4th Sep 2014

Japanese industry efforts on QKD applications

Quantum ICT Lab
Masahide Sasaki

Fact (1)

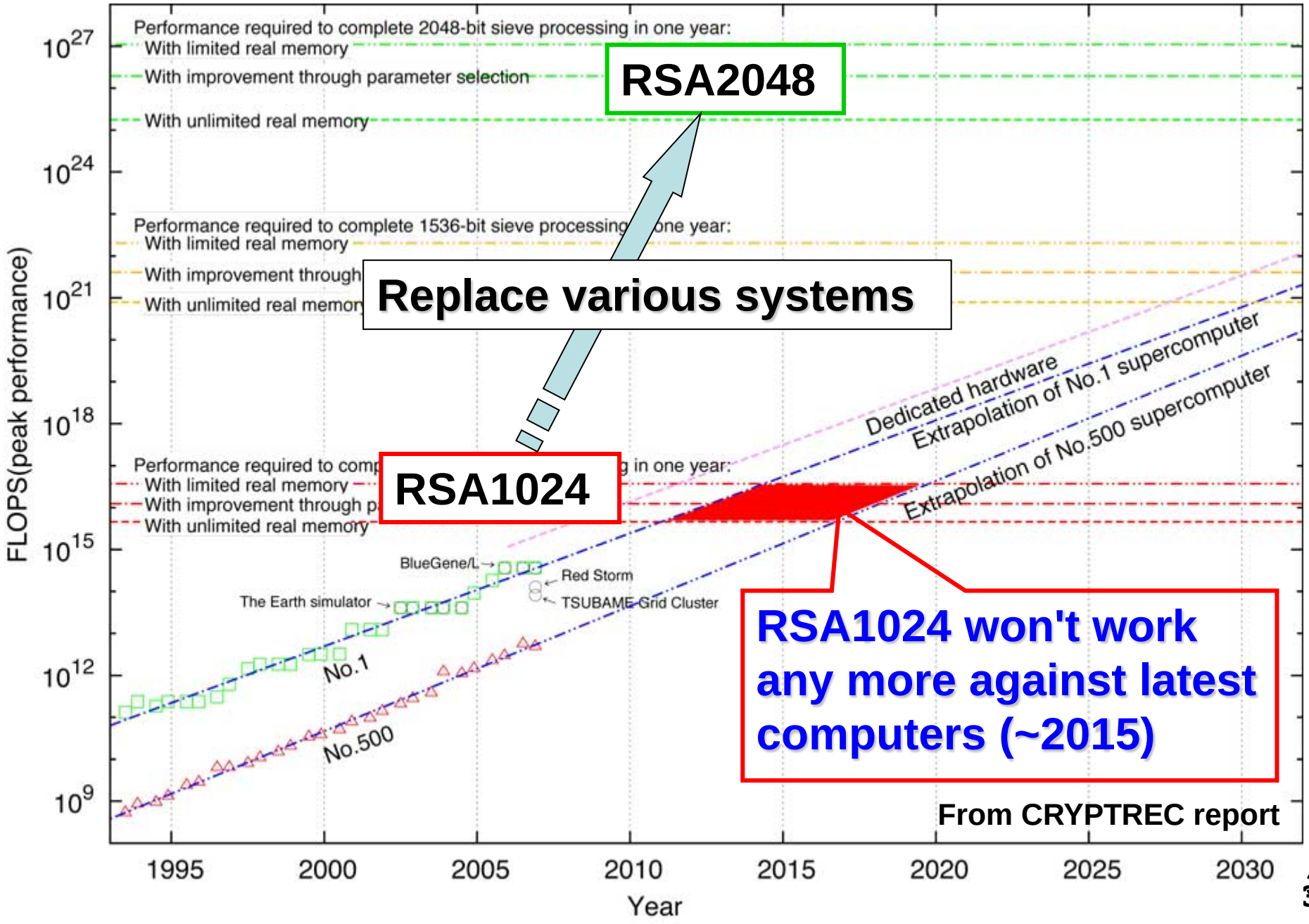
High end users (MoD, …) are seriously worried about security threats on the physical layer after the Snowden files, but have not decided yet to introduce QKD. They are still watching.

The strongest security is not necessarily a reason for the scheme to be adopted.

There are many strong crypto-schemes, but most of them have not been used in practice yet.

Ex. Most of users still use RSA1024 even after doubling the key length was strongly recommended.

Computational complexity vs advancement of computers



Implication from Fact (1)

Stand alone QKD is hard to be accepted.
Start with an existing security system,
then integrate QKD into it, and realize new values.

Algorithmic cryptography	New values of QKD
1. Not provable --> Need to be updated	1. Updating the scheme itself is not necessary
2. Cannot detect hacking	2. Can detect hacking
3. Specs of high-end solutions are usually not disclosed. -->Hard to interconnect the systems of different divisions even in the same organization.	3. Simplest encryption : one-time pad, C=X + K --> No processing latency --> Seamless cryptic connectivity can be realized if key IDs are properly managed.

Fact (2)

Responses to our press releases on QKD technology remarkably increased this year.

Ex. QKD-assisted secure smart phone (May 2014)

Potential customers who have asked us on it includes

- **Ministries (MIC, MHLW)**
- **Prefectural office**
- **General construction company**
- **Banks**
- **Car company**
- **Print company**

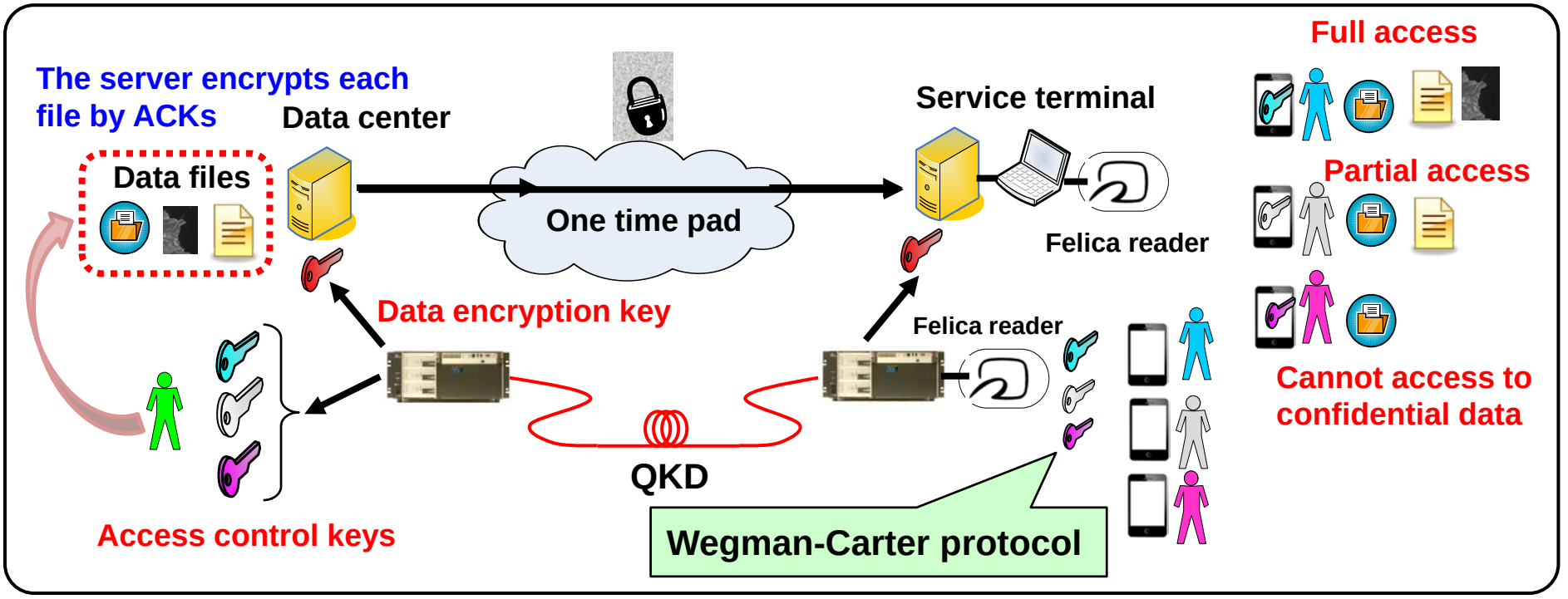
They are looking at future society based on the Internet of Things, and want to know what kind of security technology they should introduce, and how to revise their security systems.

Conversation with them are very inspiring.

QKD-key + smart phone is something marvelous !

QKD-assisted secure smart phone

Hierarchical access control to confidential data files



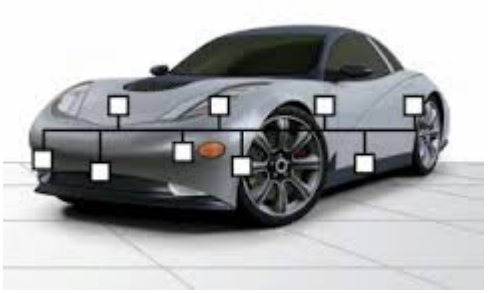
Useful to protect state secrets and medical chart

Implication from Fact (2)

There are new fields where security is becoming a new concern. That is,
modern crypto and QKD are at the same start line.

- **Medical network**
- **Controller Area Network (CAN)**
- **Robot network**

…..

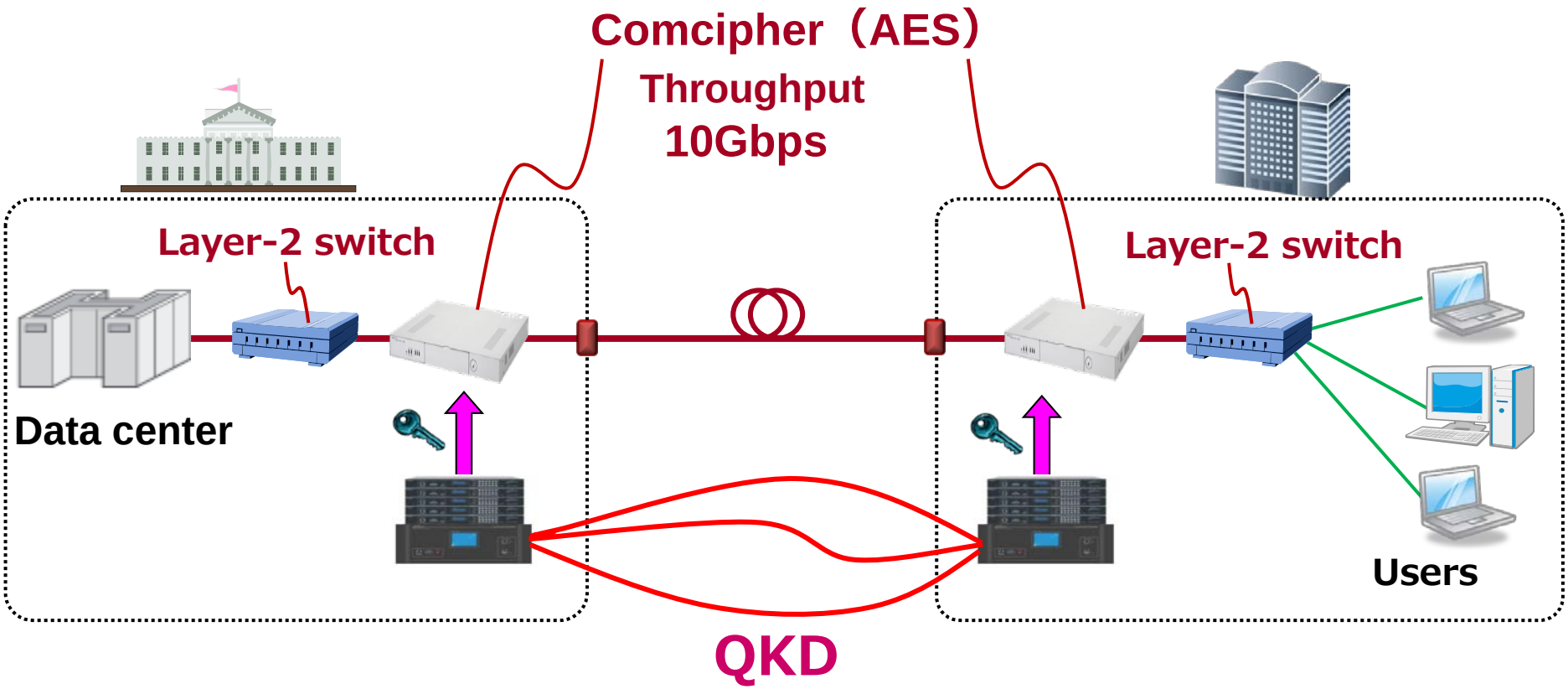


How to share symmetric keys between control units and how to manage them?

Security standards have not been decided yet.

Integrate QKD with a commercial product, *Comcipher*

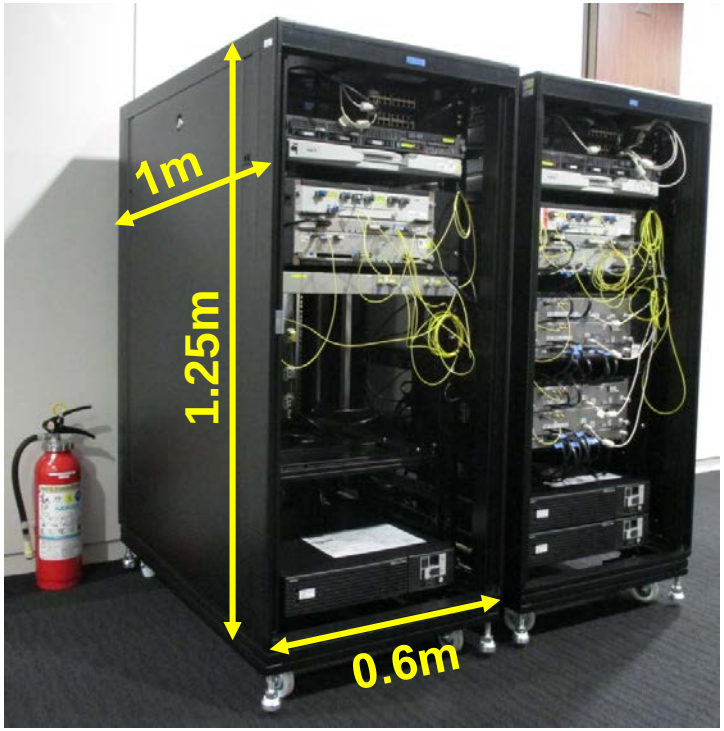
Most of mission critical channels are made in the 2nd layer (data layer), not going up to the 3rd layer (IP network layer)

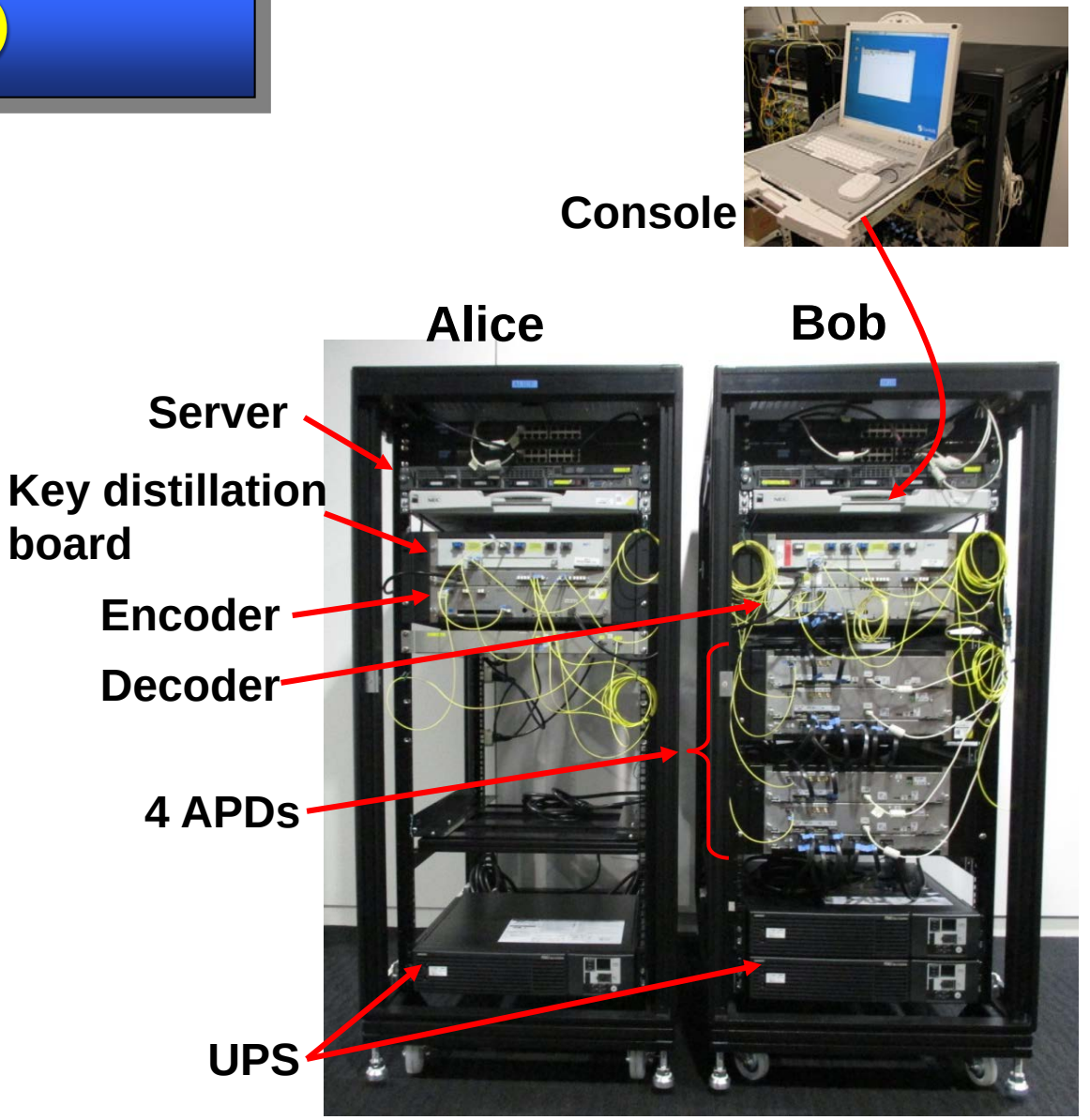


- Enhance the security of AES by key refresh
- One-time pad mode is optional for high-end use.

NEC demonstration model
(Decoyed BB84)

Key rate 100kbps
Distance 60km
(for fiber loss 0.2dB/km)
Clock rate 1.24GHz

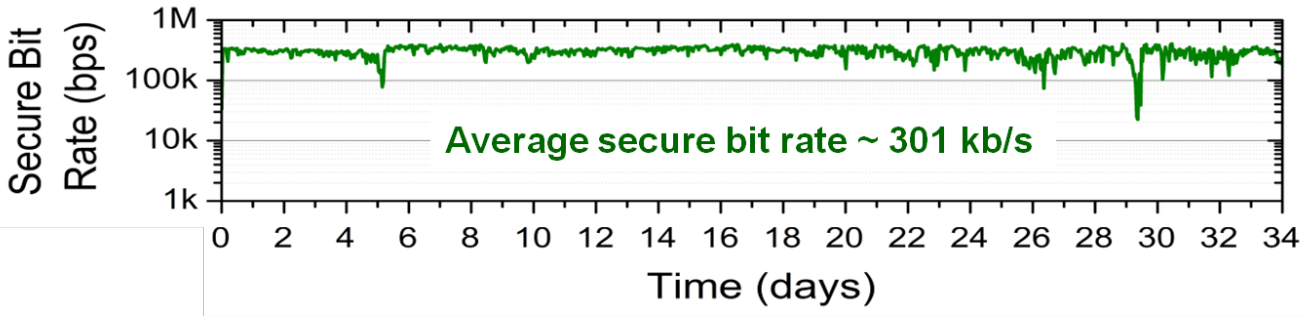




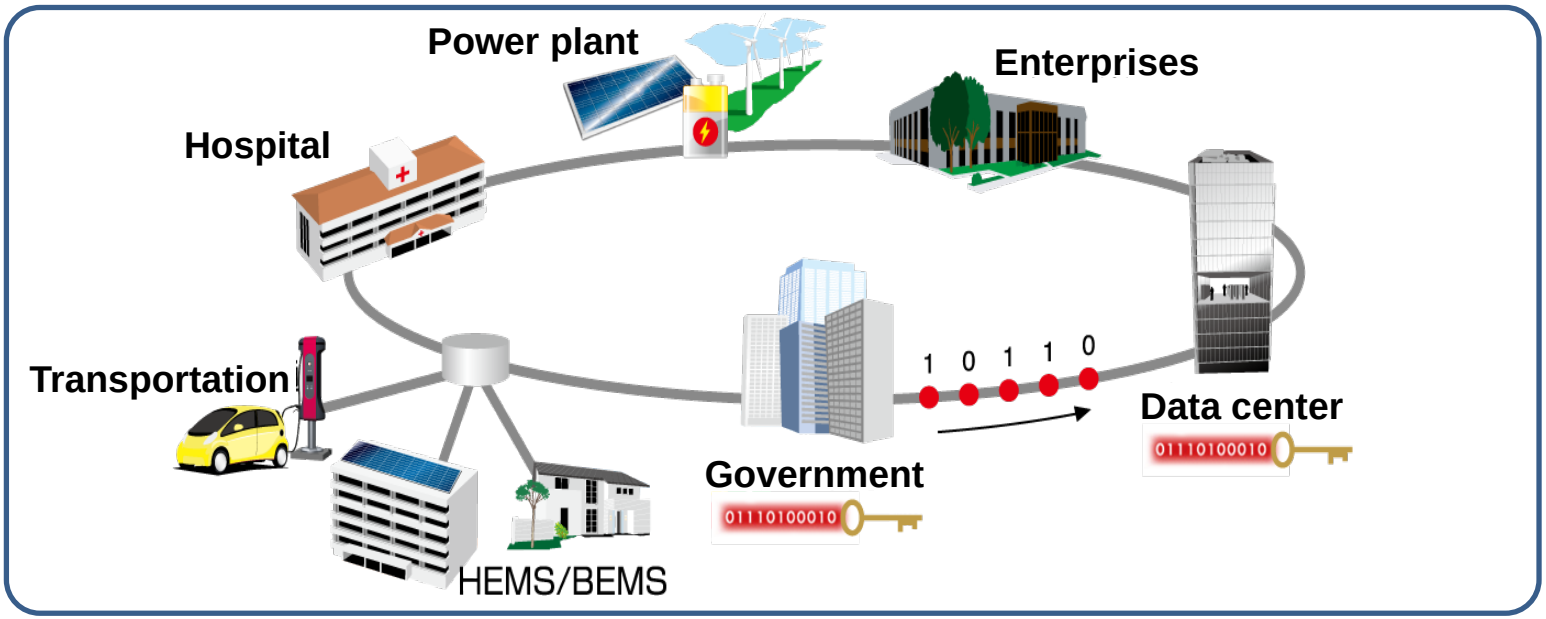
Toshiba

Key rate 300kbps
Distance 60km
(for fiber loss 0.2dB/km)
Clock rate 1GHz

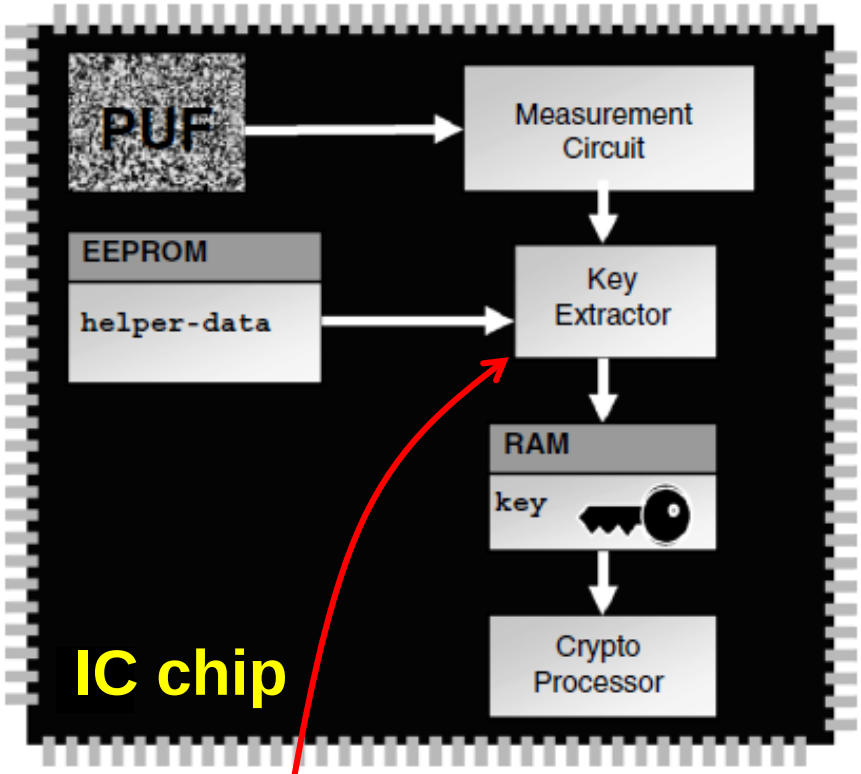
Marked largest ever volume of secure key in field fibre on overhead poles (14.5dB)



Secure smart community



QKD smart phone



Apply Privacy Amp of QKD to modern crypto-tech

Ex. Key extractor for

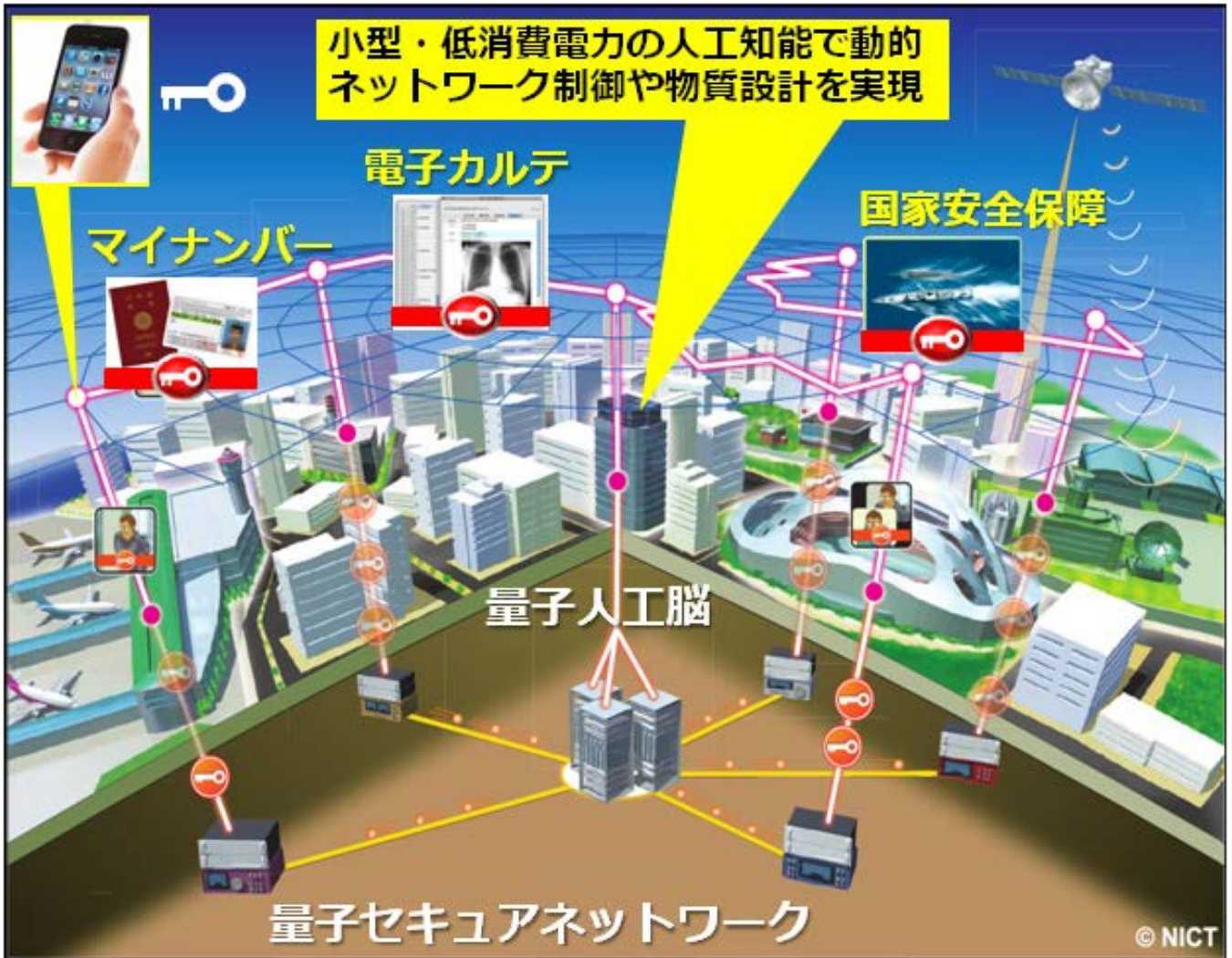
- **Physical Unclonable Function (PuF)**
- **Biometrics**

Make a QKD show case for Tokyo Olympic 2020

Safest Tokyo Network

ImPACT Program (Oct 2014-Mar 2019) by the Cabinet office

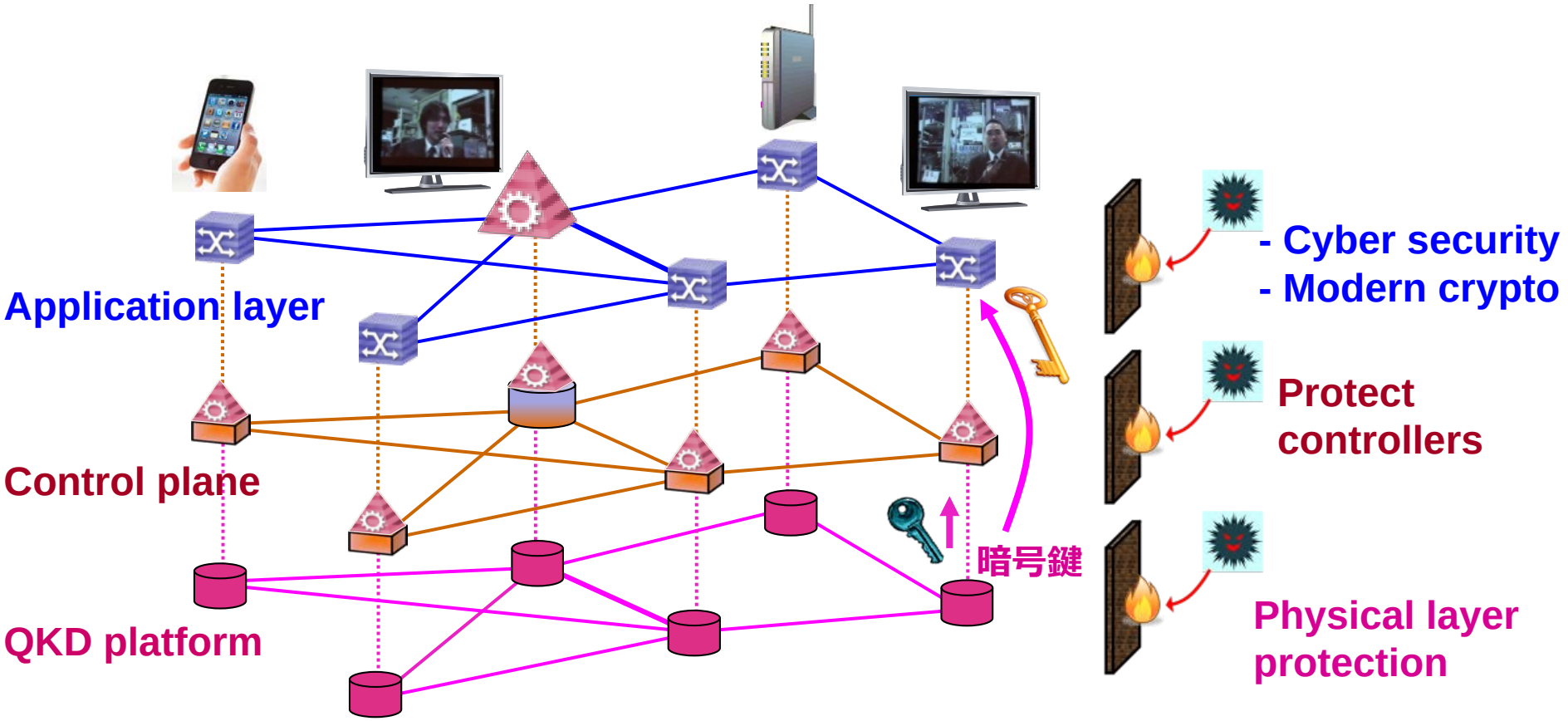
Impulsing PAradigm Change through disruptive Technologies



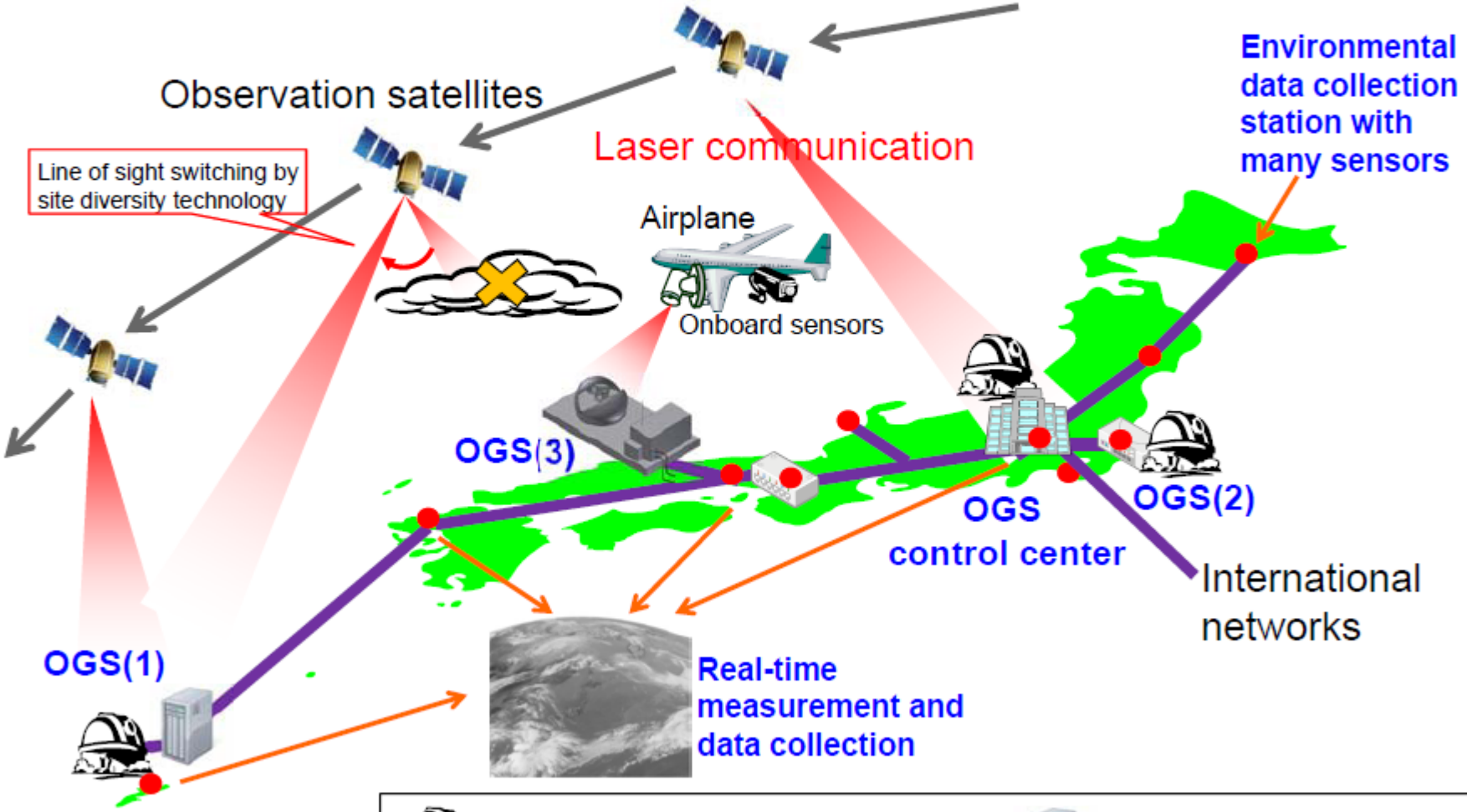
Security defense in depth

Multi-layered monitoring and protection system

Collaboration with modern cryptographers and cyber security engineers

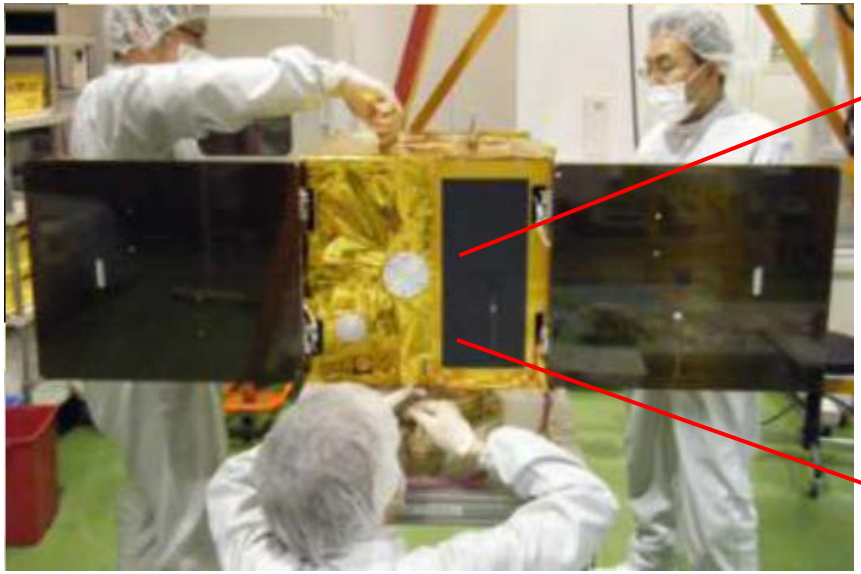


Satellite airborne network business



Small satellite SOCRATES
(NICT, AES, NEC, JAXA)

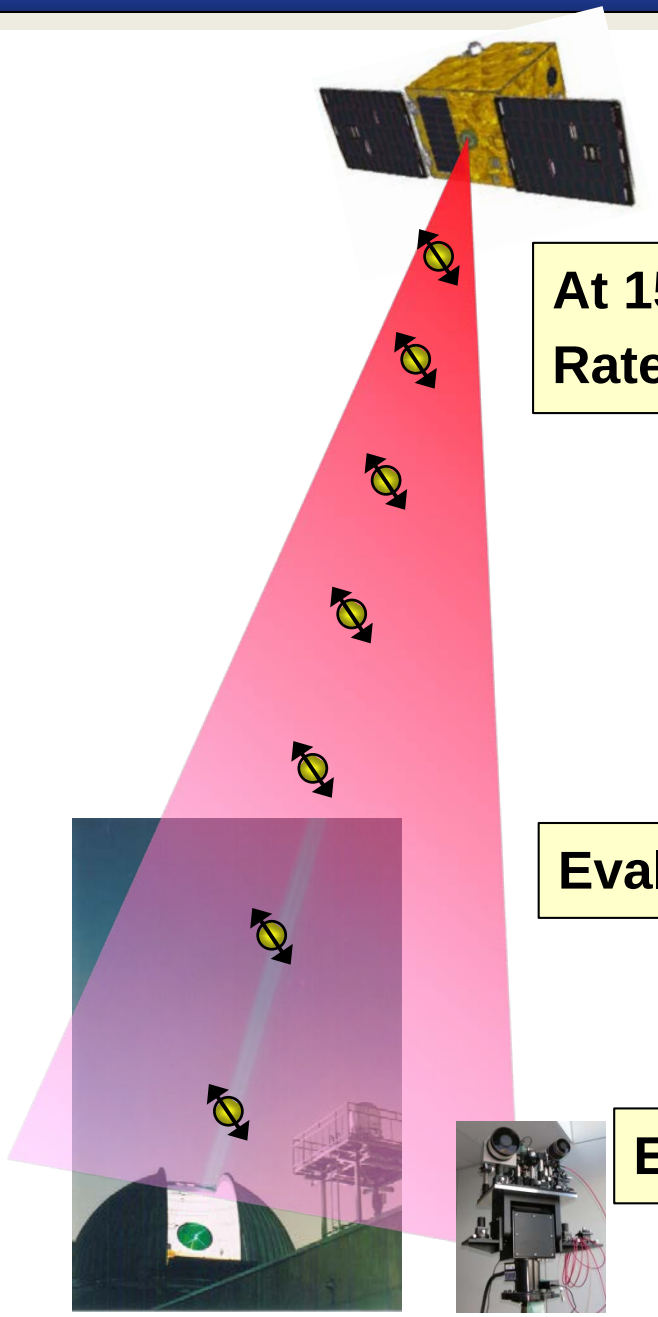
- Launched on 24 May 2014
- Successfully put on the orbit(628km)
- Now under preparation for operation



50kg-satellite bus

Small optical transponder
6.2kg

Satellite-ground laser link

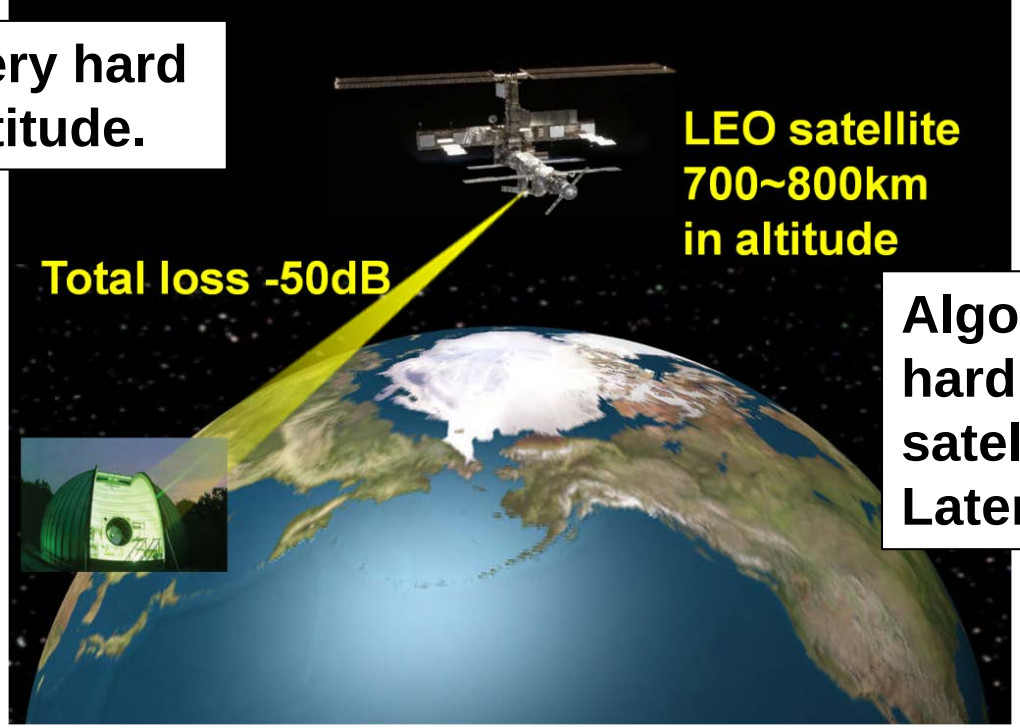


At 1550nm, 800nm, 967nm
Rate 1Mbps or 10Mbps

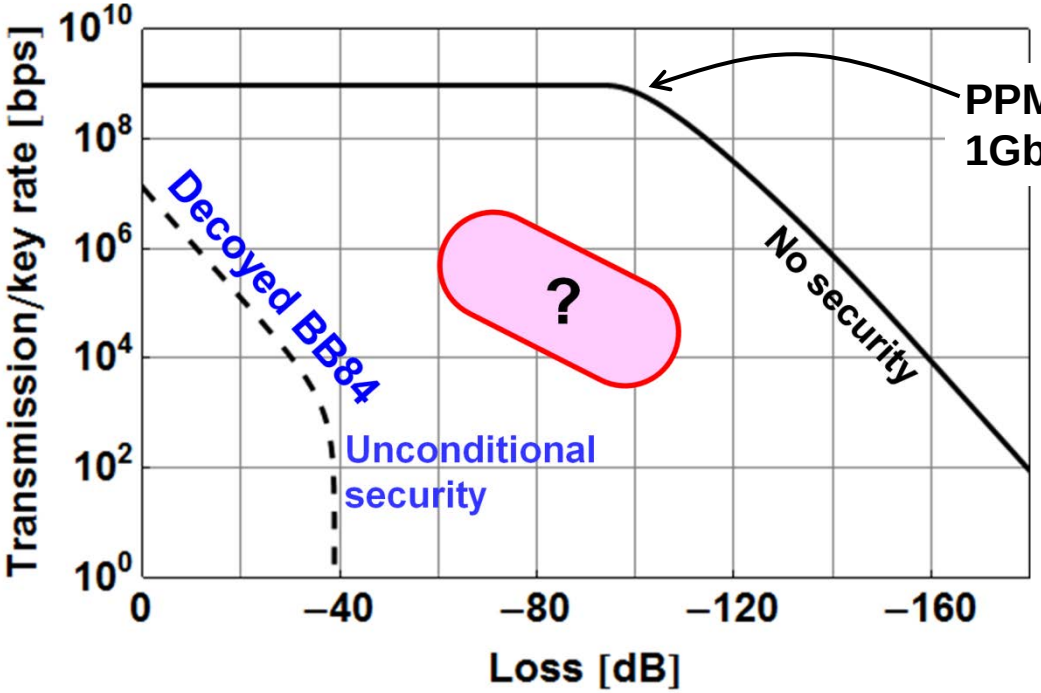
Evaluate polarization encoding

Evaluate footprint jitter and wiretap risk

QKD is very hard at LEO altitude.

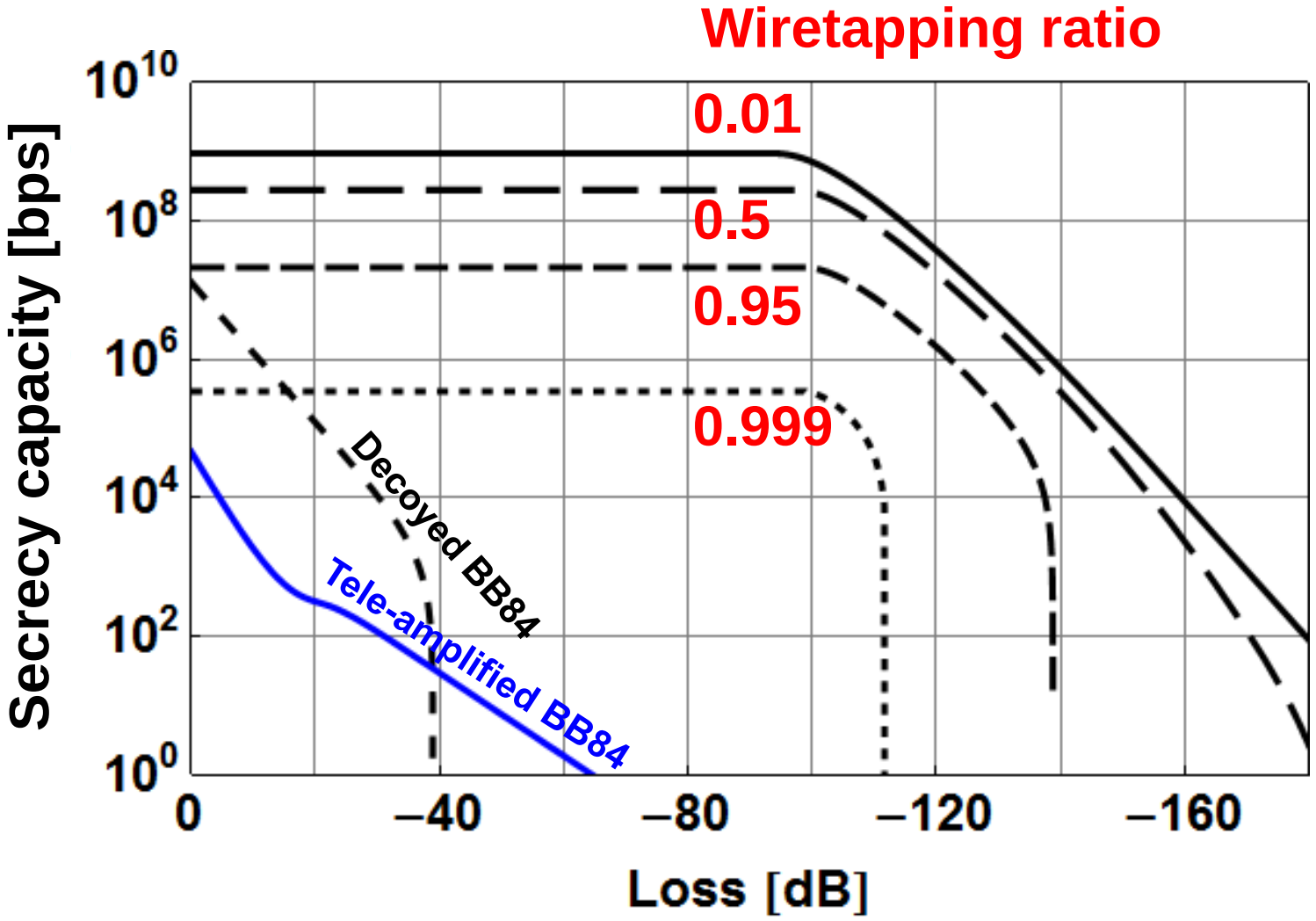


Algorithmic crypto is hard to be updated in satellites.
Latency is also a matter.



Physical layer cryptography

Secrecy capacity $C_S = \max_{P_x} [I(X;Y) - I(X;Z)]$

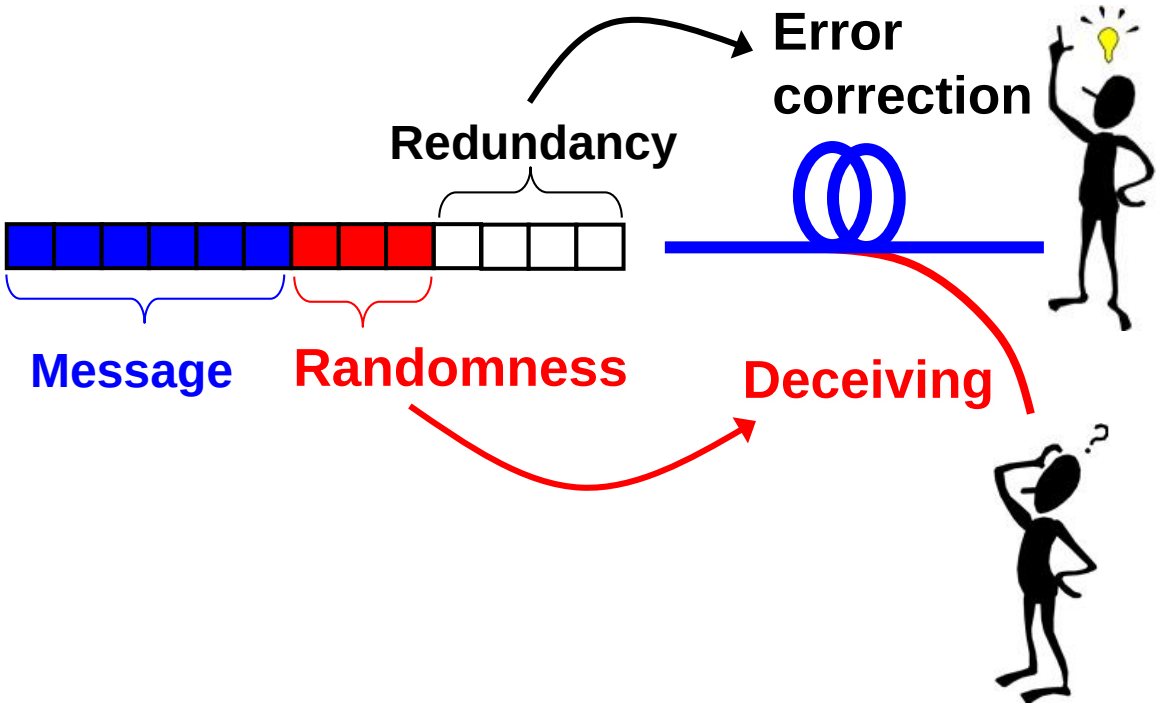


Physical layer cryptography

Opportunistic link when

Eve's channel is physically bounded.

"Information theoretic security" at higher rate



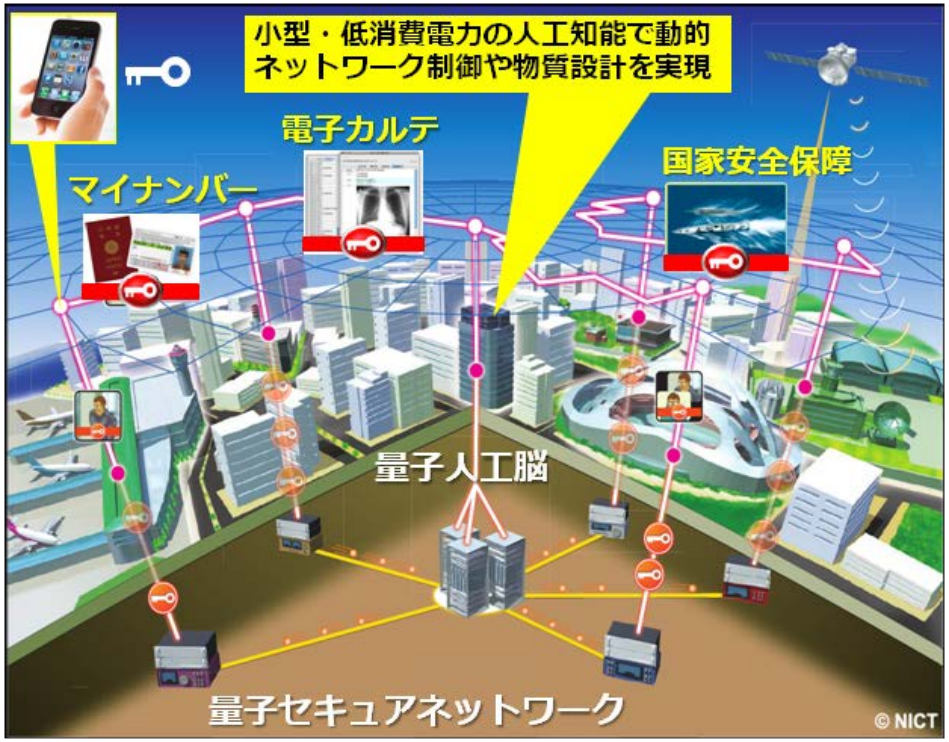
Han, Endo, & Sasaki, arXiv:1307.0608 [cs.IT]

New generation secure network

QKD ⟷ Phys Layer Crypto ⟷ Algorithmic Crypto

Combine Physics laws, Coding, PA, & Algorithms

Quantum noise
(Optical domain)



Thermal noise
(RF domain)

Trinity College DublinのHPより転載