December 10-14, 2018
ITU-T TSAG
Geneva

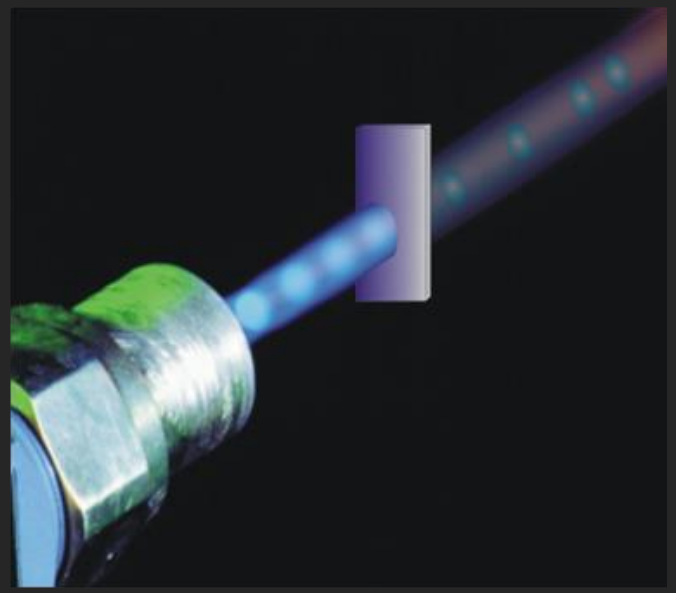
Introduction to Quantum Information Technology and Network Evolution

Kai Chen

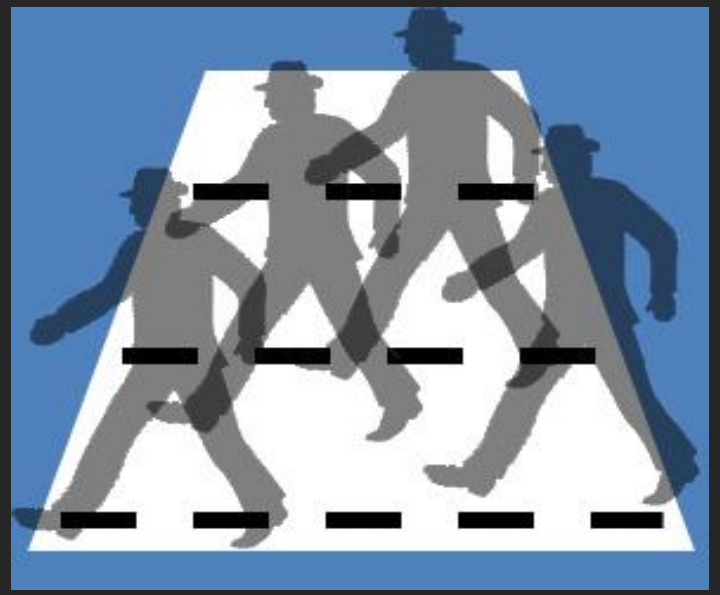
University of Science and Technology of China

Quantum Information Technology Overview

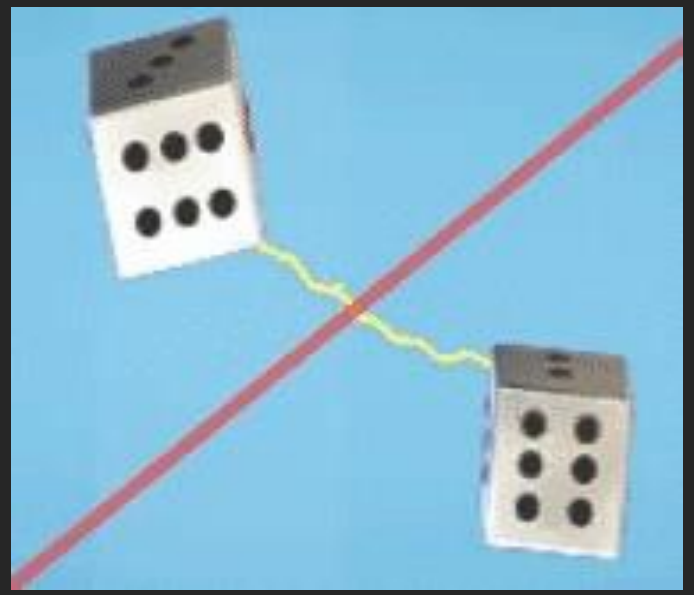
Characteristics of the quantum world



Energy quantization indivisibility of single photon

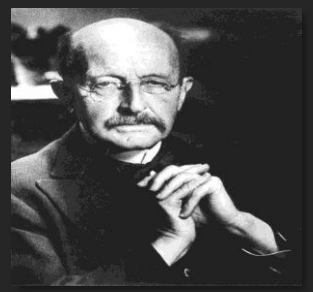


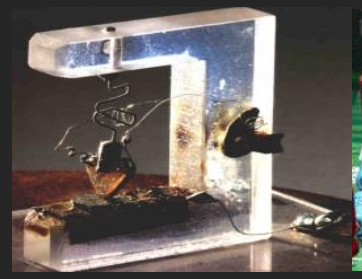
Quantum superposition

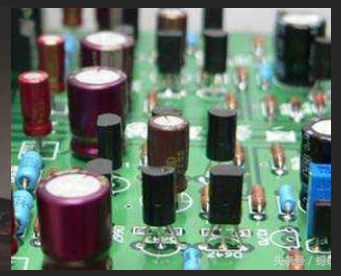


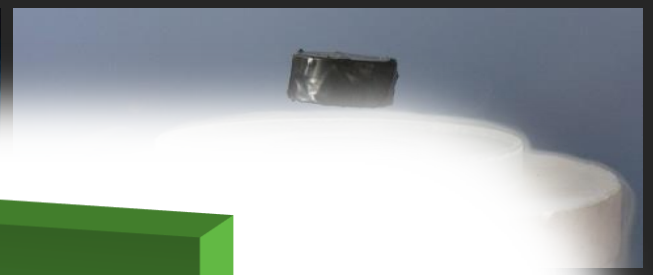
Quantum entanglement nonlocality

Applications of quantum theory: The first quantum revolution









Plank's quantum theory

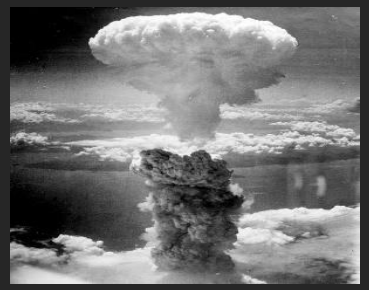
Transistor

1895 1900 1945 1947 1960 1973 19

Top-down: Passive observation and macroscopic manifestation of quantum principles

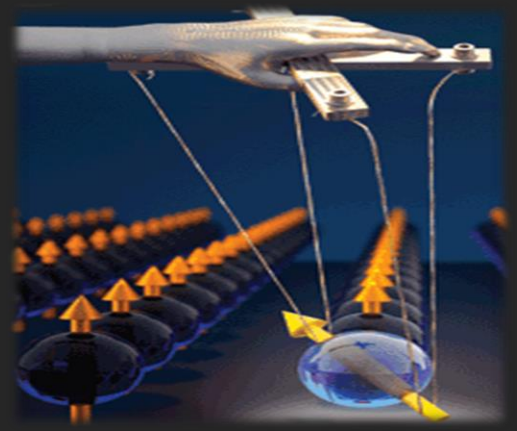
X-ray

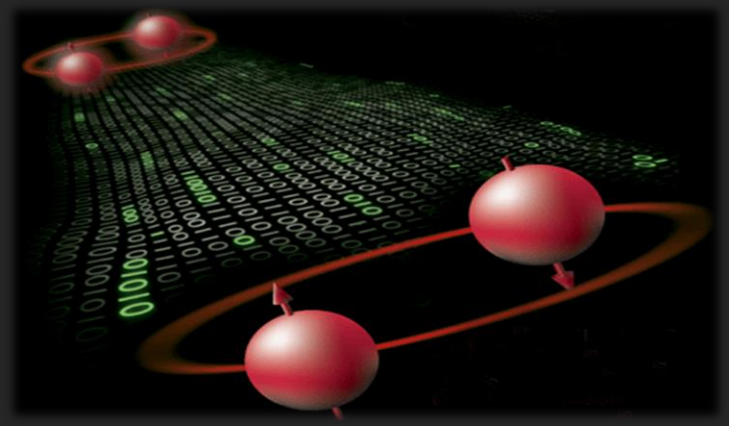
Atomic boom



Applications of quantum theory: The second quantum revolution

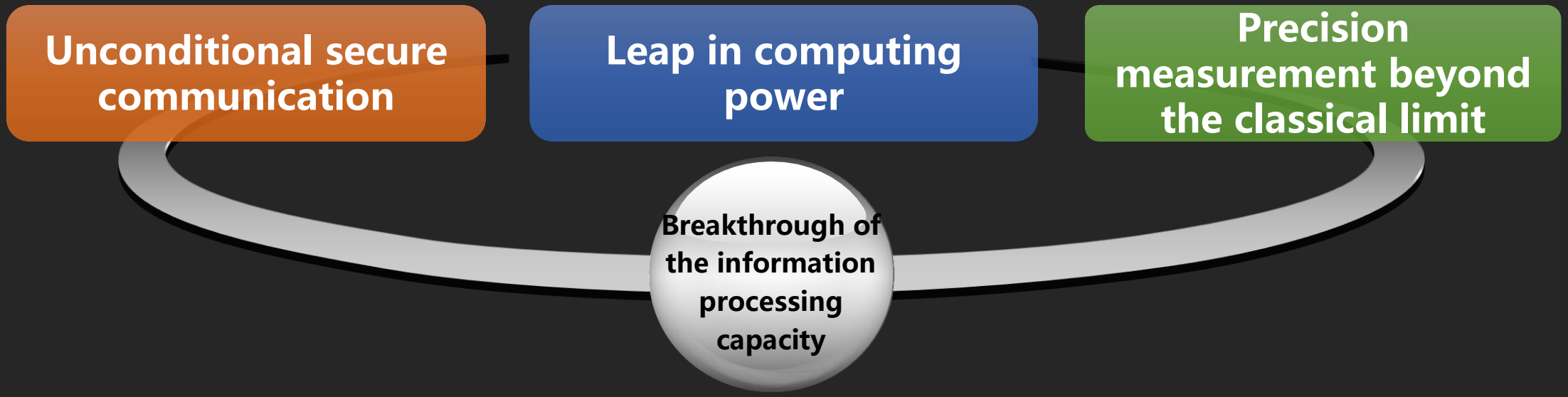
Bottom-up: **Active manipulation of single quantum particle and interaction between multiple quantum particles.**





Quantum information technology

Quantum Information Technology



Quantum Information Technology

Quantum Communication

Quantum Computing/Simulation

Quantum Metrology/Sensing

Quantum Computation

Shor's Algorithm (1994):

E.g. factor a 300-digit number with

- Classical THz computer: 150,000 years
- Quantum THz computer: 1 second!

- Code-breaking can be done in minutes, not in millennia
- Public key encryption, based on factoring, will be vulnerable!

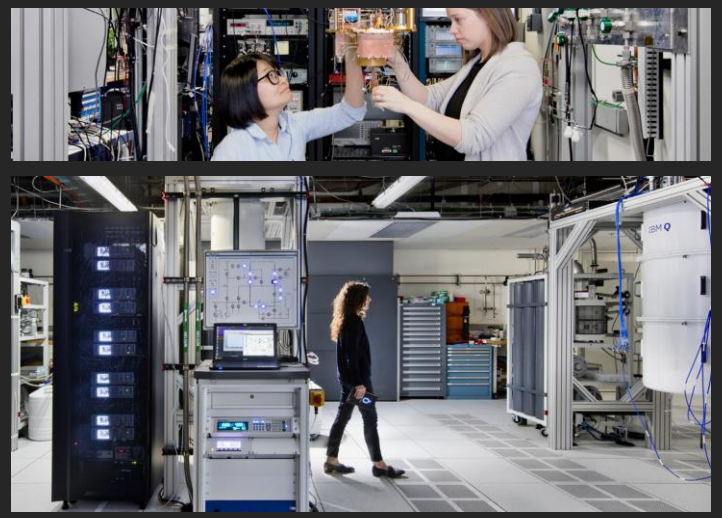
Code-breaking

Weather forecast

Financial analysis

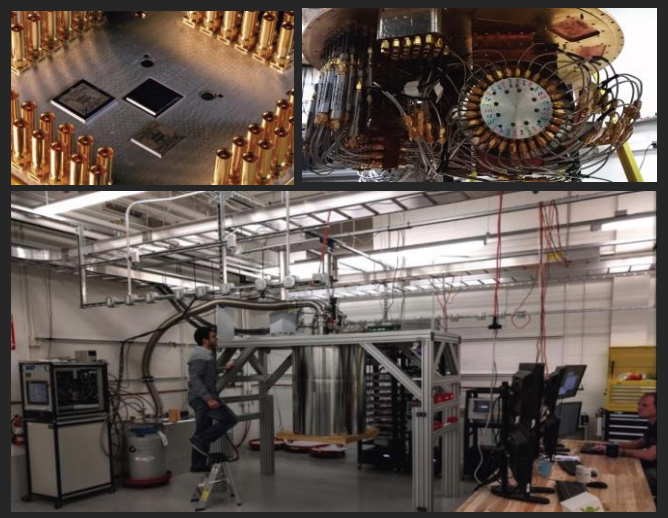
Drug design

Quantum Computation



IBM

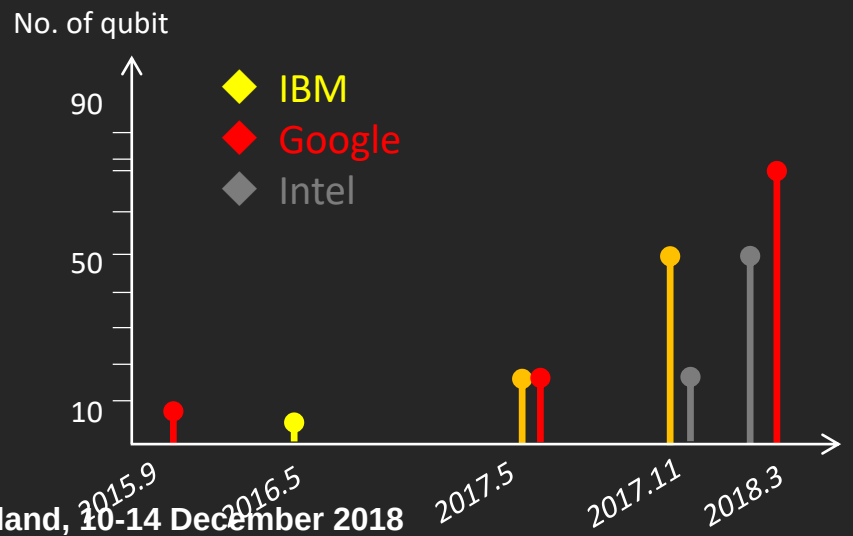
VS



Google

VS

Intel

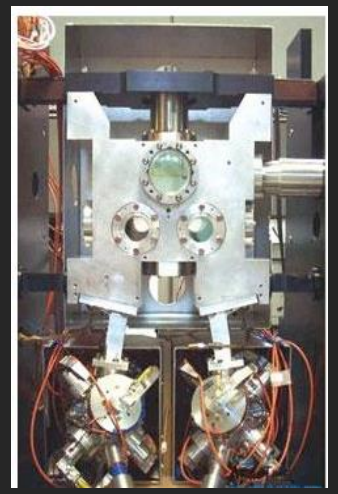


Quantum supremacy

- Readout error: 1%
- Single-qubit gate error: 0.1%
- Two-qubit gate error: 0.6%
- No. of qubits: 50

Quantum Metrology

Atomic accelerometer

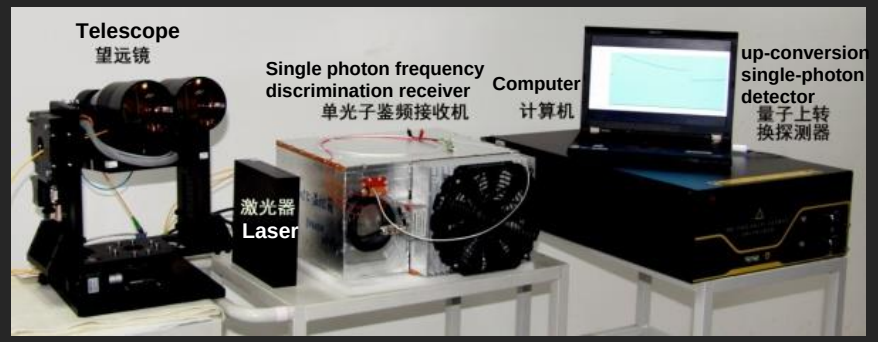


Atomic gyroscope

Quantum superposition → Quantum interference

Measurement of (gravity) acceleration by Atomic interferometer: $6.7\times10^{-12}g$

Application to high-precision autonomous navigation



Single-photon detection strengthened laser radar

Improve the laser radar range and detection sensitivity with a single photon detector, and improve the weak energy detection capability by 2-4 orders of magnitude or more.

Quantum Communication

- Definition: technology that encode/decode and transmit information via quantum state

Encode information into the quantum state of photons,

e.g., polarization degree of freedom

Quantum Communication

- Definition: technology that encode/decode and transmit information via quantum state

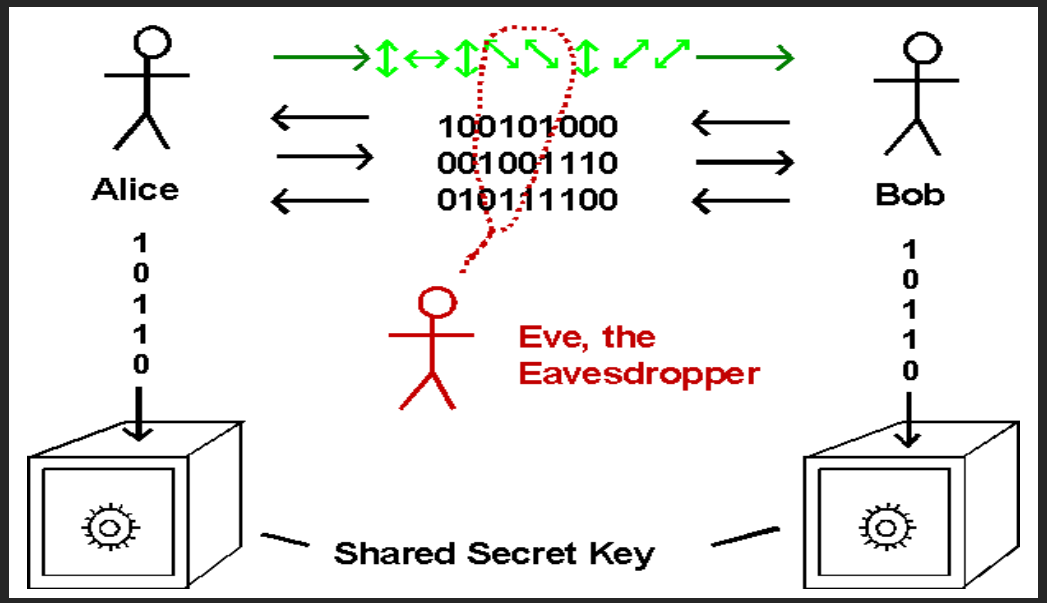
Quantum key distribution

Quantum teleportation

Others …

Quantum Key Distribution (QKD)

- Single-photon-based key distribution: [Bennett & Brassard 1984 protocol]



Unconditional secure in principle

Any eavesdropping will be detected

➡ Secure key!

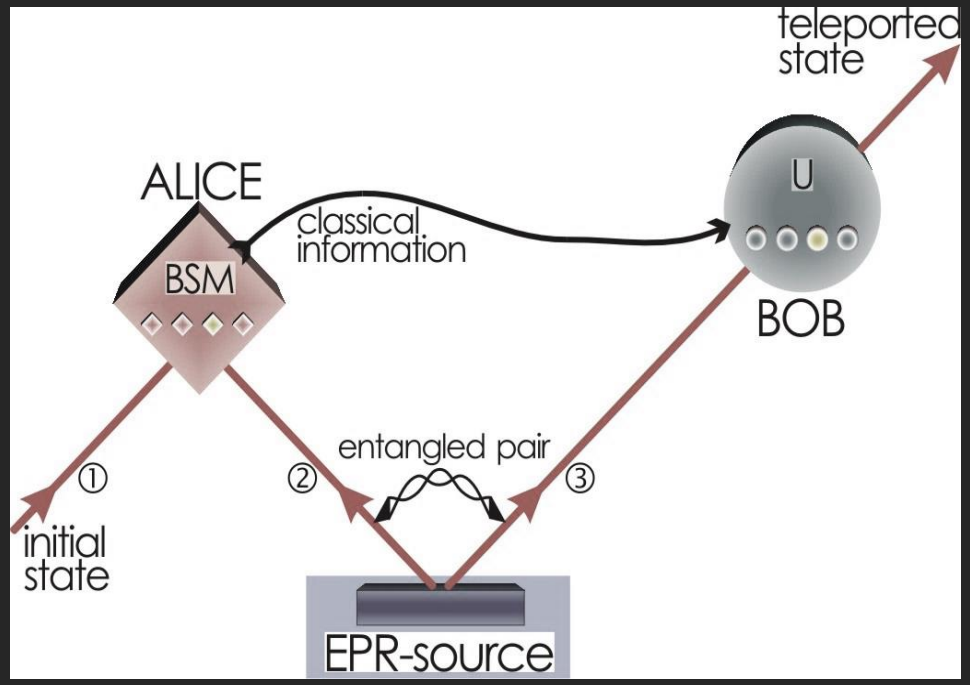
One-time pad encryption

➡ Unhackable!

- Entanglement-based key distribution: [Ekert, PRL 67, 661 (1991)]

Quantum Teleportation

- Transmit quantum state via pre-shared entangled pair

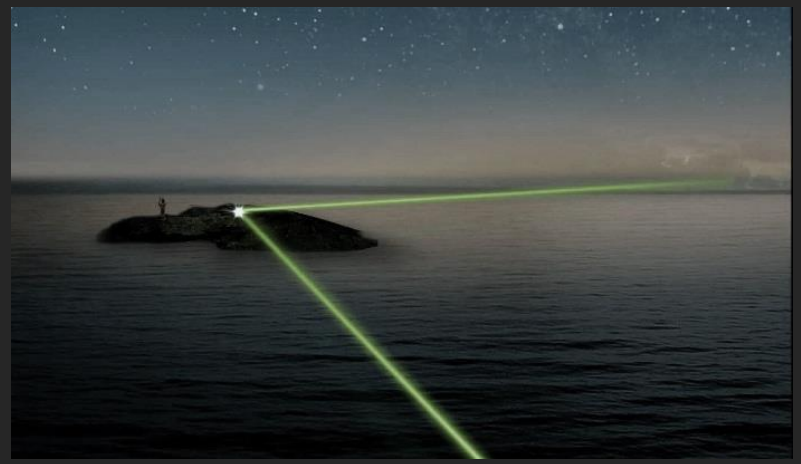


Bennett *et al.*, PRL 73, 3801 (1993)

Essential ingredient for distributed quantum network

Towards Long-distance Quamtum Communication

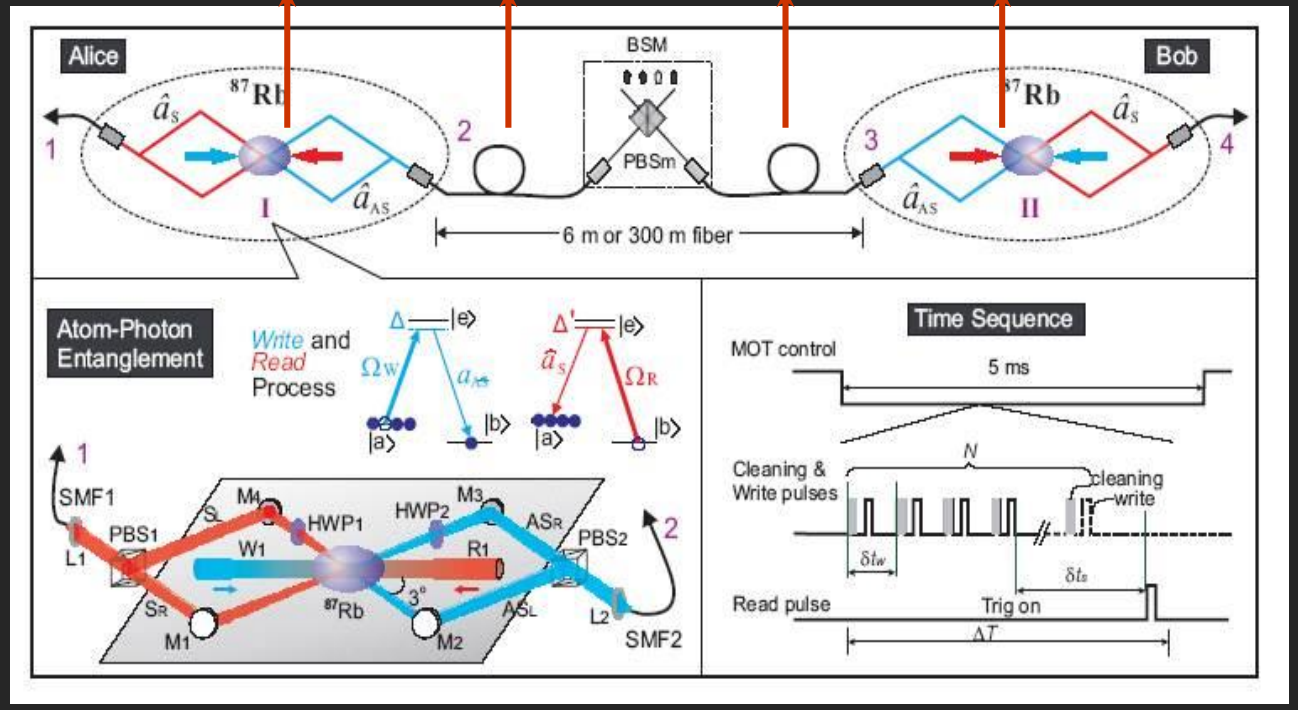
- Records of long-distance QKD in fiber:
  - Boris *et al.*, Nature Photonics 9, 163–168 (2015) ~300km
  - Yin *et al.*, PRL 117, 190501 (2016) ~400km
- Records of long-distance quantum teleportation:
  - Yin *et al.*, Nature 488, 185 (2012), by Chinese group ~100km
  - Ma *et al.*, Nature 489, 269 (2012), by Austrian group ~100km



Communication distance and be further increased by developing quantum repeaters

Quantum Repeater Nodes

Atom-Photon entanglement Atom-Photon entanglement



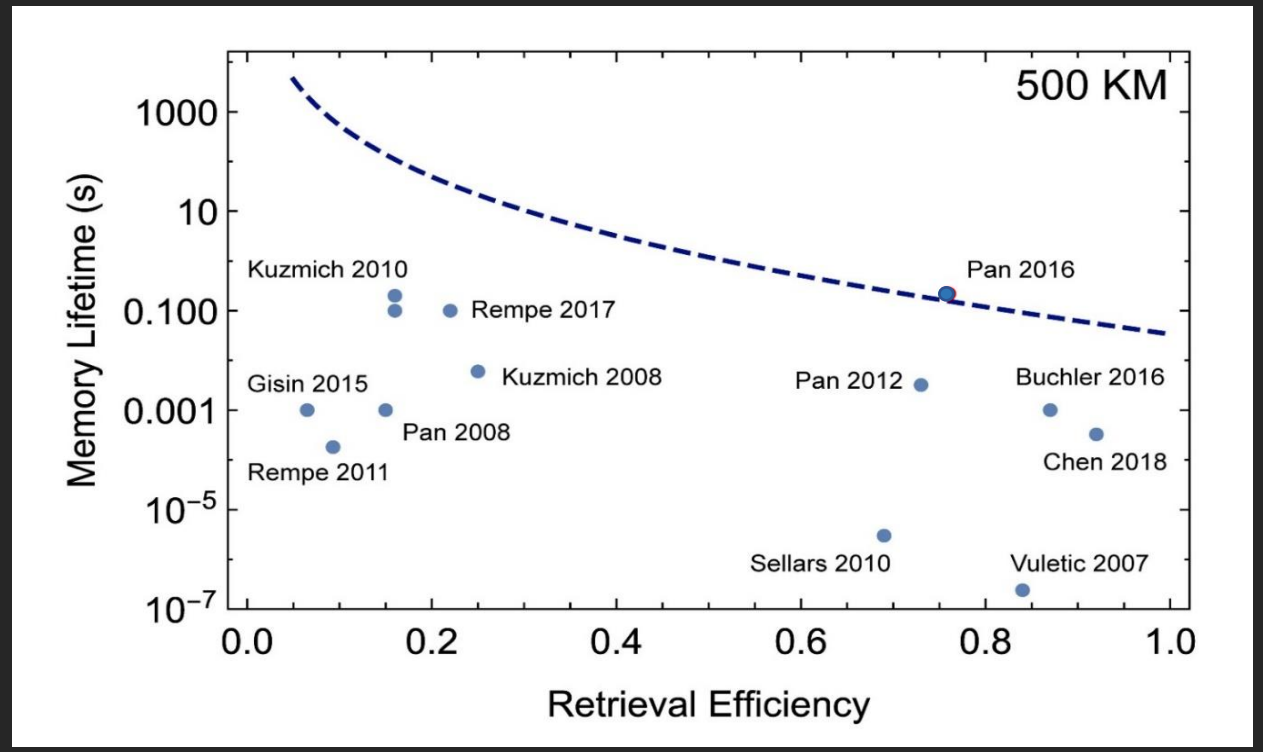
Robust BDCZ quantum repeater with atomic quantum memories

- Scheme: Zhao *et al.*, PRL 98, 240502 (2007)
- Experiment: Yuan *et al.*, Nature 454, 1098 (2008)

Efficient and Long-lived Quantum Memory

Long lifetime: storage time must be long enough to ensure every node creates an entangled pair

High retrieve efficiency: the stored quantum state must be converted into photon with sufficient high efficiency to establish remote entanglement



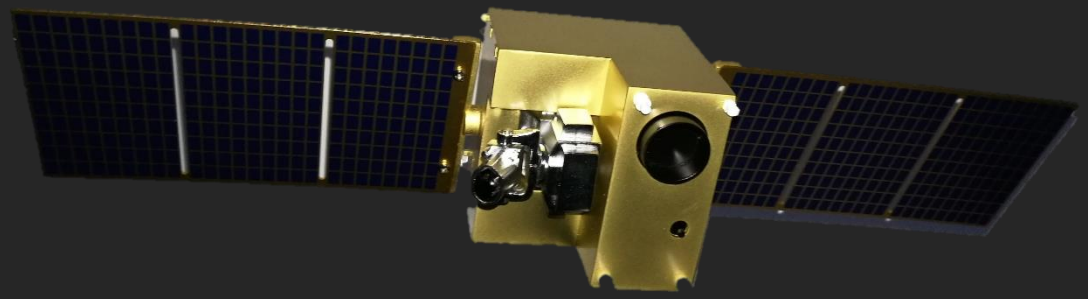
☑ Support quantum repeaters enabling quantum communication at a range of ~500km

More Efficient Way: Free-Space Quantum Communication

- ☑ Non-obstruction from terrestrial curve and barrier
- ☑ Effective thickness of atmosphere is only ~10km
- ☑ No decoherence in outer space

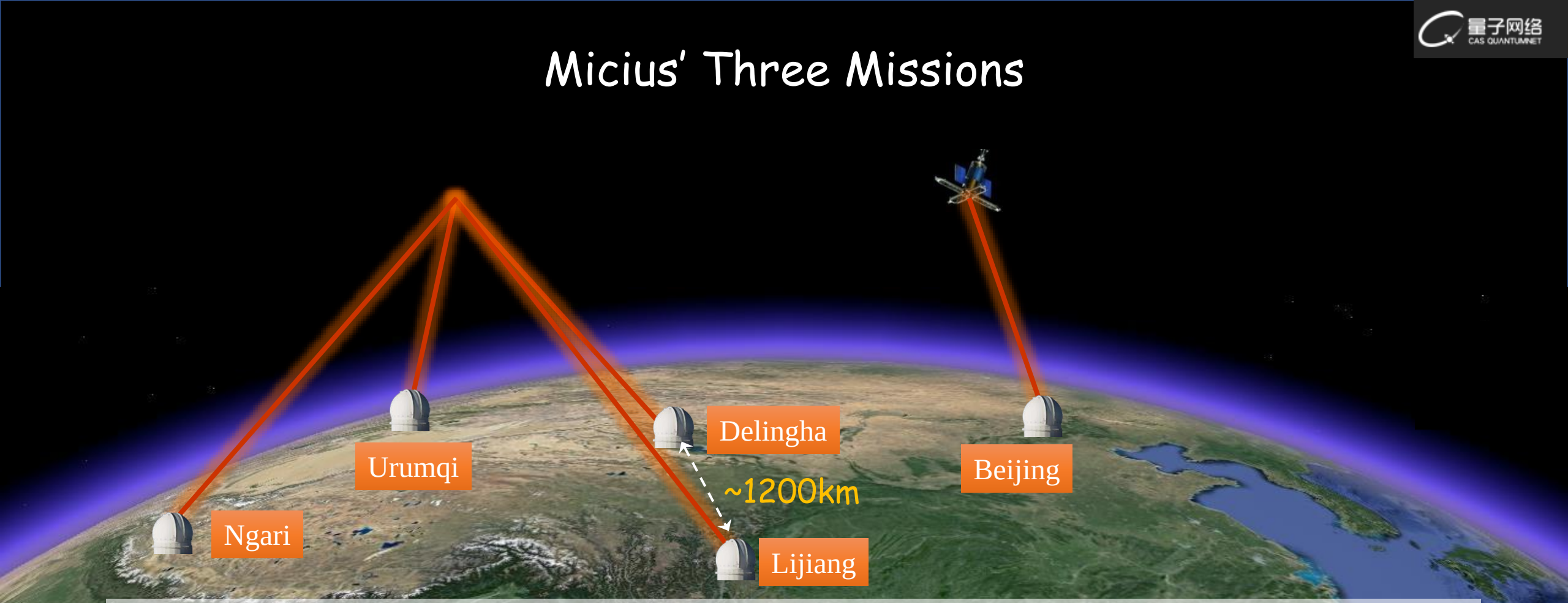
Quantum Science Satellite "Micius"

Launched on 16th Aug, 2016 in Jiuquan Satellite Launch Center



- Weight: ~640kg
- Power: 560W
- Sun-synchronous orbit, altitude 500km

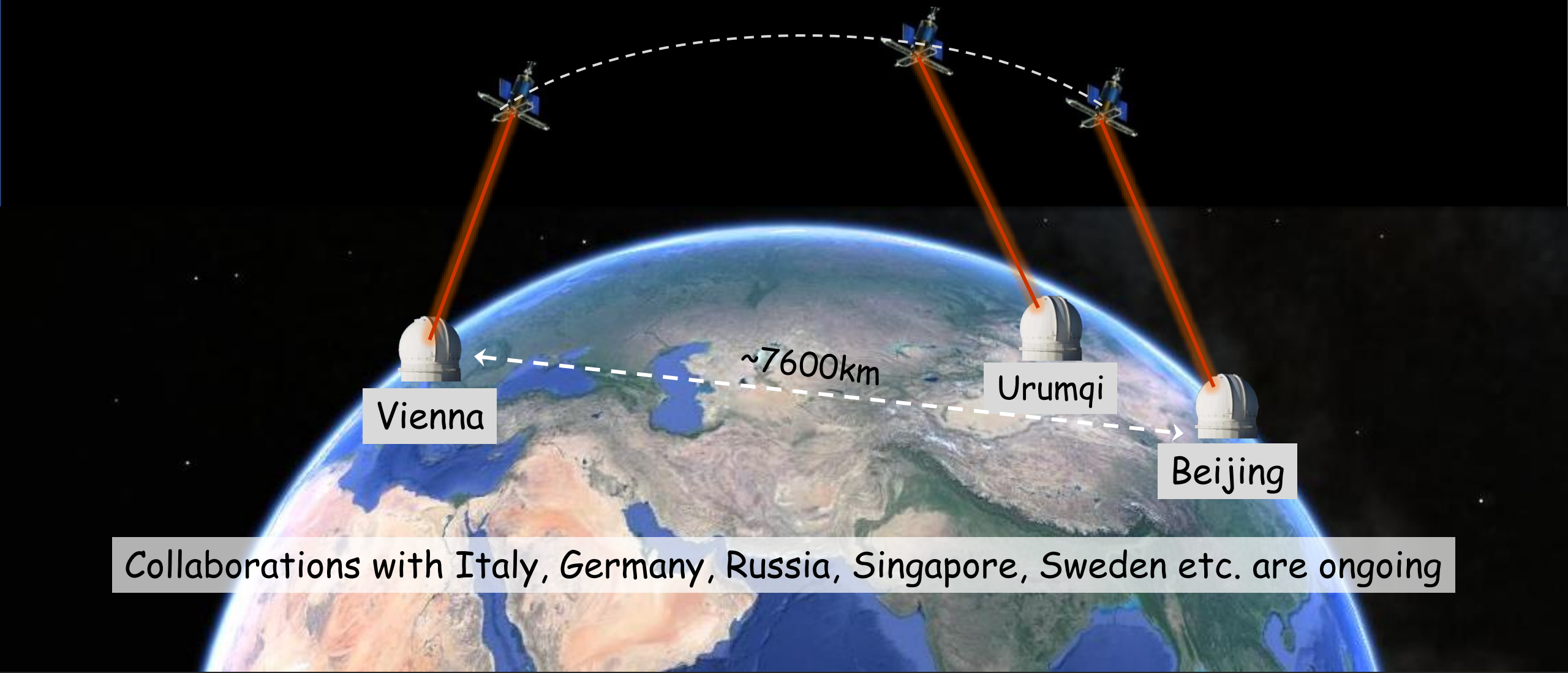
Micius' Three Missions



- QKD between satellite and ground, key rate ~1kbps (recently ~400kbps) ➡ 20 orders of magnitudes higher than using fiber channel at 1200 km [Nature 549, 43 (2017)]
- Quantum entanglement distribution from satellite, test of quantum nonlocality under strict Einstein's locality condition [Science 356, 1140 (2017)]
- Quantum teleportation between ground and satellite [Nature 549, 70 (2017)]

Intercontinental Quantum Key Distribution

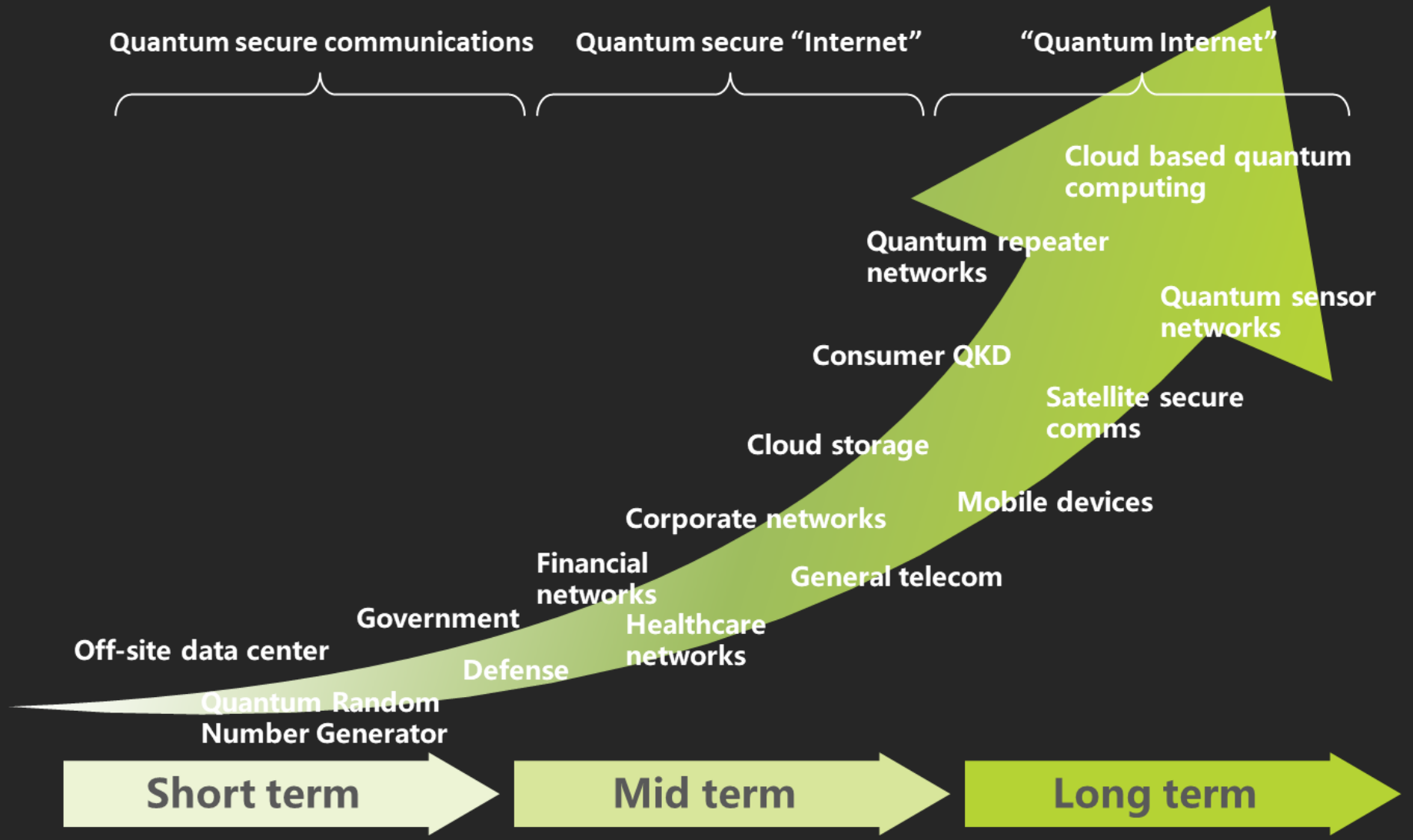
Satellite as a trusted relay [Liao *et al.*, PRL 120, 030501 (2018)]



Collaborations with Italy, Germany, Russia, Singapore, Sweden etc. are ongoing

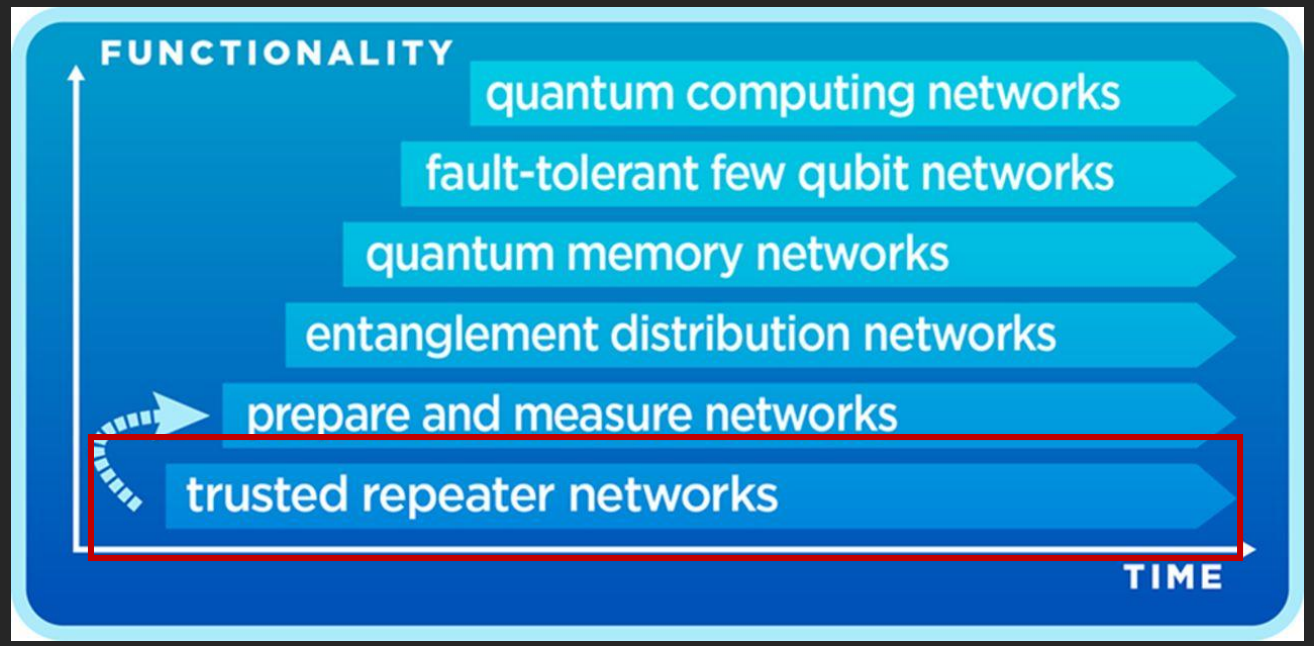
Quantum Information Network Evolution

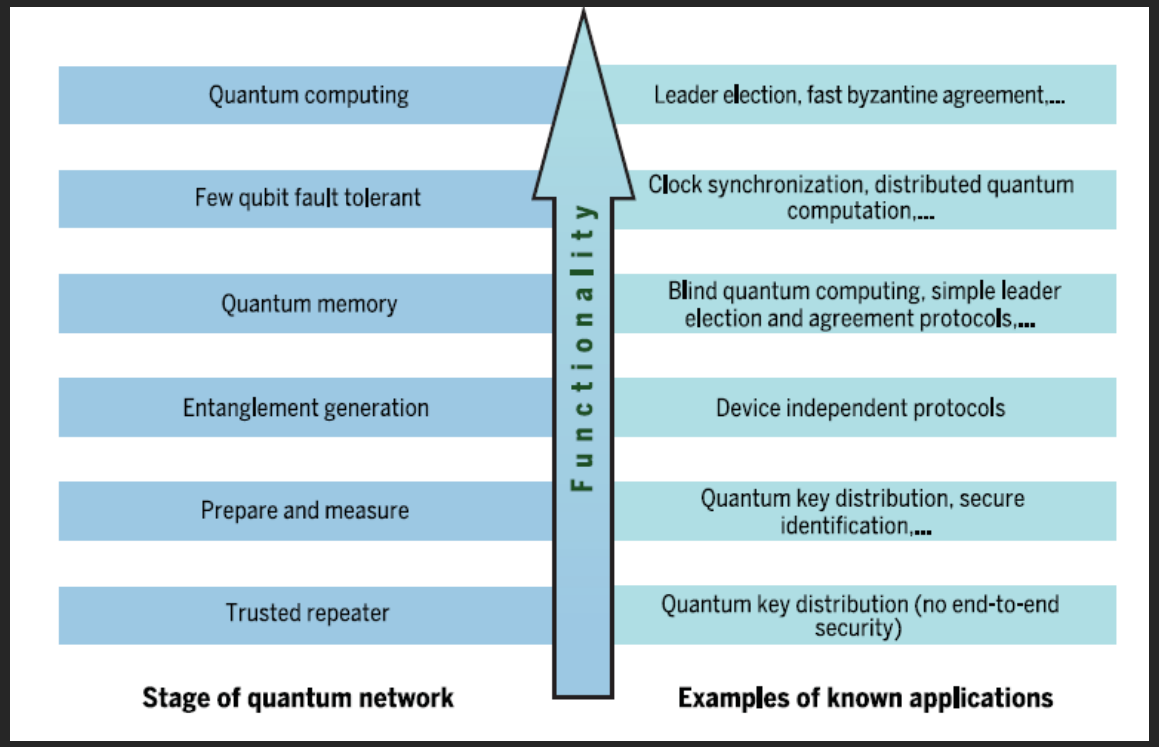
Applications of Quantum Communication



from "The Quantum Age: technological opportunities", the Government Office for Science, UK (2016)

Quantum-Information-based Network Evolutions





Stages in the development of a quantum internet

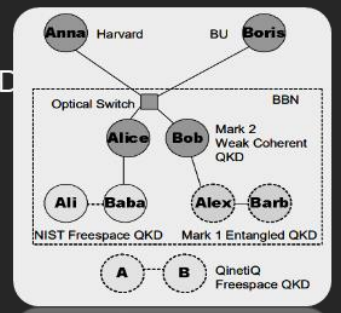
* Wehner, Stephanie, David Elkouss, and Ronald Hanson. "Quantum Internet: A Vision for the Road Ahead." *Science 362, no. 6412 (2018).*

QKD Networks: a glance from theory to practice

1984
Bennett & Brassard Invent BB84 Protocol

1989
IBM: first lab test for quantum information transmission（32cm）

2003
US: DARPA QKD network with 10 nodes



2016: “Micius” quantum satellite launched

EU: SECOQC network initiated, finished at 2008

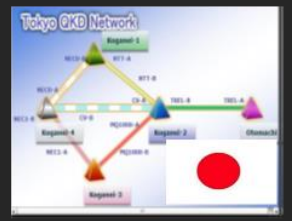
2004

2005: Decoy-state solution proposed to extend QKD to more than 100KM *

2008
Hefei 3 nodes telephone network (20KM)

2009
- Hefei 5 nodes full-pass QKD network
- Geneva QKD network
- Madrid QKD network

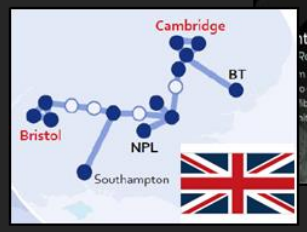
2010
JP: Tokyo QKD network

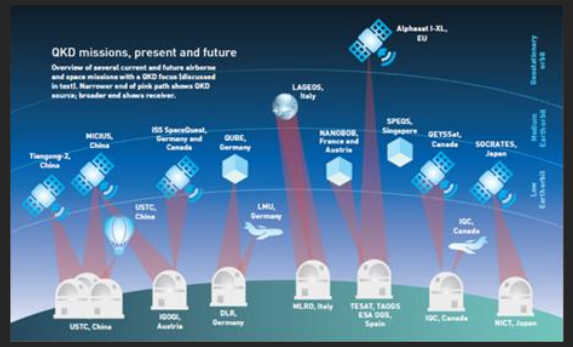


2012
Hefei QKD metro network (46 nodes)

2013
- Jinan metro QKD network (56 nodes)
- **Beijing-shanghai trunk initiated**

Global large scale QKD network plans accelerating

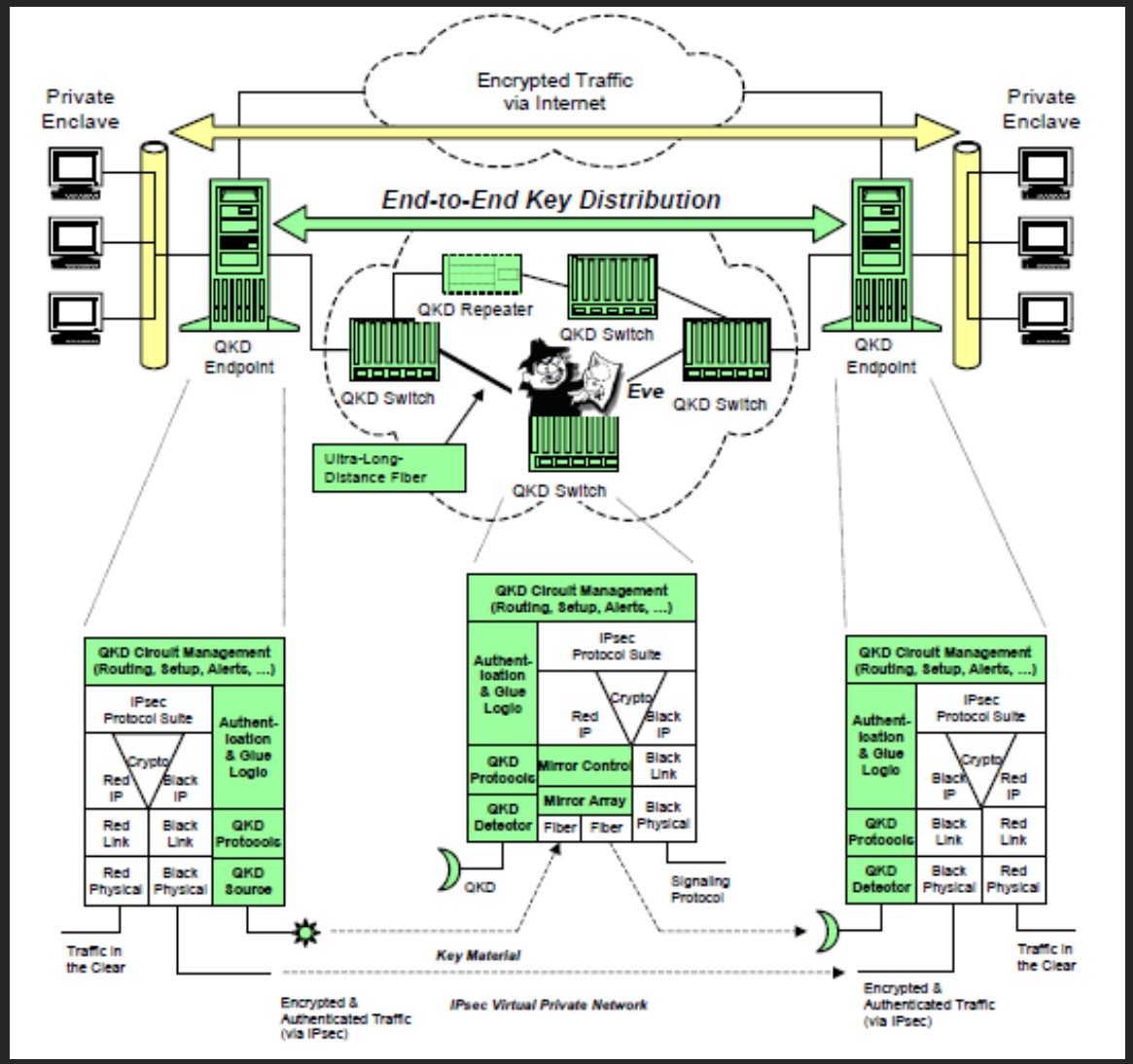




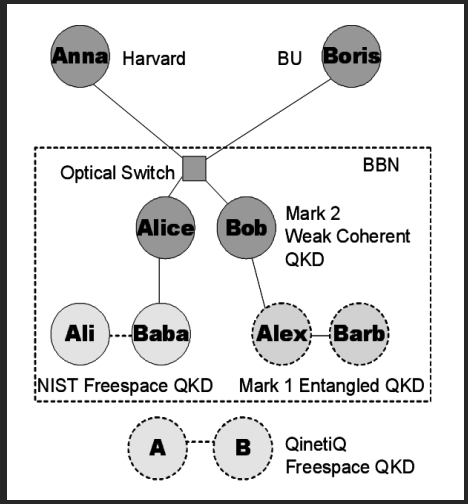
Global satellite QKD projects initiated

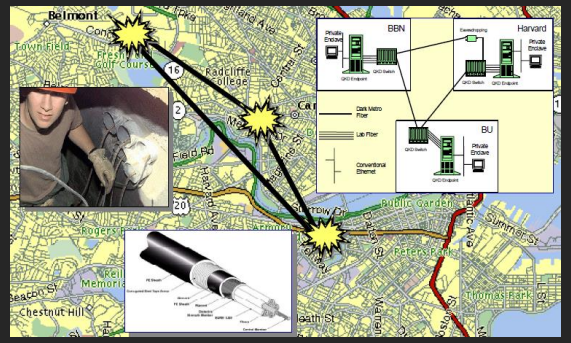
* Wang, Xiang-Bin. *(2005): 230503.*
Lo, Hoi-Kwong, Xiongfeng Ma, and Kai Chen. *(2005): 230504.*

Retrospect | US DARPA QKD network



- **World's first QKD network (2002~2007)**
- **10 nodes: 4 fiber, 4 free-space, 2 entangle**
- **Introduce optical switch and trusted relay for multi-user key transport**
- **Integrate with IPSEC/IKE to encrypt Internet traffic based on QKD**
- **No decoy-state, cannot avoid PNS attack**



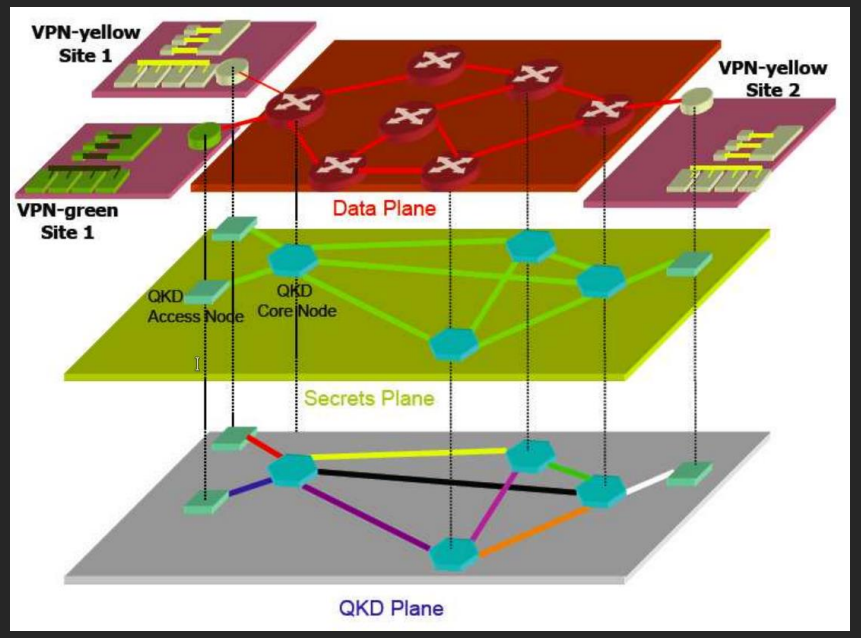


◀ architecture

▲ topology

* "DARPA QUANTUM NETWORK TESTBED", BBN Technology, July 2007

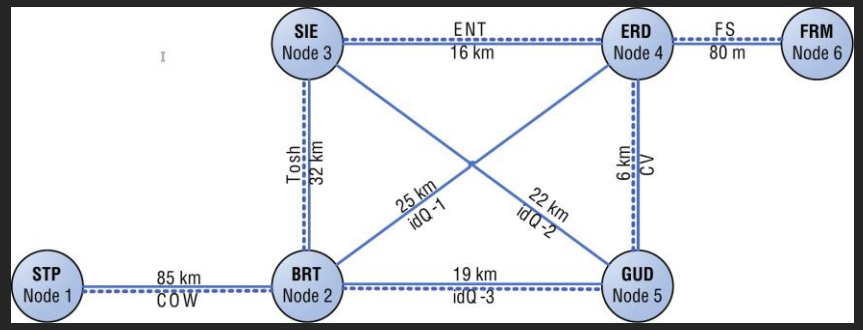
Retrospect | EU SECOQC QKD network

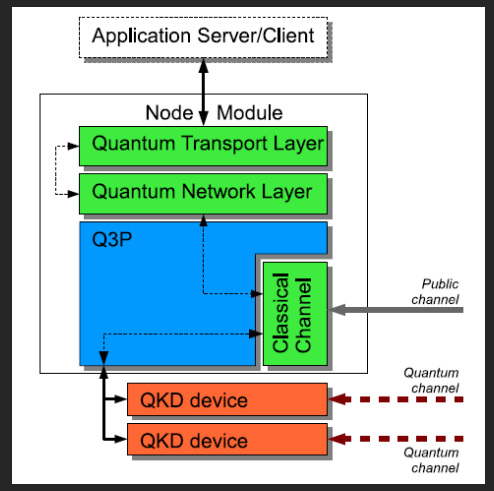


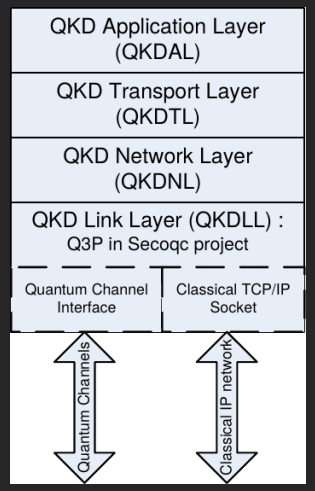
- **QKD MAN in Vienna(2004~2008)**
- **Introduce concepts of QKD Backbone and Access network**
- **Integrate QKD with PPP protocol(Q3P)**
- **Networking based on trusted relay**
- **Routing based on OSPF**

◀ Layered architecture

topology ▶







◀ Node Module

* Mehrdad Dianatil, et al., Security Comm. Networks., 10.1002/sec.13(2008)

Retrospect | SwissQuantum QKD network

- 3 nodes QKD network based on trusted relay installed in the Geneva metropolitan area in March 2009
- Multiplexing quantum channel with classical channels on a single fiber

Fig. 1. Map of the SwissQuantum QKD network. Two nodes are in Geneva city centre and the third is on the site of CERN in France.

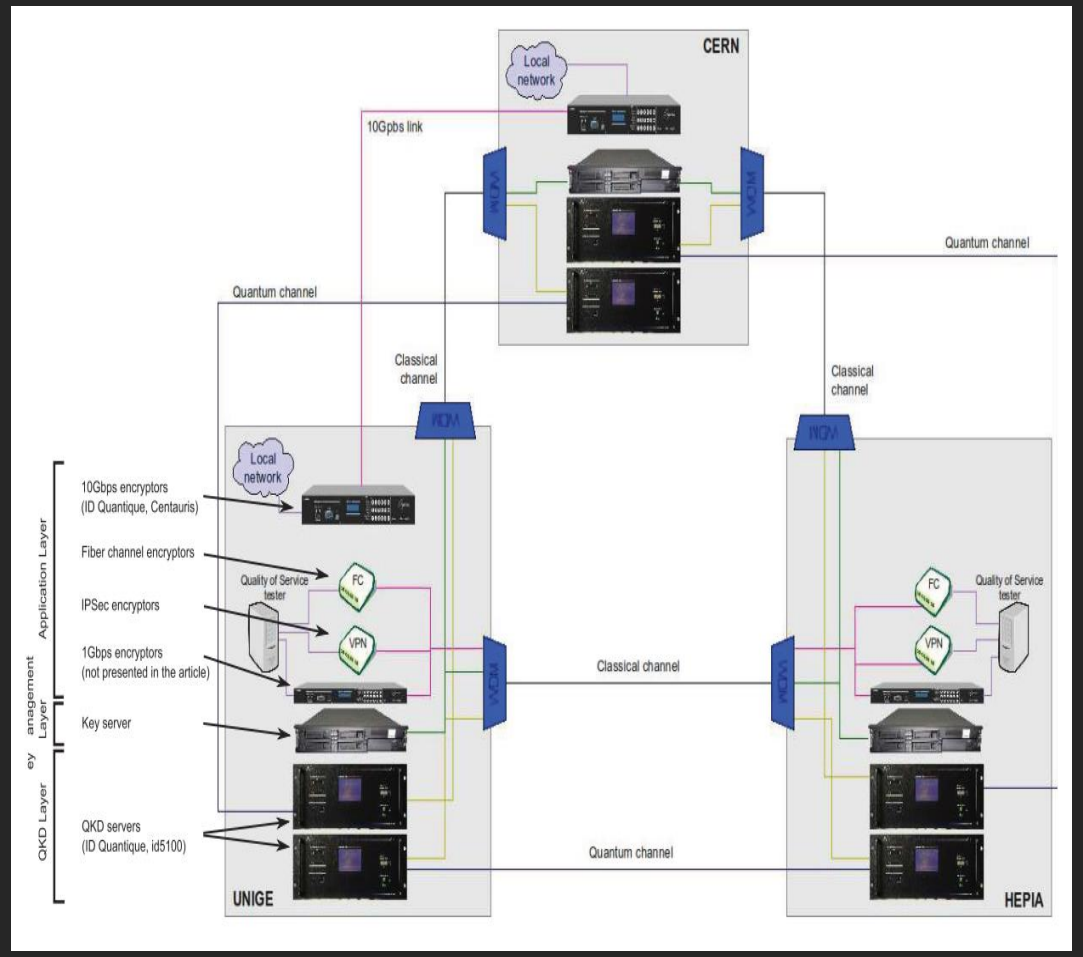
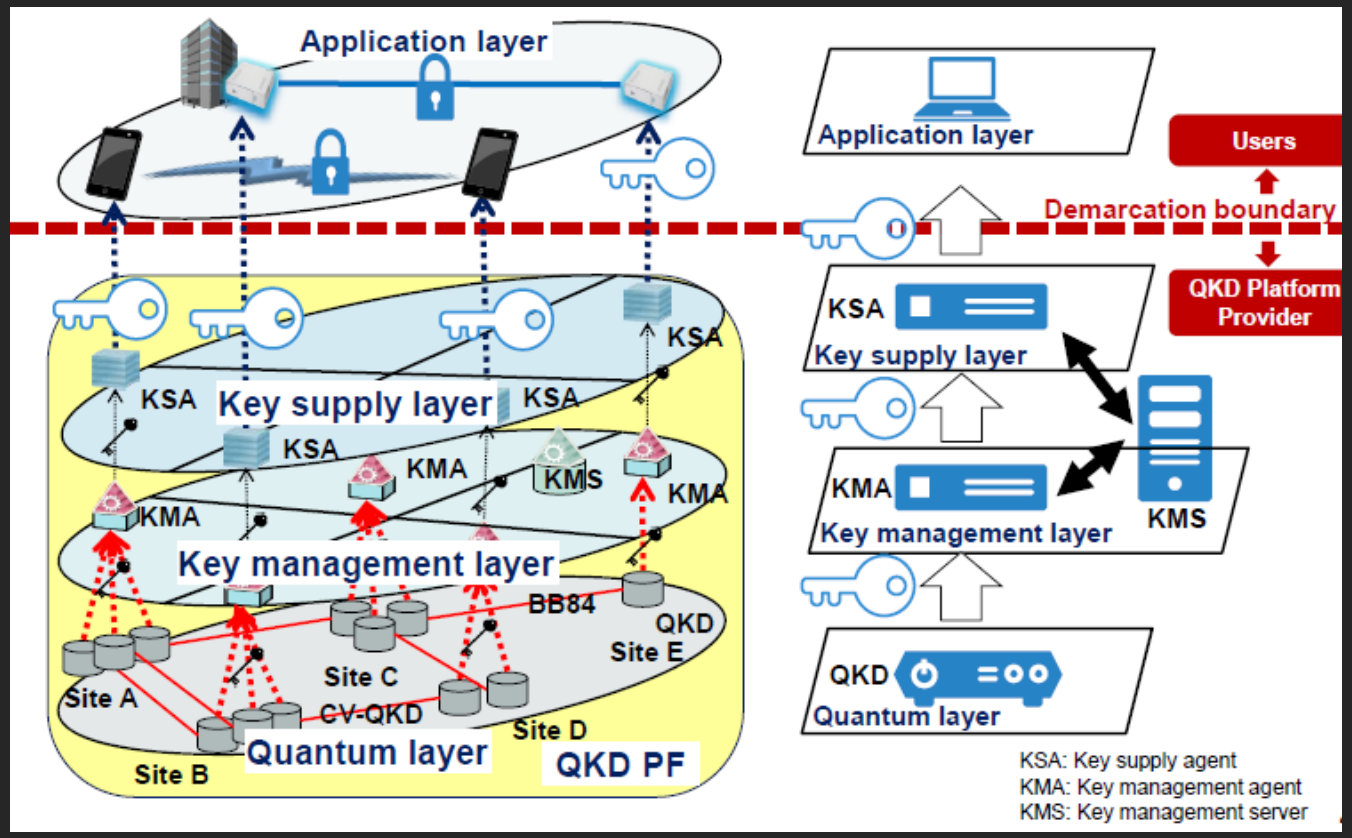


Fig. 2. Detailed topology of the SwissQuantum QKD network.

* D. Stucki *et al.*, “Long-term performance of the SwissQuantum quantum key distribution network in a field environment,” New J. Phys. **13**(12), 123001 (2011).

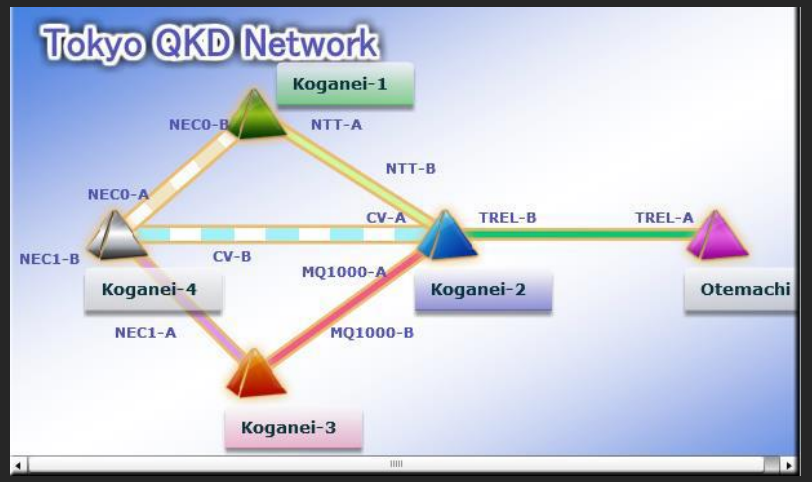
Retrospect | JP Tokyo QKD network



▲ Layered architecture

- **5 nodes, BB84, CV, DPS (2011~)**
- **Trusted relay, layered design, support various topology**
- **Introduce KMS for centralized network management**
- **Introduce the concept of QKD platform to provide various applications including smartphone**

topology ▶



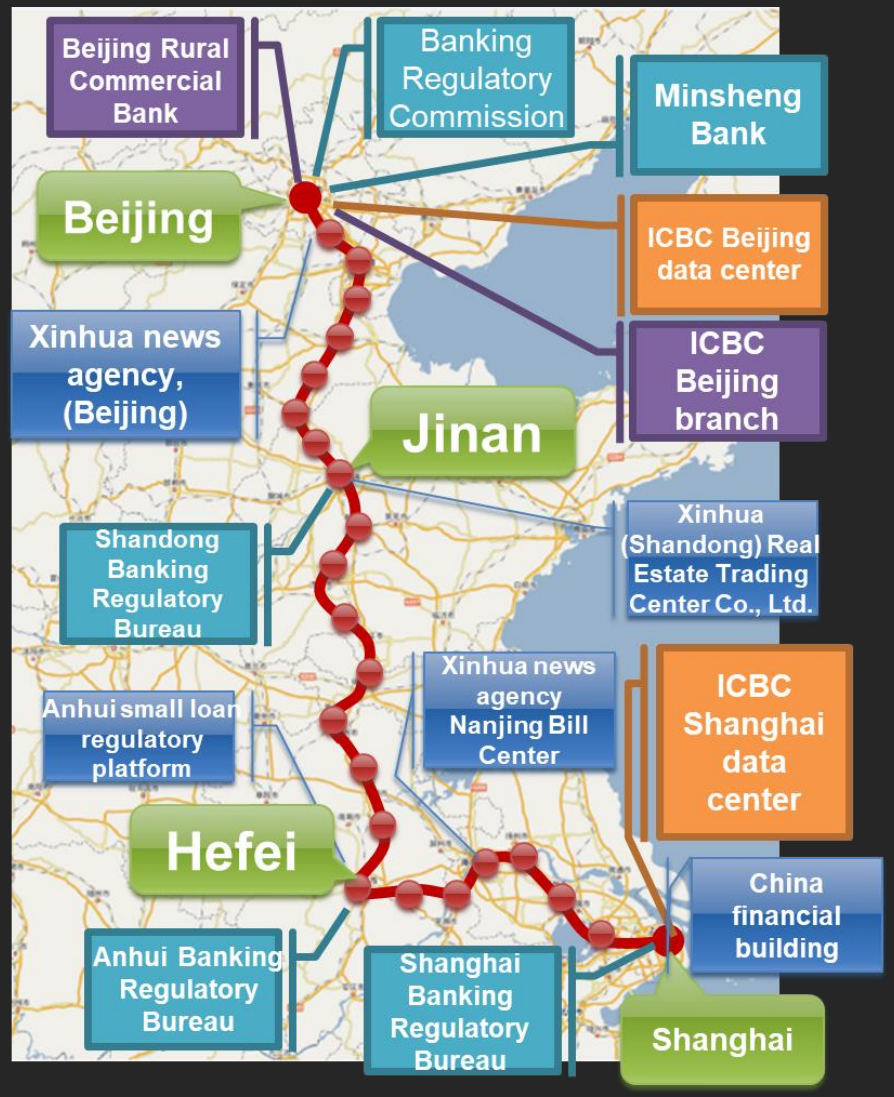
http://tokyoqkd.jp

* M. Sasaki, et al., Optical Express, OE.19.010387 (2011)

Retrospect | CN Satellite-Ground Integrated QKD networks

- **2000 km Beijing-to-Shanghai backbone (2013~2017)**
- **World's first quantum satellite (2016~)**
- **Hierarchical: metropolitan access network, wide-area fiber backbone network, Inter-continental satellite network**
- **Scalable: based on trusted relay and optical switch**
- **Support various topology and applications, e.g., ITS voice, AES encrypted video, IPSEC VPN, etc.**

▲ Satellite-ground integrated QKD network plan



▲ QKD applications along Beijing-Shanghai trunk

Retrospect | Integration of QKD and Classical Networks

China Unicom and USTC field trial (2018)

- **Integrating quantum key distribution with classical communications in backbone fiber network**

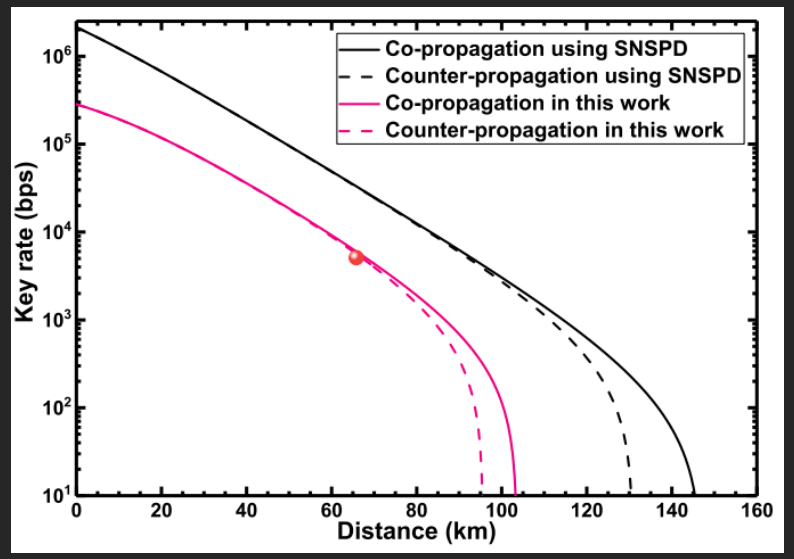


Fig. 2. Calculated secure key rates of QKD as a function of distance for co-propagation and counter-propagation.

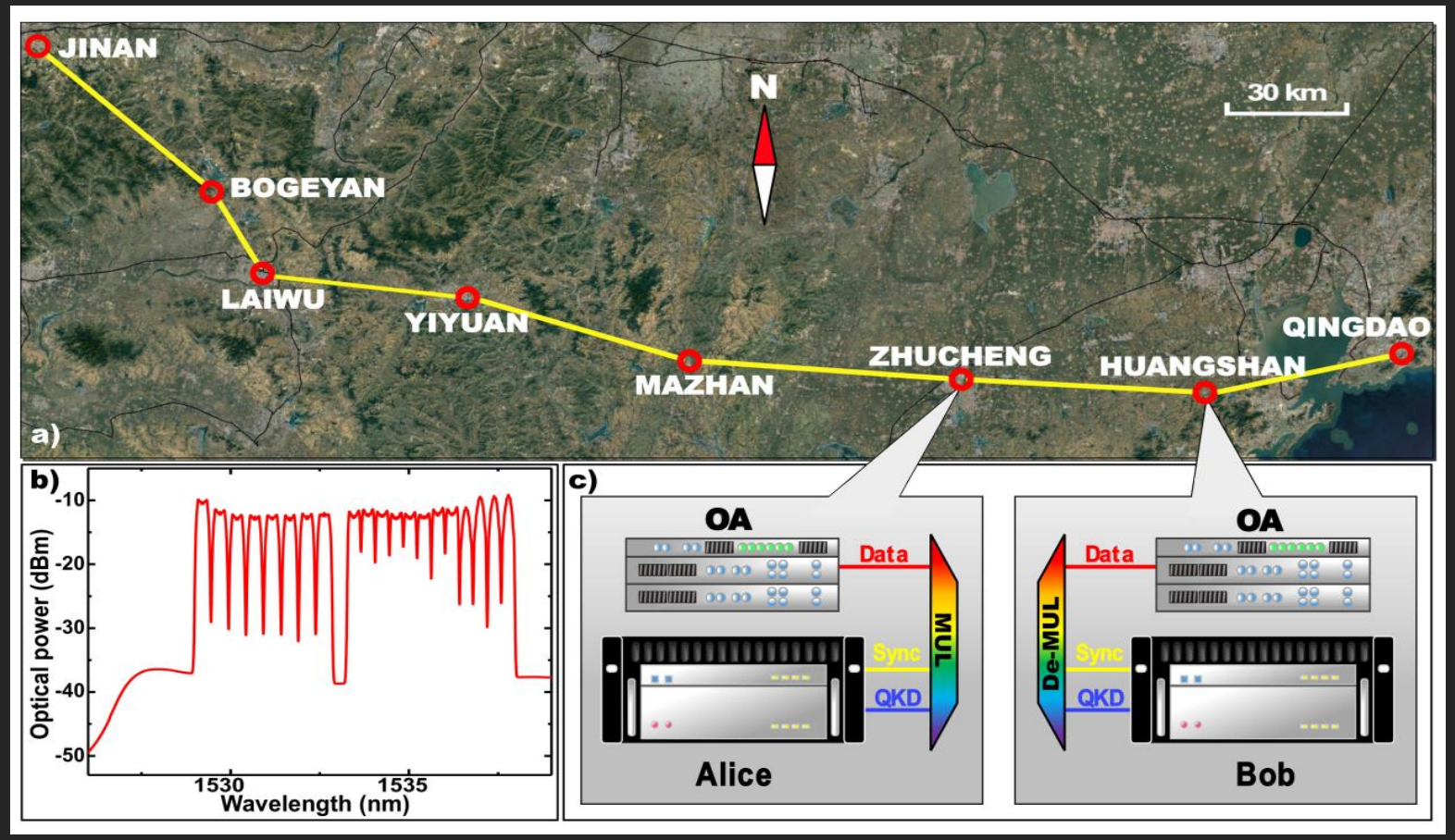
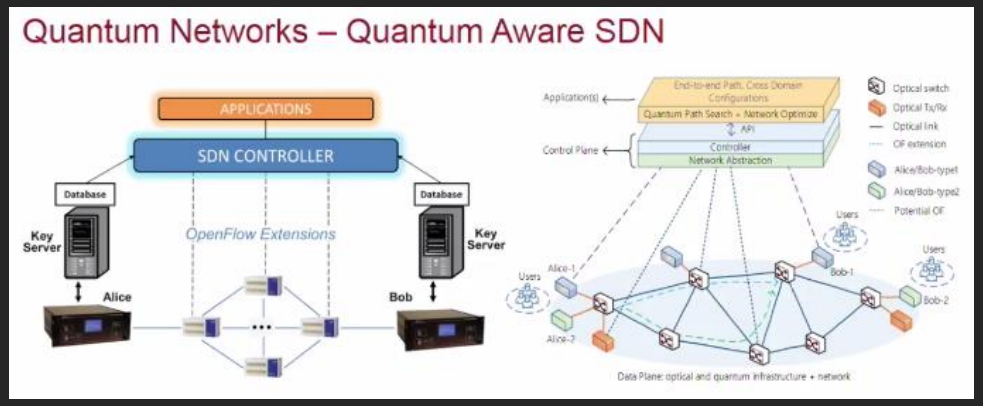


Fig. 1. (a) Field configurations of the experiment. (b) Spectrum of the CC measured at Zhucheng. (c) Coexistence schematics of the experiment.

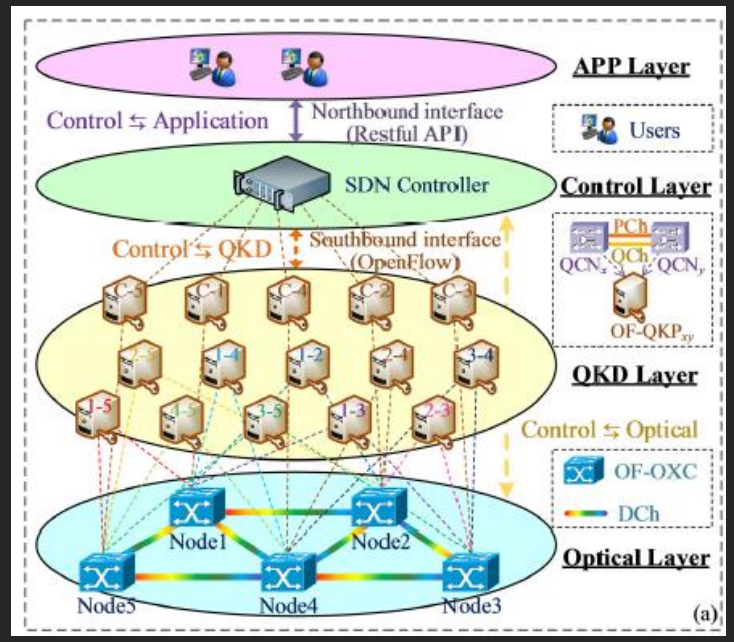
*Y. Mao *et al.*, "Integrating quantum key distribution with classical communications in backbone fiber network," Opt. Express **26**(5), 6010–6020 (2018).

Retrospect | Software-defined QKD network

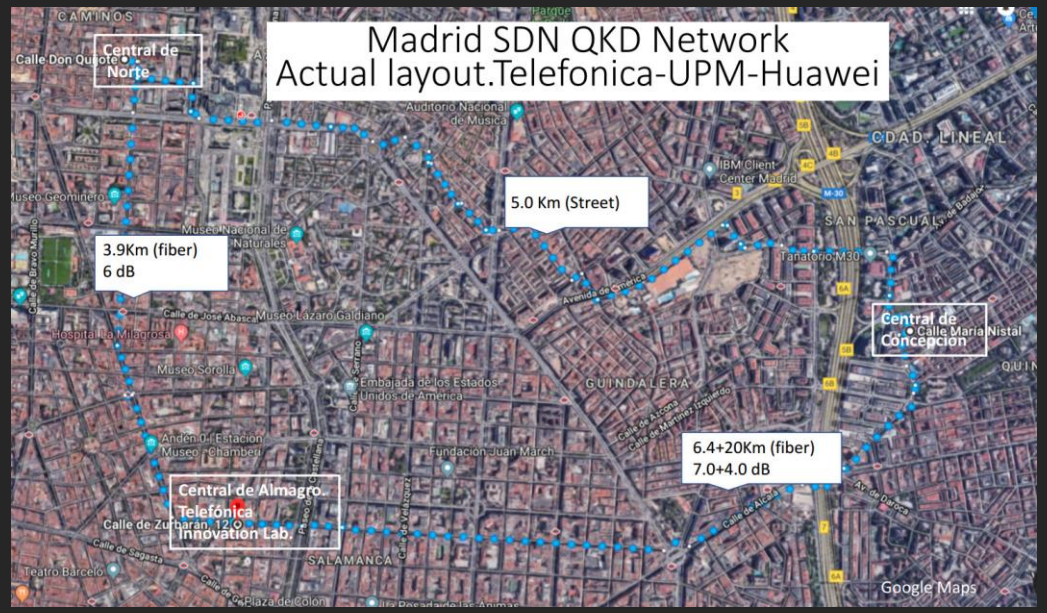


▲ Bristol Univ. Philip Sibson et al., Qcrypt17 Mo24(2017)

- **IEEE & ETSI initiate standardization work (2016-)**
- **Bristol univ., UPM, BUPT, etc. start research and experiments (2016-)**
- **Telefónica, Huawei and UPM perform field trial(2018)**
- **SD-QKD network separate data and control plane**
- **Use SDN protocols based on Yang model to enable simple and flexible network management**



Madrid SD-QKDN field test
http://www.gcc.fi.upm.es
(2018)
▶



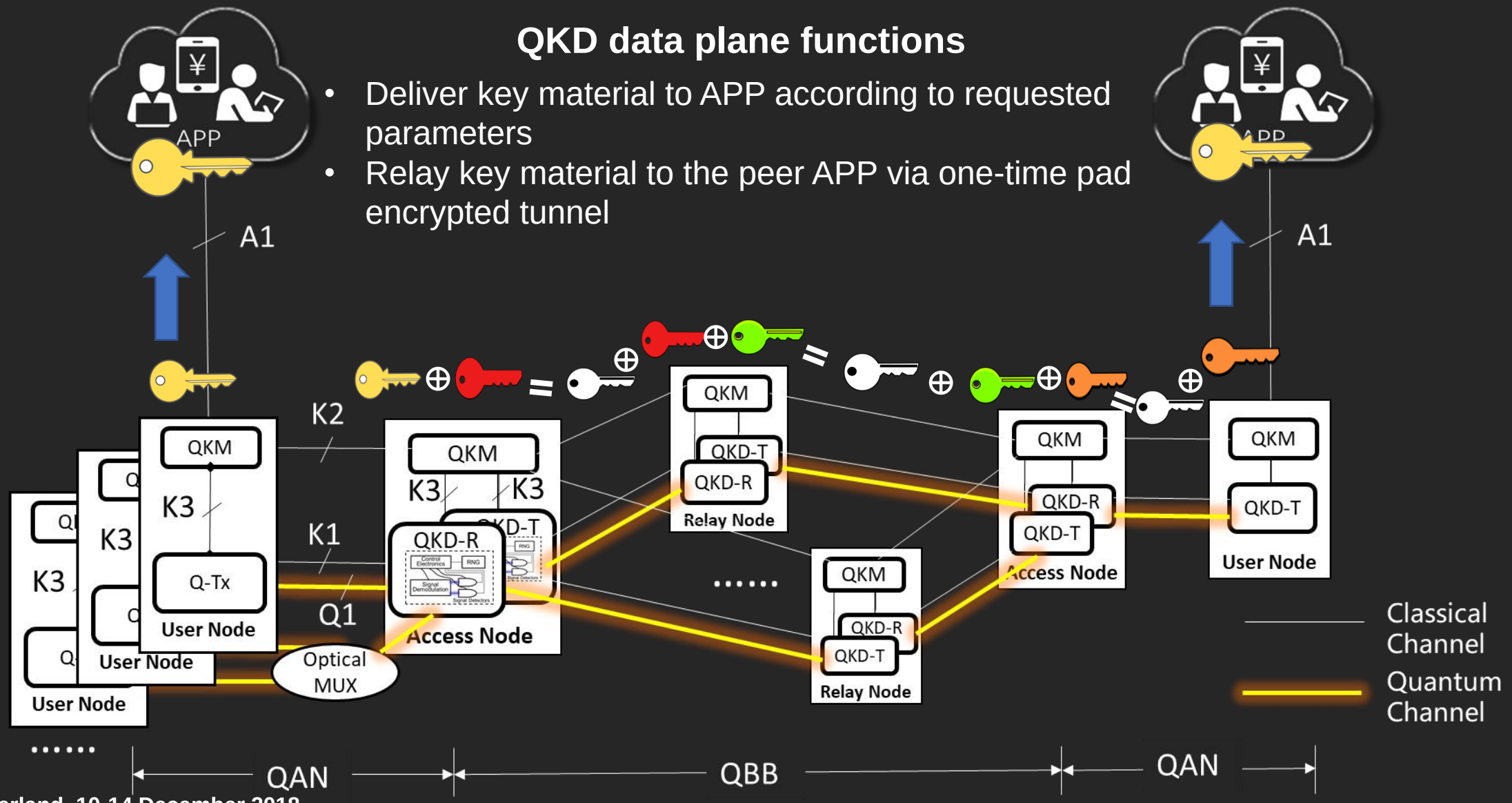
◀ BUPT
Y. Cao, Y. Zhao, et al., Optics Express, OE.25.026453 (2017)

Vision of QKD network deployment and applications

QKD Network Abstraction | Data-plane functions

QKD data plane functions

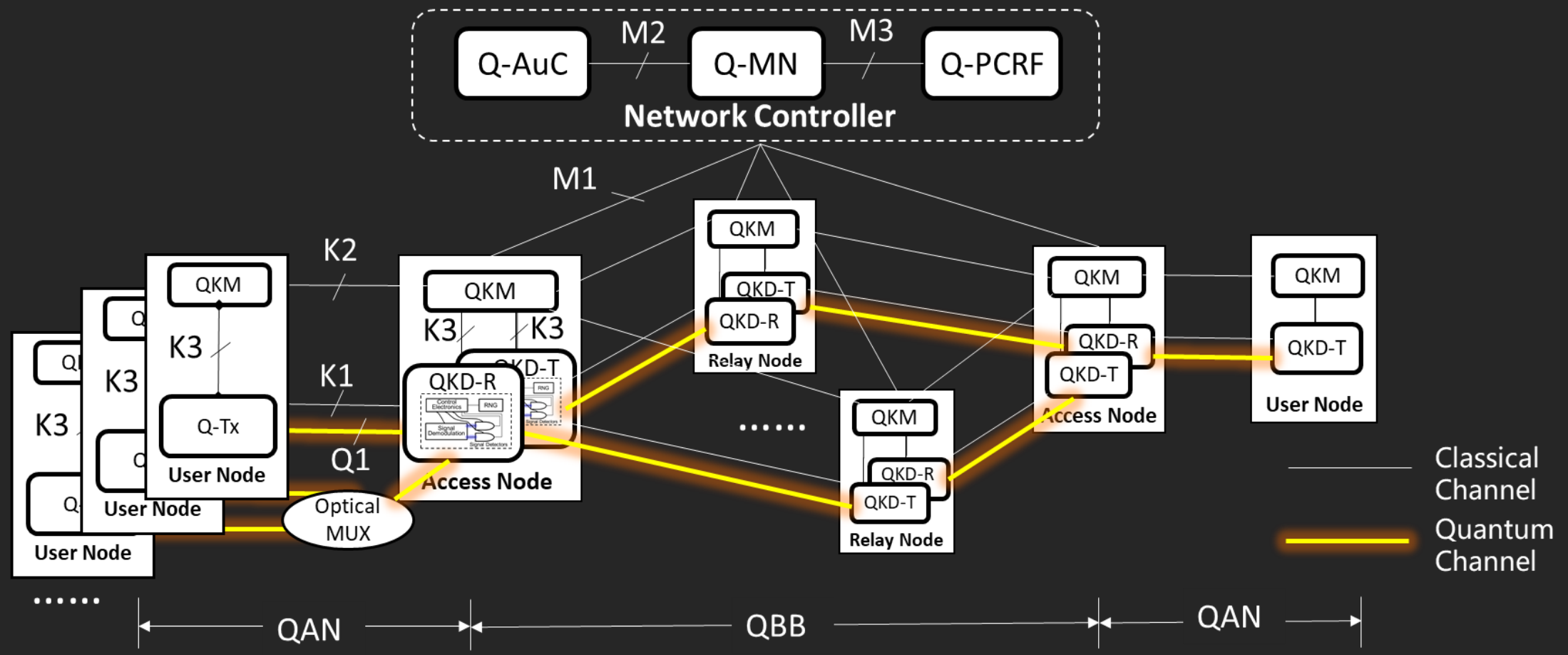
- Deliver key material to APP according to requested parameters
- Relay key material to the peer APP via one-time pad encrypted tunnel



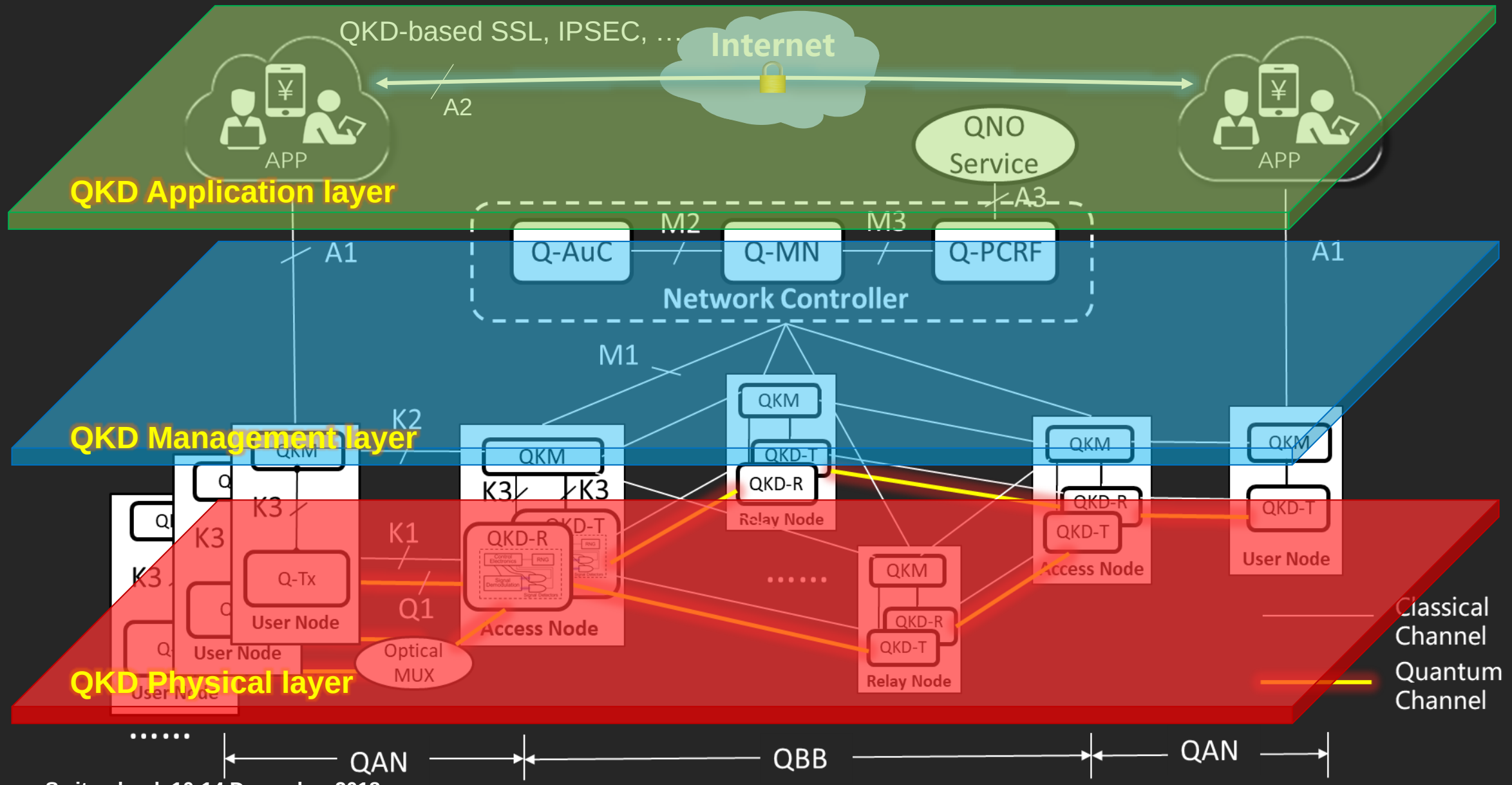
QKD Network Abstraction | Control-plane functions

QKD Control plane functions

- **Q-AuC:** Node Register and Authentication
- **Q-PCRF:** QoS Policy and Charging Rules control
- **Q-MN:** Routing and Resource Management, e.g., load balancing



QKD Network Abstraction | Network Elements and Interfaces



Global Quantum Information Technology Standardization Activities

- 2018: SG 13 and SG17 initiate new WI/SIs on QKD network framework and security aspects

- 2017: The study item of "Security requirements, test and evaluation methods for quantum key distribution" initiated
- 2018: New study group on Quantum Computing is to be established

- 2016: P1913 Software Defined Quantum Communication WG initiated
- 2018: P7130 and P7131 on Quantum Computing Definition and Performance Metrics & Benchmarking

- 2014: Quantum-safe security WG founded, several reports on QKD and post-quantum cryptography have been released

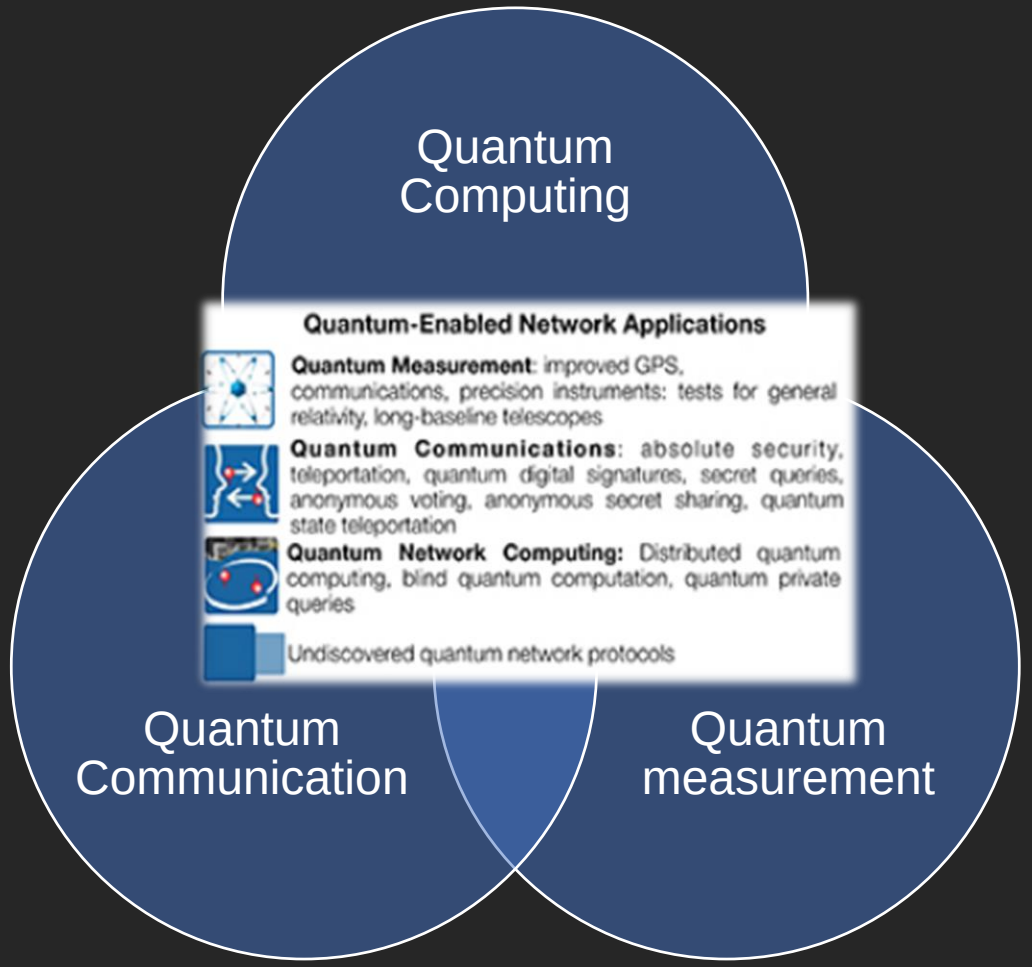
- 2009: Proposed "IKE for IPsec with QKD" but remain draft

- 2008: ETSI ISG QKD founded, 6 specifications have been published

Key issues for further study

How to integrate quantum information technology into existing network infrastructures?

How to develop future networks based on quantum information technologies?



Standardization Landscape

Quantum Information Technology (QIT) for Networks*

Analyze impacts of QITs on network technologies → Study QKD network level issues to facilitate and accelerate ongoing and upcoming QKD activities → Study further evolution from trusted relay to quantum repeater based "Quantum Internet"

* To be initiated

Quantum Computing

ISO JTC1 IEC INFORMATION TECHNOLOGY STANDARDS

IEEE

Quantum Computing Definition, Performance Metrics & Benchmarking, etc.

Quantum Key Distribution

ITU

SG13
QKD Network Framework

SG17
QKD and QRNG security framework

QKD networking related issues*

ETSI World Class Standards

QKD integration into Existing Infrastructure
QKD Security Certification, Complementary Research

ISO JTC1 IEC INFORMATION TECHNOLOGY STANDARDS

QKD Certification Process

Future Work for QIT4N

Quantum Information Technology (QIT) for Networks

Analyze impacts of QITs on network technologies → Study QKD network level issues to facilitate and accelerate ongoing and upcoming QKD activities → Study further evolution from trusted relay to quantum repeater based "Quantum Internet"

- Security threats and enhancements
- Performance and Information processing capability improvements
- Enabling new applications
- ……

- New QKD application scenarios to extend its applications to wider ICT domains
- QKD networking issues, e.g, routing, resource management, QoS and charging control.
- Integration of QKD networks with existing optical networks, e.g., co-fibre transmission of quantum and classical signals.
- New solutions to extend QKD distances, e.g., quantum relay and repeaters
- ……

- Key components and enabling technologies to realize quantum information transmission and networking
- Potential use cases for future quantum information network, connecting distributed quantum computers or sensors.
- Architecture of future quantum information network, relationship with existing networks and the evolution roadmaps.
- ……

Thanks!

Q&A

CAICT 中国信通院

中国科学技术大学
University of Science and Technology of China

量子网络
CAS QUANTUMNET

国盾量子
QuantumCTek

Geneva, Switzerland, 10-14 December 2018