Orchestrating a brighter world NEC

[NEC Group Internal Use Only]

AQIS2016

Quantum Key Distribution Network for Multiple Applications

A. Tajima[1], T. Kondoh[1], T. Ochi[1], M. Fujiwara[2], K. Yoshino[1], H. Iizuka[1], T. Sakamoto[1], A. Tomita[3], E. Shimamura[1], S. Asami[1] and M. Sasaki[2]

1 NEC Corporation
2 National Institute of Information and Communications Technology
3 Hokkaido University

Orchestrating a brighter world

NEC brings together and integrates technology and expertise to create the ICT-enabled society of tomorrow.
We collaborate closely with partners and customers around the world, orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to greater safety, security, efficiency and equality, and enable people to live brighter lives.

Outline

1. Introduction
2. Quantum Key Distribution (QKD) Network
   - Requirements
   - QKD Platform (QKD PF)
3. Robust QKD System
4. Introductory Video (6 min.) 
5. Applications on the QKD PF
   - QKD-AES Hybrid System
   - Secure Smartphone
6. Summary

Introduction

Eavesdropping optical channel is reality.

- National secret communication is at risk for tapping and decoding.
- The Snowden files;

http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

- In the near future, critical information of individuals may also be at risk.
  - Banking information
  - Information about the human genome

For encrypted communication secret crypto-key sharing between remote parties is large issue.

- By modern cryptography (guaranteed by numerical complexity)
  - Public-key crypto, Symmetric-key crypto
- By hand delivery (based on trust in human).

Also, it is difficult to detect eavesdroppers.

Ultimately secure key distribution technique is needed.

GCHQ: Government Communications Headquarters

© NEC Corporation 2016

QKD can be powerful option

Acronis press release

- Acronics announced partnership with IDQ to apply quantum-safe encryption to cloud system.

Acronis Partners with ID Quantique to Bring Quantum-Safe Encryption to Cloud Data Protection

Burlington, Massachusetts | September 28, 2015

http://www.acronis.com/en-us/pr/2015/09/28-12-24.html

NIKKEI ASIAN REVIEW

- Alibaba group and Chinese Academy of Science will collaborate on QKD.

October 15, 2015 2:19 am JST

Cybersecurity

Alibaba, Chinese academy team on quantum cryptography

WATARU KODAKA, Nikkei staff writer

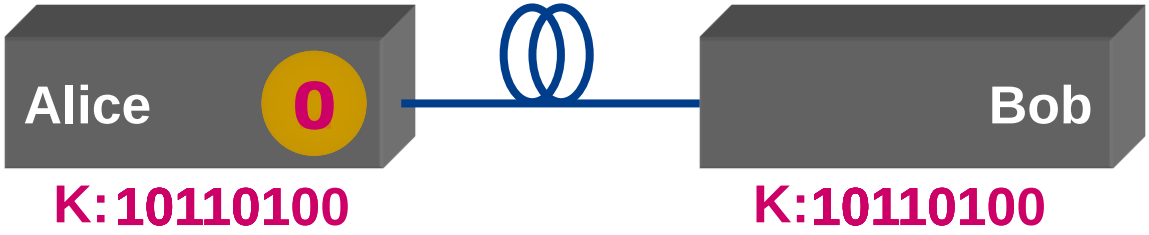
http://asia.nikkei.com/Business/Companies/Alibaba-Chinese-academy-team-on-quantum-cryptography

© NEC Corporation 2016

Quantum Key Distribution (QKD)

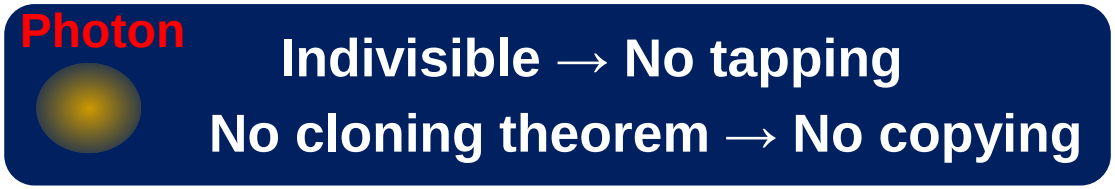
What is QKD?

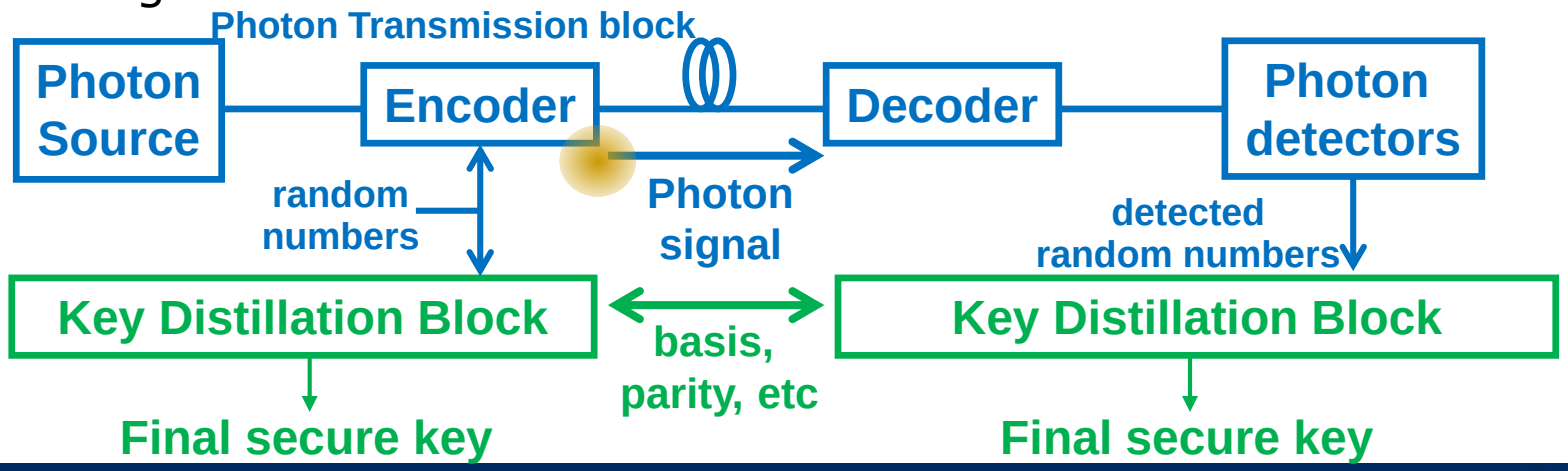
- Distribute crypto-key using single photons.
- Any eavesdropping attack can be detected.
- We can share the secure key. (Point to point link)



Typical System

- Block diagram





© NEC Corporation 2016

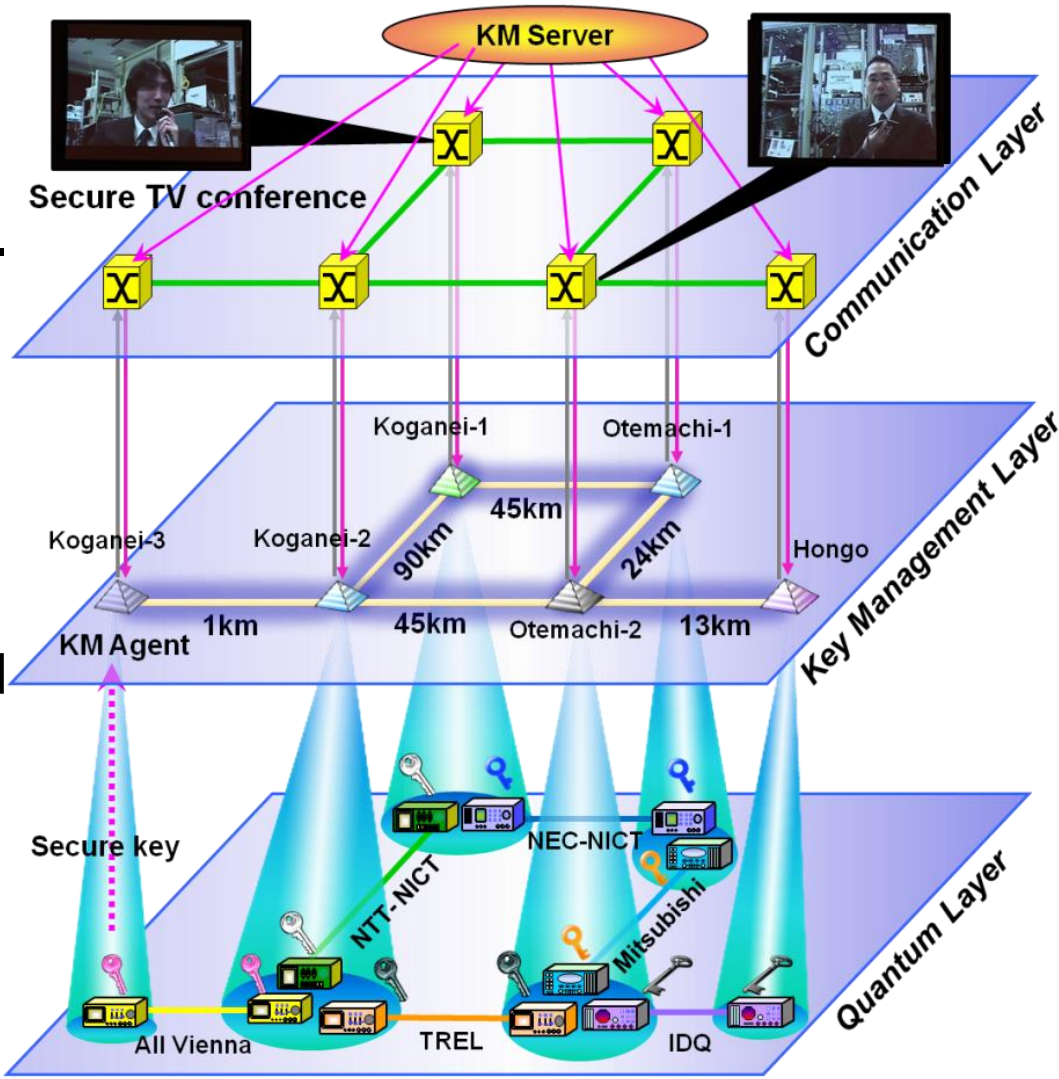
Tokyo QKD Network in 2010

Tokyo QKD Network in 2010

- QKD network with 6 nodes.
- Several kinds of QKD link.
  - NEC, TREL, NTT, All Viena, IDQ, Mitsubishi

Secure TV conference was demonstrated.

- Encrypted by one-time-pad (OTP) with quantum-key.
- Point to point (PTP) communication.
- Dedicated to the applications



To expand applications new network architecture, management and functions are needed.

© NEC Corporation 2016

Requirements for a Secure Network with QKD

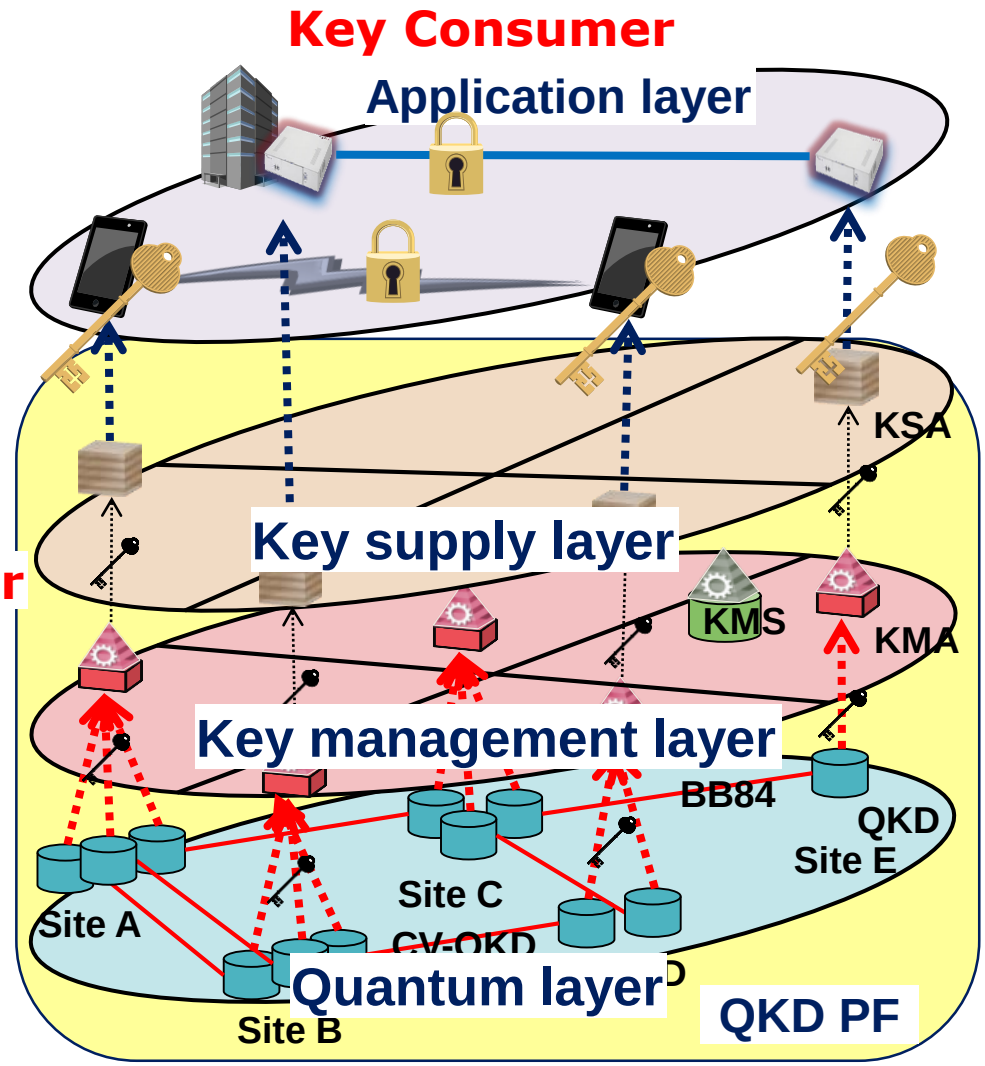
1. Application independent secure key supply.
   1. High-speed secure PTP communication
      - Between a data center and a remote backup center
   2. Multipoint-to-multipoint (MPTMP) communications
      - Secure smartphone communication between multiple terminals
2. Crypto-key management that corresponds to various types of QKD.
   1. BB84
      - NEC, Toshiba
   2. CV-QKD
      - Gakushuin Univ.
   3. RR-QKD, etc.

3. Support a wide variety of network topologies.
   1. Point to point
   2. Ring, Mesh, etc.

© NEC Corporation 2016

Quantum Key Distribution Platform (QKD PF)

- QKD PF: A QKD network with enhanced application interfaces.
- Three layer architecture.
  1. Key supply layer
  2. Key management layer
  3. Quantum layer
- "Key Supplier" and "Key Consumer" are separated.



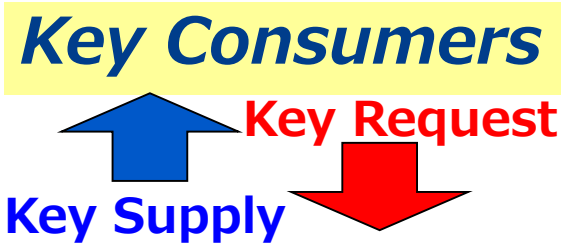
KSA: Key supply agent
KMA: Key management agent
KMS: Key management server

© NEC Corporation 2016

Functions of Each Layer with Key Format

Key supply layer

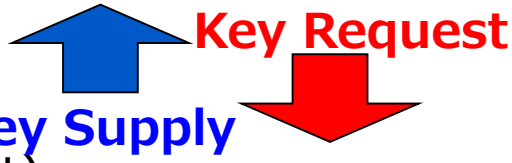
- Supply the key to the consumers corresponding to the requests.



KSA Key ID	Distribution Time	Key Size		Source "A"	Destination "C"	Application ID

Key management layer

- Store, relay (->see next slide), manage
- Performance monitor (error rate, key amount)
- Supply the key to the key supply layer.



Relay Information

KMA Key ID	Key Gen. Time	QKD Name "B"	Opposite QKD "C"	Key Size		Relay Time	Relay Source "B"	Relay Destination"A"

Quantum layer

- Each QKD link generates quantum-keys in its own way.

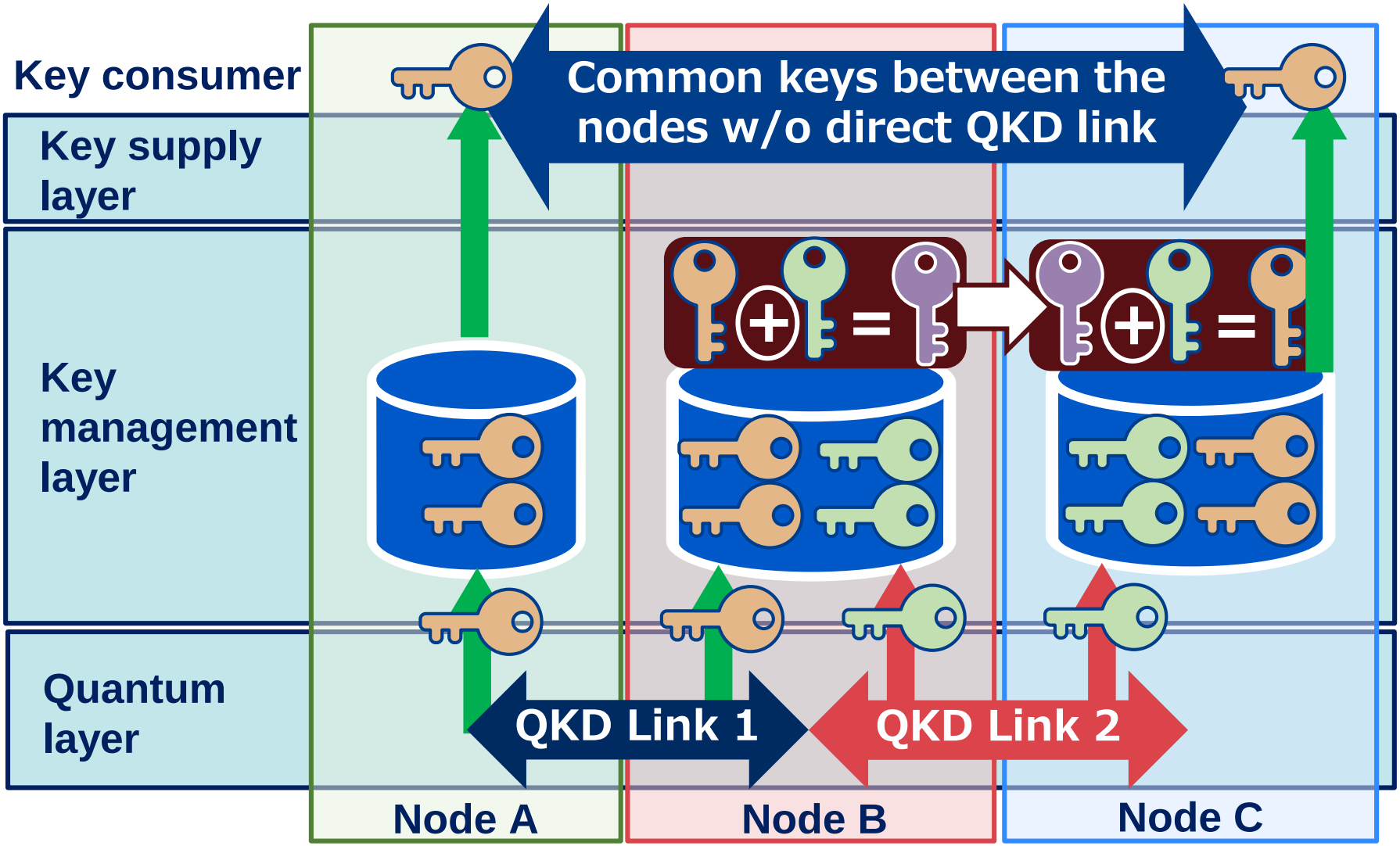
Sequence No.	Key Size	

Quantum key

© NEC Corporation 2016

Key Encapsulation Relay

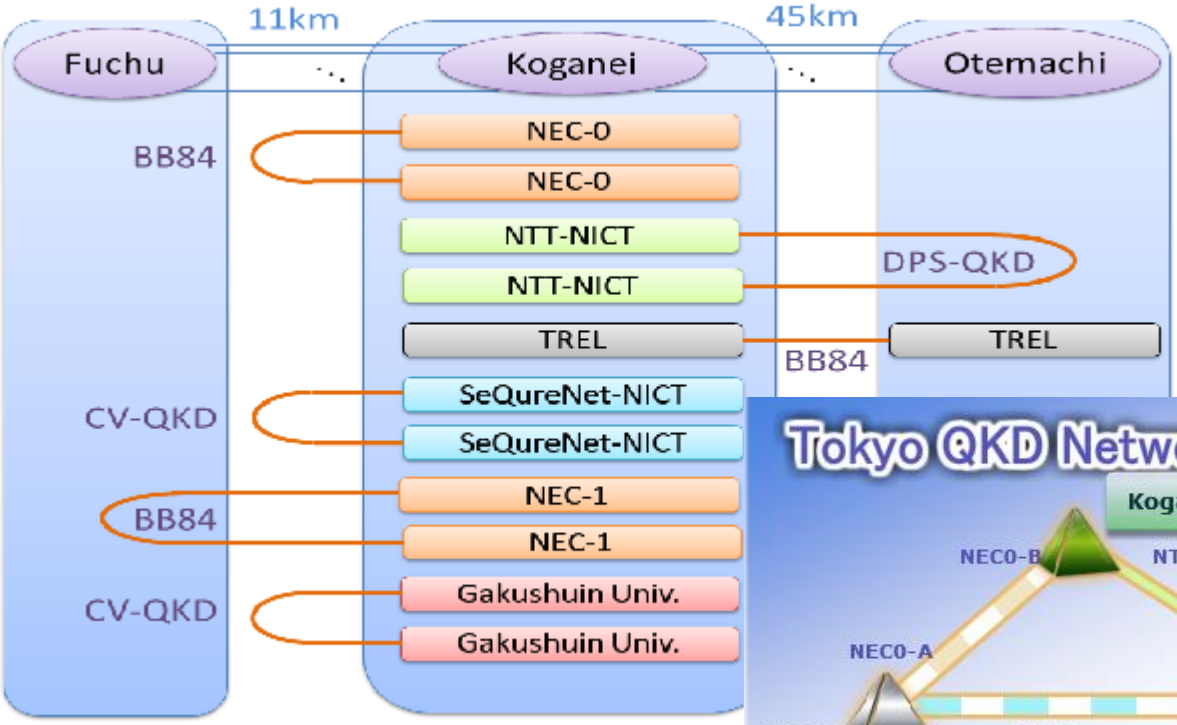
- Enables key sharing on a various network topologies.

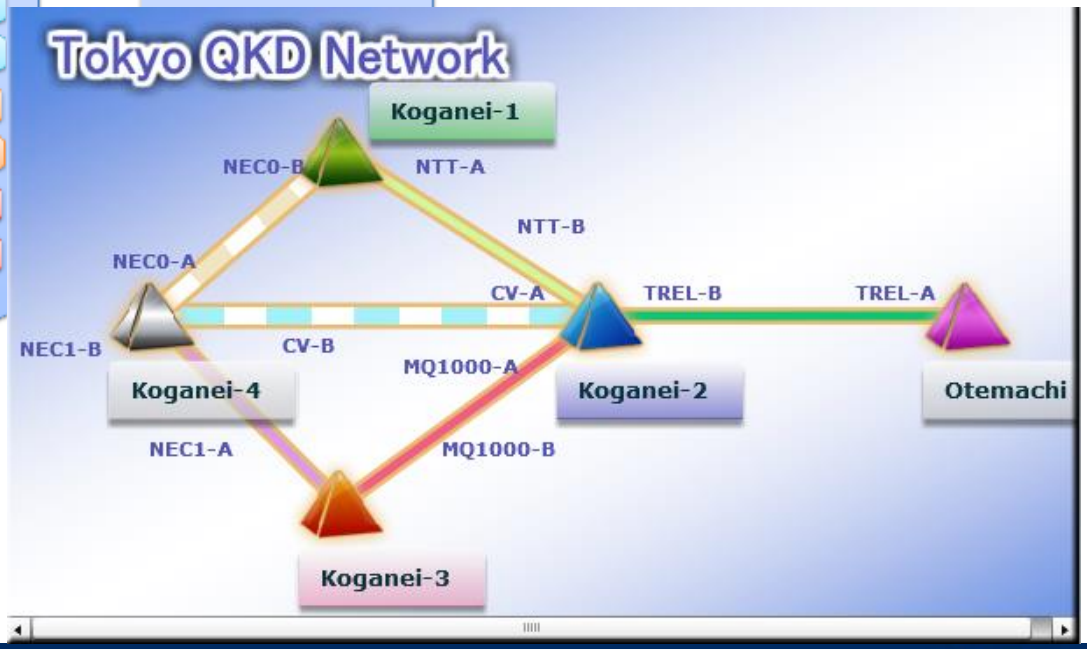


© NEC Corporation 2016

The Updated Tokyo QKD Network

- The Tokyo QKD Network was updated and has been operated on the network architecture.





URL: http://www.tokyoqkd.jp/

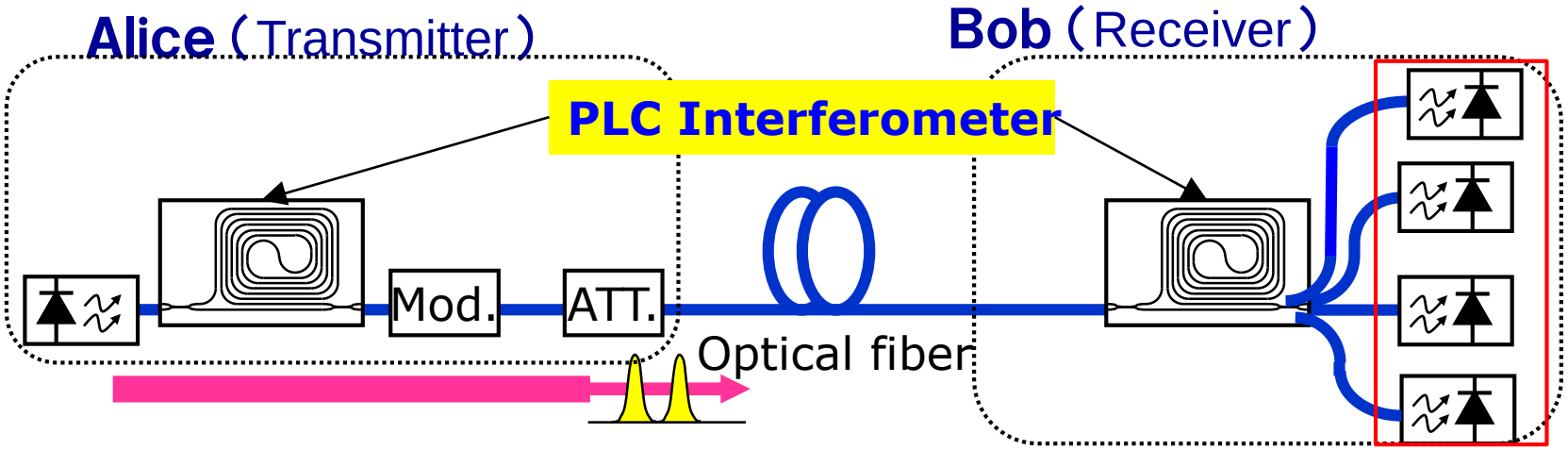
© NEC Corporation 2016

Robust QKD System

Key technology

- PLC* optical interferometer (NEC's original)
  - Stable photon transmission without environmental fluctuations.
    - –Temperature independent.
    - –Polarization of optical signal independent.
  - Mechanical device free
    - –Without polarization controller and fiber stretcher.
    - –Reliable.
    - –Telecom operator requires high reliability.

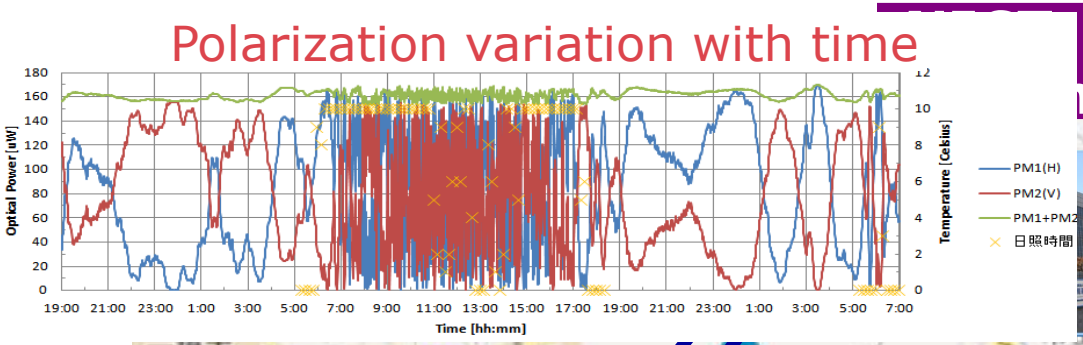
* PLC: Planar Lightwave Circuit



Stable photon transmission without mechanical device is achieved.

© NEC Corporation 2016

Environmental Fluctuations Independent Operation



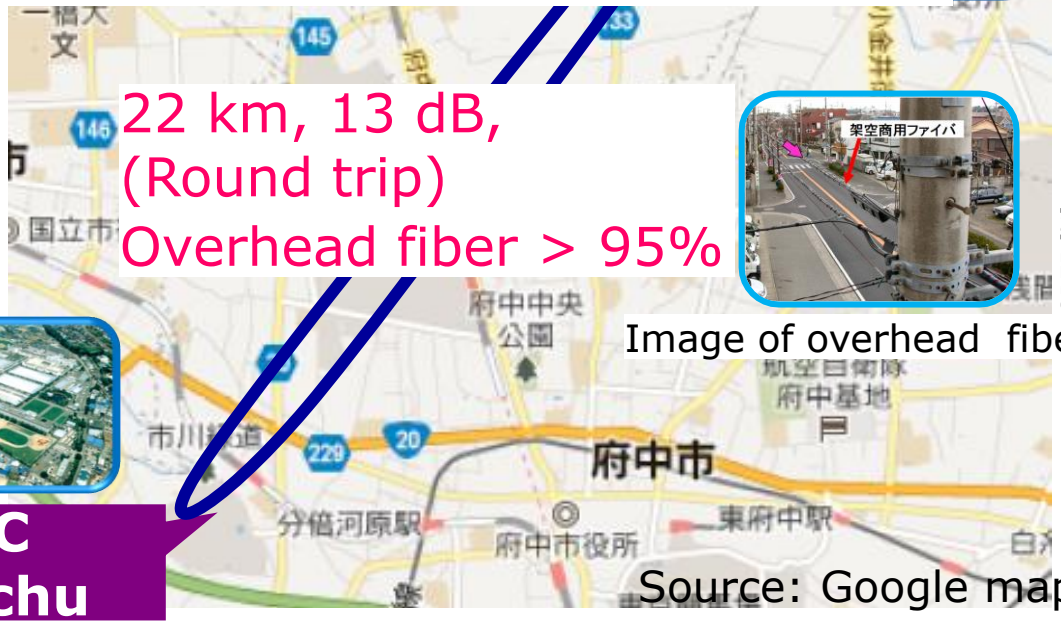
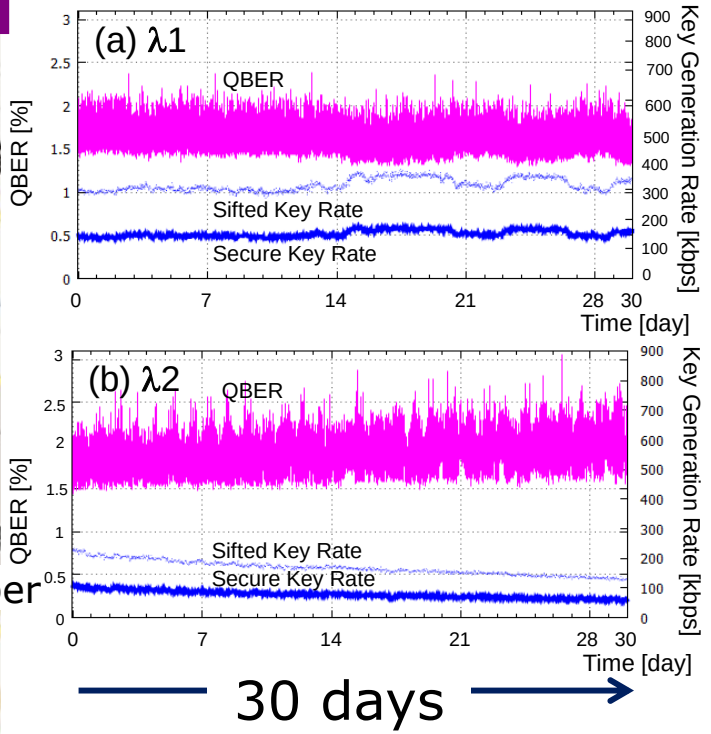


Image of overhead fiber



	QBER [%]	Sifted Key	Secure Key
2λ Total	1.70	483.3 kbps	112.4 kbps

K. Yoshino et al., Optics Express, Vol. 21, Issue 25, pp. 31395–31401, 2013.

© NEC Corporation 2016

Introductory Video

https://www.youtube.com/watch?v=AETUdYLgpYY&feature=youtu.be

© NEC Corporation 2016

Long-term Field Test in "Cyber Security Factory"

Cyber Security Factory

- Core facility for our counter-cyber-attack activities
  - 24/7 network monitoring
  - Cyber incident analysis
  - Gathering cyber intelligence

Deployed QKD system and carried out long-term field test

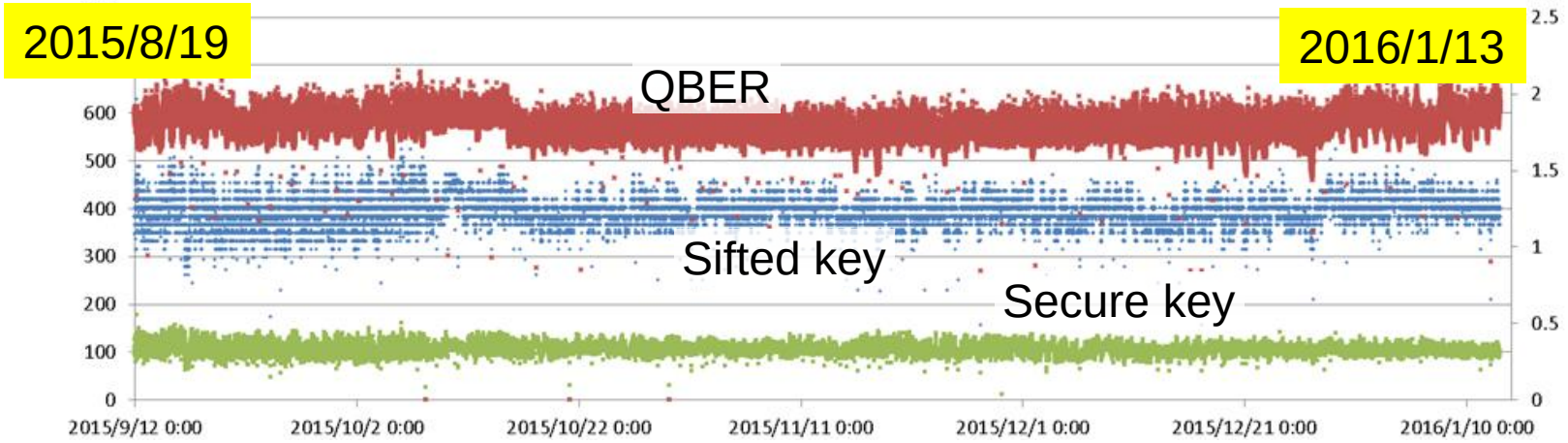
- "QKD-AES Hybrid System"
  - Secure keys are provided for AES encryptor "COMCIPHER" for high-speed transmission.
- Environment
  - Alice in machine room
  - Bob in office area condition

Cyber Security Factory

© NEC Corporation 2016

21-week Test Results

Cyber Security Factory（1λ） 21 week



	QBER [%]	Sifted key rate	Secure key rate
1λ	1.79	393.2 kbps	107.7 kbps

- Under the practical environmental condition
- Secure key rate: 107.7 kbps (@11.5 dB loss)
- Standard deviation: ±8.6%

Consecutive stable operation for 21 weeks was achieved

© NEC Corporation 2016

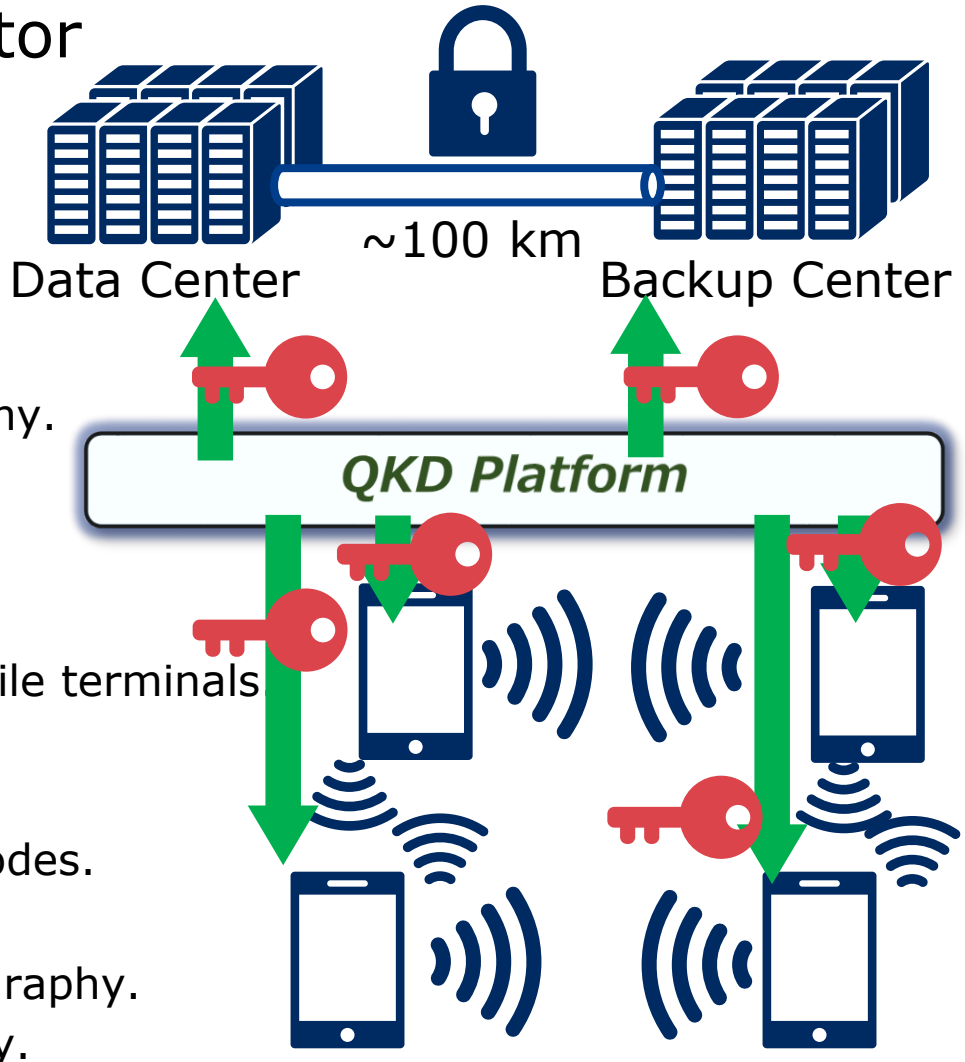
Applications on the QKD PF

1. Layer 2 Network Encryptor

- Technical issues
  - Large capacity communication.
  - Consumption of secure key is large.
  - Long distance communication.
- Approach
  - Integration with modern cryptography.
  - Key relay to support long distance.

2. Secure smartphone

- Technical issues
  - Limited key storage capacity in mobile terminals
  - Support MPTMP communications.
  - Authentication of mobile terminals
  - Key distribution between any two nodes.
- Approach
  - Integration with the modern cryptography.
  - Authentication with the quantum key.
  - Key relay to support MPTMP.

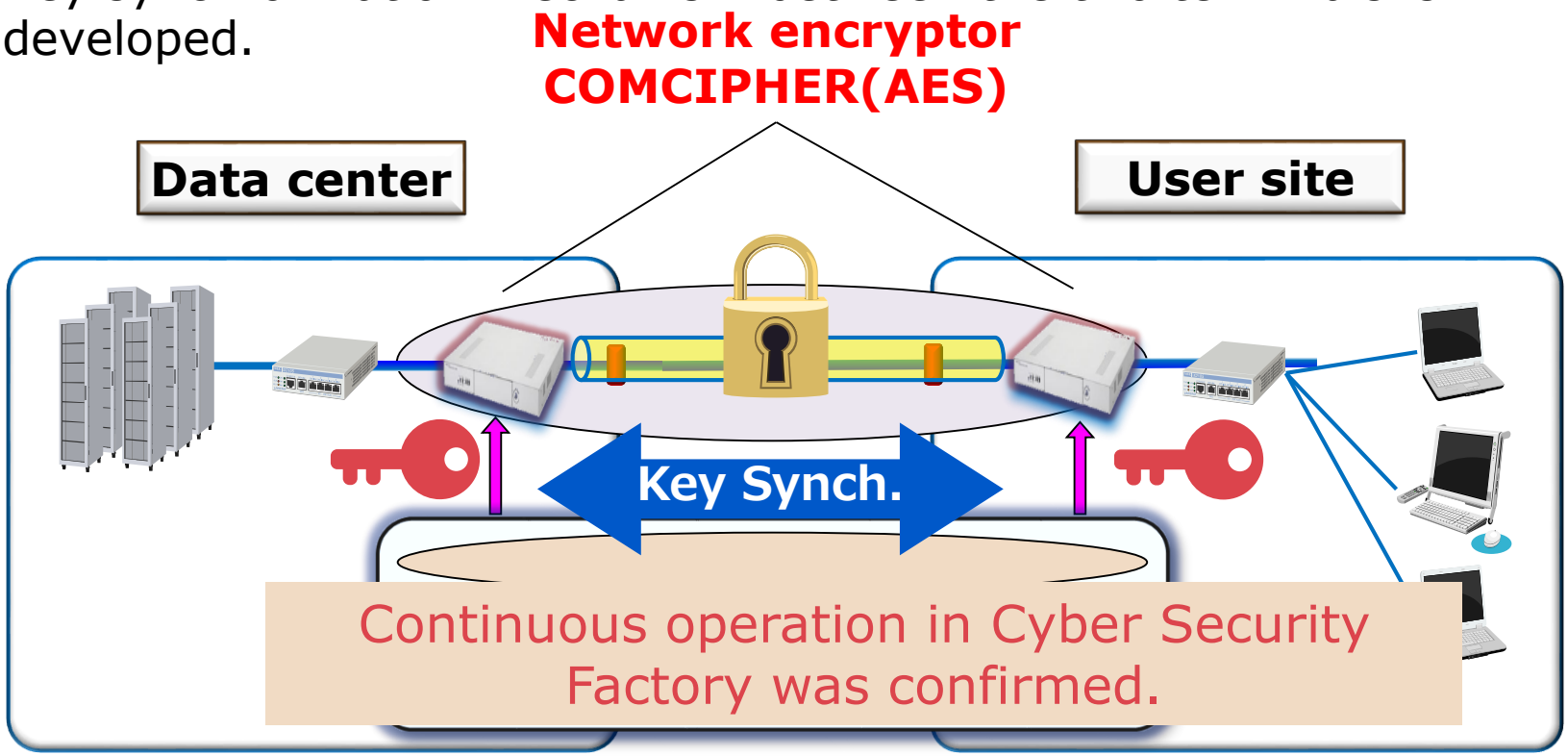


© NEC Corporation 2016

QKD-AES Hybrid System

Integration with NEC's layer 2 network encryptor "COMCIPHER(AES)"

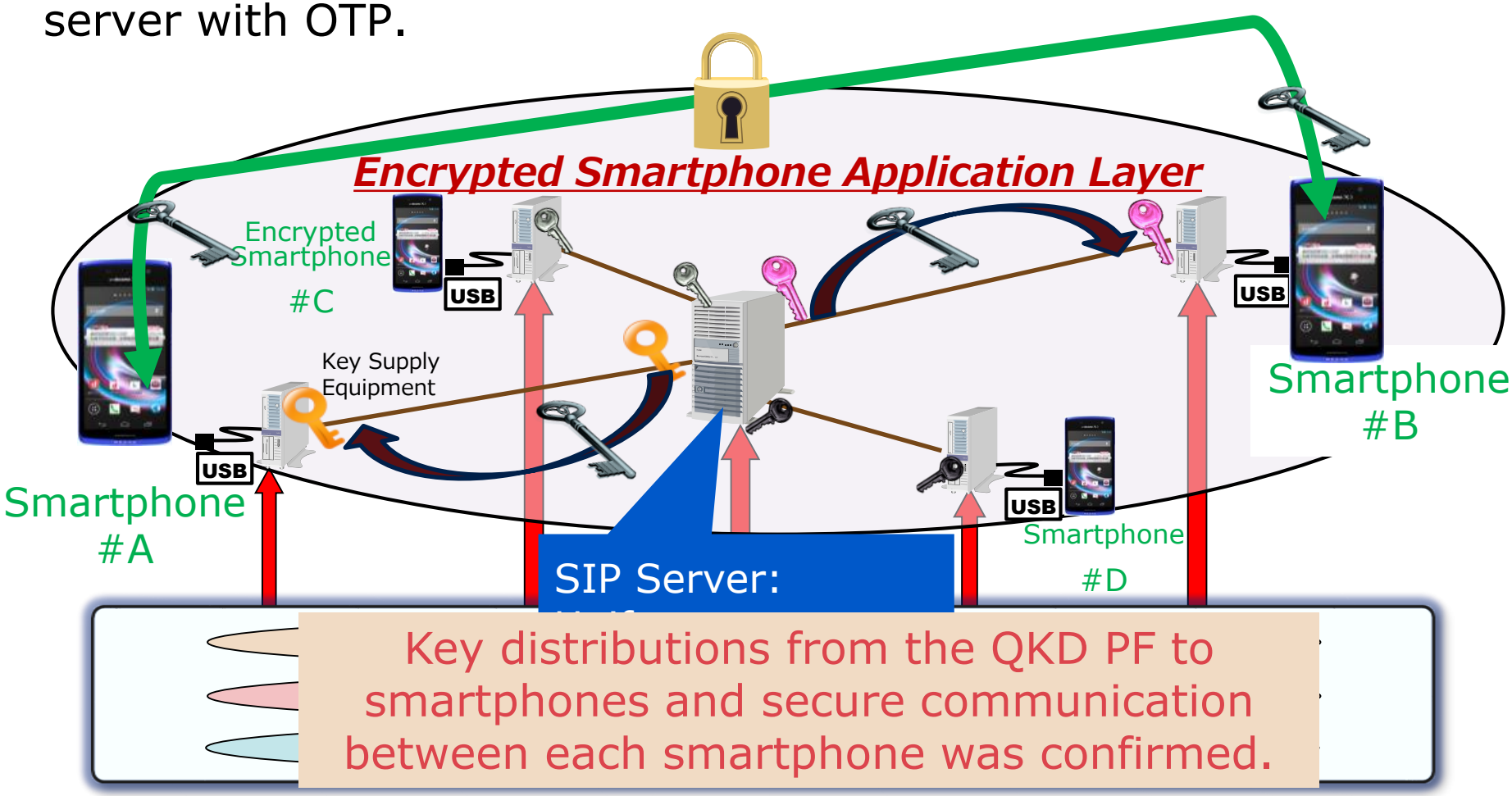
- Data over Ethernet are encrypted with AES.
- AES key is periodical refreshed by the quantum key from the QKD PF.
- Key synchronization mechanism between the two terminals is developed.



© NEC Corporation 2016

Secure Smartphone for Multiuser

- Call sessions are encrypted with AES.
- Quantum keys are used for authentications and AES symmetric key deliveries. AES symmetric key is delivered from center server with OTP.



© NEC Corporation 2016

Summary

The basic architecture and functions of a QKD network are explained.

- Quantum Key Distribution Platform.
  - 3-layer architecture
- Robust QKD System integral for QKD network.
  - Long-term and highly stable operation was achieved.
- Applications on the QKD Platform.
  - QKD-AES hybrid system
  - Secure smartphone system

Secure communication infrastructure with these technologies will be constructed in the near future.

Tokyo QKD Network at present.
URL: http://www.tokyoqkd.jp/

© NEC Corporation 2016

Thank you for your attention.