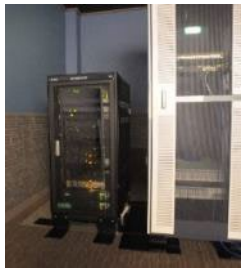
Functions expected of the quantum internet and roadmap in Japan

National Institute of Information and Communications Technology
Quantum ICT Laboratory
Mikio Fujiwara

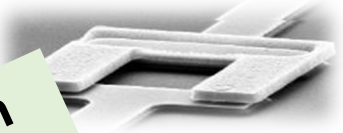
2022.09.21

Definition of Quantum internet



QKD device

Quantum computer



nsmon qubit

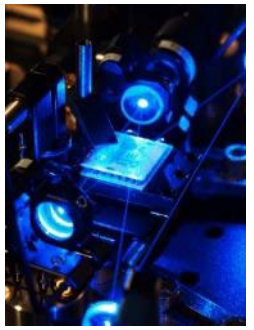
Optical clock

Ion trap

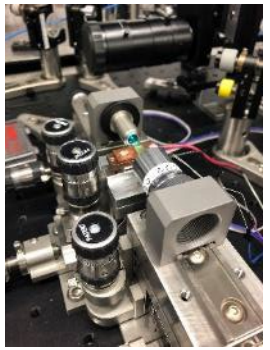
We define the "Quantum Internet" as a platform that can integrate computation, communication, and sensing with quantum states.

Quantum memory (Visible)

Quantum computer (Microwave)



Entangled photon pair (Telecom)



Quantum frequency converter

Expected function of Q-internet

Quantum internet is expected to achieve speed, safety, and accuracy beyond classical technology (computing, communications, sensing).

Necessary technology?

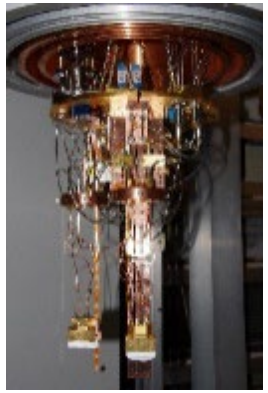
Loss tolerance, error correction, and high-precision synchronization technologies are essential.

To some extent, the required skills are almost identical.

Quantum computation, communication, and sensing are borderlessly connected and will likely be integrated into the same concept and architecture in the future.

Obviously, there are differences in the difficulty of realization.
The most efficient approach is to optimize quantum/classical hybrids according to the required functionality.

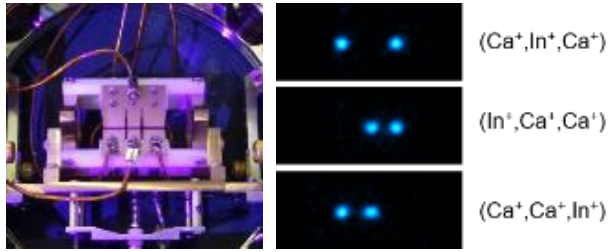
How to hybridize?



Quantum computing

- Classical accelerator + Ising type quantum computer, NISQ

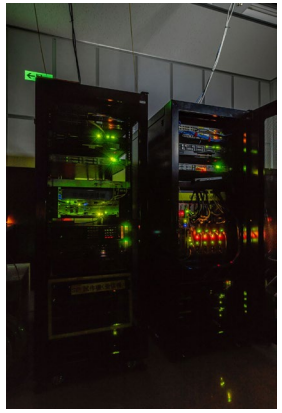
These would play complementary roles to the classical computer and show usefulness.
→ full scale quantum computer



Quantum sensing

- Utilization of optical lattice clock, Single ion atom clock

These technologies are also useful for the advanced coherent optical communications.
→ Improving CV-QKD, TF-QKD, and networkig positioning sensing



Quantum communications

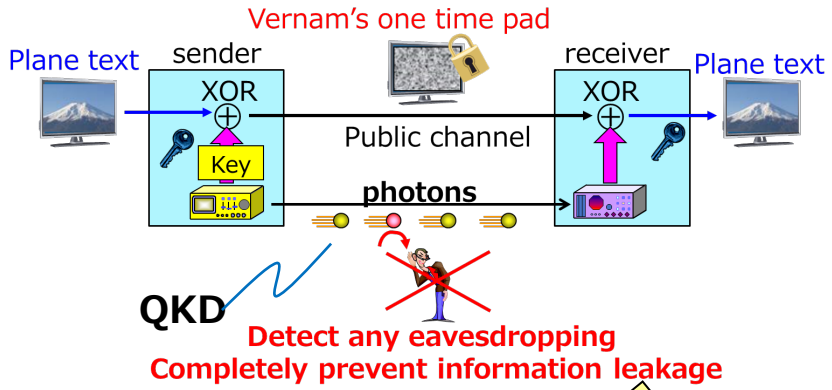
- Improving security of the QKD network

Combination with trusted node based network, installing multi-function in QKD network.
→ Quantum secure cloud

Quantum Secure Cloud

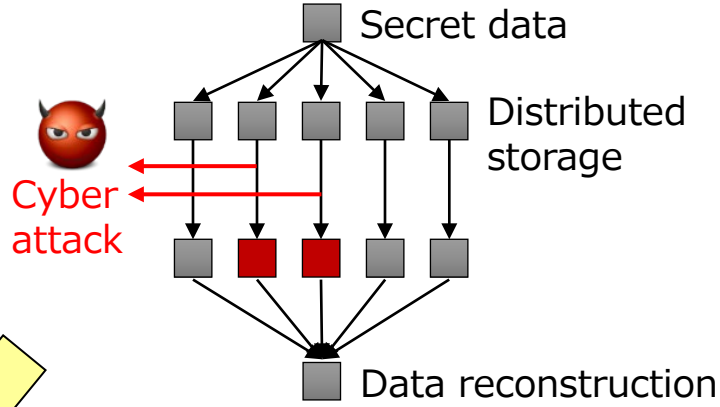
Quantum key distribution (QKD)

The only cryptograph that can prove that it cannot be decrypted by any computer.



Secret sharing (SS)

The secret data is divided into several "shares" and distributed to share holders. Data storage with information theoretical security can be realized.



Combine

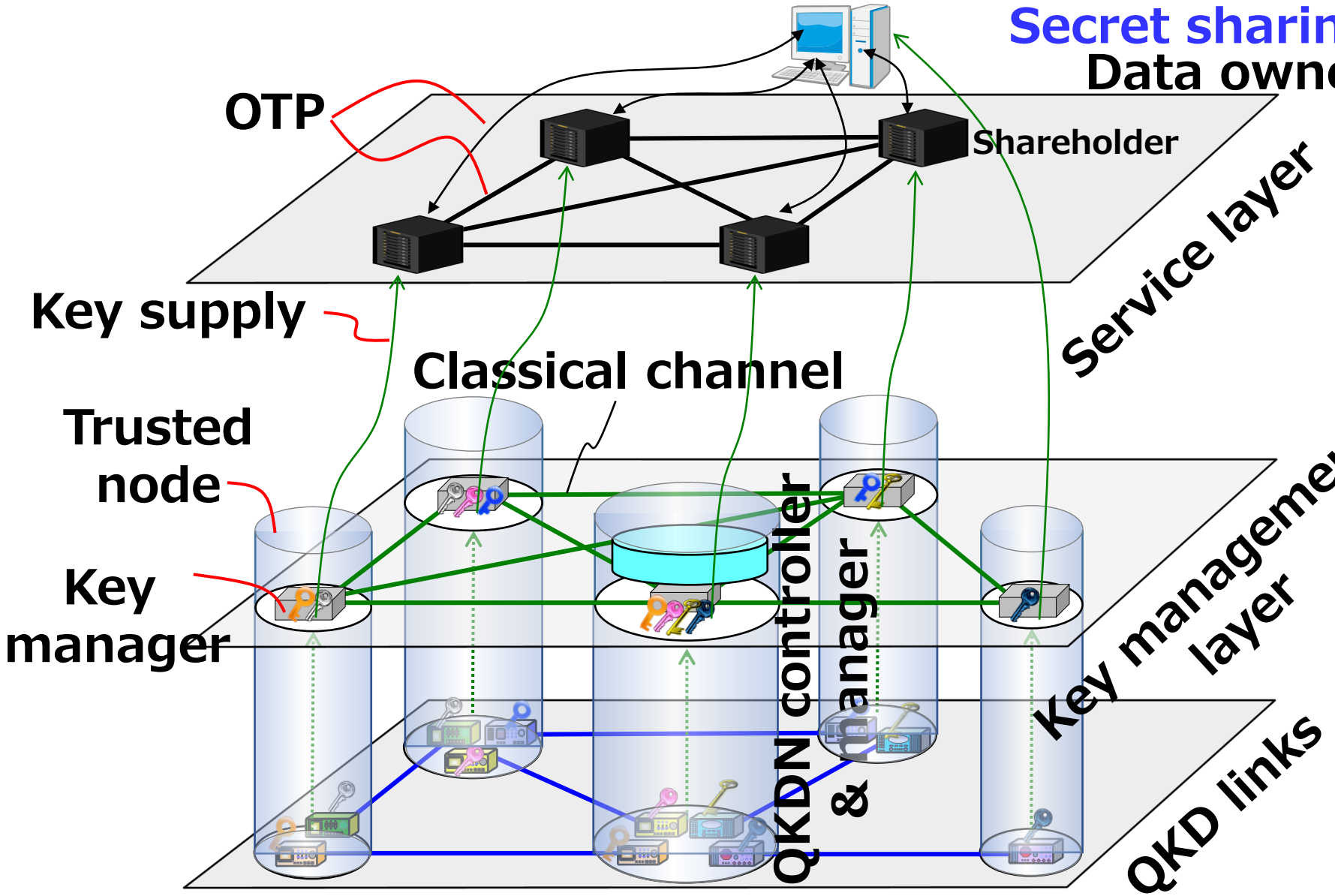
Fujiwara, et al., Scientific Reports, 6:28988 (2016).

Information theoretically secure authentication using a single pass-word (using multi-party computation)

『Quantum secure cloud』

- ✓ **Information theoretical confidentiality**
- ✓ **Availability (redundancy of share holders)**
- ✓ **Secure secondary use of secret data**

Quantum Secure Cloud



Secret sharing,
Secure computation
NICT, ZenmuTech

Security certification:
Univ. Tokyo,
Hokkaidou univ.

Module vender:
NEC, Toshiba,
Gakushuin

Secure authentication using a single password

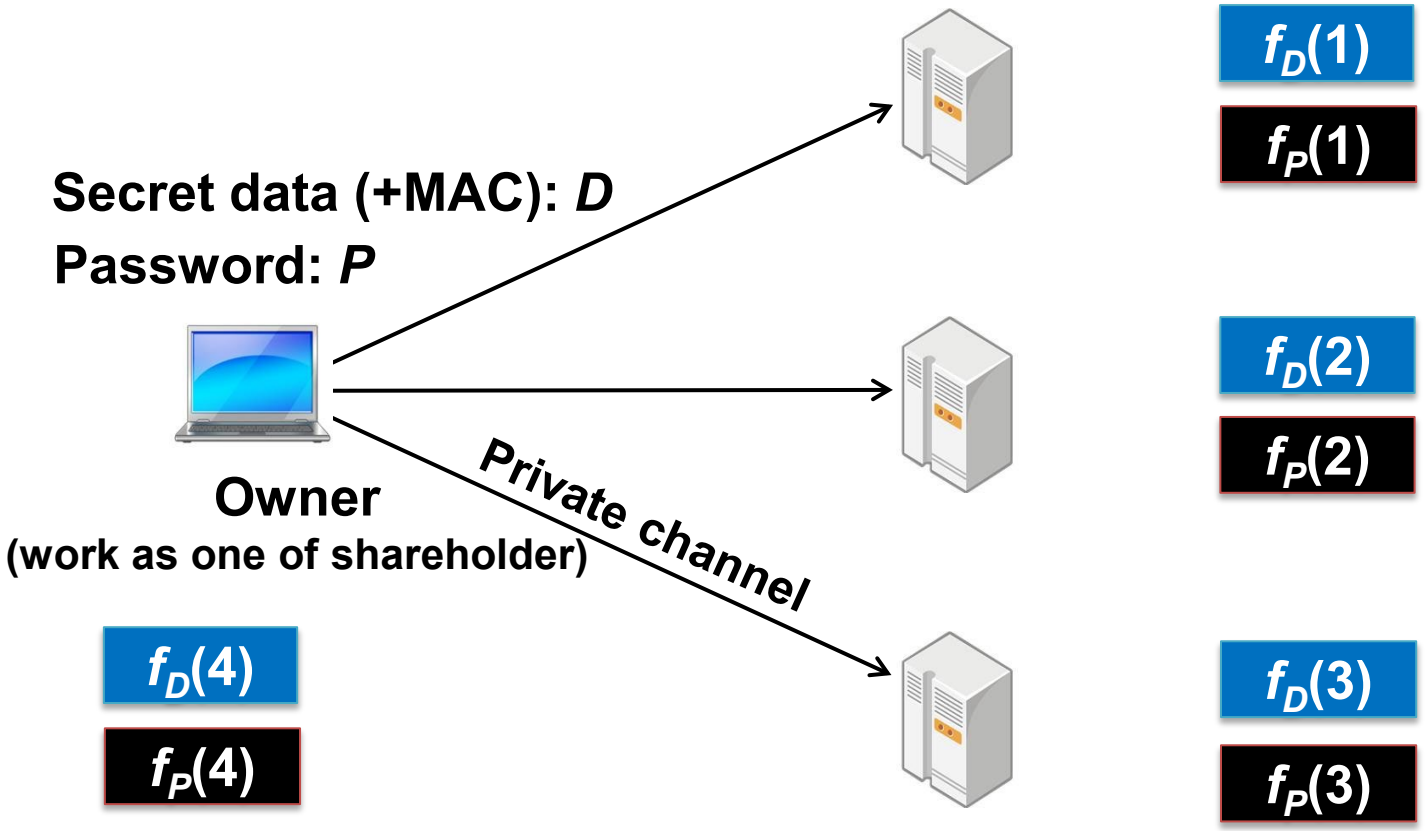
Registration of data and password sharing phase

(1) Owner creates and sends shares of *D* and *P* by using

2nd order polynomial $f_D(x) = D + a_D^{(1)} x + a_D^{(2)} x^2$

(3, 4) threshold for secret data

1st order polynomial $f_P(x) = P + a_P^{(1)} x$



Secure authentication using a single password

Pre-computation and communication among servers phase

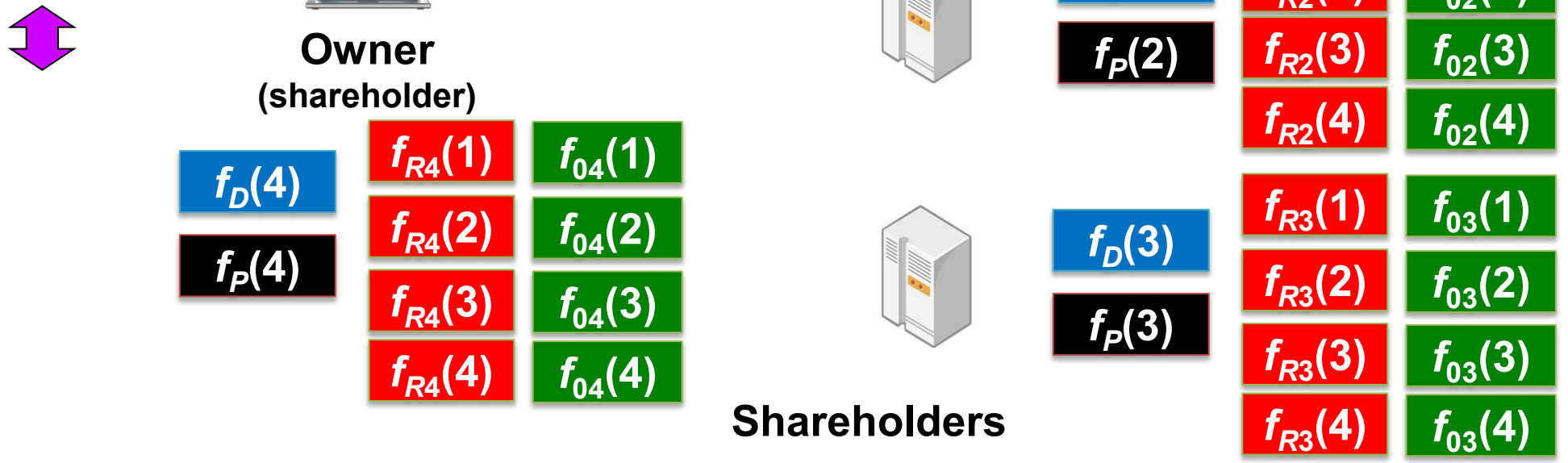
(2) Each shareholder makes shares of *Rj* by using

1st order polynomial $f_R(x) = R + a_R^{(1)} x$

2nd order polynomial $f_0(x) = a_0^{(1)} x + a_0^{(2)}$

x^2 such that $f_{0j}(0) = 0$ (constant term=0

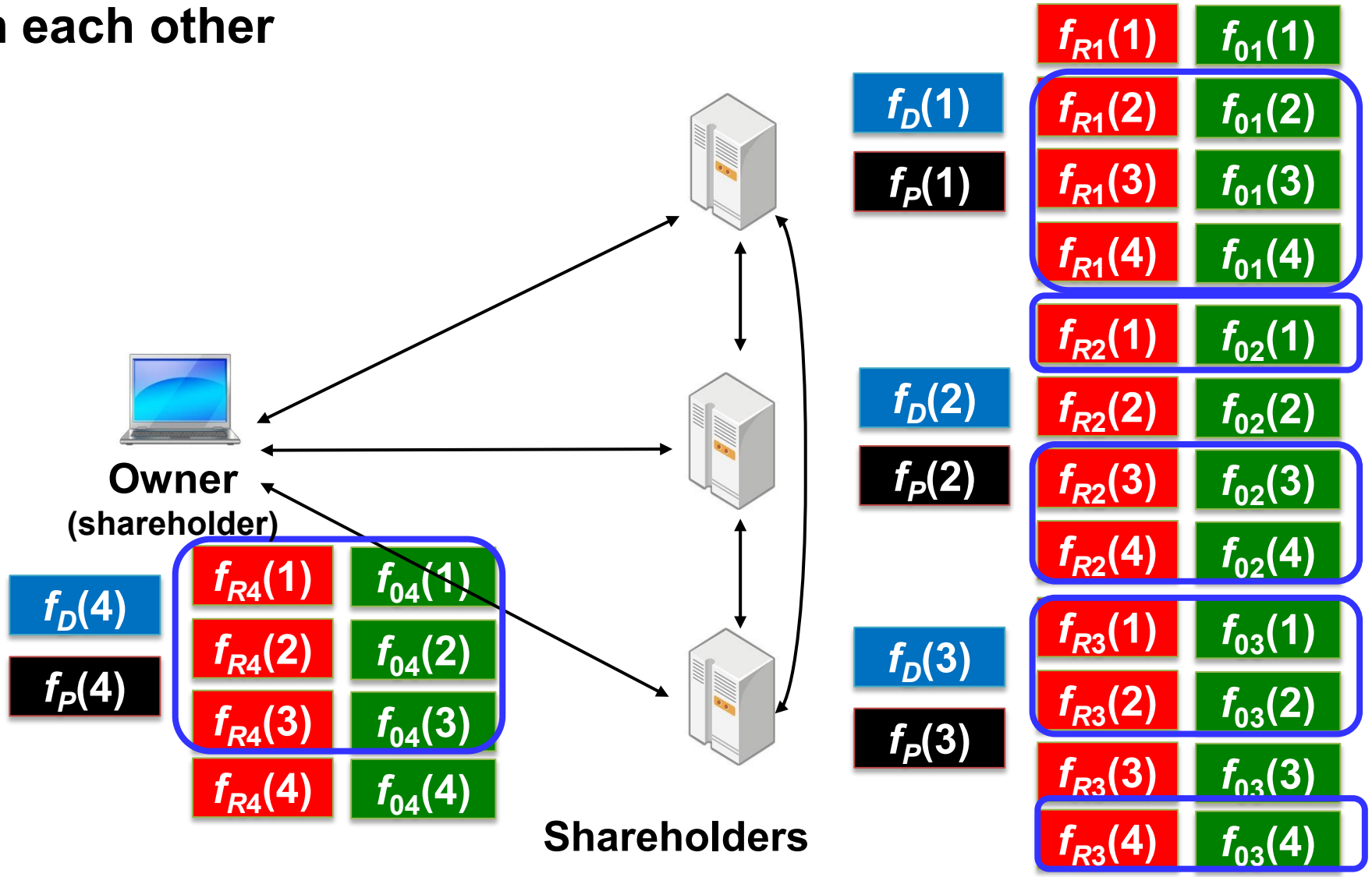
To mask secret data shares $f_D(j)$ in the re-construction phase.



Secure authentication using a single password

Pre-computation and communication among servers phase

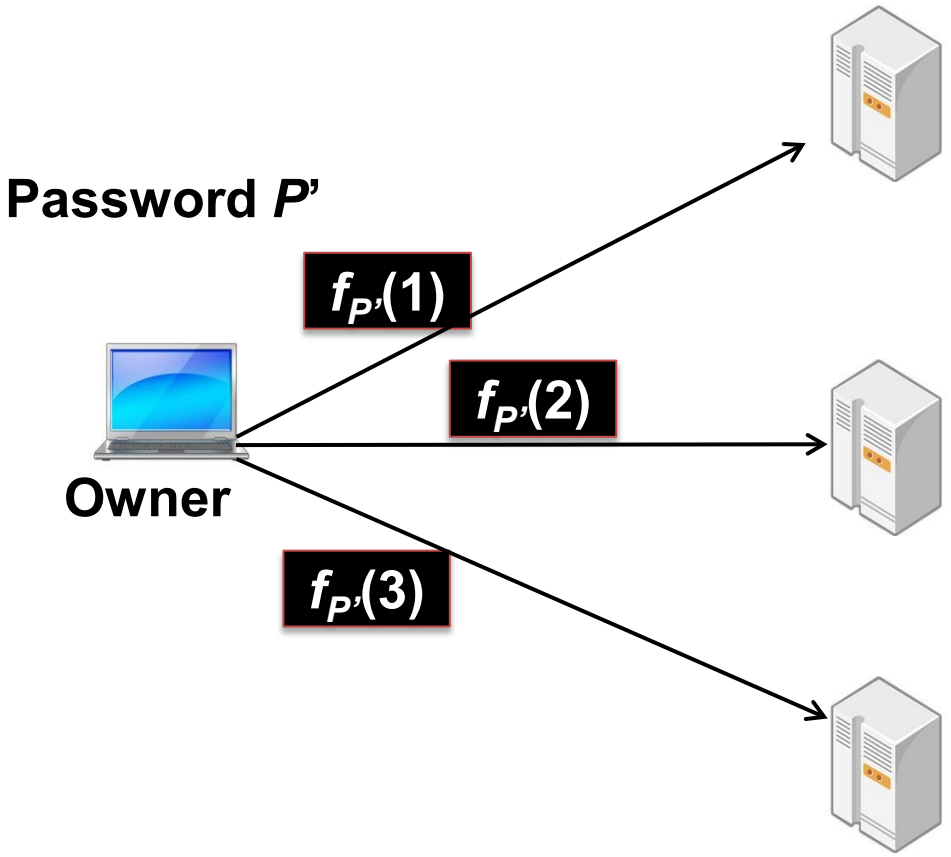
(3) Shareholders exchange shares of *Rj* and "0" with each other



Secure authentication using a single password

Data re-construction phase

(4) Owner remembers the password, which is *P'*, and generates shares of *P'* by using 1st order polynomial $f_{P'}(x) = P' + a_{P'}^{(1)} x$.



	$f_{R1}(1)$	$f_{01}(1)$
$f_D(1)$	$f_{R2}(1)$	$f_{02}(1)$
$f_P(1)$	$f_{R3}(1)$	$f_{03}(1)$
$f_{P'}(1)$	$f_{R4}(1)$	$f_{04}(1)$
	$f_{R1}(2)$	$f_{01}(2)$
$f_D(2)$	$f_{R2}(2)$	$f_{02}(2)$
$f_P(2)$	$f_{R3}(2)$	$f_{03}(2)$
$f_{P'}(2)$	$f_{R4}(2)$	$f_{04}(2)$
	$f_{R1}(3)$	$f_{01}(3)$
$f_D(3)$	$f_{R2}(3)$	$f_{02}(3)$
$f_P(3)$	$f_{R3}(3)$	$f_{03}(3)$
$f_{P'}(3)$	$f_{R4}(3)$	$f_{04}(3)$

Secure authentication using a single password

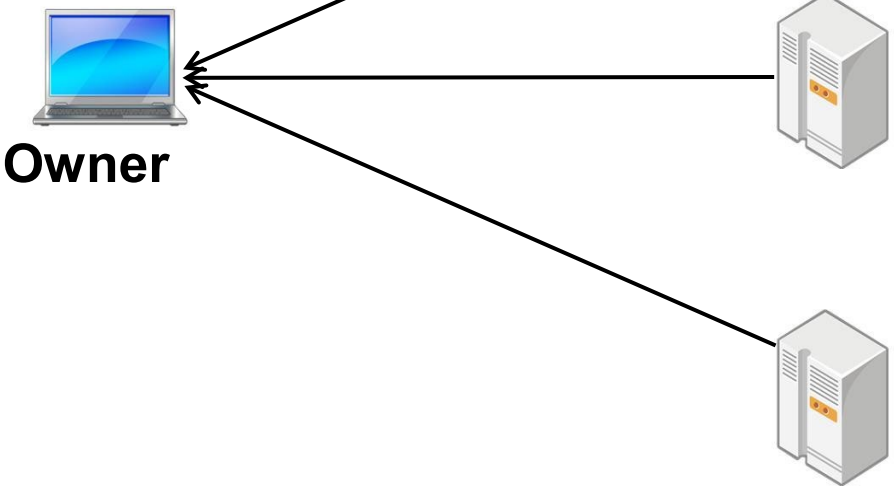
Data re-construction phase

(5) Shares F_1, F_2 and F_3 are sent back to the owner. If the password is wrong, $P' \neq P$, then shares $f_D(1)$, $f_D(2)$ and $f_D(3)$ are masked by R_1, R_2, R_3, Z_1, Z_2 and Z_3. Therefore no information on D is leaked.

$F_1 = [f_P(1)-f_{P'}(1)]R_1 + Z_1 + f_D(1)$

$F_2 = [f_P(2)-f_{P'}(2)]R_2 + Z_2 + f_D(2)$

$F_3 = [f_P(3)-f_{P'}(3)]R_3 + Z_3 + f_D(3)$



Owner

Shareholders

$R_1 = f_{R1}(1)+f_{R2}(1)+f_{R3}(1)$

$Z_1 = f_{01}(1)+f_{02}(1)+f_{03}(1)$

$F_1 = [f_P(1)-f_{P'}(1)]R_1 + Z_1 + f_D(1)$

$R_2 = f_{R1}(2)+f_{R2}(2)+f_{R3}(2)$

$Z_2 = f_{01}(2)+f_{02}(2)+f_{03}(2)$

$F_2 = [f_P(2)-f_{P'}(2)]R_2 + Z_2 + f_D(2)$

$R_3 = f_{R1}(3)+f_{R2}(3)+f_{R3}(3)$

$Z_3 = f_{01}(3)+f_{02}(3)+f_{03}(3)$

$F_3 = [f_P(3)-f_{P'}(3)]R_3 + Z_3 + f_D(3)$

Secure authentication using a single password

Data re-construction phase

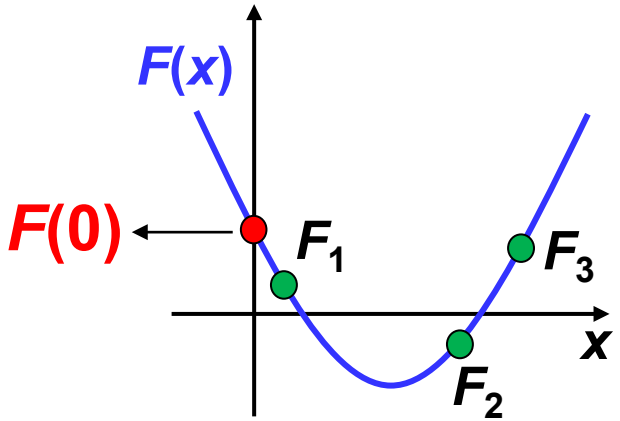
(6) If the password is correct, $P'=P$, then

$$F_j = [f_P(j)-f_{P'}(j)]R_j + Z_j + f_D(j)$$

$[f_P(j)-f_{P'}(j)]R_j$ terms canceled

Z_j terms → "0"

Owner



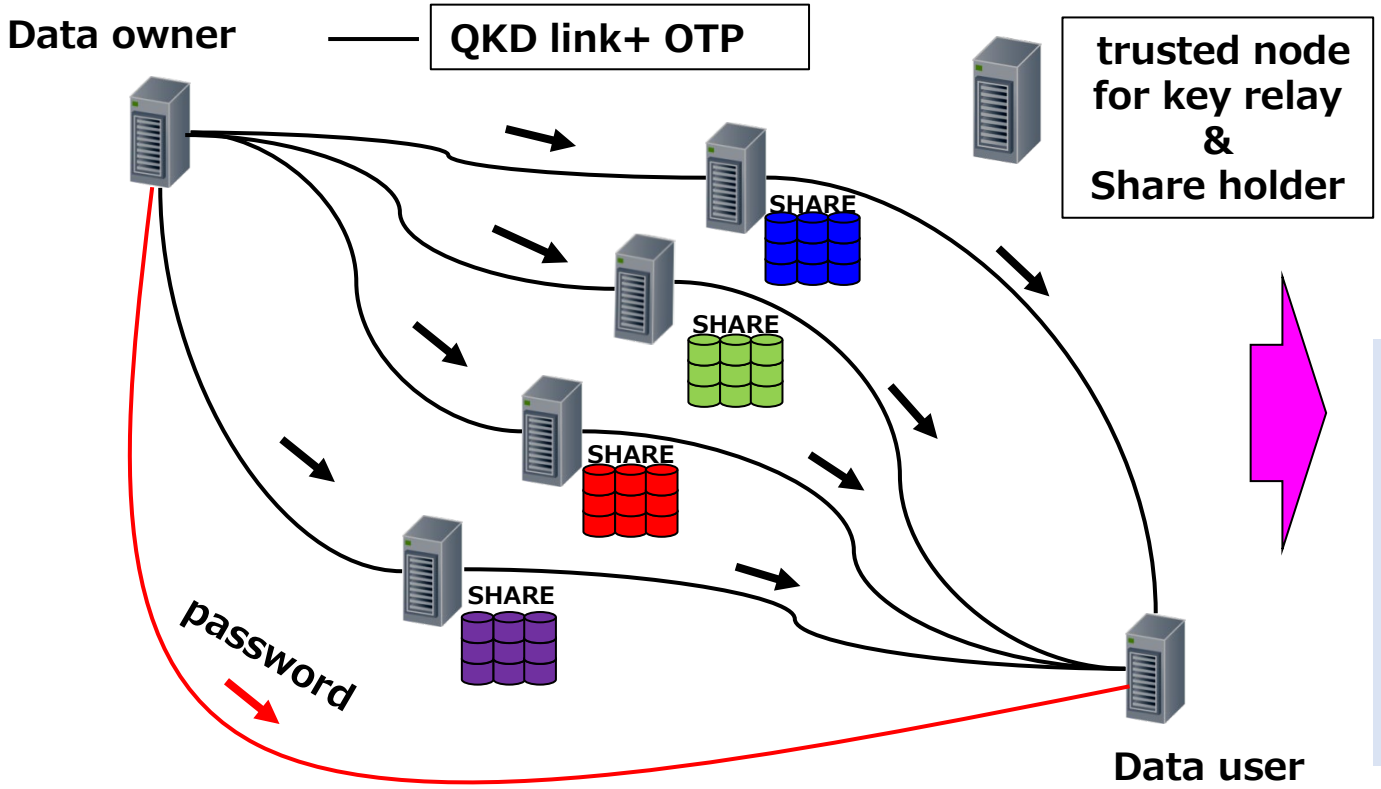
The owner re-constructs the original data as

$$F(0)=f_D(0)=D \text{ (secret data +MAC)}$$

The owner calculates MAC and checks integrity.

Secure data relay

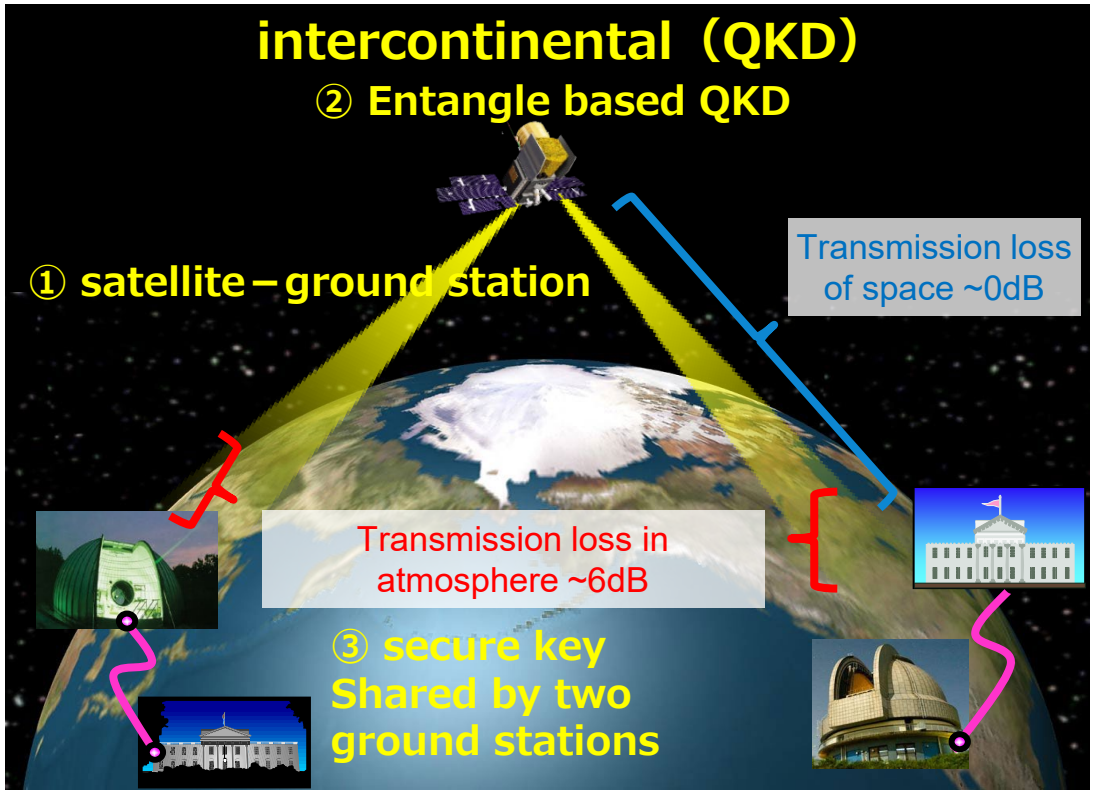
If the password is sent by OTP using key from a single QKD link,
Information theoretically secure data relay by using this protocol can be achieved,
even if the security level required of nodes is slightly relaxed.
(Security is maintained as long as the administrators of each node do not collude.)
→Long distance QKD link is necessary (throughput is small but sufficient).
Quantum relay, satellite QKD link, and twin-field QKD would work as this single link.



Expanding data relay length with information theoretical security

National project developing global quantum communication including quantum memory and twin-field QKD has started in 2020.

Satellite QKD

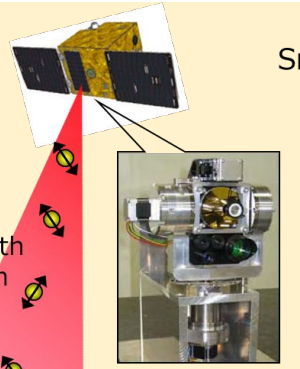


Transmission loss

Fiber: 0.2dB/km
Space: ~R^2 (40dB at 400km)
→ Inter continental QKD can be achieved by a low orbit satellite

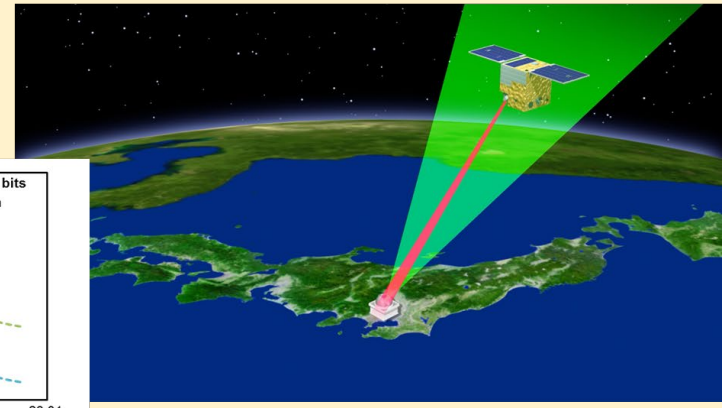
Low Earth Orbit
650km

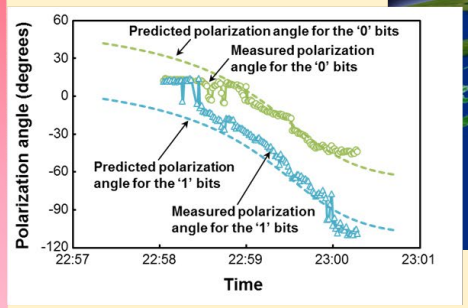
Small Optical Transponder (SOTA)
・Mass 5.9kg
・Laser wavelength 0.8mm, 1.5mm
・Repetition rate 10Mbps



Small SOCRATES (50kg)
developed by AES Corp. and NICT
Launched in May 2014

Quantum communication experiment by using the small satellite(2017)





H. Takenaka, et al., Nature Photonics, 11, pp. 502-508 (2017)

National project（2018～2022）

Optical beam
⇒ random bits

RF public channel
⇒ for key Distillation

Equipment for Onboard small satellite

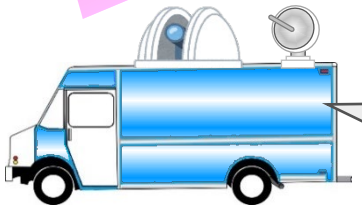
Ⅰ small transmitter QKD/Physical layer cryptography (NICT/ U-Tokyo)

- QKD
- Physical layer cryptography
- switching

Ⅲ pointing technology (SONY/NICT)

- Fine pointing
- Coarse pointing

Ⅱ mobile ground station (NICT)

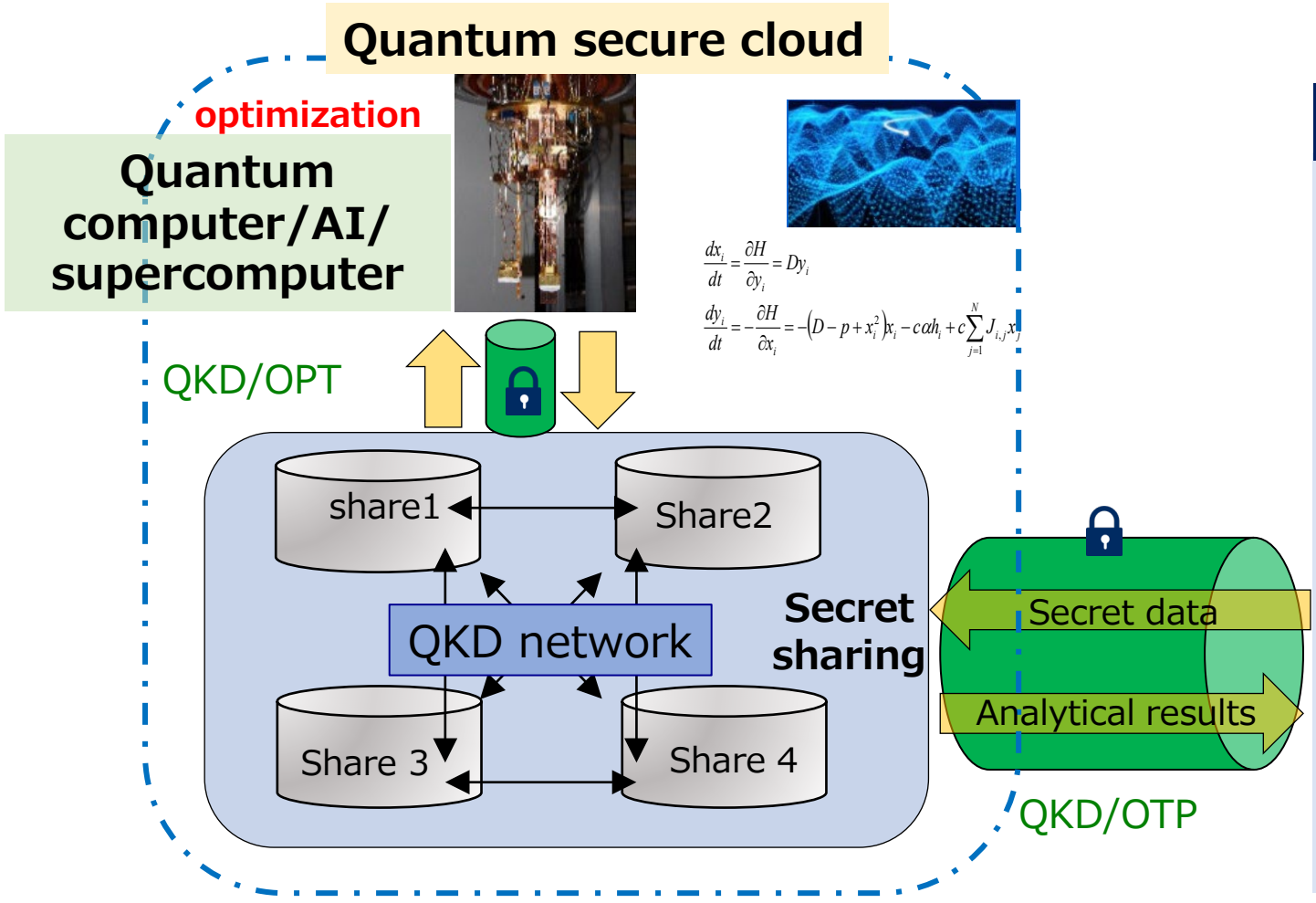


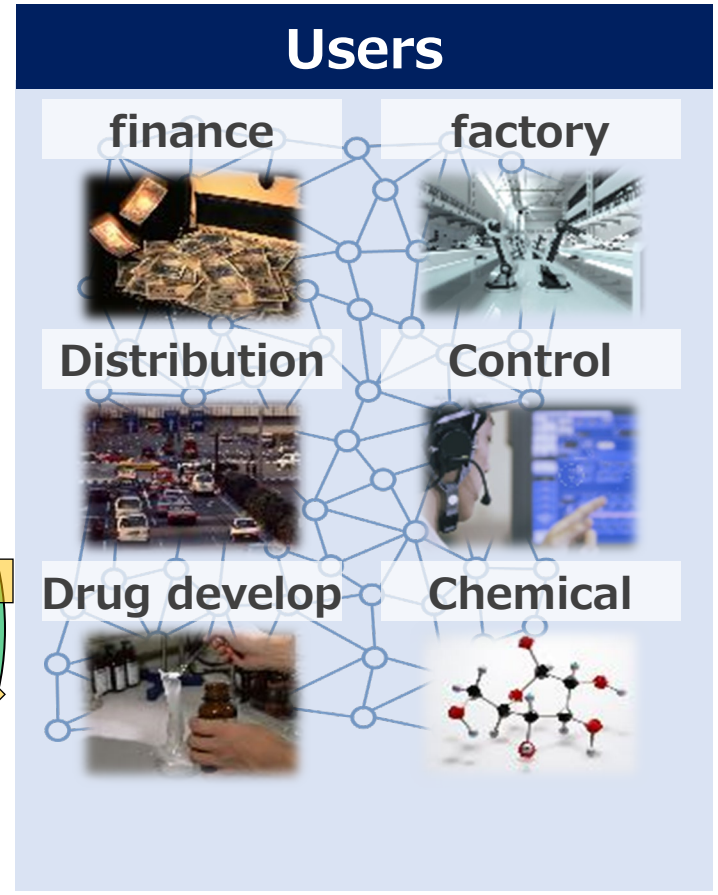
- QKD receiver
- Physical layer Cryptography receiver
- Coarse pointing
- Fine pointing

Ⅳ integration (NESTRA, JSAT, NICT)

Quantum secure cloud on quantum internet

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

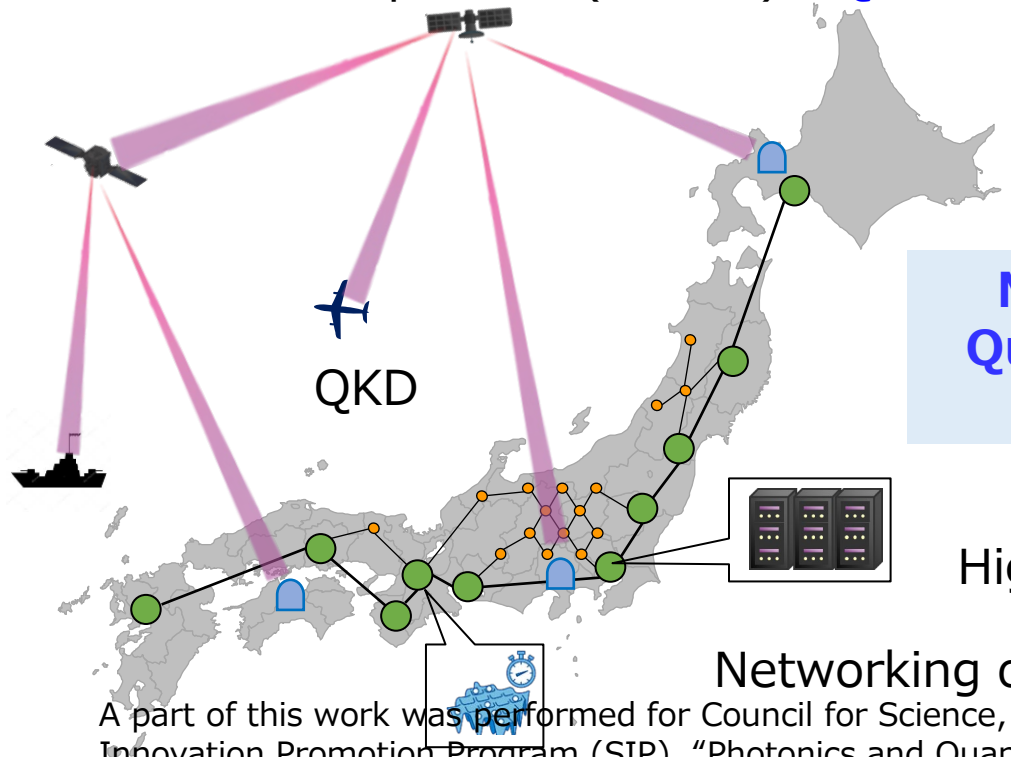




Roadmap in Japan

By Expanding Tokyo QKD Network, we would like to enhance the functionality of the Quantum Internet using a hybrid of classical technology.

First step (~2023) : QKD network around Tokyo
Second step (~2025) : QKD network colony established in big cities
Third step (~2030) : Fiber based QKD + satellite QKD Network
Forth step (~2035) : Global QKD Network
Fifth step (~2040) : **Quantum internet** (joint with quantum relay network)



Multi-function Quantum secure cloud

⇒Expanding the market while demonstrating

Quantum computer/
High performance FPGA, GPU

Networking optical clock

A part of this work was performed for Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Photonics and Quantum Technology for Society 5.0”(Funding agency : QST).

Summary

The "Quantum Internet" would work as a platform that can integrate computation, communication, and sensing with quantum states.

↓ There are many extremely difficult technical challenges.

Introduce mature quantum technologies in stages to upgrade the Internet (step by step).

↓ It is necessary to demonstrate functions that are not possible without quantum technology.

It is important to realize the best mix of classical and quantum technologies in accordance with the times of the era.

We need to show that quantum technology is interesting and useful, while increasing the number of supporters regarding the development of quantum technology.

Thank you for your attention