ITU WORKSHOP ON QUANTUM INFORMATION TECHNOLOGY (QIT) FOR NETWORKS
量子信息技术国际研讨会

CAICT 中国信息通信研究院
China Academy of Information and Communications Technology

Development and evaluation of QKD-based secure communication in China

China Academy of Information and Communication Technology（CAICT）

Wen-yu Zhao

Email: zhaowenyu@caict.ac.cn

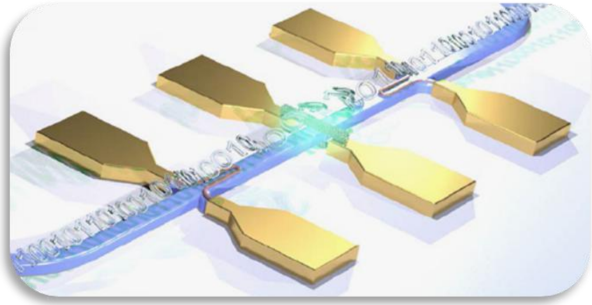
6 June 2019

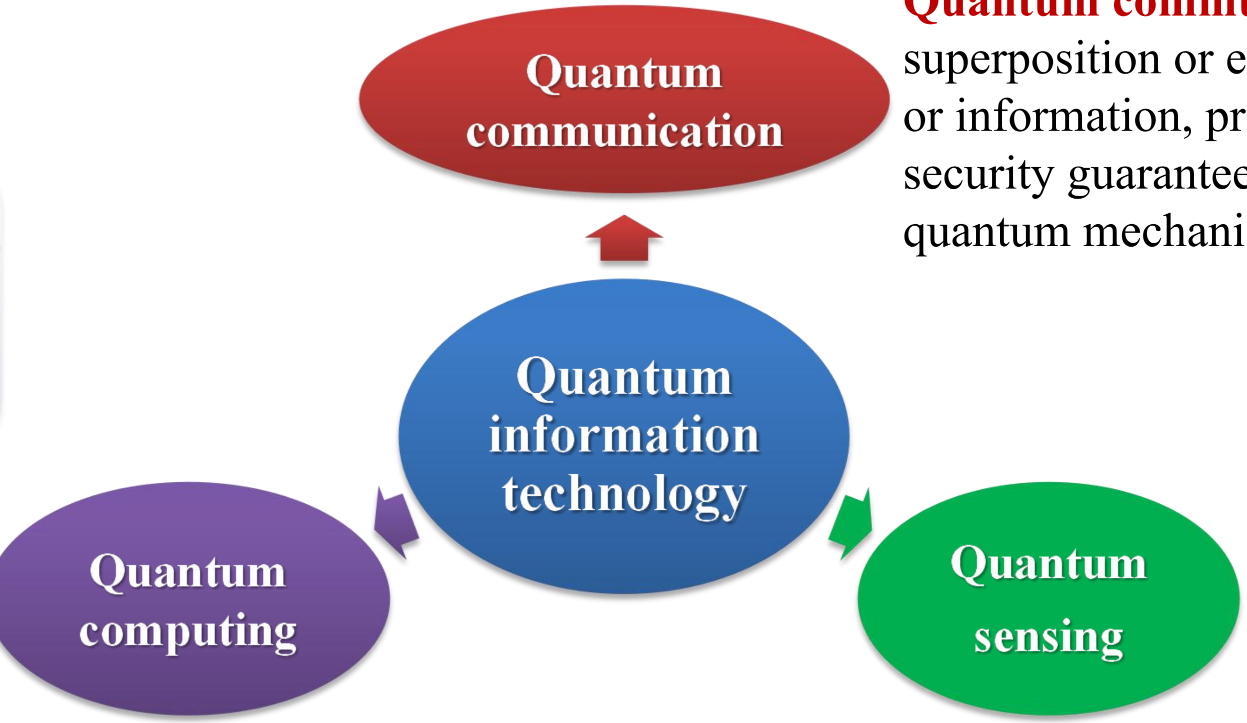
中国信息通信研究院
http://www.caict.ac.cn

Outline

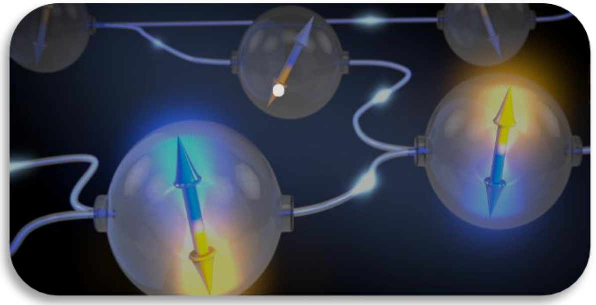
- Background
- Status of QKD-based secure communication(QSC) in China
- Test and evaluation of QSC
- Conclusion

Quantum information technology (QIT) overview

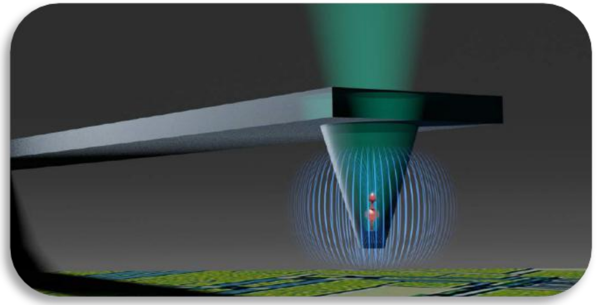




Quantum communication use quantum superposition or entanglement to transmit key or information, provides information theory security guarantee based on the principle of quantum mechanics.

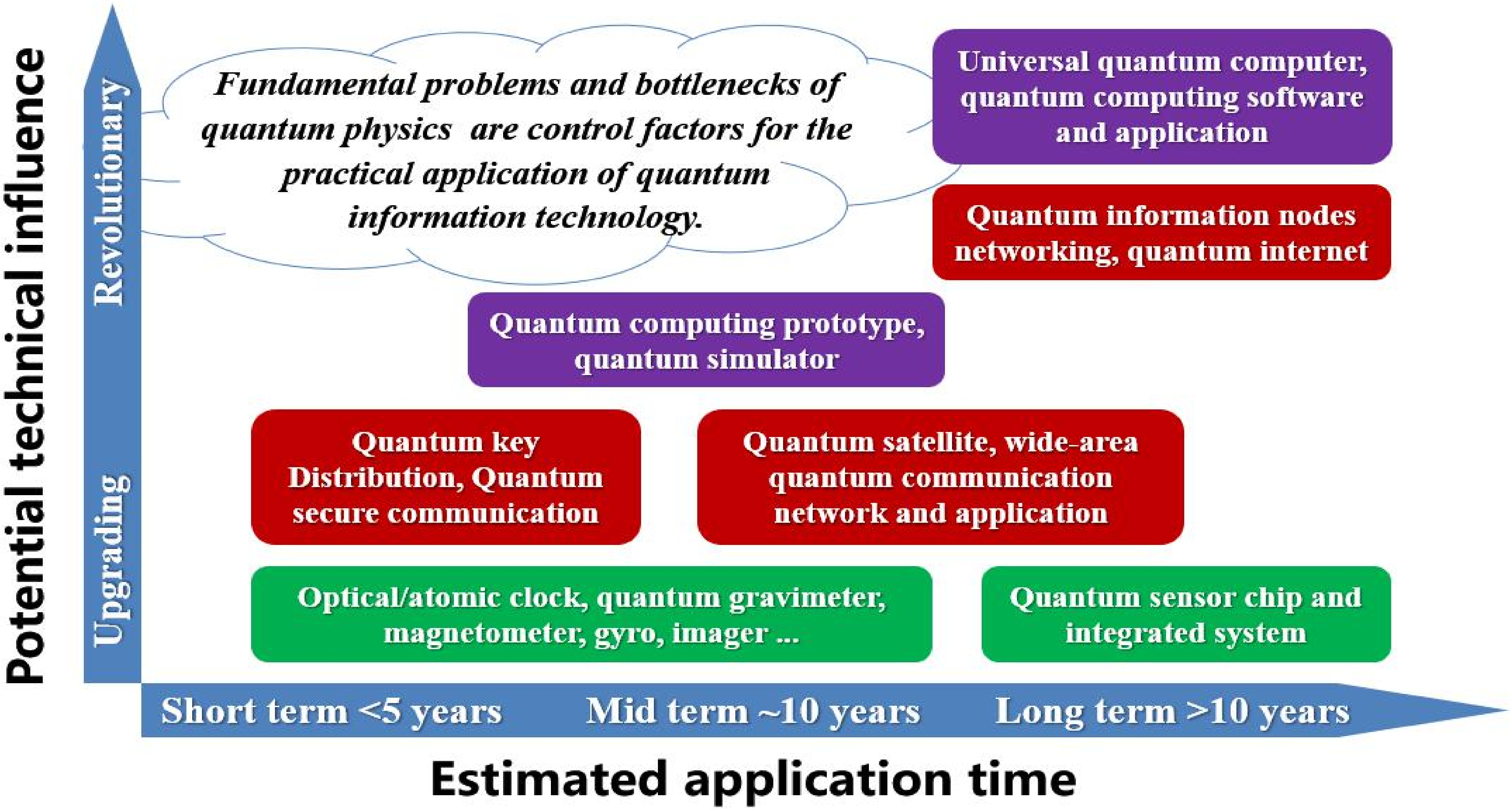


Quantum computing use quantum bits to realize information coding , storage and processing through the controlled evolution of quantum states, which can provides superior computing and information processing capability.



Quantum sensing manipulate and detect the particle quantum state to measure various physical quantities such as gravity, magnetic field and time, which has advantages in accuracy, sensitivity and stability.

Prospects of future QIT application and influence



Potential technical influence

Revolutionary

Upgrading

Fundamental problems and bottlenecks of quantum physics are control factors for the practical application of quantum information technology.

Universal quantum computer, quantum computing software and application

Quantum information nodes networking, quantum internet

Quantum computing prototype, quantum simulator

Quantum key Distribution, Quantum secure communication

Quantum satellite, wide-area quantum communication network and application

Optical/atomic clock, quantum gravimeter, magnetometer, gyro, imager ...

Quantum sensor chip and integrated system

Short term <5 years

Mid term ~10 years

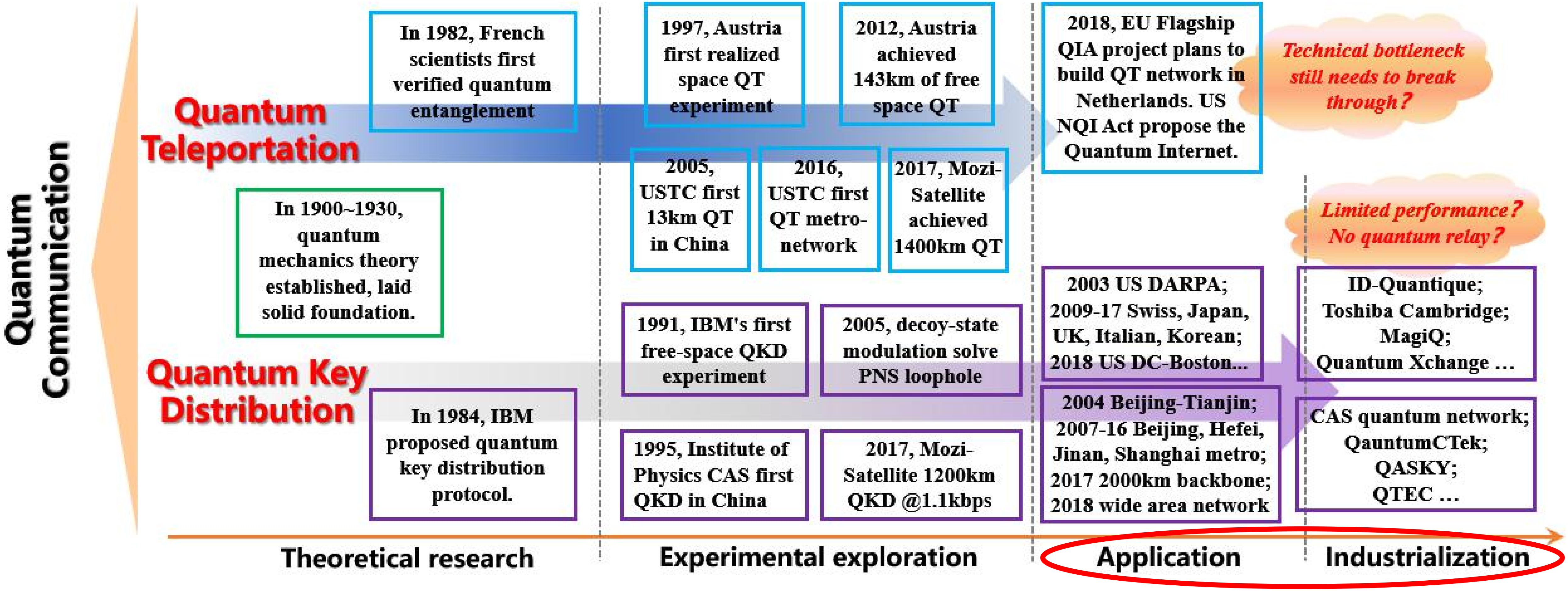
Long term >10 years

Estimated application time

Brief of quantum communication development

CAICT

- **Quantum teleportation** can realize direct transmission of quantum information, is still in the stage of experimental research. **Quantum key distribution** can share keys between the two parties and use the keys to encrypt information, has entered the preliminary practical stage.



Quantum Communication

Quantum Teleportation

Quantum Key Distribution

Theoretical research

In 1900~1930, quantum mechanics theory established, laid solid foundation.

In 1982, French scientists first verified quantum entanglement

In 1984, IBM proposed quantum key distribution protocol.

Experimental exploration

1997, Austria first realized space QT experiment

2012, Austria achieved 143km of free space QT

2005, USTC first 13km QT in China

2016, USTC first QT metro-network

2017, Mozi-Satellite achieved 1400km QT

1991, IBM's first free-space QKD experiment

2005, decoy-state modulation solve PNS loophole

1995, Institute of Physics CAS first QKD in China

2017, Mozi-Satellite 1200km QKD @1.1kbps

Application

2018, EU Flagship QIA project plans to build QT network in Netherlands. US NQI Act propose the Quantum Internet.

2003 US DARPA; 2009-17 Swiss, Japan, UK, Italian, Korean; 2018 US DC-Boston...

2004 Beijing-Tianjin; 2007-16 Beijing, Hefei, Jinan, Shanghai metro; 2017 2000km backbone; 2018 wide area network

Industrialization

Technical bottleneck still needs to break through?

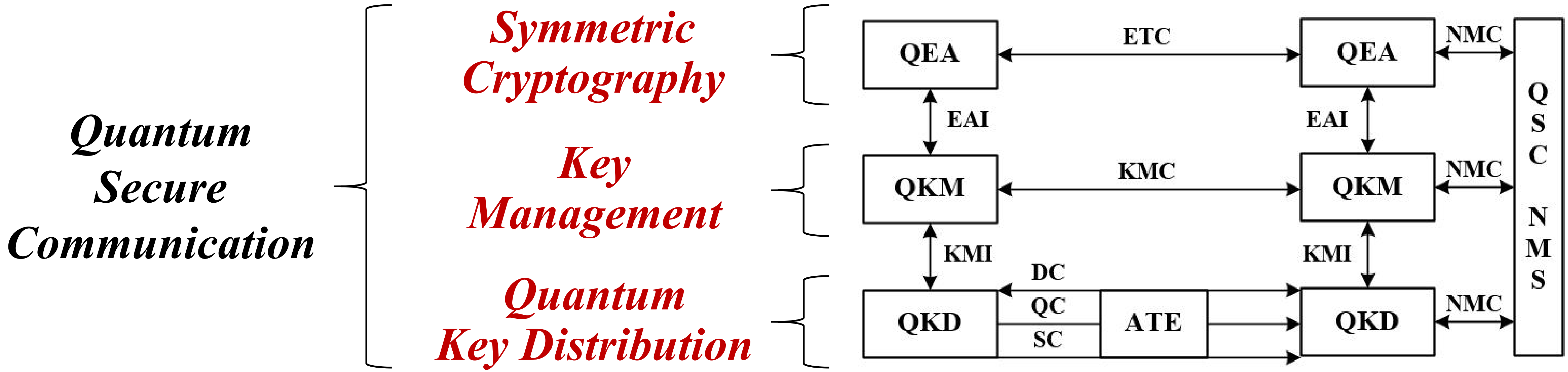
Limited performance? No quantum relay?

ID-Quantique; Toshiba Cambridge; MagiQ; Quantum Xchange …

CAS quantum network; QauntumCTek; QASKY; QTEC …

QKD-based secure communication

- ➢ Quantum key distribution (QKD) , typically Decoyed-BB84, can provide theoretically unconditional security of key sharing based on the laws of quantum physics only.
- ➢ QKD based symmetric cryptography, which can be referred as **quantum secure communication (QSC)**, is one of the promising information security solutions in the post-quantum era.



Quantum Secure Communication

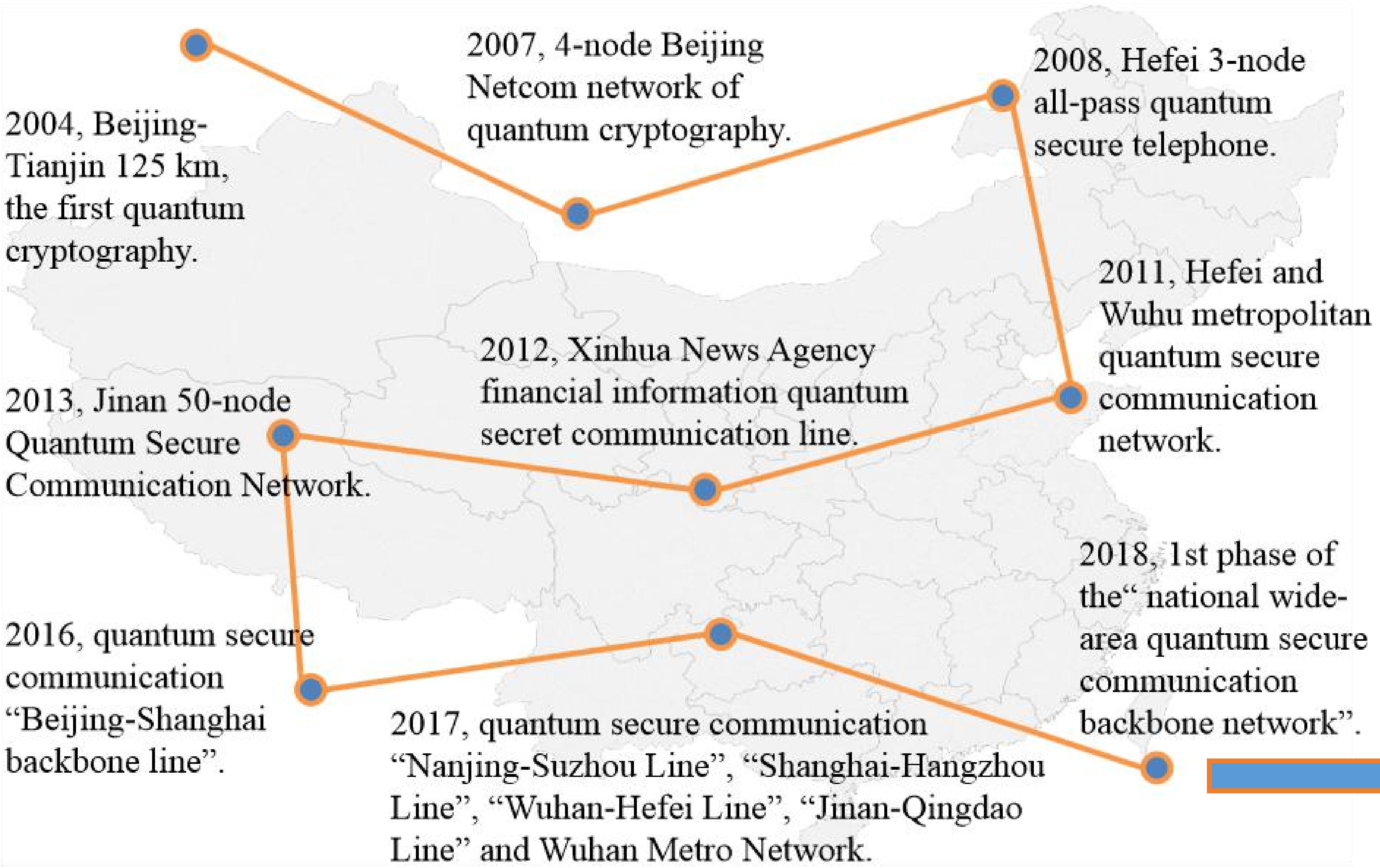
Symmetric Cryptography

Key Management

Quantum Key Distribution

ATE:	auxiliary transmission equipment	KMC:	key manage channel	QEA:	quantum encryption application
DC:	quantum channel	KMI:	key manage interface	QKM:	quantum key management
EAI:	encryption application interface	NMC:	network manage channel	SC:	synchronization channel
ETC:	encrypted transmission channel	QC:	quantum channel		

QKD-based QSC demo and trial network in China



2004, Beijing-Tianjin 125 km, the first quantum cryptography.

2007, 4-node Beijing Netcom network of quantum cryptography.

2008, Hefei 3-node all-pass quantum secure telephone.

2011, Hefei and Wuhu metropolitan quantum secure communication network.

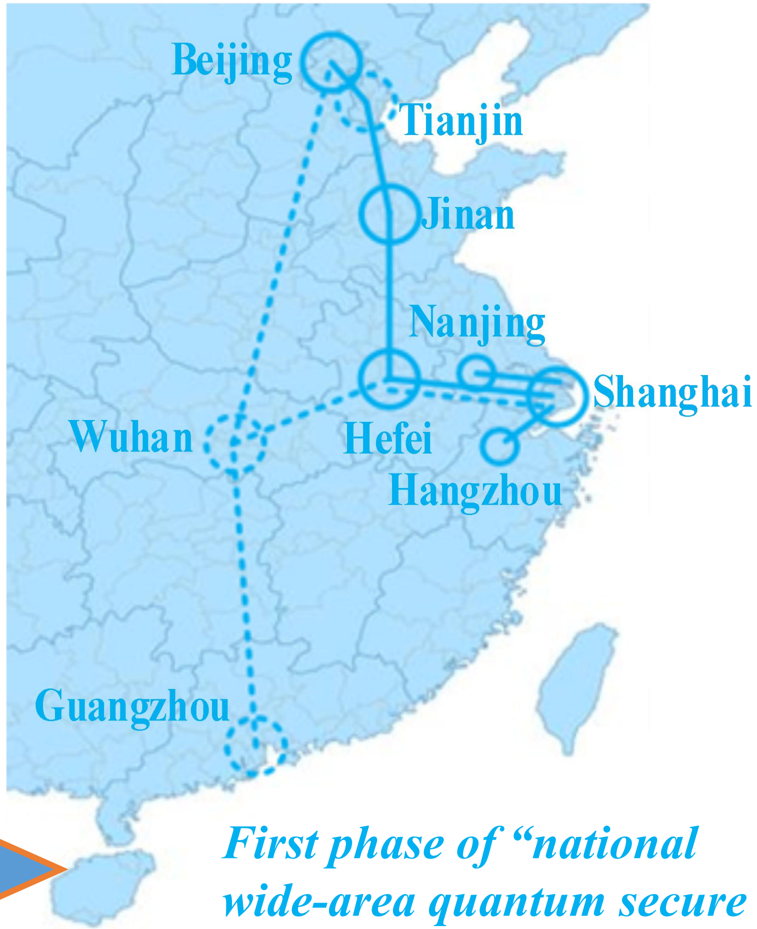
2012, Xinhua News Agency financial information quantum secret communication line.

2013, Jinan 50-node Quantum Secure Communication Network.

2016, quantum secure communication “Beijing-Shanghai backbone line”.

2017, quantum secure communication “Nanjing-Suzhou Line”, “Shanghai-Hangzhou Line”, “Wuhan-Hefei Line”, “Jinan-Qingdao Line” and Wuhan Metro Network.

2018, 1st phase of the“ national wide-area quantum secure communication backbone network”.



First phase of “national wide-area quantum secure communication backbone network “project

QSC industry status in China

CAICT

Information Security Application

Government

Hefei

Jinan

Wuhan…

Financial

中国工商银行
INDUSTRIAL AND COMMERCIAL BANK OF CHINA

交通银行
BANK OF COMMUNICATIONS

Infrastructure

国家电网
STATE GRID

Data center

阿里云

腾讯云

…

Network Construction & Operation

量子网络
CAS QUANTUMNET

HTGD 亨通集团
HENGTONG GROUP

中国有线

中国通信建设
CITCC

QUSENJOY
神州量子

问创力量子

神州信息
DCITS

中国通信服务
CHINA COMSERVICE

…

System Research & Development

国盾量子
QuantumCTek

asky

循态量子
XT Quantech

皖通邮电

QTEC
九州量子

国腾量子
NATIONAL-QUANTUM

HUAWEI

Accelink

…

Academic Research & Experiment

USTC THU SXU NJU BUPT PKU SJTU JNIQ SCNU

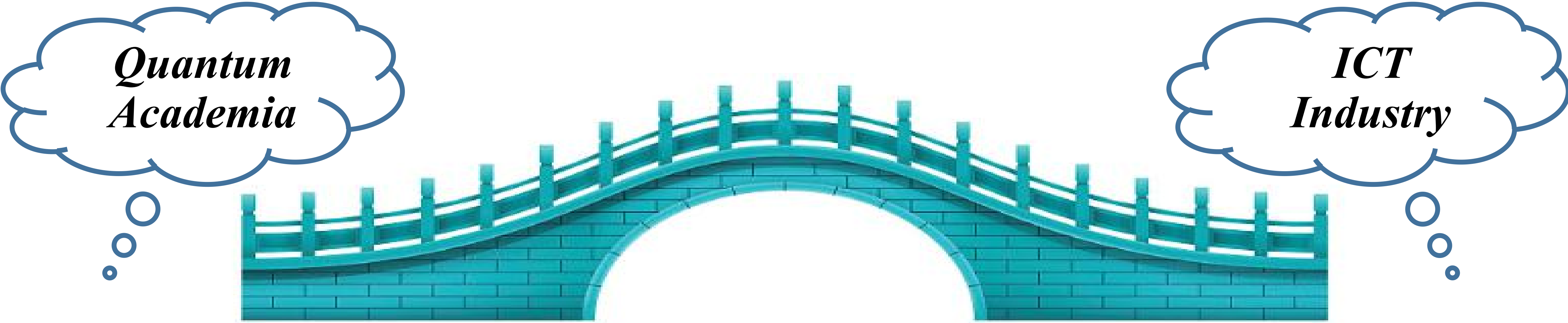
…

The role of CAICT in QSC industry

- ➢ Frontier scientific research
- ➢ Hero experiments
- ➢ Demonstration application
- ➢ …

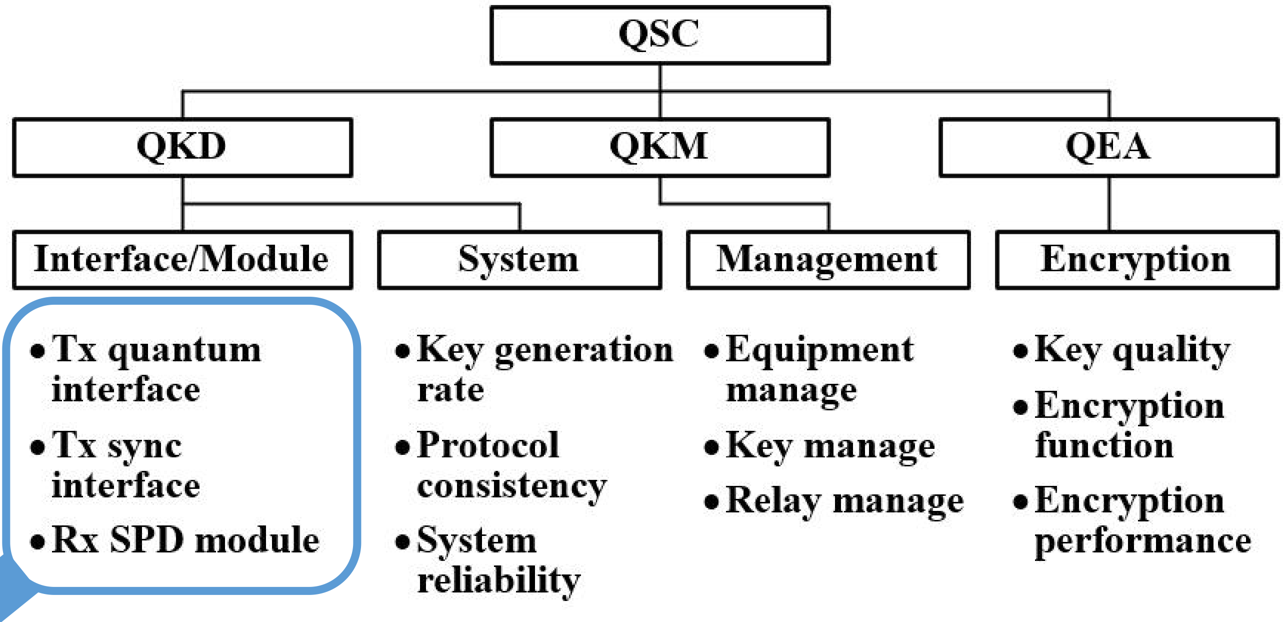
- ➢ **Industrialization research**
- ➢ **Test and evaluation**
- ➢ **Standardization**
- ➢ …

- ➢ Industrial application
- ➢ Network deployment
- ➢ Business operation
- ➢ …



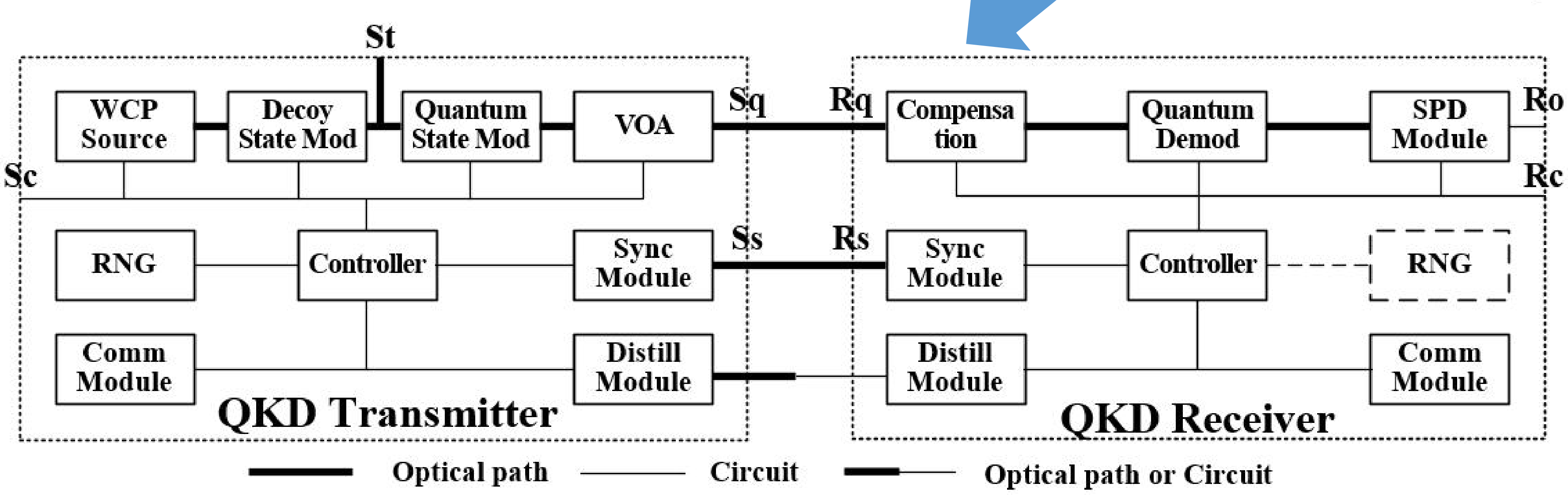
Test and evaluation framework of QSC system

- Test and evaluation is indispensable step for QKD-based QSC technology to get industrial application and large scale deployment.
- Test evaluation framework of QKD/QSC system function and performance has been established. Requirements of QSC system and network verification have been considered.



QSC

- QKD
  - Interface/Module
    - Tx quantum interface
    - Tx sync interface
    - Rx SPD module
  - System
    - Key generation rate
    - Protocol consistency
    - System reliability
- QKM
  - Management
    - Equipment manage
    - Key manage
    - Relay manage
- QEA
  - Encryption
    - Key quality
    - Encryption function
    - Encryption performance

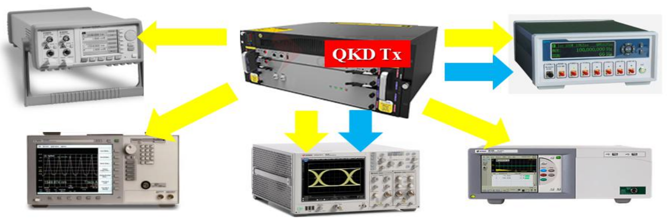


Reference points

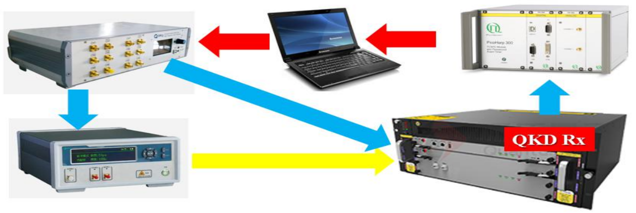
Sc:	Transmitter clock signal
Sq:	Transmitter quantum signal
Ss:	Transmitter synchronization signal
St:	Transmitter test signal
Rc:	Receiver clock signal
Ro:	Receiver SPD output signal
Rq:	Receiver quantum signal
Rs:	Receiver synchronization signal

Quantum key distribution system evaluation

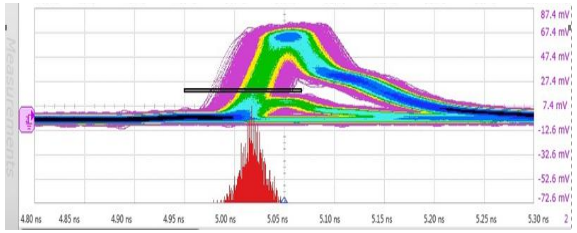
- SPD in QKD receiver is directly related to system key rate and transmission performance. The detecting probability (η), after-pulse probability, dark count, dead time, and detection response of SPD can be measured by a comprehensive test environment.
- G.652D SSMF and VOA are used to test QKD system key rate under different channel loss. BB84 protocol consistency can be checked by distillation channel packet capture analysis.

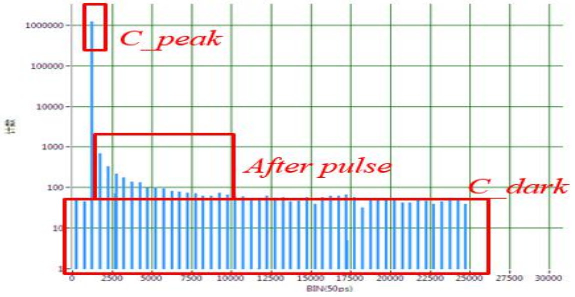


QKD transmitter test



QKD receiver test



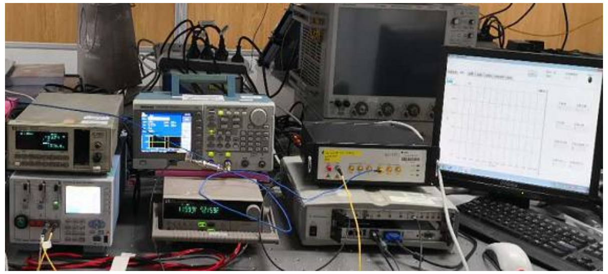


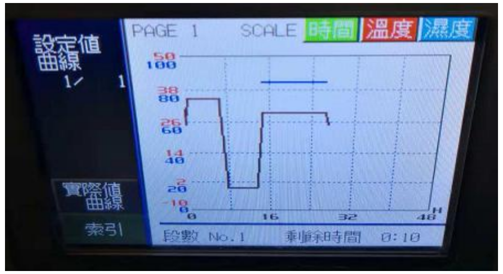
QKD system test projects
Transmitter
Quantum channel time domain: frequency, pulse width, …
Quantum channel frequency domain: wavelength, …
Quantum channel mean-photon-number
Synchronization channel time domain: frequency, pulse width, …
Synchronization channel frequency domain: wavelength, …
QRNG Randomness
Receiver
Gated signal time domain: frequency, jitter, …
SPD dark count
SPD detection efficiency
SPD after-pulse-probability
SPD dead time
Synchronization channel receiving sensitivity
System
Key generation rate and relation with channel loss
Key consistency and randomness
BB84 protocol consistency
System startup time
System redundancy protection
System long-term work stability
System reliability under environmental change

Quantum secure communication system evaluation

- Quantum encryption equipment can be VPN, IP router, OTN, or other kind of data transmission equipment which support symmetric encryption and quantum key source input. Several encryption algorithms and check algorithms can be supported, and encrypted channel capacity is various.
- Traditional IKE key backup for the absence of quantum key is also supported. Temperature and humidity variation test are performed to verify system reliability.

QSC system test projects
Auxiliary transmission equipment
WDM: inster loss, wavelength, spectrum, isolation, … Optical lane switch: inster loss, wavelength, switching, …
Key management equipment
Device management function, Key management function Networking management function
Encryption application equipment
Encryption algorithms and functions Encryption service performance Key source backup and switching function Encryption service redundancy protection
System
System startup time System redundancy protection System long-term work stability System reliability under environmental change Clock synchronization function





Typical technical challenges for future QSC application

Practical Security

- Security proof of practical QKD system and protecting solutions against various component loopholes, system side-channels, and attack schemes are under study. The practical QKD and QSC system security test evaluation and standardization are still open questions.

Interoperability

- Because of the point-to-point nature of QKD, the interoperability of QSC network can be considered in the QKM layer. Consistent understanding of key relay strategy, networking interface and management solutions are the prerequisite for further standardization.

Engineering

- QSC system still has some room for improvement in terms of equipment performance, engineering level, standardization degree, stability and reliability, operation and maintenance support capability. It is necessary to further make improvement and test verification.

Conclusion

- *Quantum information technology (QIT) is becoming a hot topic in ICT, QKD-based QSC is one of the promising information security solutions in the post-quantum era.*

- *QSC networks have been constructed in several cities, wide-area network project is under construction, industrial chain will get further development.*

- *Function and performance test evaluation framework of QSC system and network have been established, and some critical parameters of QKD and QSC systems are evaluated by CAICT as a third-party .*

- *There are still some technical challenges and problems for QSC application need to be solved, including practical security, interoperability, and more robust engineering.*

Thanks for your attention!

China Academy of Information and Communication Technology（CAICT）
Wen-yu Zhao
Email: zhaowenyu@caict.ac.cn

6 June 2019