HOKKAIDO UNIVERSITY

9th ETSI/IQC Quantum Safe Cryptography Event

Feb. 14, 2023

Research and Development Activities for Quantum Secure Cloud in Japan

Akihisa Tomita

Quantum Technology and Innovation Strategy

○**Quantum technology is an important fundamental technology** in terms of industry and security as well as brings drastic changes to economy and society.

○**To achieve "quantum technology and innovation"** as soon as possible, Japan promotes R&D, industrialization and commercialization of key technologies with taking own advantage

Ⅰ Priority areas

Accelerate an achievement of innovation

✓**Set "Key Technology Areas" & "Integrated Quantum Innovation Areas" for priority support and investments**

(e.g. Gate-based quantum computer, Solid-state quantum sensor, Link Technologies for Quantum Communication and Cryptography, Quantum AI technology)

✓**Create "Technology Roadmap" & "Integrated Area Roadmap"**

Ⅱ Quantum hubs

Make a face-to-face communication

✓**Establish international "Quantum technology Innovation Hubs"**

(e.g. Quantum software hub, Quantum inertial sensor hub)

✓**Hub conducts basic research, demonstration and HR development**

Ⅲ International collaboration

Collaboration with US & EU for industry and security

✓**Early development of multilateral/bilateral cooperative frameworks**

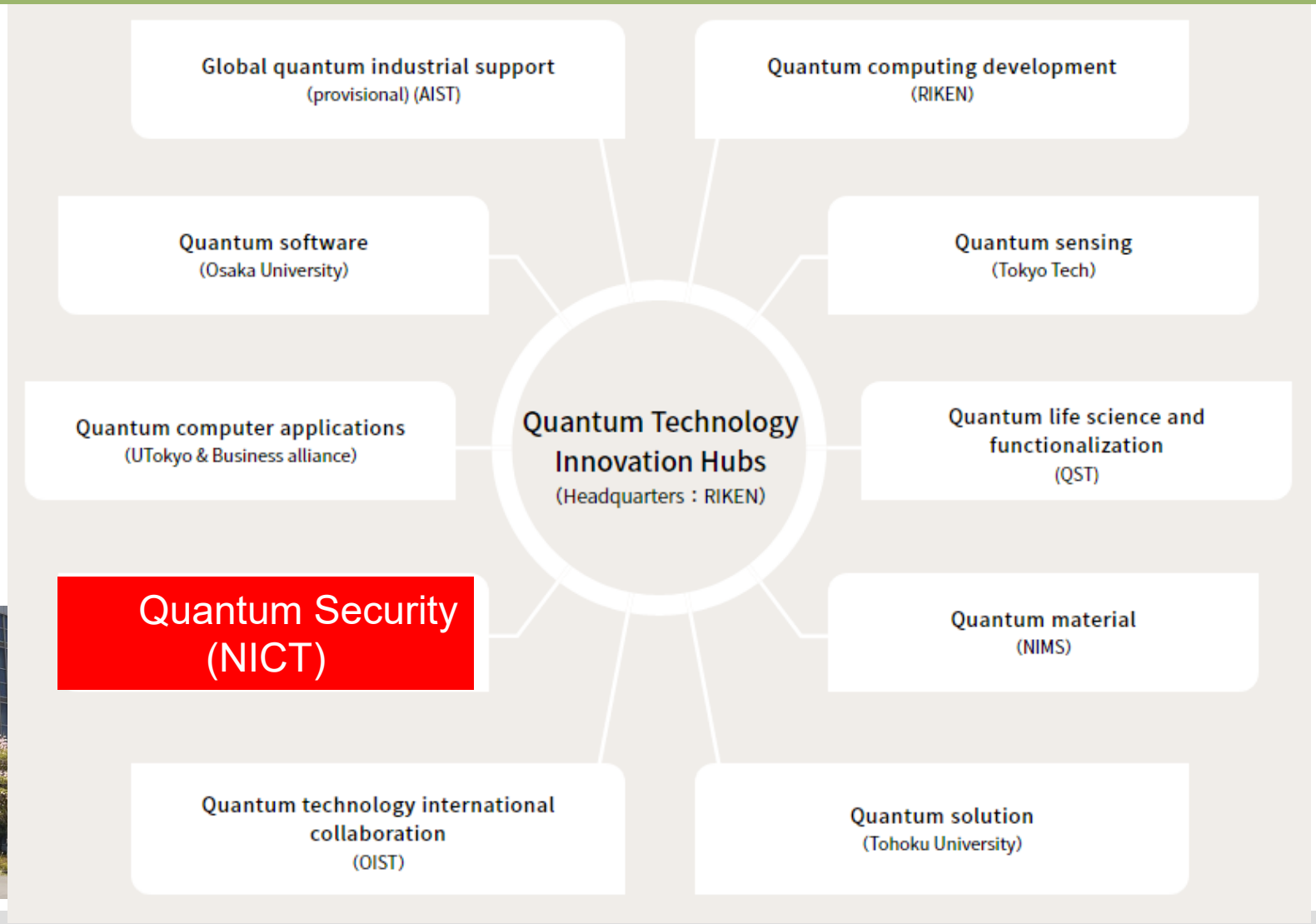
(e.g. Japan-US-EU multilateral symposium in December 2019)

✓**Ensure and strengthen security trade control**

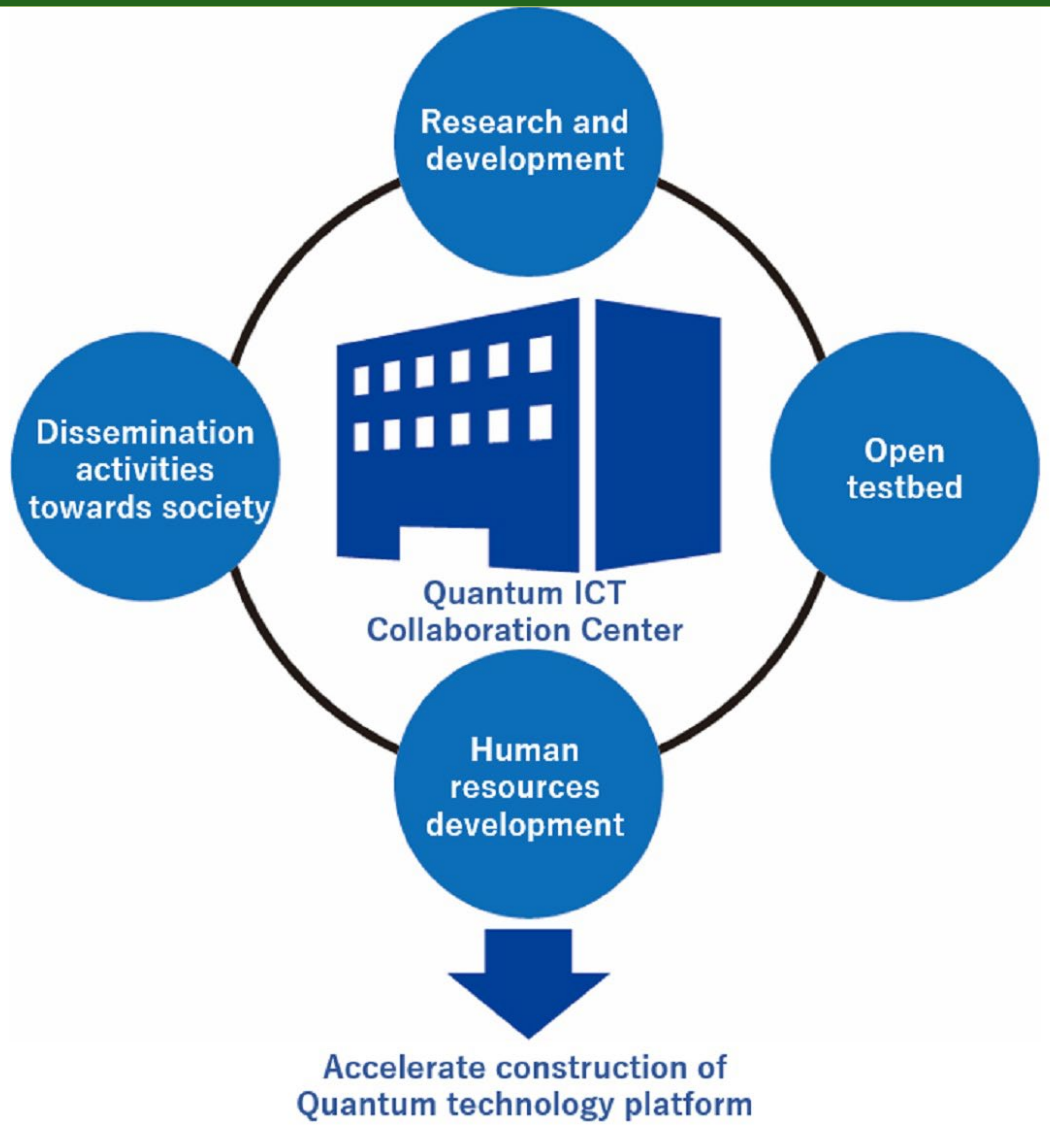
Five pillars towards an achievement of quantum technology and innovation

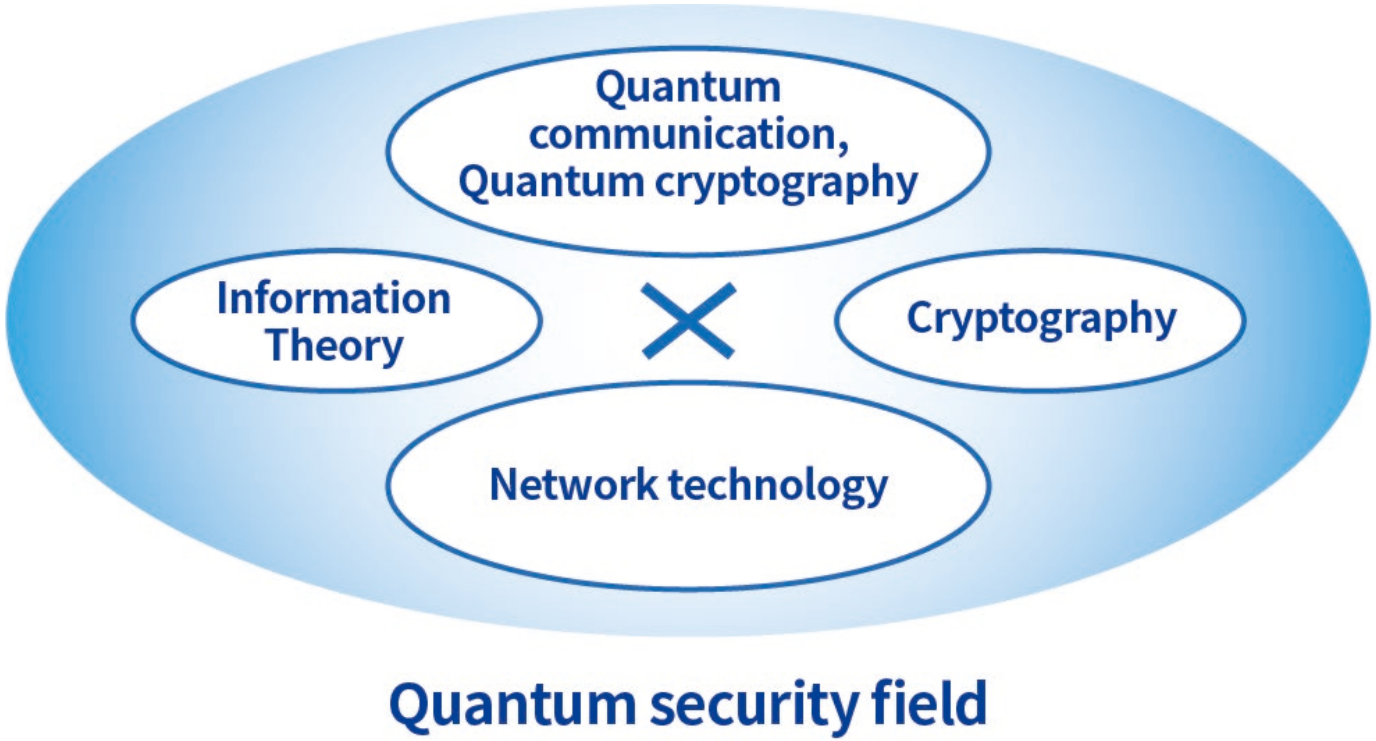
(1) Technology development	(2) International collaboration	(3) Industrialization and innovation	(4) Intellectual property and international standardization	(5) Human resource development

Quantum Technology Innovation Hubs



Quantum ICT Collaboration Center (NICT)





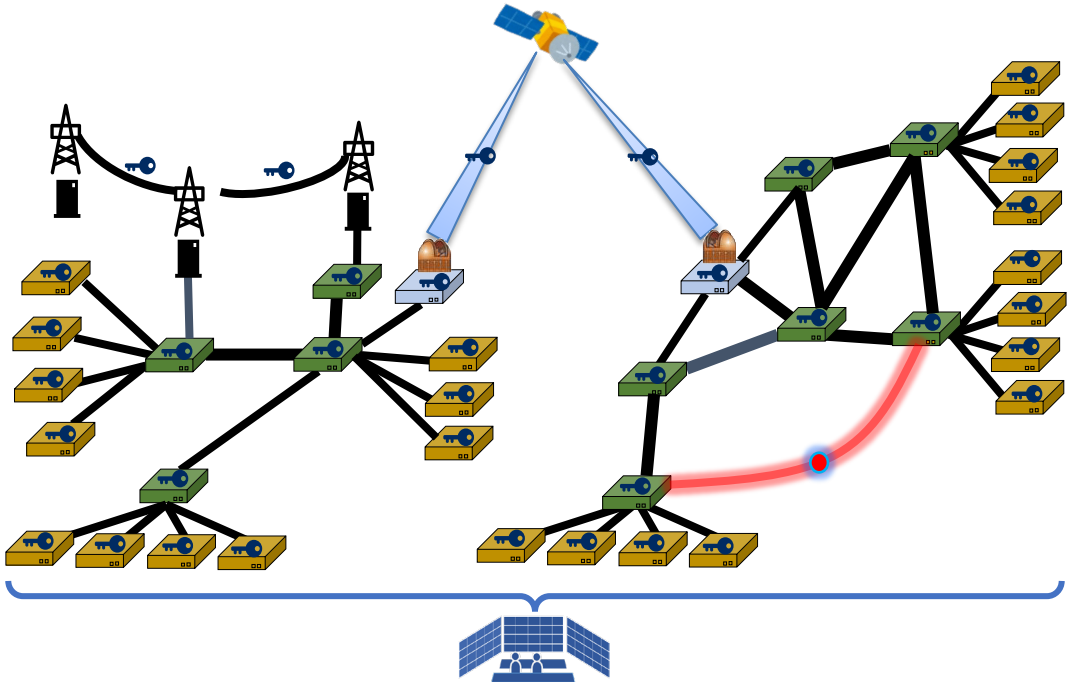
National R&D projects on Quantum Security

SIP 戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

- Photonics and Quantum Technology for Society 5.0 (FY2018-2022)

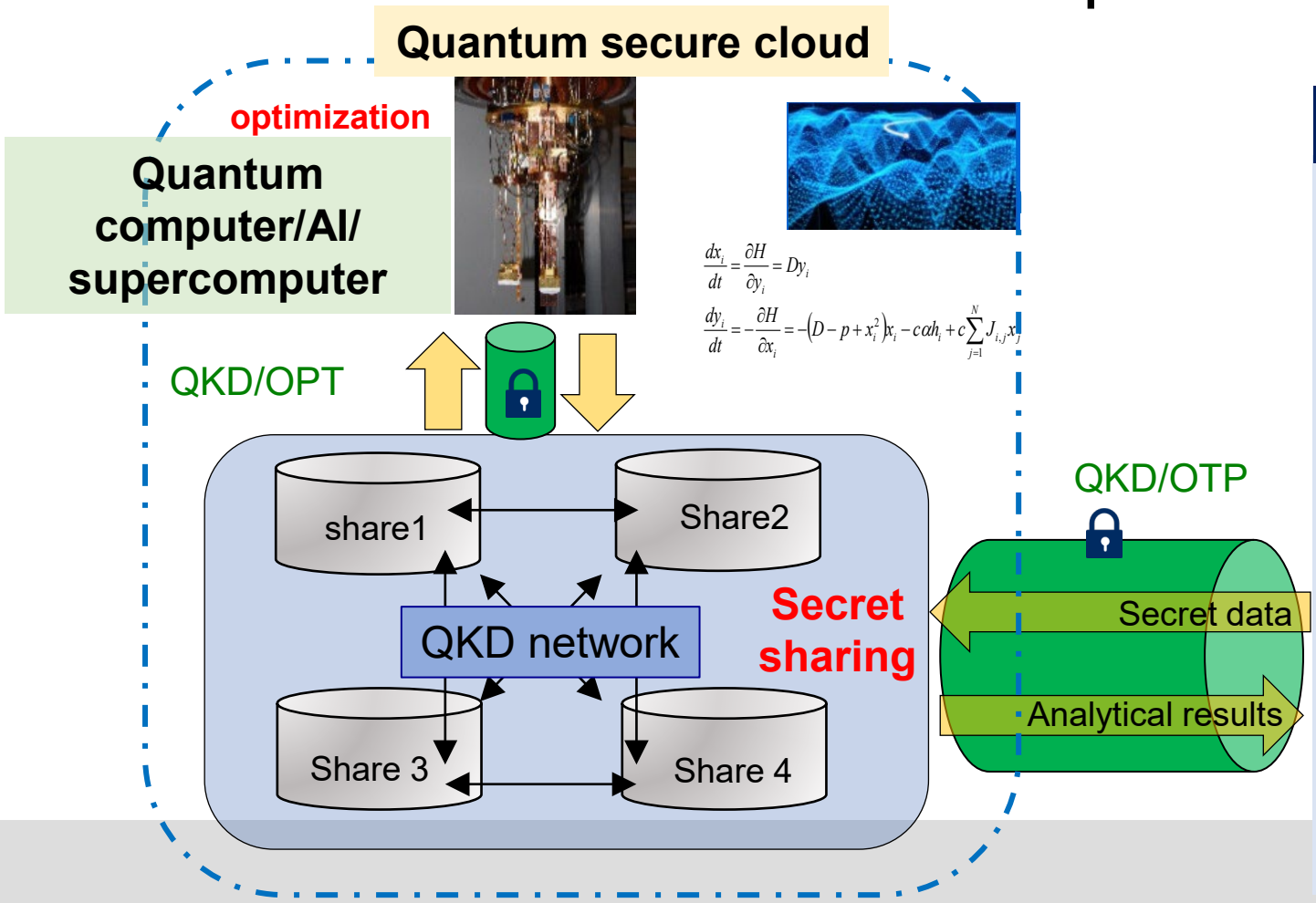
Ministry of Internal Affairs and Communications, JAPAN

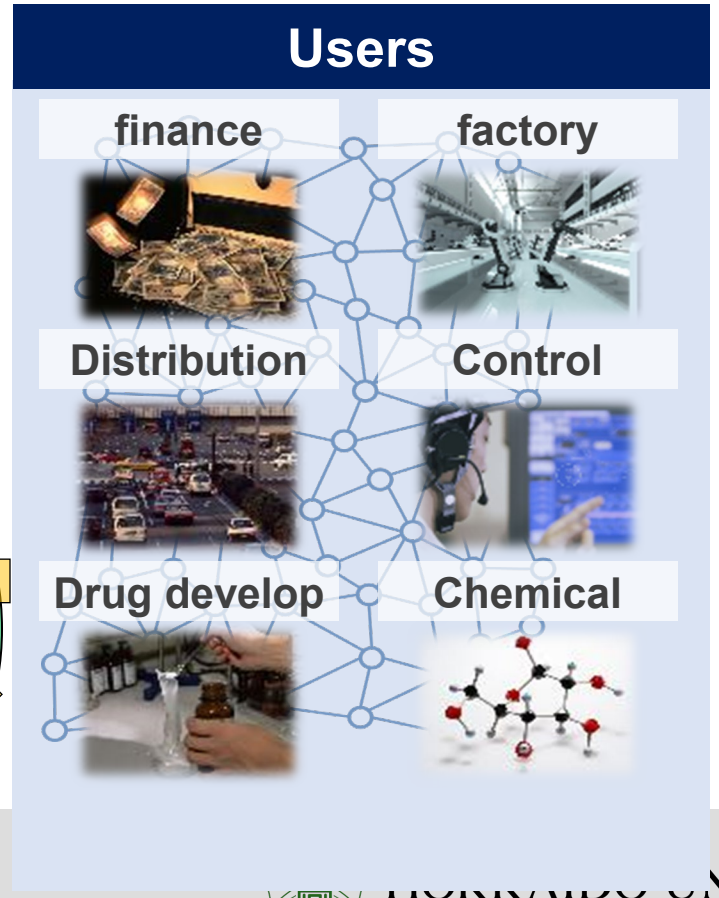
- R&D for Construction of a Global Quantum Cryptography Network (FY2020-2024)
- R&D of satellite quantum cryptography technology for building a global quantum cryptography communications network (FY2021-2025)



Quantum secure cloud

Future vision of a quantum secure cloud with secure computation function.
Several specialized computers (including quantum computers)
are embedded in the quantum secure cloud.





NICT National Institute of Information and Communications Technology

HOKKAIDO UNIVERSITY

Value brought by QKD

<QKD>		<Conventional>
Long term Security	⇔	Compromise and Generation change
Light and Secure	⇔	Secure but Complex

- Secure communication between devices with **limited CPU power**
- Low latency communication in 5G, B5G

Information theoretically secure Message Authentication

- Shorter key（~log (M)) than for secure data transmission
- Critical infrastructure

No update required

- Deprecated or compromised cryptographic suits are still used

Can we make value > cost?

Overview of the POC projects

National Institute of Information and Communications Technology

(1)e-Medical Record
Confidential transmission with symmetric key crypt.
Medical data storage with Secret Sharing

Kochi Medical

Sendai

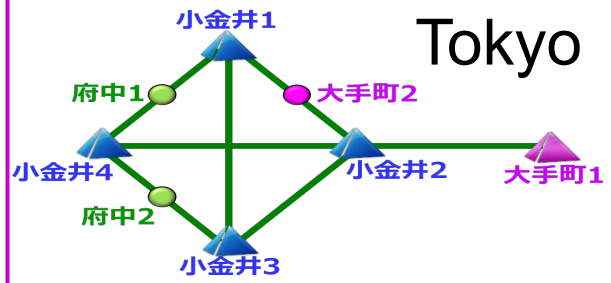
(2) Genome data
transmission,
Secret Sharing

Osaka

Nagoya

(3) Smart manufacture

Tokyo



(1) e-Medical Record
(4) Biometric data
(5) Financial data

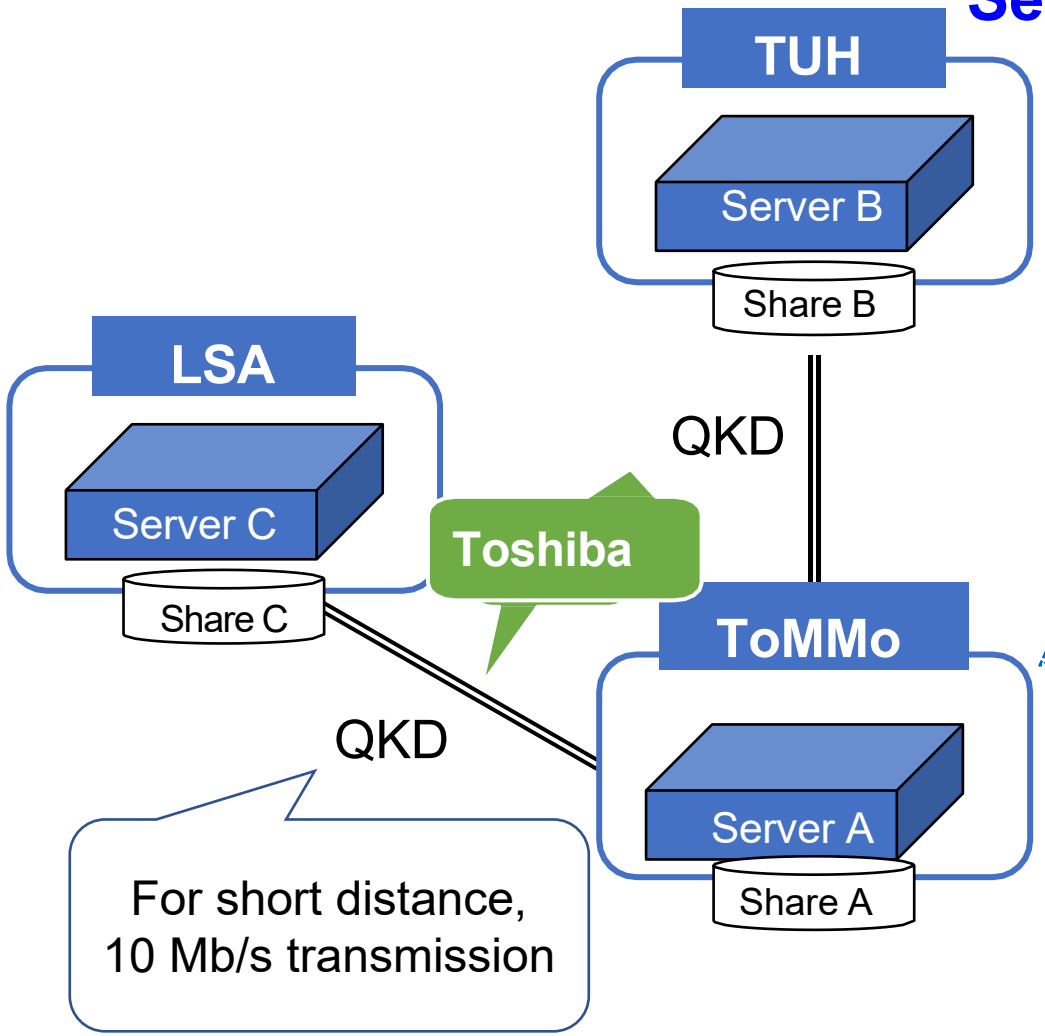
HOKKAIDO UNIVERSITY

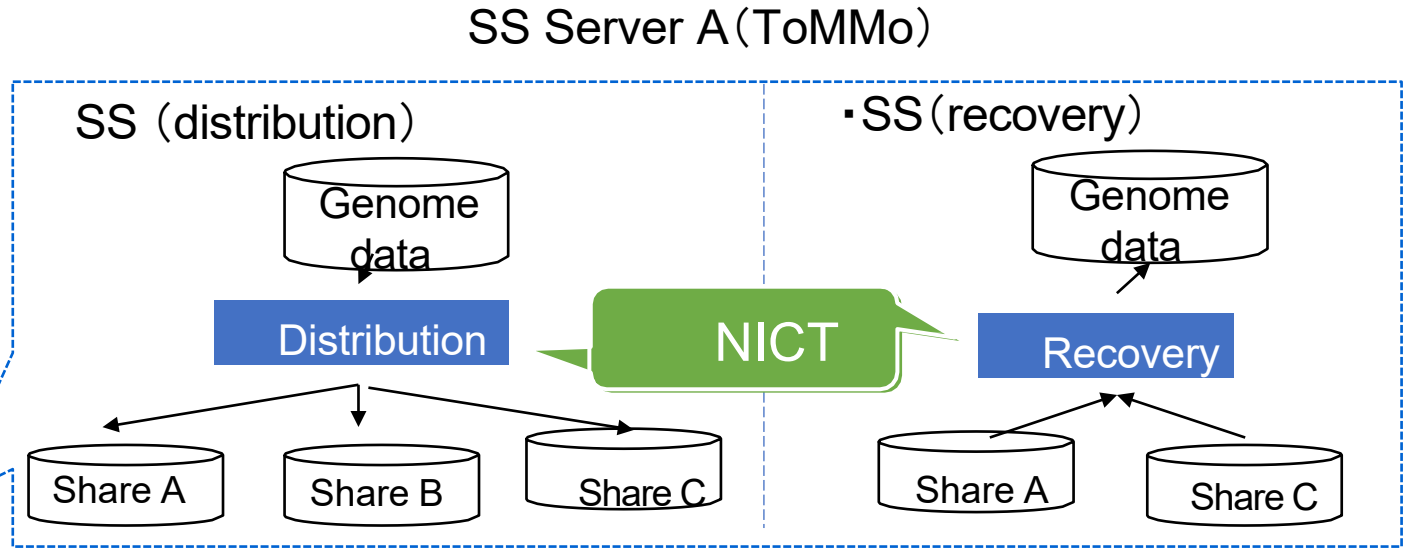
Genome Medical Application

Long term security
Light & secure

Secure transmission and secret sharing (SS)

80 GB data were distributed to 3 servers in a few hours

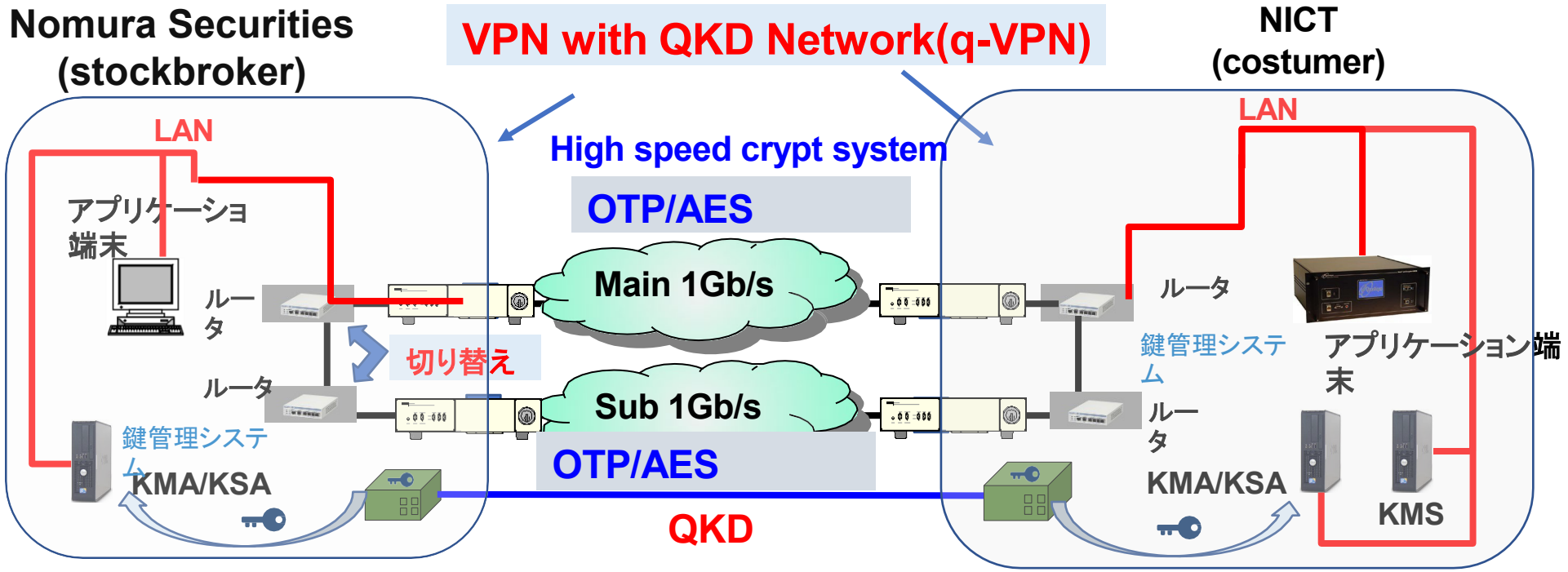




LSA：Toshiba Life Science Analysis Center
ToMMo：Tohoku U. Tohoku Medical Megabank Organization
TUH：Tohoku U. Hospital

Confidential transmission of Financial data

Long term security
Light & secure



Nomura: Financial Application
Toshiba: QKD system
NEC: High speed crypt system
NICT: High speed OTP system

- QKD key rate: 100k~300kbps
- **Stored key/day: 3.2GB**
- **Transmitted data/day: 4.2GB**
- **One Time Pad / AES (when key is short)**
- **Switching Main/Sub in 200ms**
- **4.2GB/day data transmission for one week**

Stored key was used

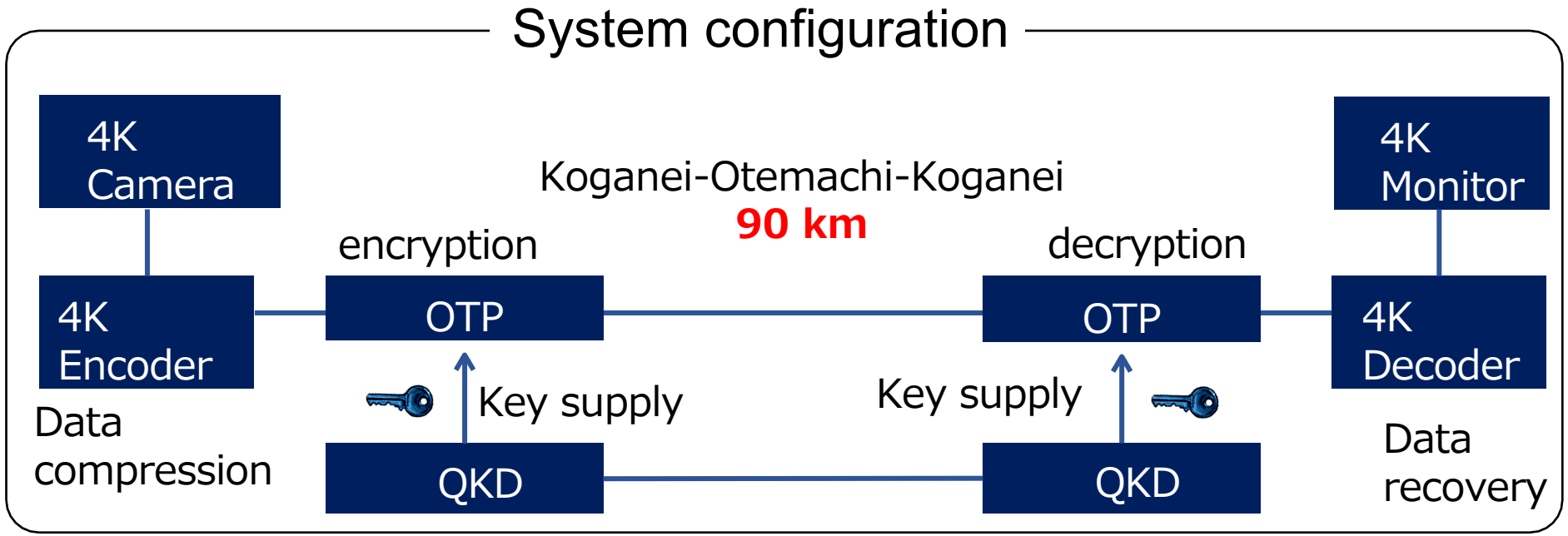
Low latency demonstration

(Long term security)
Light & secure

4K-resolution video data transmission with QKD＋OTP

- Confidential data transmission **at 1Gb/s with OTP over 90 km** installed fiber link

Stored key was used



Feasible for remote diagnosis and surgery

NICT National Institute of Information and Communications Technology

Future Research Directions of QKD

More

- *Higher Performances*
- *Implementation Security Certification, Standardization*
- *Reliability*

MORE THAN

- *Networking*
- *Quantum-Classical Integration*

BEYOND

- *Quantum Repeater ~ Quantum Internet*
- *Quantum Cryptography Other than QKD*
- *Cryptographic Protocols beyond Quantum*

Funding and Collaboration

SIP

科学研究費助成事業
Grants-in-Aid for Scientific Research
科研費 KAKENHI
(学術研究助成基金助成金／科学研究費補助金)

総務省
MIC Ministry of Internal Affairs and Communications

光・量子を活用したSociety5.0実現化技術
Photonics and Quantum Technology for Society 5.0

NICT National Institute of Information and Communications Technology
TOSHIBA
NEC
学習院大学 GAKUSHUIN UNIVERSITY
東京大学 THE UNIVERSITY OF TOKYO
ZENMU TECH