Quantum Physics & Quantum Information

Large-scale Quantum Network: From Intra-city to Inter-City to Global

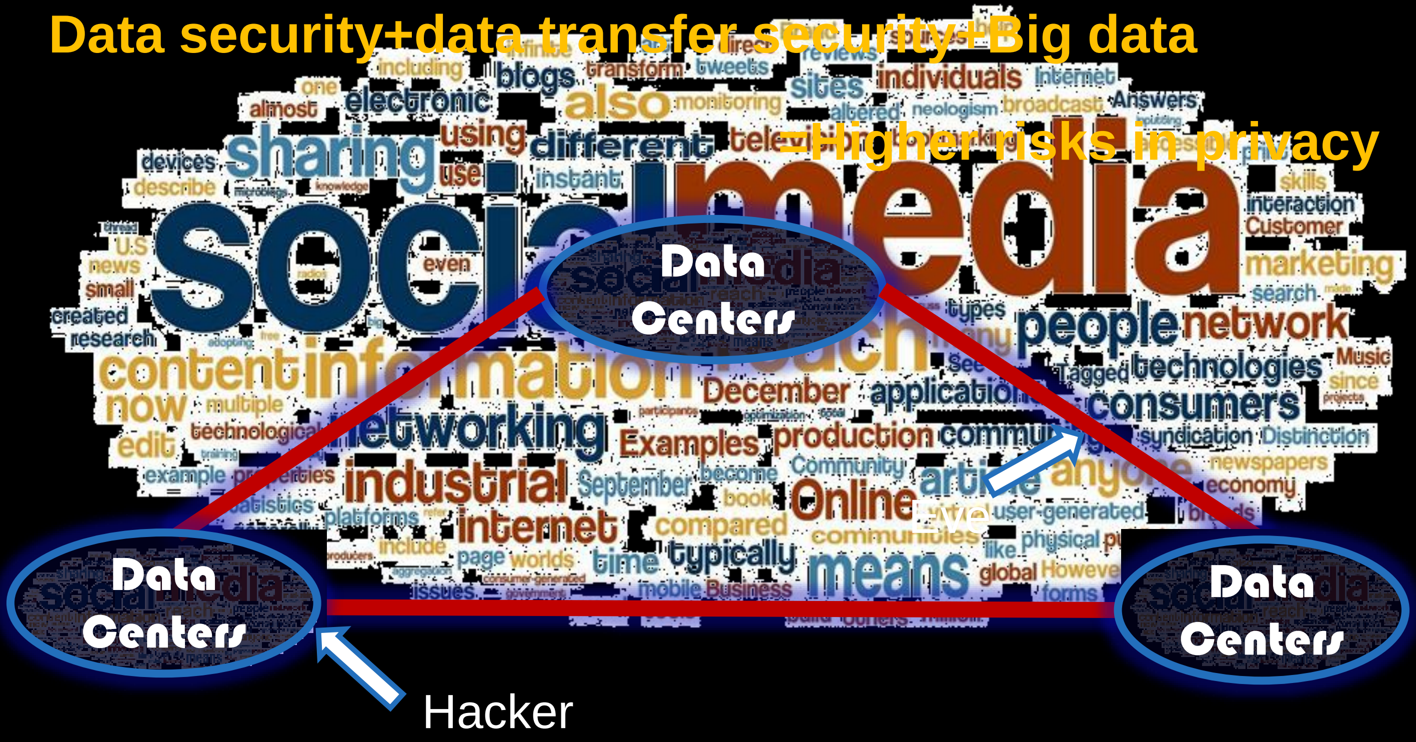
陈宇翔

Yu-Ao Chen

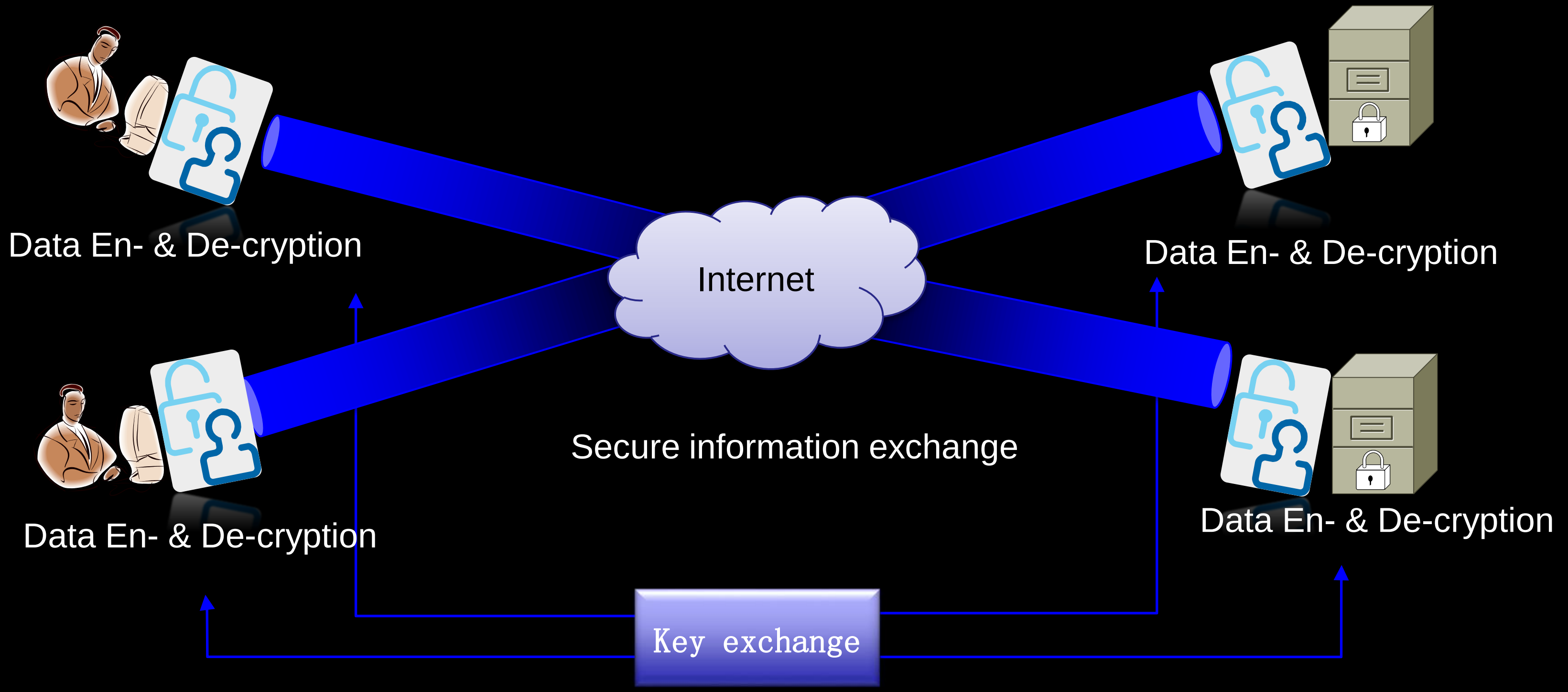
National Lab for Physical Sciences at the Microscale, University of Science and Technology of China

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

Information securities



Information securities



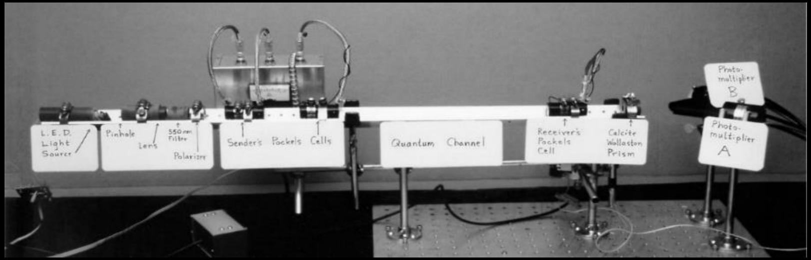
Secure Communication = Secure encryption + Secure Key exchange

Classical	Encryption	Key exchange
Symmetric encryption	One-time pad	?
Asymmetric encryption	RSA ECC	RSA ECC D-H

- RSA 512: Cracked in 1999,
- RSA 768: Cracked in 2000,
- RSA 1024: Cracked?
  shall not be used from 2014 by NIST

- All classical asymmetric encryption can be cracked by quantum Shor algorithm

Proof of Concept Demostrations of QKD



First demonstration (32 cm)

Bennett *et al.*, J. Cryptol. 5, 3 (1992)

- Cambridge-Toshiba: 122km (2004)
- NEC, Japan: 150km (2004)
- China: 125km (2005)

……

Security loopholes due to imperfection of realistic quantum devices!

Imperfect single-photon source

Photon-number-splitting attack: eavesdrop keys with occasional two identical photons events

Brassard *et al.*, PRL 85,1330 (2000)

Imperfect single-photon detectors

Blinding attack: can fully control detectors by specially tailored bright illumination

Lydersen *et al.*, Nature Photonics 4, 686 (2010)

Security of QKD with Realistic Devices

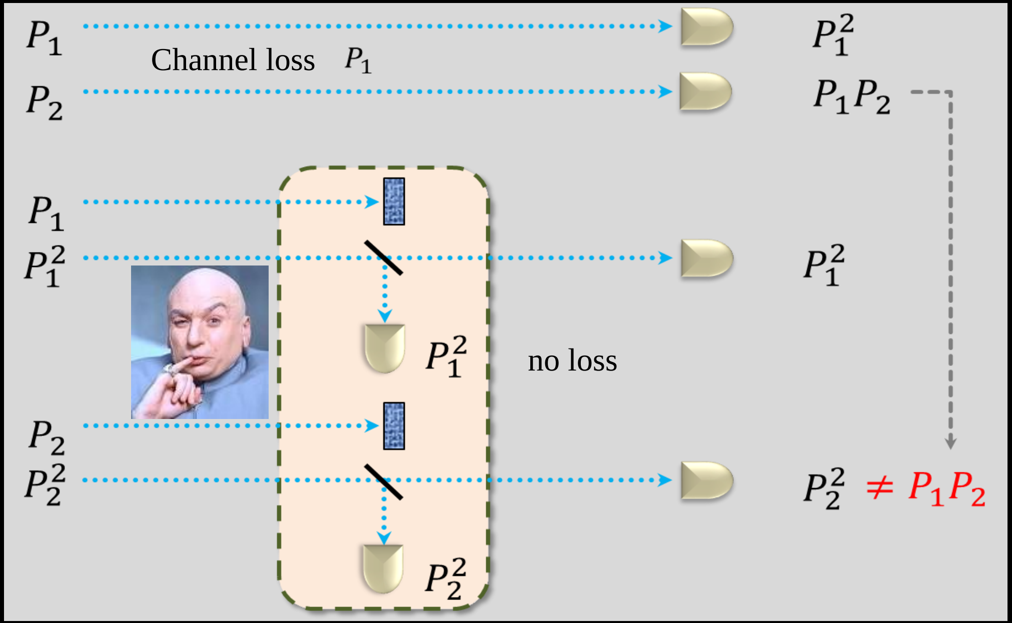
- Solution to the loophole of photon source
  Decoy-state QKD ➡ Secure distance of fiber QKD extended 100km

Scheme:
- Wang, PRL 94, 230503 (2005)
- Lo *et al.*, PRL 94, 230504 (2005)

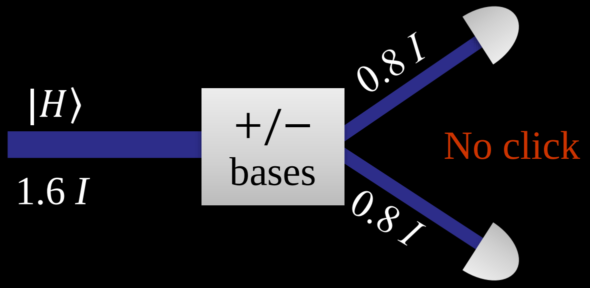
Experiments:
- Rosenberg *et al.*, PRL 98, 010503 (2007)
- Peng *et al.*, PRL 98, 010505 (2007)

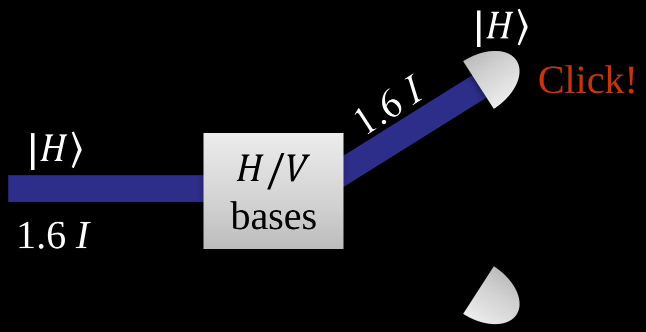
w/o attack

with attacking



Security of QKD with Realistic Devices





- Solution to the loophole of detectors

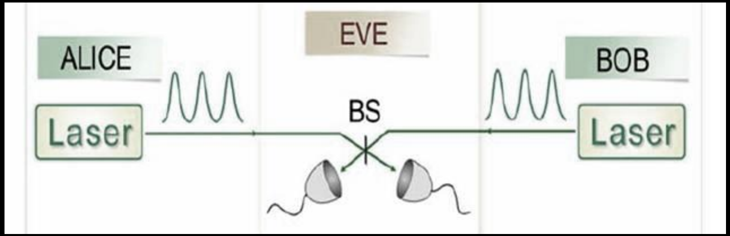
  Measurement Device Independent QKD ➡ Immune to any attack on detectors

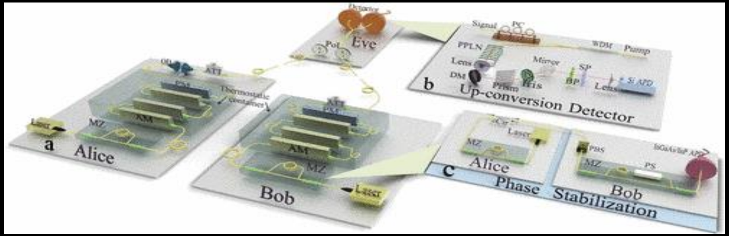
Scheme:

Lo *et al.*, PRL 108, 130503 (2012)

Experiments:

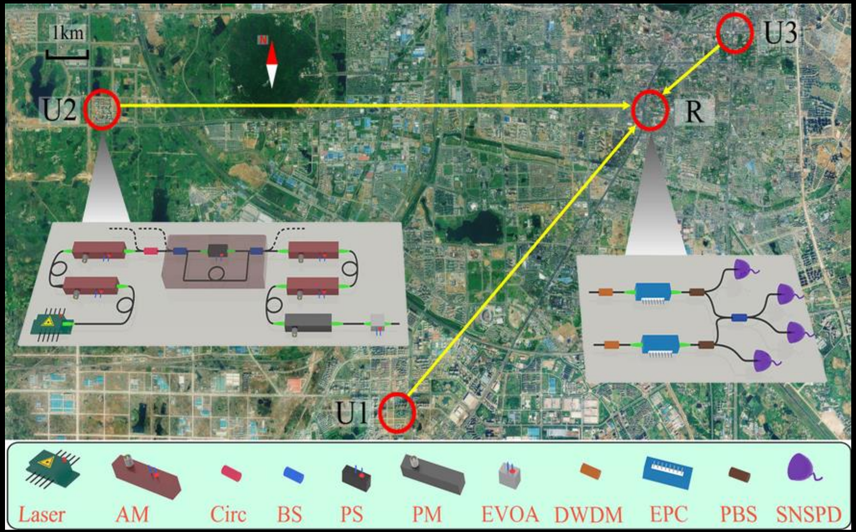
- Liu *et al.*, PRL 111, 130502 (2013) (50 km)
- [Tang et al., PRL 113, 190501 (2014)] (200 km)





Security of QKD with Realistic Devices

Field test
[Tang et al., IEEE JSTQE 21, 6600407(2015)]

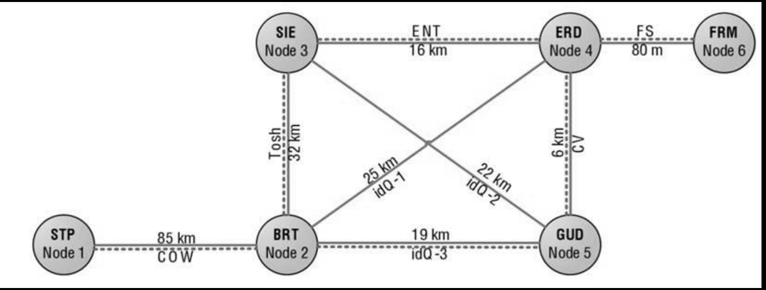


Network test
[Tang et al., PRX 6, 011024(2016)]

Practical Metropolitan QKD Networks

First all-pass network (Hefei, China)

Chen *et al.*, Optics Express 17, 6540 (2009)



SECOQC Network (Europe)

Peev *et al.*, New J. Phys. 11, 075001 (2009)

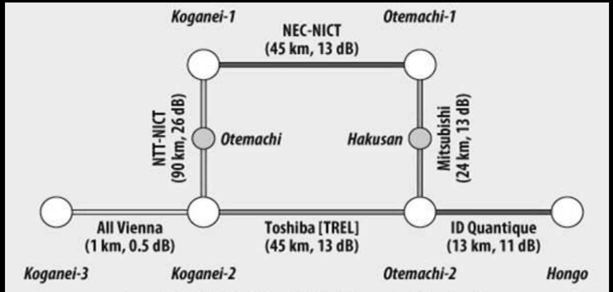
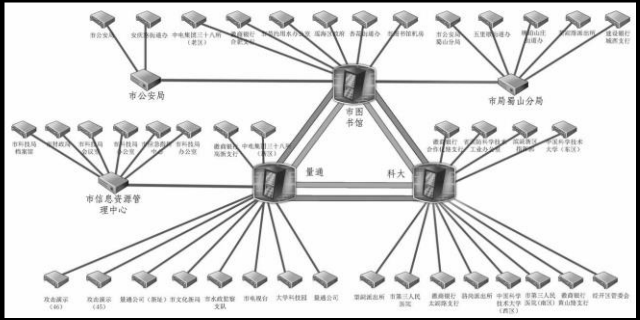


Fig. 3 Topological Map of the Tokyo QKD Network

Tokyo QKD Network (Japan)

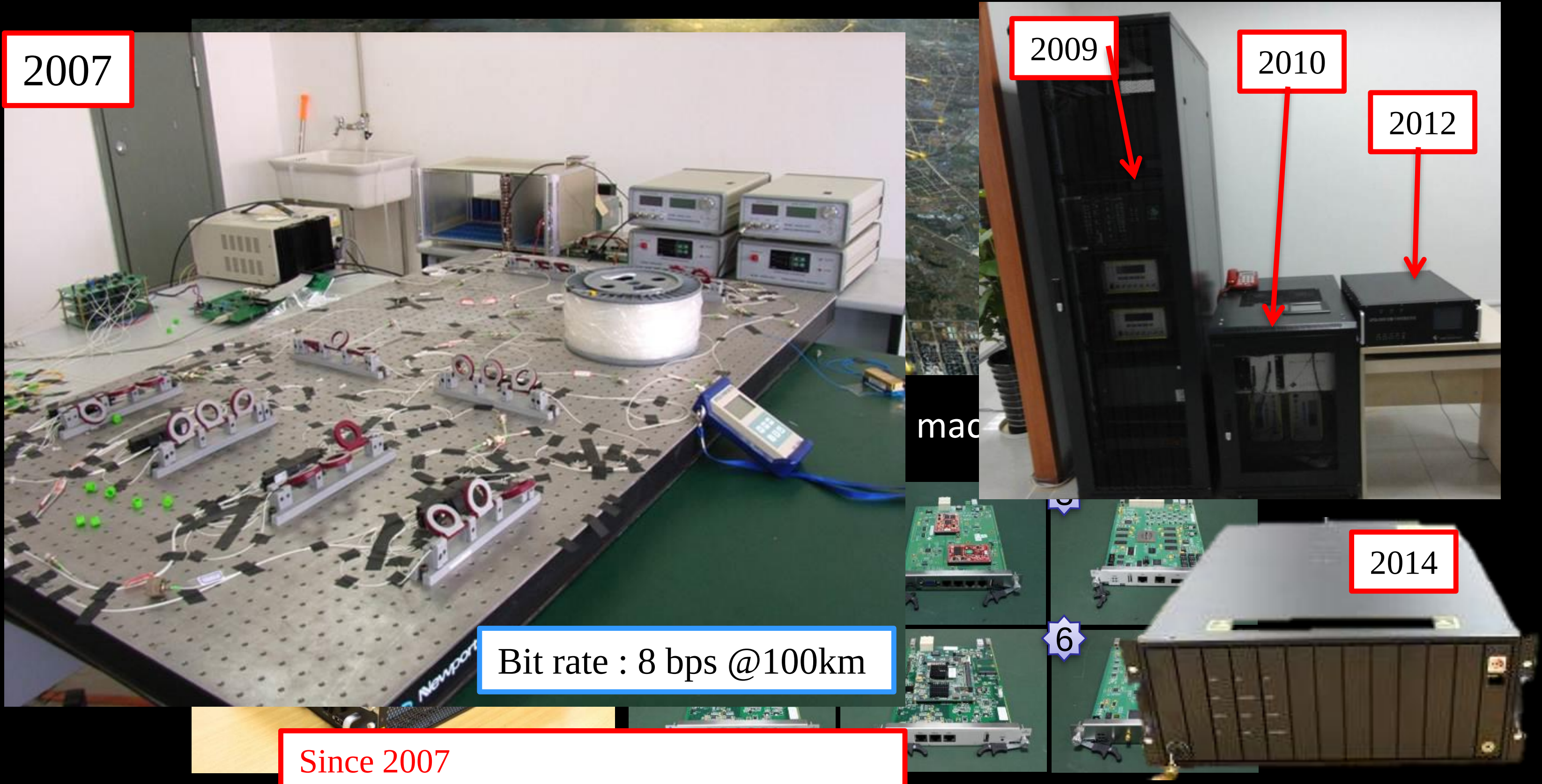
M. Sasaki *et al.*, Opt. Express 19, 10387 (2011)



First scaled metropolitan network

Hefei intra-city QKD network (46 nodes, 2012)

Practical Metropolitan QKD Networks



Since 2007
Size: decrease 10 times
Bit rate: increase 1000 times

Bit rate： 8kbps@100km

Symmetric encryption (e.g. AES, SM4): Same seed key for En- & De-

Advantages: hard to crack, more efficient to encrypt

Disadvantages: security for key exchange

More difficult for multi users, seed key update rate slow

10 kbps@100 km

In combination with classical symmetric encryption:

☑ Secure the key exchange process

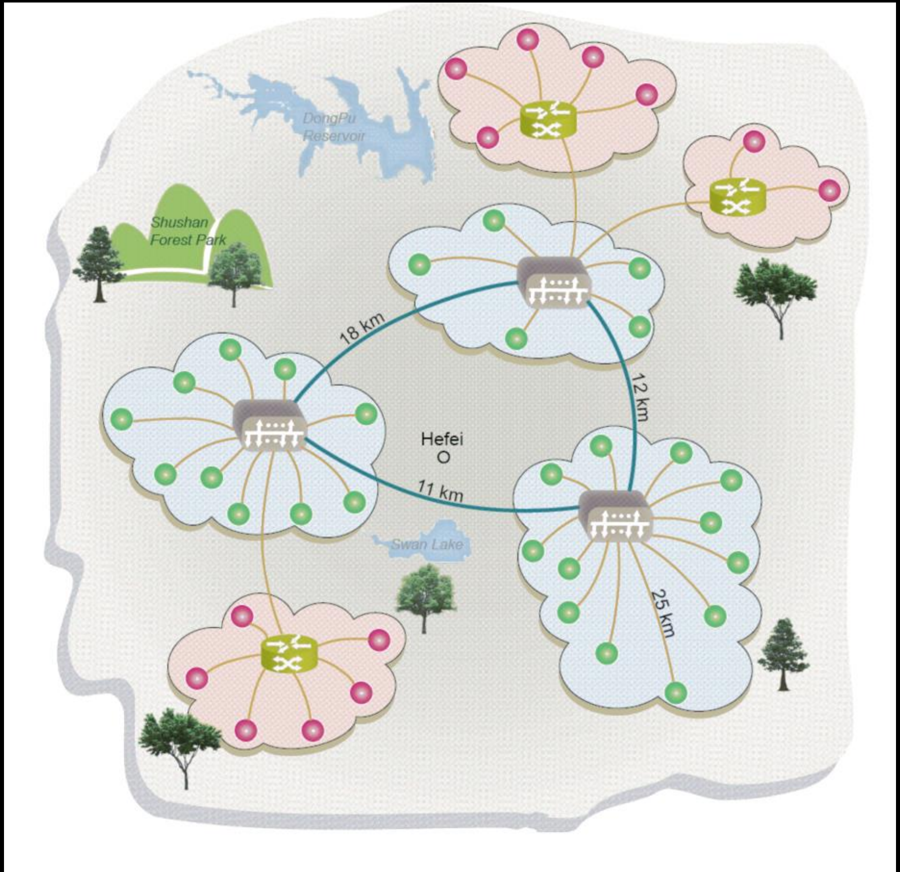
☑ >10Gbps encrypted data

☑ Seed key update rate greatly enhanced

This is an important result: it buys time for further improvements while denying an enemy breaking DH in (say) 2015 all of our traffic before 2015!

-- DARPA Quantum Network Testbed, Final technical report, No. AFRL-IF-RS-TR-2007-180, (2007)

Practical Metropolitan QKD Networks

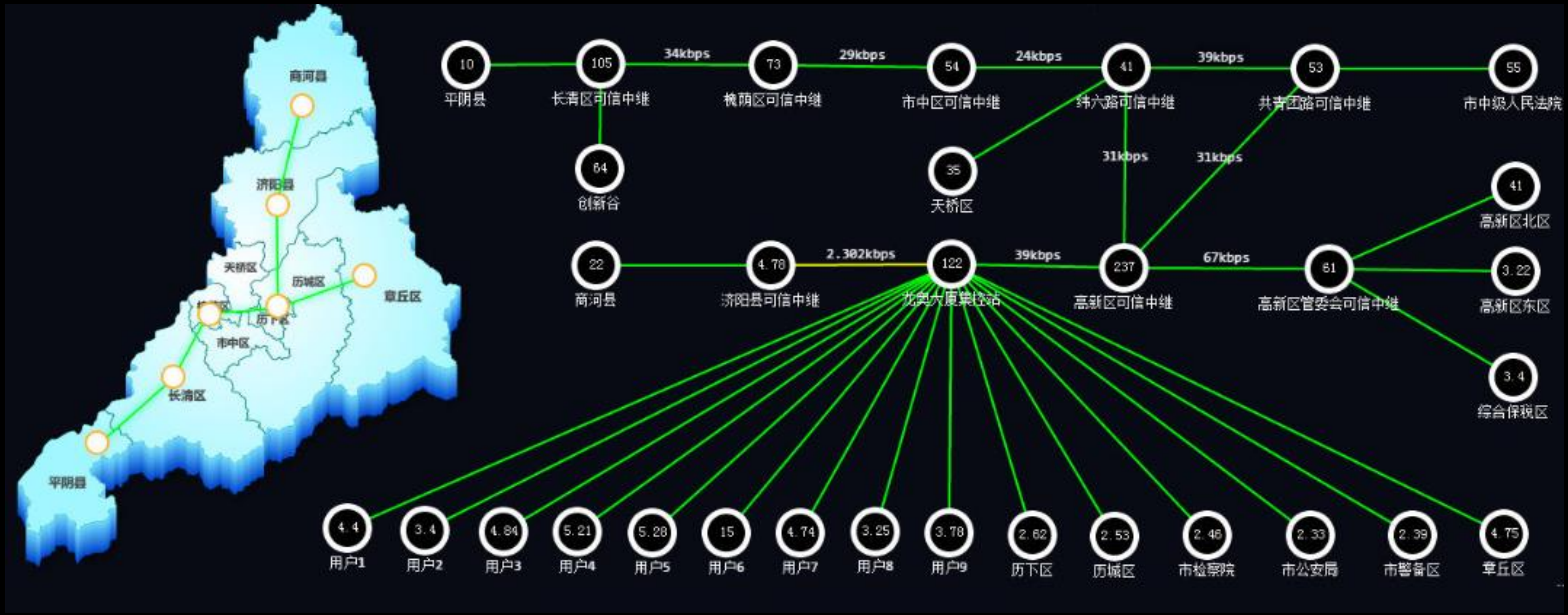


- Three level of users
  - Relay Station
  - VIP users (red spot)
  - General end users (green spot)

- Three type topology
  - Circle
  - Star
  - Tree

46 Nodes Hefei

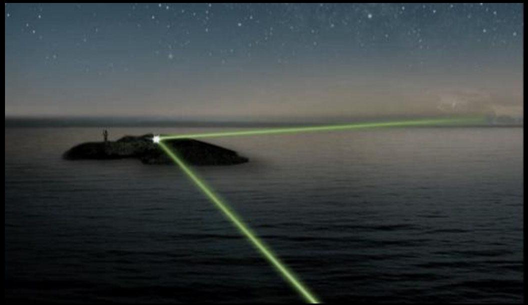
Practical Metropolitan QKD Networks



Jian Government private QKD network **Operated at Aug. 2017**

Challenge towards Scalable Quantum Communications

- Longest distance of point-to-point MDI-QKD in fiber: ~400km
  Yin *et al.*, PRL 117, 190501 (2016)
- Longest distance of quantum teleportation in terrestrial free space: ~100km



Yin *et al.*, Nature 488, 185 (2012) by Chinese group

Ma *et al.*, Nature 489, 269 (2012) by Austrian group

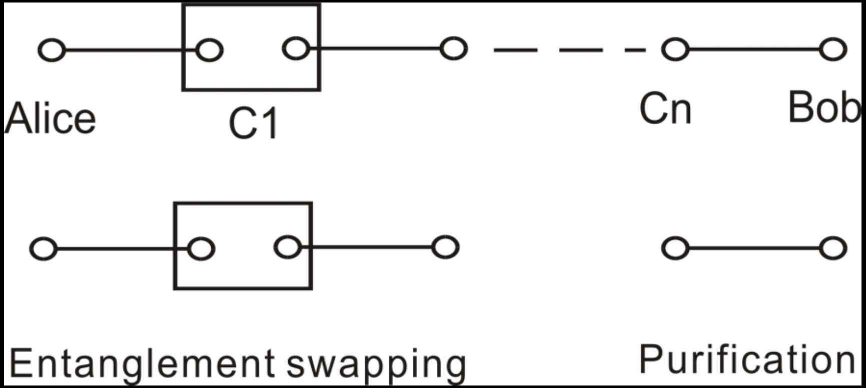
Inevitable huge photon loss in fiber and terrestrial free space channel

For 1000 km commercial fiber, even with a perfect 10 GHz single-photon source and ideal detectors, only **0.3** photon can be transmitted on average **per century!**

There are two main paths: **satellite-based** and **quantum repeaters.**

Gisin & Thew, Electronics. Lett. 46 965, (2010)

Solution 1: Quantum Repeater



Quantum repeater

Briegel *et al*., PRL 81, 5932 (1998)

➔ Solution to decoherence： Entanglement purification

Bennett *et al*., PRL 76, 722 (1996)

Pan *et al*., Nature 410, 1067 (2001)

Pan *et al*., Nature 423, 417 (2003)

➔ Solution to photon loss ： Entanglement swapping

Zukowski *et al*., PRL 71, 4287 (1993)

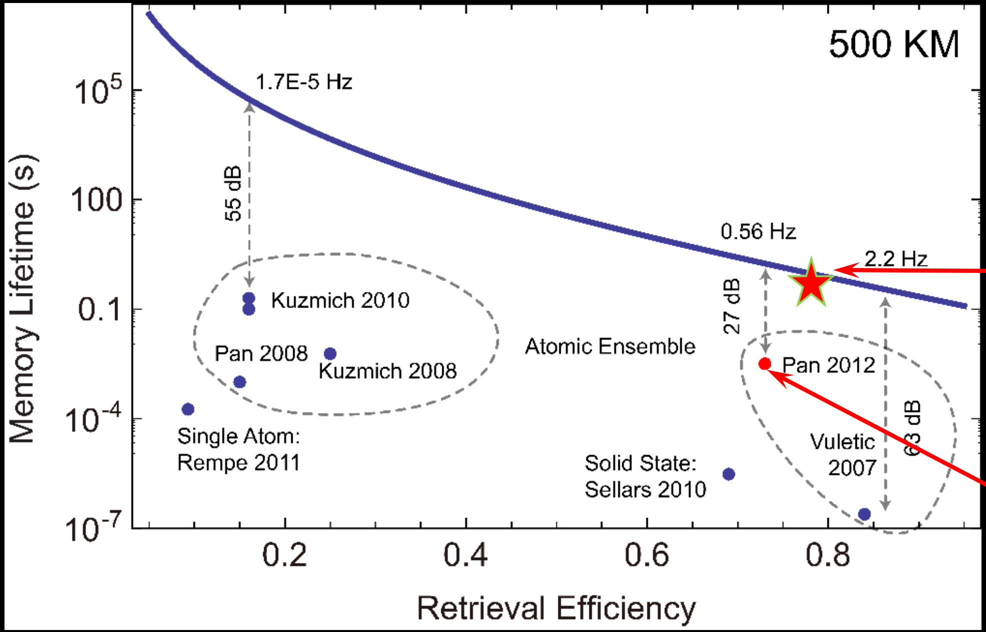
Pan *et al*., PRL 80, 3891 (1998)

Pan *et al*., Nature 421, 721 (2003)

Require:

- entanglement swapping with high precision
- entanglement purification with high precision
- quantum memory: Storage time and Retrieve Efficiency

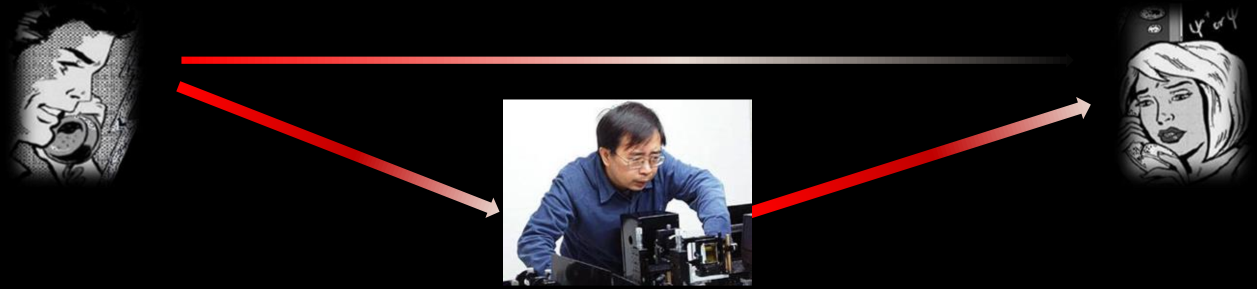
Practically Still Challenging



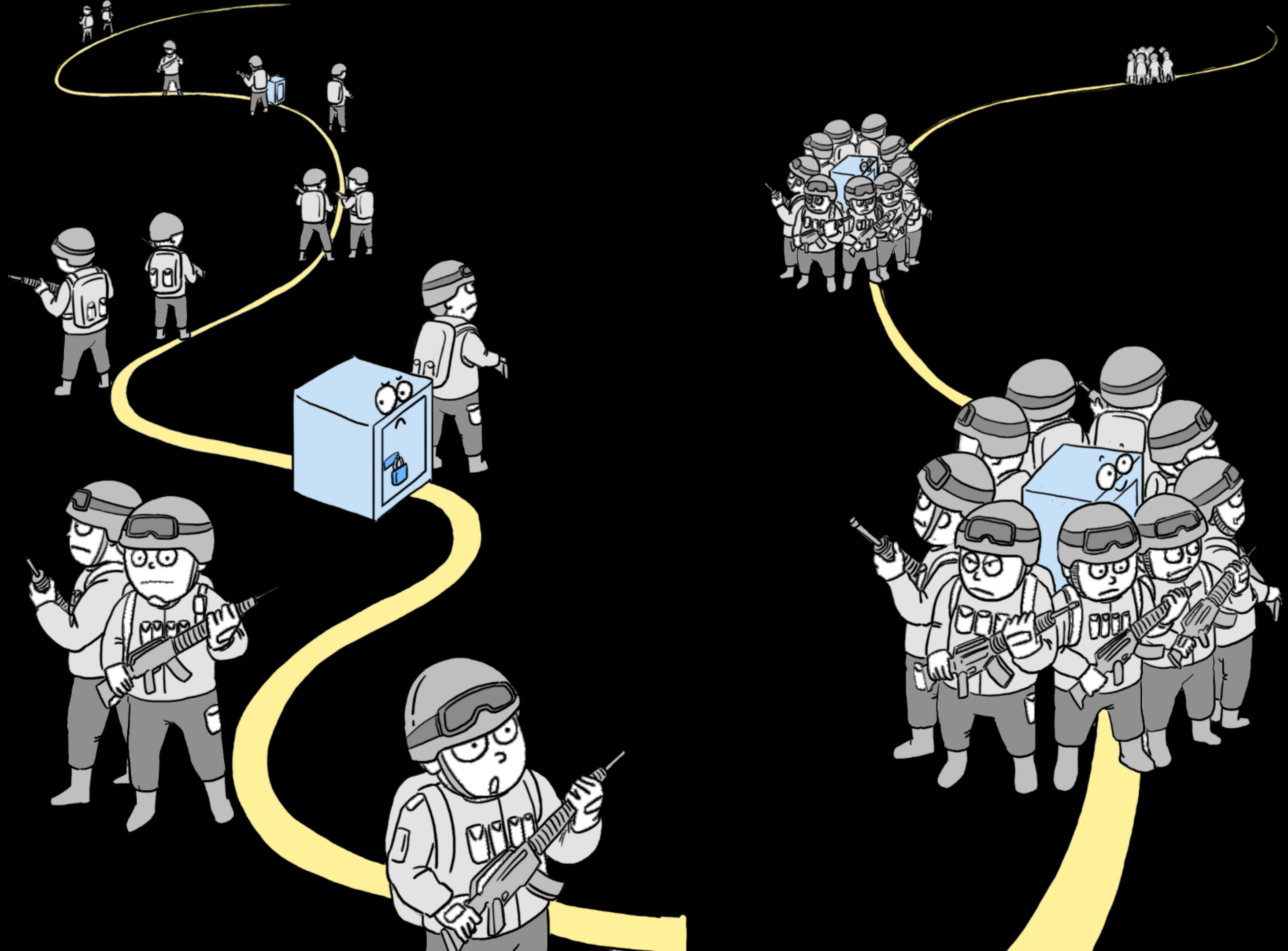
- Previous (ring cavity + collinear configuration): require lifetime to be extended about 2 orders of magnitude
- Most recently(ring cavity + optical lattice confinement + spin wave freezing): life time ~220ms, retrieve efficiency ~76%

Pan: Yang *et al*. Nature Photonics, 10, 381–384 (2016)

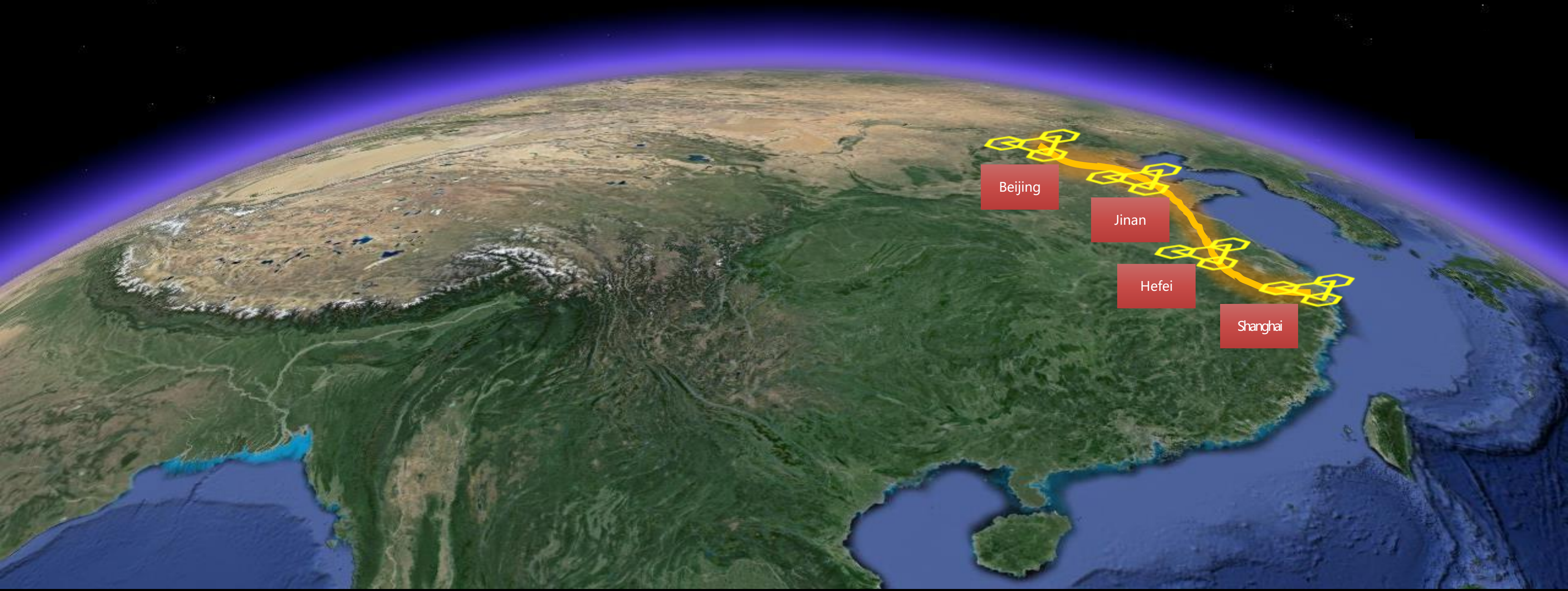
Trustable Relay Approach
- Classical Repeater



	A	Relay	B
Initial	K_{AR}	K_{AR}、K_{RB}	K_{RB}
Step 1		Announce $K_{AR} \oplus K_{RB}$	
Step 2			$K_{AR} \oplus K_{RB} \oplus K_{RB}$
Final	K_{AR}		K_{AR}

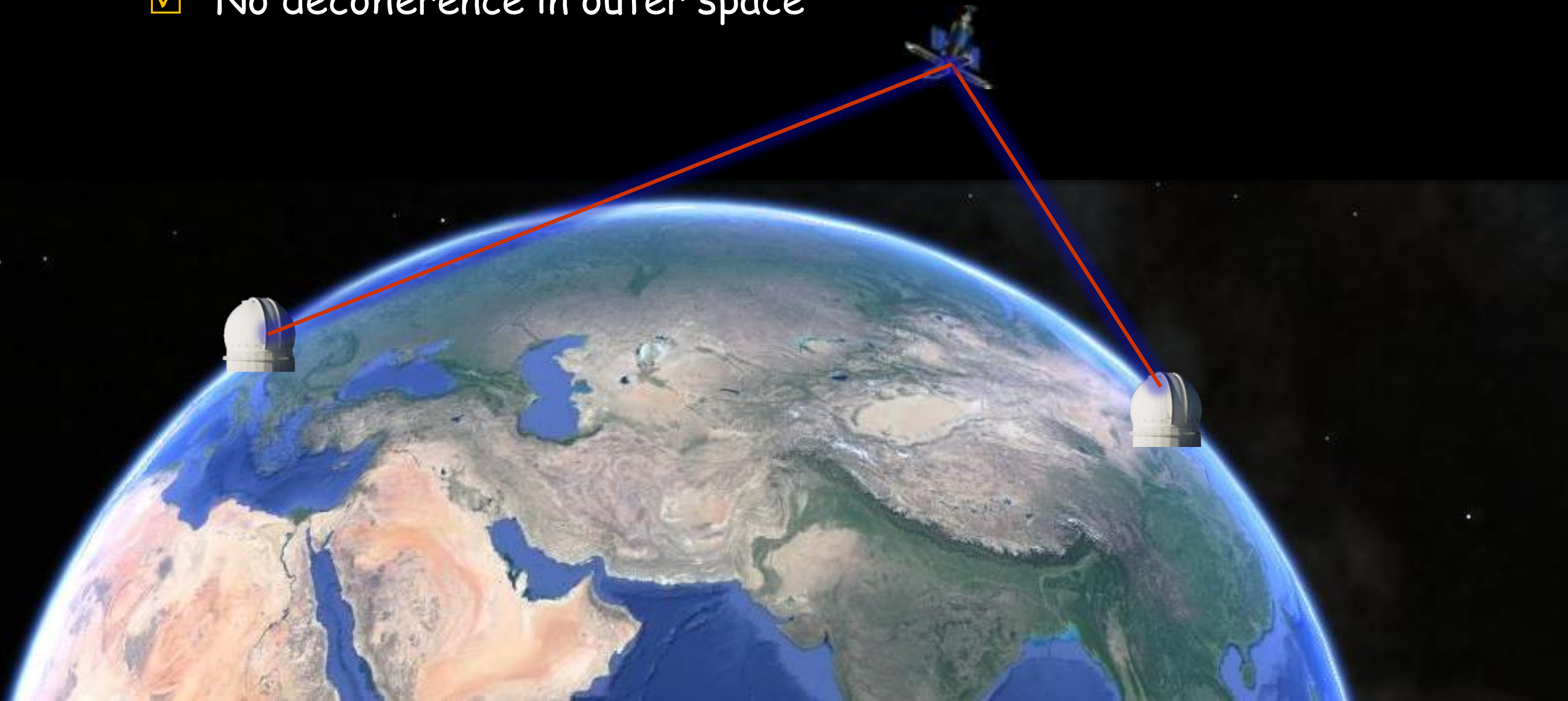


Solution 1: Quantum Secure Backbone (Trustable Relay)



Solution 2 (more effecient): Satellite-based Free Space Quantum Communication

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



Roadmap: Large Scale Quantum Communication

Metropolitan networks via fiber

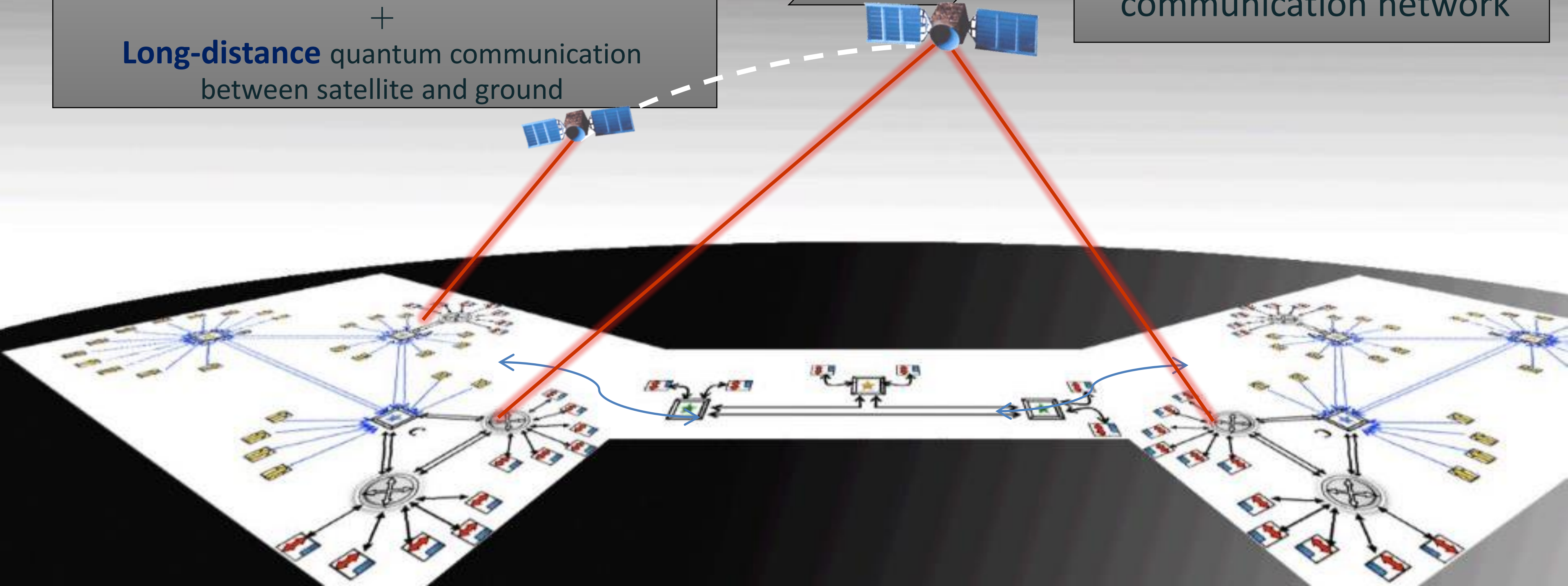
+

Inter-city networks connected by quantum repeaters or Backbone

+

Long-distance quantum communication between satellite and ground

Large scale quantum communication network



2006

- Secure distance exceed 100km with Decoy BB84

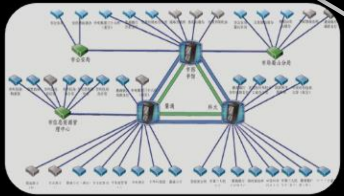
China creates quantum network

2008

- First quantum telephone network (Hefei 3 nodes)

- Secure distance exceed 200 km for the first time
- All pass network (Hefei 5 nodes)

2009



2012

- Metropolitan network (46 nodes)
- Demonstration of application in financial information transmission

2013

- Metropolitan network Jinan (56 nodes 95 users, 7×24 hours, running for more than 24 months)

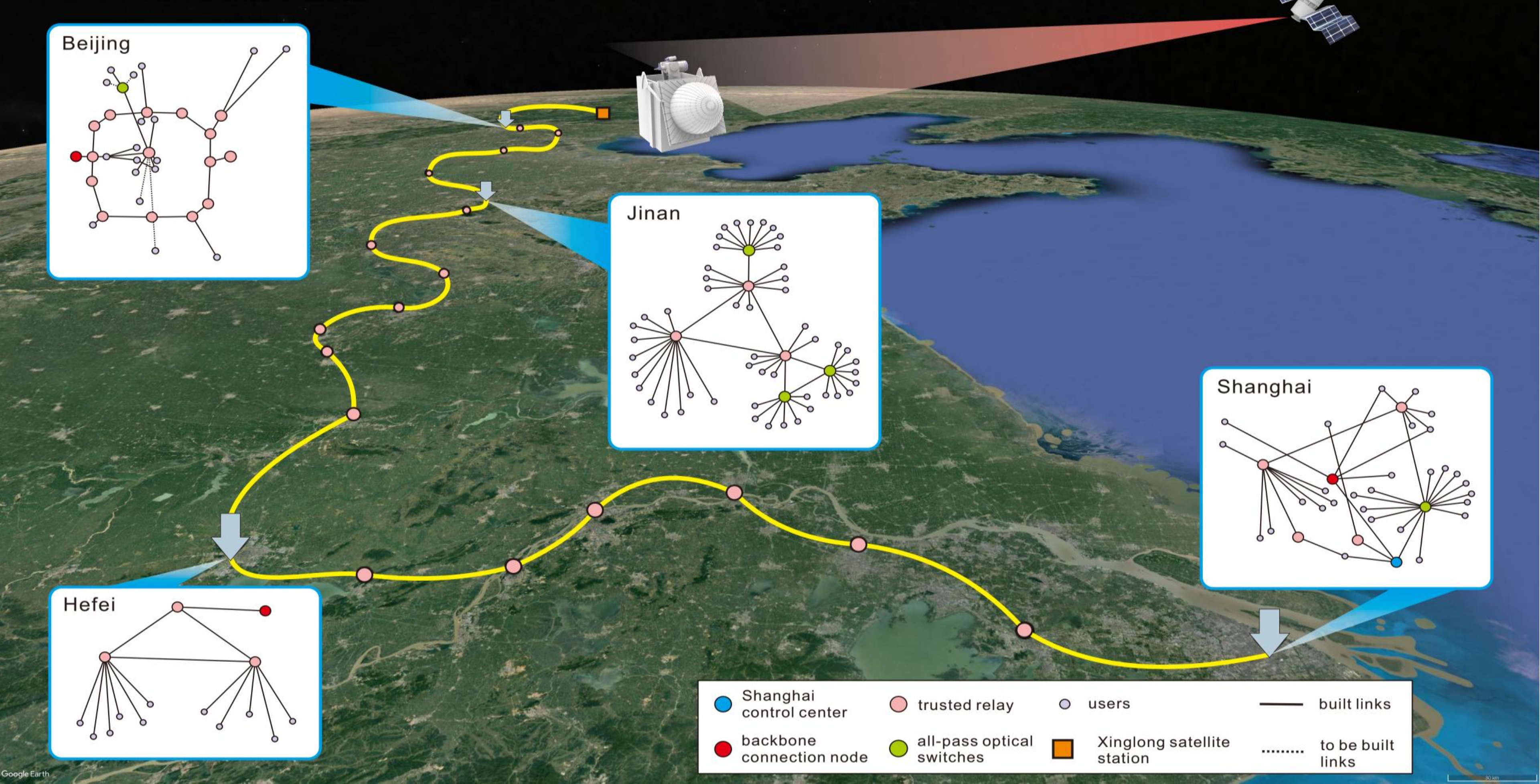
2014

- Quantum secure communication Beijing-Shanghai backbone

Quantum Secure Backbone

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes
  31 fiber links
- Metropolitan networks
  Existing: Hefei, Jinan
  New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; China Banking Regulatory Commission …
- GDP 35.6% ($3 trillion)
- Population 25.8% (0.3 billion)

Quantum Secure Backbone



In door system debugging

- ✓ A in-door platform for testing all equipments
- ✓ All devices are operated 24x7 for more than 6 months before intalled to backbone
- ✓ As of Mar. 11 2016, the the eintire line of 61 quantum links, 186 sets of quantum equipments, have been stablely operated for more than 6 month
- ✓ A 3+2 testbed has been permanently installed

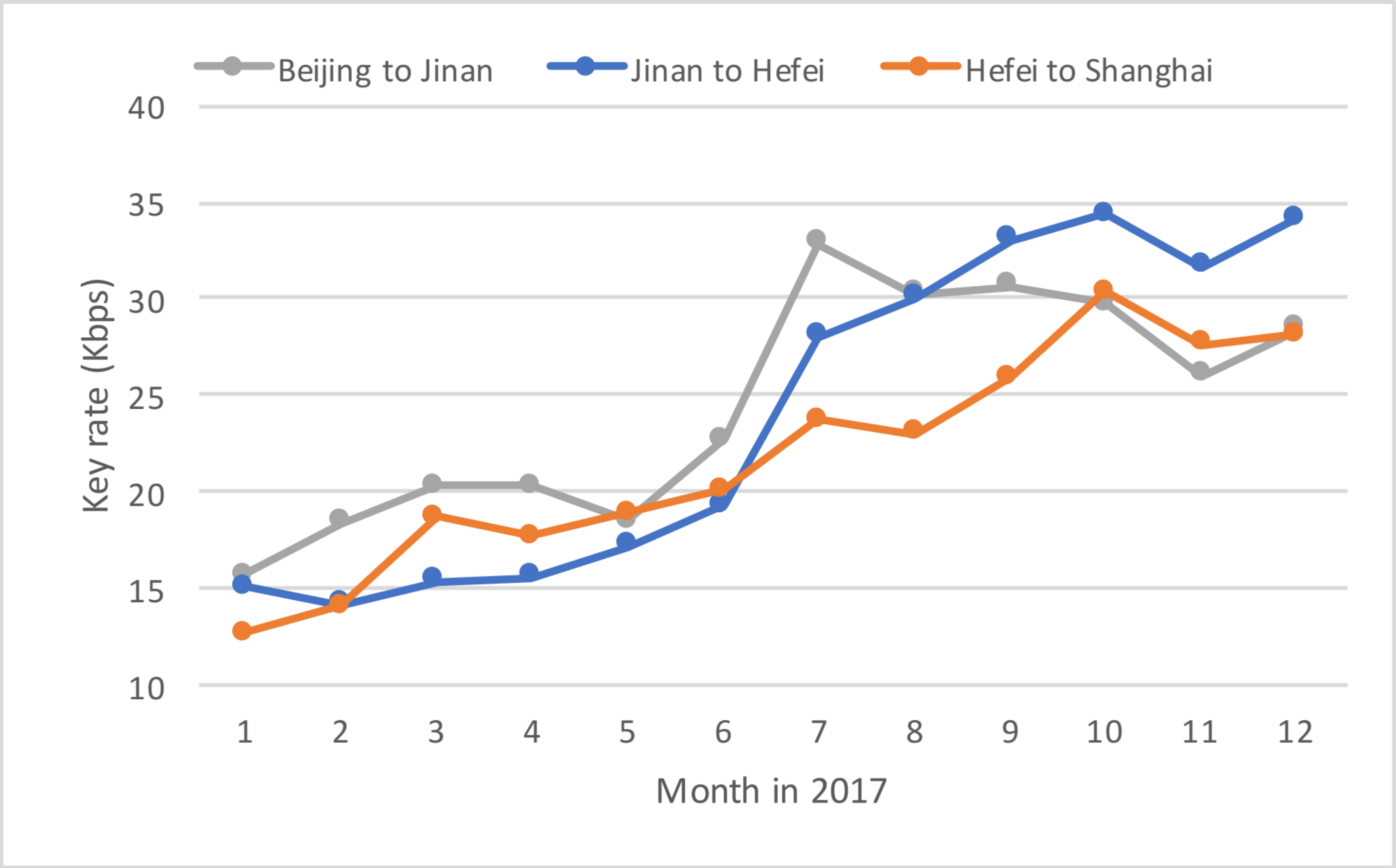
Deployment


量子保密通信上海控制中心


中国科学技术大学
University of Science and Technology of China
上海研究院

上海量子保密通信网
中国银监会
中国人民银行
工商银行（外高桥）
阿里云（外高桥）
电信华信
汇聚站
农业银行（外高桥）
东方证券
华安基金
工商银行（嘉定）
洪都村镇银行
电信真如
汇聚站
京沪干线
上海站
上海银监局
中国人民银行
上海总部
工商银行
张江管委会
兴业数金
上海农商银行
中国银行
交通银行
国泰君安期货
上海浦东发展银行
民生银行
东方证券
交通银行
国泰君安期货
民生银行
上海电信
华安基金
电信张东
接入站
中国银行
上海浦东发展银行
电信钦州
汇聚站
中国电信信息园
中科大上海研究院
量子总控中心
上海国盾量子公司
崇明
浦东
松江
闵行

北京量子保密通信网
中国银监会
中国人民银行
北京农商银行
民生银行
顺义区
量子通信星地枢纽
总控中心
工商银行（西三旗）
中国银行
光大银行
海淀区
上地集控站
工商银行
中国人民银行
金融信息中心
酒仙桥中继站
石景山区
北京农商银行
中央电视塔
（京沪干线—北京站）
广内中继站
中国人民银行
营业管理部
大悦城中继站
中国银监会
北京银监局
中国金融认证中心
朝阳区
建设银行
丰台区
北京农商银行
阿里云（亦庄）
华夏银行
北京农商银行
大兴区
通州区



Beijing to Jinan
Jinan to Hefei
Hefei to Shanghai
40
35
30
25
20
15
10
Key rate (Kbps)
1
2
3
4
5
6
7
8
9
10
11
12
Month in 2017

Applications: Industrial and Commercial Bank of China

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 **4** KB/Min

加密吞吐量：**83.28** Mbps

北京 西三旗 ⟶ 上海 外高桥

密钥更新率：**10** 次/Min **4** KB/Min

加密吞吐量：**80.6** Mbps

Applications: Selected Users

Applications: Selected Users

State Grid Co. China

- ✓ Backup for disaster recovery
- ✓ Deployment system
- ✓ Generation-Grid-Load-Storage Optimal Operation System
- ✓ Network Management of Data Transmission
- ✓ Video Conference

Quantum Science Satellite “Micius”

Quantum Science Satellite “Micius”

- Total weight of the satellite: 631kg
- Average power: 560W
- 500km sun synchronous orbit
- With the ability of pointing station

Micius, about 468-376 BC

He realized the first pinhole imaging experiment in the world, demonstrating that light travels is in a straight line

- ✓ Tracking error is about 1urad
- ✓ Polarization visibility is over 100:1
- ✓ Satellite divergence angle is 10urad
- ✓ Channel loss is roughly 30 dB

Micius'　Philosophy

- **Universal love, and peace (no war):**　“兼爱、非攻”
- **Atom:**　“端，体之无序而最前者也”

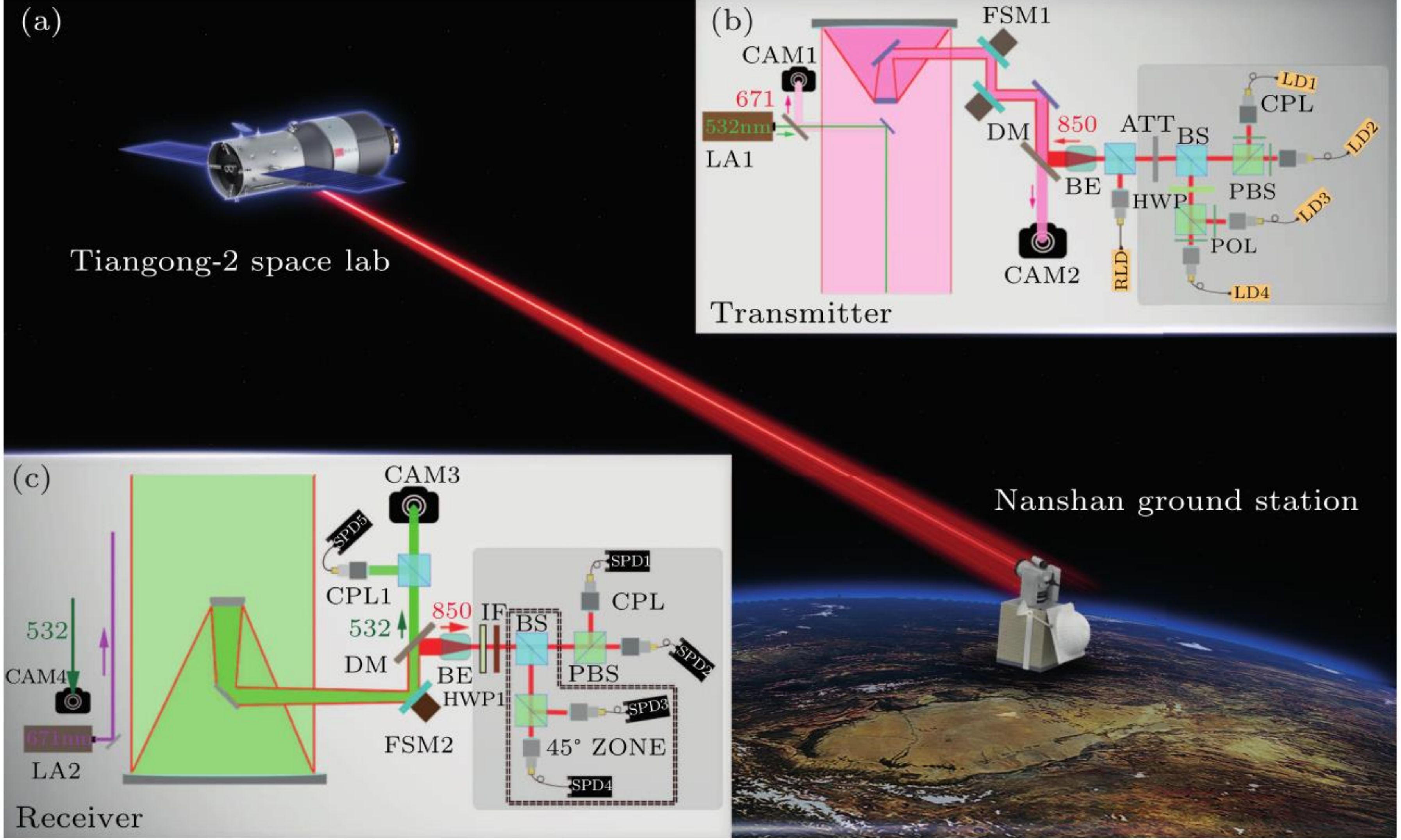
　　（“端”　is the smallest unit which cannot be cut）

About the same time as when Democritus proposed atomic theory: atoms cannot be destroyed

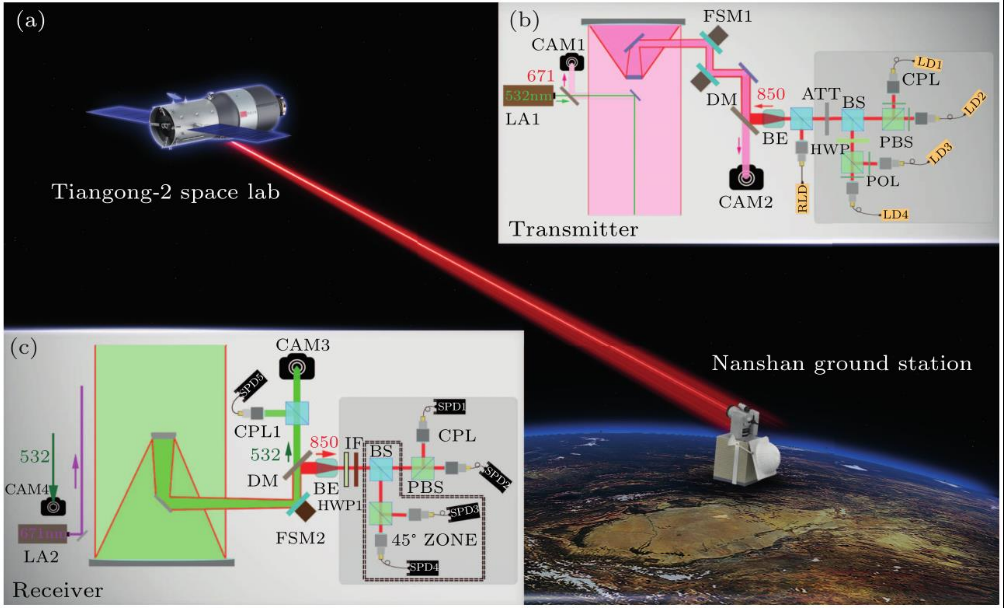
- **Prototype of law of inertia:**　“止，以久也，无久之不止”

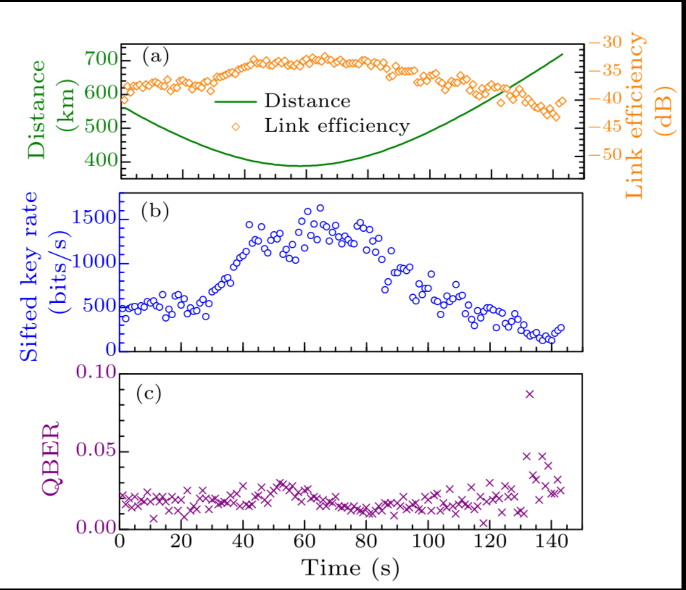
　　（In the absence of force, the movement does not stop ）

- In the meantime Greek philosopher Aristotle believed that a force was necessary to keep an object moving
- Newton's first law comes in 2000 years



(a)
Tiangong-2 space lab
Nanshan ground station
(b)
FSM1
CAM1
671
532nm
LA1
DM
850
ATT
BS
LD1
CPL
LD2
BE
HWP
PBS
LD3
POL
RLD
CAM2
LD4
Transmitter
(c)
CAM3
SPD5
SPD1
CPL1
CPL
850
IF
BS
532
532
DM
BE
PBS
SPD2
CAM4
HWP1
SPD3
FSM2
45° ZONE
671nm
LA2
SPD4
Receiver





- Total weight of the payload: 57.9 kg
- Average power: 80 W
- ~400km orbit with an inclination of 42^0

Chin. Phys. Lett. 34, 090302 (2017)

Future Prospect: QKD standardization

- **ISO/IEC JTC1 SC27 2017 Working Group Meeting**
  WG3 Study Period (SP) project "Security requirements, test and evaluation methods for QKD" was proposed


SRI
UTAH
UCSB
UCLA
1969
ARPANET


HAWAII
MOFFETT
LBL
LLL
SRI 2
XEROX
TYMSHARE
STANFORD
SUMEX
UCLA
USC
UTAH
DOCB
GWC
ANL
ILLINOIS
SCOTT
WPAFB
APWL
TEXAS
GUNTER
EGLIN
LINCOLN
MIT 44
MIT 6
CCA
RADC
NYU
RUTGERS
CMU
HARVARD
ABERDEEN
BELVOIR
NSA
NBS
NORSAR
DCEC
MITRE
ARPA
NRL
PENTAGON
LONDON
1977
ARPANET


ITHACA
PRINCETON
PITTSBURGH
BOULDER
URBANA
CHAMPAIGN
SAN
DIEGO
1988
NSFNET
Backbone

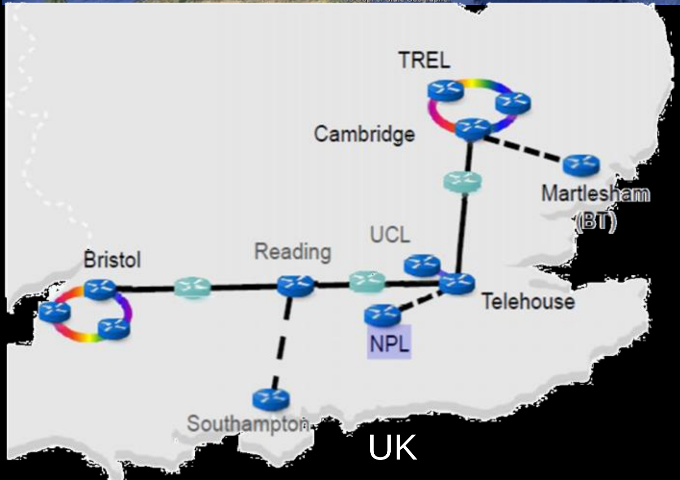

SEATTLE
PALO
ALTO
SALT
LAKE CITY
BOULDER
LINCOLN
CHICAGO
ANN
ARBOR
ITHACA
BOSTON
PRINCETON
PITTSBURGH
WASHINGTON
URBANA
CHAMPAIGN
ATLANTA
SAN
DIEGO
HOUSTON
1995
NSFNET
T3 Backbone


Data Centers of Banks
Data Centers
Super Computer Centers
乌兰巴托
哈尔滨
乌鲁木齐
比什凯克
呼和浩特
沈阳
平壤
首尔
银川
西宁
兰州
太原
济南
渤海
黄海
西安
南京
成都
合肥
东海
福州
台北
南宁
河内
海口
北部湾
南海
万象
Data © NavInfo

Future Prospect: Global Backbones

Europe Union

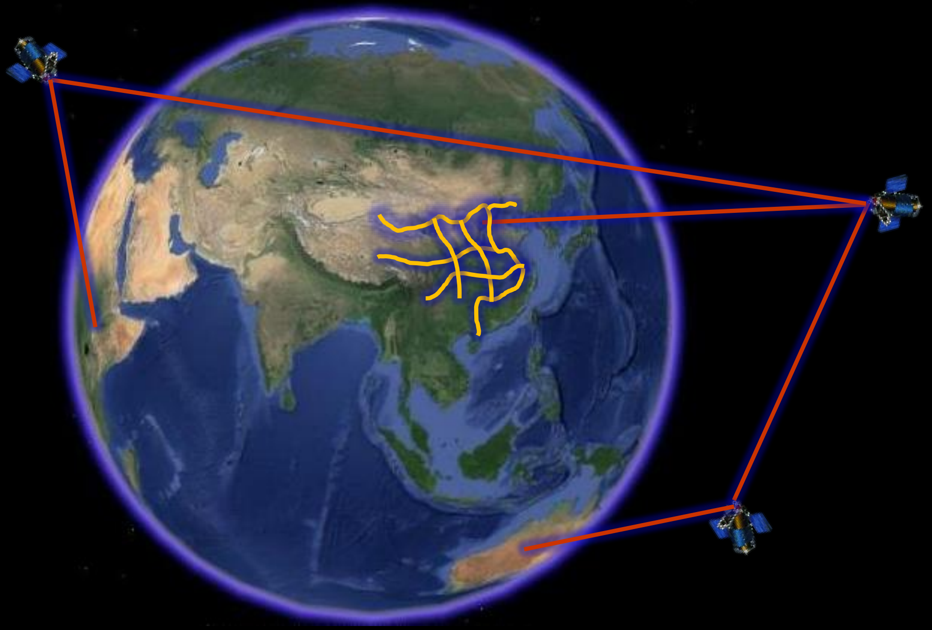
USA



UK

South Korea

Future Prospect



- Space--Ground Integrated Global quantum communication infrastructure ➡ "Quantum Internet"
- IAAS to PAAS to SAAS

Quantum Secure Every Bit

Team

Jian-Wei Pan

Chief scientist

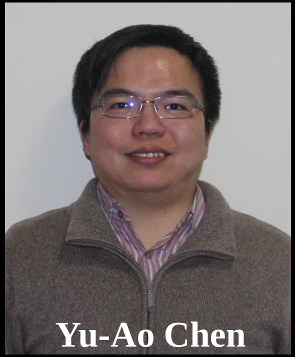
Quantum Science Satellite & Quantum Communication Backbone

Excellence Center for Quantum Information and Quantum Physics

University of Science and Technology of China

National Laboratory for Physical Sciences at Microscale

Cheng-Zhi Peng



Yu-Ao Chen

Qiang Zhang

Ji-Gang Ren

Juan Yin

Sheng-Kai Liao

Ping Xu

Yuan Cao

Jun Zhang

Teng-Yun Chen

Xiao Jiang

Yang Liu


Thanks!
Quantum
Physics & Quantum Information