ITU QIT4N Workshop
5-7 June, 2019
Shanghai, China

Towards large-scale quantum key distribution network and its applications

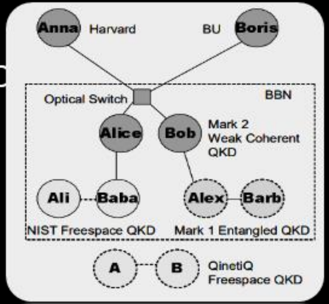
Hao Qin
CAS Quantum Network Co., Ltd.
Email: qinhao@casquantumnet.com

Quantum Key Distribution (QKD)：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



2004
EU: SECOQC network initiated, finished at 2008

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)

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

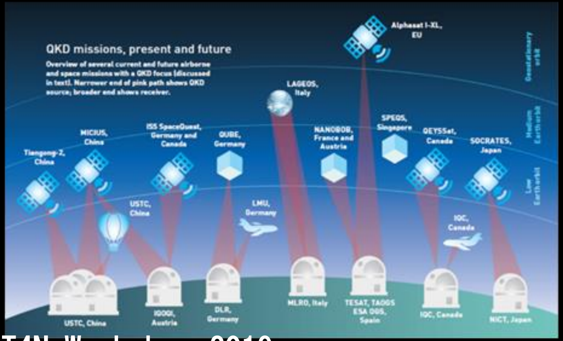
2013

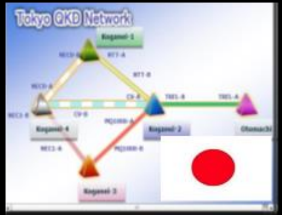
2016: Beijing-Shanghai backbone QKD network

2016: “Micius” quantum satellite launched

……

Global large scale QKD network plans accelerating

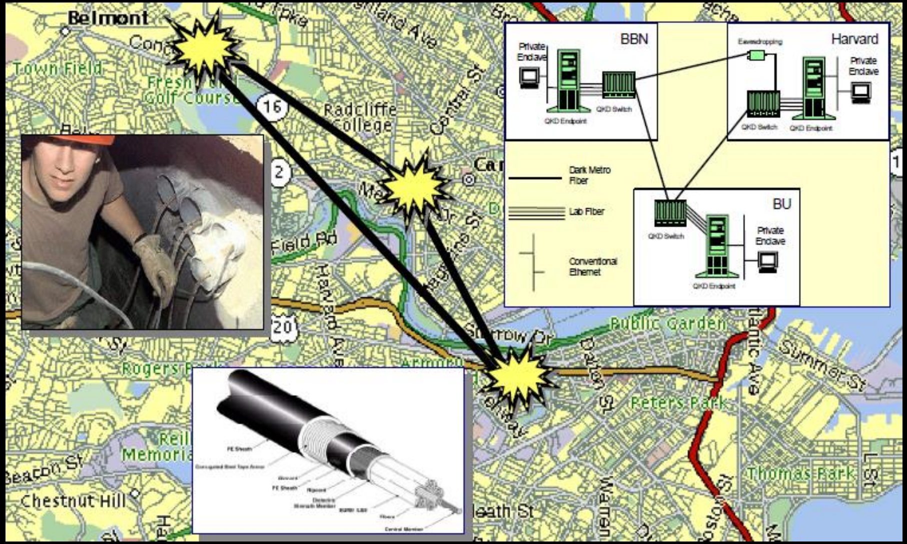

QKD missions, present and future
Overview of several current and future airborne and space missions with a QKD focus (discussed in text). Narrower end of pink path shows QKD source; broader end shows receiver.
Alphasat I-XL, EU
Geostationary orbit
LAGEOS, Italy
Medium Earth orbit
Low Earth orbit
Tiangong-2, China
MICIUS, China
ISS SpaceQuest, Germany and Canada
QUBE, Germany
NANOBOB, France and Austria
SPEQS, Singapore
QEYSSat, Canada
SOCRATES, Japan
USTC, China
LMU, Germany
IQC, Canada
USTC, China
IQOQI, Austria
DLR, Germany
MLRO, Italy
TESAT, TAOGS ESA OGS, Spain
IQC, Canada
NICT, Japan



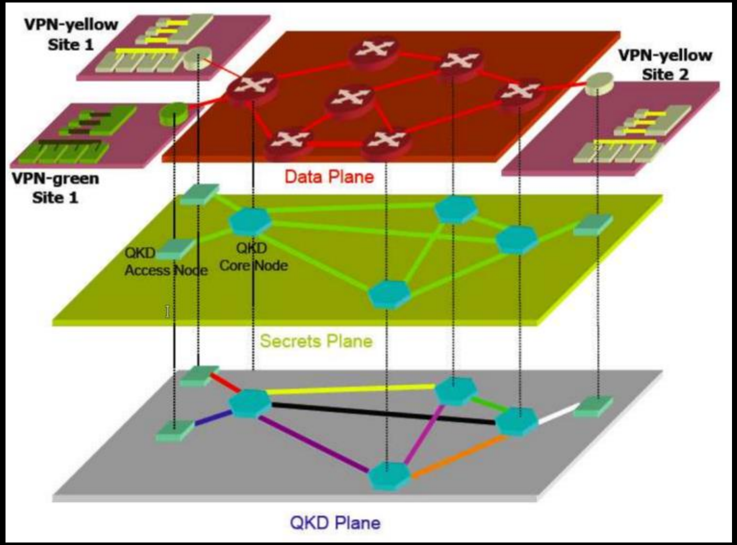
Global satellite QKD projects initiated

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

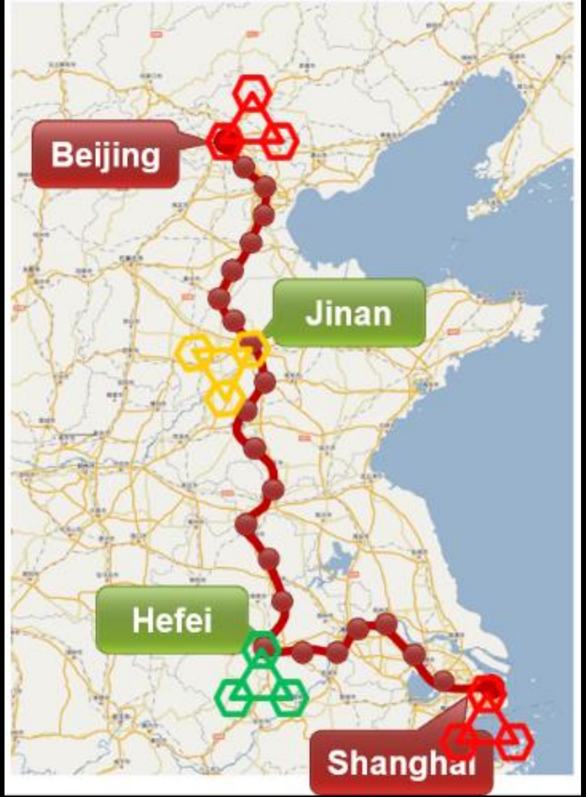
Global QKD network projects



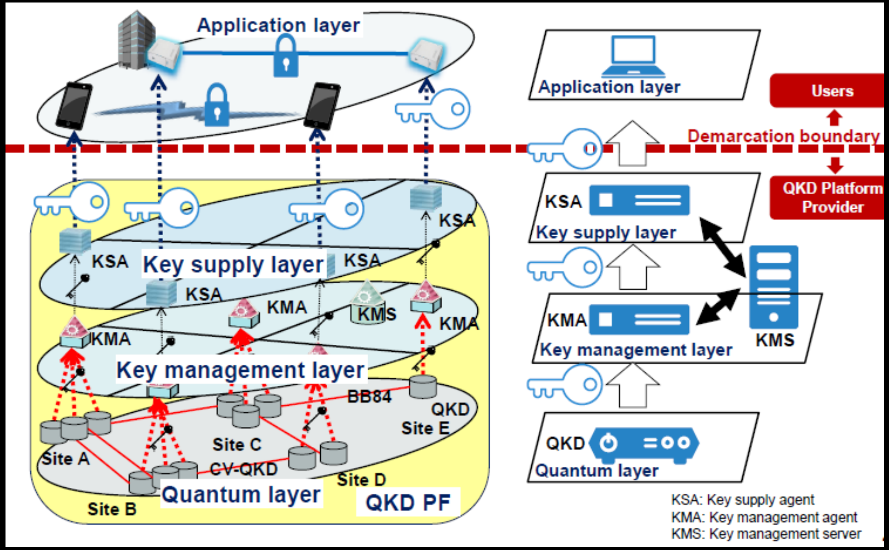
DARPA QUANTUM NETWORK，BBN Technology (2007)



EU SECOQC QKD network, 10.1002/sec.13 (2008)



Beijing-Shanghai Quantum Backbone Network



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

Tokyo QKD network, OE.19.010387 (2011)

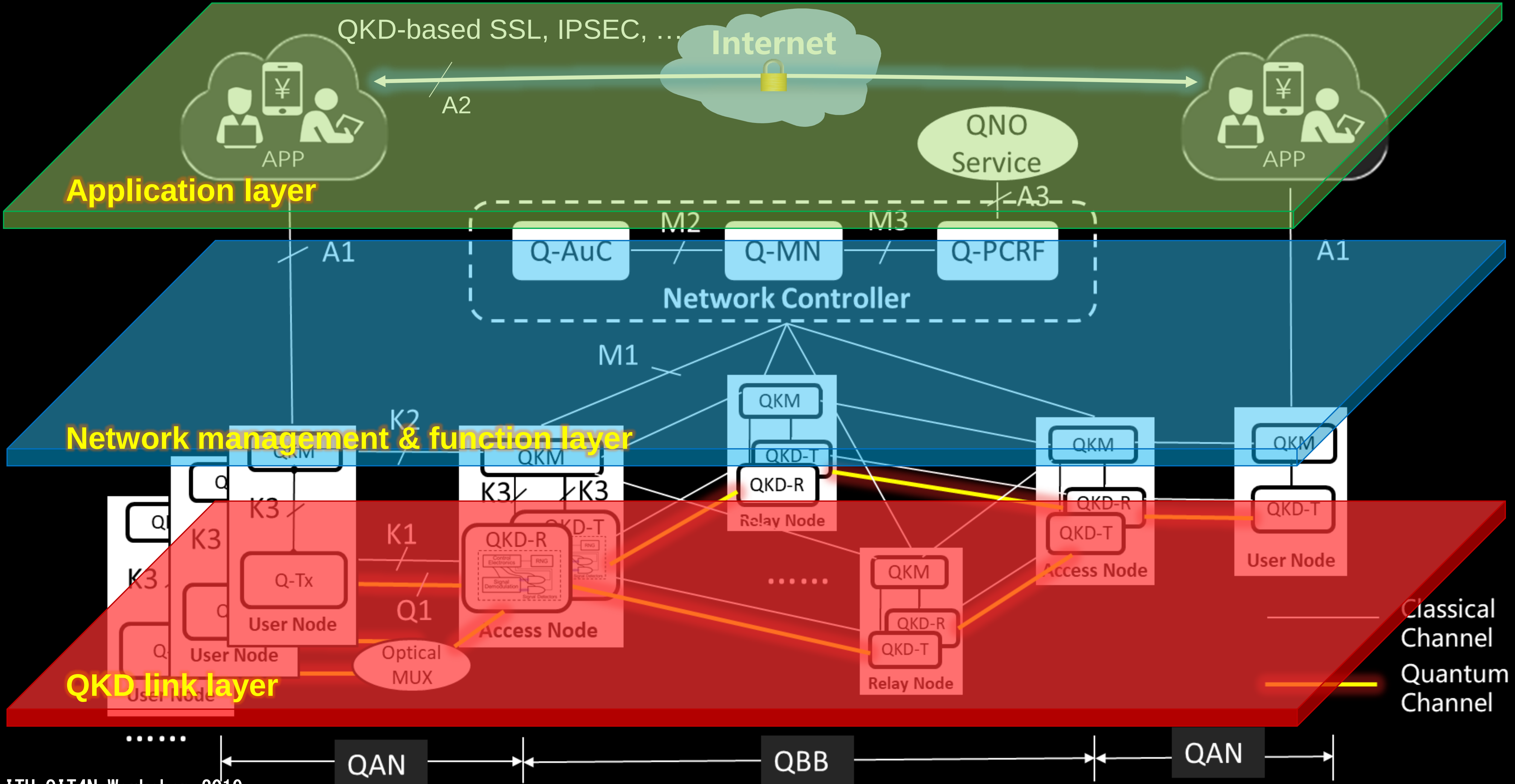
CERN
hepia
Unige

▲

SwissQuantum QKD network, NJP **13**(12), 123001 (2011)

AND SO ON……

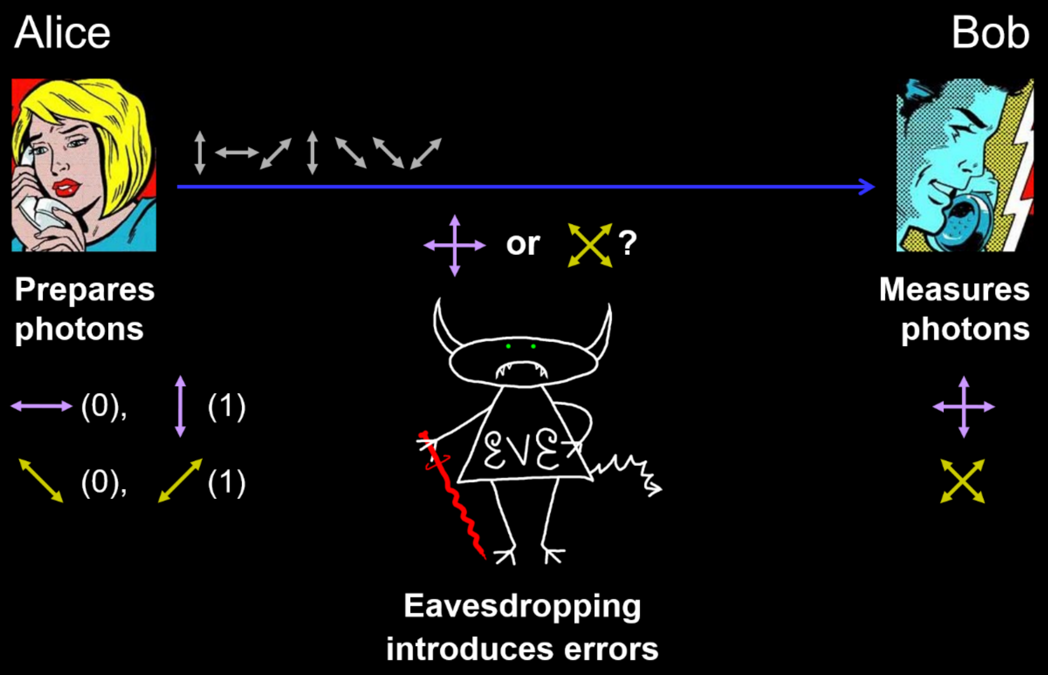
QKD network: Three layers architecture



Large-scale QKD network as infrastructures

- ➢Goal: Provide information security services through scalable, service-oriented and cost-efficient QKD networks in wide area.
- ➢ Support various services and applications based on QKD network.
- ➢Build and operate the QKD network.

Technology/standard requirements for QKD link and network layers.



[C. H. Bennett & G. Brassard, BB84 protocol (1984)]

Technology requirements: QKD link layer

量子网络 CAS QUANTUMNET

➤ **Solve the key distribution problem**

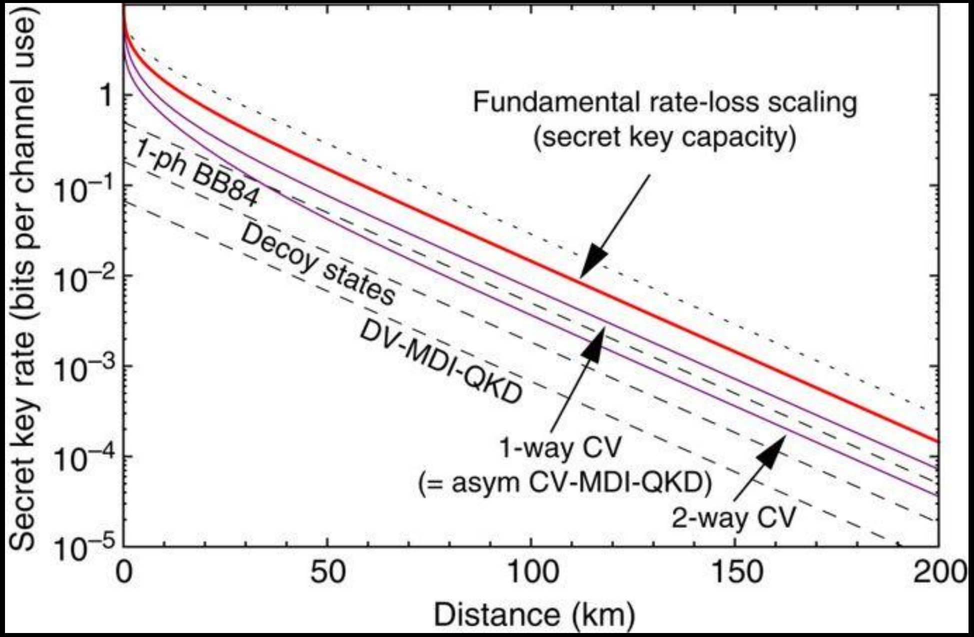
- **Security based on quantum physics: Information theoretic security**
- **Point-to-point symmetric key establishment: Rate-loss trade-off**

➤ **Not rely on single QKD protocol!**

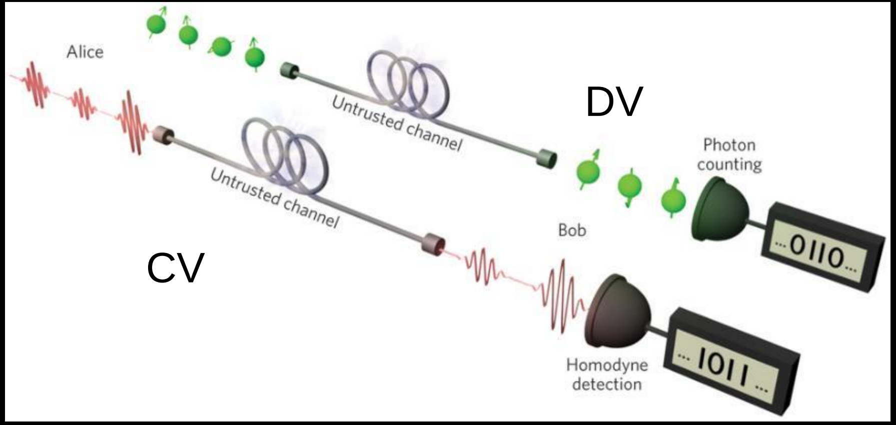
- **Well studied and mature enough: Complete security proof; robust performance in practice; efficient key rate output etc.**
- **Discrete Variable (DV) QKD: BB84 with decoy**
- **Continuous Variable (CV) QKD: GG02**
- **Polarization and phase encoding etc.**

➤ **Open for new protocols:**

- **Measurement device independent (MDI) QKD**
- HK Lo *et al.*, PRL 108, 130503 (2012)
- **Twin filed (TF)/Phase matching (PM) QKD**
- M. Lucamarini *et al.*, Nature 557, 400-403 (2018)



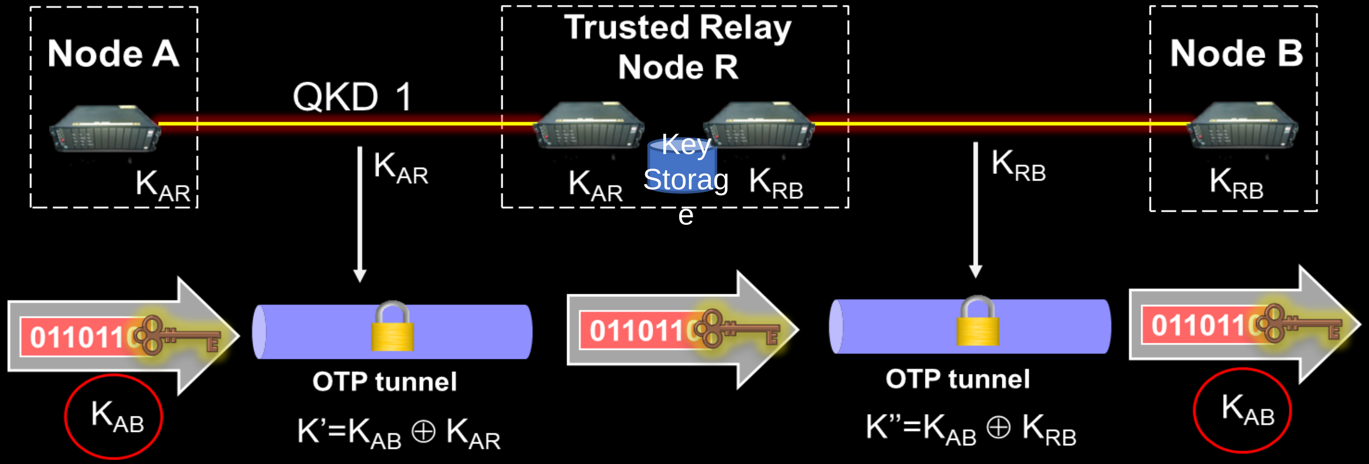
PLOB bound [Nature Commun. **8**, 15043(2017)]

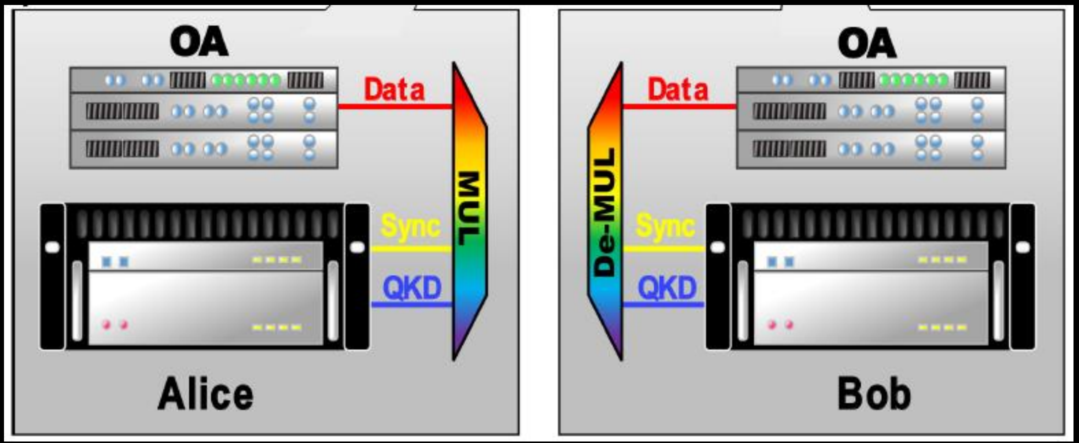


DV & CV QKD [Nature Photonics 7,350–352 (2013)]

Technology requirements: Network layer

- **Trusted node**
- **Optical switch**
- **Wavelength Division Multiplexing(WDM)**





Opt. Express 26(5), 6010–6020 (2018)

- ➢ Key materials relay: XOR operations
- ➢ Key resources or user key protection
- ➢ Protection on the trusted node
- ➢ Working with optical switches
- ➢ Quantum relay is currently not available in practice

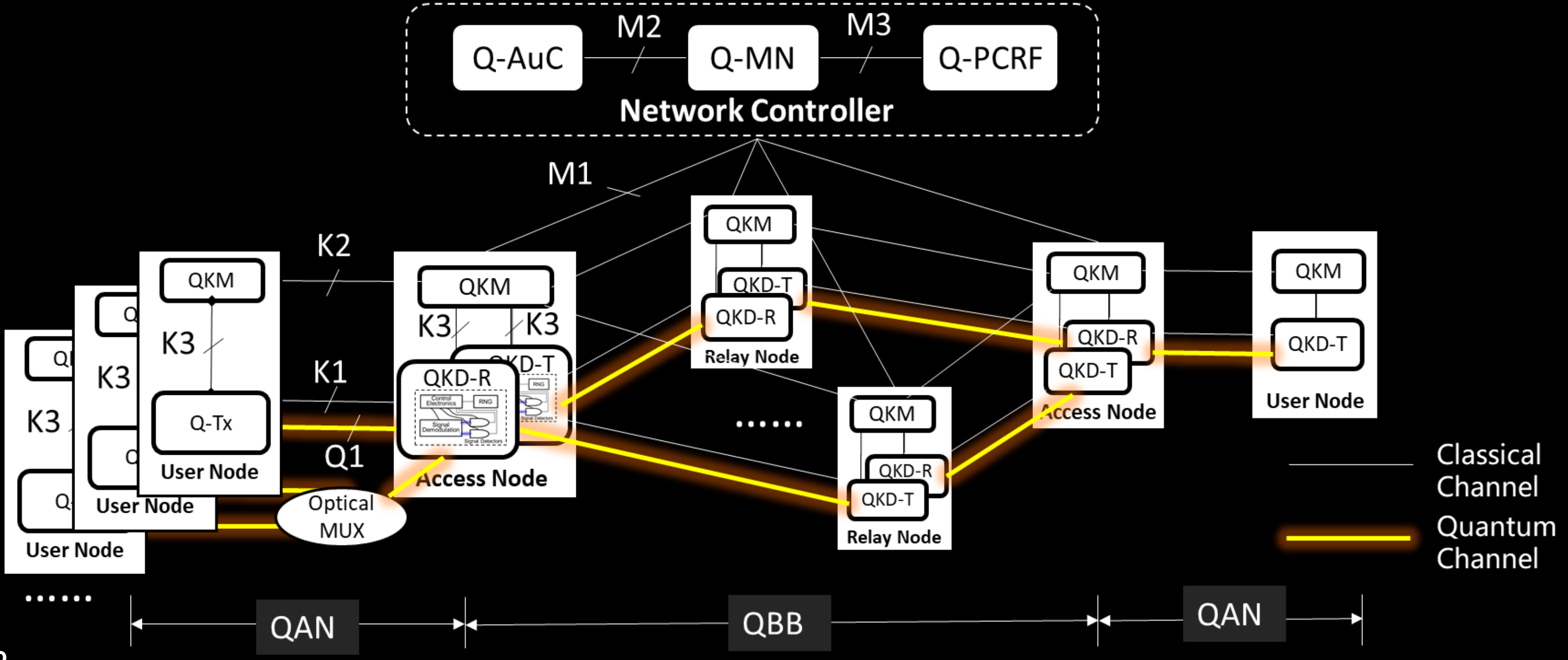
- ➢ Integration of QKD in optical WDM networks
- ➢ Quantum signals share a same fiber with classical signals
- ➢ Largely reduce fiber resources and cost

Technology requirements: Network layer

QKD network control & management functions

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

- **Interoperability: Support multi-vendor interoperability for both QKD and network management devices**
- **Scalability: Flexible and economic network expansion, flexible network topology for wide-area coverage**



CAS Quantum Network 2018

Standard requirements: QKD link layer

➢QKD basis

- Definition/Vocabulary
- Protocols
- Components
- Characterization: transmitter & receiver
- Classical post processing etc.

➢QKD security

- Security proof
- Module Security Specification
- Security statement:
  Definition , assumptions, requirements
- Security certification & evaluation of QKD
- Security analysis & Test methods of QKD

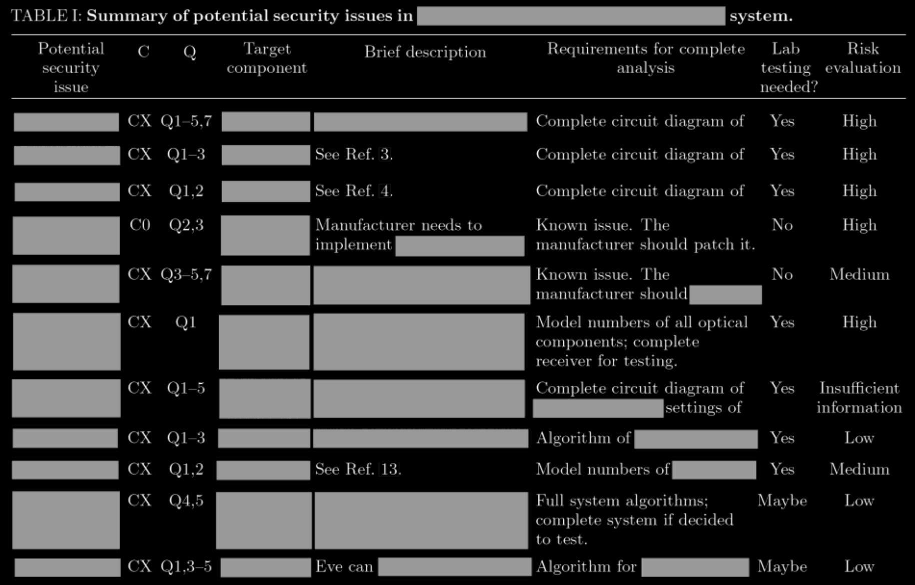


TABLE I: **Summary of potential security issues in [redacted] system.**

Potential security issue	C	Q	Target component	Brief description	Requirements for complete analysis	Lab testing needed?	Risk evaluation
[redacted]	CX	Q1–5,7	[redacted]	[redacted]	Complete circuit diagram of	Yes	High
[redacted]	CX	Q1–3	[redacted]	See Ref. 3.	Complete circuit diagram of	Yes	High
[redacted]	CX	Q1,2	[redacted]	See Ref. 4.	Complete circuit diagram of	Yes	High
[redacted]	C0	Q2,3	[redacted]	Manufacturer needs to implement [redacted]	Known issue. The manufacturer should patch it.	No	High
[redacted]	CX	Q3–5,7	[redacted]	[redacted]	Known issue. The manufacturer should [redacted]	No	Medium
[redacted]	CX	Q1	[redacted]	[redacted]	Model numbers of all optical components; complete receiver for testing.	Yes	High
[redacted]	CX	Q1–5	[redacted]	[redacted]	Complete circuit diagram of [redacted] settings of	Yes	Insufficient information
[redacted]	CX	Q1–3	[redacted]	[redacted]	Algorithm of [redacted]	Yes	Low
[redacted]	CX	Q1,2	[redacted]	See Ref. 13.	Model numbers of [redacted]	Yes	Medium
[redacted]	CX	Q4,5	[redacted]	[redacted]	Full system algorithms; complete system if decided to test.	Maybe	Low
[redacted]	CX	Q1,3–5	[redacted]	Eve can [redacted]	Algorithm for [redacted]	Maybe	Low

World Class Standards

- **Session 3A Technology "Security analysis for QKD"**
- **Session 6A Global Standardization Progress" QKD standardization in ISO/IEC JTC 1/SC 27"**

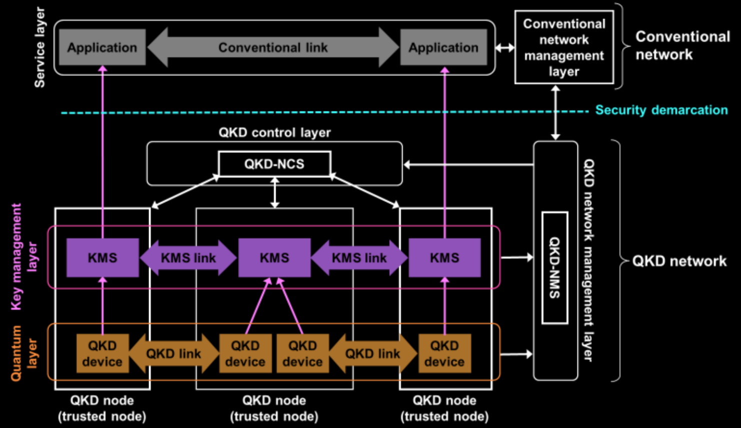
Standard requirements: Network layer

➢ Network basis

- Network architecture
- Network component function
- Software defined network(SDN)
- Trusted node key relay
- Key management
- Application Interface
- Coexistence of quantum and classical channels

➢Network security requirements

- Overall security requirement
- Link security requirement
- Key management security requirement
- Applications & services security requirement
- Trusted relay protection



General structure of QKD network
(Draft Recommendation ITU-T Y.QKDN_FR, ITU SG 13)

security requirements

Session 6A Global Standardization Progress

- **Activities within ETSI ISG QKD**
- **QKD standardization in ITU-T SG 13**
- **Quantum security standardization activities in ITU-T SG17**

QKD related standards in China

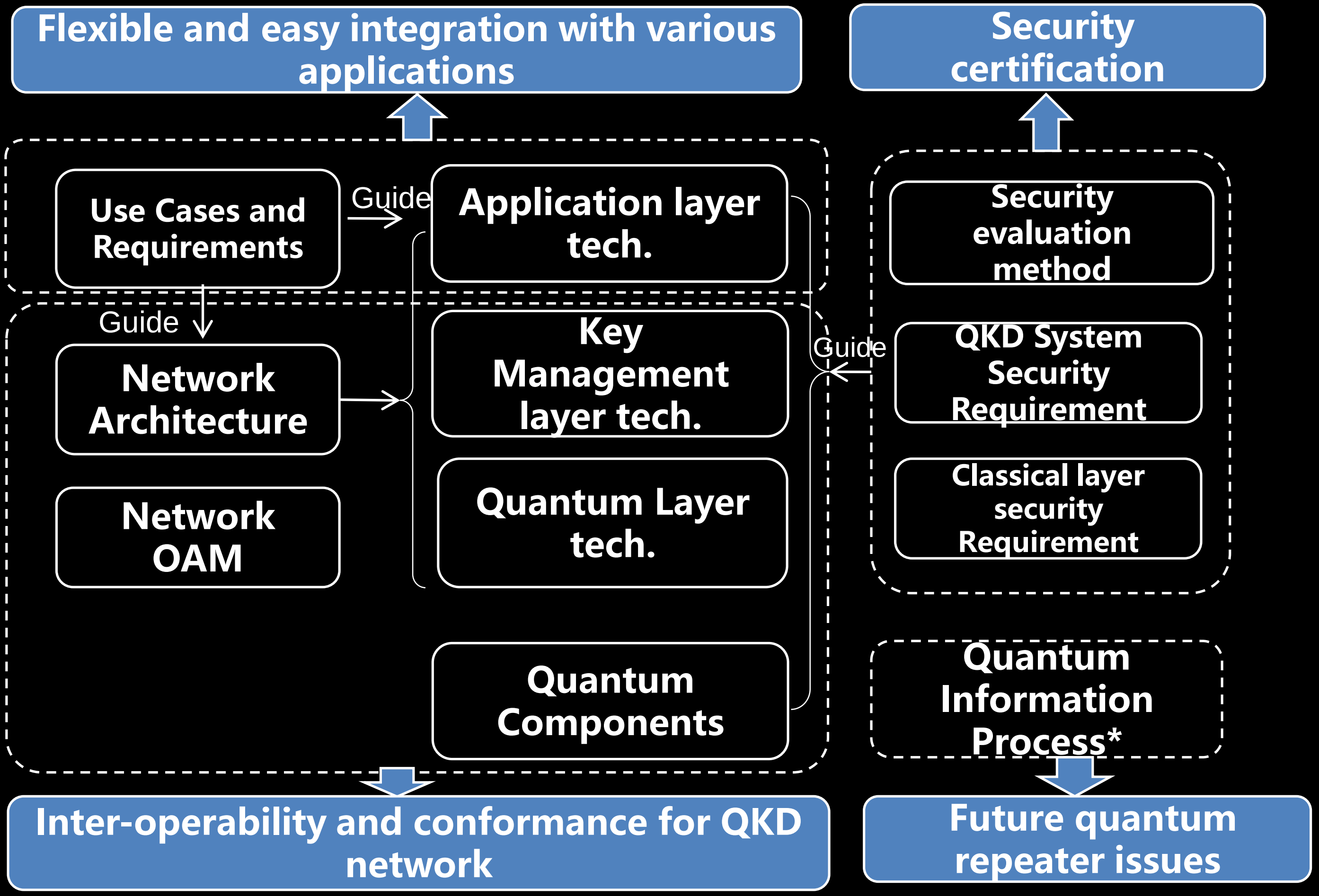
- Most of the QKD standard topics are also considered in China.
- Chinese growing QKD industries push forward standard research activities.

中国通信标准化协会
China Communications Standards Association

- In Jun. 2017, CCSA established the 7th Special Task Group (ST7) focused on QKD-based Quantum Secure Communication (QSC).

密码行业标准化技术委员会
GM
CSTC
Cryptography Standardization Technical Committee

- In 2017, cryptography standardization technical committee started the QKD standards research focusing on security requirements and test methods.

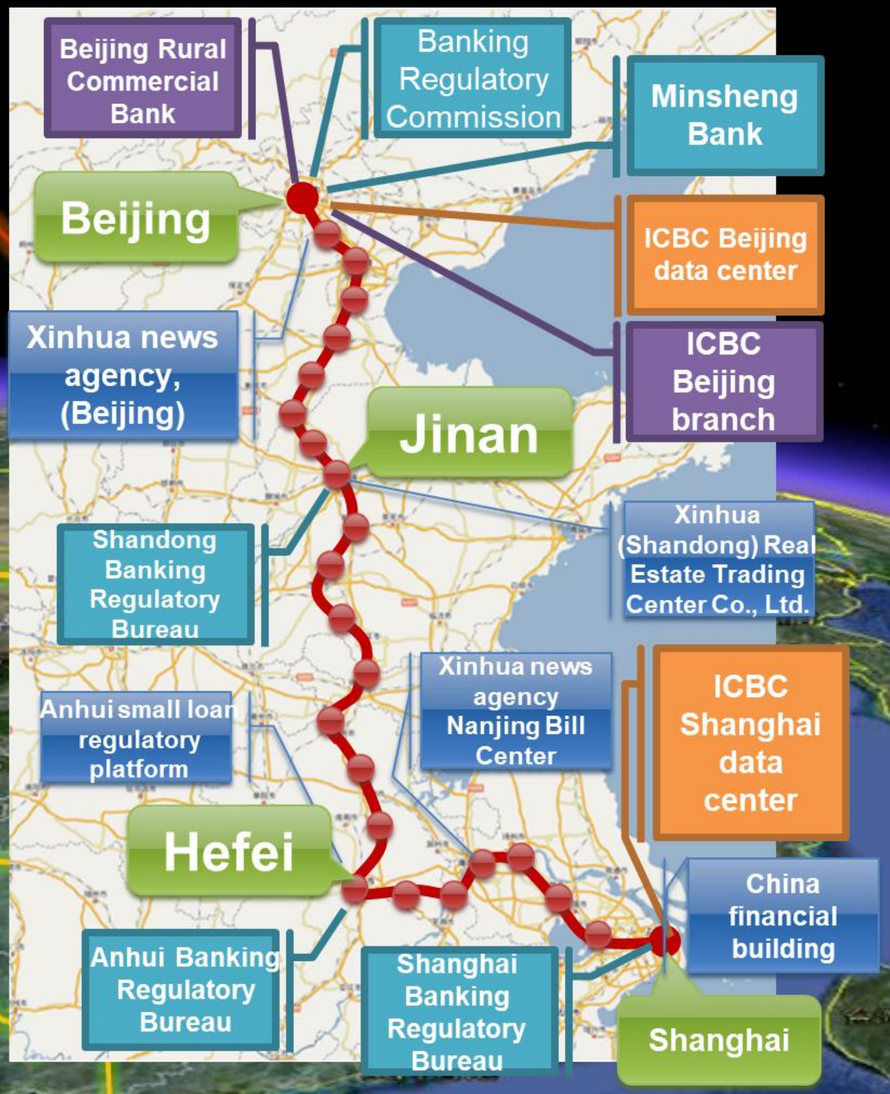

Flexible and easy integration with various applications
Security certification
Use Cases and Requirements
Guide
Application layer tech.
Guide
Network Architecture
Key Management layer tech.
Network OAM
Quantum Layer tech.
Quantum Components
Security evaluation method
Guide
QKD System Security Requirement
Classical layer security Requirement
Quantum Information Process*
Inter-operability and conformance for QKD network
Future quantum repeater issues

CCSA QKD Standardization Route*

*Session 6A Global Standardization Progress" Quantum Secure Communication Standardization in CCSA-ST7"

Satellite-ground integrated QKD networks in China

- 2000 km Beijing-to-Shanghai backbone (2013~2017)
- World‘s first quantum satellite “Micius”(2016~)
- Hierarchical: metropolitan access network, wide-area fiber backbone network and 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.



Beijing Rural Commercial Bank

Banking Regulatory Commission

Minsheng Bank

Beijing

ICBC Beijing data center

ICBC Beijing branch

Xinhua news agency, (Beijing)

Jinan

Xinhua (Shandong) Real Estate Trading Center Co., Ltd.

Shandong Banking Regulatory Bureau

Xinhua news agency Nanjing Bill Center

ICBC Shanghai data center

Anhui small loan regulatory platform

Hefei

China financial building

Anhui Banking Regulatory Bureau

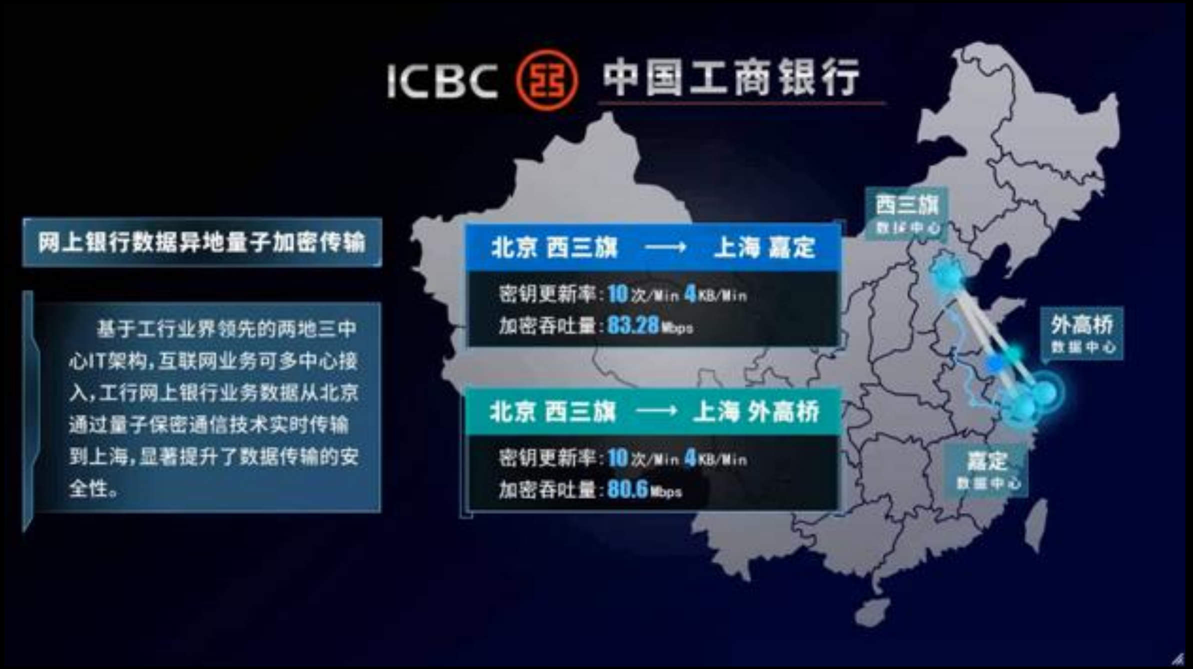
Shanghai Banking Regulatory Bureau

Shanghai

▲ QKD applications along Beijing-Shanghai trunk

QKD applications in financial sectors

量子网络
CAS QUANTUMNET



ICBC 中国工商银行

网上银行数据异地量子加密传输

基于工行业界领先的两地三中心IT架构，互联网业务可多中心接入，工行网上银行业务数据从北京通过量子保密通信技术实时传输到上海，显著提升了数据传输的安全性。

北京 西三旗 ⟶ 上海 嘉定

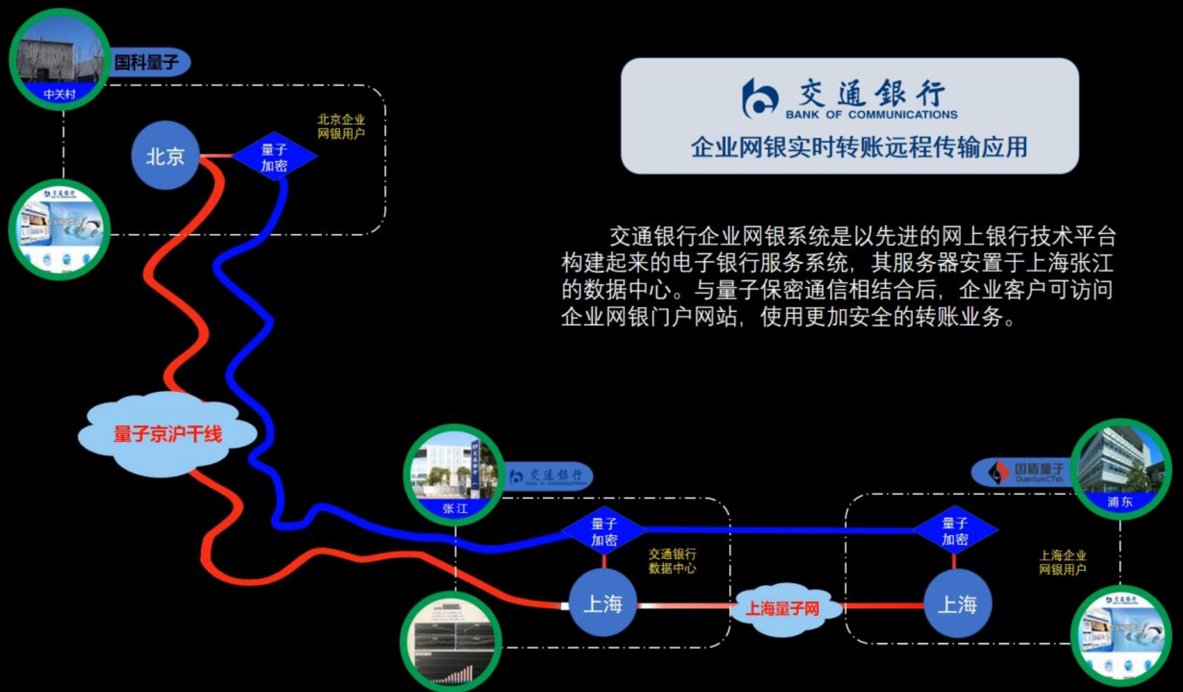
密钥更新率：10次/Min 4KB/Min

加密吞吐量：83.28Mbps

北京 西三旗 ⟶ 上海 外高桥

密钥更新率：10次/Min 4KB/Min

加密吞吐量：80.6Mbps



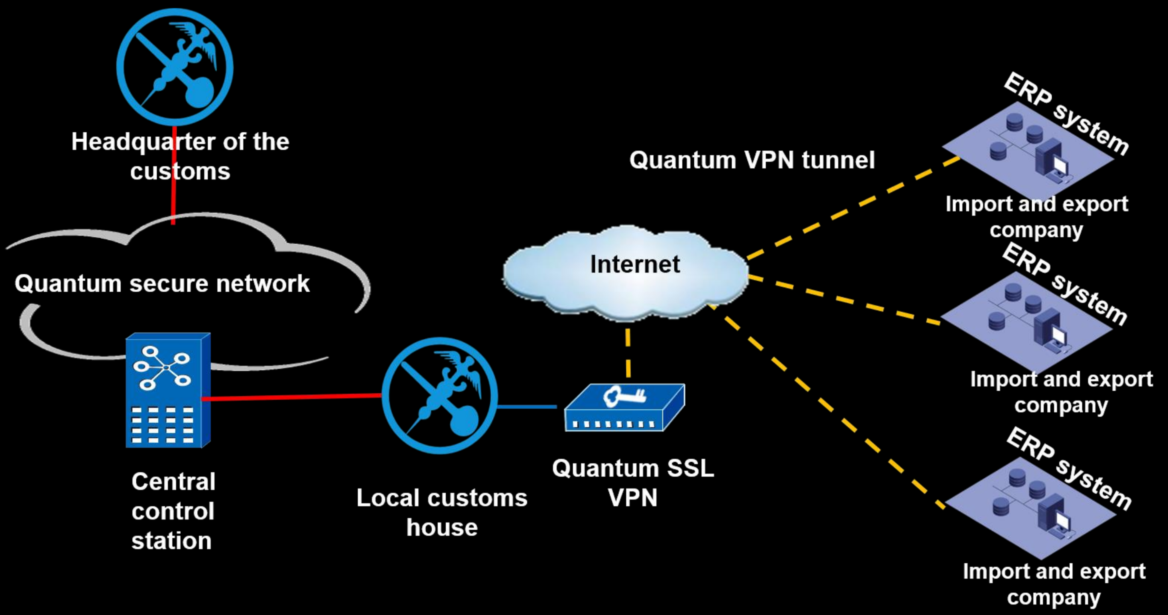
交通银行
BANK OF COMMUNICATIONS
企业网银实时转账远程传输应用

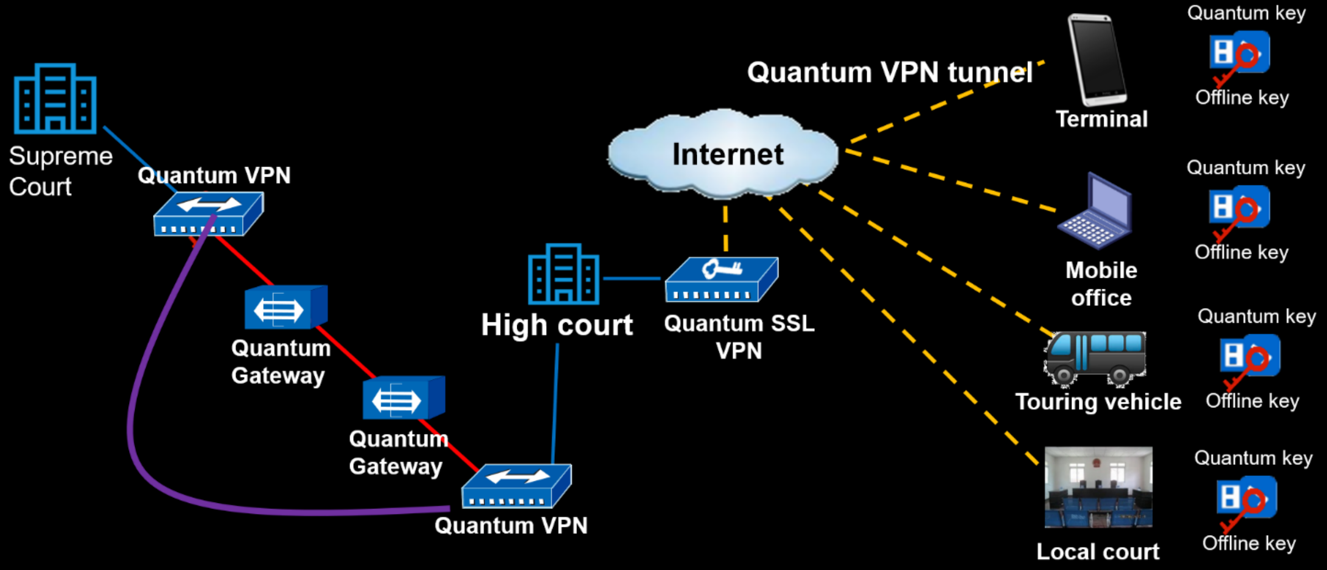
交通银行企业网银系统是以先进的网上银行技术平台构建起来的电子银行服务系统，其服务器安置于上海张江的数据中心。与量子保密通信相结合后，企业客户可访问企业网银门户网站，使用更加安全的转账业务。

- QKD network-based bank data transfer and data center backup in ICBC
- Security enhancement of business data transfer

- Online banking and transactions for enterprise users with QKD security enhancement in Bank of Communications

QKD trail applications in other domain





➢ Customs ERP network system

- Using quantum secure communication to improve the information security level of import and export enterprise network access to customs intranet and ERP data center. The project is planned to be promoted in the national customs system, covering more than 1.6 million import and export enterprises.

➢ QKD network for Court system

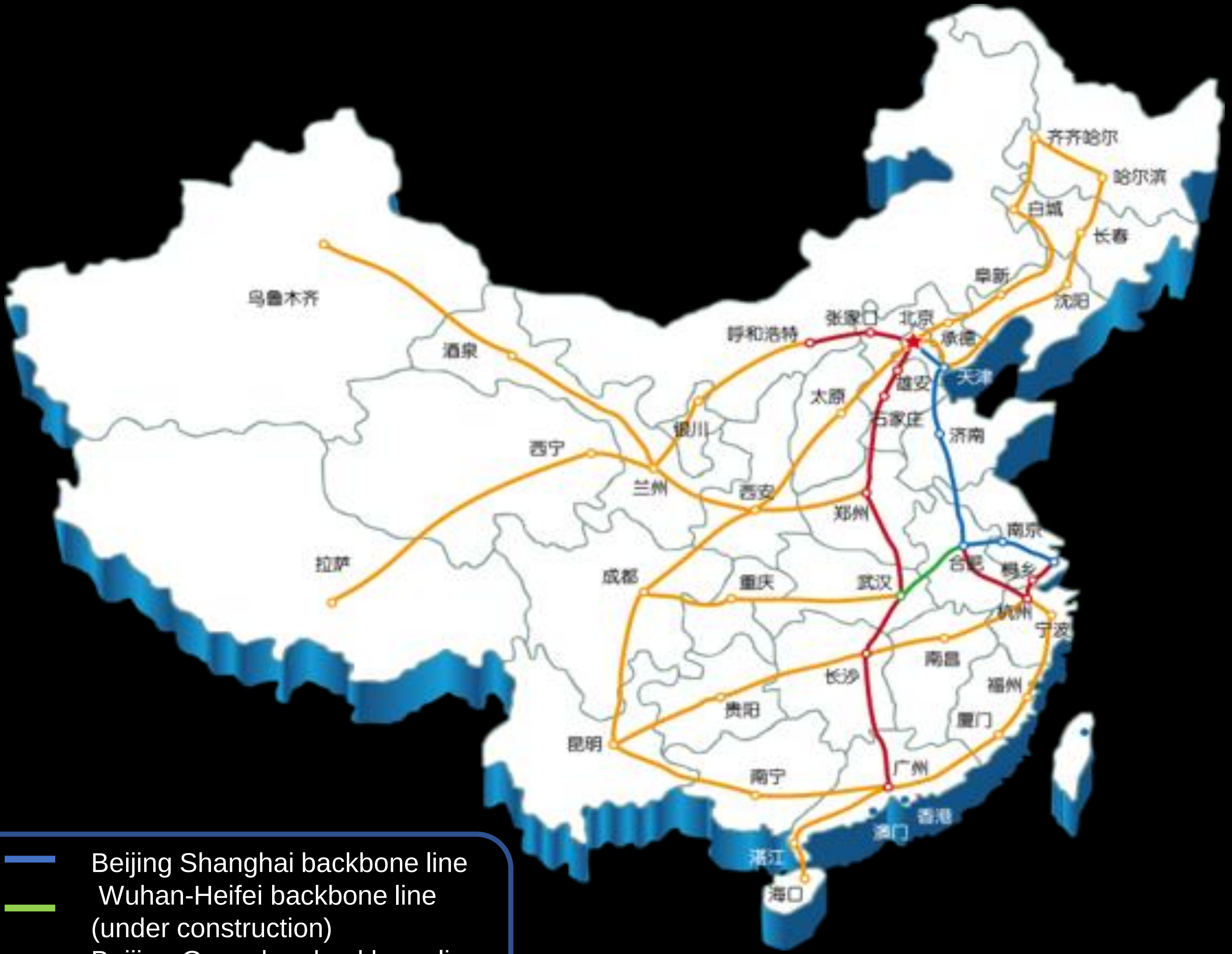
- Supreme Court and Local High Court achieve cross-province quantum encrypted data transmission through "Beijing-Shanghai quantum backbone line". High Court uses offline quantum key to ensure safe applications of the court business system in the Internet environment.

- **Session 3B Application**
- **Session 3D Products**

National quantum secure communication backbone network

量子网络
CAS QUANTUMNET

- From 2017 to 2025, we will build a national wide-area quantum communication backbone network " Satellite-ground integration, five-horizontal and six-vertical lines".
- With a total length of about 35,000 kilometers, it covers large and medium-sized cities across the country and connects to major data centers.
- Coverage extends to oversea regions, services for national strategies and secure communications with foreign institutions.



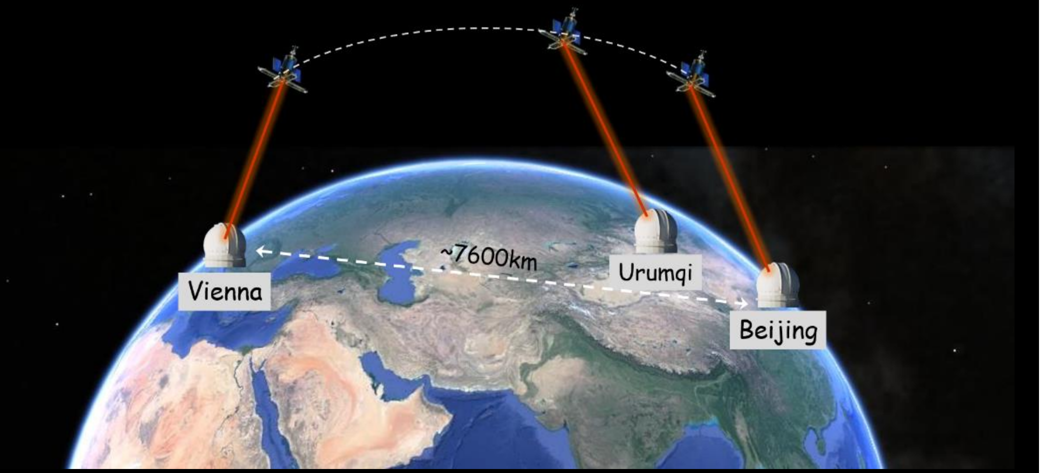
🟦 Beijing Shanghai backbone line

🟩 Wuhan-Heifei backbone line (under construction)

🟥 Beijing-Guanzhou backbone line (planned)

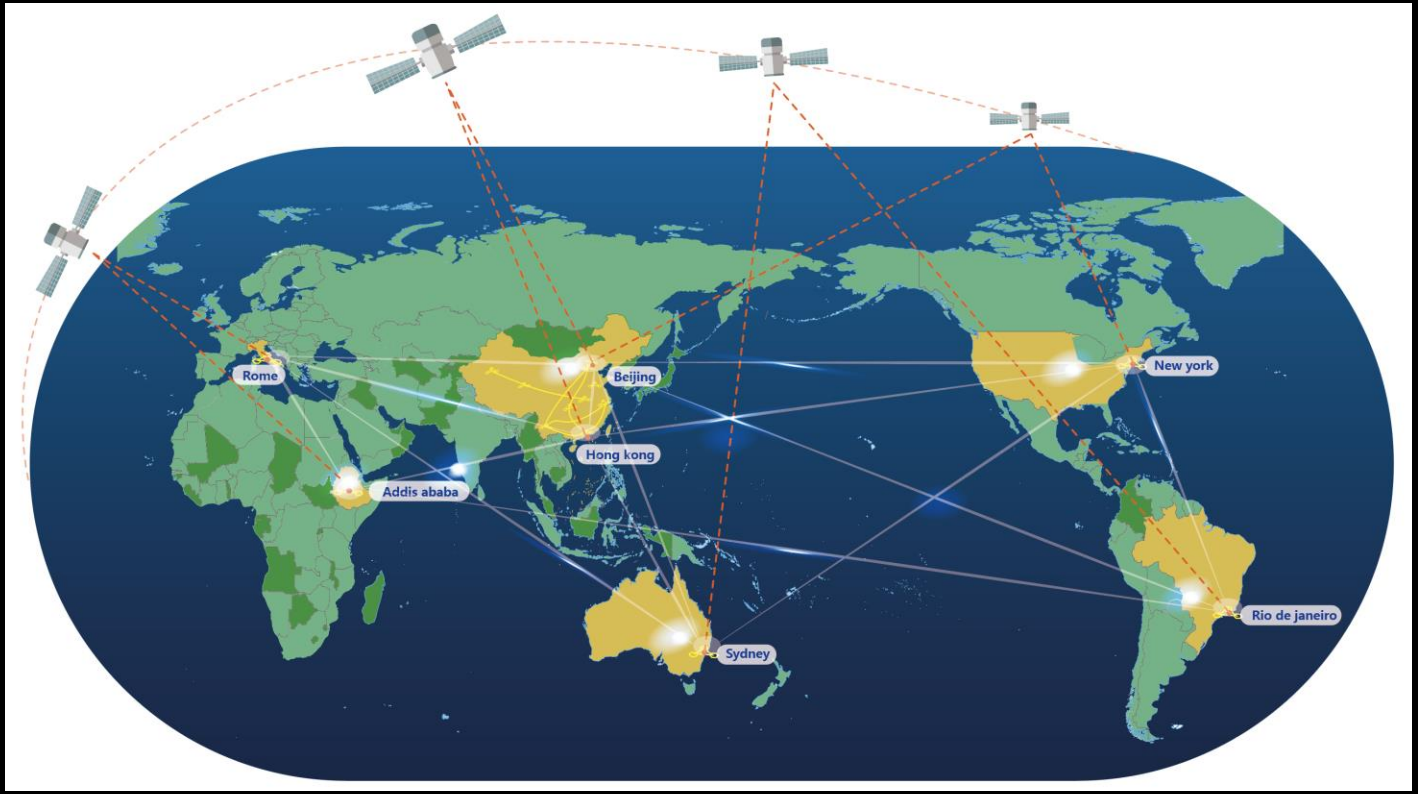
🟨 National wide (future plan)

Global satellite-based QKD network



[Liao et al., PRL 120, 030501 (2018)]

- Intercontinental QKD with "Micius" quantum satellite
- AES encrypted video call using quantum keys from QKD
- Feasibility demo: Satellite as a trusted relay



- Global Satellite-ground integrated QKD networks
- Ambitious and challenges but feasible....
- Coming in near future!

Thanks!

Q&A