Tokyo QKD Network

## and its application to distributed storage network

National Institute of Information and Communications Technology (NICT)

Masahiro Takeoka

1

Quantum Key Distribution

- New add-on security service by providing cryptographic keys to the conventional communication network
- QKD keys provide "information-theoretic security (IT-sec)" -> unbreakable by *any* computational decryption attack (even with quantum computers)

<Conventional network and QKD network>

Application network (conventional network)

(3)

(2)

QKD network

QKD

(1)
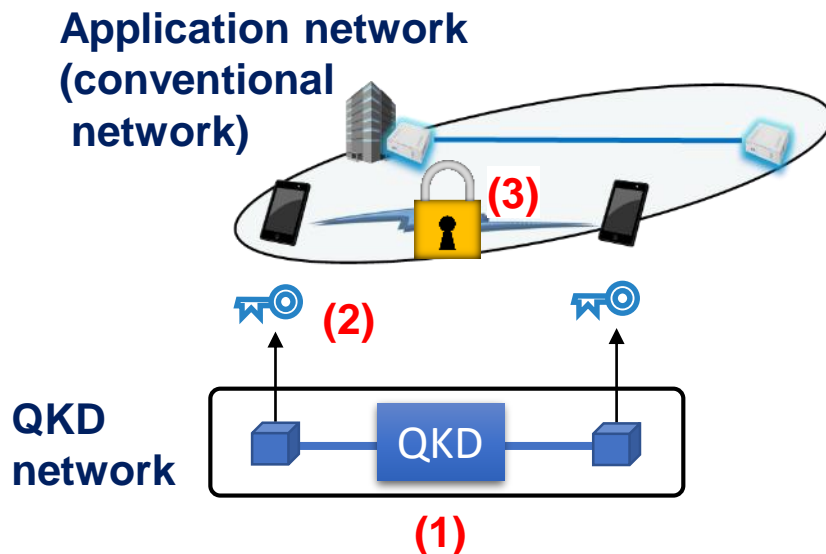
(1) QKD network shares IT-sec keys between distant parties

(2) IT-sec Keys are provided to applications

(3) Data is protected by the ITS keys

Basic features of QKD

- It protects security of data transmission
- It works in a point-to-point link, not in a multi-party link
- Speed and distance of a direct link are limited

 1M bits/s at 50km (Movie data, e.g. MPEG4)
  10k bits/s at 100km (Voice data)
  (for standard optical fiber with loss rate of 0.2dB/km)

- Networking is made by introducing the trusted nodes,
  and by relaying a key via the nodes

- QKD is vulnerable to Denial of Service attack.
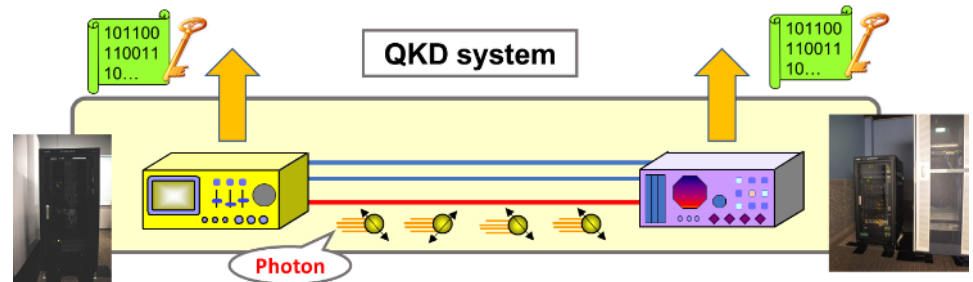 A rerouting mechanism over a network is essential.

QKD network (current)

consists of point-to-point QKD links and trusted nodes

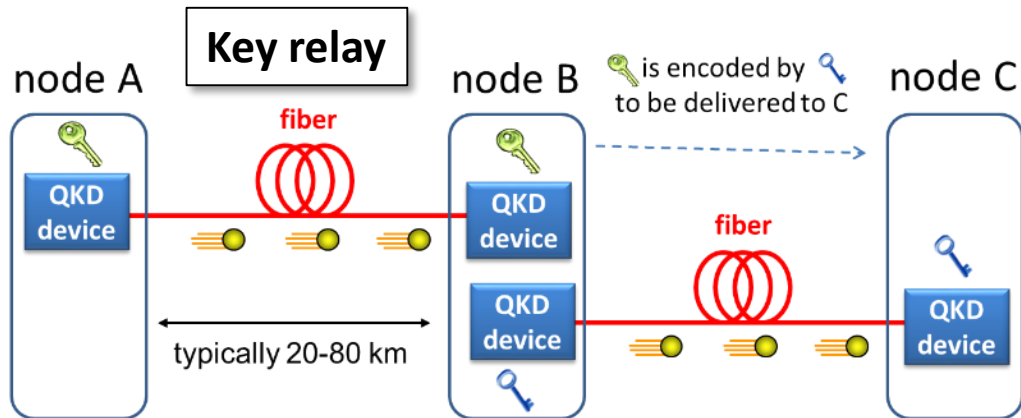QKD network

QKD link (QKD system)
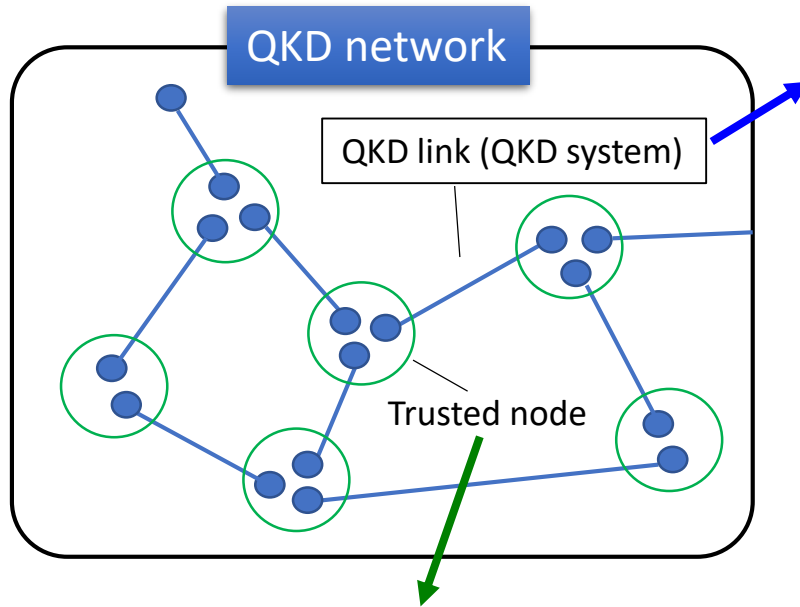
Trusted node

QKD link: deliver IT-sec keys p-to-p

Consists of quantum channel (sending photons) and classical channels (sync. & key distillation)

Trusted node: protected node to relay IT-sec keys

node A   Key relay   node B   🔑 is encoded by 🔑 to be delivered to C   node C

fiber

QKD device

typically 20-80 km

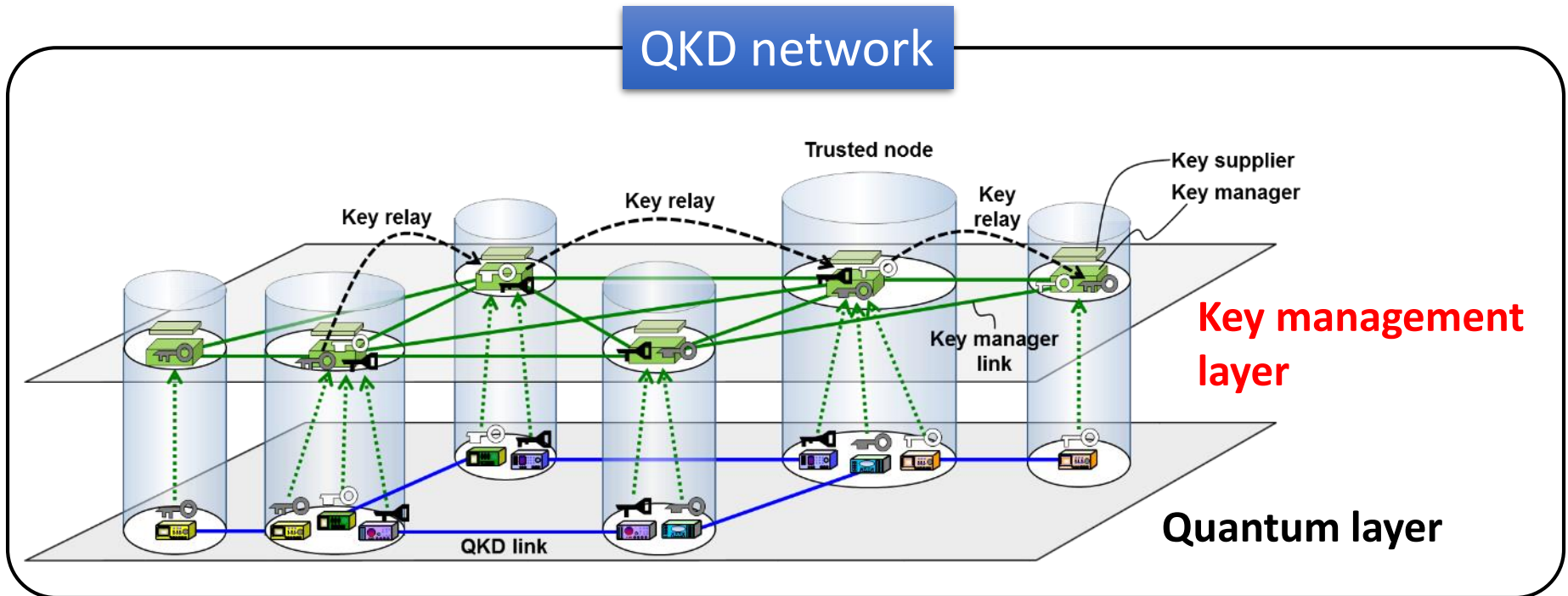QKD device

QKD device

fiber

QKD device

Why networking?

1. P-to-P QKD link distance is fundamentally limited by the photon loss (usually < 100km)

2. Network redundancy for stable operation (rerouting)

Key (relay) management

- QKD network should have a key management layer (KML)

KML: logical links (not quantum channels) managing the key relay and key supply to the conventional network (applications)
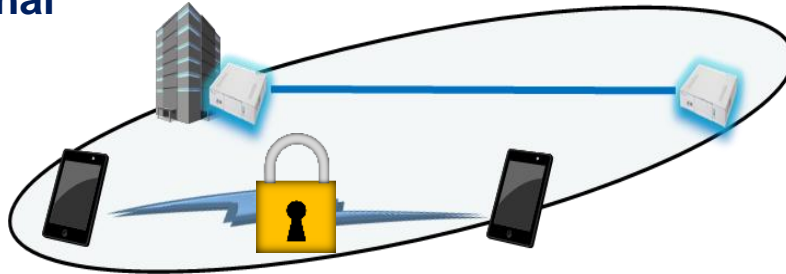

QKD network

Trusted node

Key relay

Key relay

Key relay

Key supplier
Key manager

Key manager link

Key management layer

Key relay

QKD link

Quantum layer

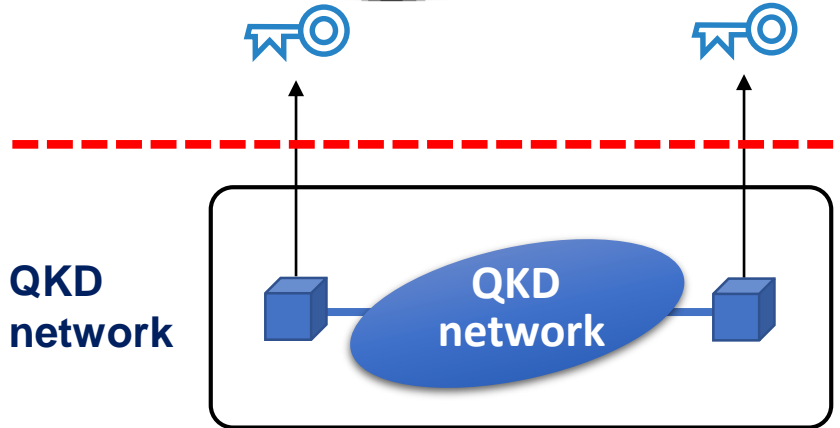The QKD operator is responsible for the secure operation of both the KML and the quantum layer

5

QKD operation/security demarcation

- It is important to clarify the security responsibility demarcation between the conventional network and the QKD network

Application network (conventional network)

Conventional network operator
Service provider

Responsibility demarcation point

QKD network

QKD network operator
Key delivery service operator

Tokyo QKD Network

Tokyo QKD Network

- QKD field testbed network on JGN-X in Tokyo, Japan

M. Sasaki et al.,
Opt. Express 19, 10387 (2011)

  - QKD links are connected via the trusted nodes
  - JGN: open testbed fiber network provided by NICT

- Constructed in 2010
  (World first TV conf. demonstration
    at UQCC2010)

In part of NICT open test bed network
"Japan Giga Bit Network"

- 4 companies
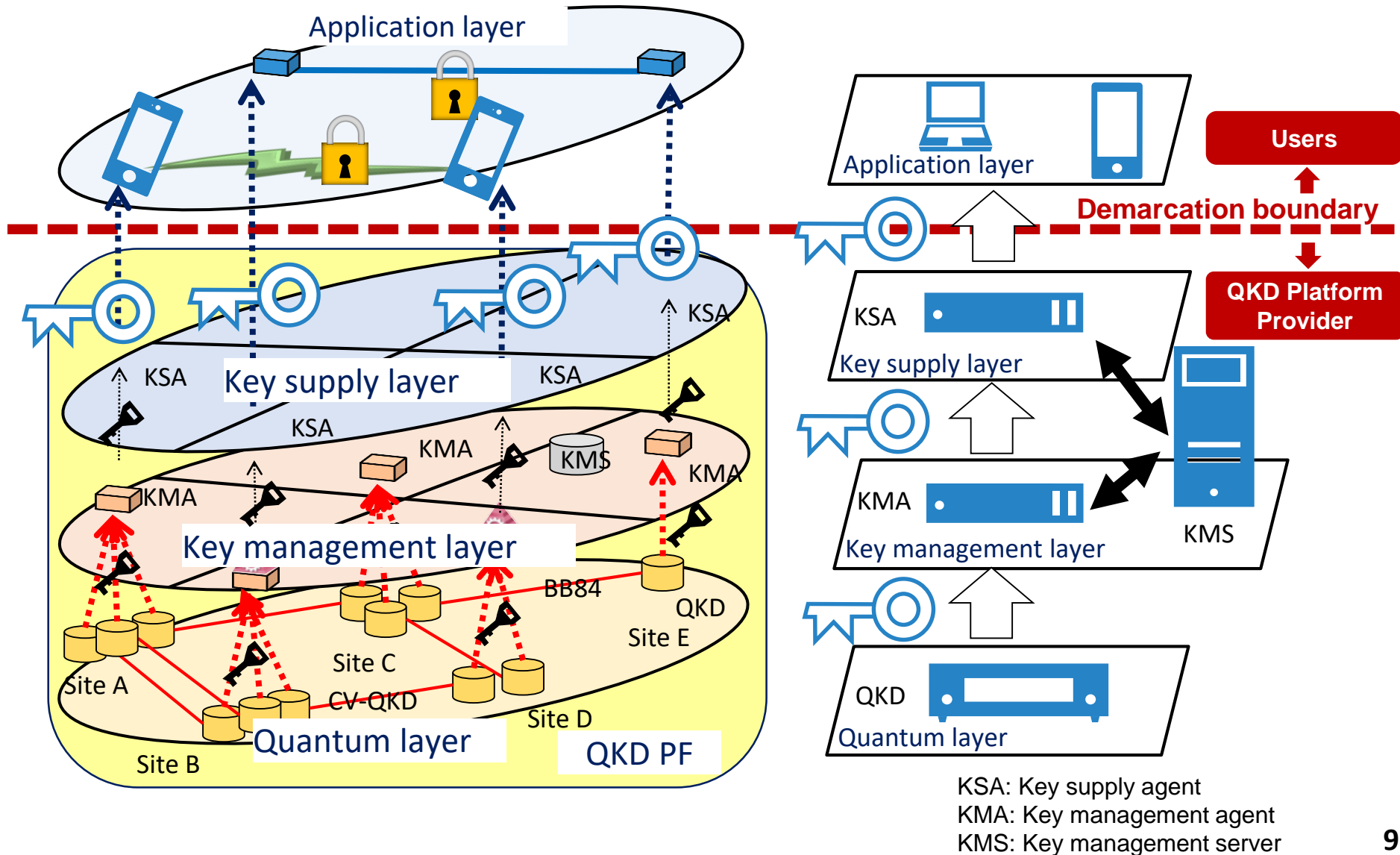 (NEC, Toshiba, MELCO, NTT),
  8 universities,
  2 national institutes

- Continuously operated for
  long-term field tests, network
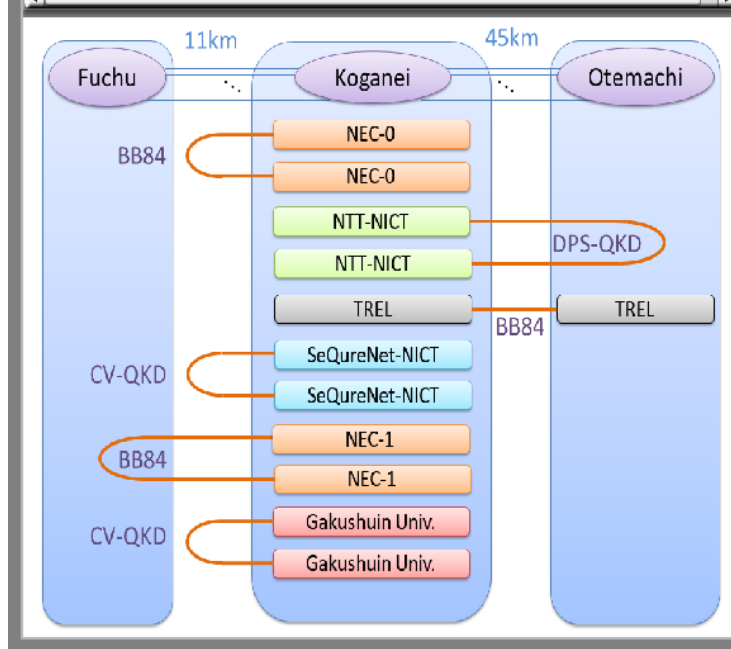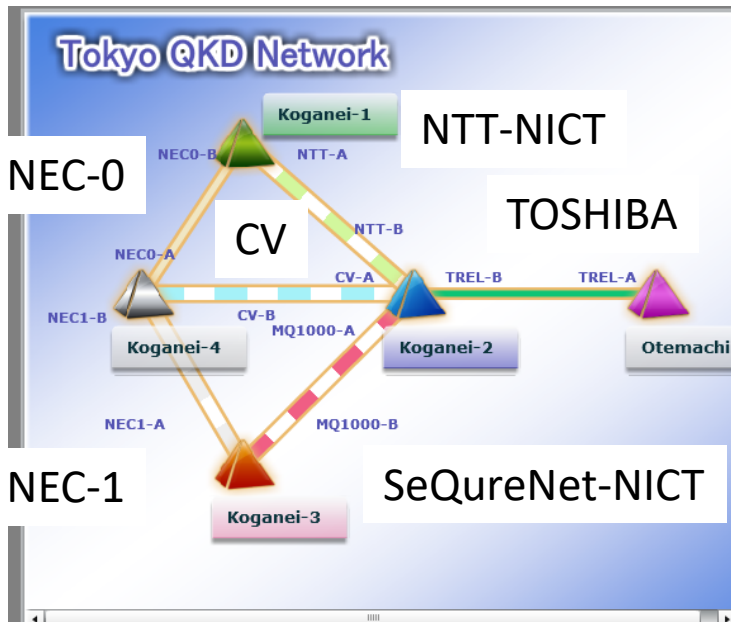 experiments, and application
  developments
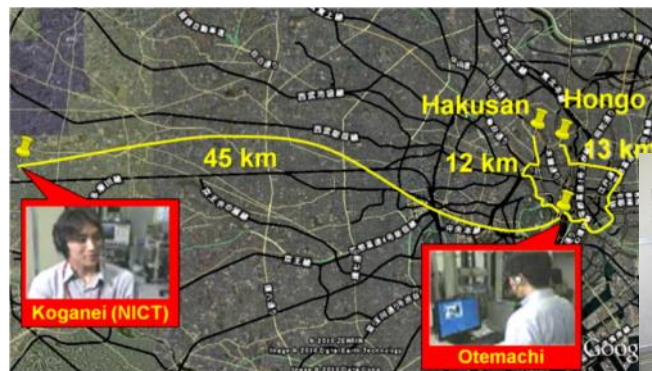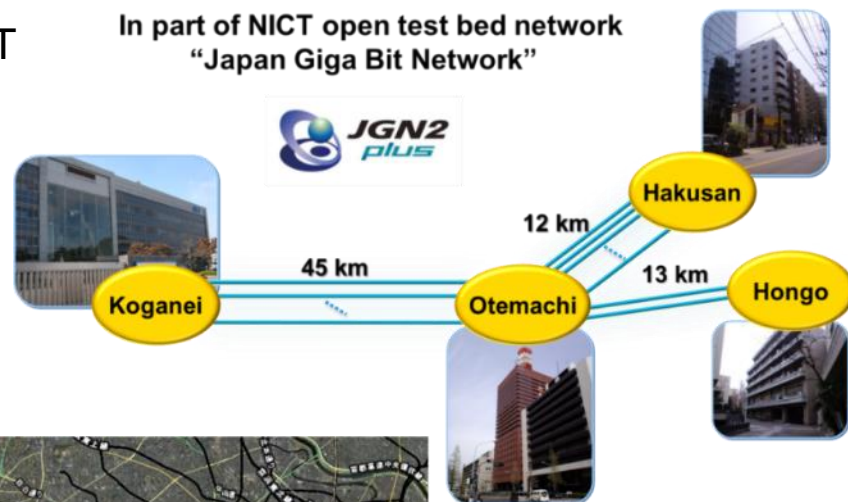
QKD sender and receiver (NEC, 2017)

http://www.uqcc.org/   http://www.tokyoqkd.jp/

8

Tokyo QKD Network Architecture

✓ **A demarcation boundary between a QKD platform provider (an ITS key provider) and users should be clearly defined.**

KSA: Key supply agent
KMA: Key management agent
KMS: Key management server

9

http://www.tokyoqkd.jp/

Application
(LINCOS)

Security lifetime

- QKD keys provide "information-theoretic security (IT-sec)"

  -> unbreakable by *any* computational decryption attack
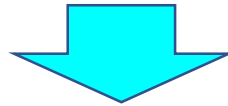
Long-term security

⇔ computational security for public key cryptos

→ Risk that it will be broken
  by *future* computing/algorithm technologies

Long-term security

t_0

Archive critical data

Time

t

Restore

$t - t_0 >$ centuries

Data in transit 🔒

Data at rest 🔒

Store now, decrypt later attack

- Disaster
- System fault
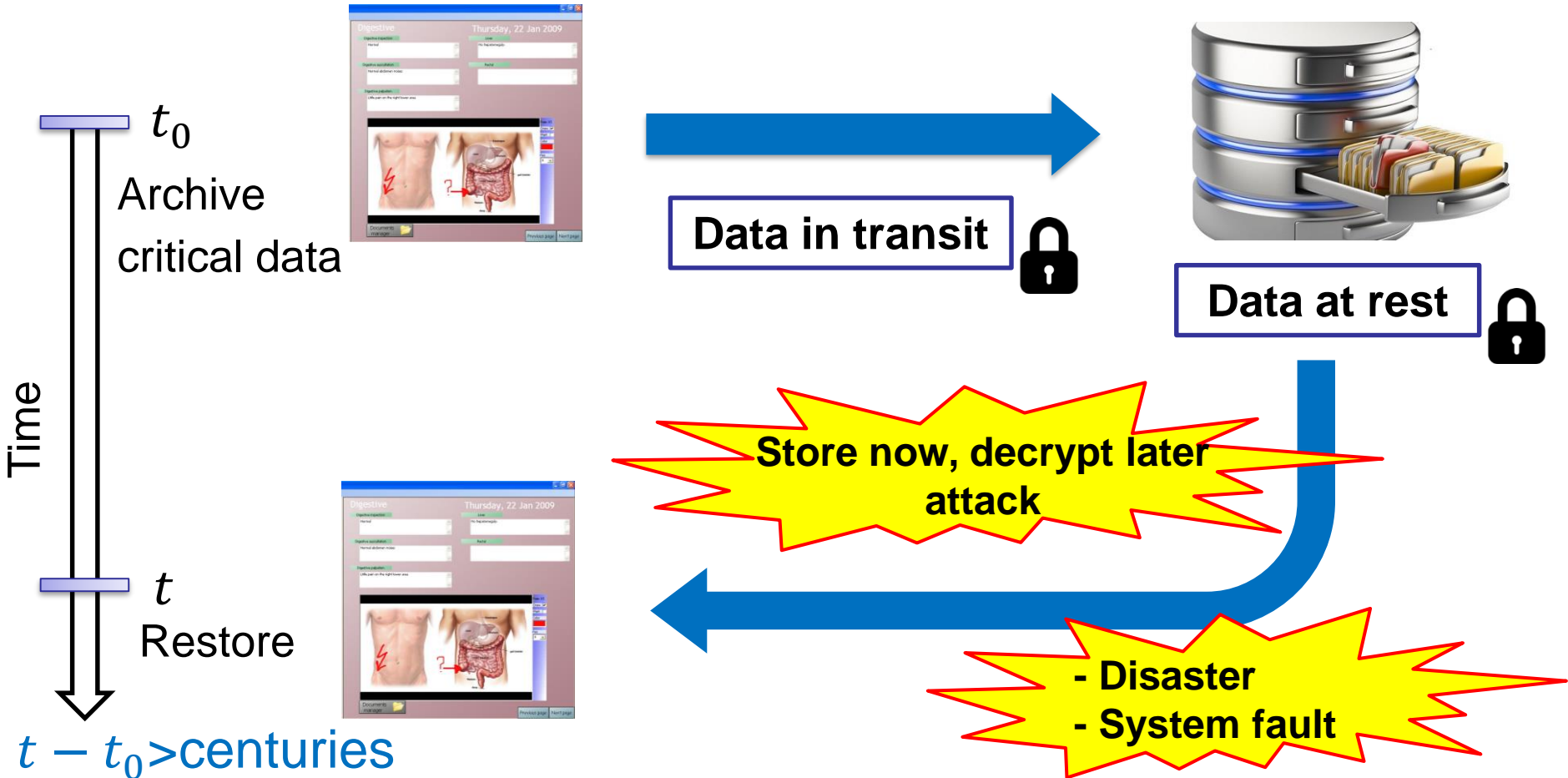
(1) Confidentiality

No information leak on the data in transit and at rest.

(2) Integrity

The data existed at time t_0 and has not been changed since.

13

Requirements for long-term security system

Requirement	Meaning	Solution
(i) Confidentiality	The data should be accessible only to authorized parties.	- **Information theoretically secure** storage and communication - Secure **access control**
(ii) Integrity	The data should remain unaltered.	Signature and authentication with **prolongable validity**
(iii) Availability	The data should be available whenever required.	**Redundant** data backup
(iv) Functionality	The data can be processed without decryption.	(Fully) **homomorphic** encryption

So far, partial solutions have been developed and used,
    i.e., long-term confidentiality only, or long-term integrity only.
However,
    no comprehensive solution has been demonstrated yet.

Long-term integrity, authenticity, and confidentiality protection system "LINCOS"

TU Darmstadt - NICT,
J. Braun et al., Proc. ACM Asia CCS2017, pp. 461-468.; ePrint 2016/742

Distributed storage network

Integrity protection system
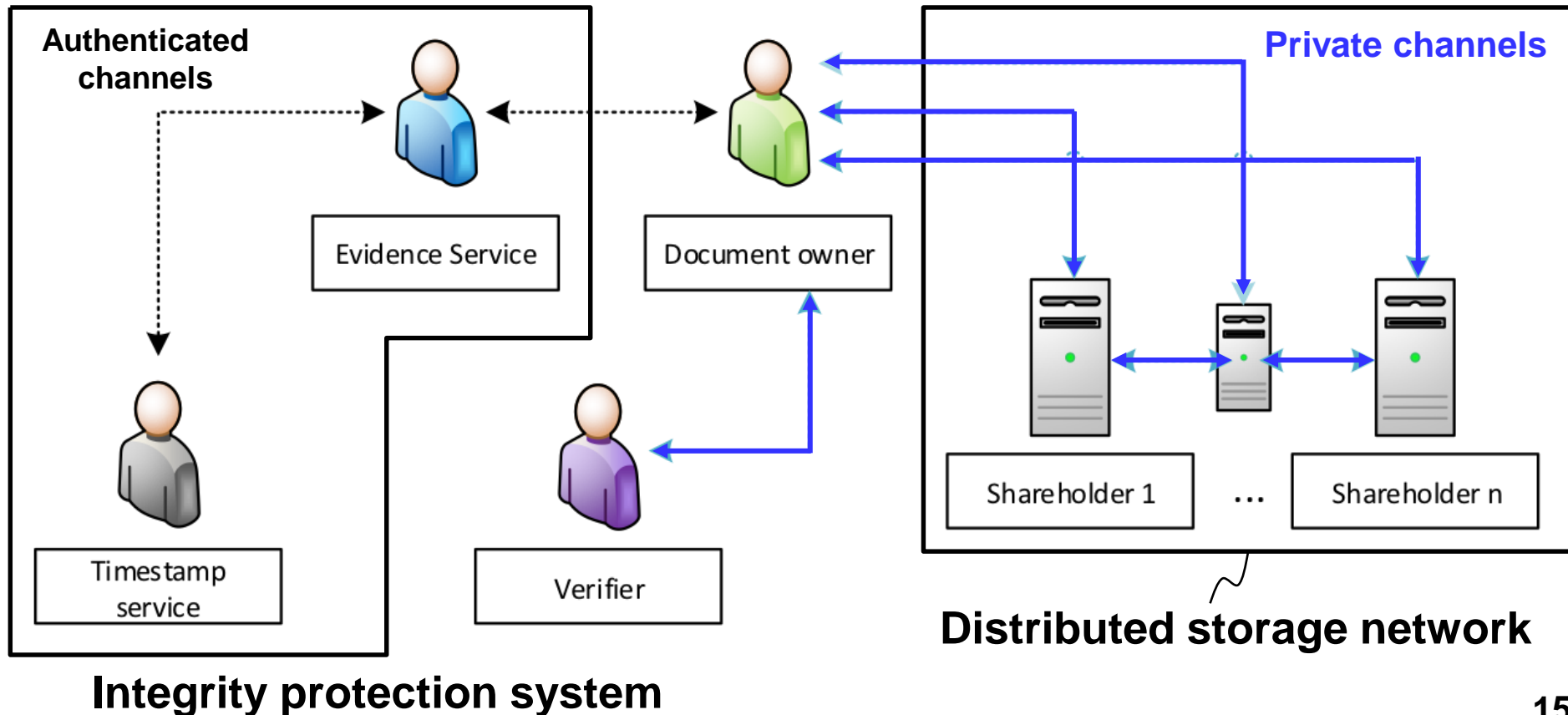
Basic components for LINCOS

1. **Information theoretic** confidentiality of storage
3. **Availability (redundant data backup)**
4. **Functionality (Multi-party secret computing)**

(1) Secret sharing

Share 2

Original data
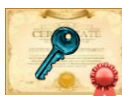
Share 1

Share 3

(3) Time-stamp chains of signature

(2) QKD + OTP

Share 4

2. **Computational but prolongable** integrity

1. **Information theoretic** confidentiality of data link

QKD + Secret Sharing

Shamir's (k, n) threshold secret sharing (info. theoretic. sec.)

Secret sharing

Genome Medical data

Share servers

QKD

Share distribution, renewal, computing, etc…
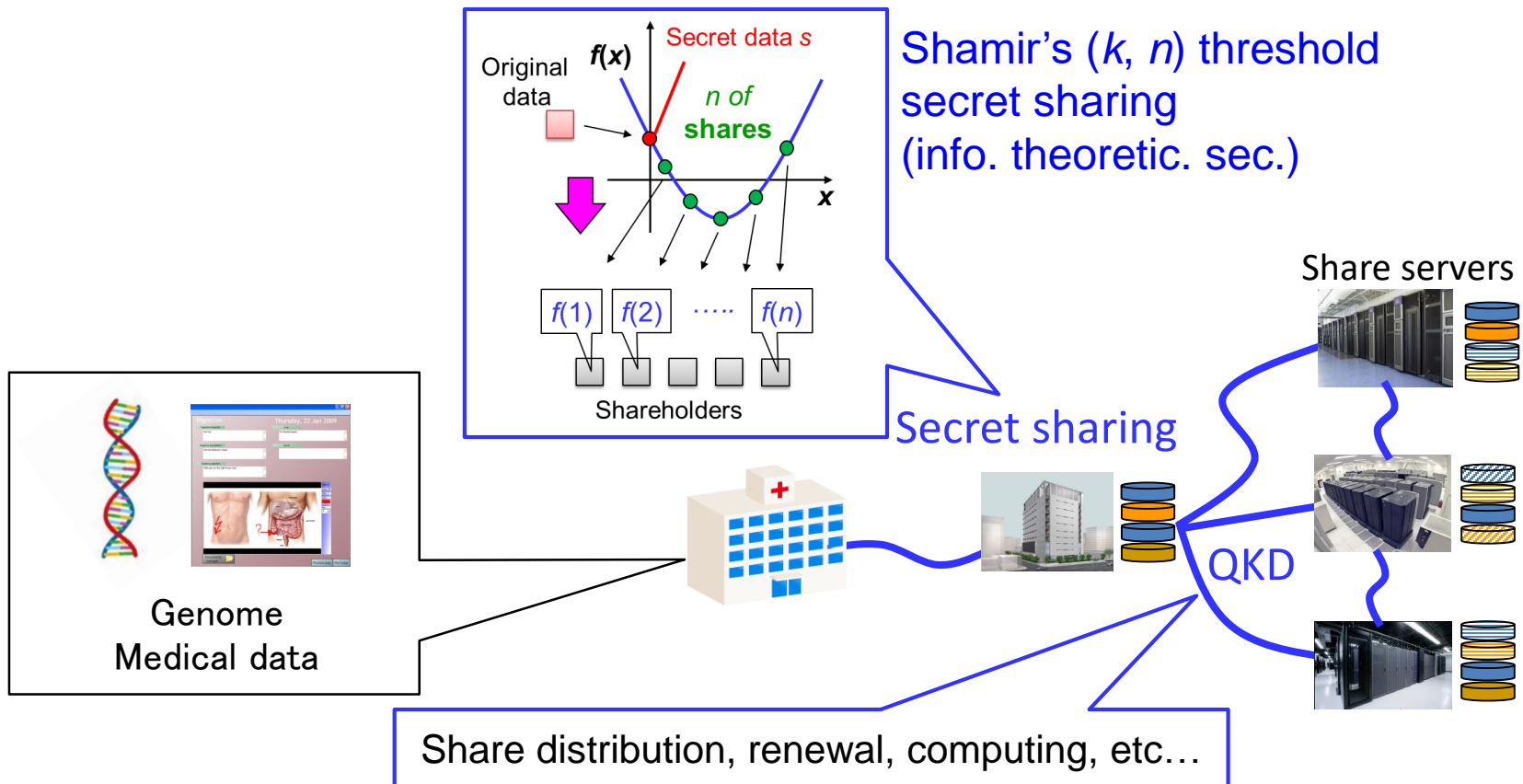
✓ Confidentiality, integrity (total information theoretic security)
✓ Availability, redundancy (data backup)
✓ Functionality (data processing without decryption)

QKD + Secret Sharing

Secret sharing

Private channel

Shareholder

Application layer

Boundary of responsivity

Secure key transfer

Authenticated classical channel

Tokyo QKD Network

KMA

KMS

Key management layer

NEC-0

NEC-1

QKD link

Quantum layer

Gakushuin   SeQureNet   NTT-NICT   Toshiba
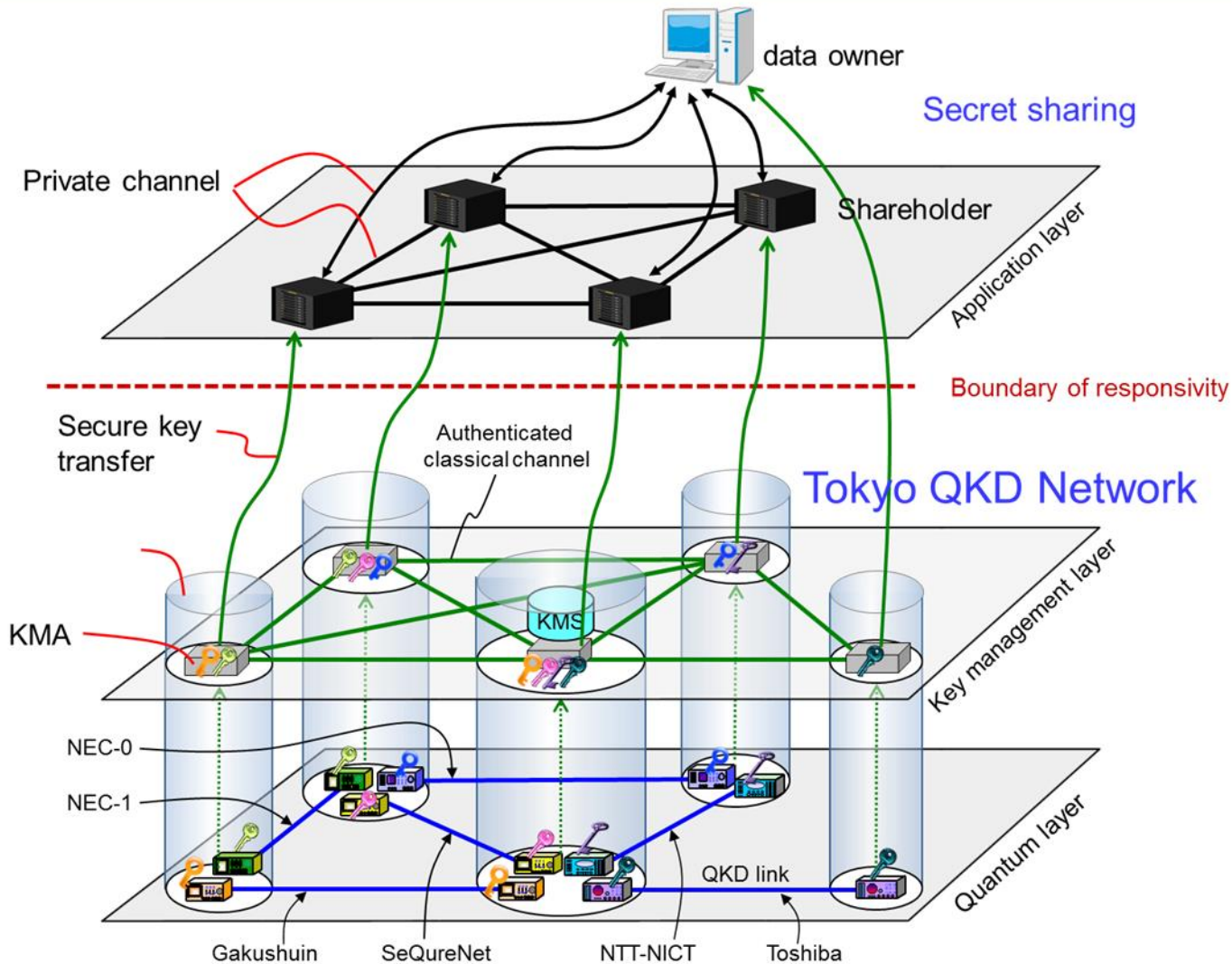
First field demonstration
Fujiwara, et al., Scientific Reports, 6:28988 (2016).

18

Proof of concept demonstration of LINCOS

Future perspective

Healthcare LINCOS network

Healthcare PQ-PKI

Root CA

CA   CA

Certificates   Certificates

PQ Crypto system

- **Signature**
- **Authentication**
- **Access control**
- **Key exchange**

Hospital A

Server

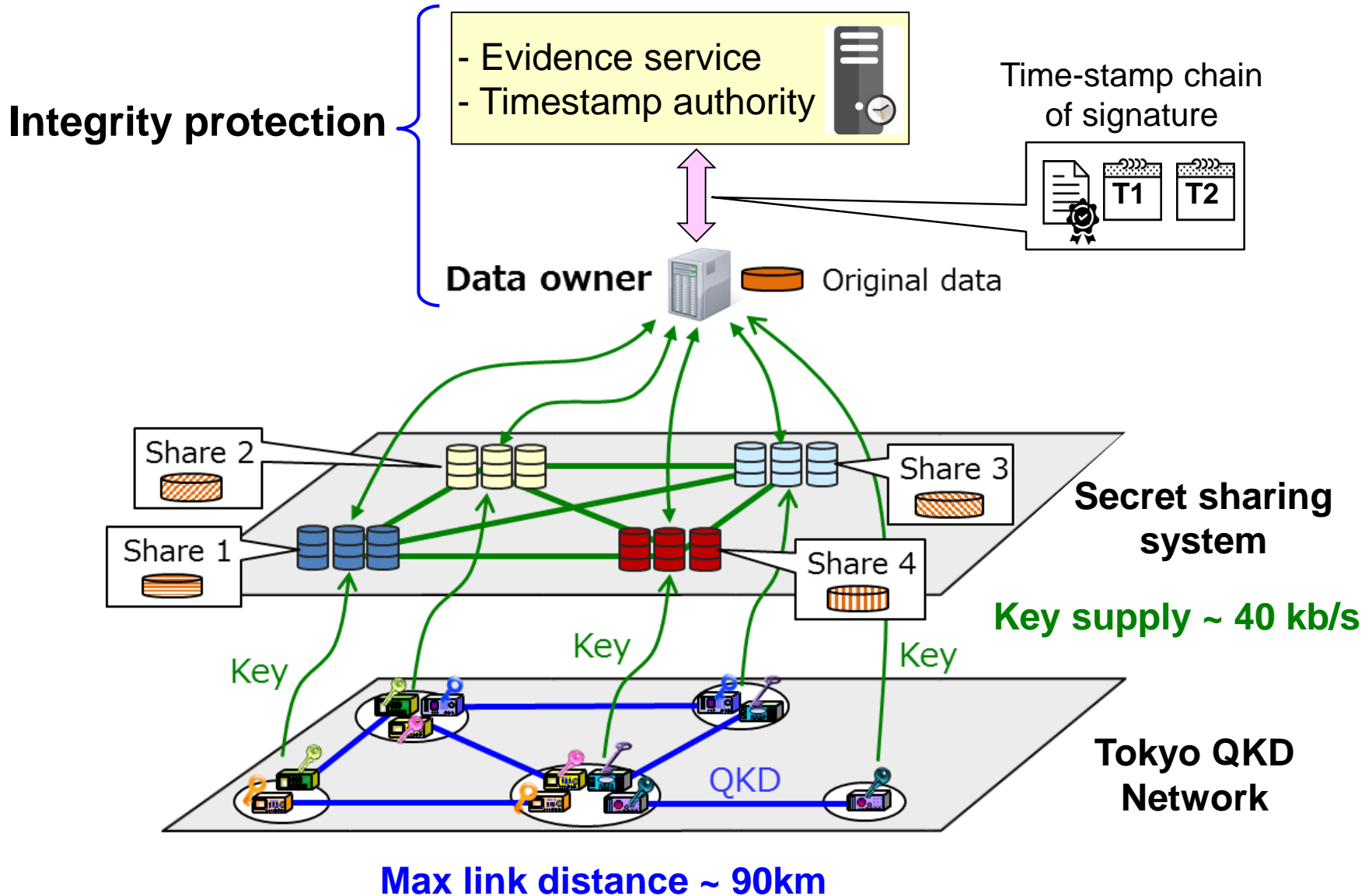**Hospital B**

Server

Electronic health record management system

AI engine

Shareholder

Private channel

- **Secret sharing**
- **Multi-party computing**

- **QKD network**

Secondary use

Anonymized data management system

Registered data management system

R&D, Pharmacy, Precision medicine, …   Healthcare

Summary

- Tokyo QKD Network:

  actively working QKD network testbed since 2010

- LINCOS: long-term integrity, authenticity, and confidentiality protection system

  - Confidentiality protection: secret sharing & QKDN

    ➡️ Information theoretic security

  - Integrity protection: timestamp chains of signature

  - Authentication and access control

    ➡️ Prolongable security (not necessarily IT-sec)

Collaborators

NEC   TOSHIBA   MITSUBISHI ELECTRIC *Changes for the Better*   NTT   GAKUSHUIN UNIVERSITY

ZENMU TECH   TOKYO TECH *Pursuing Excellence*   HOKKAIDO UNIVERSITY   UNIVERSITY OF TOYAMA   東京大学 THE UNIVERSITY OF TOKYO

Tokyo QKD Network Architecture

✓ **A demarcation boundary between a QKD platform provider (an ITS key provider) and users should be clearly defined.**

KSA: Key supply agent
KMA: Key management agent
KMS: Key management server

22