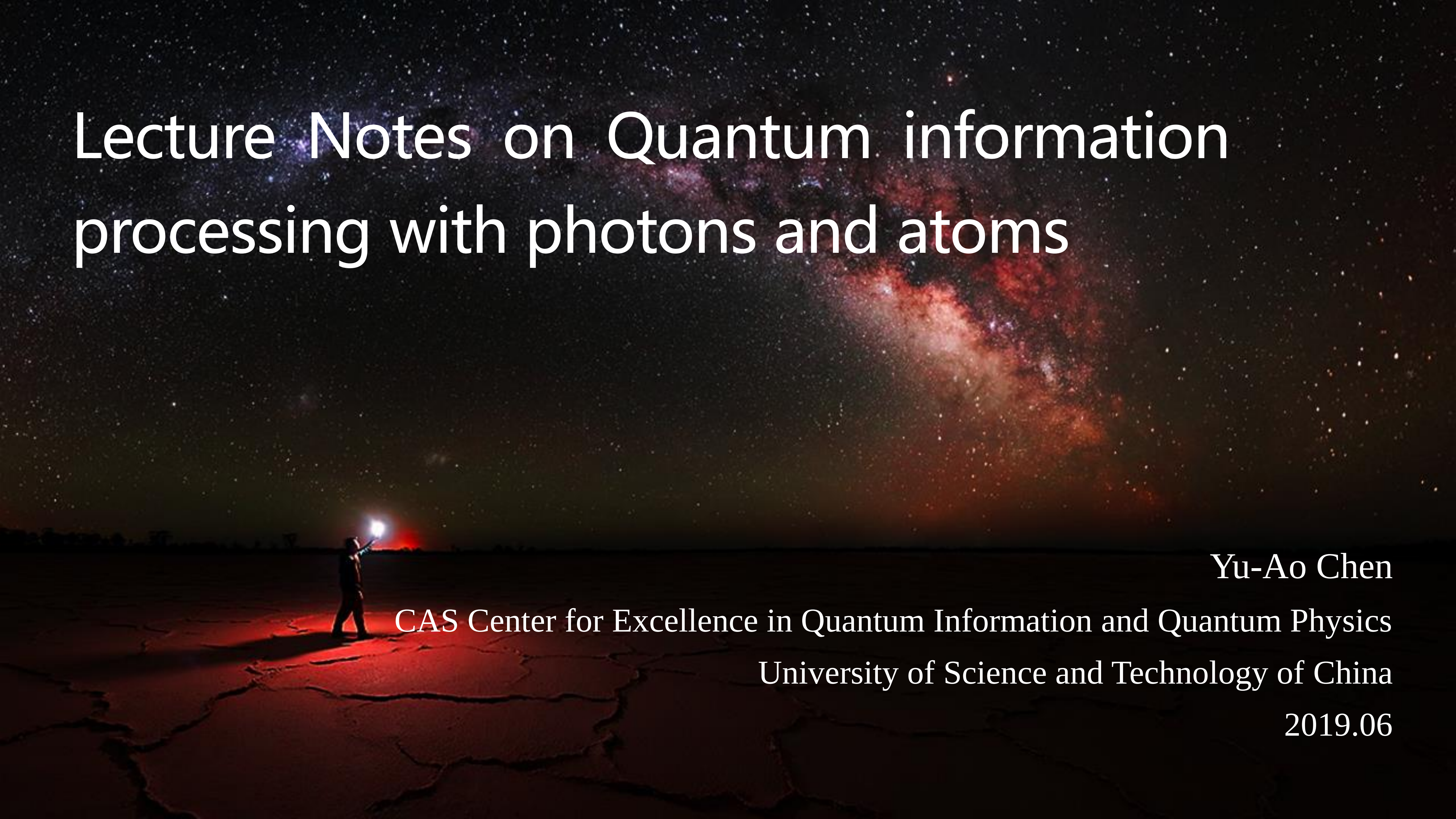


Lecture Notes on Quantum information processing with photons and atoms

Yu-Ao Chen

CAS Center for Excellence in Quantum Information and Quantum Physics

University of Science and Technology of China

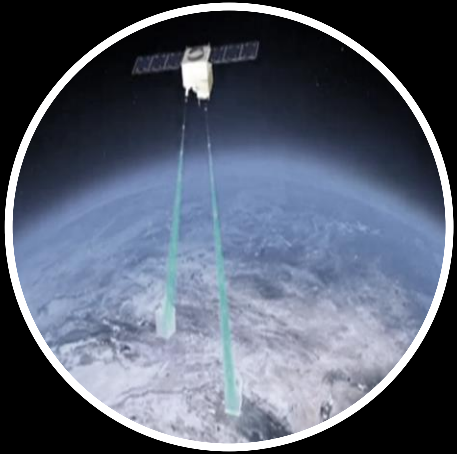
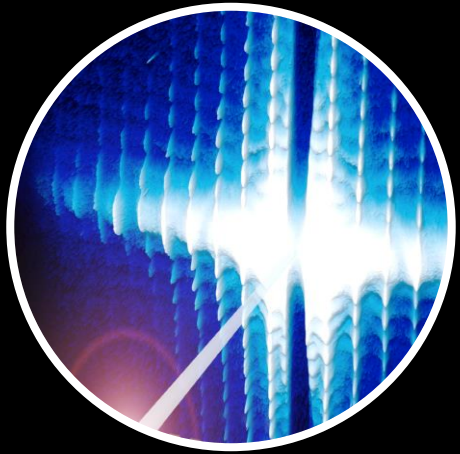
2019.06

Quantum Information Processing (QIP)

Born from the tests of "spooky action at a distance"

➡ Coherent manipulation of quantum systems

Harness the strange properties of quantum mechanics such as superposition and entanglement for enhanced ways of information processing

Unconditional security	Computational capacities	Super-resolution
		
Quantum communication	Quantum computation and simulation	Quantum metrology

Lecture 2:

Scalable Quantum Information Processing with Photons and Atoms

Part 1:

Elemental Optical Manipulations and Demonstrations of Quantum Communication

Optical Quantum Information Processing

Why do we like photons?

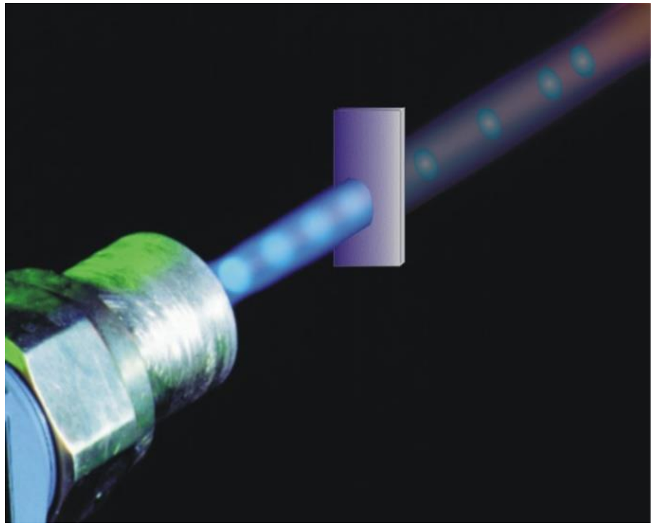
☑ Flying qubit (fastest quantum information transmitter)

☑ Robust qubit (with weak interaction with environment)

☑ High-precision manipulation with off-the-shelf devices

Single Photons: Generation & Detection

Generation of single photons



- Practical singe-photon source is far out of reach within current technologies
- Probabilistic quasi single photon: weak coherence pulse

$$|\psi\rangle \sim \sum_{n=0}^{\infty} \frac{p^n}{\sqrt{n!}} |n\rangle \xrightarrow{p \ll 1} |0\rangle + p|1\rangle$$

Single photon detector

- InGaAs Avalanche photo diode
- Si detector
- Superconducting nanowire detector……

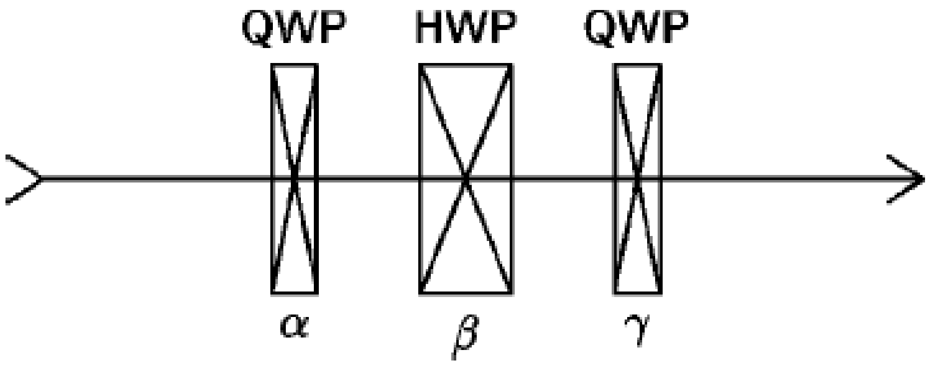
Single-qubit SU(2) Rotations

Arbitrary SU(2) rotation can be achieved by 3 elemental rotations:

$$U(\alpha,\beta,\gamma) = \exp\left(-i\frac{\alpha\sigma_x}{2}\right)\exp\left(-i\frac{\beta\sigma_z}{2}\right)\exp\left(-i\frac{\gamma\sigma_x}{2}\right)$$

Rotation around x axis with an angle of α

Rotation around z axis with an angle of β

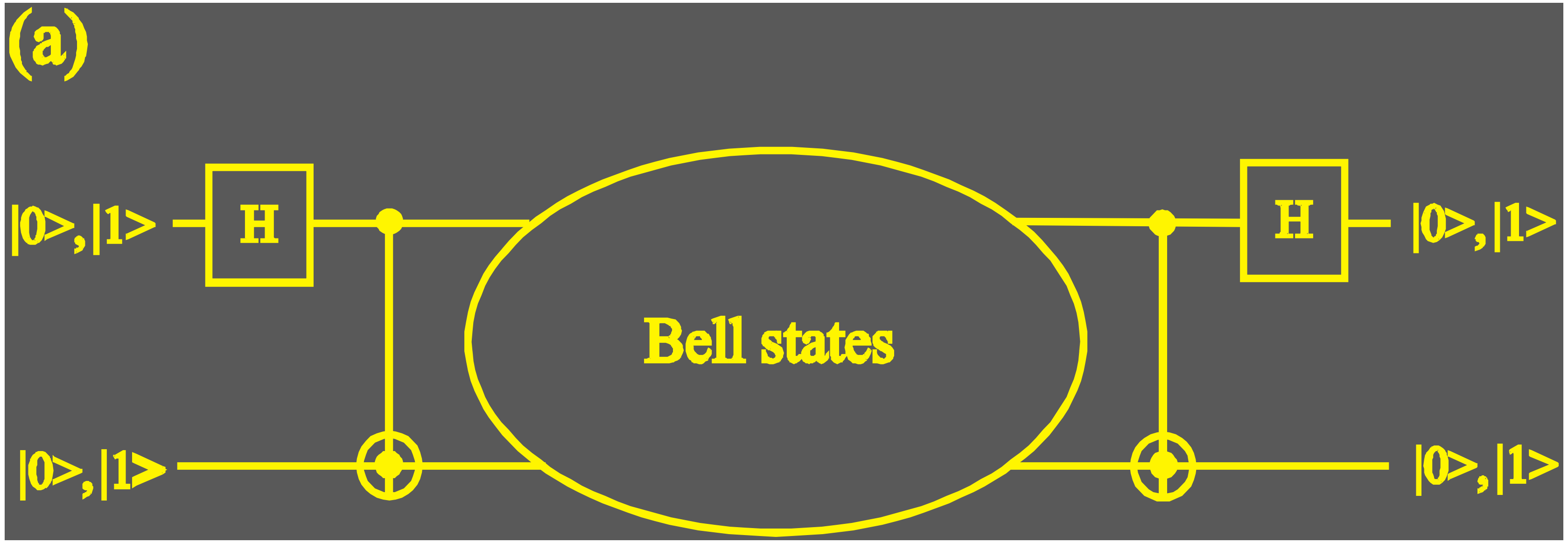


☑ It can be easily realized with polarization states of a photon undergoing two types of wave plates

QWP: quarter-wave plate

HWP: half-wave plate

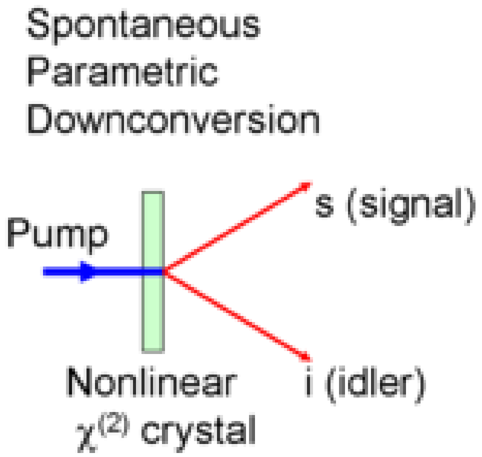
Manipulation of Entanglement

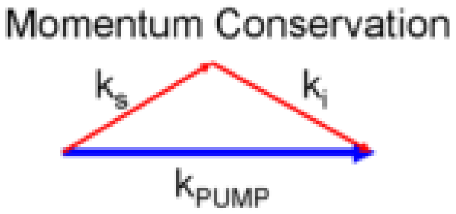


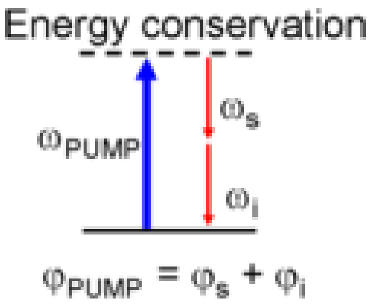
For photons, CNOT gate requires strong non-linear coupling

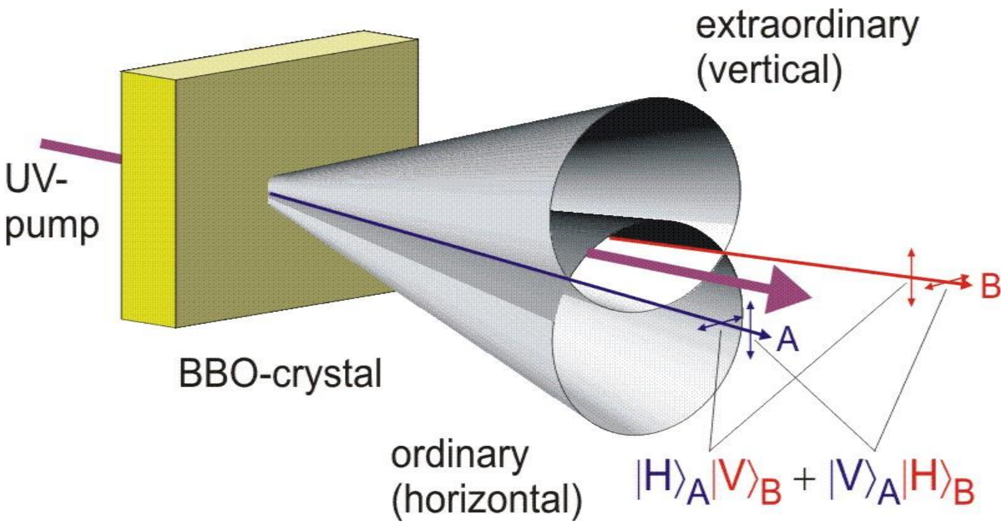
☒But the coupling between photons is negligibly weak!

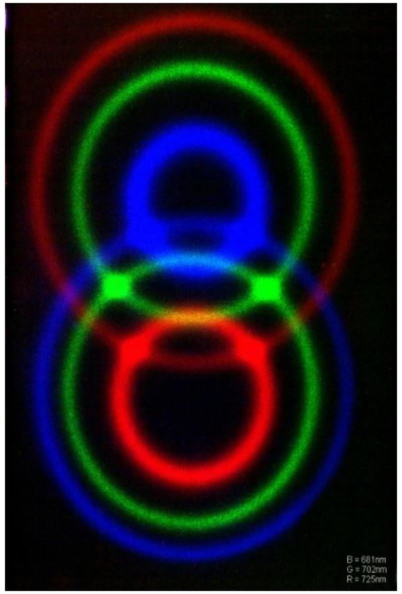
Spontaneous Parametric Down-conversion (SPDC)







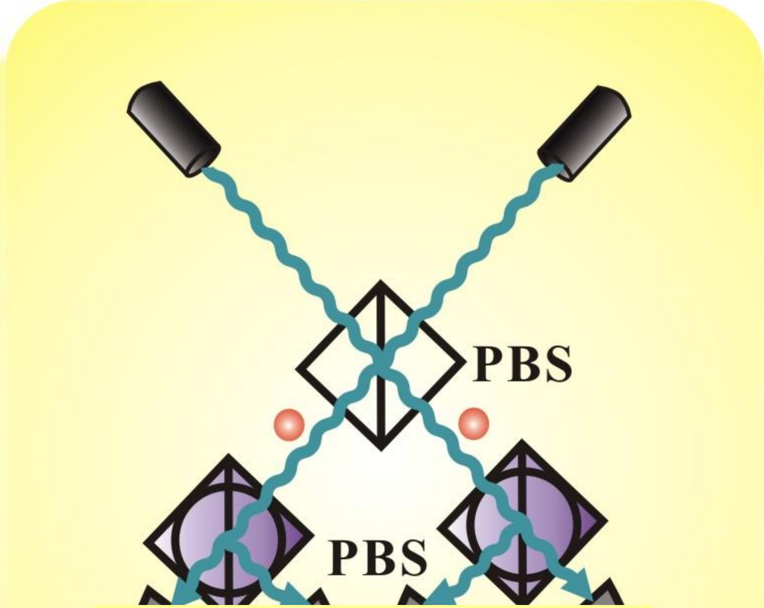




Kwiat *et al.*, PRL 75, 4337 (1995)

Bell-state Measurement (BSM) with Linear Optics

Pan and Zeilinger, PRA 57, 2208 (1998)



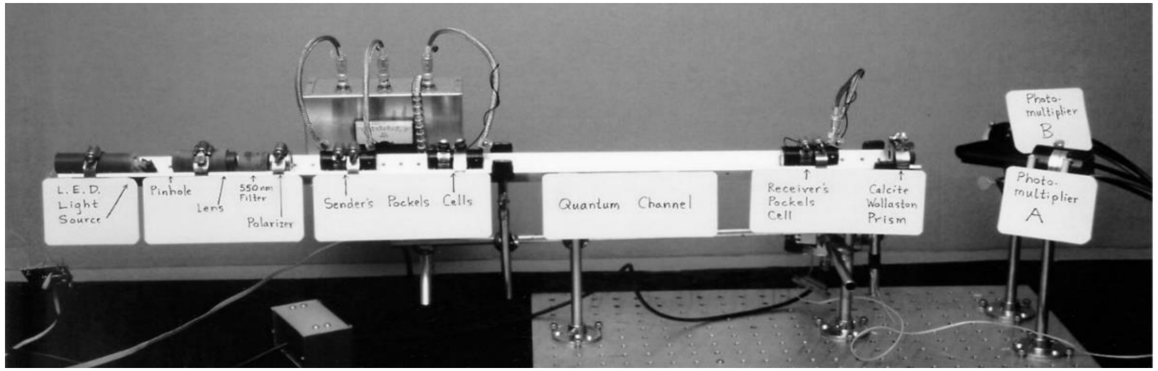
$$|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle|+\rangle + |-\rangle|-\rangle\right)$$

$$|\Phi^{-}\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle|-\rangle + |-\rangle|+\rangle\right)$$

	D1	D2
D3	$\vert\Phi^-\rangle$	$\vert\Phi^+\rangle$
D4	$\vert\Phi^+\rangle$	$\vert\Phi^-\rangle$

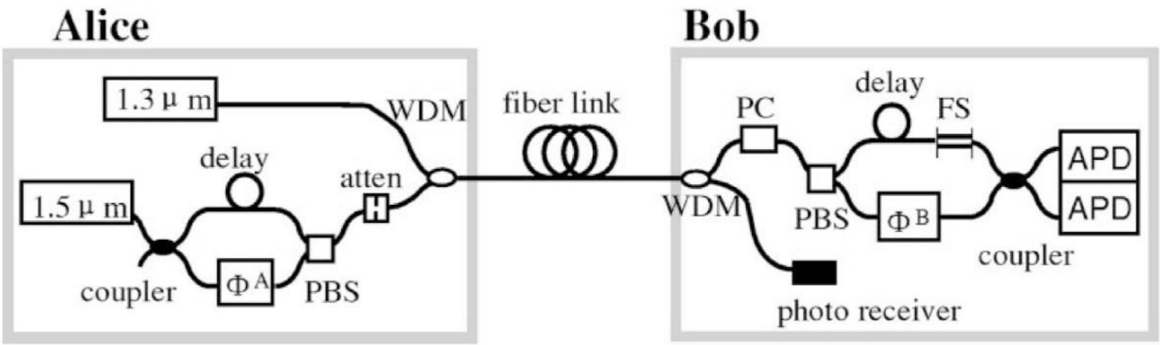
Required non-linearity of CNOT gate can be effectively induced with the help of post-selection measurements

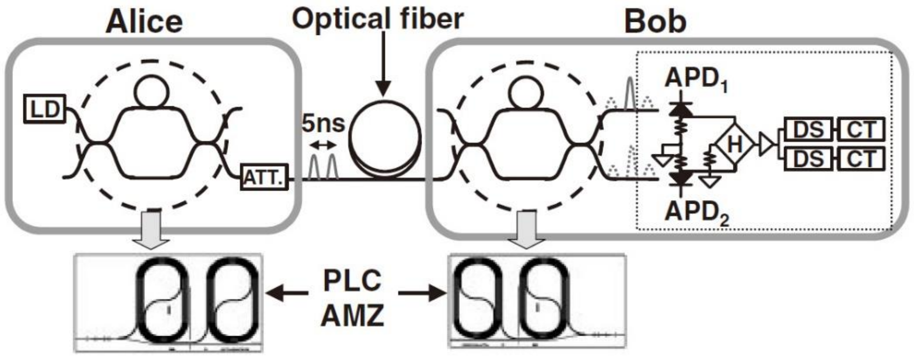
Proof of Concept Demostrations of QKD



First concept demonstration (32 cm)

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





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

……

Security of QKD with Realistic Devices

Security loopholes due to imperfection of realistic quantum devices!

Security of QKD with Realistic Devices

➡ Security loophole 1: imperfect single-photon source

Quasi single photon source:

Two identical photons per pulse with probability $P^2/2$

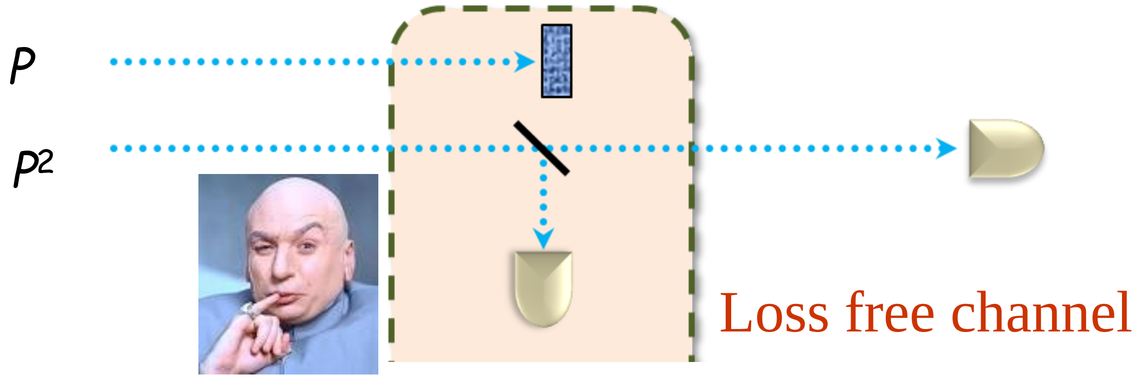
$$|\psi\rangle \sim \sum_{n=0}^{\infty} \frac{p^n}{\sqrt{n!}} |n\rangle \xrightarrow{p \ll 1} |0\rangle + p|1\rangle$$

Photon number splitting attack (PNS):

Eavesdrop the keys with two photon events

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

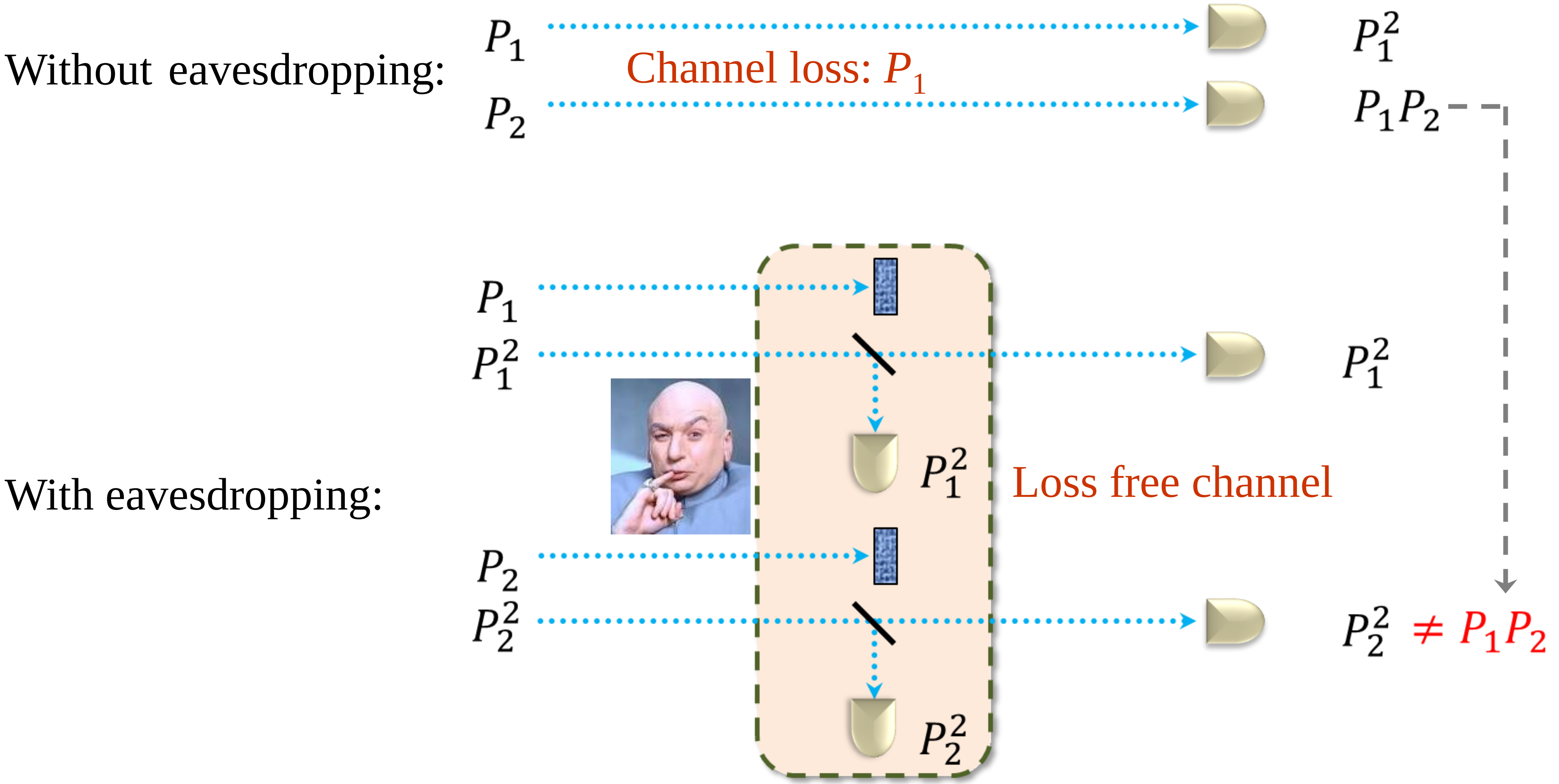
- ☒ Not secure when distance is longer than ~10km
- ☒ Very low key rate



Security of QKD with Realistic Devices

➡ Solution: Decoy-state QKD scheme: sending pulses randomly with intensity P_1 or P_2

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



Experiments

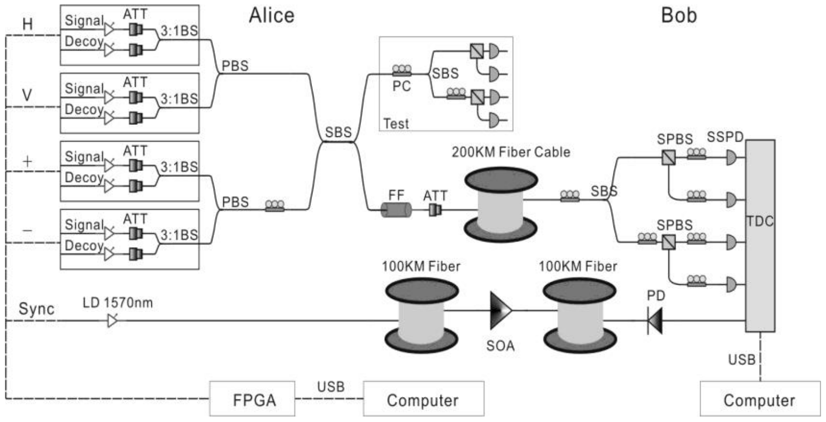
100km:

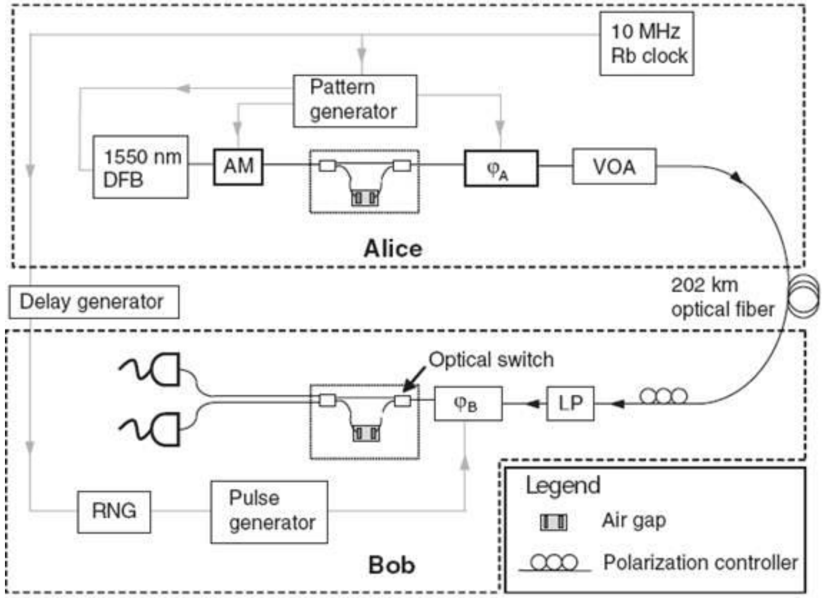
Rosenberg *et al.*, PRL 98, 010503 (2007)

Peng *et al.*, PRL 98, 010505 (2007)

200km:

Liu *et al.*, Optics Express 18, 8587 (2010)

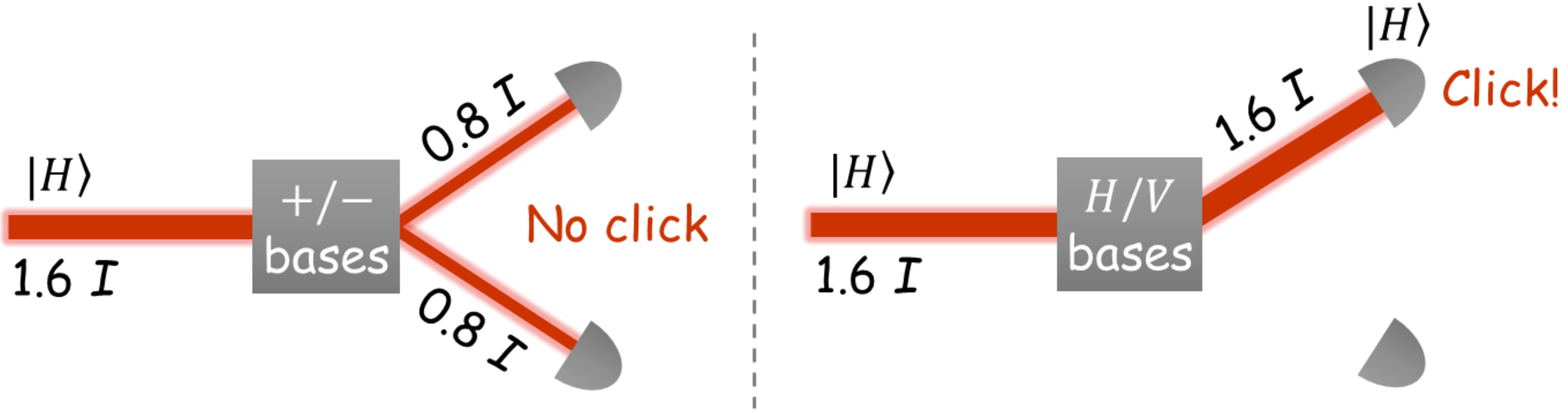




Security of QKD with Realistic Devices

➡ Security loophole 2: imperfect single-photon detectors

Blinding attack: can fully control detectors by specially tailored strong light [Lydersen *et al.*, Nature Photonics 4, 686 (2010)]

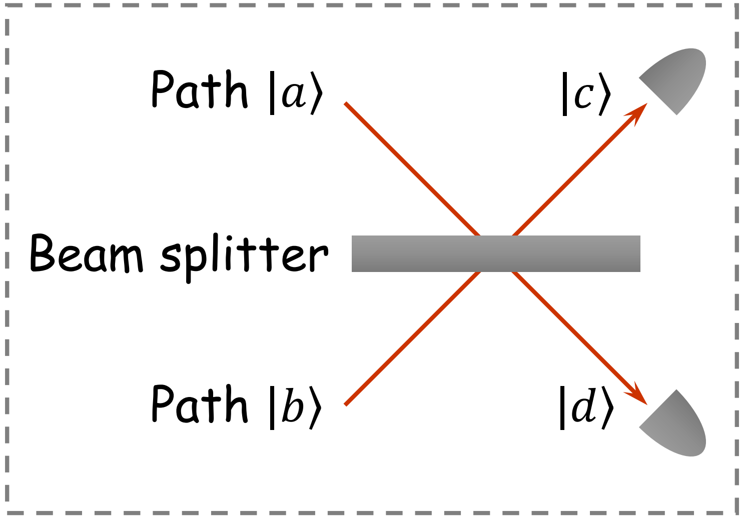


Security of QKD with Realistic Devices

- Solution: Measurement Device Independent QKD: Immune to any attack on detection
  - Scheme: Lo *et al.*, PRL 108, 130503 (2012)

Key point: two-photon interference (HOM effect)

consider simultaneously input two photons with the same polarization $\alpha|H\rangle + \beta|V\rangle$ to a BS



Effect of BS: $|a\rangle \rightarrow |c\rangle + |d\rangle, |b\rangle \rightarrow |c\rangle - |d\rangle$

Input: $|a\rangle \otimes |b\rangle \rightarrow (|c\rangle + |d\rangle)(|c\rangle - |d\rangle)$
$\rightarrow |c\rangle|c\rangle + \cancel{|d\rangle|c\rangle - |c\rangle|d\rangle} + |d\rangle|d\rangle$

Identical photons

- Two photons will output from the same side of BS
- And coincidence detection will occur only if the polarizations of two photons are different

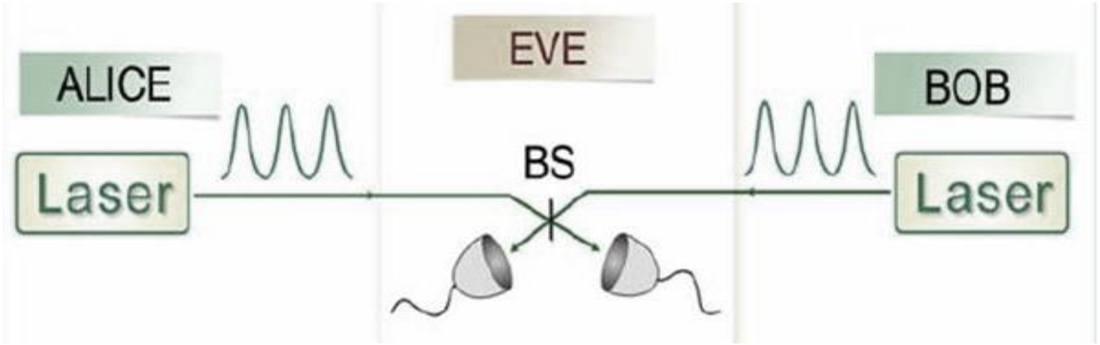
Hong, Ou & Mandel, PRL 59, 2044 (1987)

Security of QKD with Realistic Devices

- Alice and Bob send one of four polarization states randomly to measurement station

Coincident events ➡

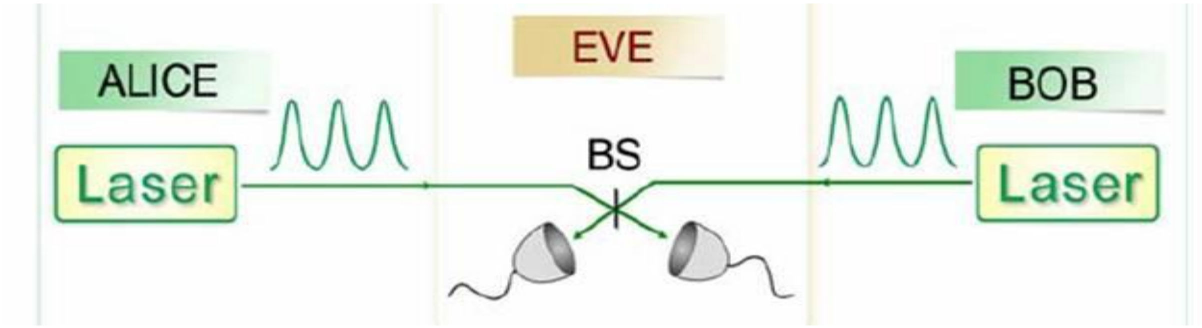
Alice's basis	Alice's state	Bob's basis	Bob's state
+	↔	+	↕
+	↔	×	⤢ or ⤡
+	↕	+	↔
+	↕	×	⤢ or ⤡
×	⤢	+	↕ or ↔
×	⤢	×	⤡
×	⤡	+	↕ or ↔
×	⤡	×	⤢



Measurement station

- Compare their basis in public channel, keep the cases that basis choices are the same
- Share key according to anti-correlation of polarizations
- Even measurement station is fully controlled by Eve, she can only reveal the correlation information, but gains no information of the key

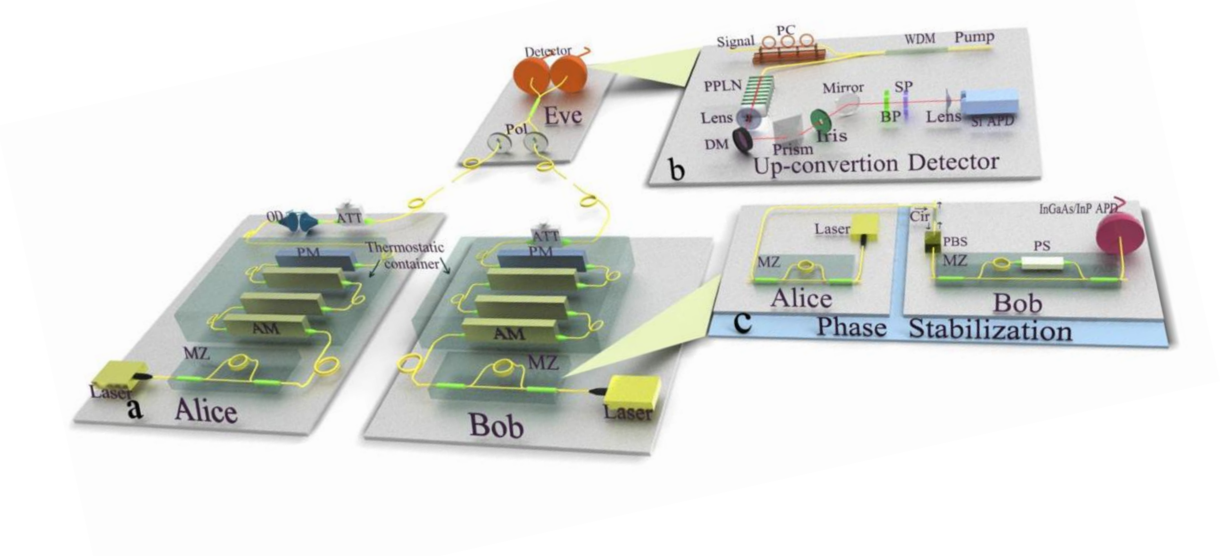
Security of QKD with Realistic Devices



High-precision interference between two remote independent lasers: relative timing jitter after hundreds km fiber < 10ps

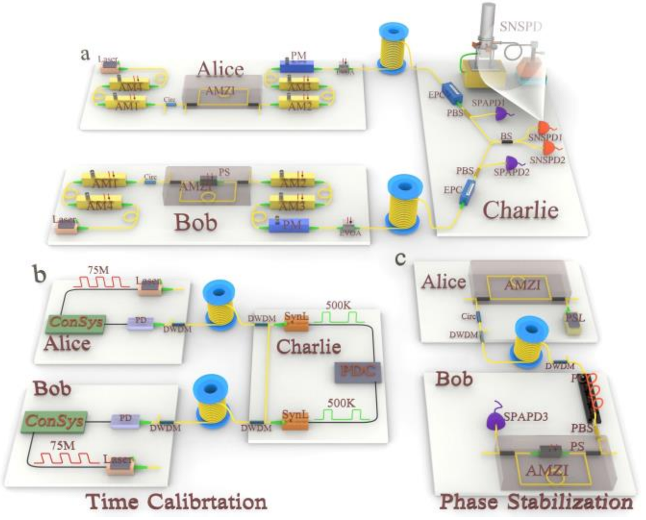
First experiment (50km):

- Liu *et al.*, PRL 111, 130502 (2013)

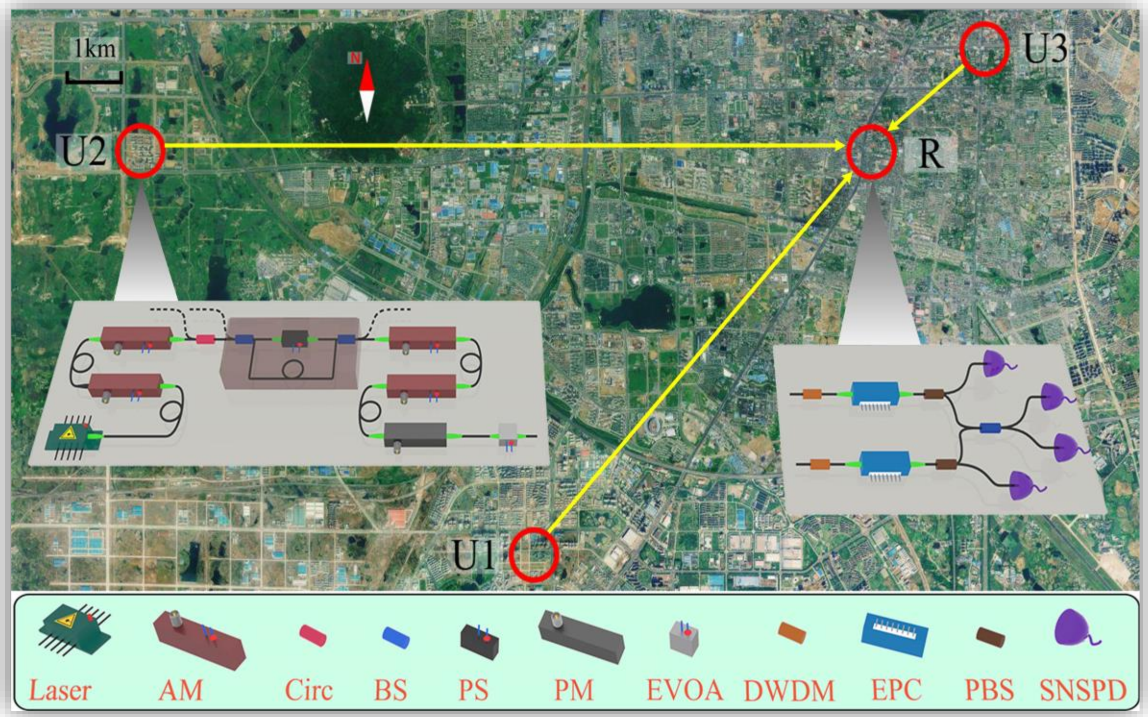


Extended distance:

- 200km: Tang *et al.*, PRL 113, 190501 (2014)
- 404km: Yin *et al.*, PRL 117, 190501 (2016)



Security of QKD with Realistic Devices



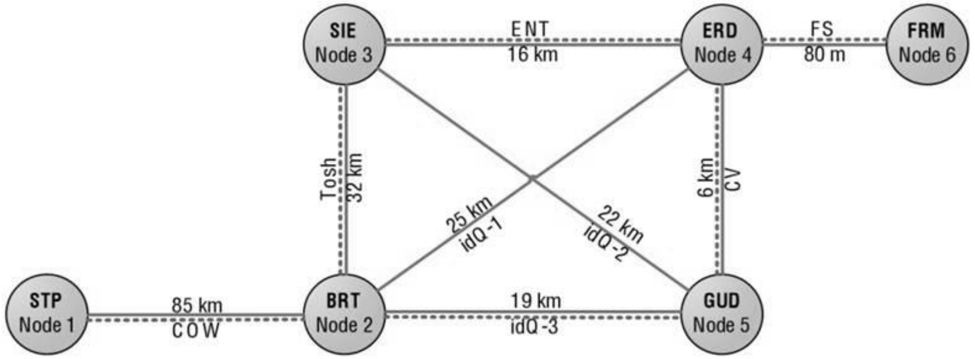
Field test
[Tang et al., IEEE JSTQE 21, 6600407(2015)]

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)

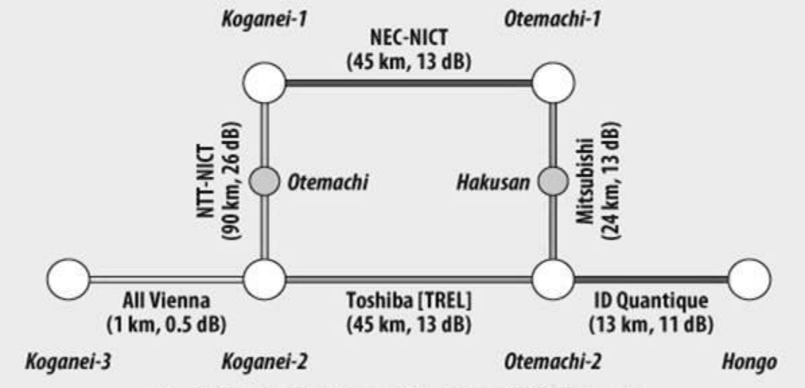
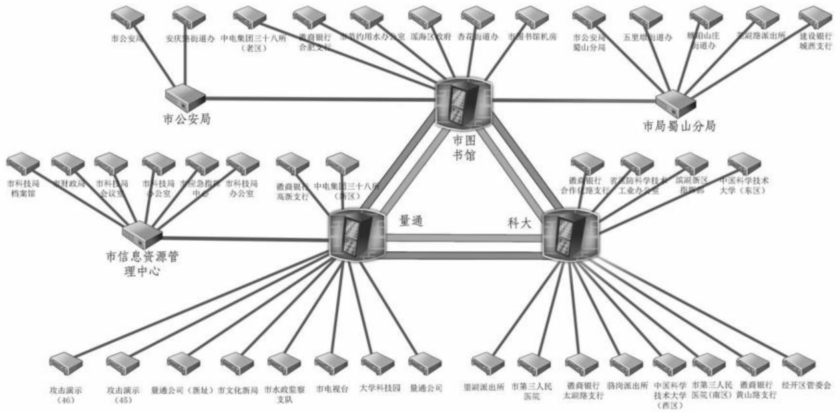


Fig. 3 Topological Map of the Tokyo QKD Network



Tokyo QKD Network (Japan)

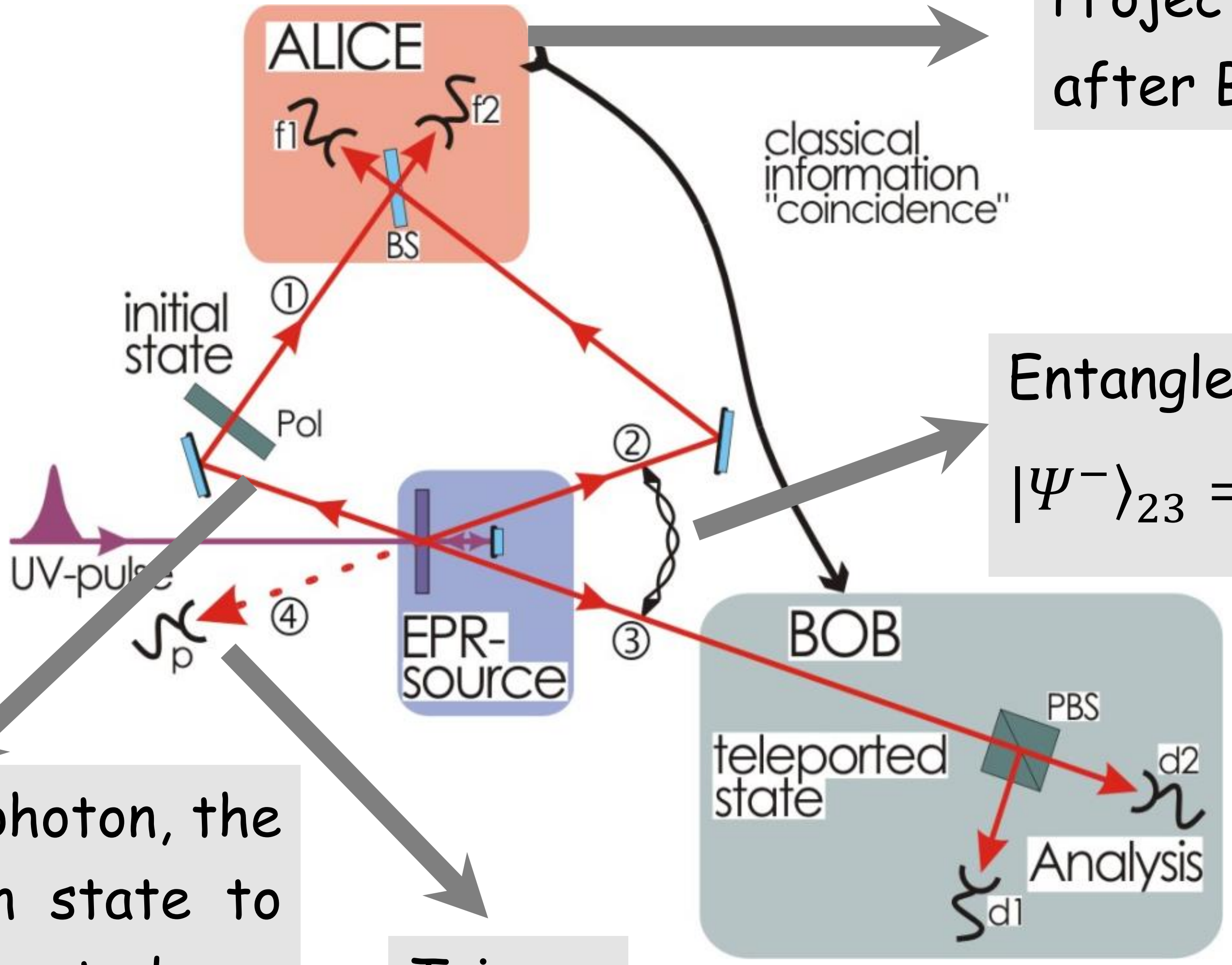
M. Sasaki *et al.*, Opt. Express 19, 10387 (2011)

First large-scale metropolitan network

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

Experimental Quantum Teleportation

Project to $|\Psi^-\rangle_{12}$ by coincidence after BS



Entangled state

$$|\Psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(|H\rangle_2|V\rangle_3 - |V\rangle_2|H\rangle_3)$$

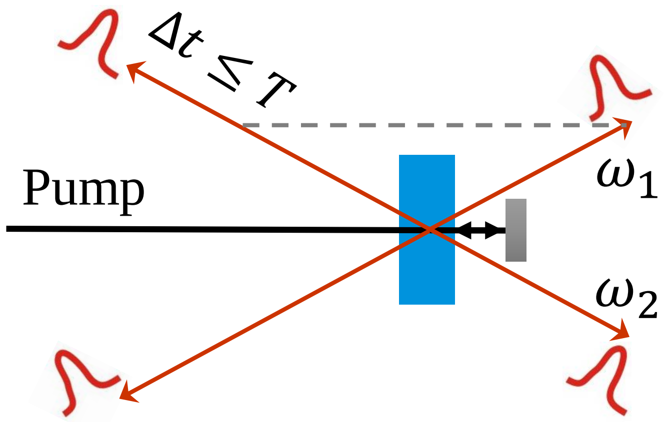
Single photon, the unknown state to be teleported

Trigger

Bouwmeester *et al.*, Nature 390, 575 (1997)

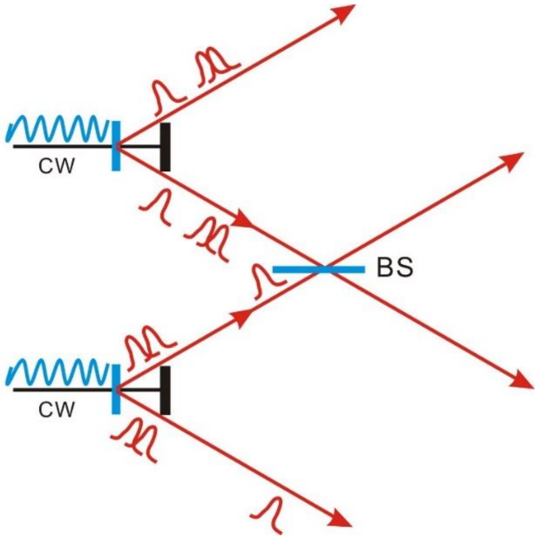
But it was not so straightforward……

Two photons must be indistinguishable on the BS ➡ be spatially and temporally overlapped on the BS perfectly



However, if the pulse duration T of pump is too long (e. g., a CW laser)

☒ A large uncertainty of generation time of two EPR pairs (~T)

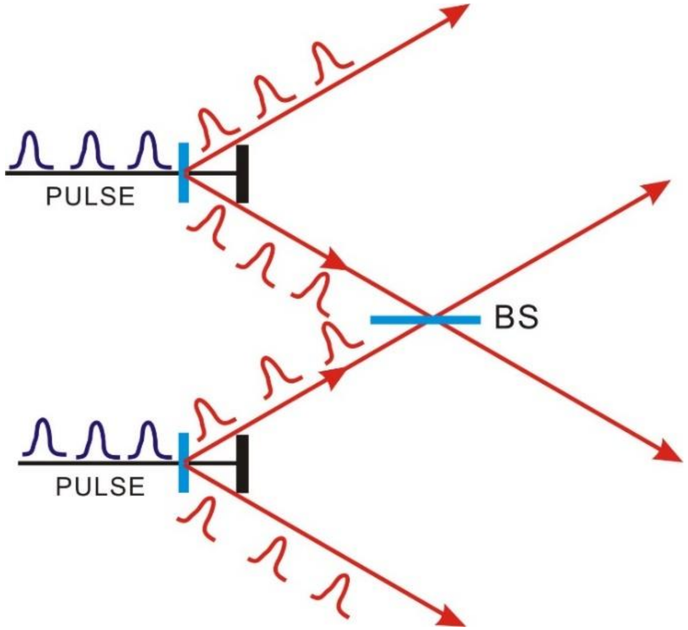


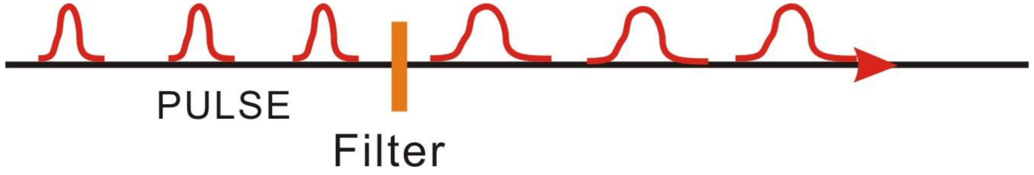
Energy conservation condition $\omega_1 + \omega_2 = \omega_{\text{pump}}$, allows some uncertainty of frequency $\delta\omega$ of EPR pair

☒ The coherent time of EPR pair ($\delta t = 1/\delta\omega$, at the order of 100fs) will be much shorter than T

Experimental Quantum Teleportation

☑ A solution is to use short pulse laser (pump pulses duration: 200 fs)





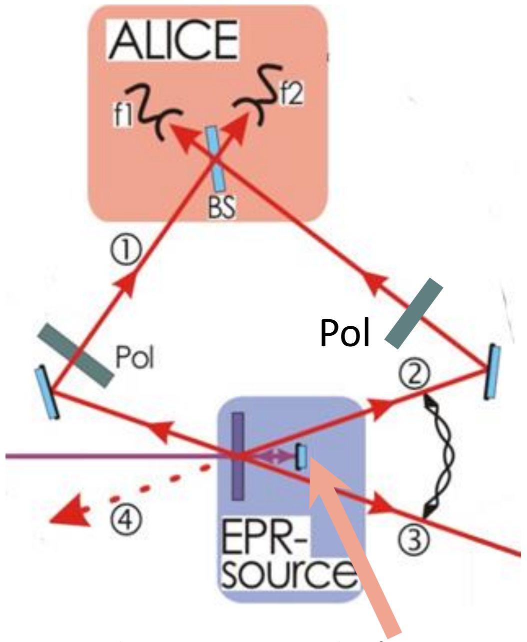
The pulse will bring some time jitter to the SPDC photon

☑ Insert a narrow band filter can extend the coherent time (4nm results in a coherence time of 520 fs)

Experimental Quantum Teleportation

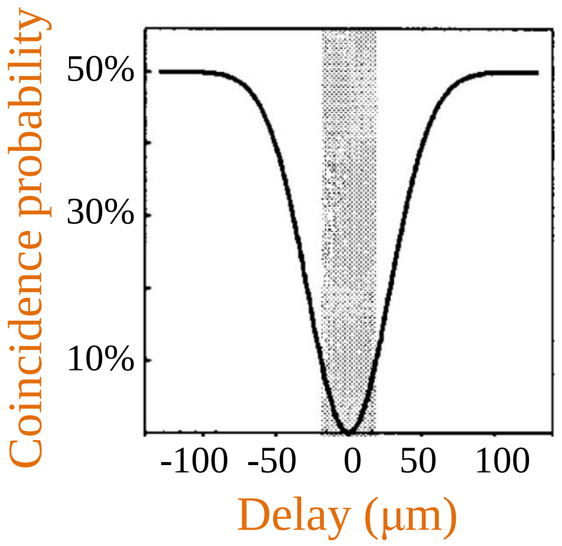
☒ The coherent time of EPR photons is definitely shorter than the time resolution of state-of-the-art single photon detectors in 1997 ➡ we cannot confirm that photons were well-overlapped at the BS by detecting the arriving time

☑ Scan the interference fringes



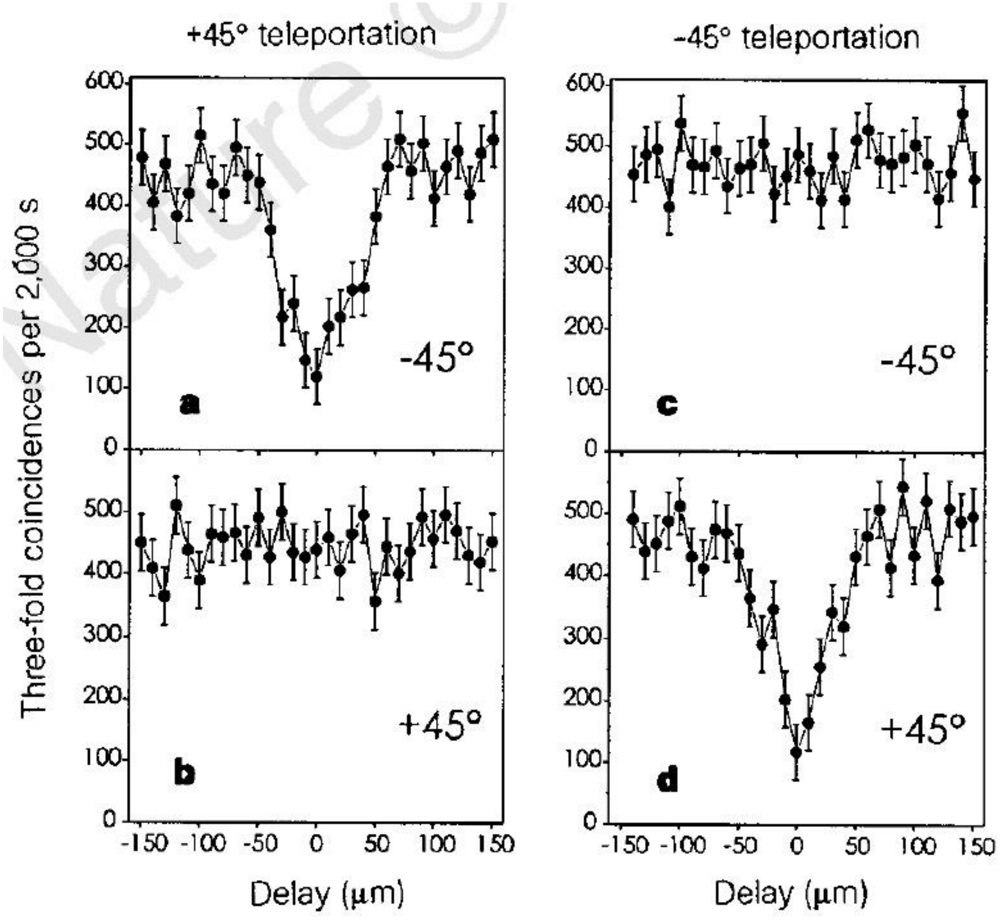
Adjusting delay between photon 1 and 2

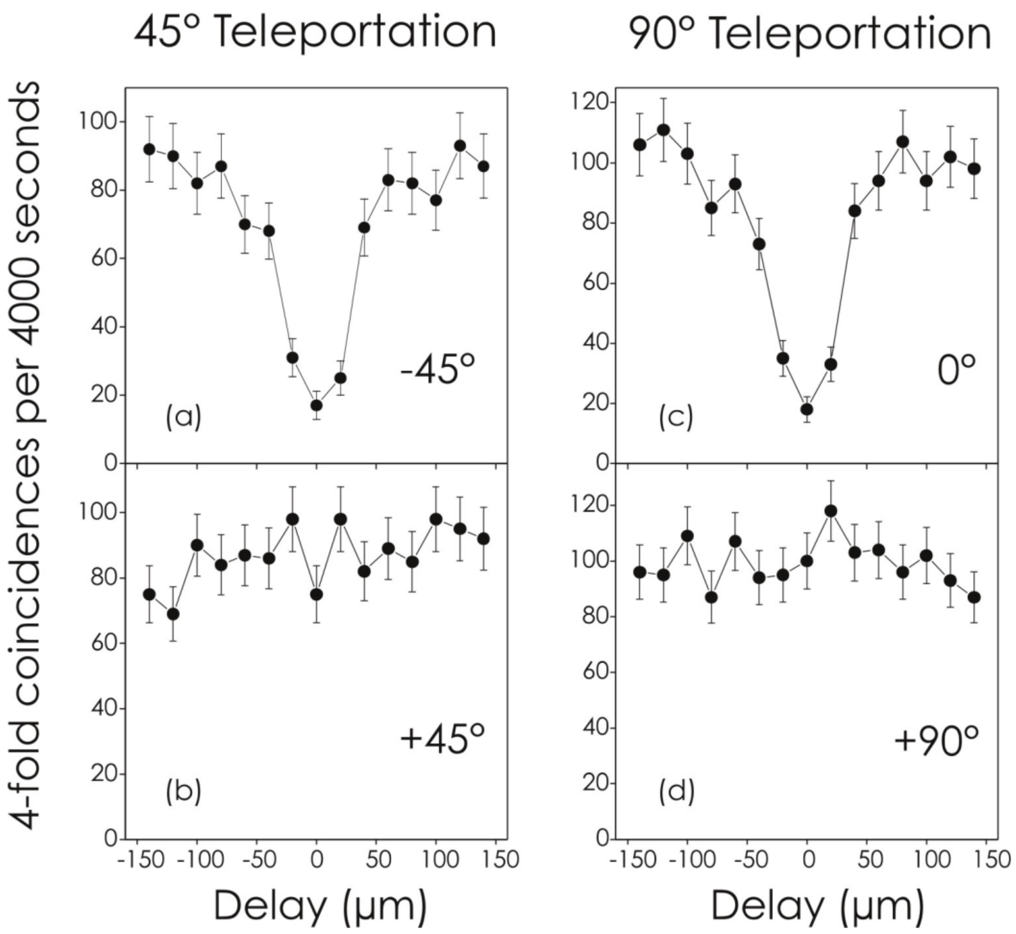
- Insert two polarizers to make the polarizations of photon 1 and 2 the same
- Due to HOM effect, there will be no coincidence in theory when two photons are well-overlapped
- Adjust delay to find the optimal position



Experimental Quantum Teleportation

The experimental results

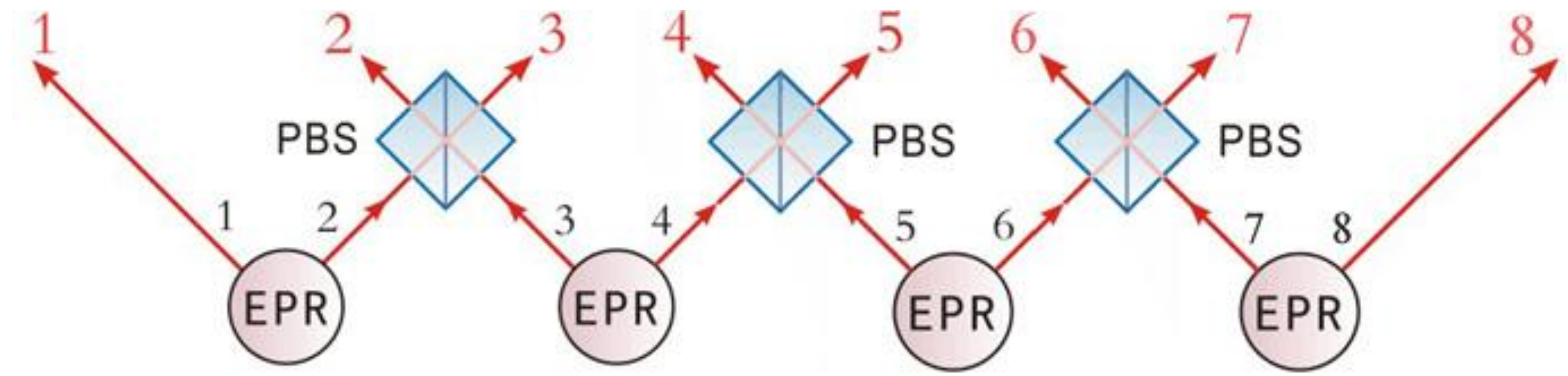




Part 2: Multi-photon Interferometry

Multi-photon Interferometry

Essential task: generation and manipulation of multi-photon entanglement!



P P P P

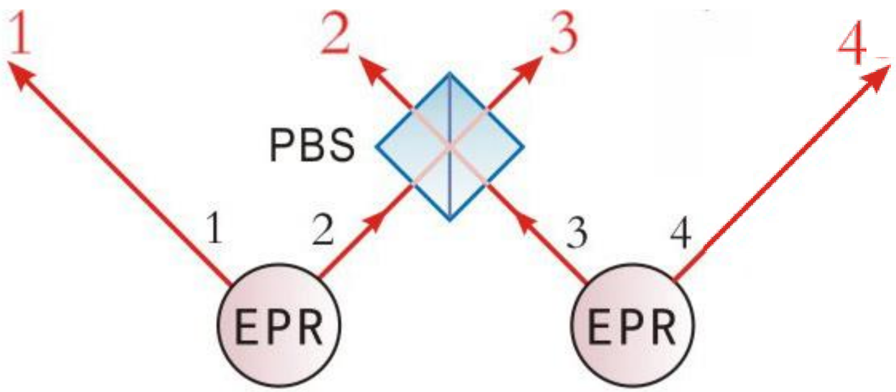
Two-photon entanglement source: P →Four-photon entanglement: $P^2/2$

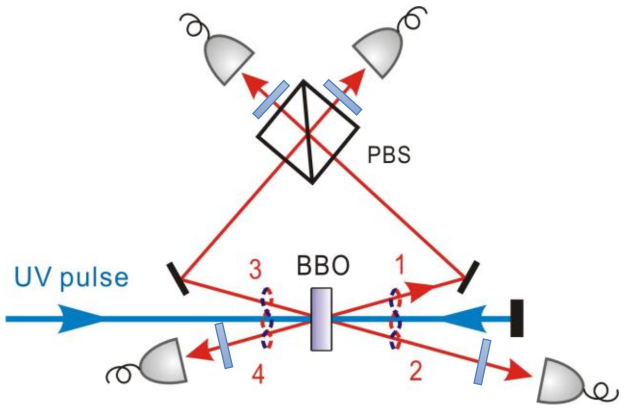
→ Six-photon entanglement: $P^3/4$ → Eight-photon entanglement: $P^4/8$…

One must need high-brightness entanglement source!

Multi-photon Interferometry

In 2001: Brightness of entanglement source: 2500pair/s@76MHZ

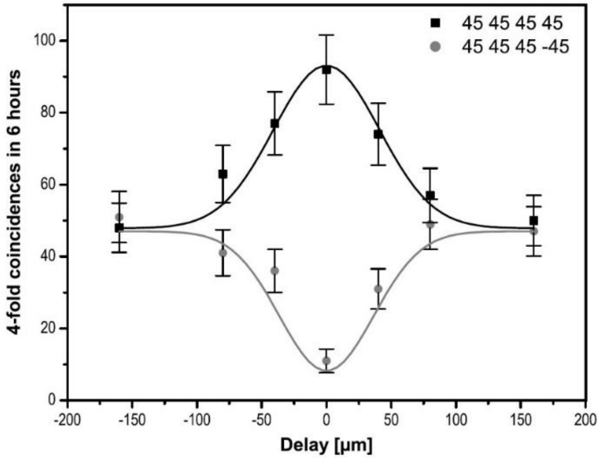




$$(HH+VV)(HH+VV)$$

$$= HHHH+\cancel{HHVV}+\cancel{VVHH}+VVVV$$

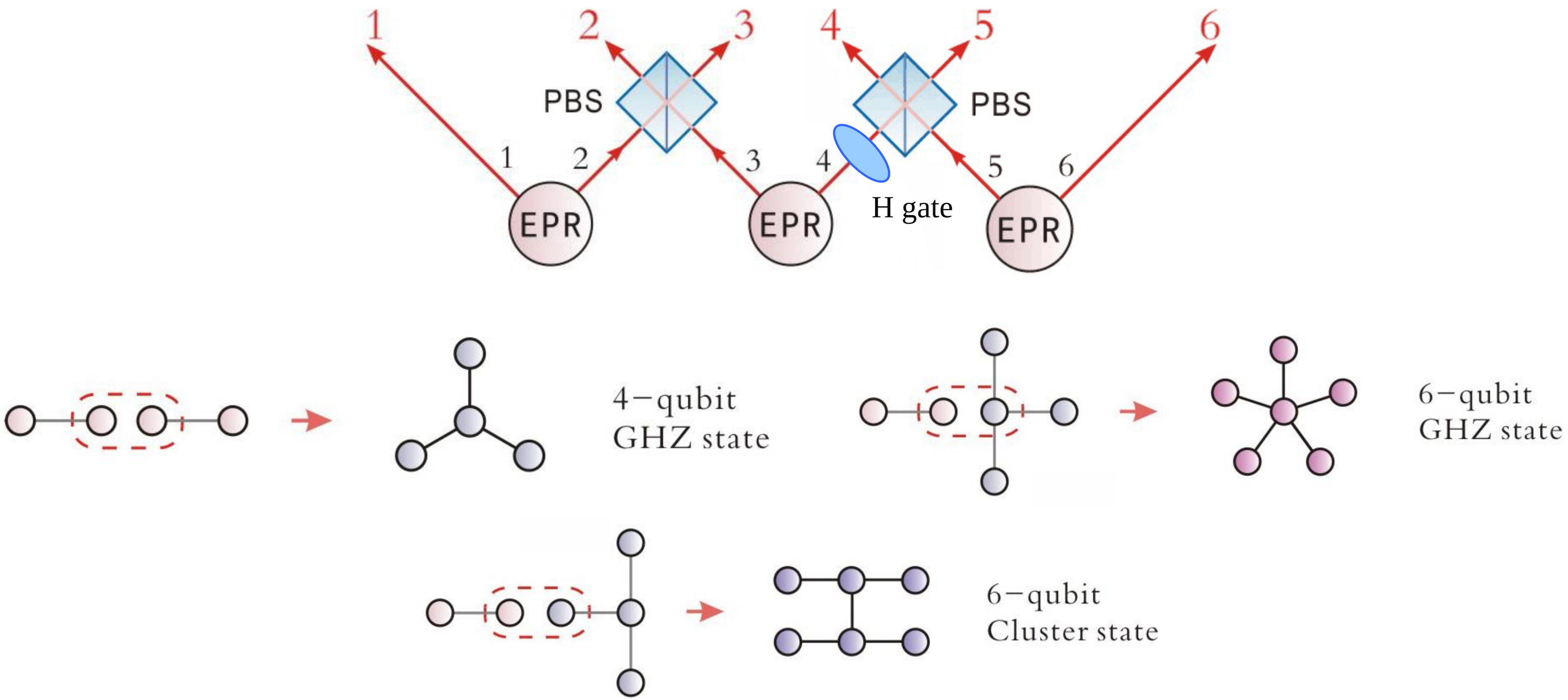
$$\rightarrow HHHH+VVVV$$



Pan *et al.*, PRL 86, 4435 (2001)

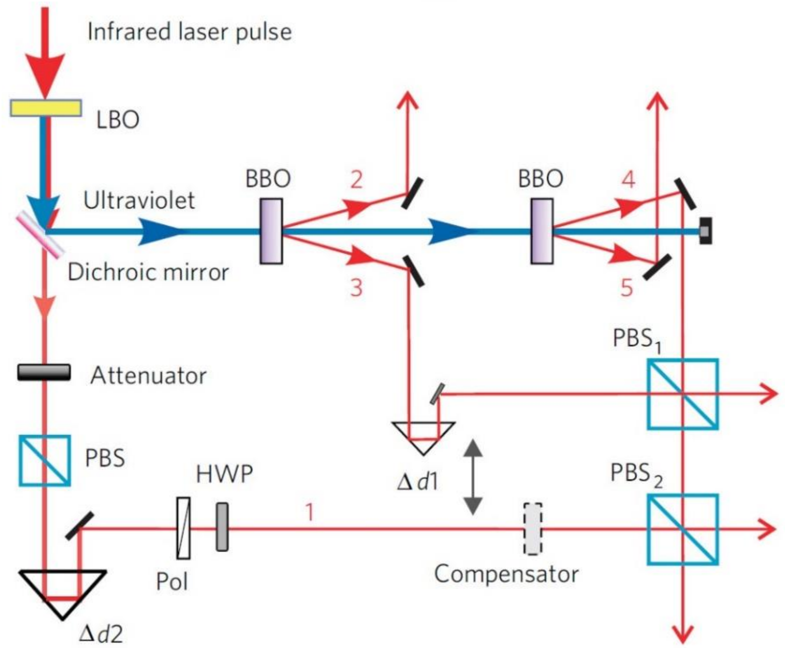
Six-photon Cluster States

In 2007: A brighter, stable laser pump source, Verdi 10W → 16W, IR ~ 2.5W
Brightness of entanglement source: 93000pair/s@76MHZ



Lu *et al.*, Nature Physics 3, 91 (2007)

Hyper-entangled Schrödinger Cat States

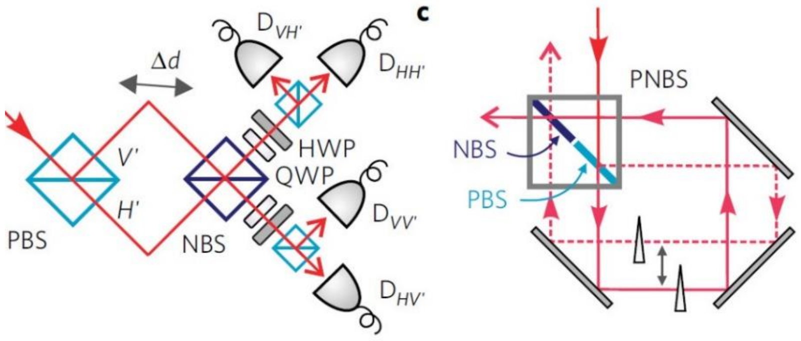


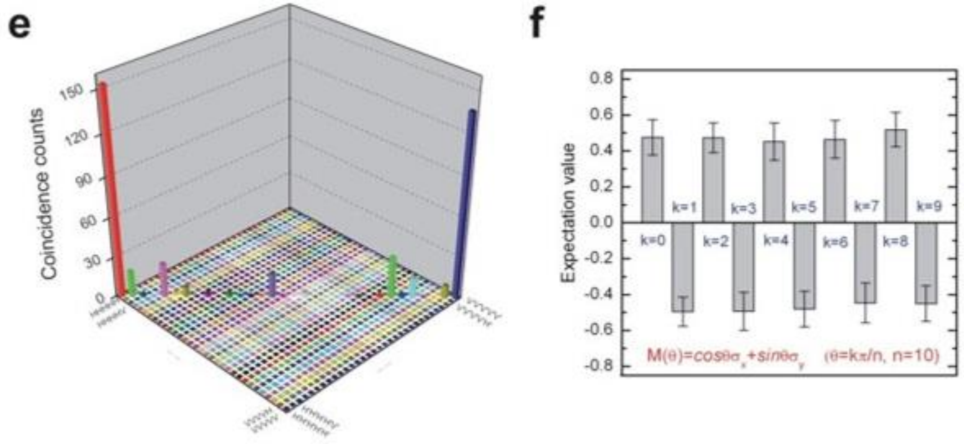
Hyper-entangled state: Polarization and spatial modes

$$\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \rightarrow \frac{1}{\sqrt{2}}(|H\rangle|H'\rangle + |V\rangle|V'\rangle)$$

5-photon 10-qubit cat state

$$\frac{1}{\sqrt{2}}\left(|H\rangle^{\otimes 5}|H'\rangle^{\otimes 5} + |V\rangle^{\otimes 5}|V'\rangle^{\otimes 5}\right)$$





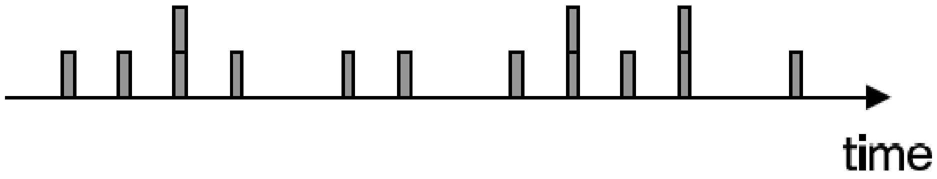
Gao *et al.*, Nature Physics 6, 331 (2010)

The Request for Both High Brightness & Fidelity

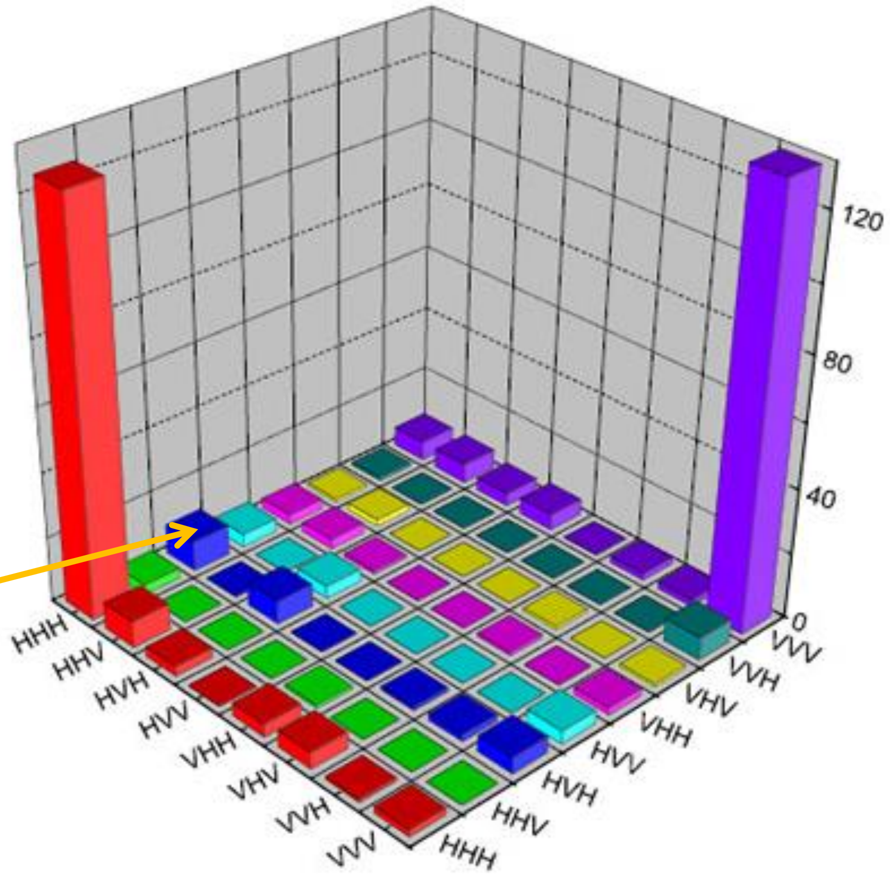
With higher pump

- ☑ Increase probability
- ☒ More double pair emissions ➡ degrades fidelity

$$P_n = \frac{\mu^n e^{-\mu}}{n!}$$

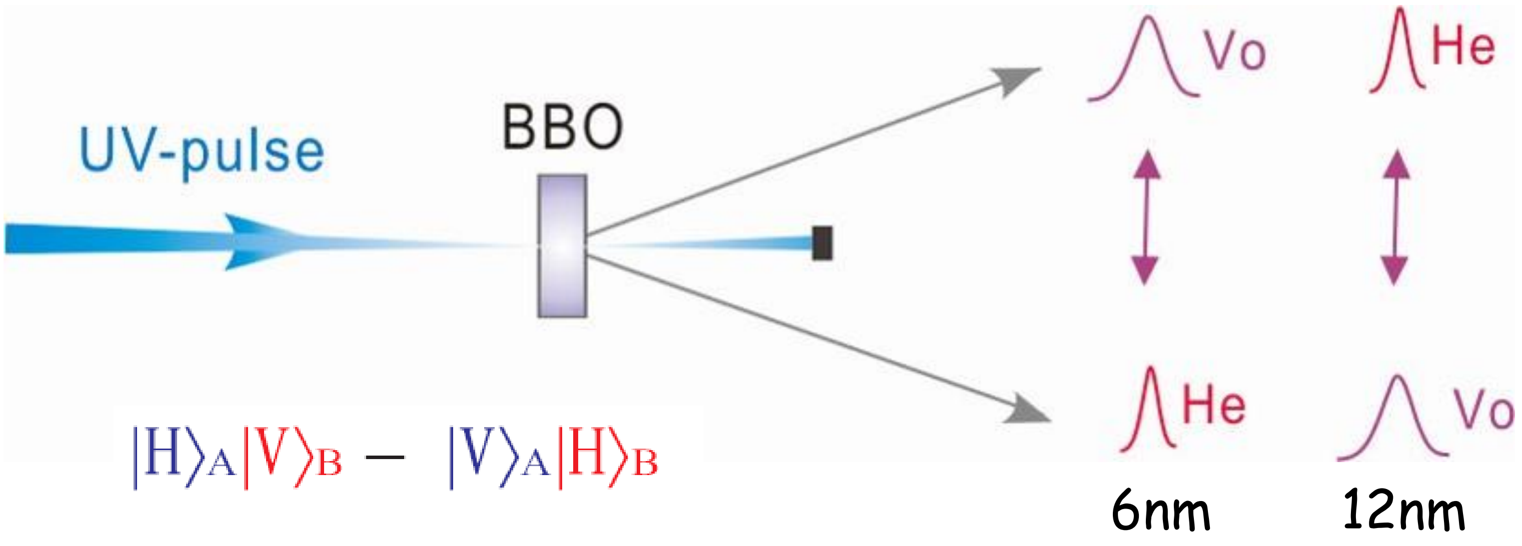


Error



Can we have very bright source of entangled photons, meanwhile with high fidelity?

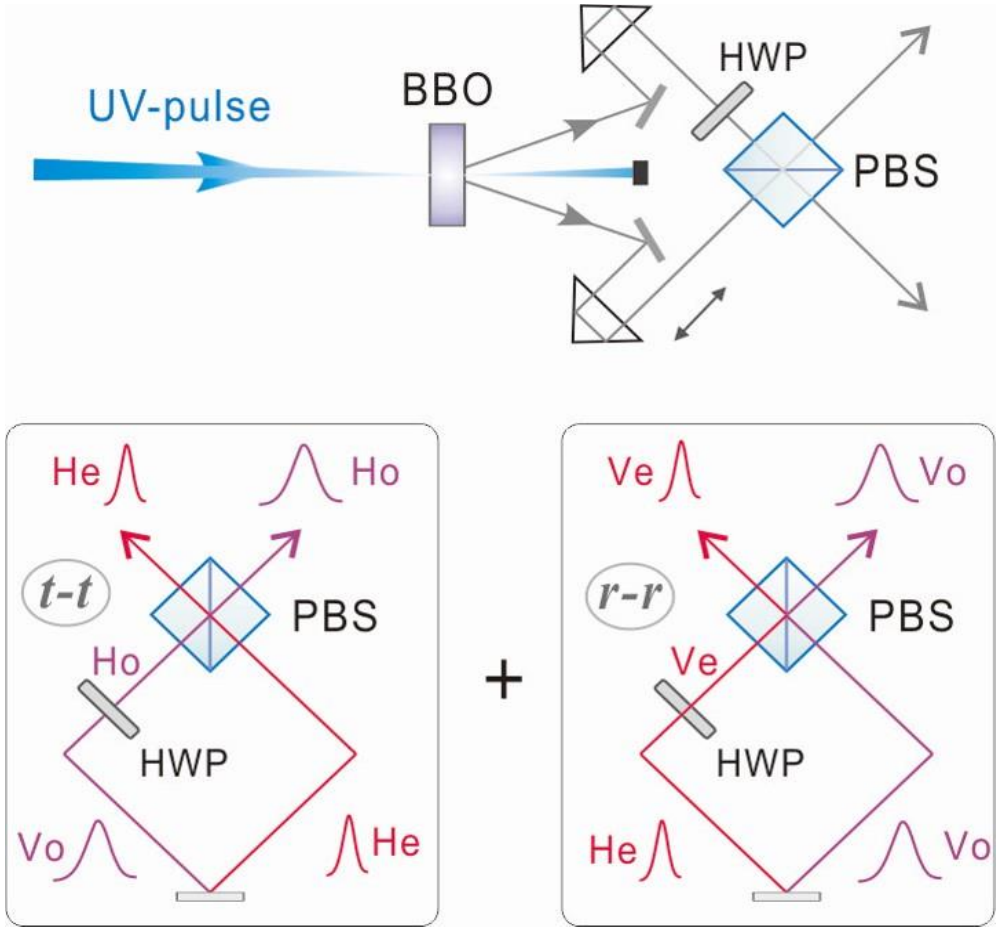
Frequency-uncorrelated Entangled Photons



$|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B$

- The o and e light differs in their spectral (and temporal) widths ➡ decrease the indistinguishability thus the fidelity
- Previous experiments: narrow-band filters (~3nm) ➡ unnecessary waste of photons

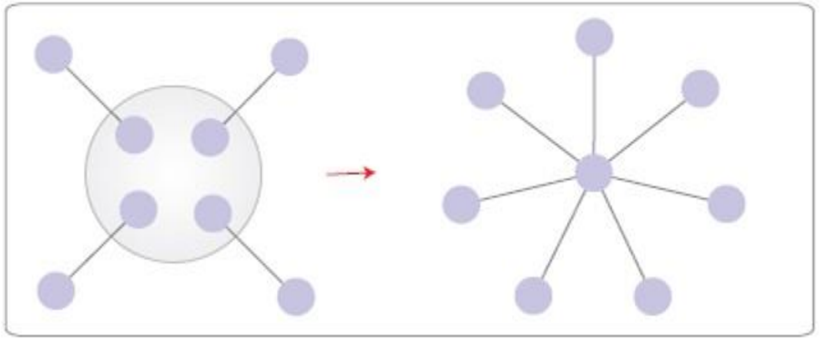
Frequency-uncorrelated Entangled Photons



☑ ~1 million coincidence counts per second without filter, with ~90% fidelity

Eight-Photon Entanglement

- Fidelity: 0.708
- Brightness: 9 counts per hour

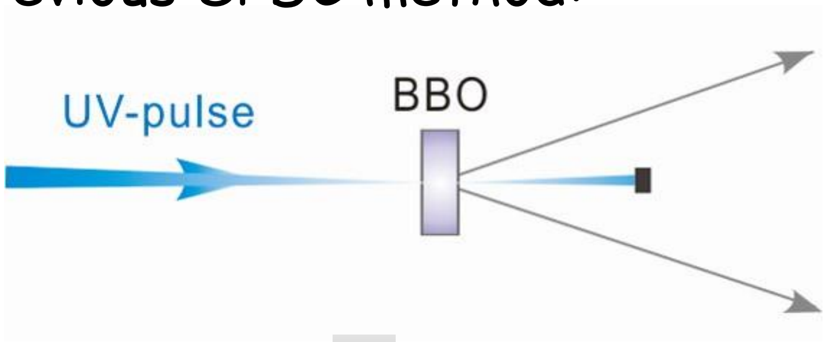


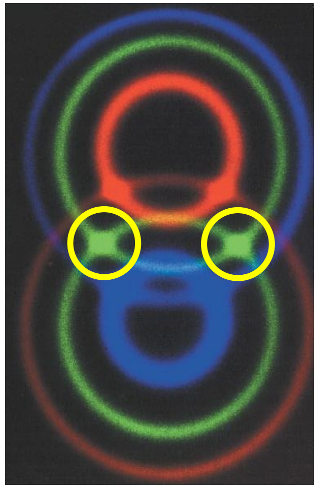
Interferometric Bell-state synthesizer: disentangles the timing from the polarization

Yao *et al.*, Nature Photonics 6, 225 (2012)

Ten-Photon Entanglement

Previous SPDC method:

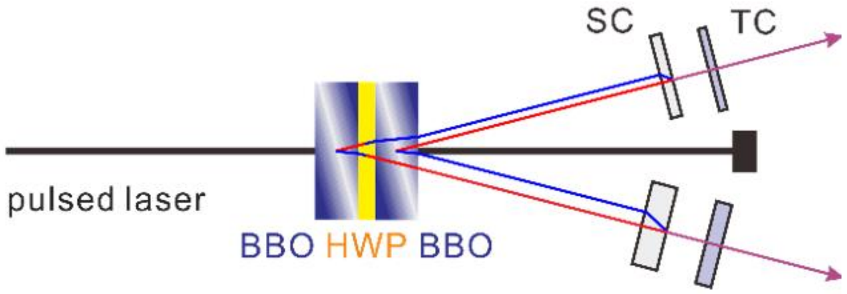


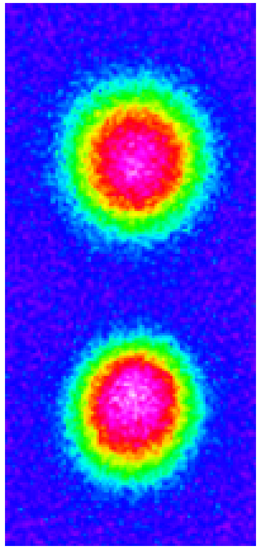


BBO->BiBO
Chen *et al.*, Optica 4 (1), 77-83

☒ Only collect photons from overlaps of up and down circles

To increase count rate:





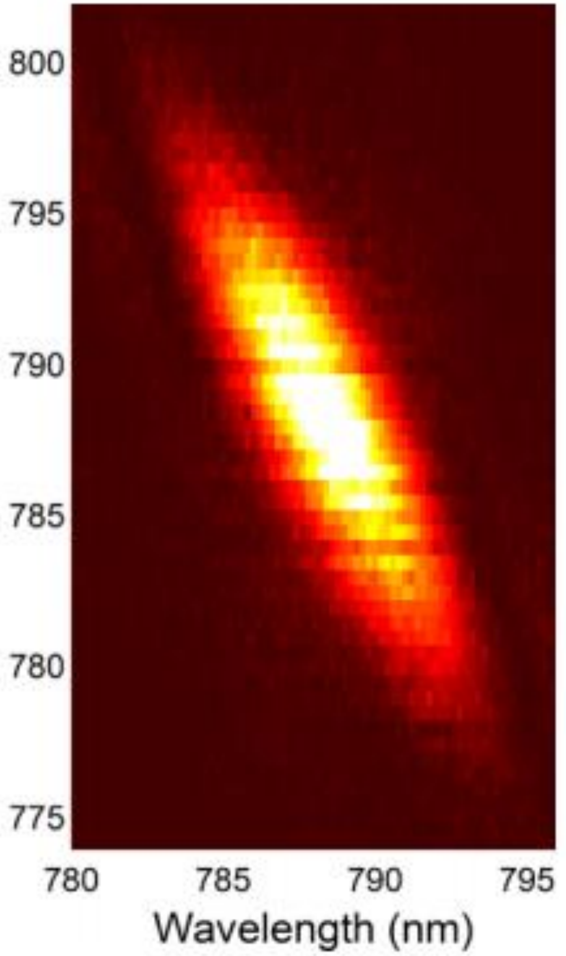
☑ Collect all photons from two separate circular beams

entangled-photon source ~4 times brighter than the previous result in eight-photon entanglement

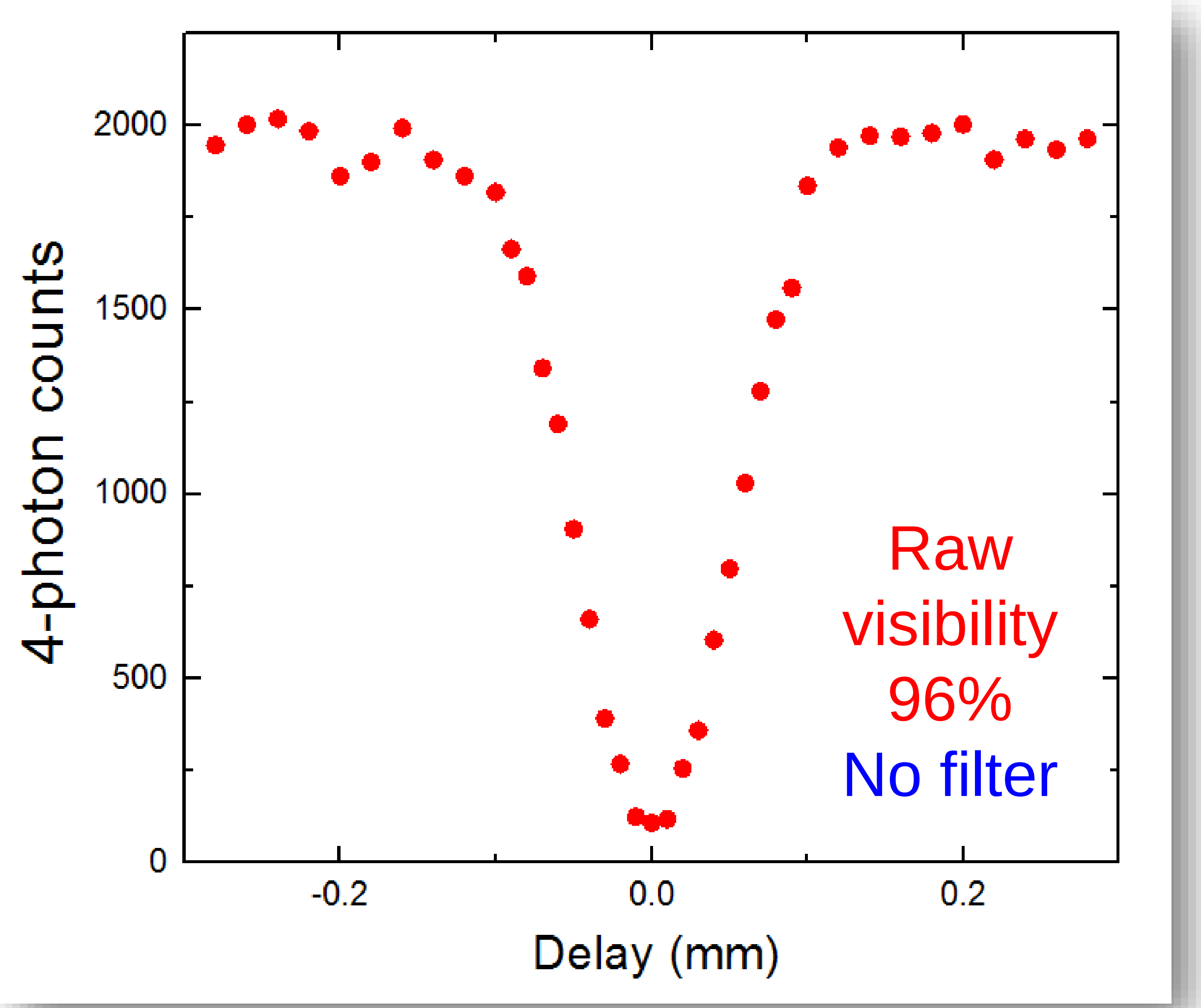
Wang *et al.*, PRL 117, 210502 (2016)

An optimal SPDC entangled photon source

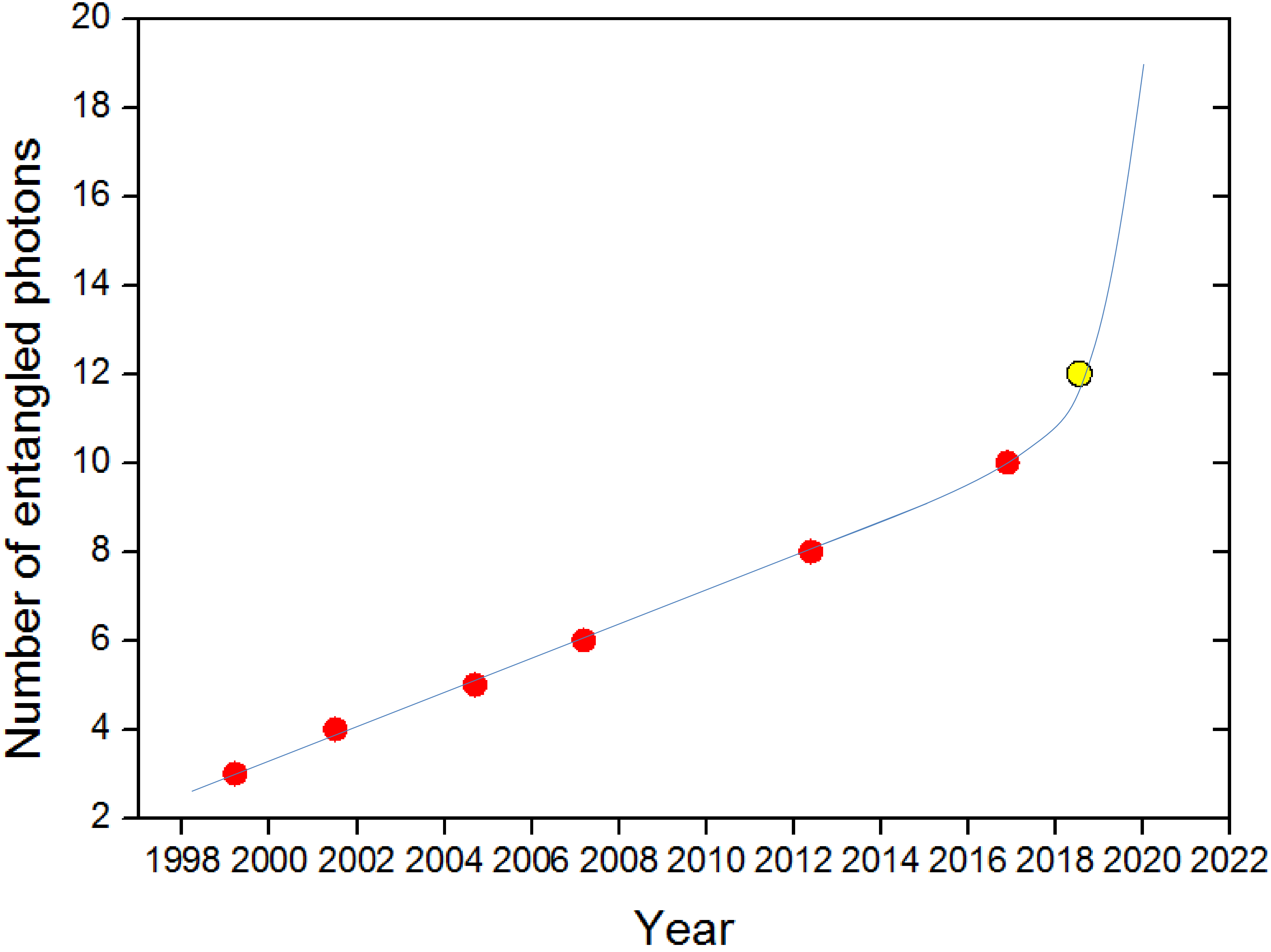
10-photon entanglement,
Wang et al. *Phys. Rev. Lett.* (2016)



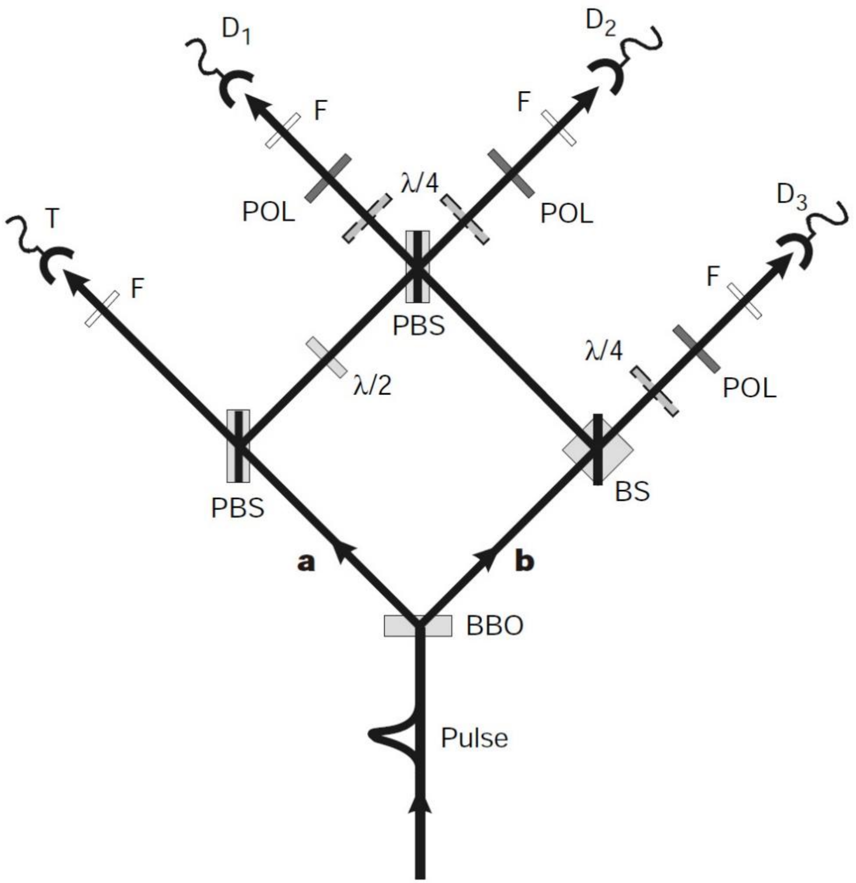
12-photon entanglement,
Zhong et al. *Phys. Rev. Lett.* (2018)

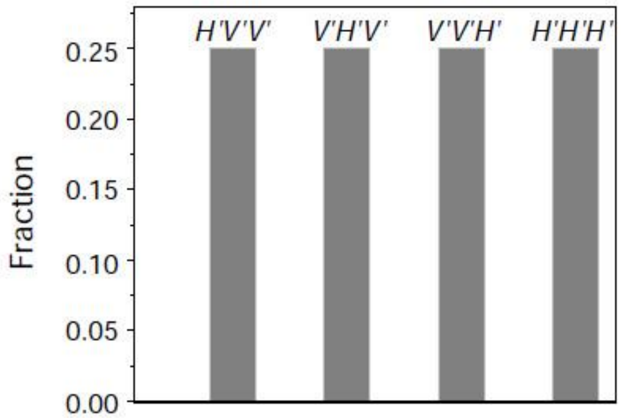


Multi-Photon Entanglement

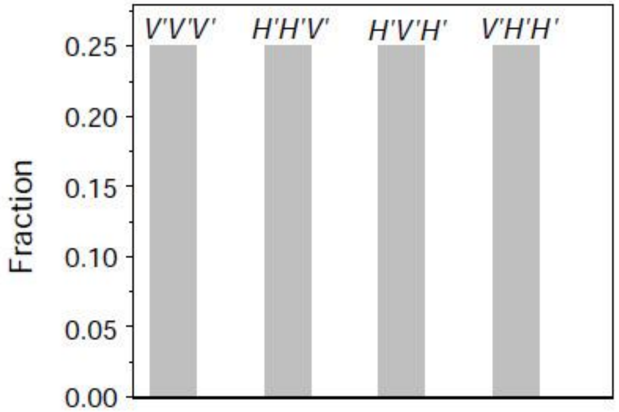


Test of Quantum Nonlocality in 3-photon GHZ entanglement

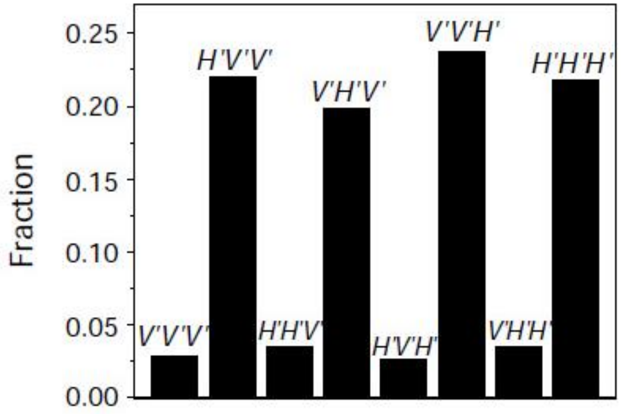




Prediction for quantum mechanics



Prediction for local realism

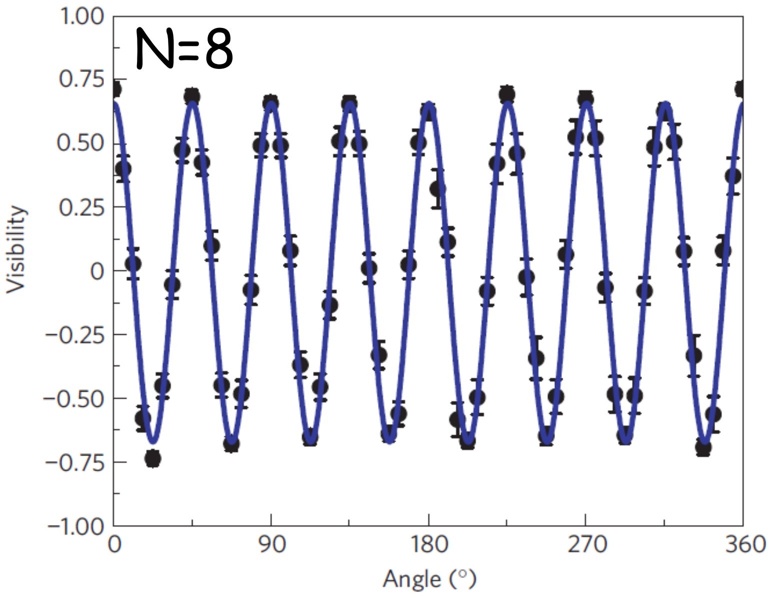


Experimental result

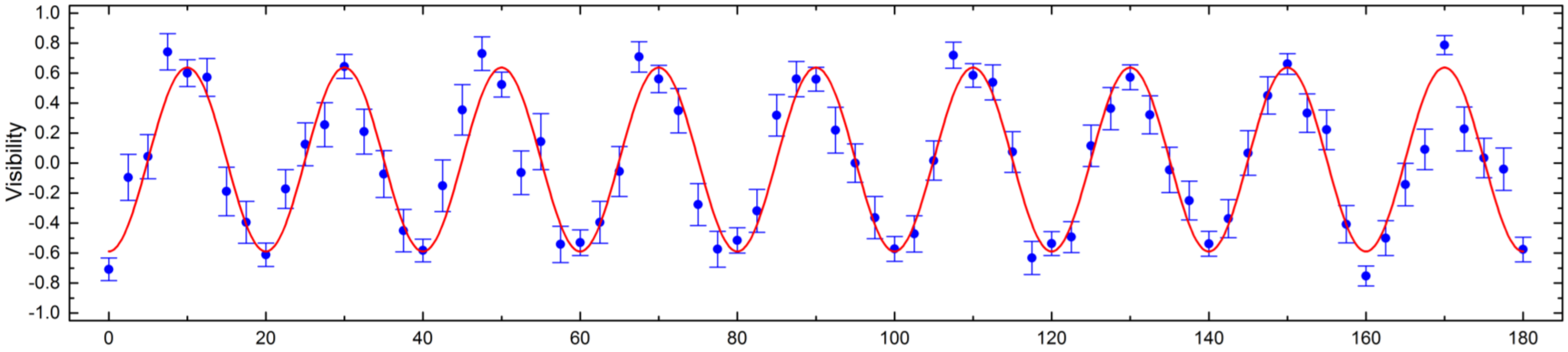
Pan *et al.*, Nature 403, 515 (2000)

Super-resolution with Multi-photon Entanglement

$$|\psi\rangle = |\underbrace{00\ldots0}_{N}\rangle + e^{iN\phi}|\underbrace{11\ldots1}_{N}\rangle$$



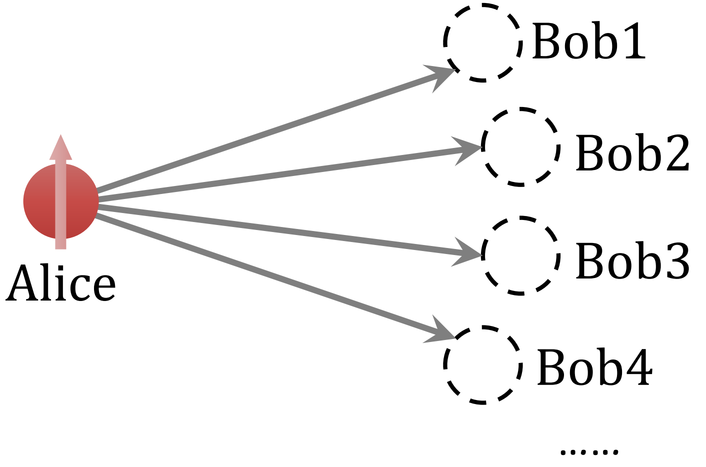
- Walther *et al.*, Nature 429, 158 (2004), N=4
- Nagata *et al.*, Science 316, 726 (2007), N=4
- Resch *et al.*, PRL 98, 223601 (2007), N=6
- Gao *et al.*, Nature Physics 6, 331 (2010), N=8



- Wang *et al.*, PRL (2018), N=18

Quantum Teleportation with Multi-photon Entanglement

- Open-destination teleportation
  Zhao *et al.*, Nature 430, 54 (2004)



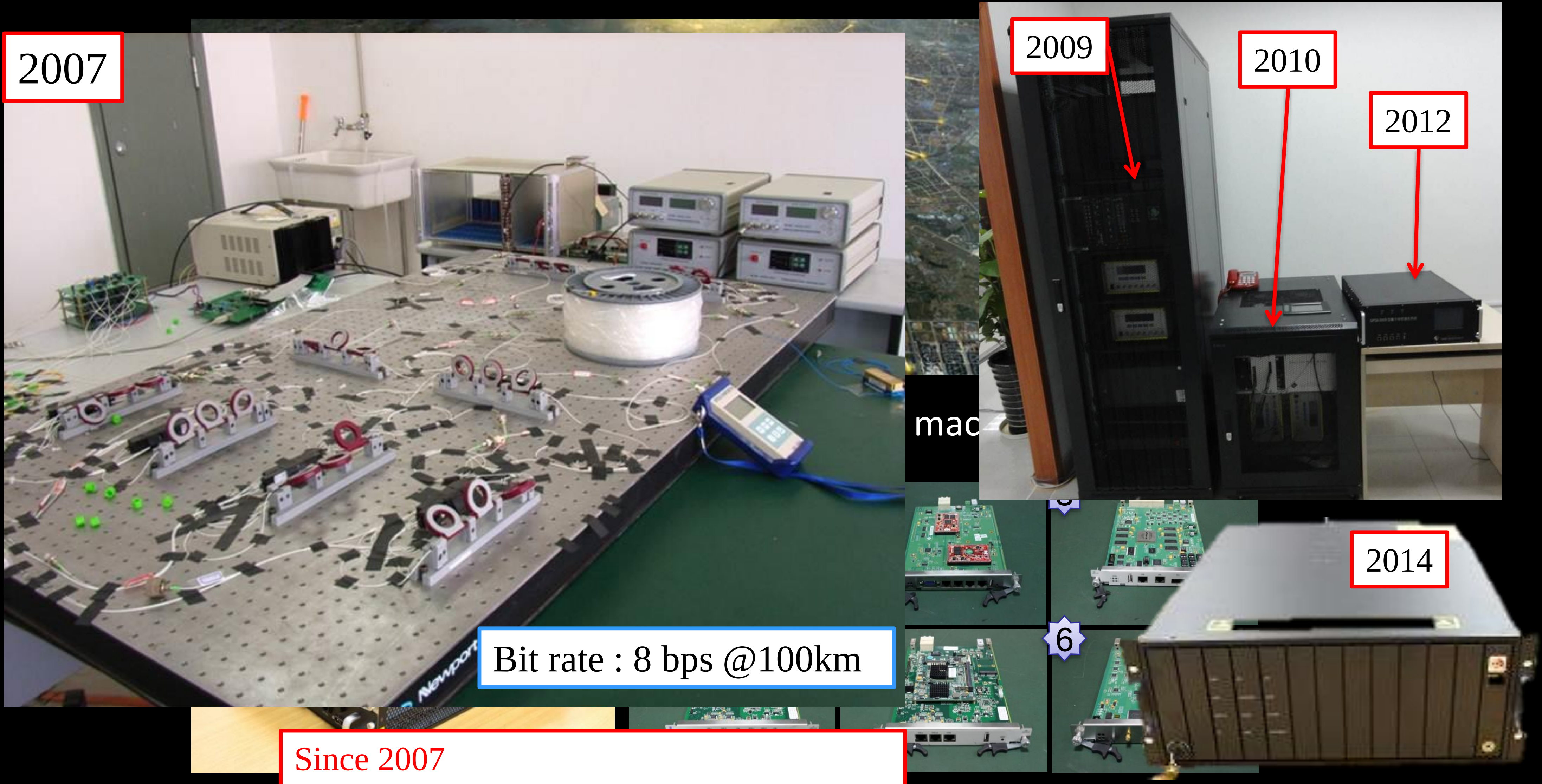
- Teleportation of a composite system
  Zhang *et al.*, Nature Physics 2, 678 (2006)

- Teleportation of multiple degrees of freedom
  Wang *et al.*, Nature 516, 518 (2015)

Quantum network → Essential element in quantum computation

Part 3: Practical Quantum Communication Network

Practical Metropolitan QKD Networks



Bit rate : 8 bps @100km

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

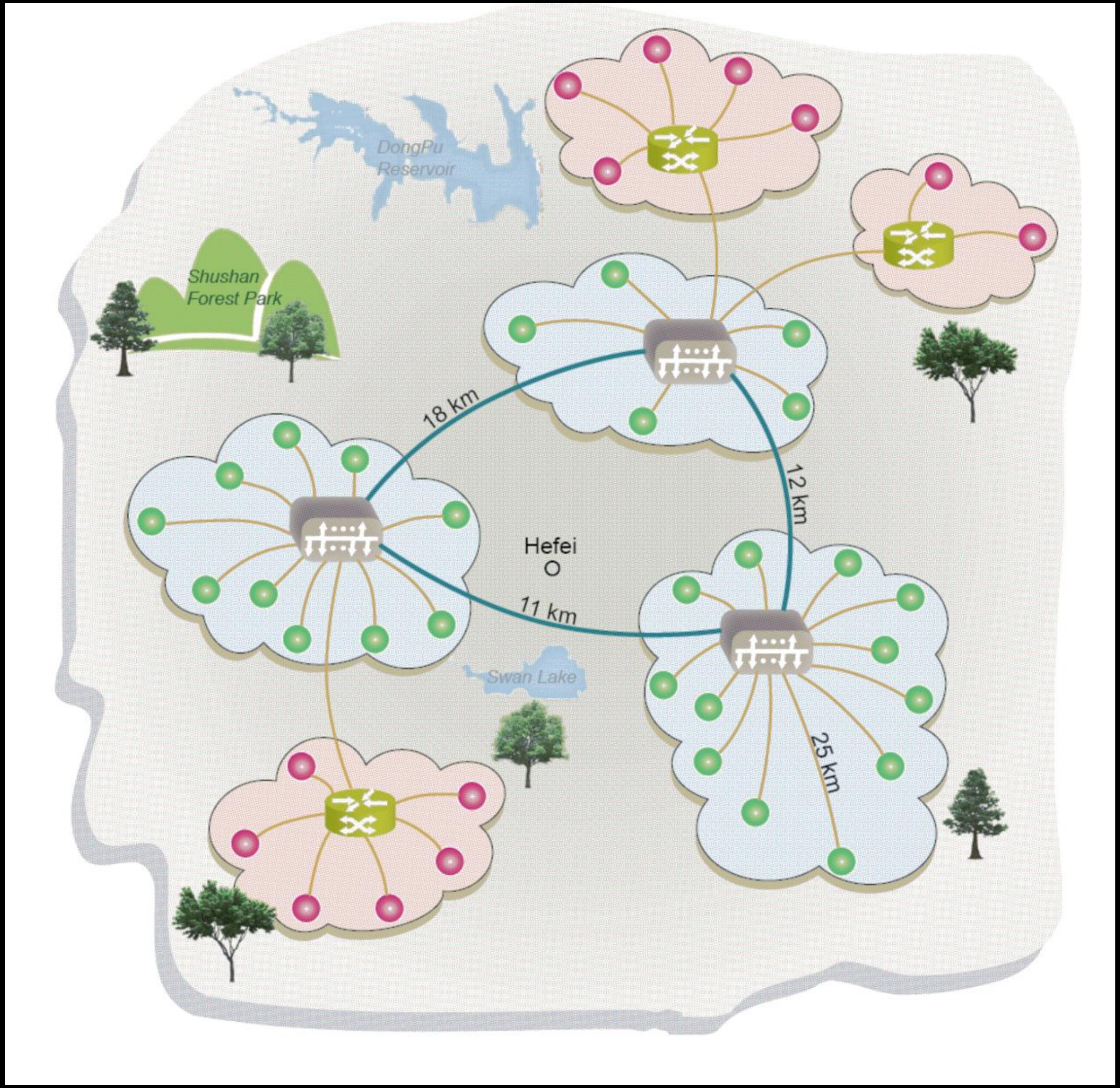
In combination with classical symmetric encryption:

- ☑ 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

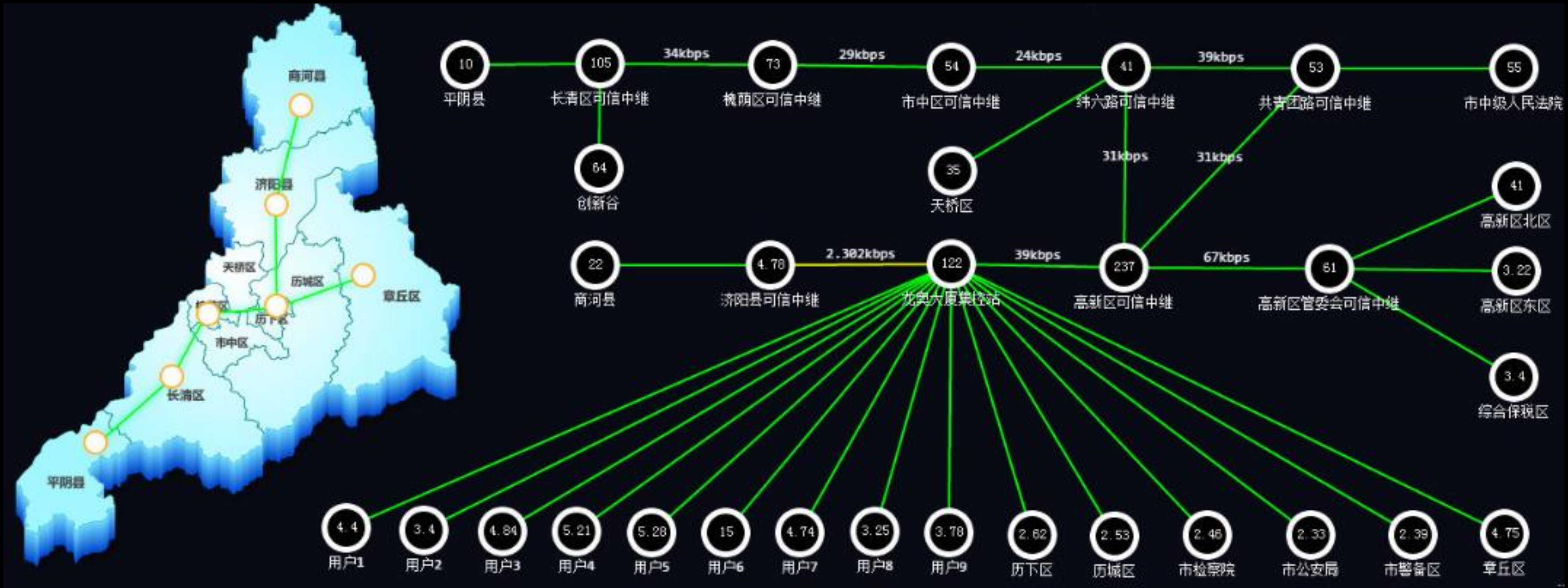


- Three level of users
  - Relay Station
  - VIP users (red spot)
  - General end users (green spot)

- Three type topology
  - Circle
  - Star
  - Tree

46 Nodes Hefei

Practical Metropolitan QKD Networks



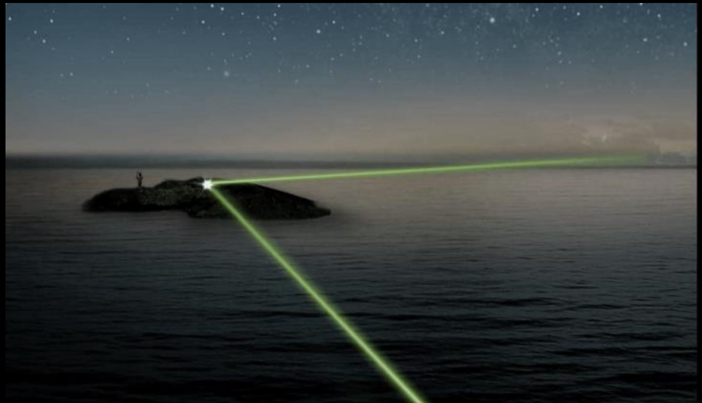
Jian Government private QKD network **Operated at Aug. 2017**

- Cover the whole Jinan City, Private QKD network for government offices, Providing quantum encrypted audio call and data transfer.
- 32 nodes and 242 users, total length 500 km.
- Channel loss≤13 dB, secure key rate >2.5 kbps; Channel loss ≤25 dB, secure key rate >1 kbps

Challenge towards Scalable Quantum Communications

- Longest distance of point-to-point MDI-QKD in fiber: ~400km

  Yin *et al.*, PRL 117, 190501 (2016); Boaron et al., Phys. Rev. Lett. 121, 190502 (2018)
- 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

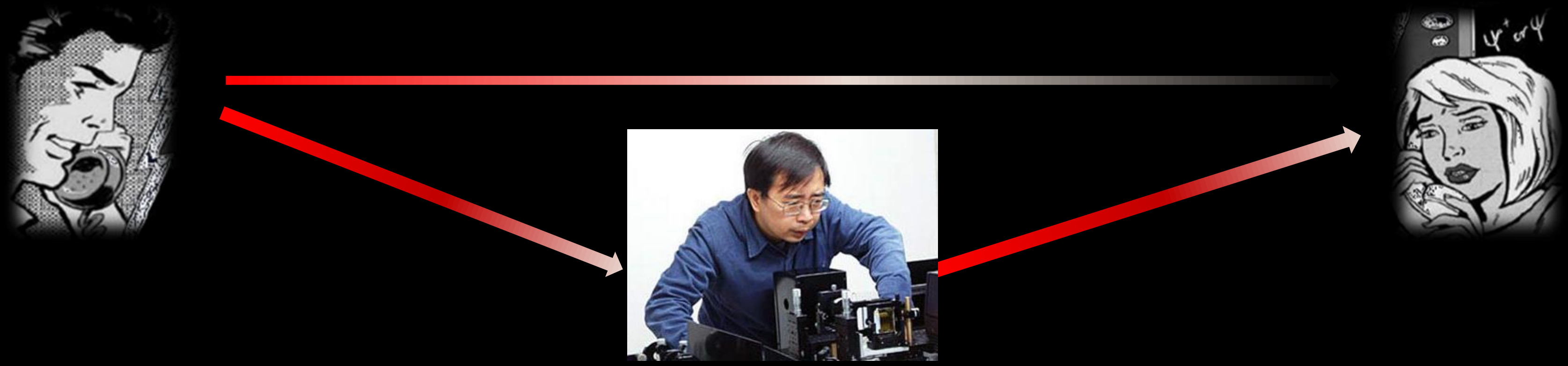
Inevitable huge photon loss in fiber and terrestrial free space channel

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!**

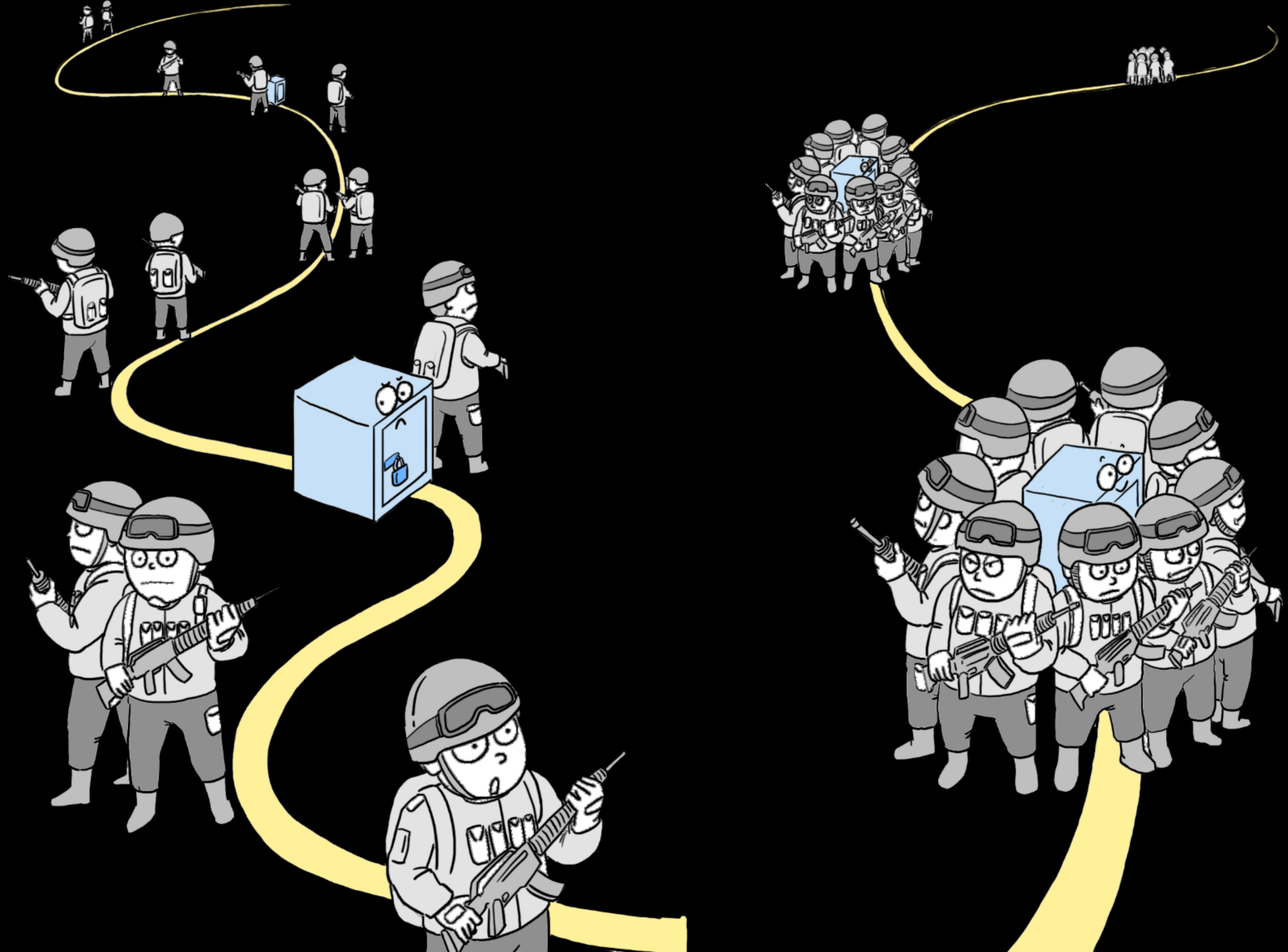
There are two main paths: **quantum repeaters** and **satellite-based.**

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

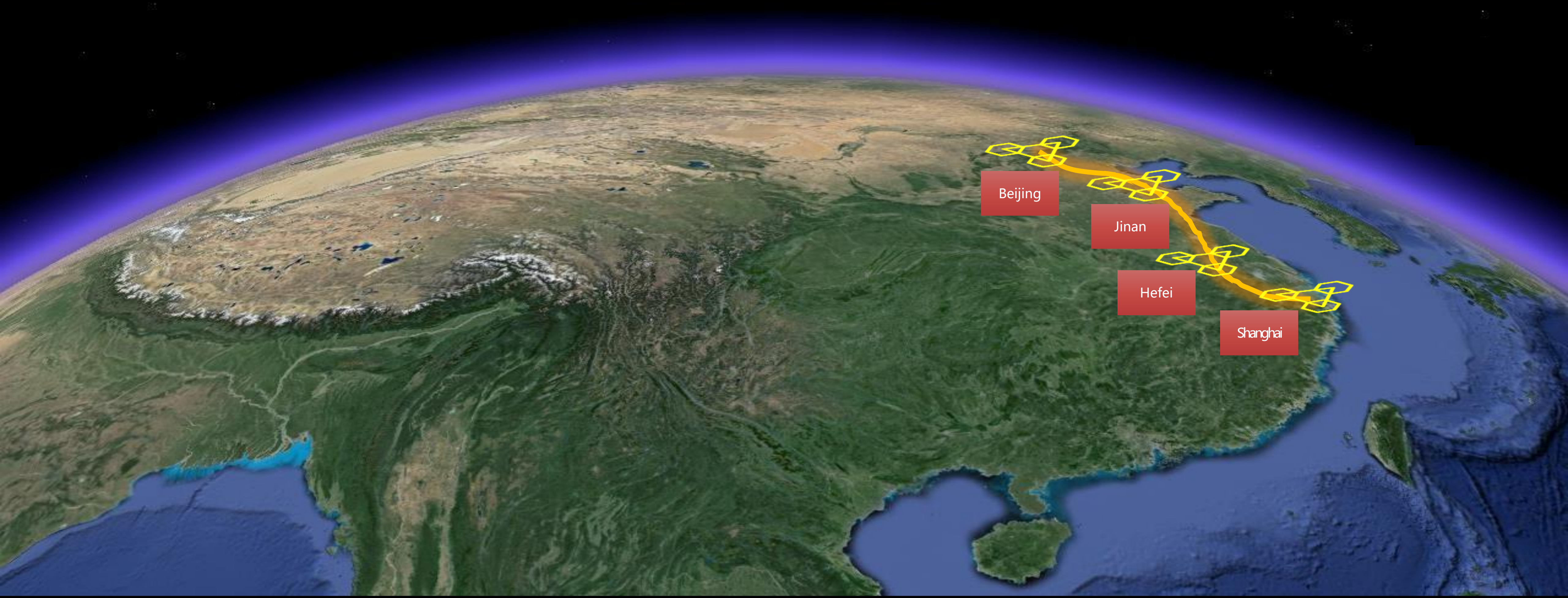
Trustable Relay Approach
- Classical Repeater



	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}

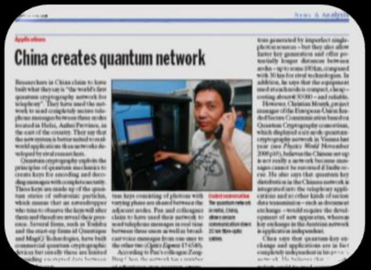


Quantum Secure Backbone (Trustable Relay)



2006

- Secure distance exceed 100km with Decoy BB84

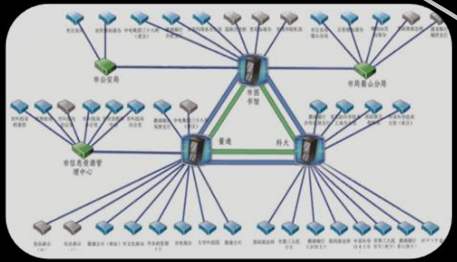

China creates quantum network

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)

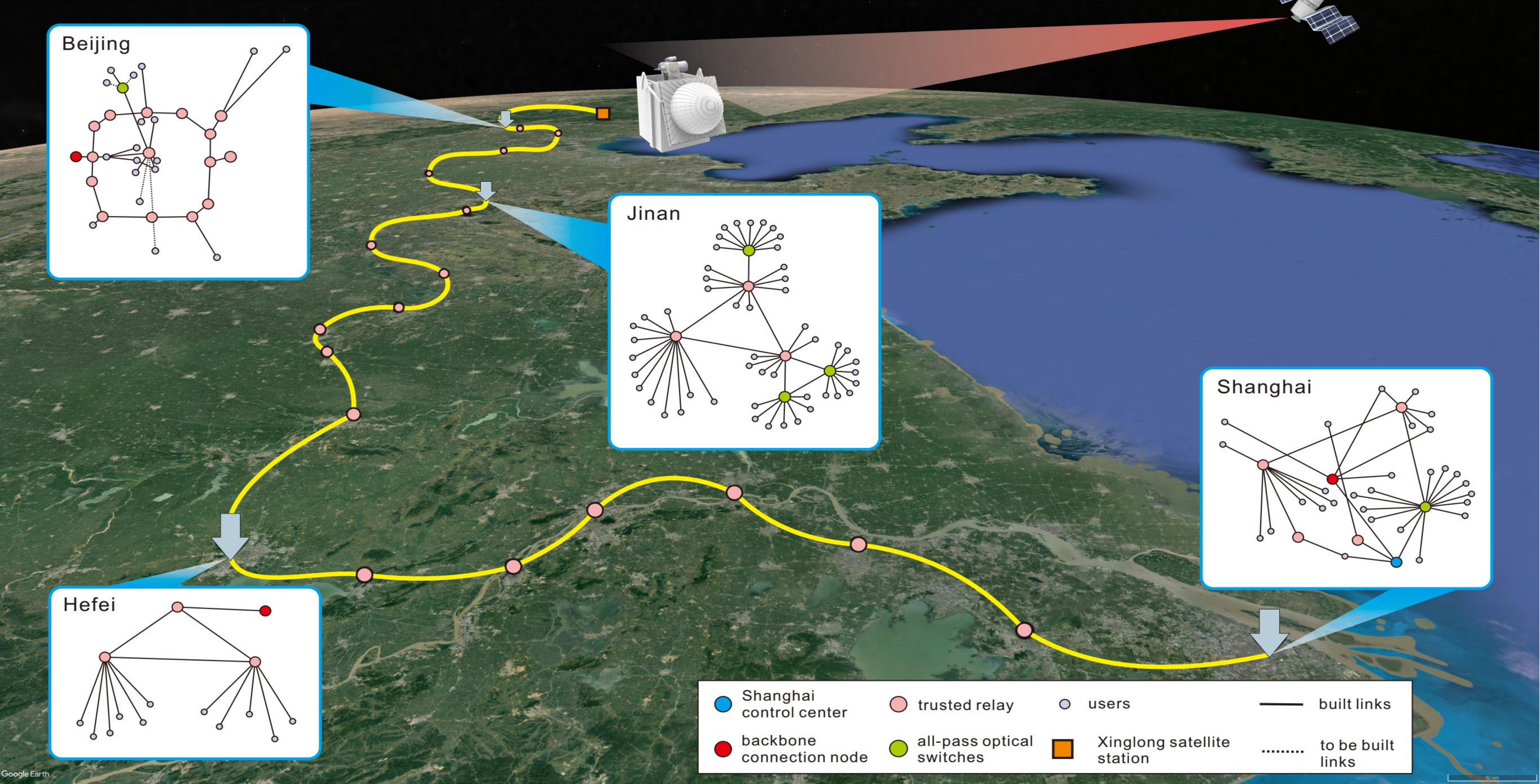
2014

- 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

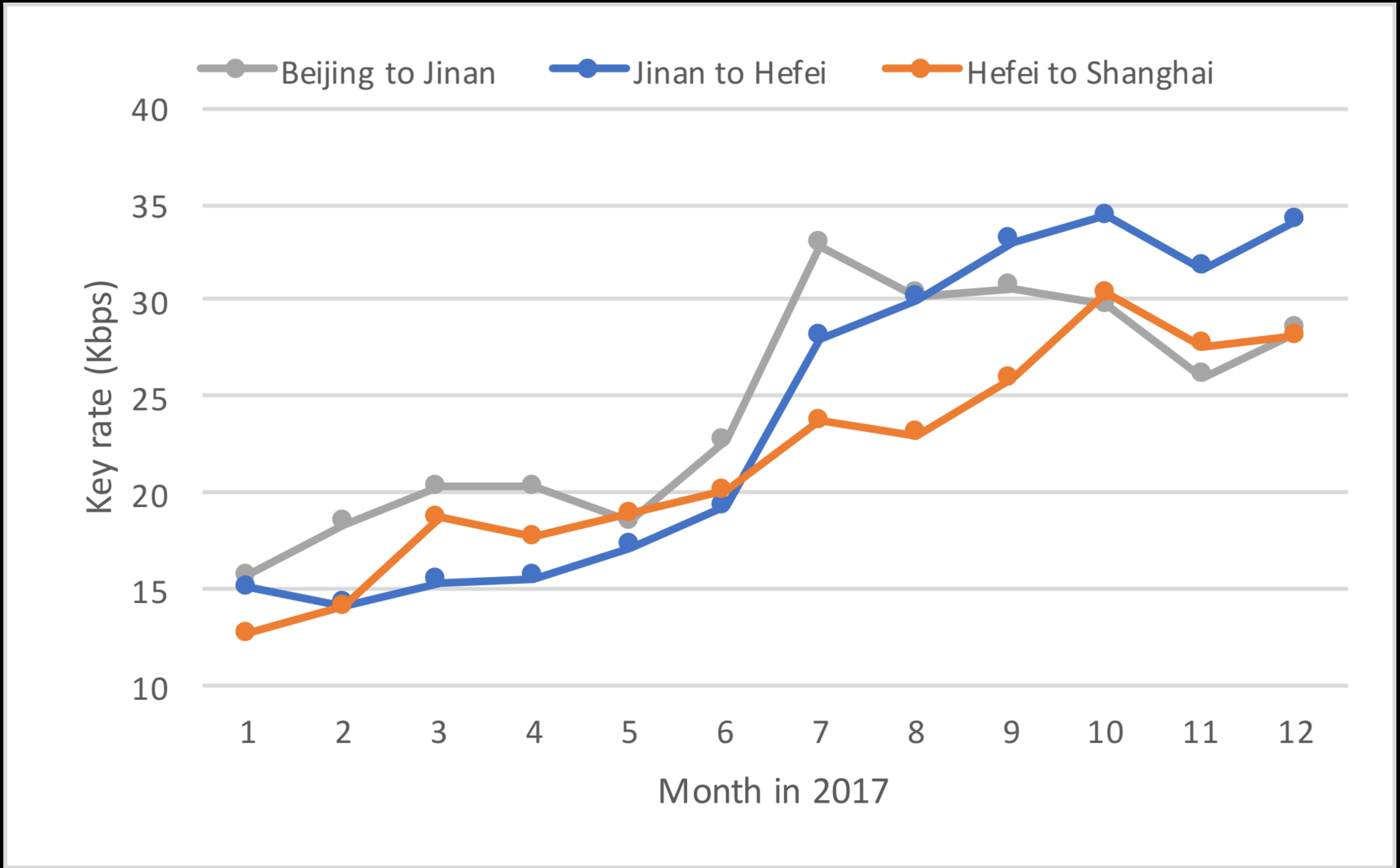
Deployment


量子保密通信上海控制中心
Shanghai Master Control Center for Quantum Secure Communications
中国科学技术大学


南山观测站
京沪干线济南中心
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
东方证券
民生银行
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
上海国盾量子公司
中科大上海研究院
量子总控中心
崇明
宝山
杨浦
静安
普陀
长宁
徐汇
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）
通州区
华夏银行
北京农商银行
大兴区

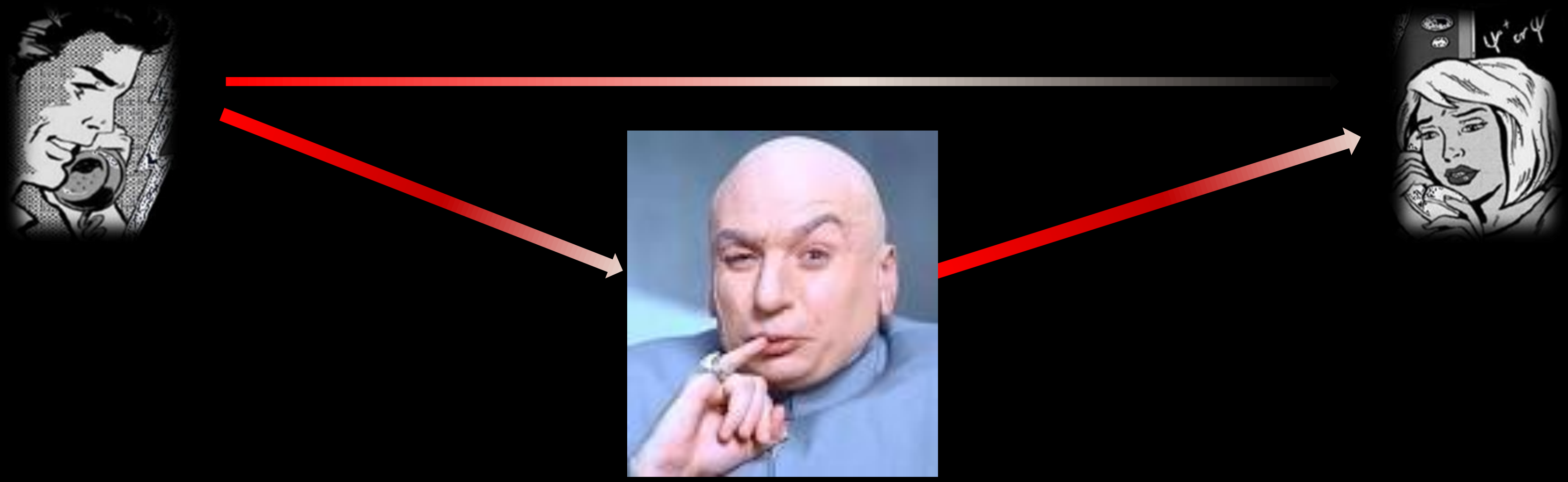


Beijing to Jinan
Jinan to Hefei
Hefei to Shanghai
Key rate (Kbps)
40
35
30
25
20
15
10
1
2
3
4
5
6
7
8
9
10
11
12
Month in 2017

Applications: Industrial and Commercial Bank of China

Part 4: Demonstrations of Quantum Repeaters

Quantum Repeater



Challenge towards Scalable Quantum Information Processing

As mentioned in Lecture 1, we need quantum repeater to overcome

☒ Absorption ➡ Photon loss

☒ Decoherence ➡ Degrading entanglement quality

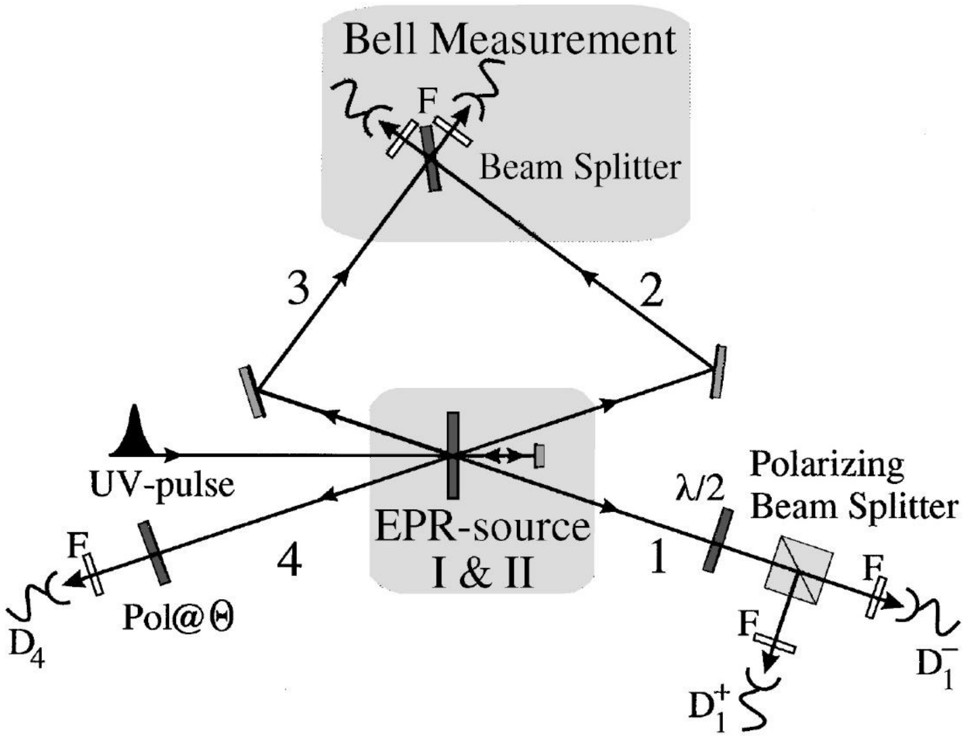
And

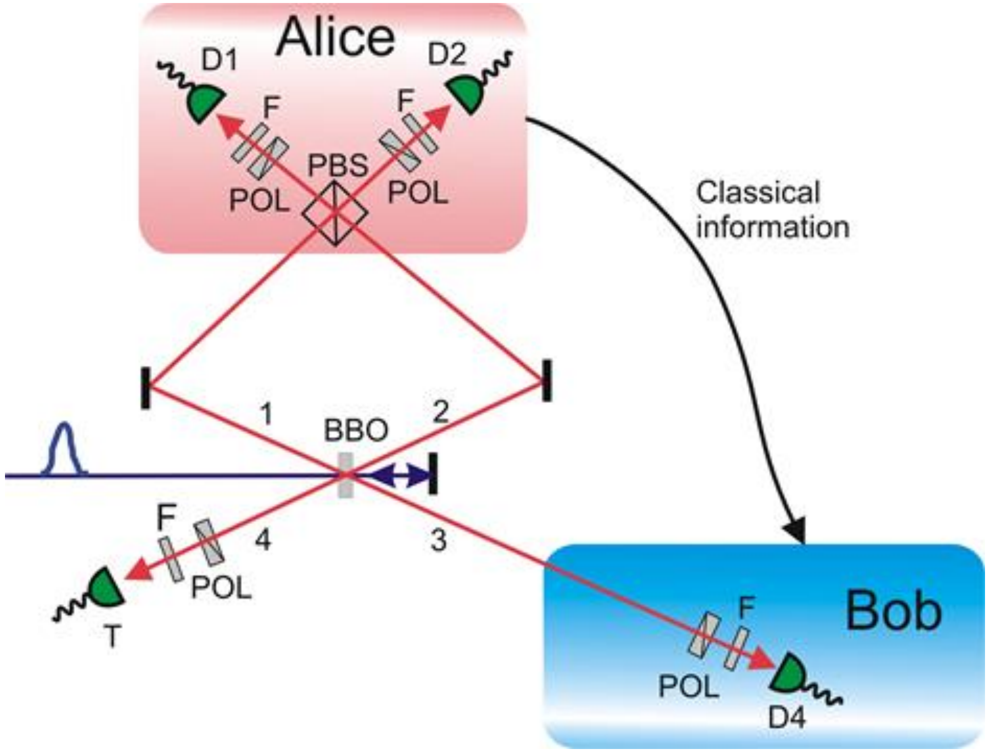
☒ Probabilistic entangled photons and single photon source ➡ Exponential resource cost

Require

- Entanglement swapping with high precision
- Entanglement purification with high precision
- Quantum memory with high performance

High Precision Entanglement Swapping





First demonstration with beam splitter

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

High precision fault-tolerable entanglement swapping

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

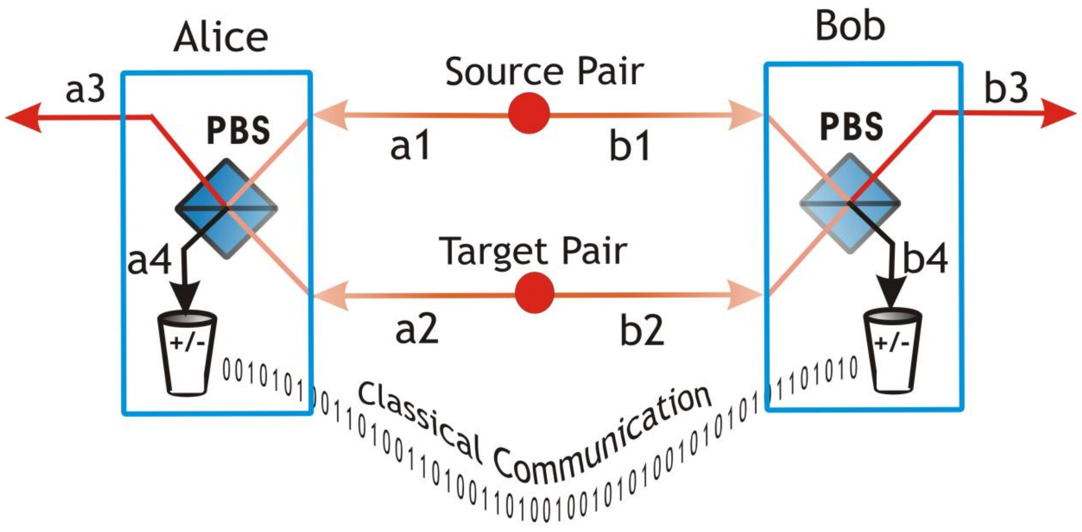
Practical Scheme for Entanglement Purification

☒ Original entanglement purification scheme requires CNOT operation between independent photons

☑ Practical scheme: non-linearity effectively induced by post-selection

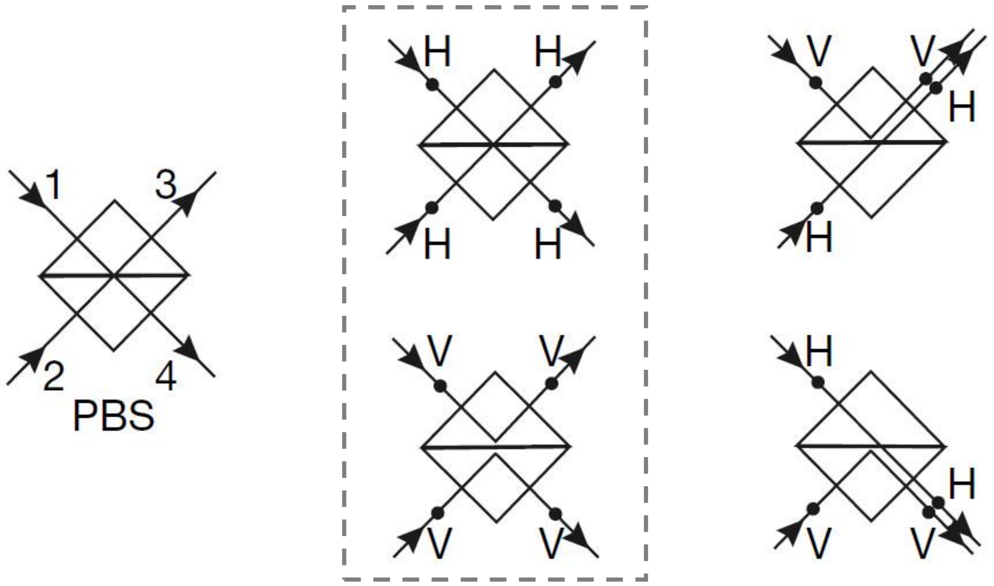
Pan *et al.*, Nature 410, 1067 (2001)

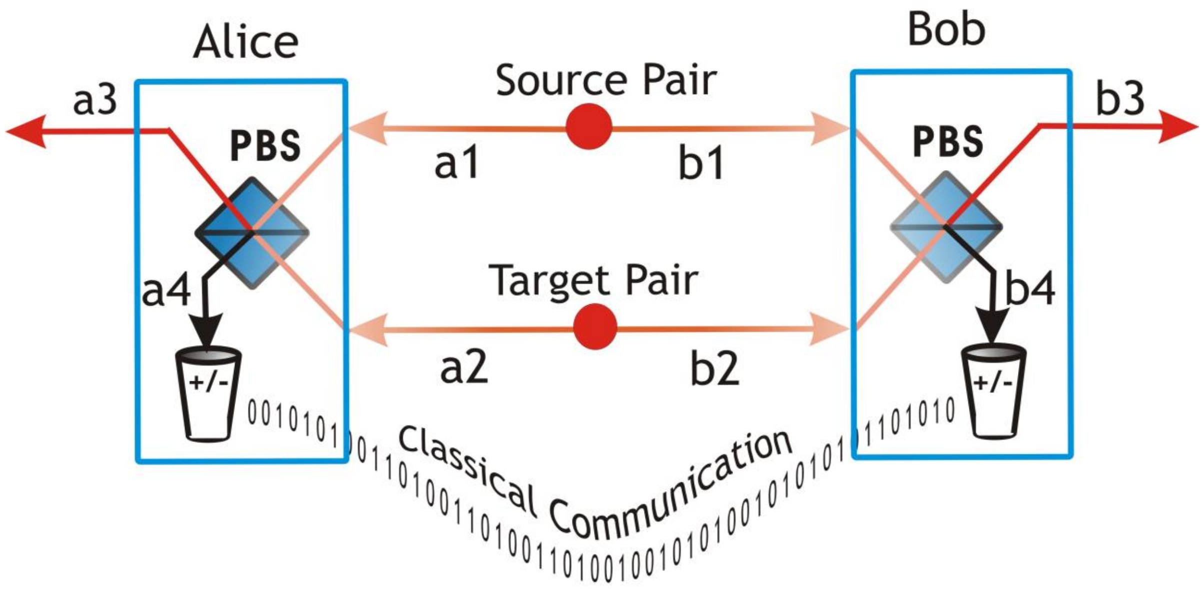
Consider a simpler case: to purify $M = F|\Phi^+\rangle\langle\Phi^+| + (1-F)|\Psi^+\rangle\langle\Psi^+|$



Keep 4-fold coincidence at a3, b3, a4, b4

Practical Scheme for Entanglement Purification





4-fold coincidence after PBS

Probability	F^2	$(1-F)^2$	$\cancel{F(1-F)}$	$\cancel{F(1-F)}$
Case	$\lvert\Phi^+\rangle_{a1b1}\lvert\Phi^+\rangle_{a2b2}$	$\lvert\Psi^+\rangle_{a1b1}\lvert\Psi^+\rangle_{a2b2}$	$\cancel{\lvert\Phi^+\rangle_{a1b1}\lvert\Psi^+\rangle_{a2b2}}$	$\cancel{\lvert\Psi^+\rangle_{a1b1}\lvert\Phi^+\rangle_{a2b2}}$

These two cases will not result in 4-fold coincidence

Practical Scheme for Entanglement Purification

- For $|\Phi^+\rangle_{a1b1}|\Phi^+\rangle_{a2b2} = \frac{1}{2}(|H\rangle_{a1}|H\rangle_{b1} + |V\rangle_{a1}|V\rangle_{b1})(|H\rangle_{a2}|H\rangle_{b2} + |V\rangle_{a2}|V\rangle_{b2})$

Four-fold events	No four-fold events
$H_{a1}H_{a2}H_{b1}H_{b2}$	$H_{a1}V_{a2}H_{b1}V_{b2}$
$V_{a1}V_{a2}V_{b1}V_{b2}$	$V_{a1}H_{a2}V_{b1}H_{b2}$

Probability of 50%

$$\frac{1}{\sqrt{2}}(|H\rangle_{a3}|H\rangle_{a4}|H\rangle_{b3}|H\rangle_{b4} + |V\rangle_{a3}|V\rangle_{a4}|V\rangle_{b3}|V\rangle_{b4})$$

- After local measurements in {+/-} base at a4 and b4:

Probability of $F^2/2$

$$|\Phi^+\rangle_{a3b3} = \frac{1}{\sqrt{2}}(|H\rangle_{a3}|H\rangle_{b3} + |H\rangle_{a3}|H\rangle_{b3})$$

Practical Scheme for Entanglement Purification

- For $|\Psi^+\rangle_{a1b1}|\Psi^+\rangle_{a2b2} = \frac{1}{2}(|H\rangle_{a1}|V\rangle_{b1} + |V\rangle_{a1}|H\rangle_{b1})(|H\rangle_{a2}|V\rangle_{b2} + |V\rangle_{a2}|H\rangle_{b2})$

Four-fold events	No four-fold events
$H_{a1}H_{a2}V_{b1}V_{b2}$	$H_{a1}V_{a2}V_{b1}H_{b2}$
$V_{a1}V_{a2}H_{b1}H_{b2}$	$V_{a1}H_{a2}H_{b1}V_{b2}$

Probability of 50%

$$\frac{1}{\sqrt{2}}(|H\rangle_{a3}|H\rangle_{a4}|V\rangle_{b3}|V\rangle_{b4} + |V\rangle_{a3}|V\rangle_{a4}|H\rangle_{b3}|H\rangle_{b4})$$

- After local measurements in {+/-} base at a4 and b4:

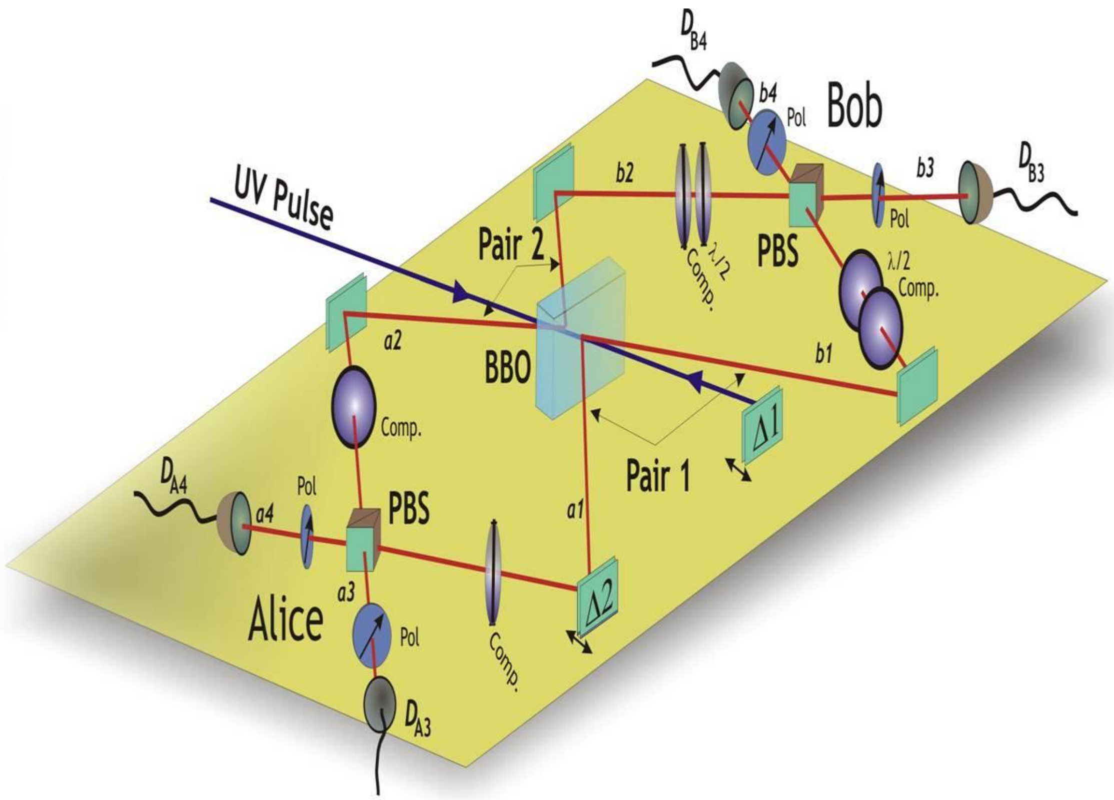
Probability of $(1\text{-}F)^2/2$

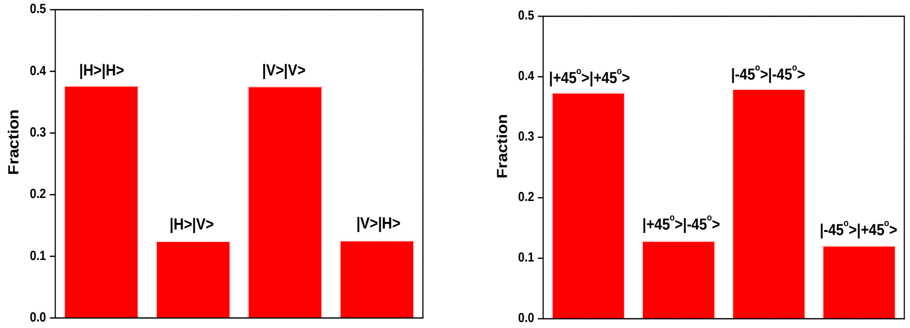
$$|\Psi^+\rangle_{a3b3} = \frac{1}{\sqrt{2}}(|H\rangle_{a3}|V\rangle_{b3} + |V\rangle_{a3}|H\rangle_{b3})$$

- Final state: $F'|\Phi^+\rangle\langle\Phi^+| + (1-F')|\Psi^+\rangle\langle\Psi^+|$

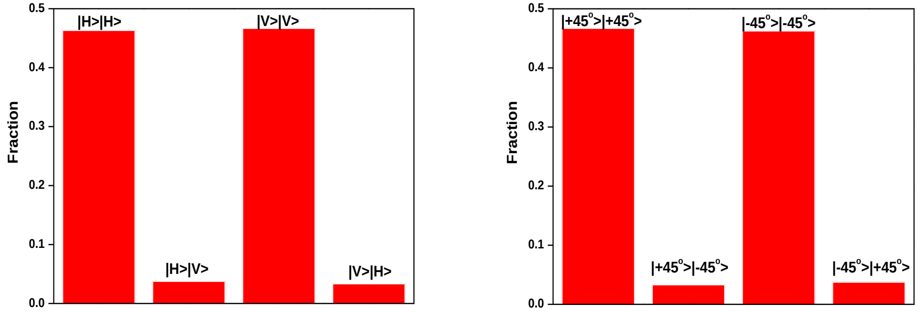
$$F' = \frac{F^2}{F^2 + (1-F)^2} > F \left(\text{if } F > \frac{1}{2}\right)$$

High Precision Entanglement Purification





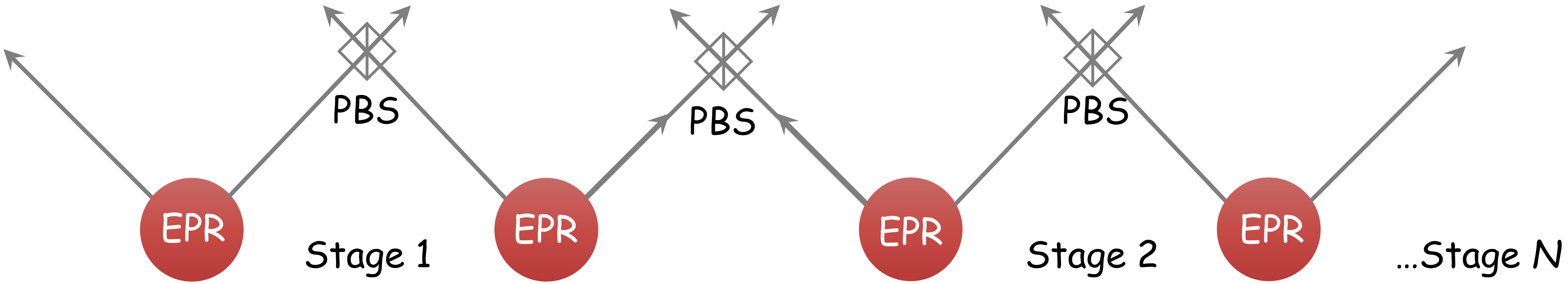
Before purification, F=3/4



After purification, F=13/14

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

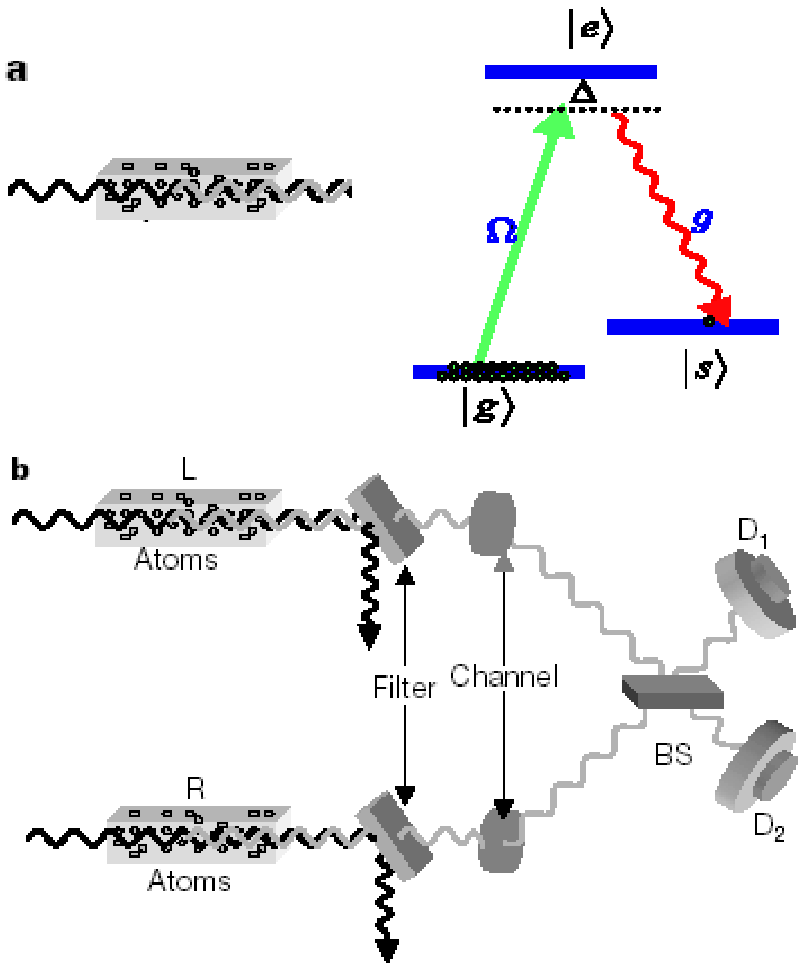
Quantum Memory



Probabilistic EPR source, Channel loss, Probabilistic entanglement purification

- ☒ Without quantum memory, the cost of resource in multi-stage experiments ~ $1/P^{2N}$, thus not scalable
- ☑ If we know when photon pair is created and can store them on demand, then implement entanglement purification and swapping, the total cost ~ $1/P^2$

Triggered and Storable Entanglement Generation



$$|\phi\rangle = |0_a\rangle\big|0_p\big\rangle + \sqrt{p_c}S^\dagger a^\dagger|0_a\rangle\big|0_p\big\rangle + o(p_c)$$

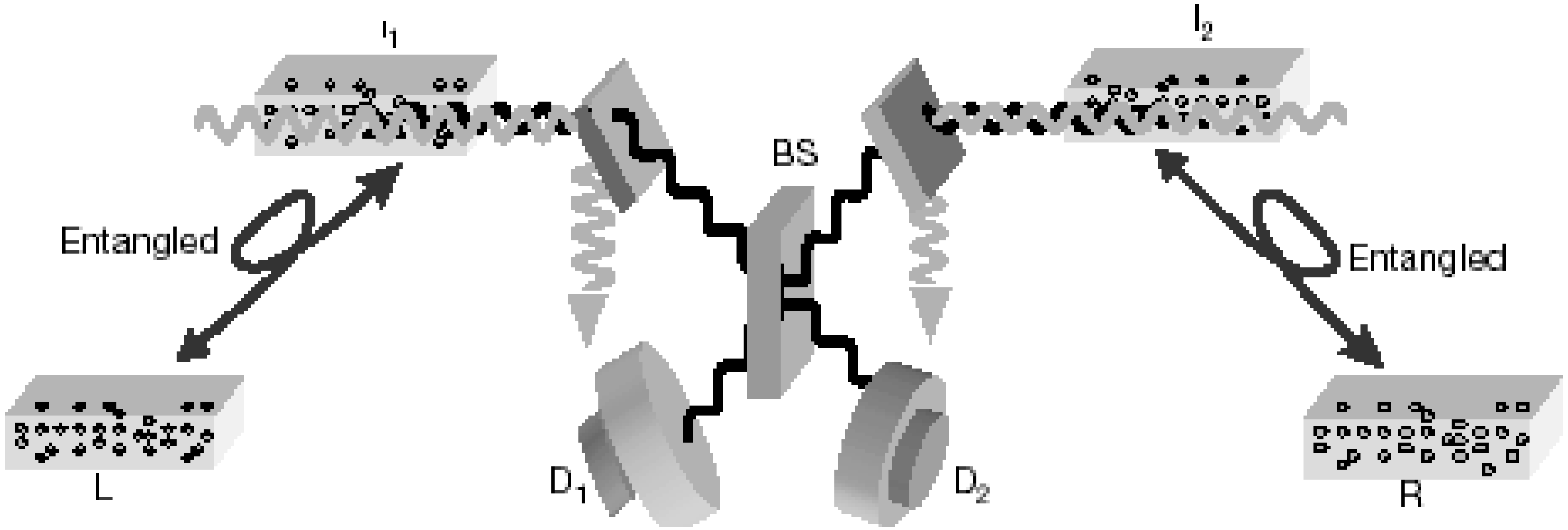
$$\begin{aligned}|\psi\rangle_{LR} &= \big\langle 0_p 0_p\big|(a_L \pm a_R)|\phi\rangle|\phi\rangle \\ &= (h_L^\dagger \pm h_R^\dagger)|0_a 0_a\rangle_{LR} \\ &= |0_a 1_a\rangle_{LR} \pm |1_a 0_a\rangle_{LR}\end{aligned}$$

DLCZ scheme

Duan *et al.*, Nature 414, 413 (2001)

Maximally entangled in the number basis

Entanglement Connection



- Apply a reverse laser pulse to transfer atomic excitation back to optical excitation
- Succeeds if D1 or D2 registers a single photon

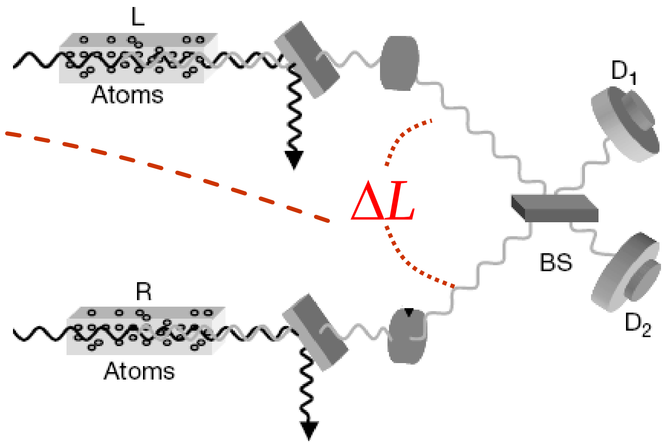
$$(h_L^+ + h_I^+)(h_{I'}^+ + h_R^+)|0000\rangle \rightarrow |\psi\rangle_{LR} = (h_L^+ + h_R^+)|00\rangle$$

- Fails otherwise, and repeat every step from entanglement generation

Drawbacks in DLCZ Scheme

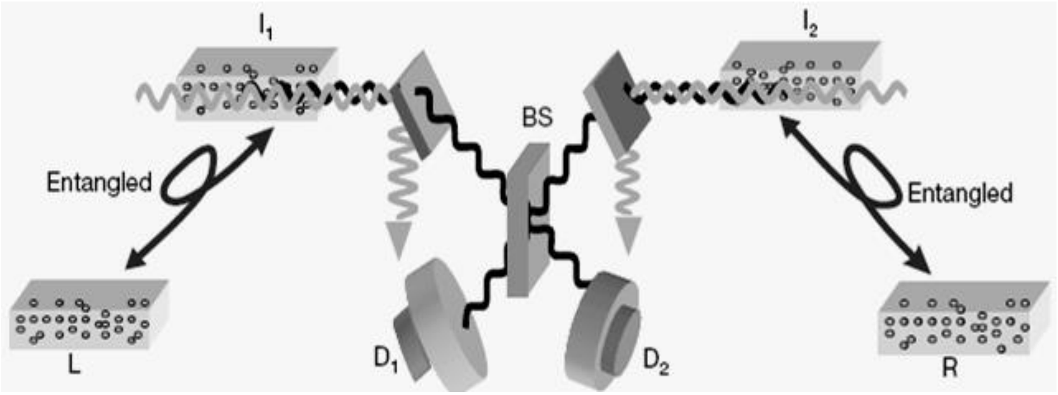
- Phase stabilization

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle_{LR} \pm e^{i\phi}|01\rangle_{RL}\right)$$



- Error rate grows rapidly with distance

  Vacuum term becomes dominant after a few connections



- Short Lifetime

  Achieved lifetime ~ 30 μs

  Preparation time ~ 100 μs → lifetime needed ~ 1 ms!

Deterministic Entanglement Generation

Solution:

- Phase stability:

  Sub-wavelength 100nm

  Sub-coherence length ~ 1m

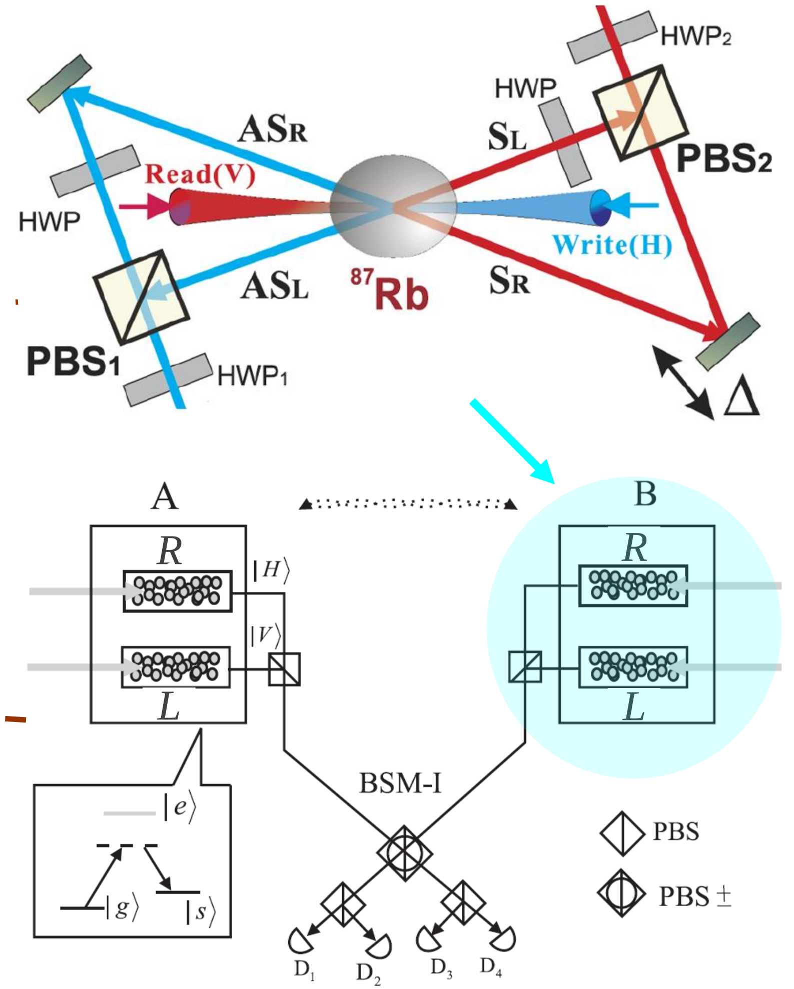
$$|\psi\rangle_{\mathrm{at-ph}} = \frac{1}{\sqrt{2}}\left(|R\rangle|H\rangle + e^{i\phi_1}|L\rangle|V\rangle\right)$$

$$|\psi\rangle_{\mathrm{ph-ph}} = \frac{1}{\sqrt{2}}e^{i\phi_2}\left(|H\rangle|H\rangle + |V\rangle|V\rangle\right)$$

- Lower error rate

  Vacuum term is NO more dominant

- Higher efficiency

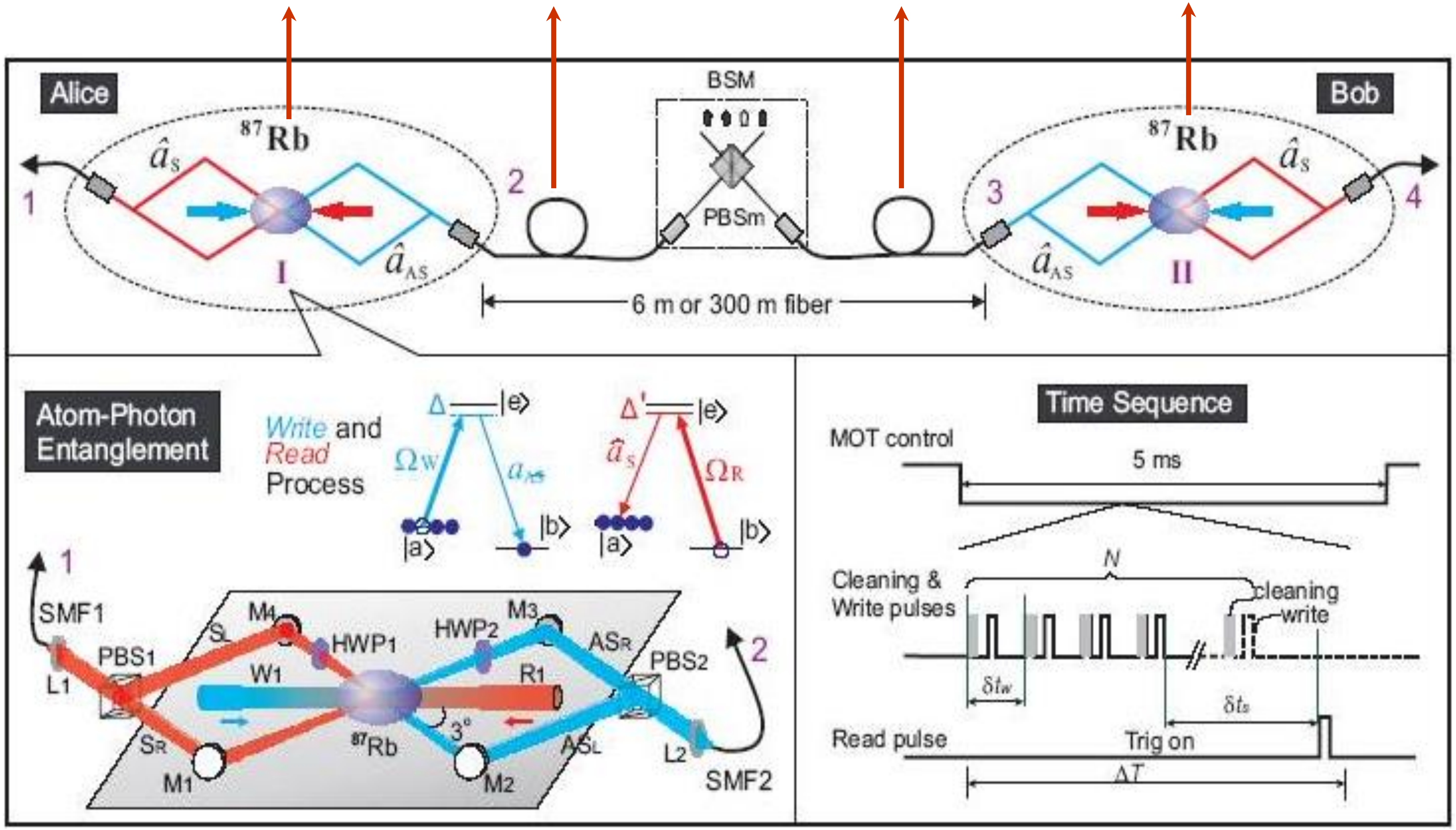


Zhao *et al.*, PRL 98, 240502 (2007)

Quantum Repeater Nodes

Atom-Photon entanglement

Atom-Photon entanglement



Experiment: Yuan *et al.*, Nature 454, 1098 (2008)

Efficient and Long-lived Quantum Memory

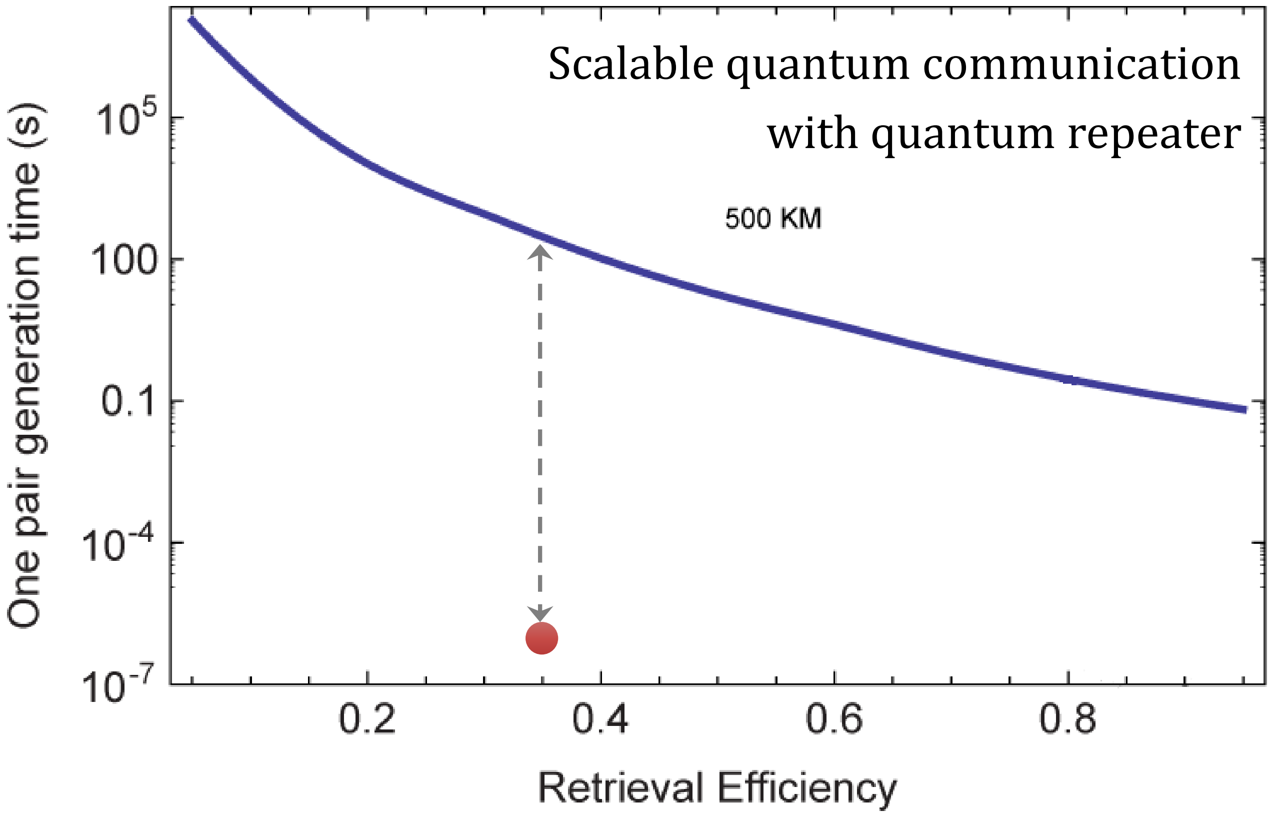
Long lifetime: storage time must be long enough to ensure every node creates an entangled pair

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

In 2008 experiment,

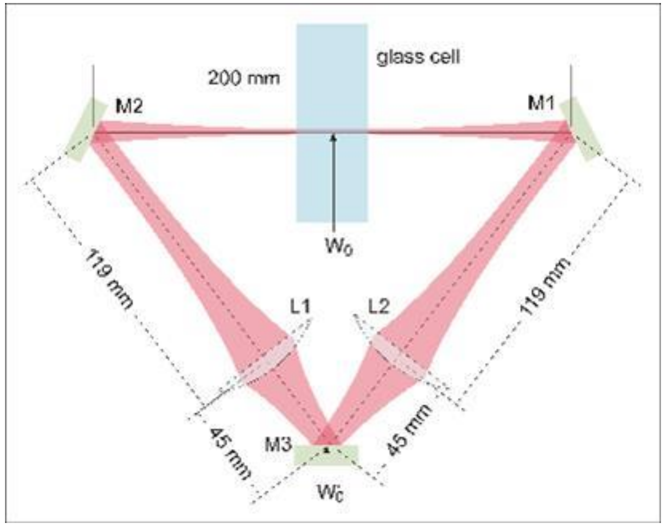
- Life time: 1μs
- Retrieve efficiency: 35%

Require lifetime to be extended about 8 orders of magnitude!



Efficient and Long-lived Quantum Memory

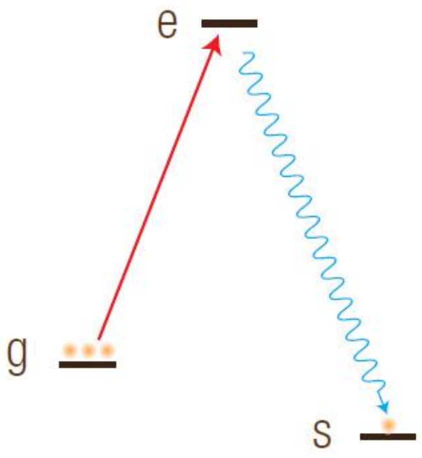
- **Increasing retrieval efficiency:**
  - ☑ Ring cavity enhancement: increase interaction strength



- **To Increase life time, need to overcome:**
  - ☒ Inhomogeneity of magnetic field
  - ☒ Loss of atoms duo to gravity and atomic random motion
  - ☒ Spin-wave dephasing

Efficient and Long-lived Quantum Memory

- Collective excitation state (spin-wave) of atomic ensemble:



Raman process:

- Absorbing a photon with momentum $\hbar\mathbf{k}_1$
- Emitting a photon with momentum $\hbar\mathbf{k}_2$

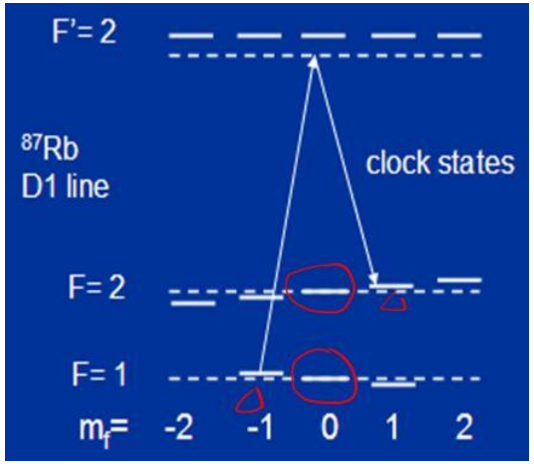
$$|\psi\rangle_a = \frac{1}{\sqrt{N}}\sum_j e^{i\Delta\mathbf{k}\cdot\mathbf{r}_j}|g \ldots s_j \ldots g\rangle$$

$\Delta\mathbf{k} = \mathbf{k}_1$-$\mathbf{k}_2$,
$\mathbf{r}_j$ is the position of atom j

☒ Inhomogeneity of magnetic field:

The evolution phase given by each atom $\phi_j = \frac{E_{sj}-E_{gj}}{\hbar} = \frac{\Delta E_j}{\hbar}$

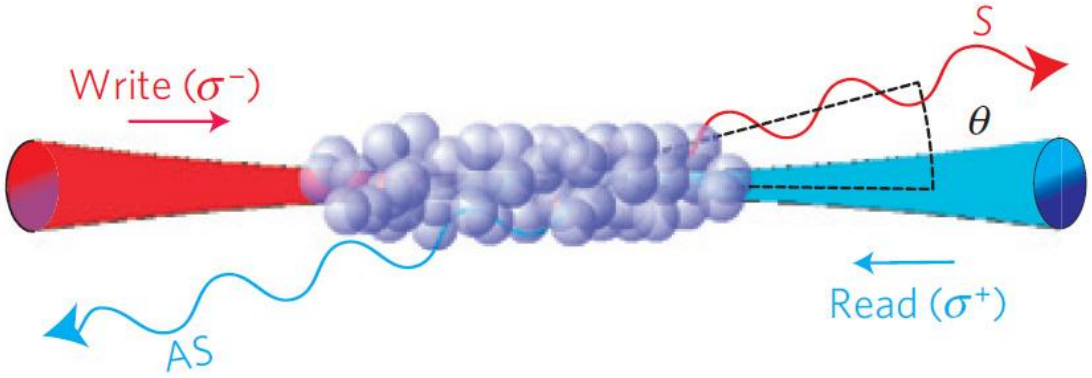
Inhomogeous magnetic field may cause different ΔE_j ➡ uncertain additional phase



☑ Solution: "clock states" (ΔE is not sensitive to magnetic field)

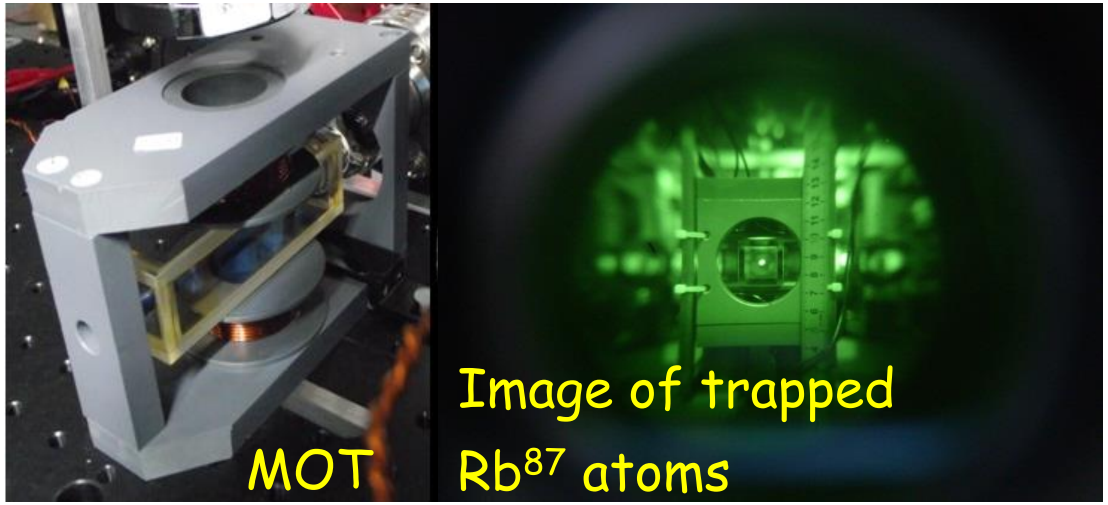
Efficient and Long-lived Quantum Memory

☒ Loss of atoms due to gravity and atomic random motion: atoms will diffuse or fall

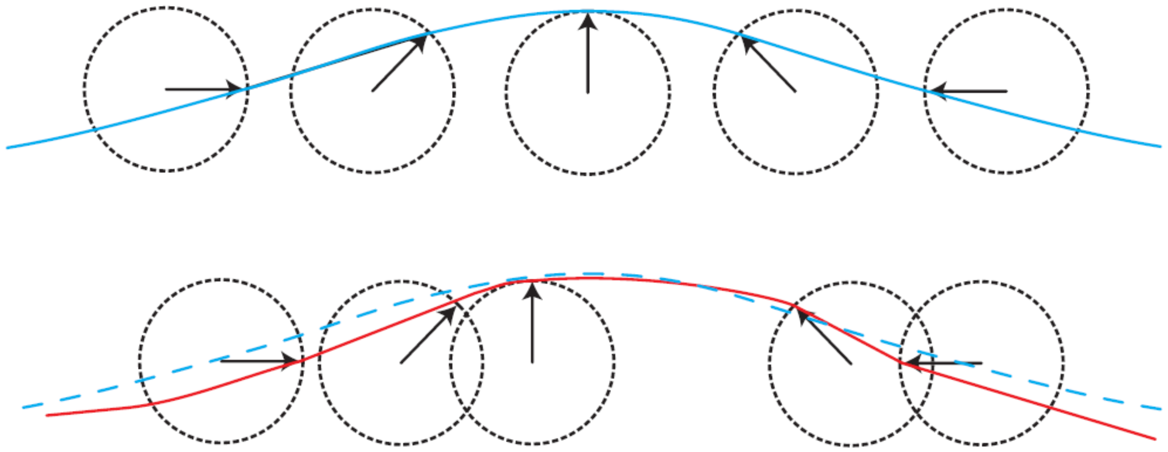


☑ Solution:

- Cooling atoms with optical molasses
- Write/Read in the gravitational direction



Efficient and Long-lived Quantum Memory



☒ Spin-wave dephasing

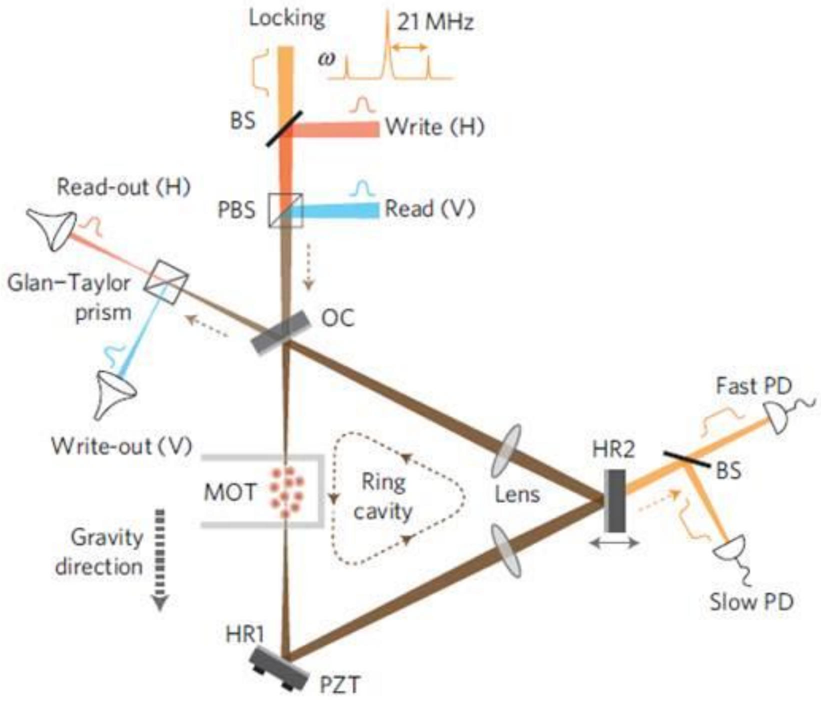
$$|\psi\rangle_a = \frac{1}{\sqrt{N}} \sum_j e^{i\Delta\mathbf{k}\cdot\mathbf{r}_j} |g \ldots s_j \ldots g\rangle$$

Different $\mathbf{r_j}(t)$ due to atomic random motion

☑ Solution: collinear recoil, smallest $\Delta\mathbf{k}$ ➡ evolution phase $\Delta\mathbf{k}\cdot\mathbf{r}$ is almost fixed to 0

Efficient and Long-lived Quantum Memory

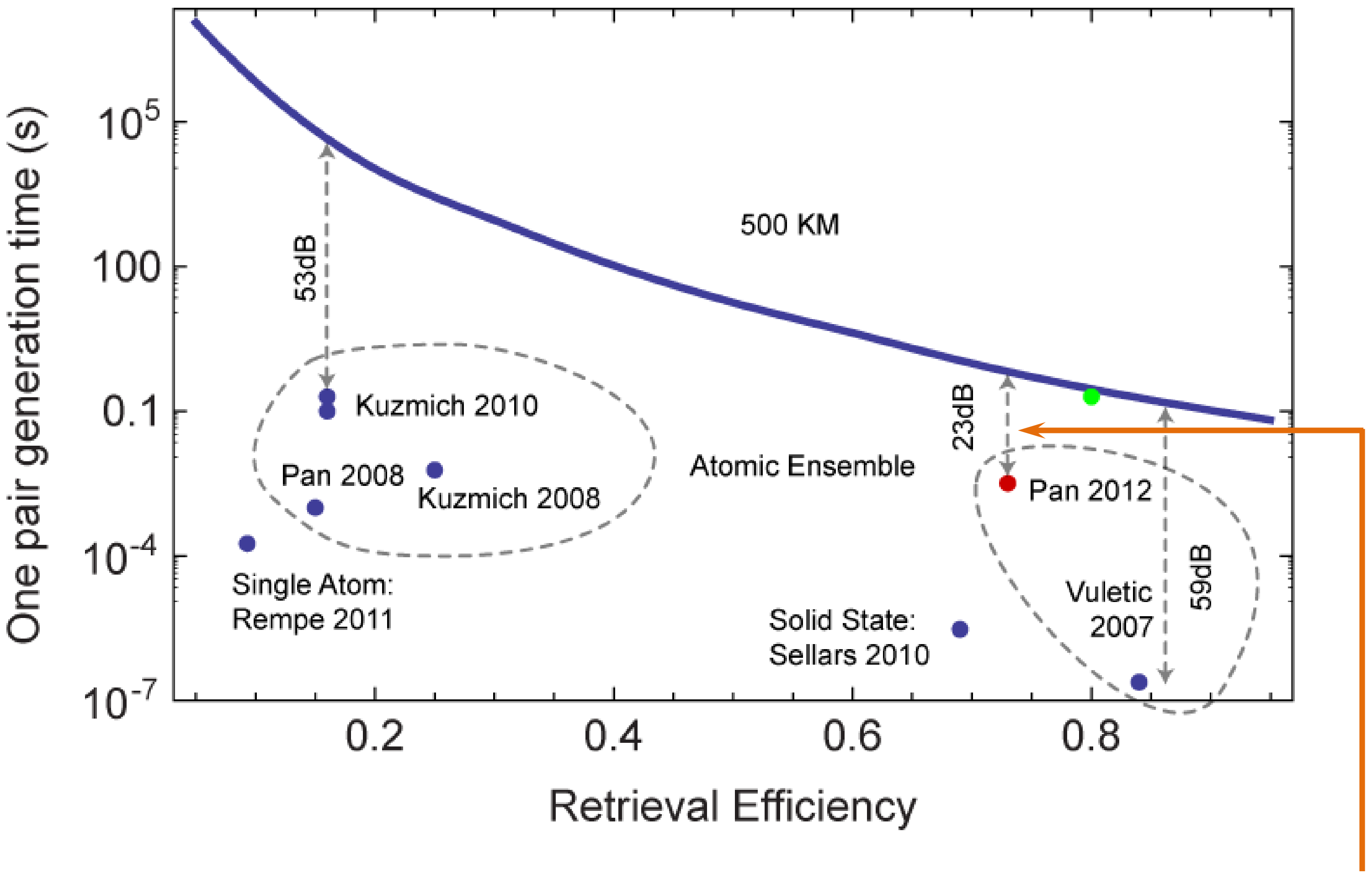
- ☑ Ring cavity (finesse=48)
- ☑ Clock state
- ☑ Optical molasses
- ☑ Write/Read in the gravitational direction
- ☑ Collinear configuration



Life time 3ms, retrieve efficiency 73%

Bao *et al.*, Nature Physics 8, 517 (2012)

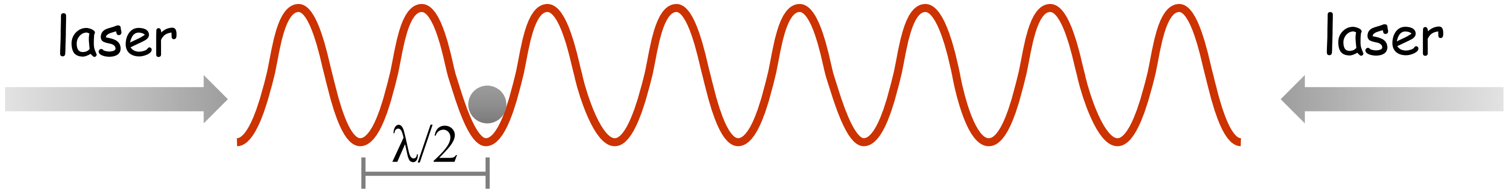
Efficient and Long-lived Quantum Memory



Require lifetime to be extended about 2 orders of magnitude

Efficient and Long-lived Quantum Memory

Optical lattice confinement

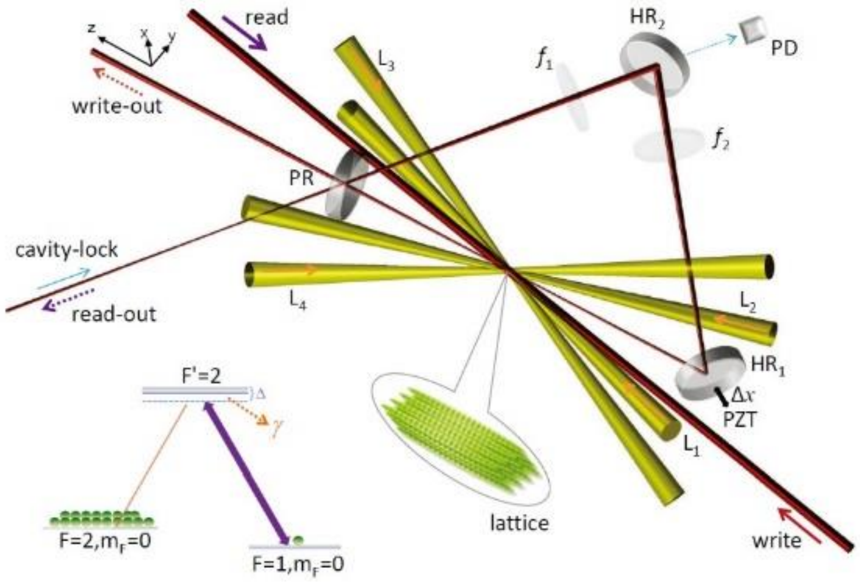


- Interference of counter-propagating laser beams ➡ a spatially periodic pattern
- "Lattice": periodic optical dipole potential ➡ atoms are cooled and congregate in the locations of potential minima

We use:

- 3D Lattice (0~180μk, distance between adjacent wells: dx~2.8μm, dy~5.9μm, dz~0.54 μm)
- Spin-wave excitation (Λ~15 μm)

Limits atomic motion in all direction to suppresses atomic collision-induced decoherence

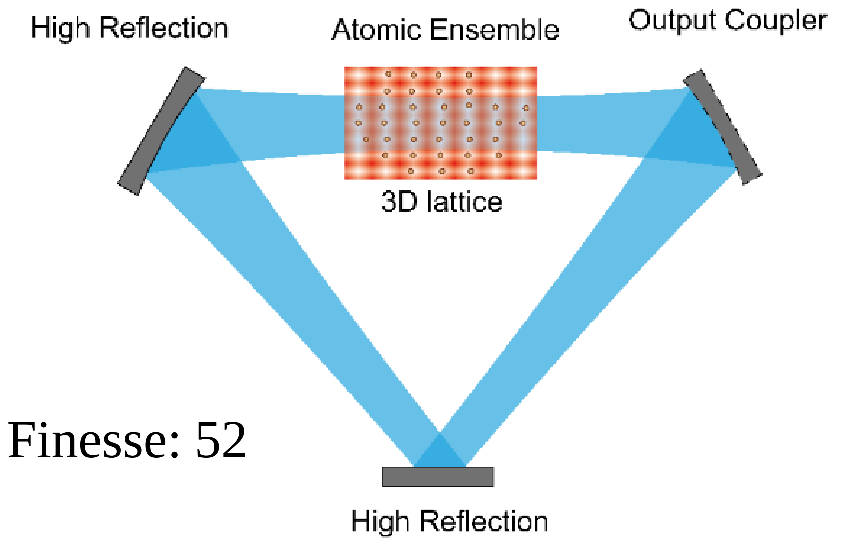


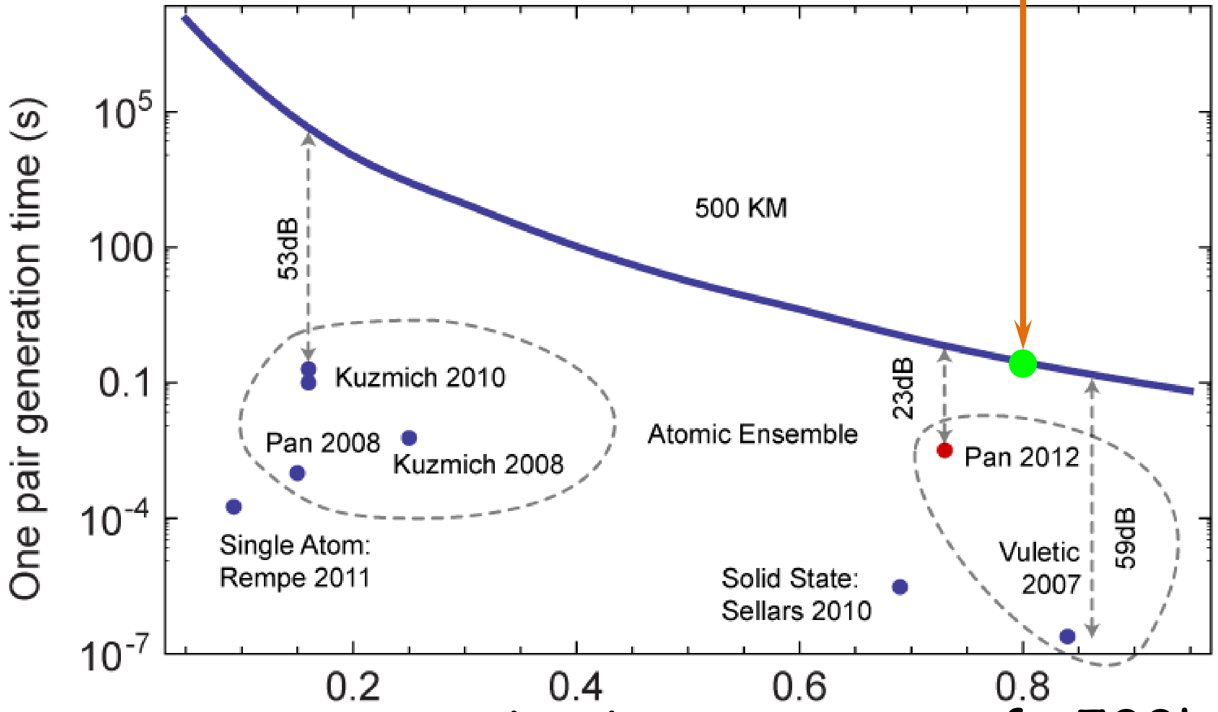
Efficient and Long-lived Quantum Memory

With ring cavity + optical lattice confinement:

Life time 220ms, retrieve efficiency 76%

Yang *et al.*, Nature Photonics 10, 381 (2016)





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

☒ But the probability of generating photon-atom entanglement is still low (~1%)

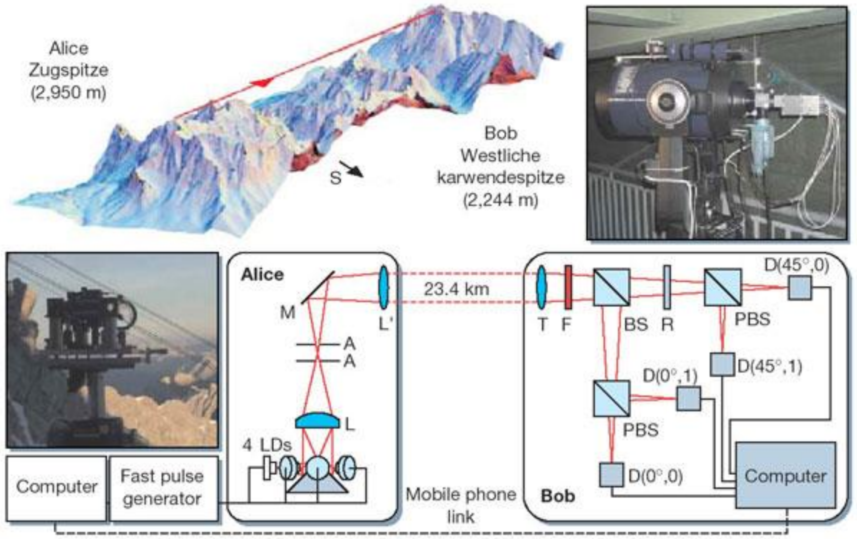
☒ **A practical quantum repeater might still need 10 more years**

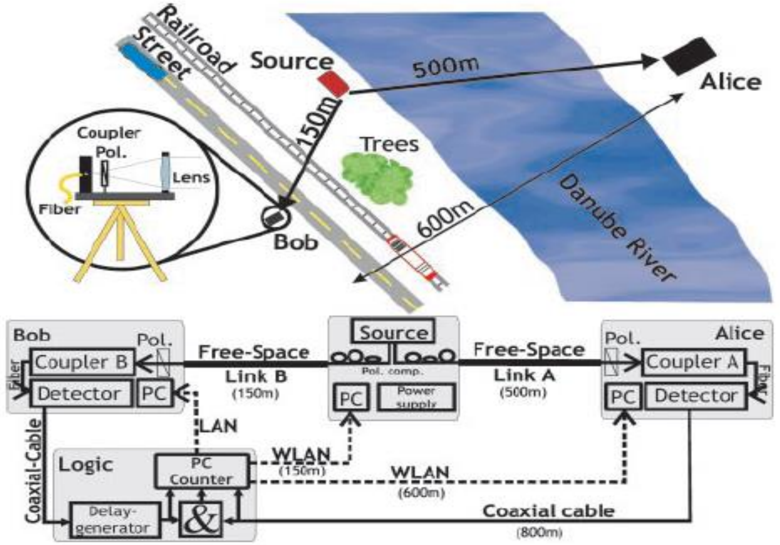
Part 5: Free-Space Quantum Communication

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

Attempt to Free-space Quantum Communication





- QKD with weak conherent pulse, 23.4km: Kurtsiefer *et al.*, Nature 419, 450 (2002)
  Security distance ~5km

- Distribution of entanglement ~600m: Aspelmeyer *et al.*, Science 301, 621 (2003)

Major question: could the quantum states of single and entangled photons still survive after passing through atmosphere?

Ground Tests for Satellite Quantum Communication

Phase 1: The possibility of single and entangled photons passing through atmosphere

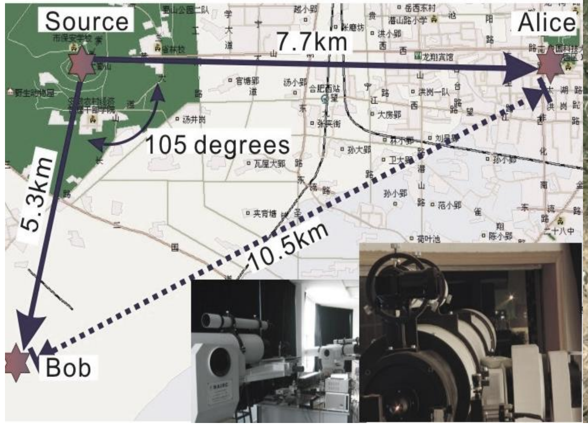
- Free-space entanglement distribution (13km) [PRL 94, 150501 (2005)]
- Free-space quantum teleportation (16km) [Nature Photonics 4, 376 (2010)]

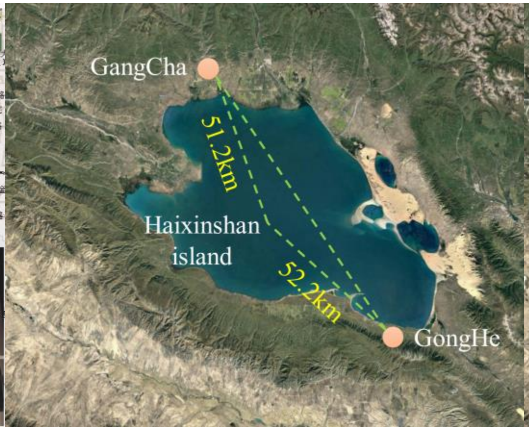
Phase 2: The feasibility of quantum communication in high-loss satellite-to-ground channel

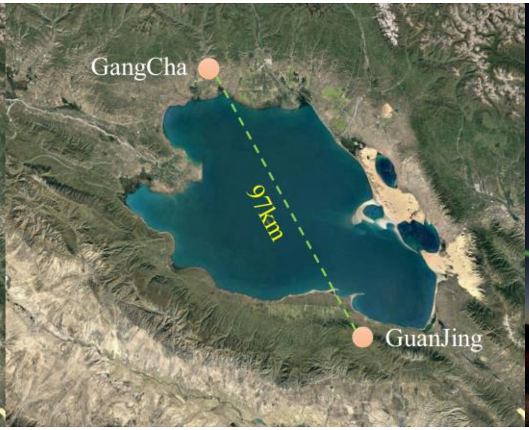
- Free-Space quantum teleportation and entanglement distribution ~100km [Nature 488, 185 (2012)]

Phase 3: Overcoming all the demanding conditions for ground-satellite QKD

- Mimicking rapid motion, vibration, random movement of satellites [Nature Photonics 7, 387 (2013)]







Quantum Science Satellite “Micius”

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

2011

The “Quantum Science Satellite” project was officially approved

2012

The first prototype satellite started

2014

The first prototype satellite was completed and the ground station in Xinglong was completed

2015

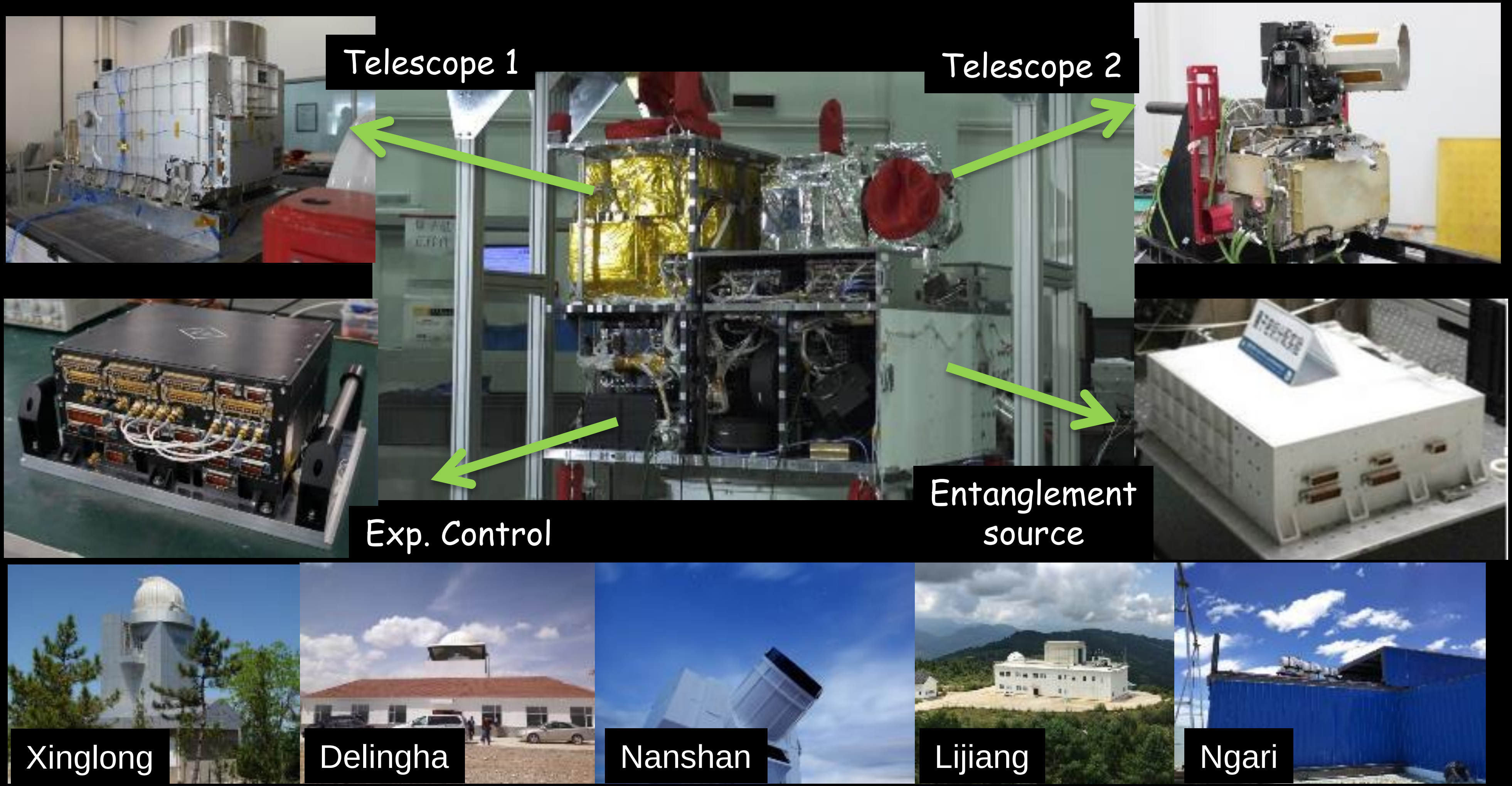
The flight model of the satellite was completed. The ground stations in Nanshan and Delingha were completed.

2016

Lijiang and Ali was complete.

The satellite was launched.

Quantum Science Satellite "Micius"



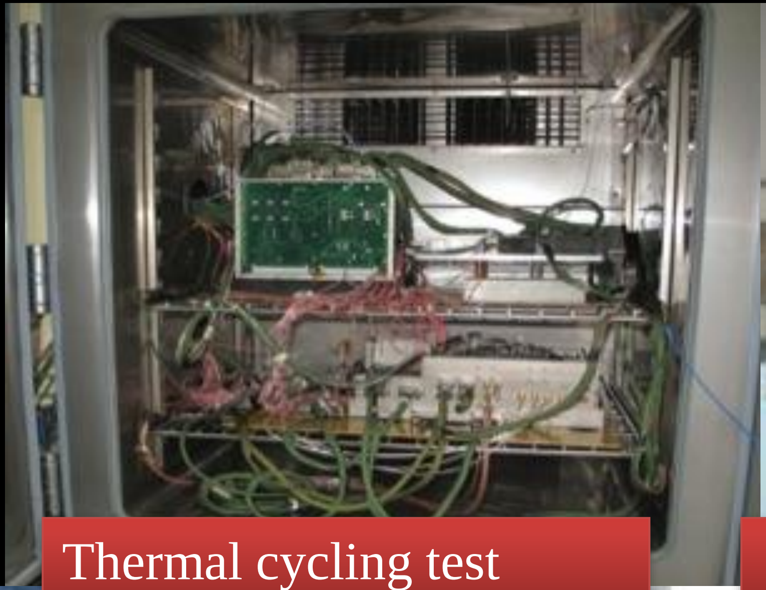
1958

SITP

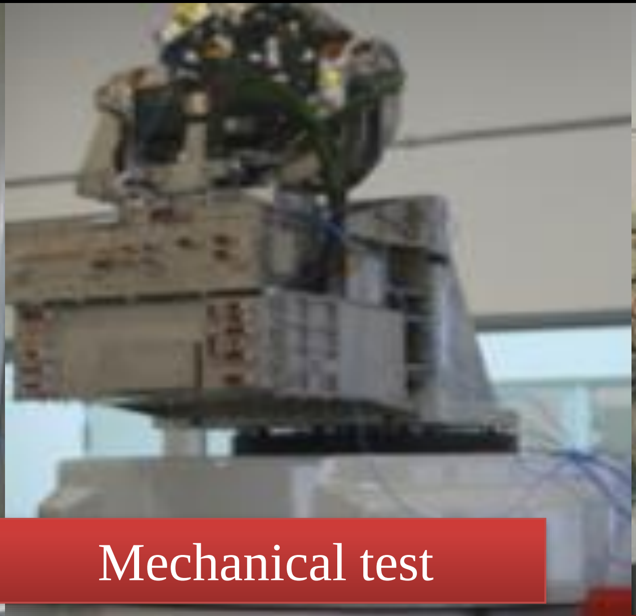
microsat

NAOC

Space circumstance experiments

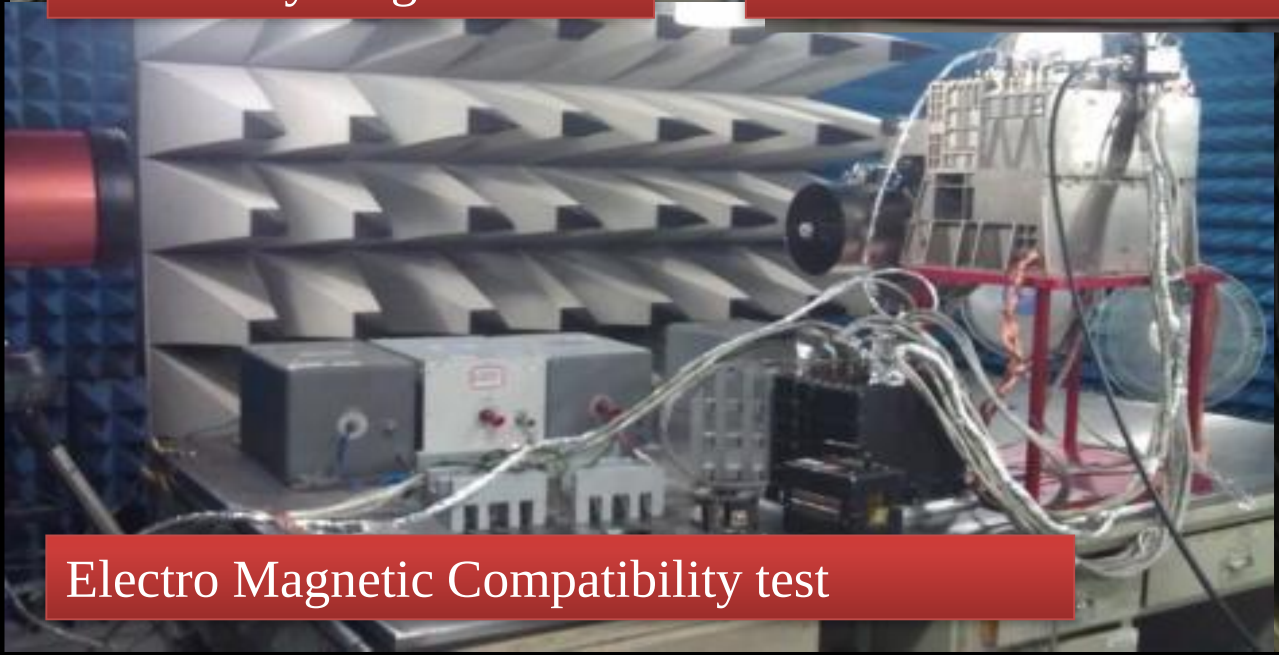


Thermal cycling test



Mechanical test

Thermal vacuum test

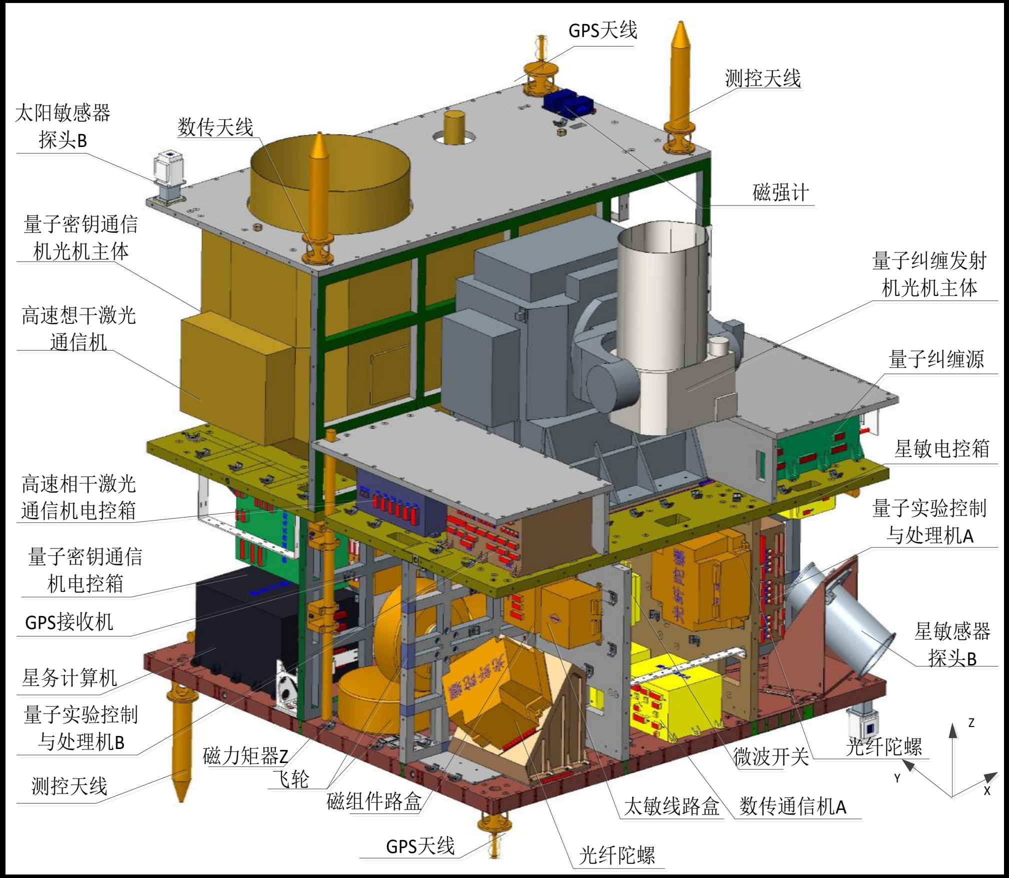


Electro Magnetic Compatibility test

Reliability test

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

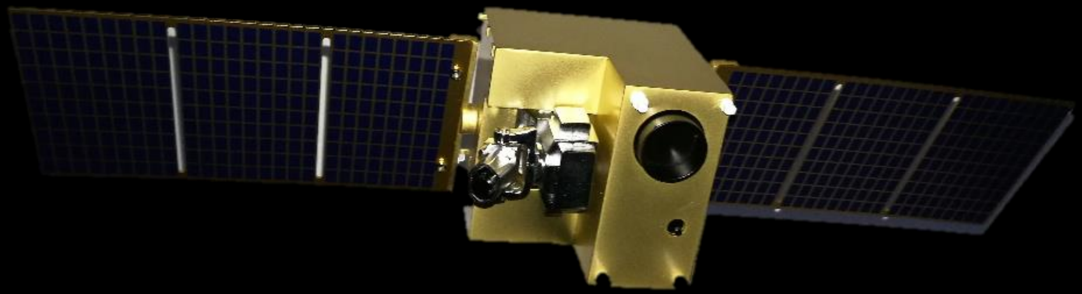
- **Prototype of law of inertia:** "止，以久也，无久之不止"

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

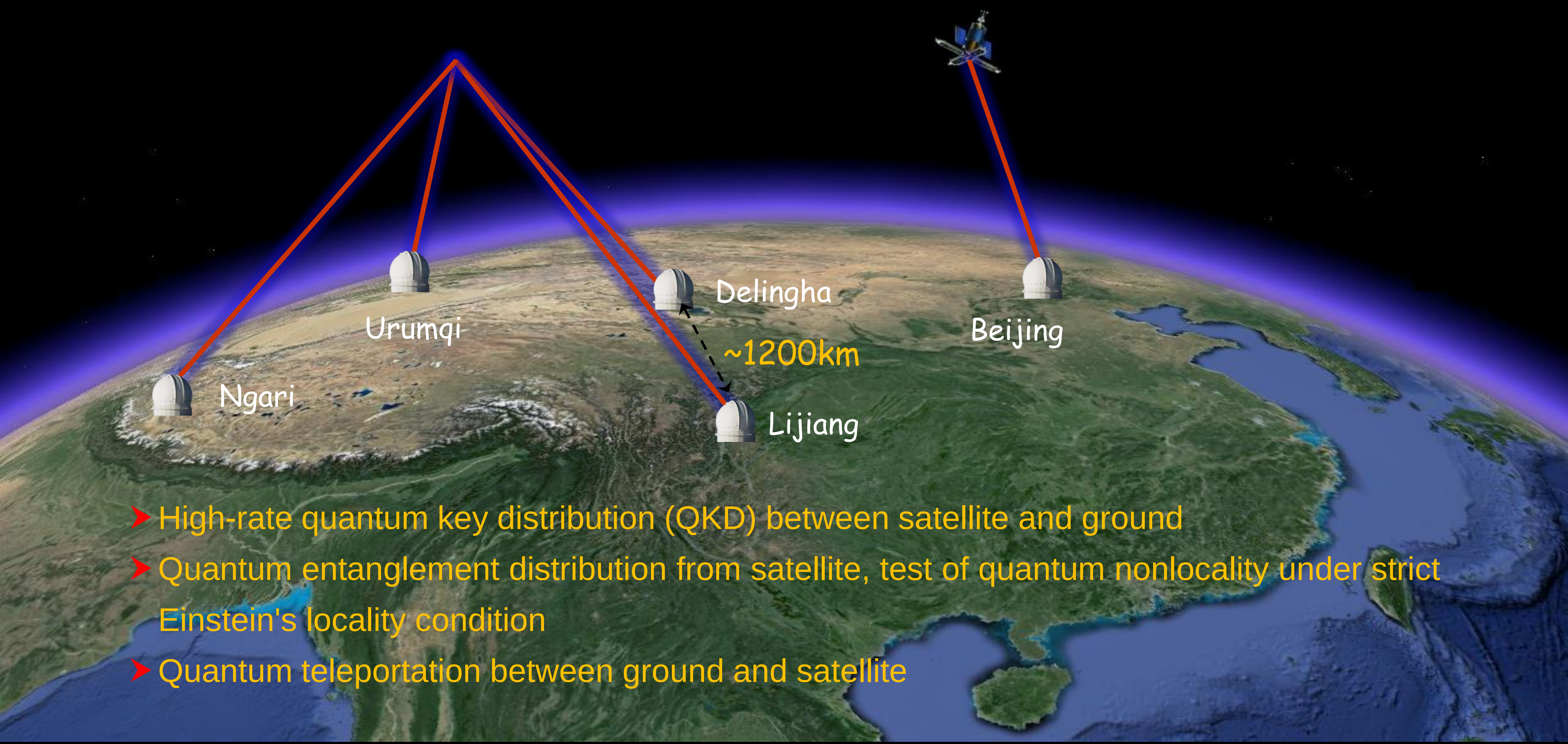
  - In the meantime Greek philosopher Aristotle believed that a force was necessary to keep an object moving
  - Newton's first law comes in 2000 years

Quantum Science Satellite "Micius"

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



Micius' Three Missions



- High-rate quantum key distribution (QKD) between satellite and ground
- Quantum entanglement distribution from satellite, test of quantum nonlocality under strict Einstein's locality condition
- Quantum teleportation between ground and satellite

Quantum Key Distribution

☑ May 2017, in Nanshan, Ulumqi

Entanglement Distribution

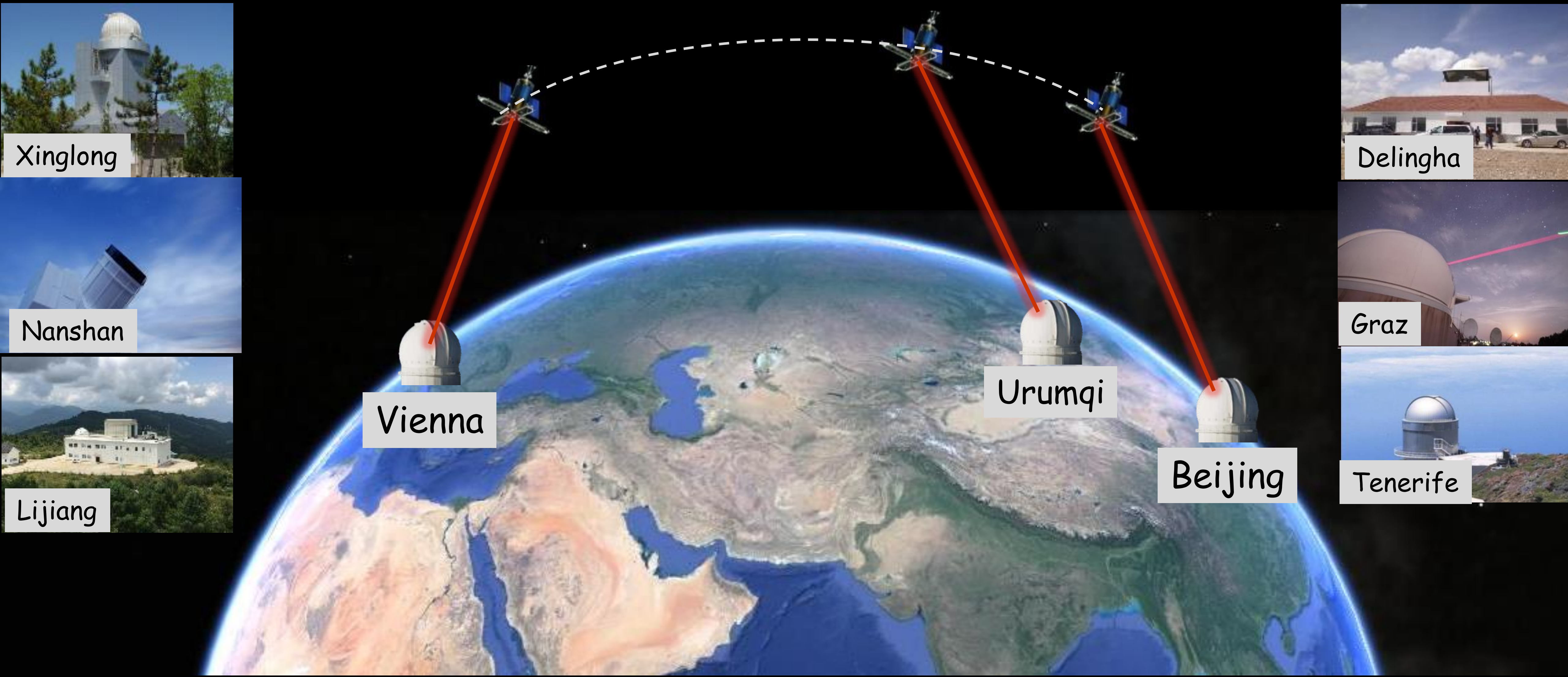
☑ April 2017, in Lijiang

Quantum Teleportation

☑ December 2016, in Ali

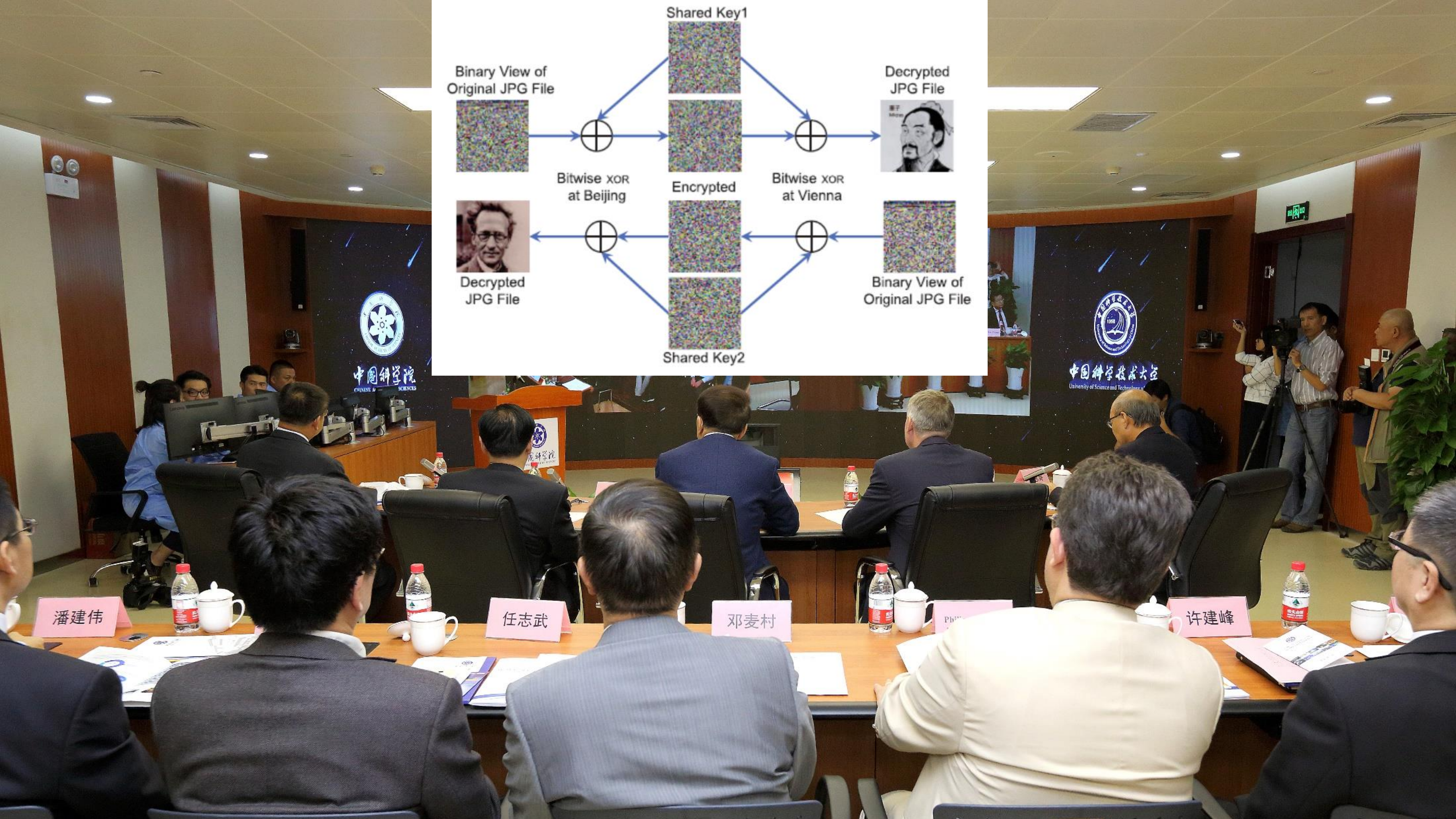
Intercontinental Quantum Key Distribution

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

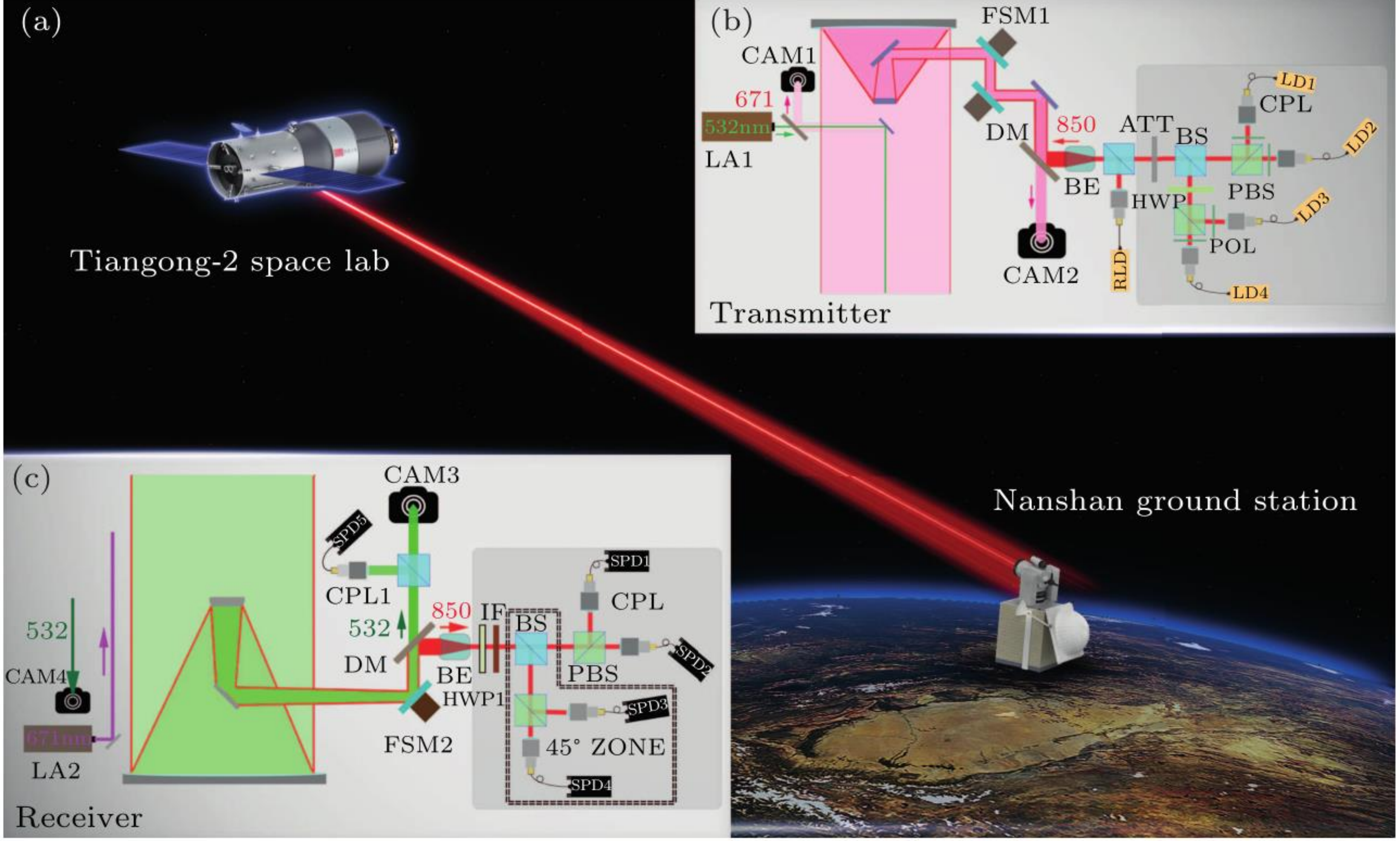


Intercontinental Quantum Key Distribution

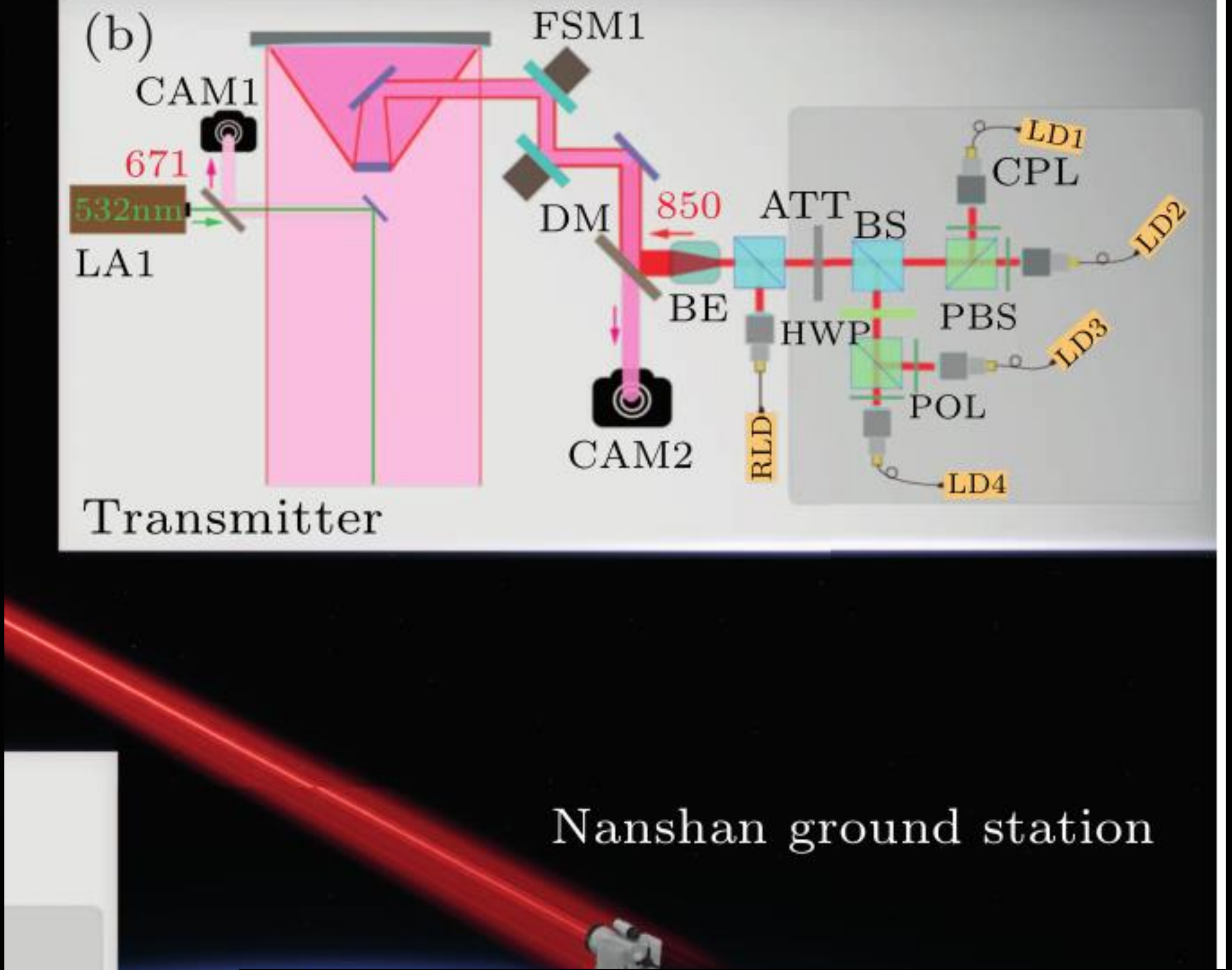
☑ June 2017, in Graz



Shared Key1
Binary View of Original JPG File
Decrypted JPG File
Bitwise XOR at Beijing
Encrypted
Bitwise XOR at Vienna
Decrypted JPG File
Binary View of Original JPG File
Shared Key2
中国科学院
中国科学技术大学
潘建伟
任志武
邓麦村
许建峰



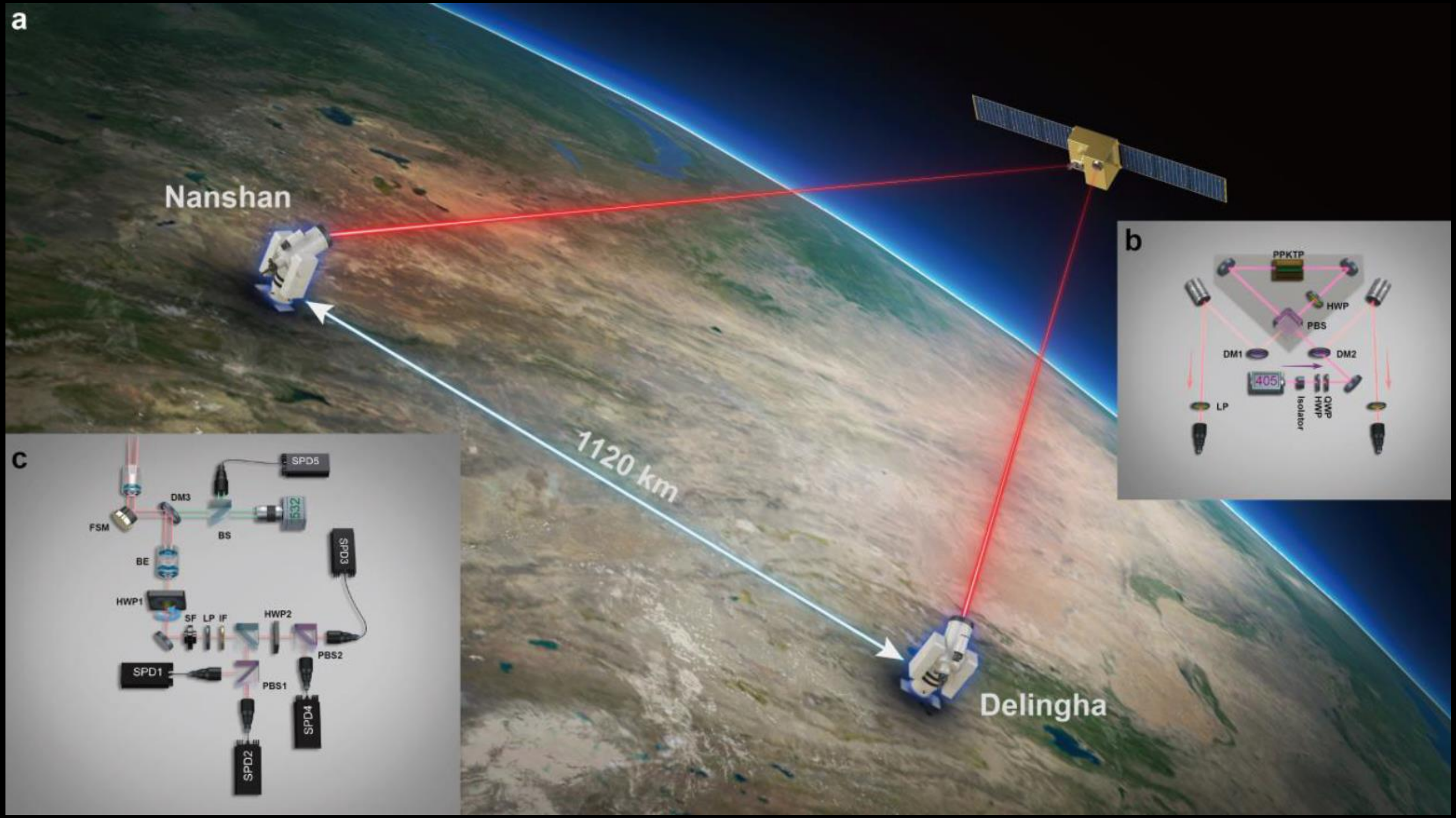
(a)
Tiangong-2 space lab
Nanshan ground station
(b)
FSM1
CAM1
671
532nm
LA1
DM
850
ATT
BS
LD1
CPL
LD2
BE
PBS
HWP
LD3
POL
CAM2
RLD
LD4
Transmitter
(c)
CAM3
SPD5
SPD1
CPL1
CPL
850
IF
BS
532
532
DM
BE
PBS
SPD2
CAM4
HWP1
SPD3
671nm
FSM2
45° ZONE
LA2
SPD4
Receiver



- Total weight of the payload: 59 kg
- Average power: 80 W
- ~400-km orbit with 42^0 inclination

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

Recent Progress with Micius

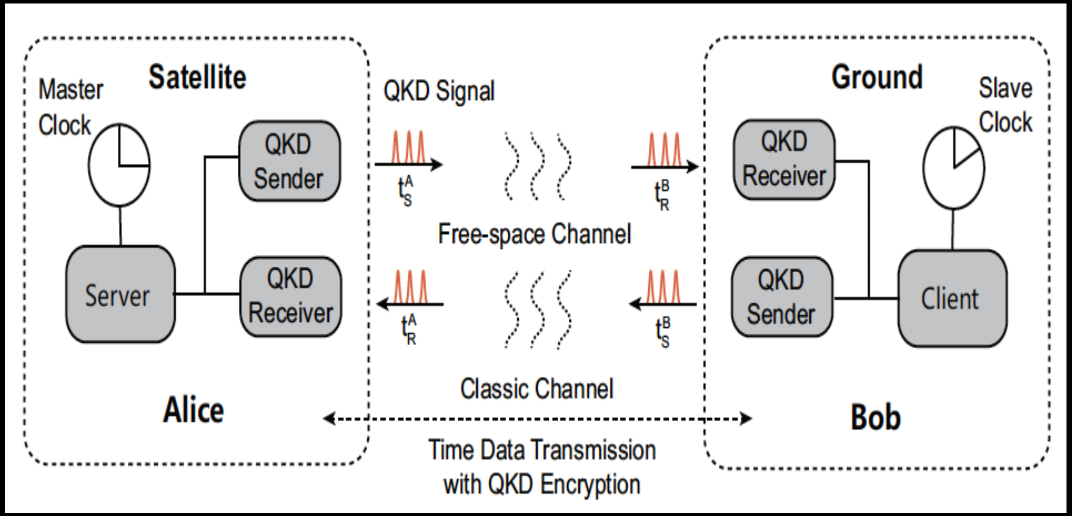


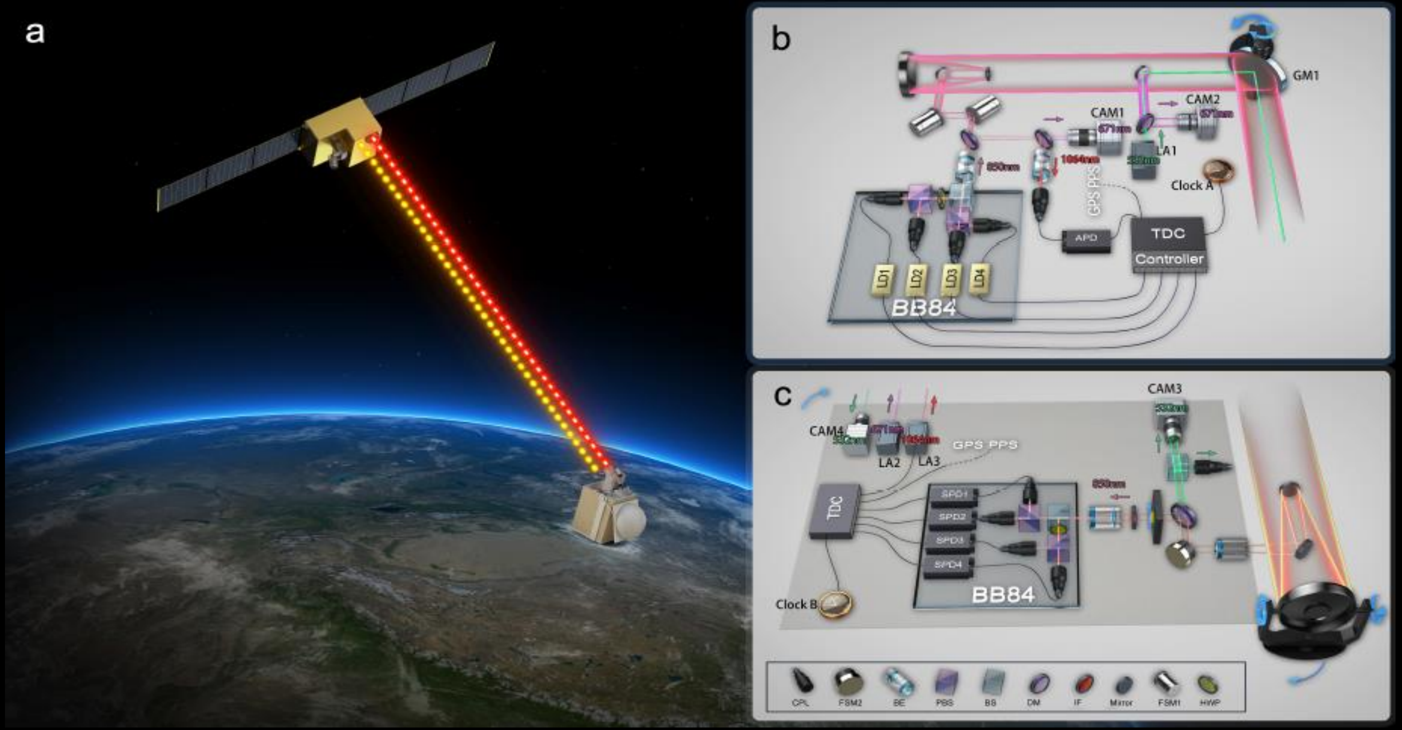
- ✓ The raw key rate of 0.43 bits/s over 1120 km
- ✓ Without relying on trusted relays
- ✓ Immunity to all known side channels.

Entanglement-based secure quantum cryptography between two ground stations separated by 1120 kilometers

Recent Progress with Micius

Satellite-based quantum-secure time transfer





Quantum data origin authentication:

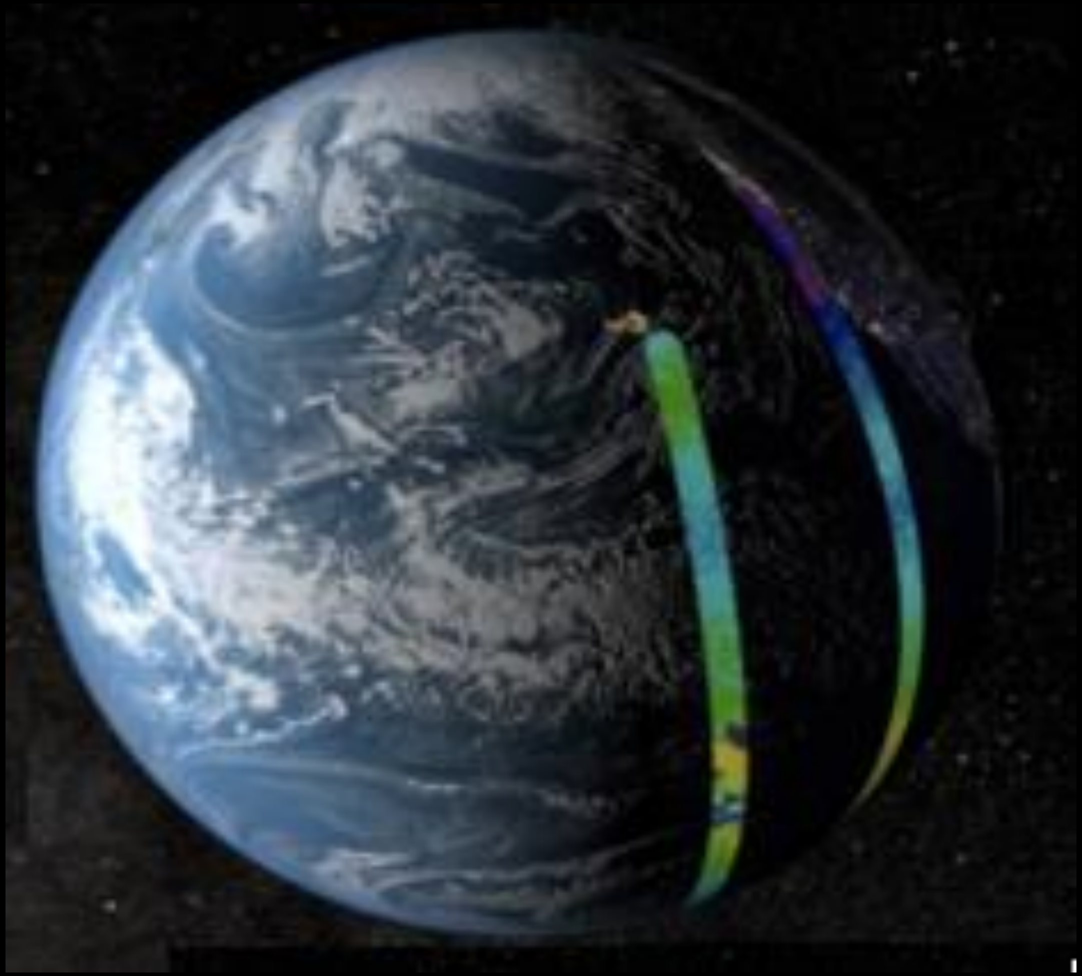
Sync signal: carried by quantum signals

Time data: QKD encryption transmission

- QBER of less than 1%
- Time-transfer precision of 30 ps

Part 6: Future Prospects

Challenge of global-scale quantum network



The limitation of Micius

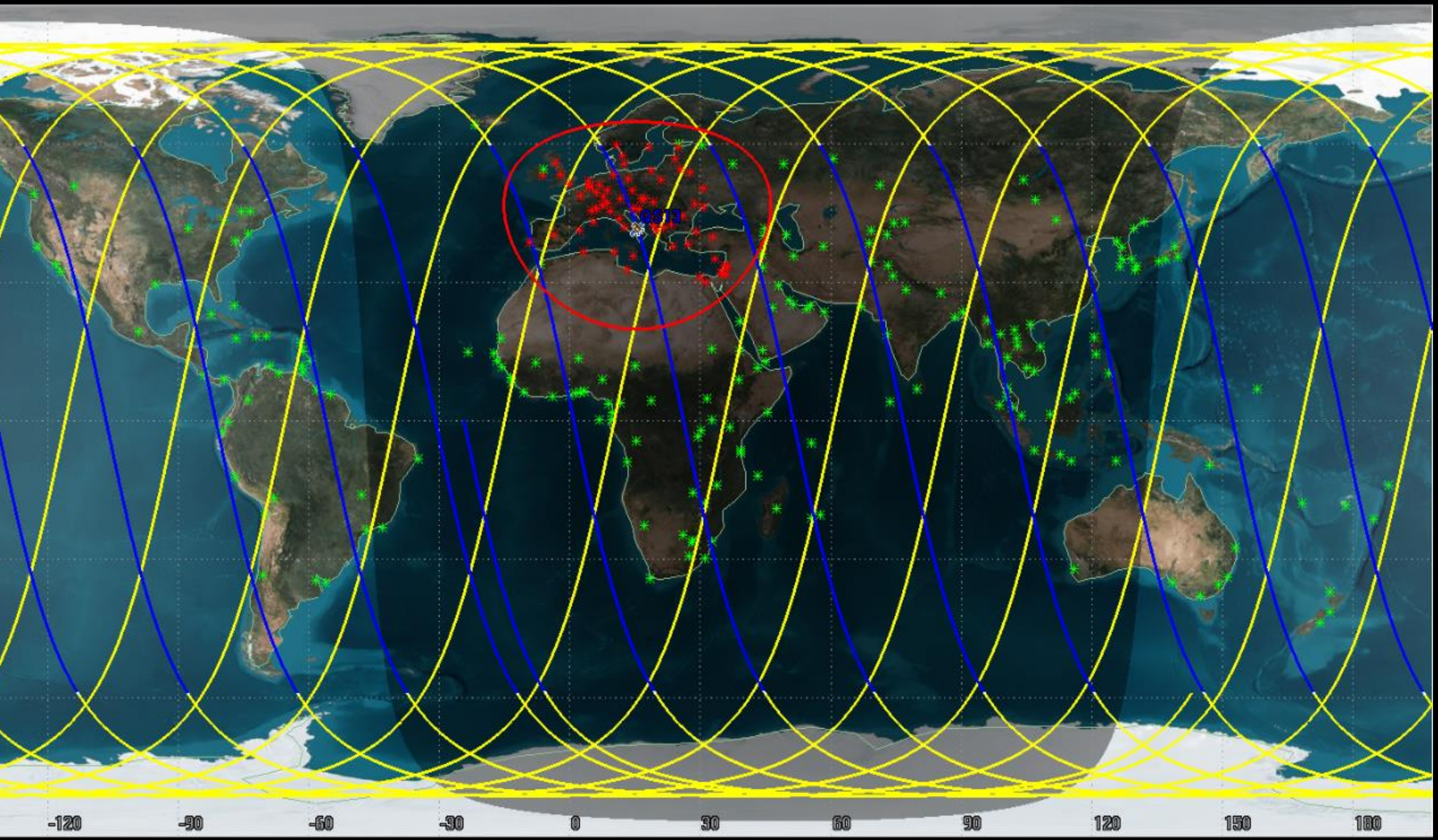
- **Experiment time is ~ 6 minutes for each pass**
- **Coverage range is about 500km (Radius)**
- **Have to be in the shadow of earth**
- **Weather condition affects**

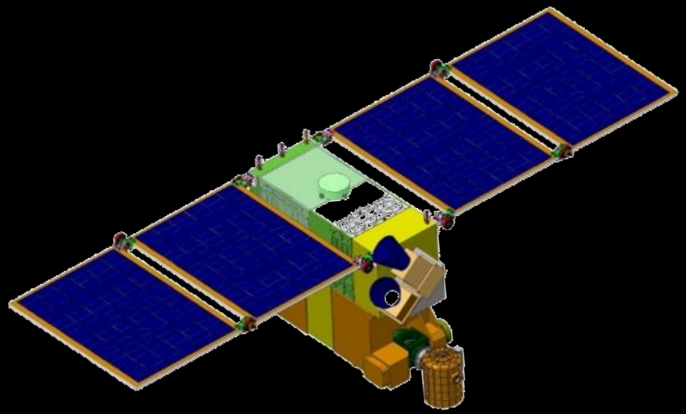
☑ Quantum constellation with LEO nano satellites

☑ The MEO-to-GEO quantum satellite

☑ Upgrade fiber quantum backbone network

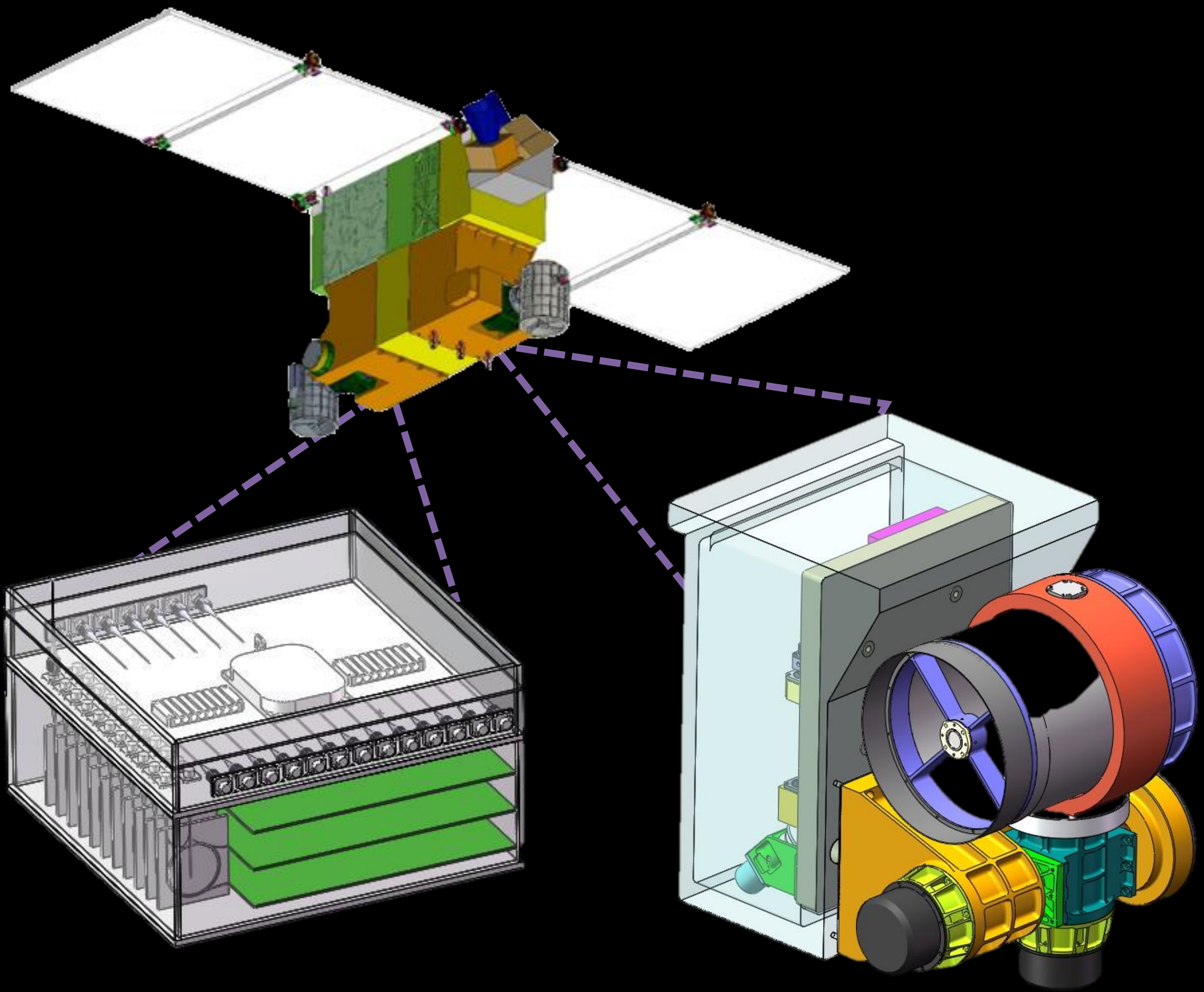
Quantum constellation with LEO nano satellites





- ☑ 800km Sun synchronization orbit
- ☑ 3 or 5 Nano quantum satellites
- ☑ More than 100 users
- ☑ Key weekly update
- ☑ Deliver over 5Gbits/year

Quantum constellation with LEO nano satellites



- ☑ Twin telescope can serve two users for one passage of the satellite
- ☑ Four sets of the quantum cryptograph device for different users
- ☑ Repetition rate of quantum source is over 500 MHz
- ☑ Divergence angle of the telescope is below 11 μrad

Quantum constellation with LEO nano satellites

- ☑ Smaller, lighter and cheaper quantum communication ground station
- ☑ Freely configure the number of telescopes on demand
- ☑ Diameter of one telescope is 280mm
- ☑ Receive efficiency of one telescope is more than 50%
- ☑ Easy to place, install and use

The movable ground station

Onboard

Recent progress based on compact ground stations

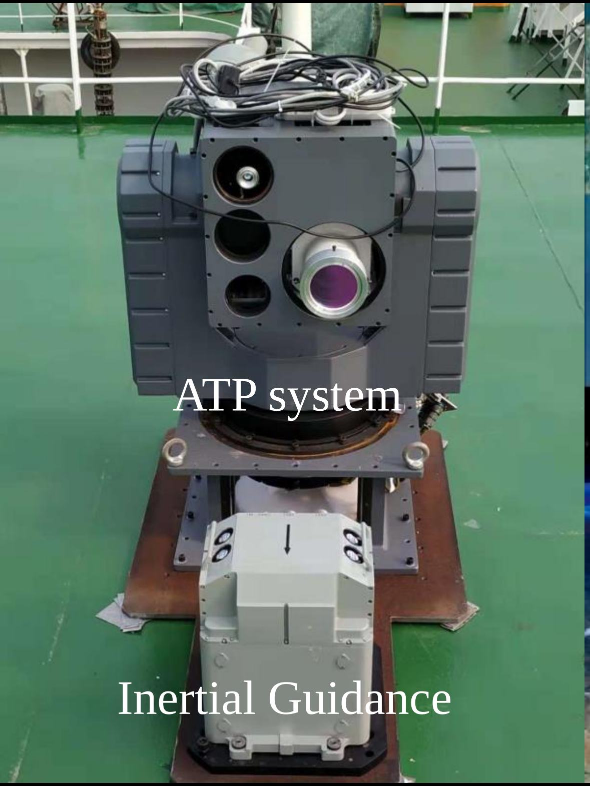
Dual-telescope

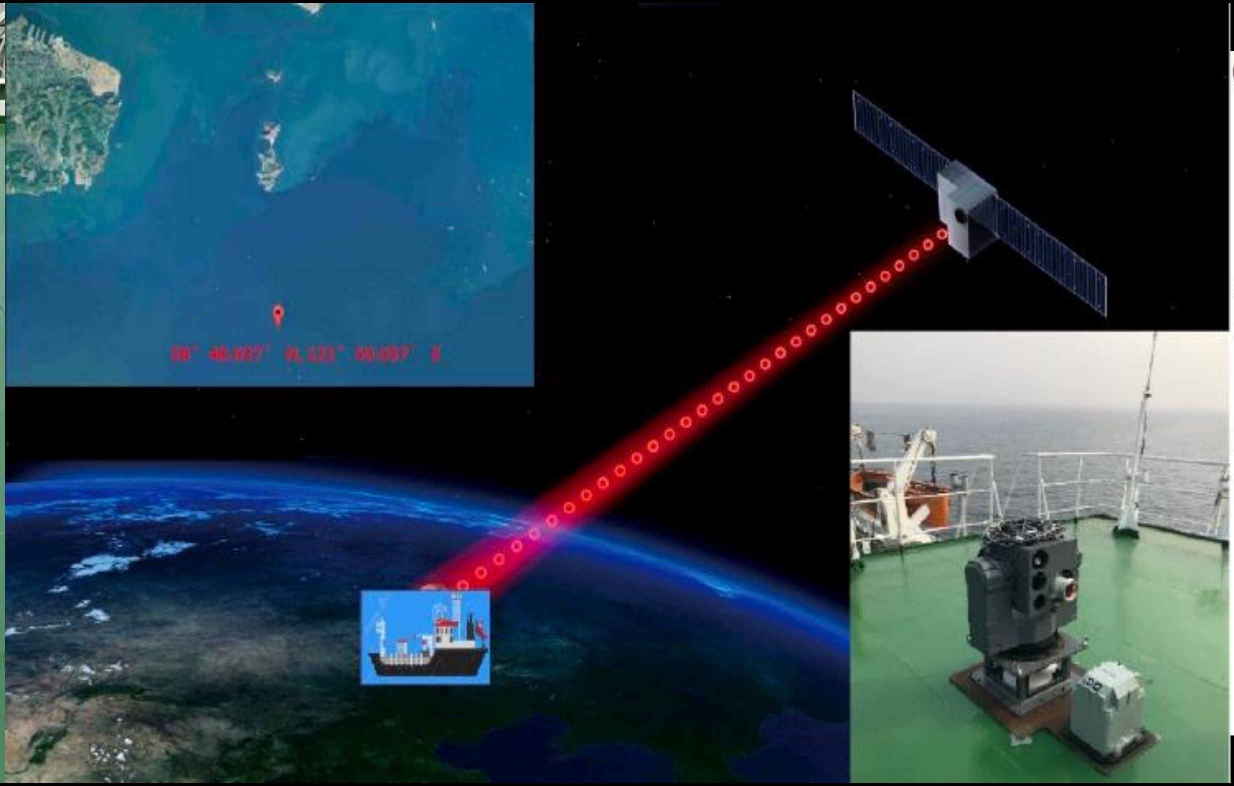
Single-telescope

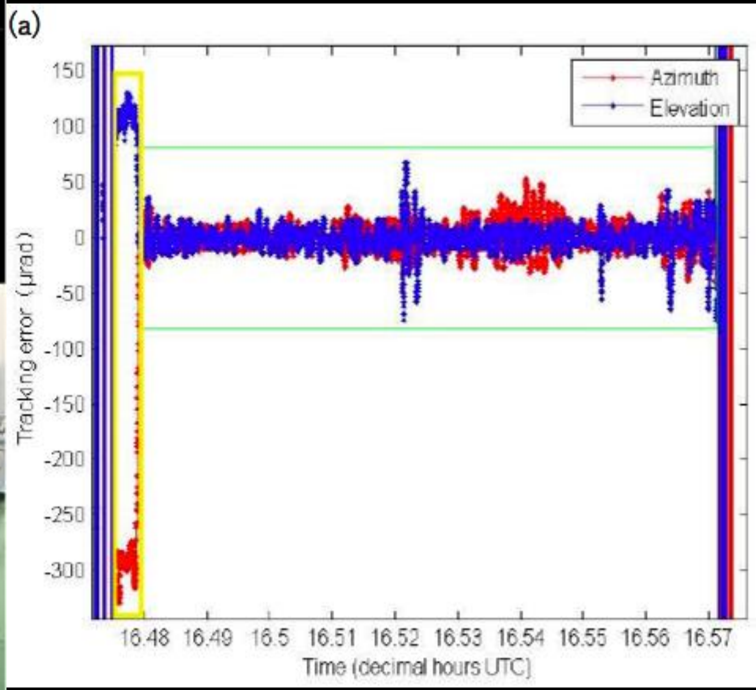
Satellite-based QKD in Weihai
(On the roof)

- ✓ With the compact ground stations, totally completed more than **20 times** Satellite-based QKD in **Shanghai, Lijiang, and Weihai**.
- ✓ The sifted key rate is ~ **2k bps**.

Recent progress based on compact ground stations



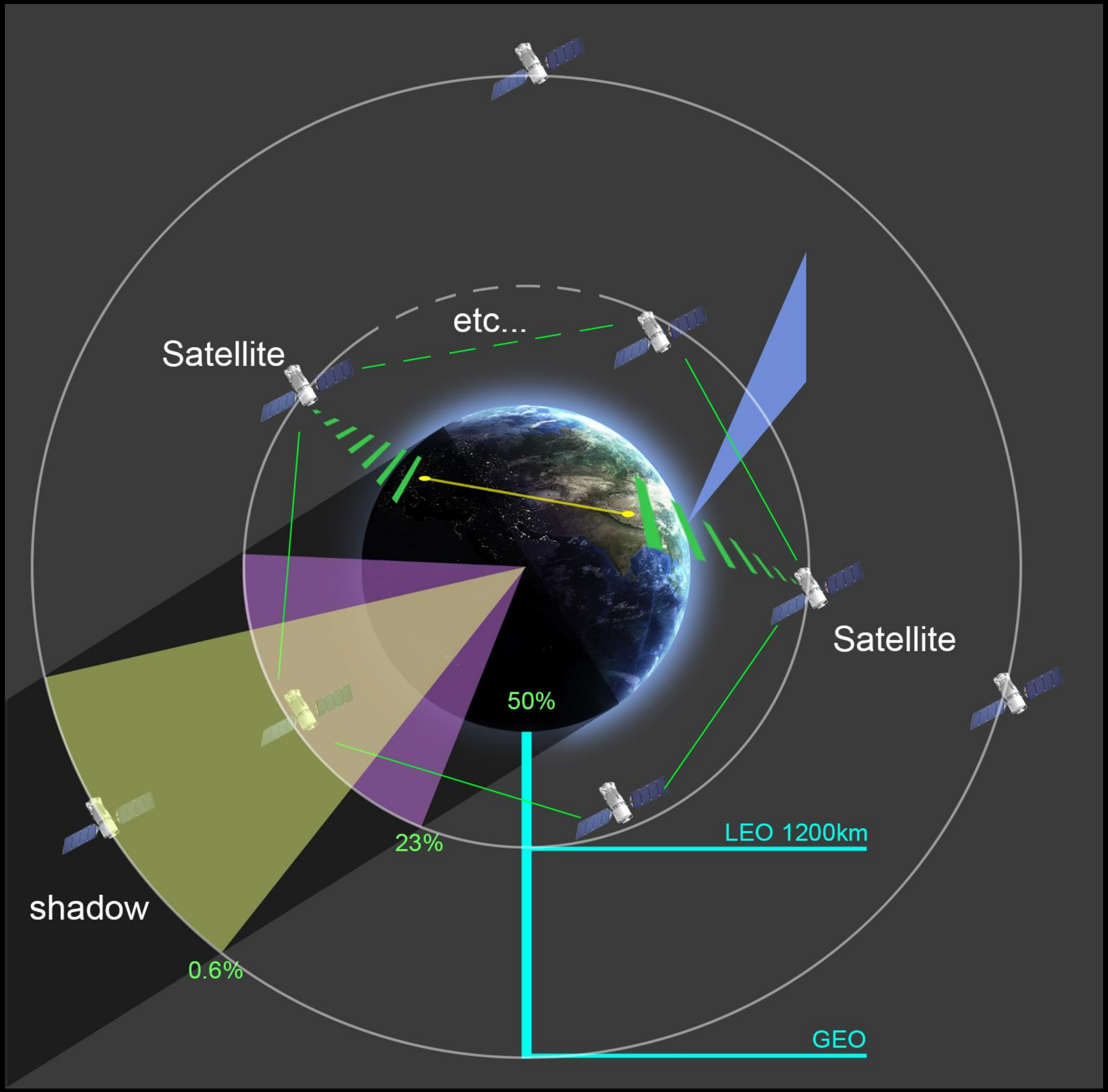




The test of ship-borne acquisition, tracking, and pointing (ATP) system between the ship and Micius satellite

The satellite-to-ship QKD is on going.

The MEO-to-GEO quantum satellite



Focus on all-day quantum communications research and fundamental problems:

☑ Wider space scale

☑ 10000-36000km（all over）

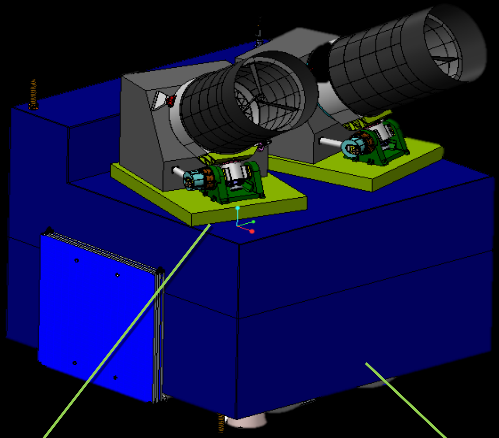
☑ Longer experiment duration

☑ Form minutes to hours

☑ Breakthrough earth shadow limit

☑ Generate Key 24 hours

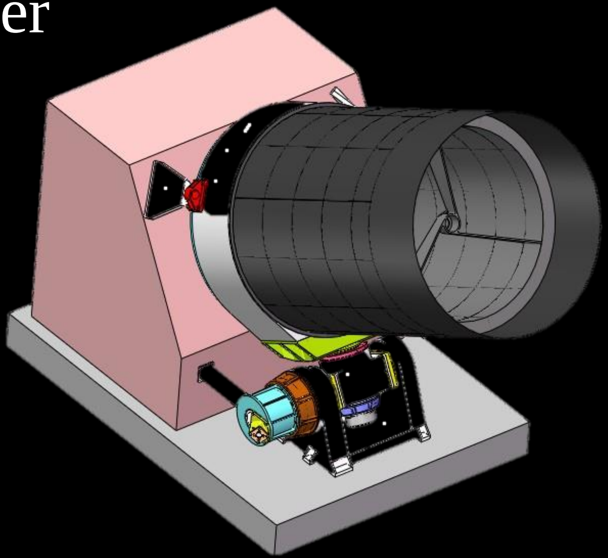
The MEO-to-GEO quantum satellite



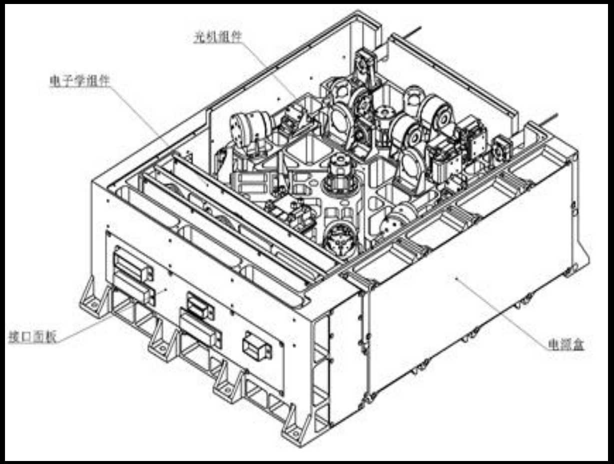
Satellite platform

- ☑ Ultra static and stable
- ☑ Orbital transfer ability

- ☑ Over 600 mm diameter
- ☑ Divergence angle:
  $< 3\ \mu rad$
- ☑ Tracking accuracy:
  < 100 nrad



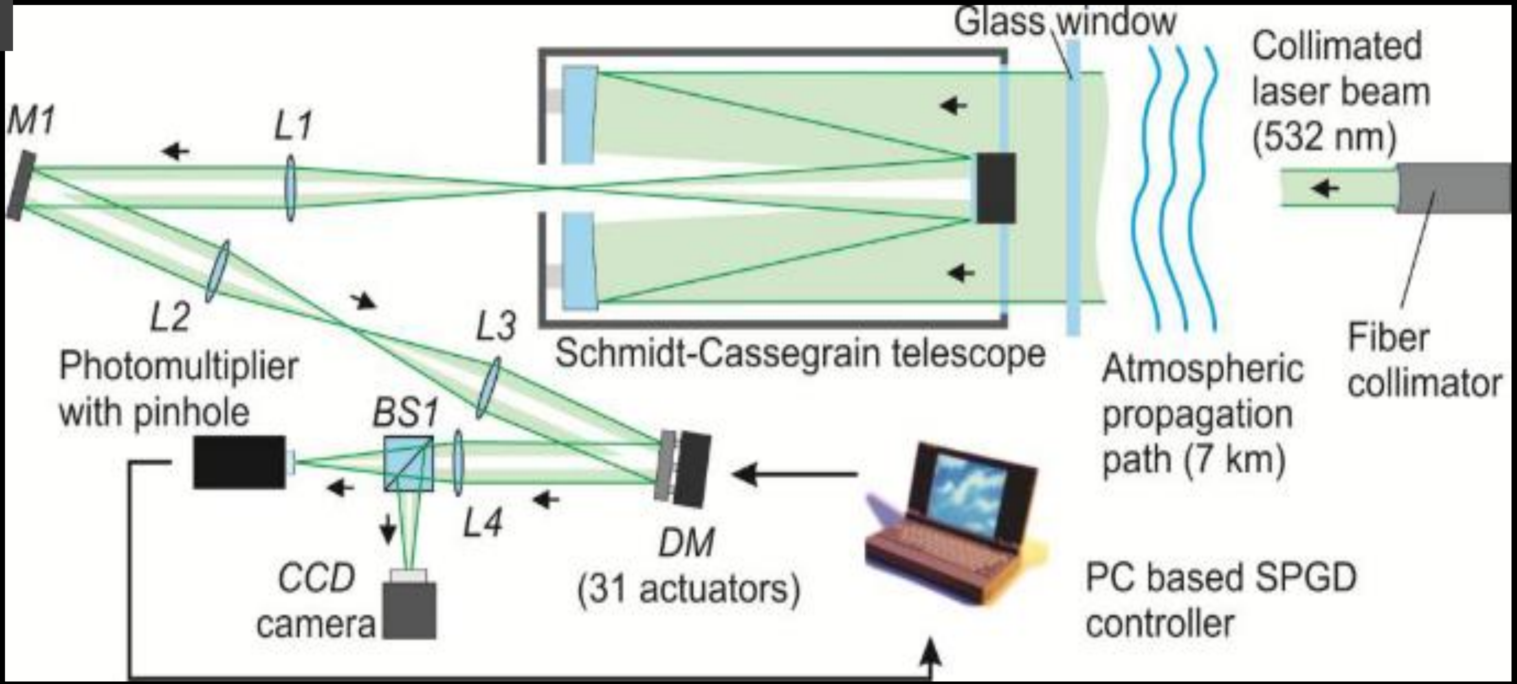
Photon transmission

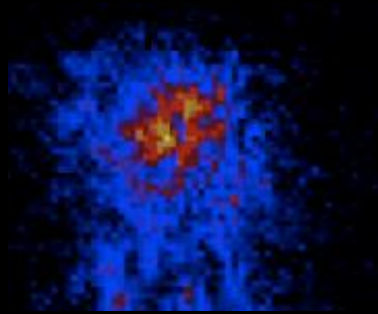


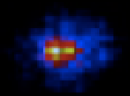
Quantum communication

- ☑ GHz entanglement source
- ☑ GHz decoy state QKD source
- ☑ Laser communication

The MEO-to-GEO quantum satellite







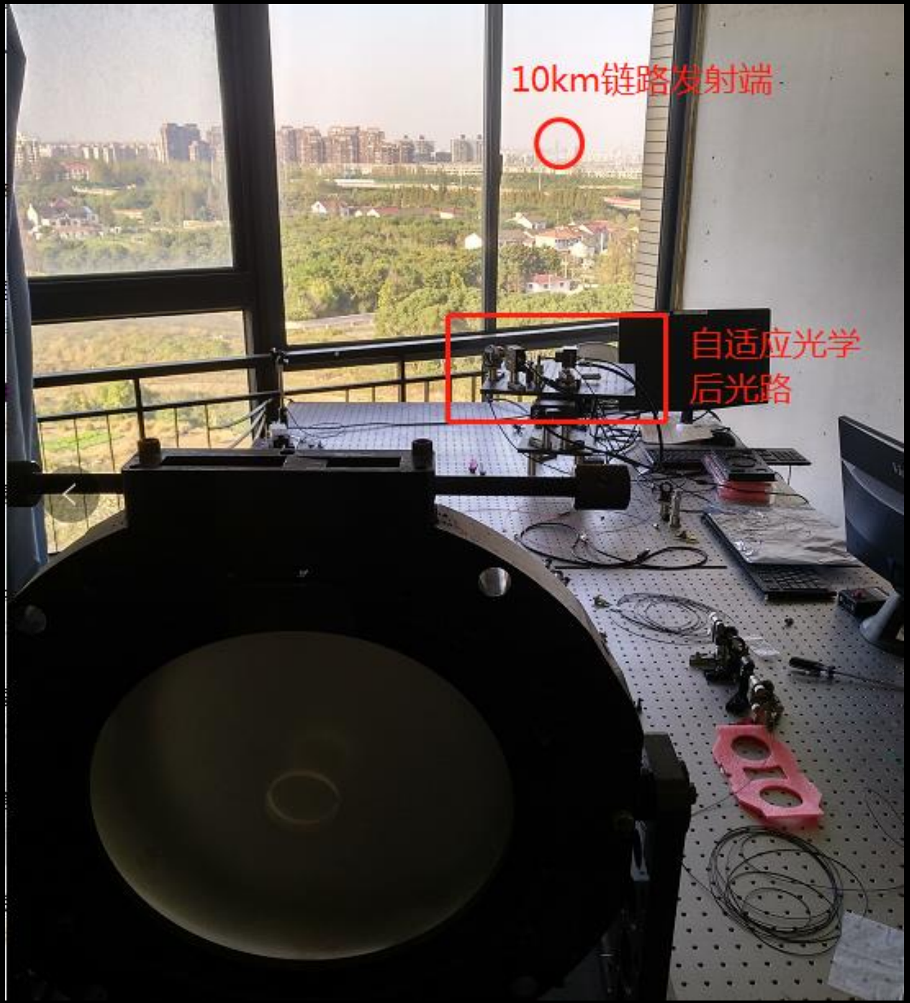
Upgrade the large aperture optical telescope on the ground:

☑ Utilizing adaptive optics to improve the coupling efficiency of single-mode fiber

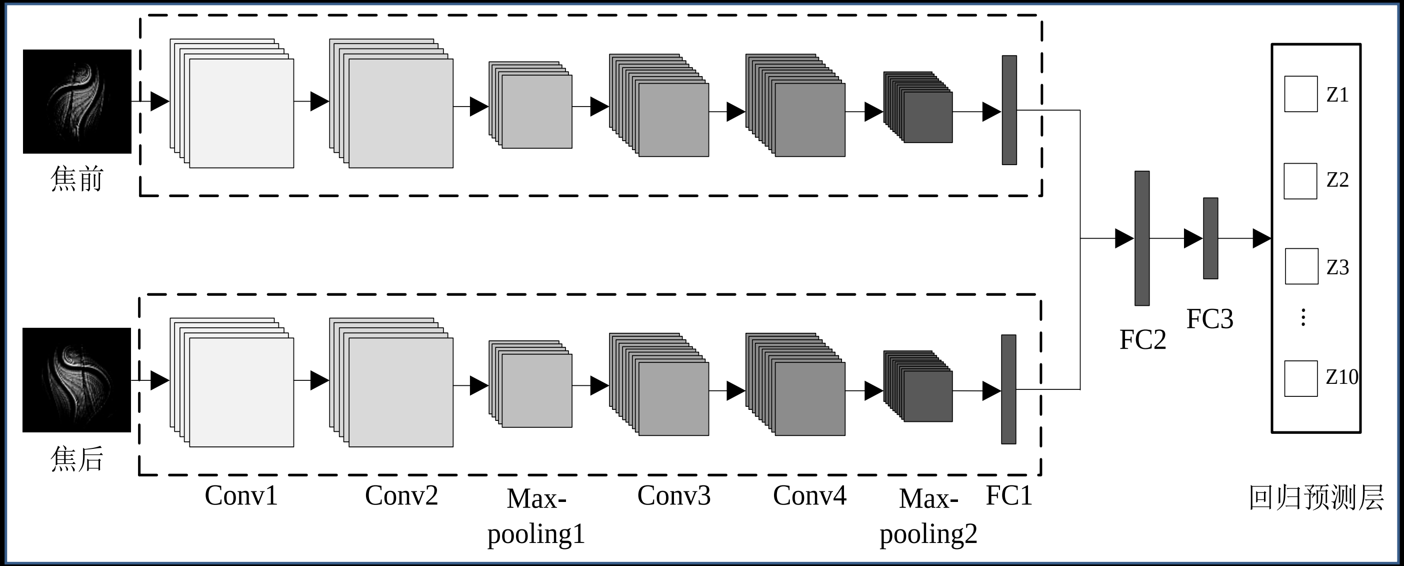
☑ Further improving the filtering technology

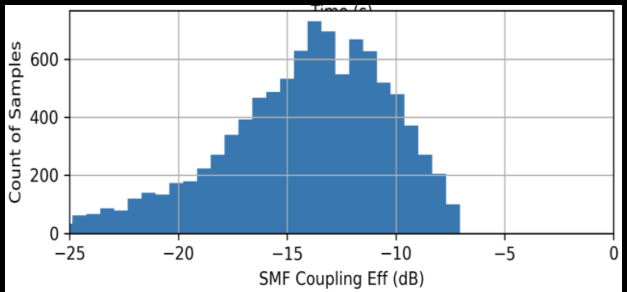
Recent progress on the adaptive optics (AO)

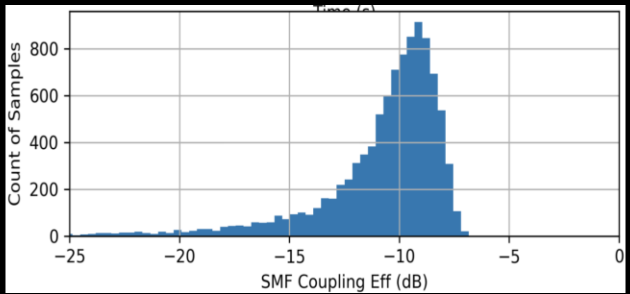
- ✓ Without wavefront detection for low cost
- ✓ Using SPDG and Deep Learning



Test performance of our developed AO over 10-km freespace channel in Shanghai

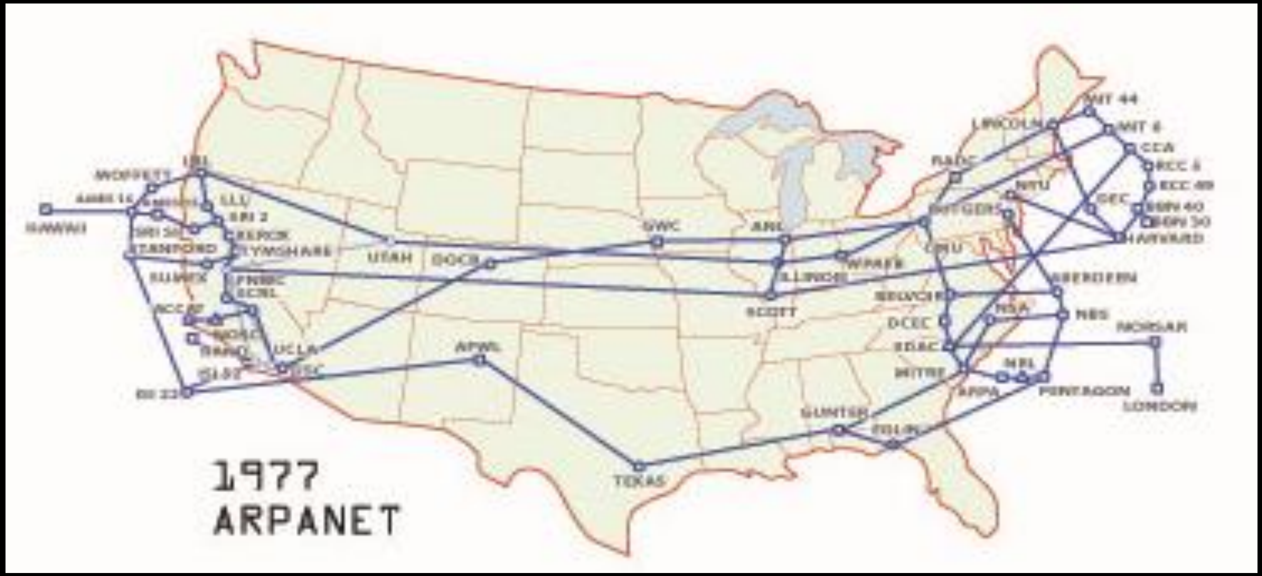


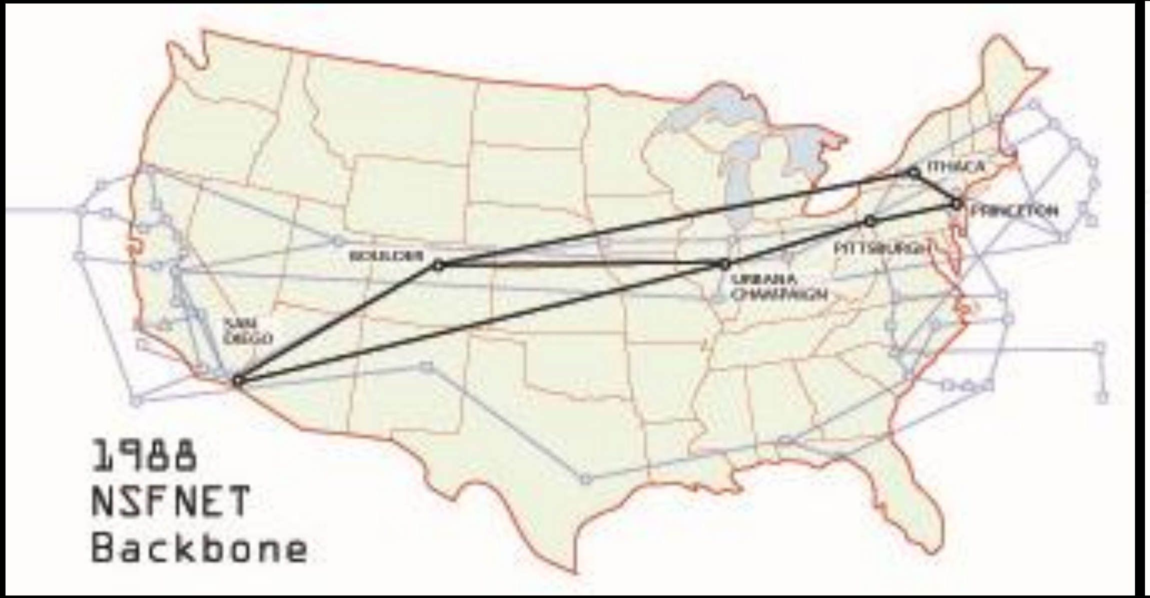




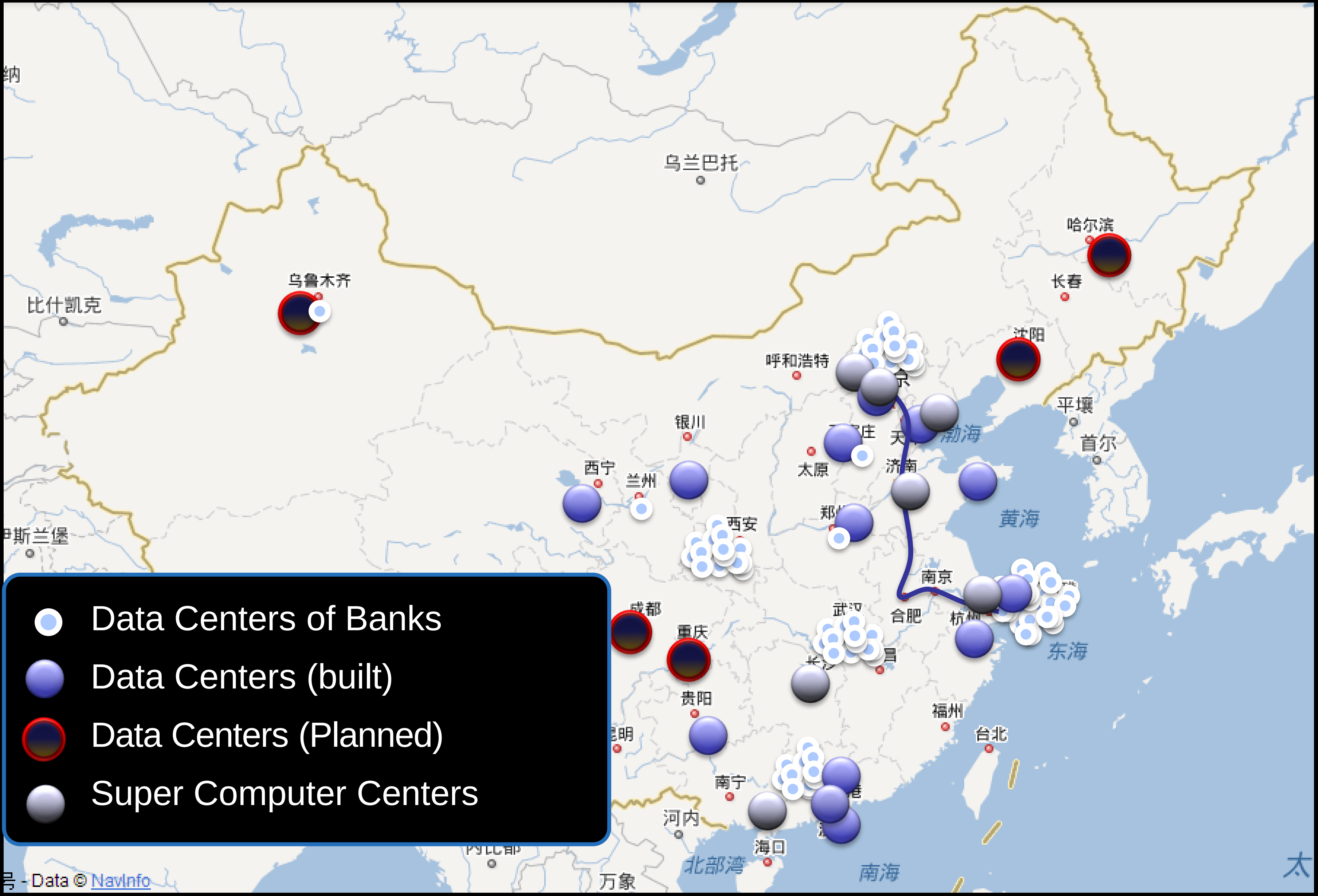
The SMF coupling eff. is increased by ~ 6 dB at 10-km freespace channel when using AO

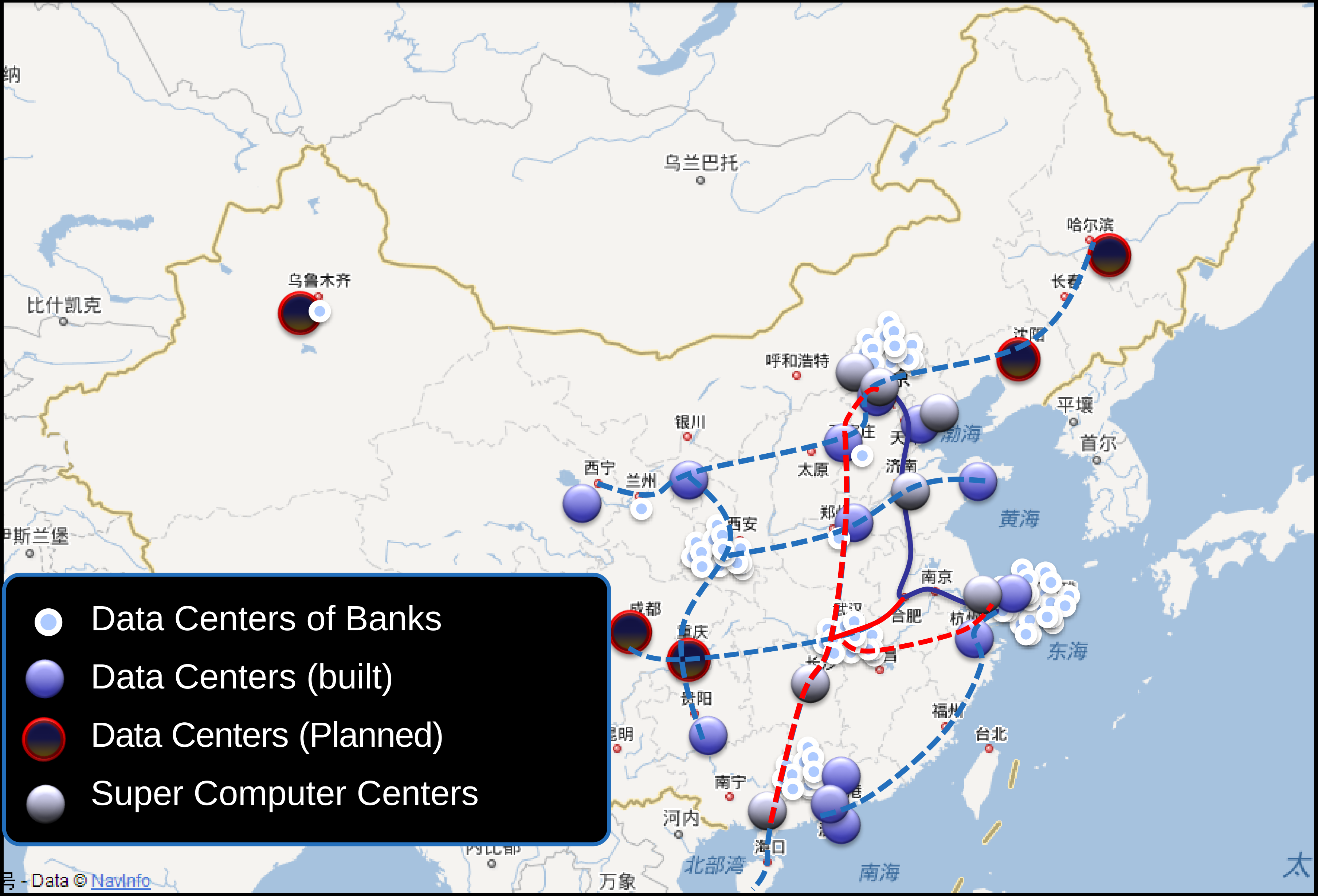

SRI
UTAH
UCSB
UCLA
1969
ARPANET


LINCOLN
RADC
NYU
RUTGERS
CMU
HARVARD
ABERDEEN
NBS
NSA
NORSAR
DCEC
MITRE
NRL
PENTAGON
LONDON
GUNTER
EGLIN
TEXAS
UCLA
UTAH
GWC
ANL
ILLINOIS
SCOTT
STANFORD
TYMSHARE
HAWAII
1977
ARPANET

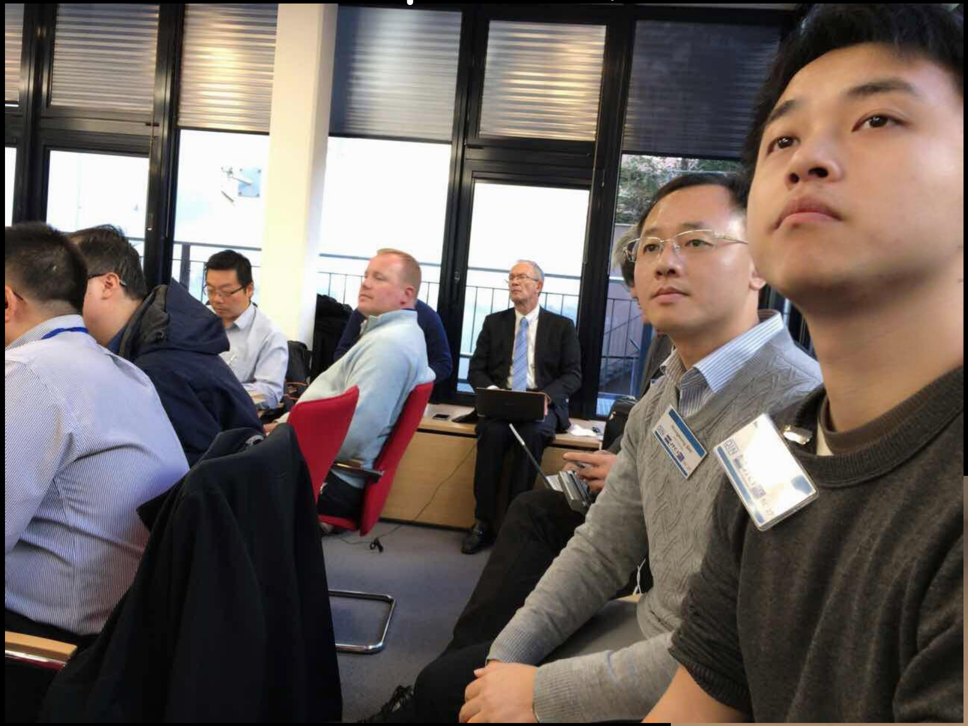

ITHACA
PRINCETON
PITTSBURGH
BOULDER
URBANA CHAMPAIGN
SAN DIEGO
1988
NSFNET
Backbone


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 (built)
Data Centers (Planned)
Super Computer Centers
乌兰巴托
哈尔滨
长春
乌鲁木齐
比什凯克
呼和浩特
平壤
首尔
银川
太原
渤海
西宁
兰州
黄海
西安
南京
合肥
成都
重庆
东海
贵阳
福州
台北
南宁
河内
海口
北部湾
南海
万象
Data © NavInfo


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

Future Prospect: QKD standardization



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

Standardization on Quantum Key Distribution

- **2008-2018:** ETSI ISG QKD founded in 2008, and has published 6 specifications: use case, application interface, security proof, module security, optical components, etc.
- **2019~:** the progress is accelerated with 3 more specifications released: QKD vocabulary, deployment parameters, key delivery interface.

ETSI	Specification/Report	Publish date
GS QKD 002	Quantum Key Distribution (QKD); Use Cases	Jun-10
GR QKD 003	Quantum Key Distribution (QKD); Components and Internal Interfaces	Mar-18
GS QKD 004	Quantum Key Distribution (QKD); Application Interface	Dec-10
GS QKD 005	Quantum Key Distribution (QKD); Security Proofs	Dec-10
GR QKD 007	Quantum Key Distribution (QKD); Vocabulary	Dec-18
GS QKD 008	Quantum Key Distribution (QKD); QKD Module Security Specification	Dec-10
GS QKD 010	Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems	Drafting
GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems	May-16
GS QKD 012	Quantum Key Distribution (QKD) Device and Communication Channel Parameters for QKD Deployment	Feb-19
GS QKD 013	Quantum Key Distribution (QKD); Characterisation of Optical Output of QKD transmitter modules	Drafting
GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of key delivery API to Applications;	Feb-19
GS QKD 015	Quantum Key Distribution (QKD); Quantum Key Distribution Control Interface for Software Defined Networks	Drafting

Standardization on Quantum Key Distribution

- **2017:** The study item "Security requirements, test and evaluation methods for quantum key distribution" was initiated
- **2019:** Study period was finished and new work item ISO/IEC 23837 (Part 1&2) was approved and initiated

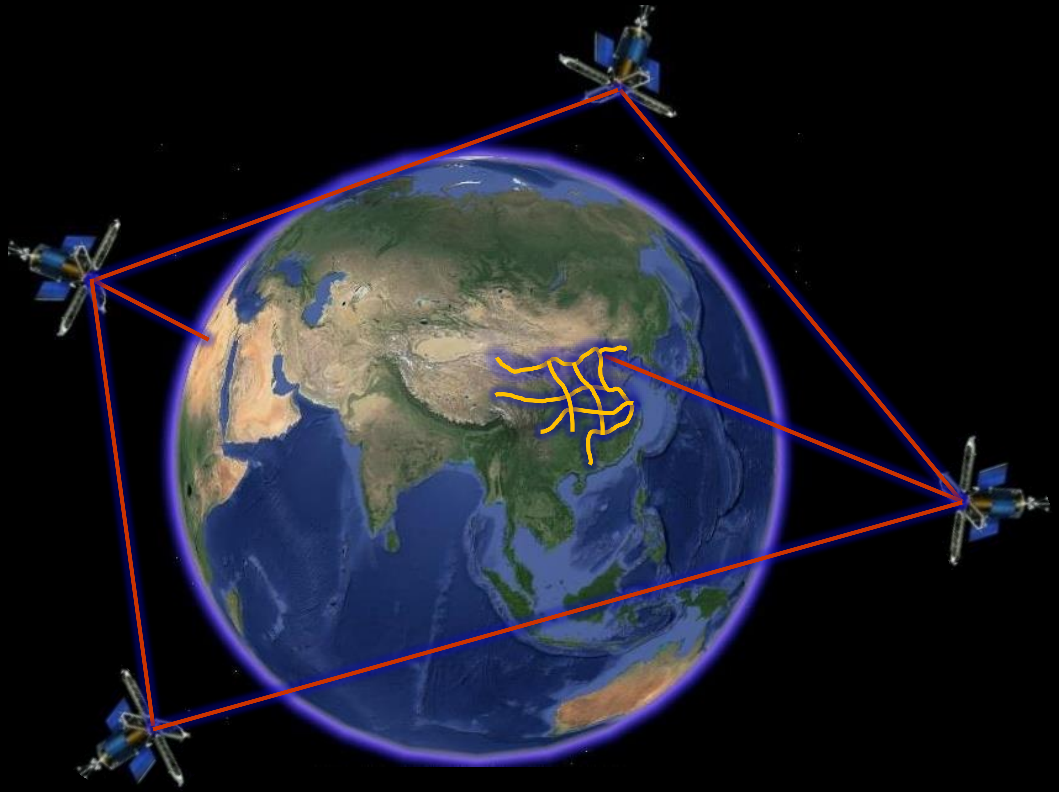
ISO/IEC	Standard/Report	Status
Study Period	Security requirements, test and evaluation methods for quantum key distribution	Finished
ISO/IEC 23837-1	Security requirements, test and evaluation methods for quantum key distribution Part 1: requirements	Ongoing
ISO/IEC 23837-2	Security requirements, test and evaluation methods for quantum key distribution Part 2: test and evaluation methods	Ongoing

Standardization on Quantum Key Distribution

- **2018:** SG 13 (future network) initiated new work item (WI) on QKD network framework; SG17(Security) initiated study on QKD network security framework and WI on quantum random number generator architecture.
- **2019:** SG13 initiated 2 WIs on QKD network architecture and key management; SG17 initiated 3 WIs on QKD network security requirements

ITU-T	Recommendation/Report	Status
Y.QKDN_FR	Framework for Networks to supporting Quantum Key Distribution	Drafting
Y.QKDN_Arch	Functional architecture of the Quantum Key Distribution network	Drafting
Y.QKDN_KM	Key management for Quantum Key Distribution network	Drafting
X.qrng-a	Quantum Noise Random Number Generator Architecture	Drafting
X.sec_QKDN_ov	Security Requirements for QKD Networks - Overview	Drafting
X.sec_QKDN_km	Security Requirements for QKD Networks - Key Management	Drafting
X.cf_QKDN	The use of cryptographic functions on a key generated by a Quantum Key Distribution networks	Drafting
TR.sec_QKD	Security framework for Quantum Key Distribution in Telecom network	Drafting

Future Prospect



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

Quantum Secure Every Bit

Thanks for your attention!