Quantum Secure Communication Networks:

Products and Solutions

QuantumCTek

Yong Zhao

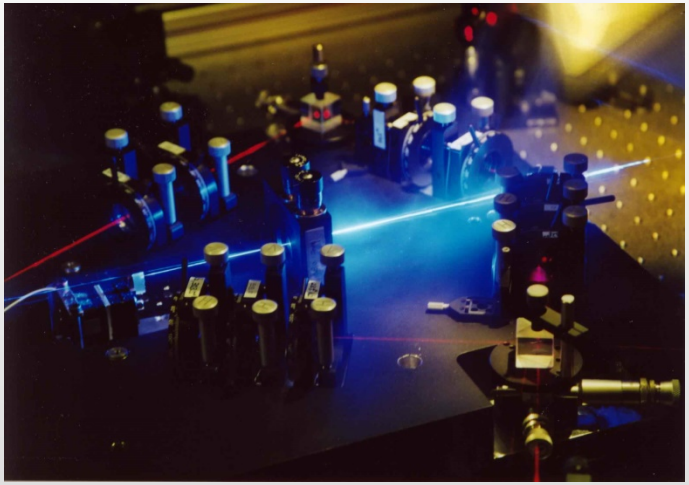
2014-09-04

1 Foundation

Quantum
Communication Technology Co. Ltd., Anhui
安徽量子通信技术有限公司

- Initially founded by the university (USTC) and private investors in 2009

Research Lab (USTC)	Company (QuantumCTeK)



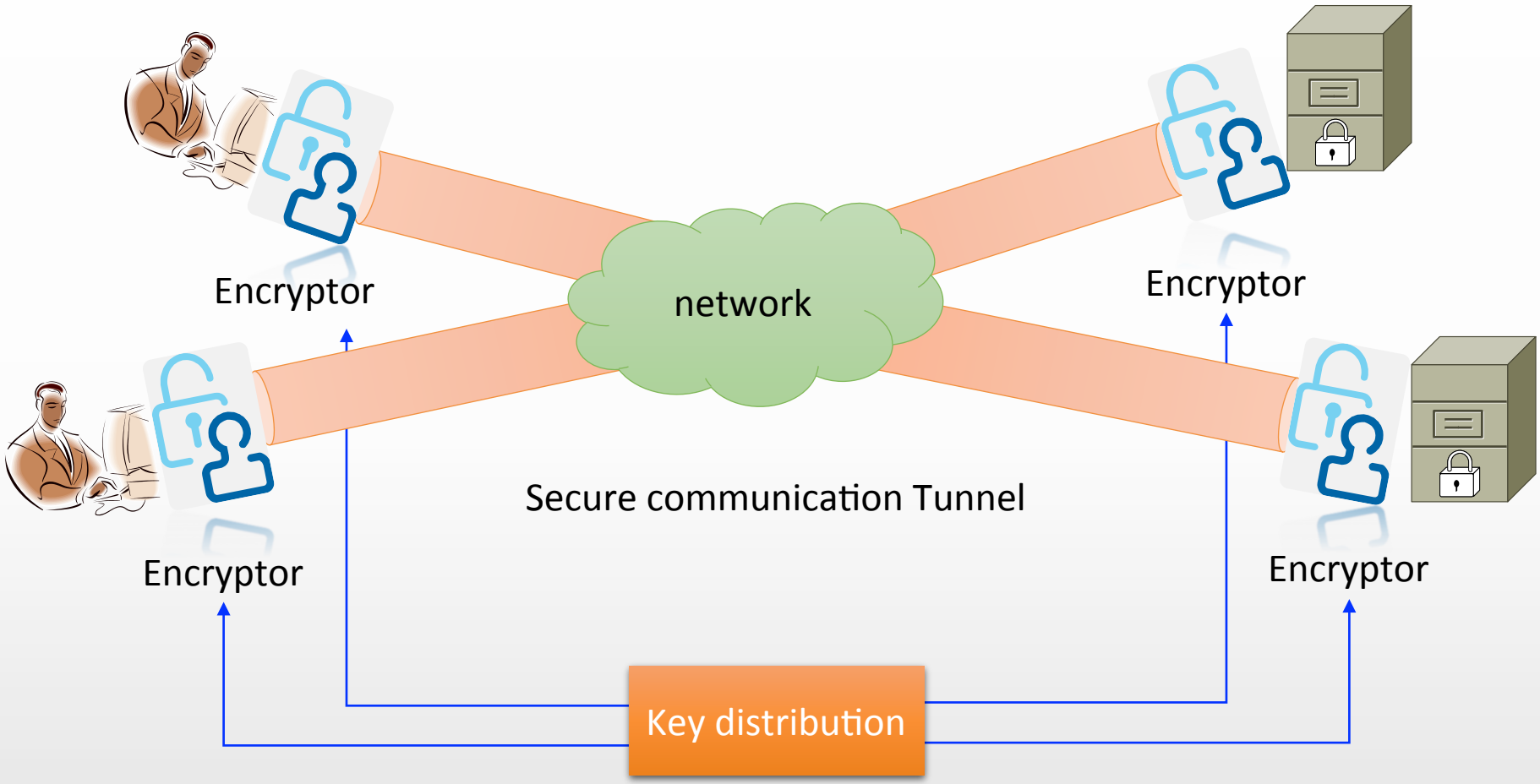
Quantum
Communication Technology Co. Ltd., Anhui
安徽量子通信技术有限公司

- Initially founded by the university (USTC) and private investors in 2009
- Hefei head quarter, three other branches
- Equip commercial fiber with QKD products

Company (QuantumCTeK)

Why QKD and Q-network

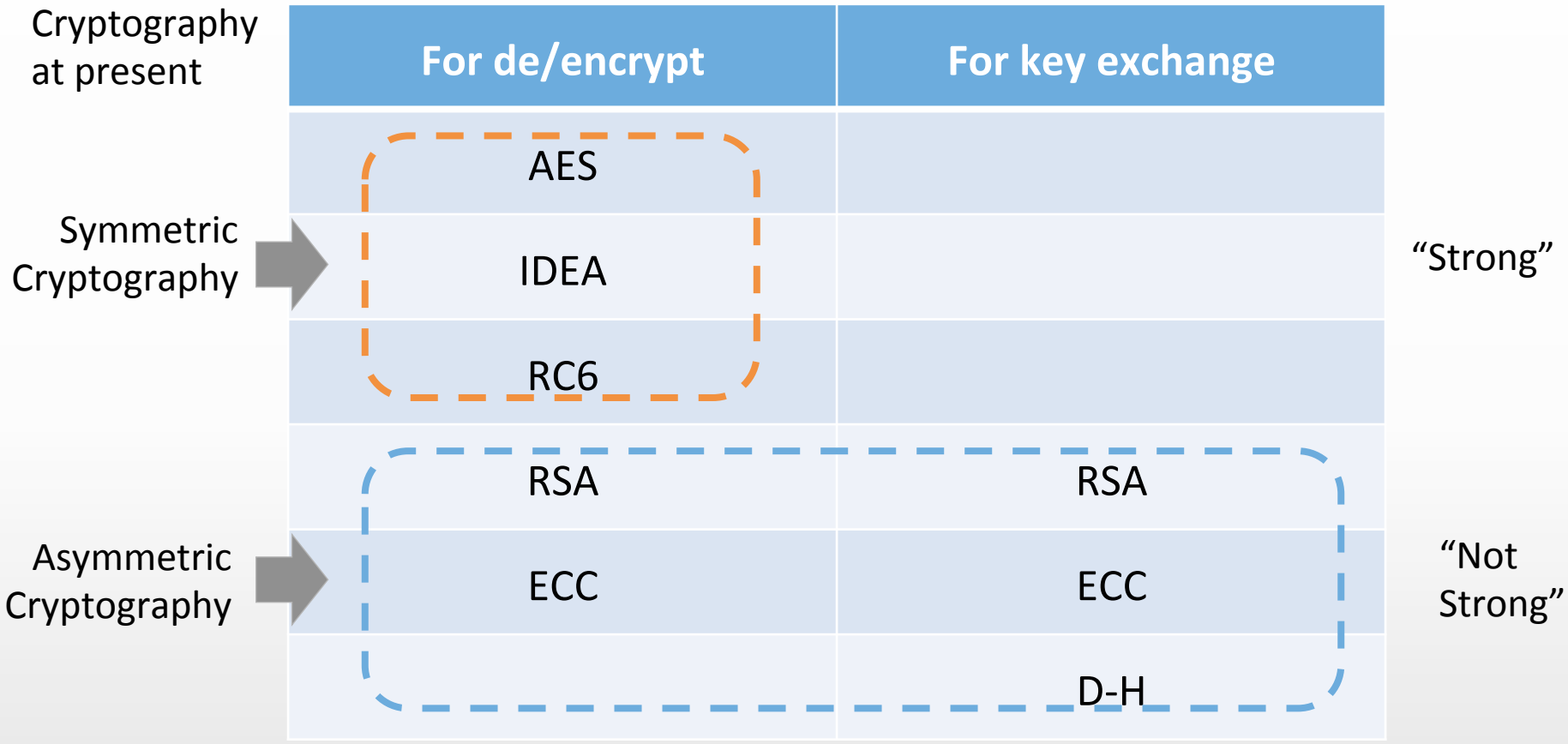
QuantumCTek



Secure communication = Secure encryption + Secure key distribution

Why QKD and Q-network

QuantumCTek

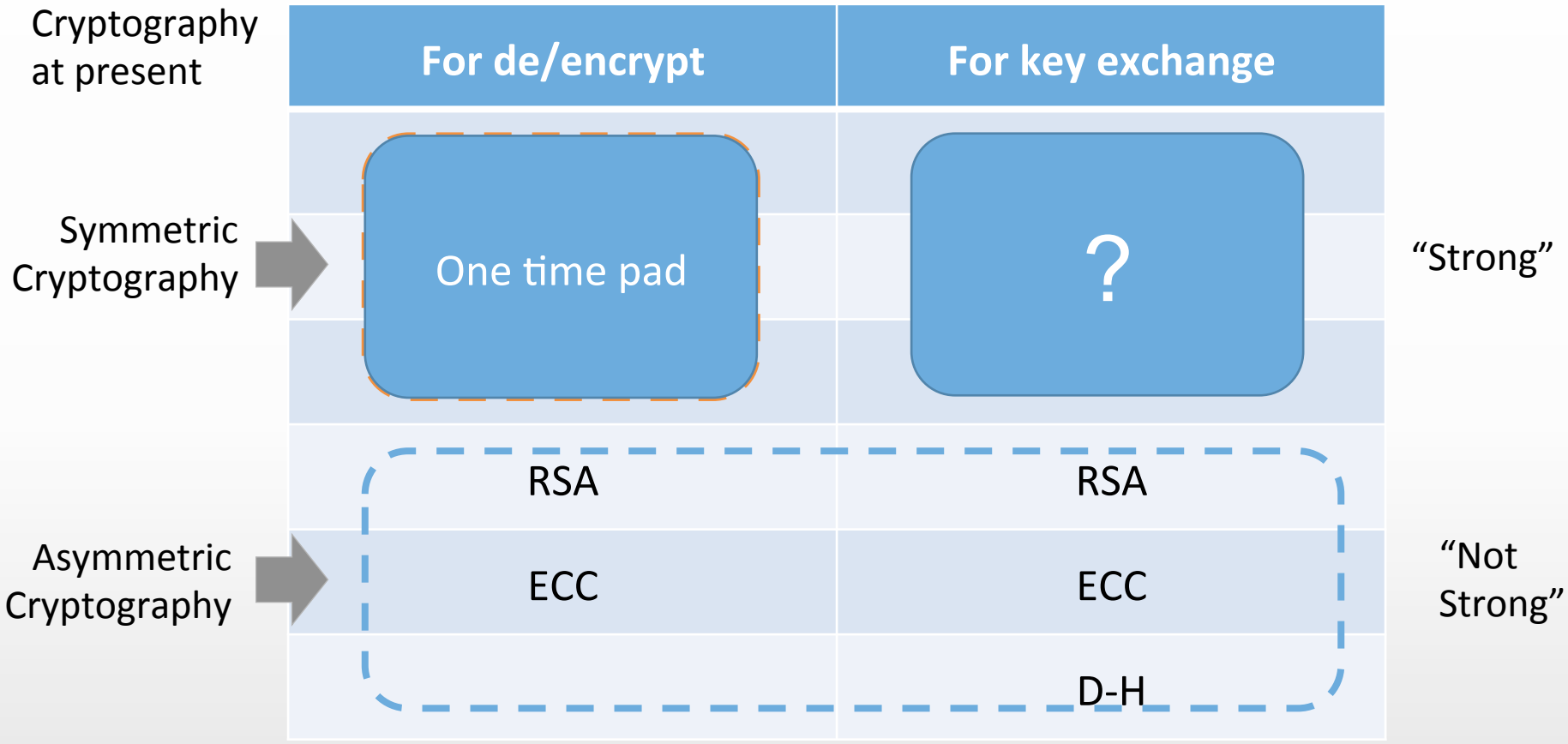


- RSA512 is broken in 1999
- RSA768 is broken in 2009
- RSA1024 is broken in …….

- All Asymmetric Cryptography at present can be broken by Shor's quantum algorithm
- No asymmetric Cryptography can be unconditional secure

Why QKD and Q-network

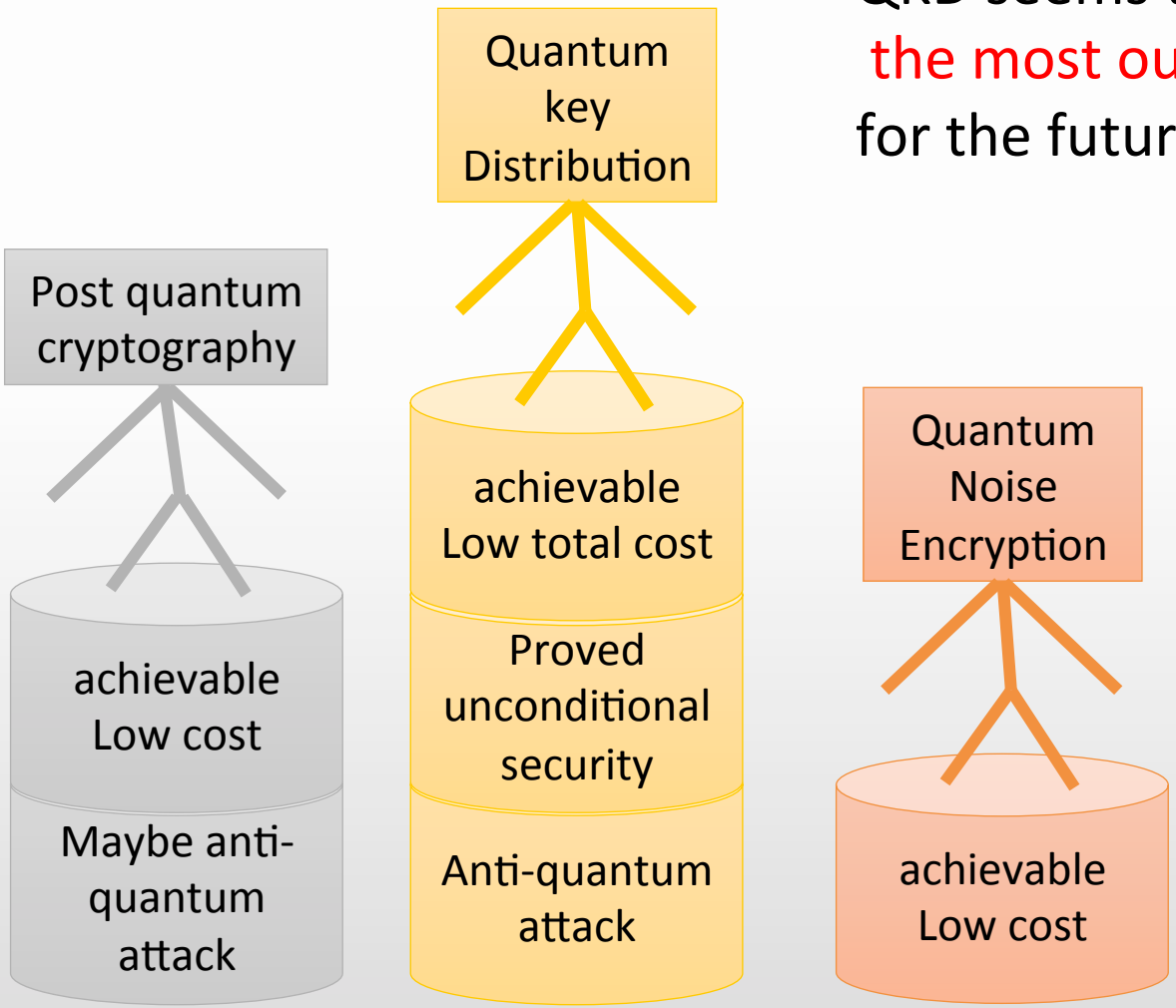
QuantumCTek



- RSA512 is broken in 1999
- RSA768 is broken in 2009
- RSA1024 is broken in …….

- All Asymmetric Cryptography at present can be broken by Shor's quantum algorithm
- No asymmetric Cryptography can be unconditional secure

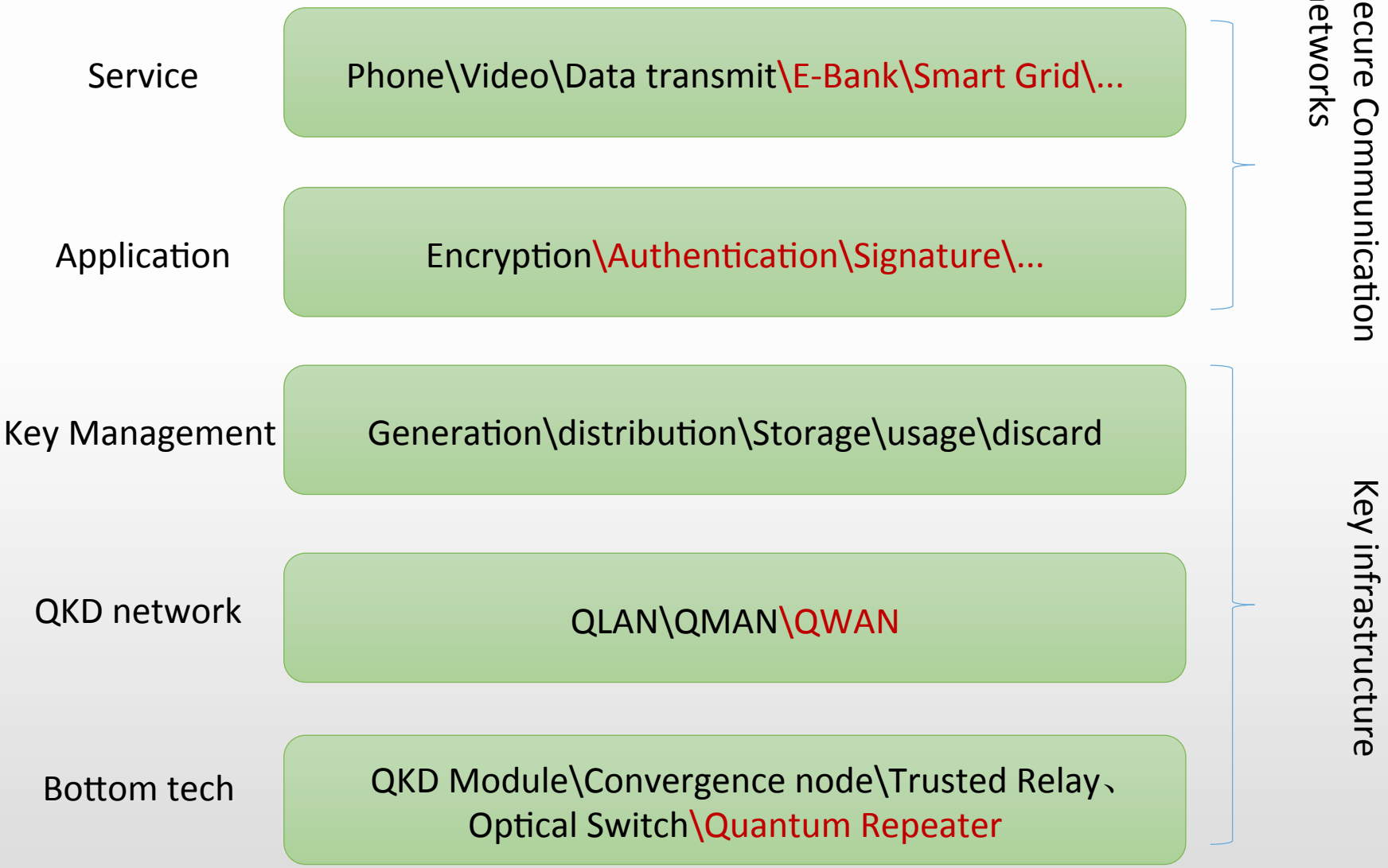
Why QKD and Q-network



QKD seems to be
the most outstanding Candidate
for the future key infrastructure

The goals:

Secure communication networks over Quantum key infrastructure



The Roadmap of QKD network in China

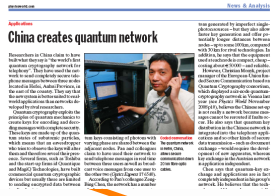
QuantumCTek

2006

- World's first Decoy QKD experiment over 100km

2008

- Quantum phone network(3-nodes)

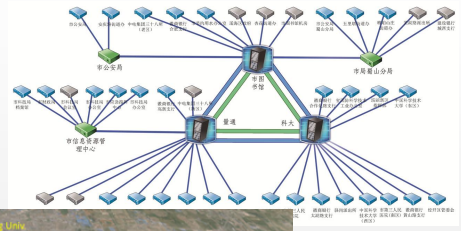

China creates quantum network

2009

- World's first Decoy QKD experiment over 200km
- All pass Metro-area QKD network (5 nodes)

2012

- Hefei Metro-Quantum network(46 nodes)



2013

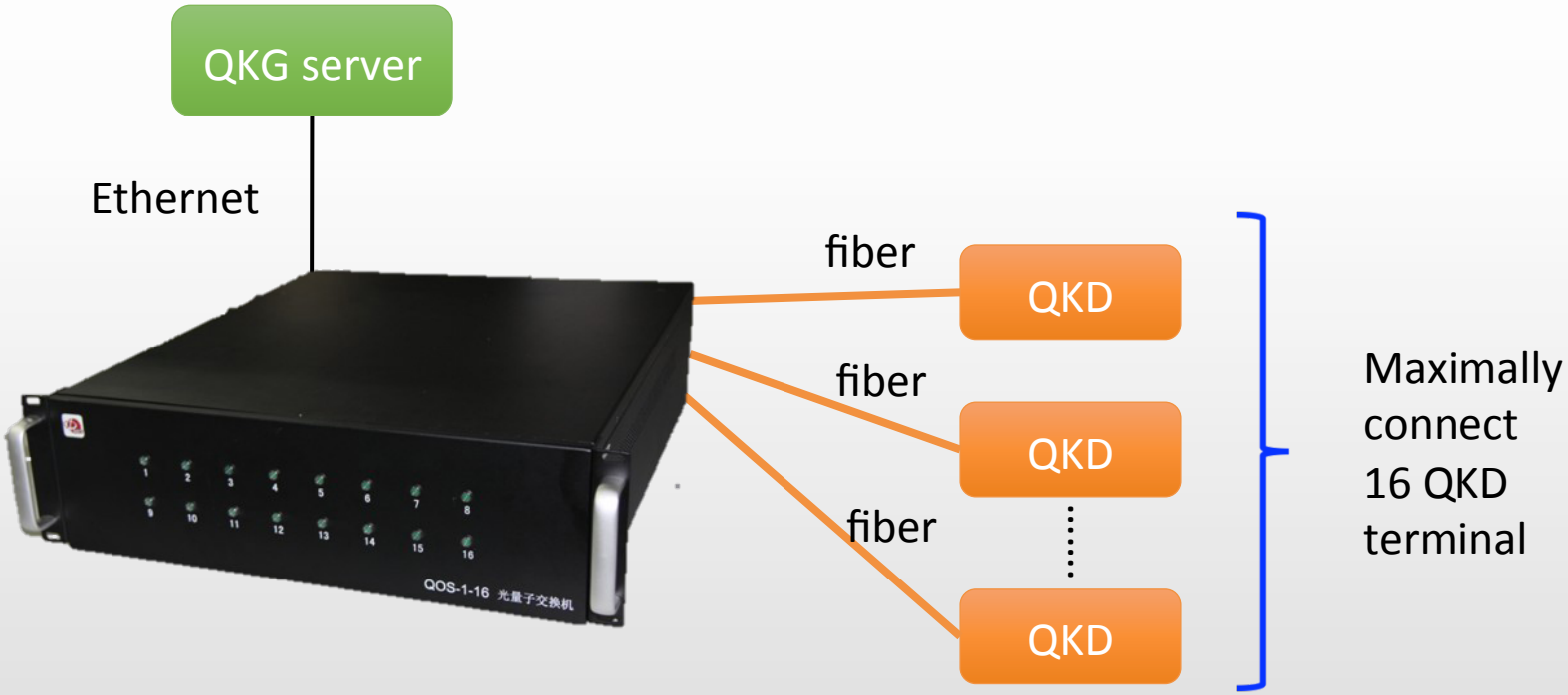
- Jinan Metro-Quantum network (56 nodes,>90users)
（7×24 running for 9 month already）

2014

- National Quantum Backbone network (Over 2000km)

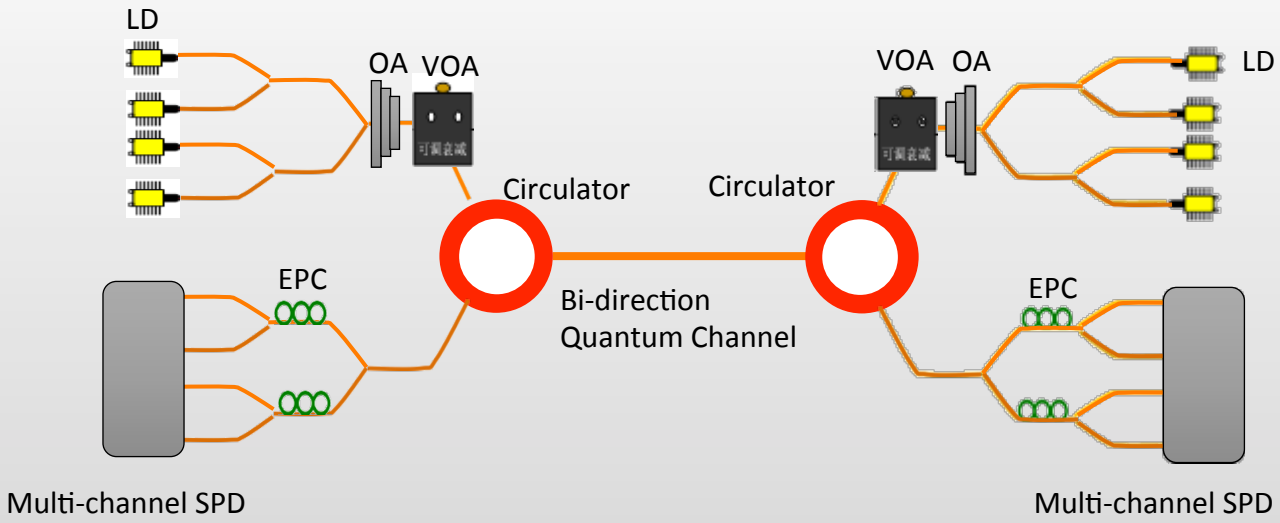
All-pass Optical Switch

- 16 FC-PC optical interface
- Optical loss less than 1.5dB
- Ethernet Control interface



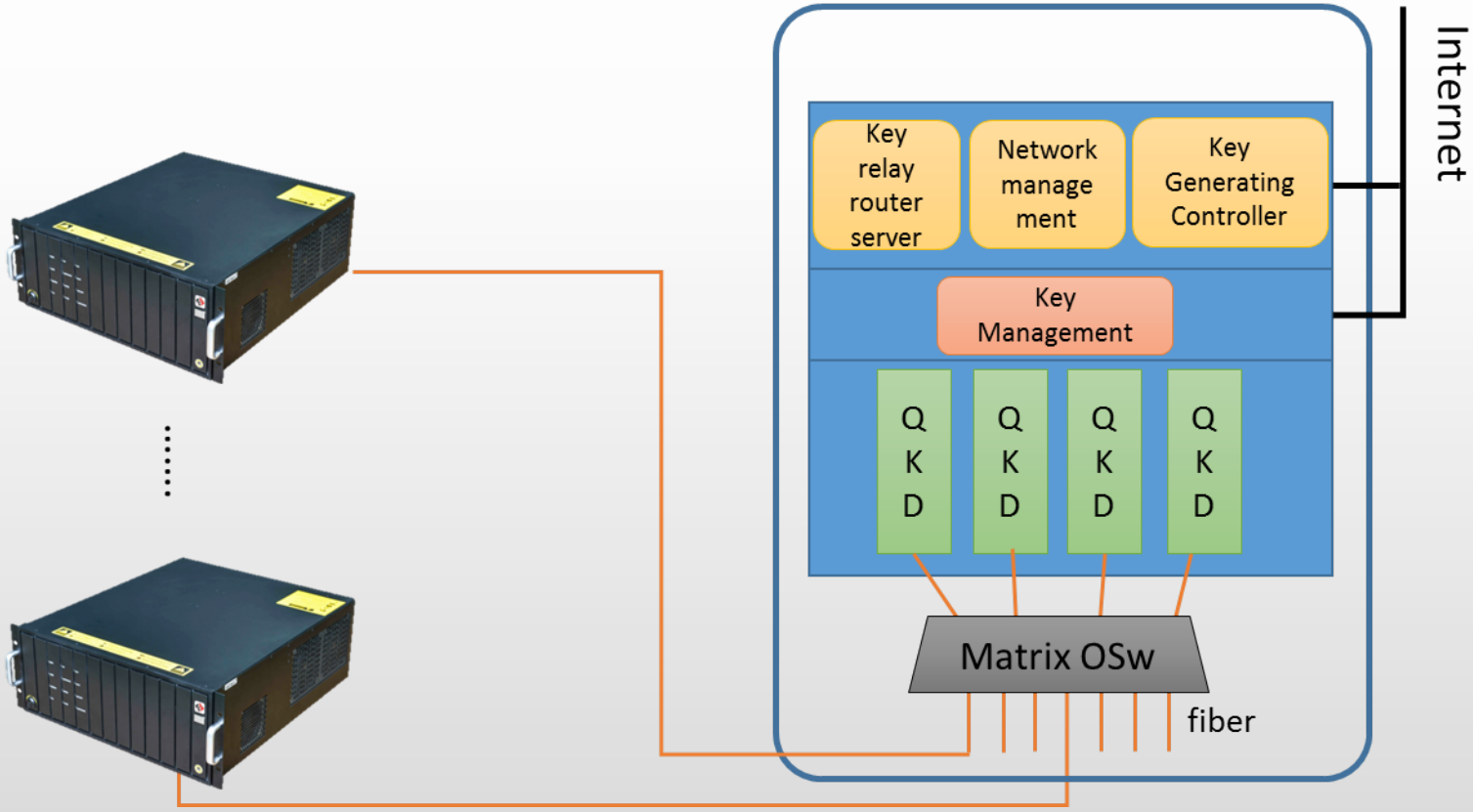
Terminal – QKD transceiver

- BB84 Decoy state protocol
- Special design for all-pass type QLAN
- Higher rate and less cost
- Resistant to all known quantum hacker
- Fully hardware designed
- Optical path loss tolerance up to 18dB



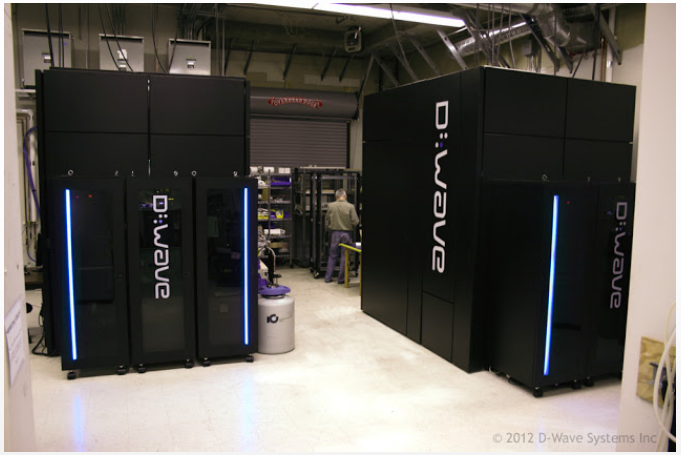
Centralized Control Station

- Convergence node and trusted relay in MAN
- Time Division Multiplexing to reduce total-cost



Why trusted relay?

There was a gap between the period of practical Quantum computer and Quantum repeater, meanwhile the trusted relay is the best choice



A huge quantum computer like this may be fatal to asymmetric cryptography

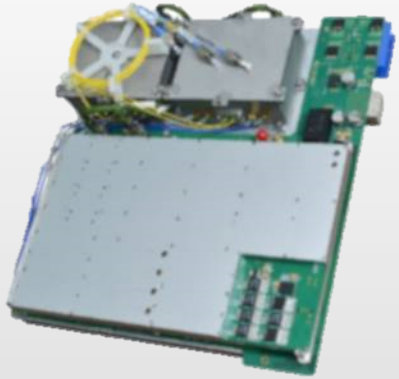
But a quantum repeater of similar size can not be set up in the most today telecom carrier room

GHz QKD Module

- Design for Backbone QKD network
- Optical path Loss tolerance up to more than 25dB
- Final key rate up to 1Mbps
- Fully hardware designed
- ATCA adapt

- Easy installation and maintenance

Data process module

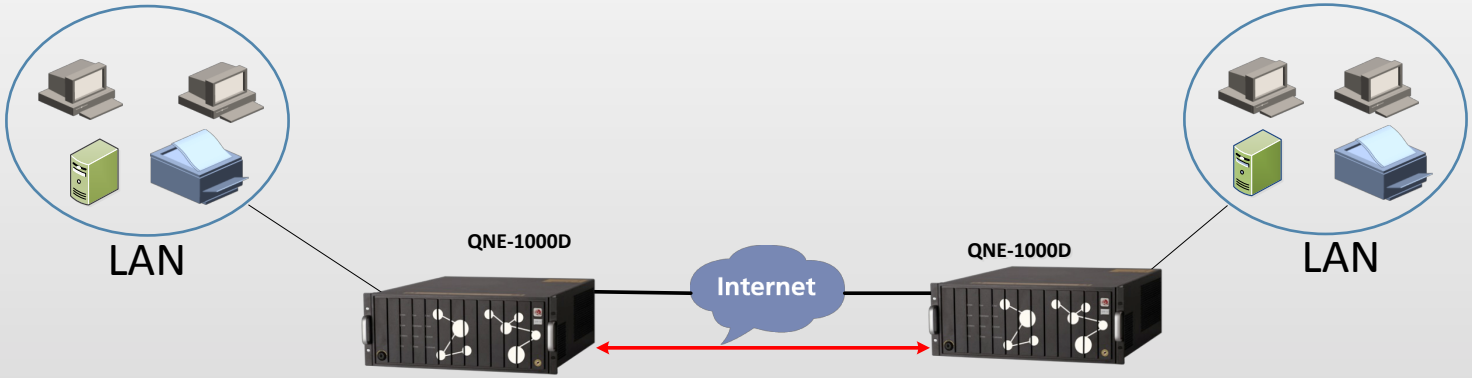


Single Photon Detector Module

Quantum Ethernet Encryptor

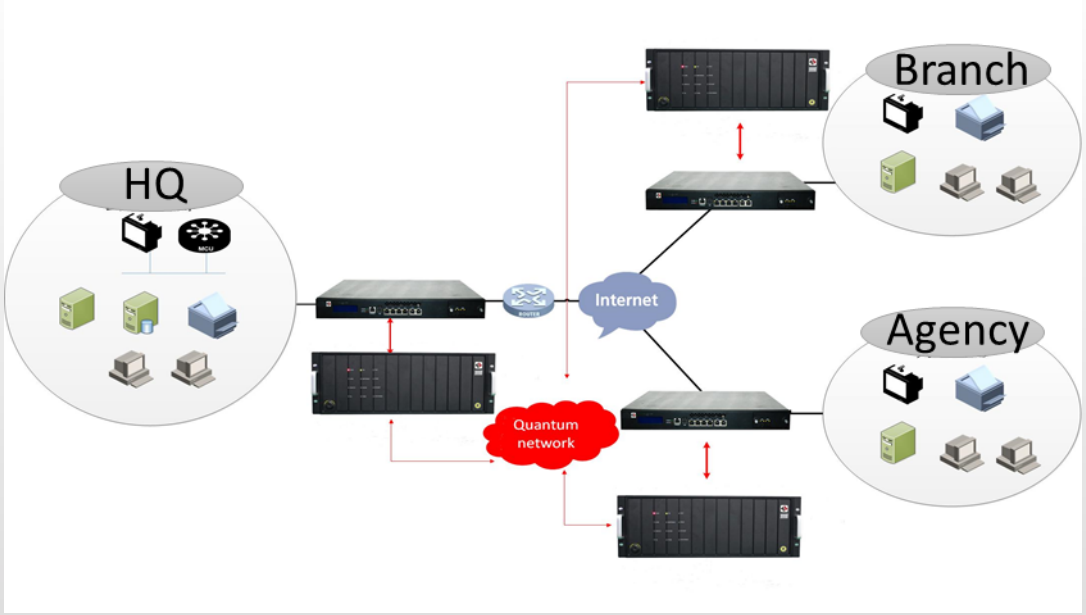
- Integrated design(QKD and Encryptor in one Chassis)
- Hardware(FPGA) Encryption up to 10Gbps
- Key(128bits) refresh rate up to 1000key/s
- Ethernet network interface
- Comply with Chinese national standards with the certificate

QNE-1000D

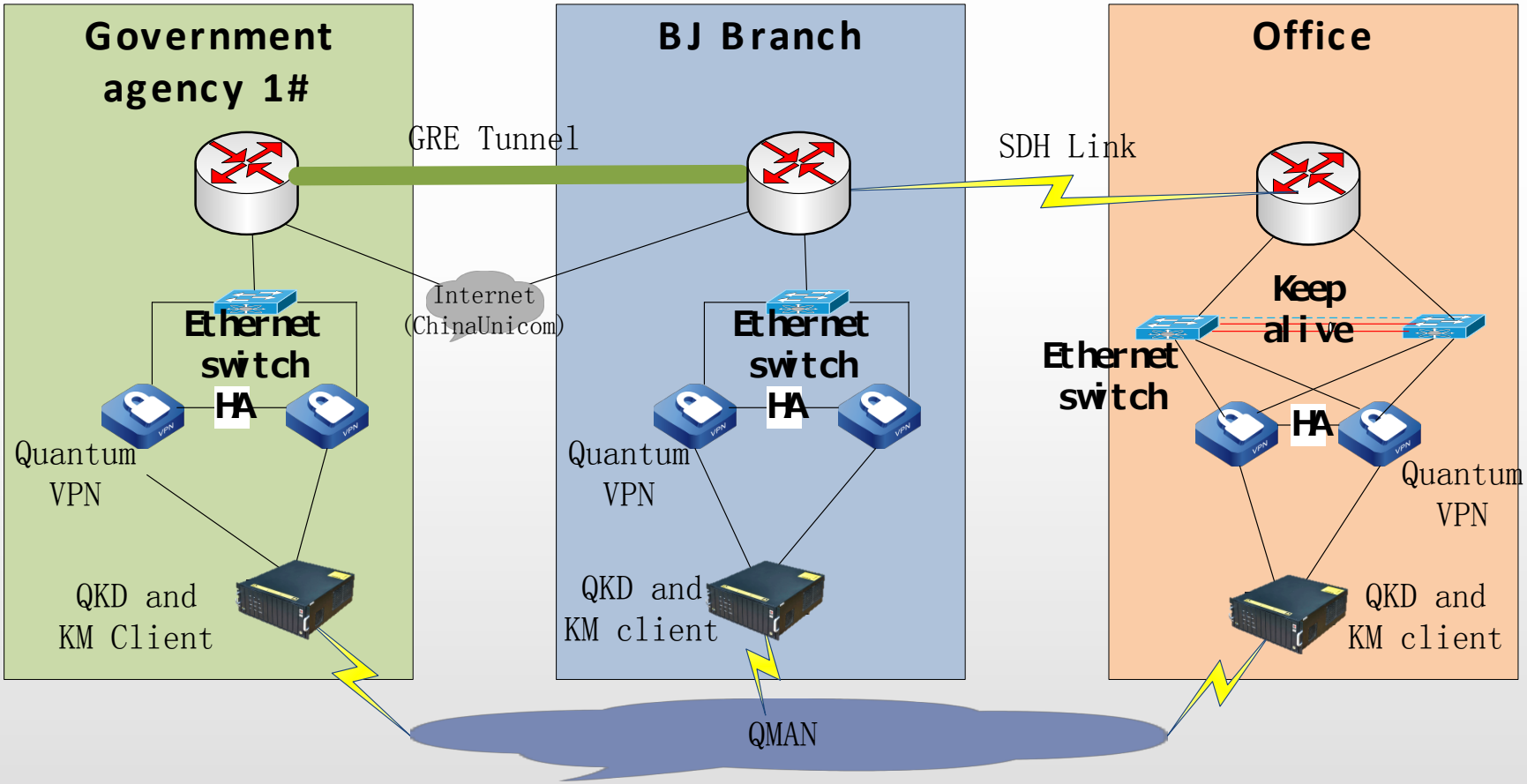


Quantum VPN

- Dual key(IKE key and Quantum key)
- encryption up to 10Gbps(CBC mode)
- Key refresh rate up to 100key/s
- Ethernet\SFP\XFP network interface
- Stackable

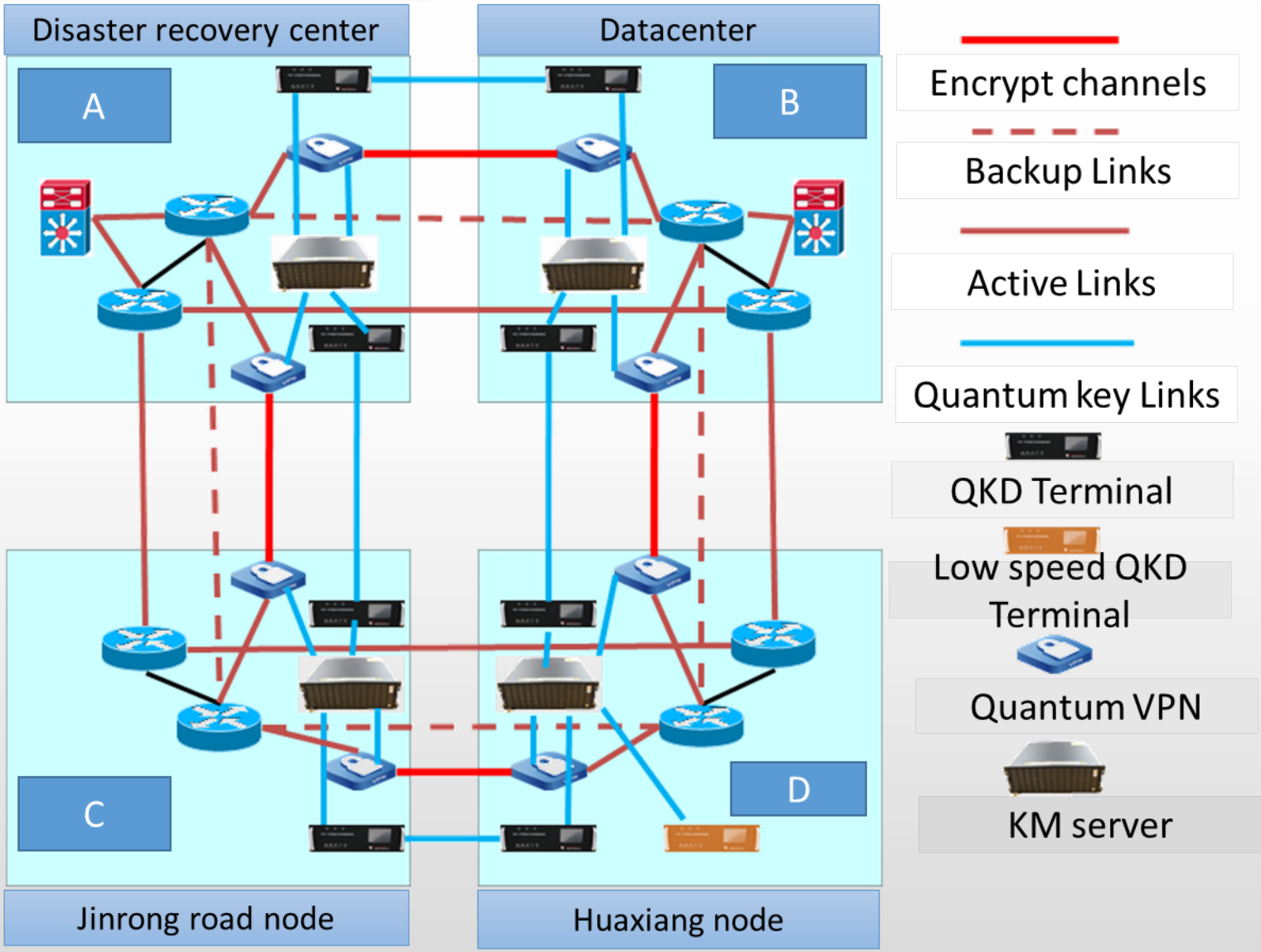


Government application case



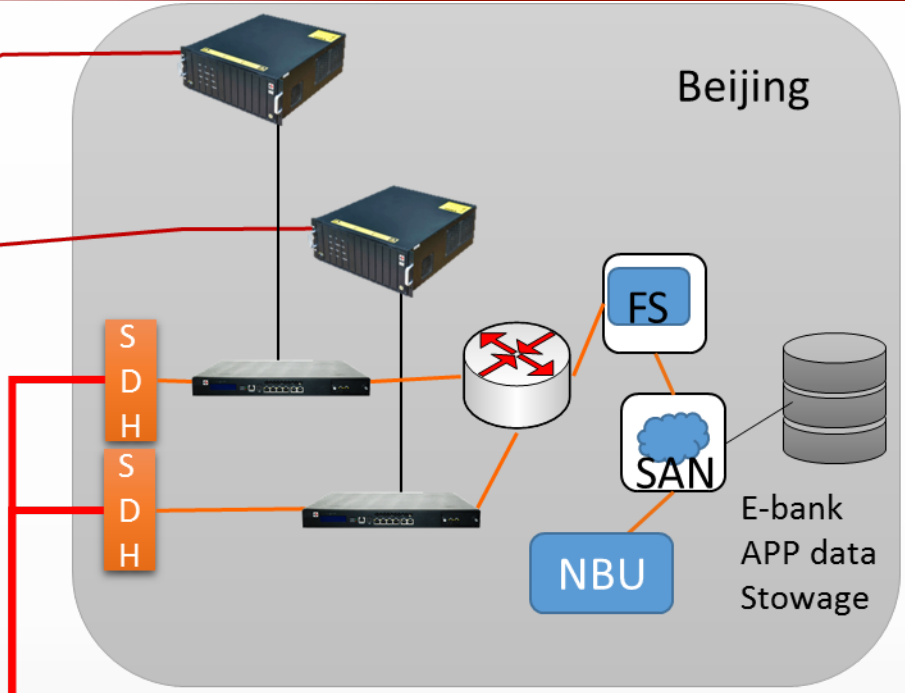
QuantumCTek

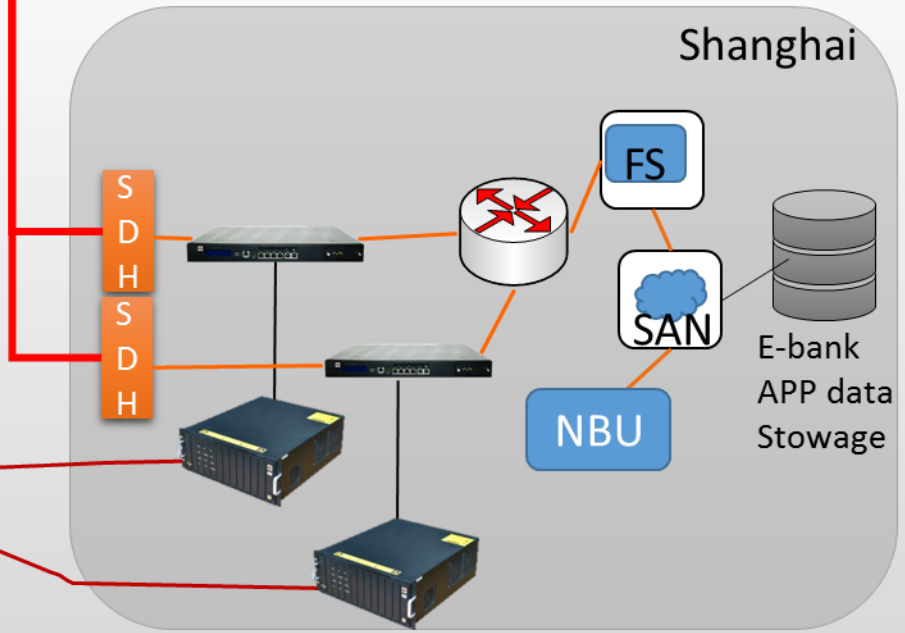
Local bank application case



QuantumCTek

Backbone Bank application case





4 Collaboration and Market

Thanks for your attention!

Website: www.quantum-info.com