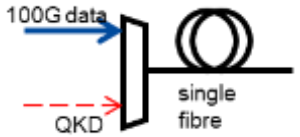
Technology Development

QKD 100km

QKD >1 Mb/s

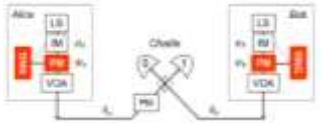


Quantum Access Network



QKD multiplexing

QKD > 10 Mb/s



TF-QKD (>600km)

Chip QKD

Fast Satellite QKD

QKD system commercialisation

2002 2010 2014 2016 2018 2020 2022 2024

QKD network
SECOQC
Vienna, 2004-08

GHz QKD network
Tokyo, 2010-15

Multiplexed QKD Trial
QCommHub,
Cambridge, 2015-20

QKD testbeds in 6 cities
& use case development,
OpenQKD, 2019-23

Supplier to EuroQCI
consortia, 2023-

Commercial QKD
services trial with BT,
London, 2022-

Technology Validation

Confidential

Toshiba QKD: Value through Technology

- **Leading technology providing better business outcomes today**
  - **Highest optical loss budget** (30 dB) for robust deployments
  - **Highest key rates** (300 kbit/s @ 10 dB) for maximum network capacity
  - **Multiplexing** capability to reduce deployment costs
  - **High reliability & stability** due to patented active stabilization technology

- **Pipeline of new technologies to fully exploit potential of quantum**
  - National networks: **Long distance QKD & Twin-Field QKD**
  - Continental networks: **Satellite Quantum Comms**
  - Scalability: **QComm on a chip**
  - Quantum internet**: Entanglement & Quantum Repeater**

Commercial QKD systems

- Long Distance C-band system
- Multiplexed O-band system
- Flexible C-band system

High secure key rates

Long range

QKD deployed over a single fibre strand or a fibre pair

Co-existence with multiple channel, high power classical DWDM data services

In-line multiplexing for ease of deployment

Auto set-up and alignment

Integrated key delivery system

Flexible system offers user selectable wavelengths

ETSI standardised interface

Security parameter < 10^{-10}

Recent Quantum Safe Network Deployments

Implemented PoC for financial blockchain with US-based **J.P. Morgan Chase & Co.** (Feb 2022)

Quebec Quantum Network Project with **Numana** (Aug 2023)

Environment & Smart Grid testing– **Oak Ridge National Labs** (Aug 2022)

Jointly constructed a quantum test bed with the US Quantum Technology Community **CQE** (Apr 2022)

CHICAGO QUANTUM EXCHANGE

Continuing trial with US-based **Verizon** (since sept 2020)

QKD trial in smart manufacturing with **NCC**, **CFMS** and **BT** (Oct 2020)

Orange France

- Evaluation of QKD & classical co-existence (Jun 2023)
- Evaluation of QKD in multi link, trusted node architecture (Feb 2024)

European testbeds, via **OpenQKD** (since 2019)

- Quantum safe 5G -**Germany**
- DC/DC QKD - **Poland**
- QKD on railway fibre - **Czechia**
- QKD & SDN - **Spain**
- Securing medical data - **Austria**

Launched the world ‘s first commercial quantum-secured metro network trial in London with **BT** (Launched in April 2022)

Supplier to multiple quantum secured networks as part of **EuroQCI**

Tokyo metro QKD network (2023)

QKD & PQC OTN with **NTT** (Nov 2021)

IPsec QKD VPN, **Softbank** (Sept 2023)
QKD & Optical wireless, **Softbank** (Mar 2024)

Toshiba and **KT** demonstrate hybrid quantum secure communications with South Korea’s **Shinhan bank** (April 2024)

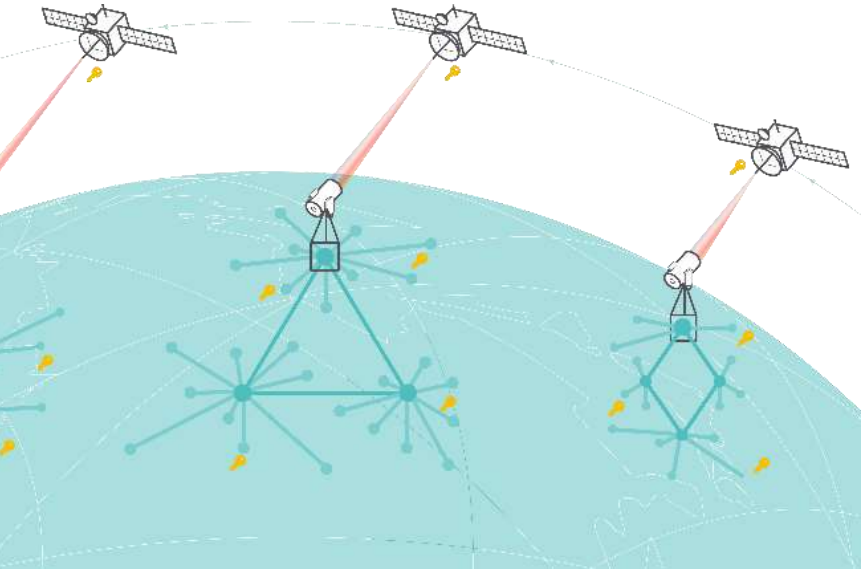
Partnership with **SpeQtral** and **SPTel** to build Singapore’s NQSN+ Nationwide Quantum Safe Network (since August 2021)

Recent Quantum Safe Network Deployments

Orange Business and Toshiba partner to launch first commercial quantum-safe network service in France

- Orange Quantum Defender is provided over the existing Orange commercial fibre network in Paris using Toshiba's QKD technology.
- A defence-in-depth principle combines hardware-based QKD and software-based PQC technologies to both protect sensitive data and ensure future data secrecy.
- The combination of QKD and PQC means organisations can benefit from a multi-layered security approach, providing the most secure network possible.

Toshiba Roadmap for Quantum Networking



Qu. Computing Networks
Remote (quantum secure) access
to quantum computer
Distributed quantum computing

Entanglement Networks

Global QSN

National QSN

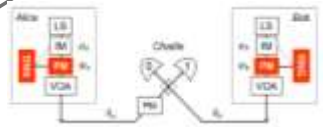
Metro QSN

2024 — 2025 — 2027 — 2030 — 2040

Scalable Quantum Repeater

Quantum Repeater

Quantum Memory



Twin Field QKD

Satellite QKD

Multi-Photon Entanglement

Chip QKD

Entangled Pair Source

Platform for future quantum computing and communications

TOSHIBA