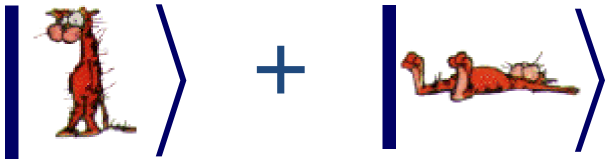
Quantum Leap: From Tests of Quantum Foundations to New Quantum Technologies

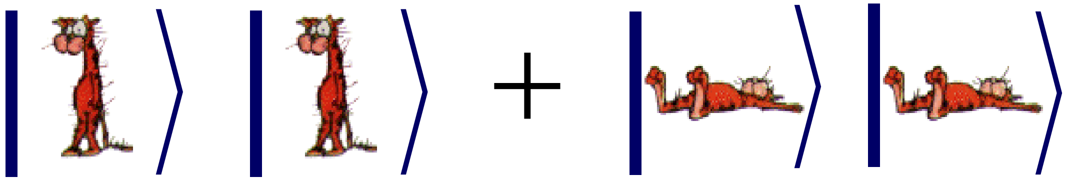
Jian-Wei Pan
CAS Center for Excellence in Quantum Information and Quantum Physics
University of Science and Technology of China

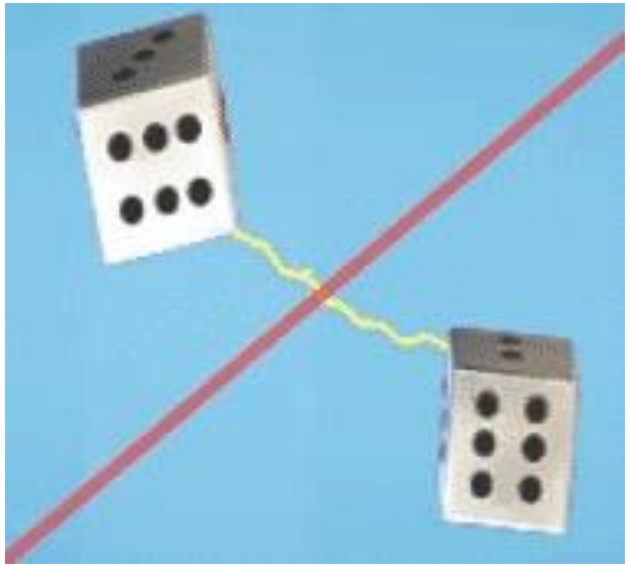
Quantum Superposition and Quantum Entanglement

Classical Physics: “bit”  or 

Quantum Physics: “qubit” 

Quantum entanglement:

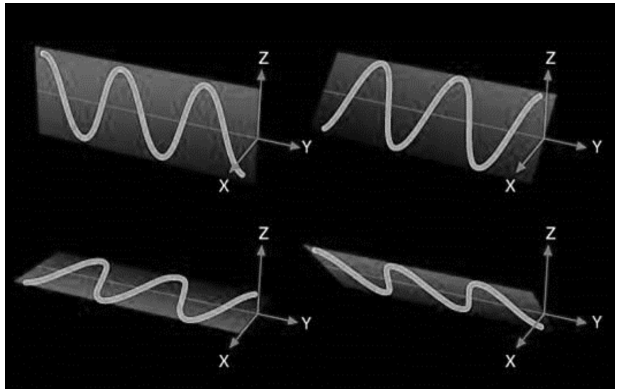




Albert Einstein: Spooky action at a distance

Quantum Superposition and Quantum Entanglement

One bit of information per photon (encoded in polarization)



$|H\rangle = |0\rangle$

$|V\rangle = |1\rangle$

Qubit: $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle, |\alpha|^2 + |\beta|^2 = 1$

Bell states – maximally entangled states:

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2)$$

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2)$$

Spooky Action at a Distance?

Entangled pair

Einstein believed that :

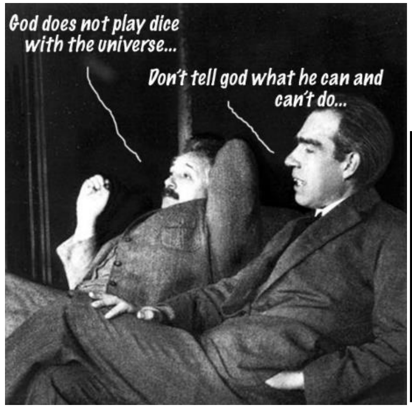
- The outcome of a measurement on any physical system is determined prior to and independent of the measurement
- the outcome cannot depend on any actions in space-like separated regions

A seemingly reasonable assumptions of "local realism"

Quantum mechanics predicts that:

- Initially, the individual states of two particles are not identified
- The measurement outcome on particle A will not only determine its state, but also the state of particle B immediately!

Spooky Action at a Distance?



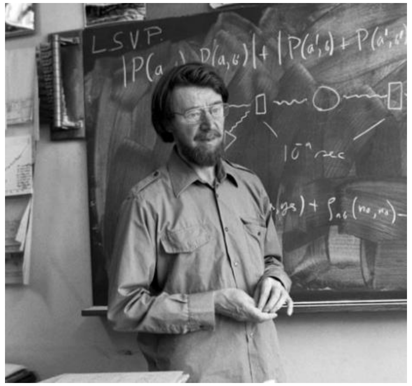
A philosophical argument

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

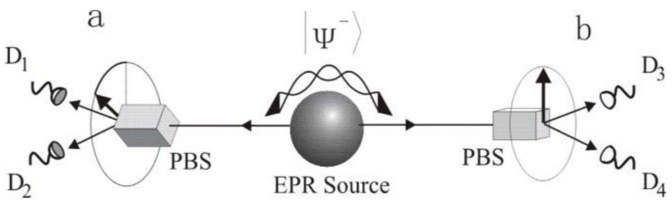
Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)



Experimental testable inequality: Bell, Physics 1, 195 (1964)



$S = |E(\phi_A\phi_A) - E(\phi_A\phi'_B) + E(\phi'_A\phi_B) + E(\phi'_A\phi'_B)|$

- Einstein's local realism: $S_{\max} \le 2$
- Quantum mechanics: $S_{\max} = 2\sqrt{2}$

Experimental tests

- Clauser *et al.*, PRL 28, 938 (1972)
- Zeilinger *et al.*, PRL 81, 5039 (1998)
- Aspect *et al.*, PRL 47, 460 (1981)
- Hensen *et al.*, Nature 526, 682 (2015)

Quantum mechanics is right! But still with loopholes…

Bell's Inequality: Testing the Battle

Instruments may "cheat"?

☒ Freedom of choice loophole: random number generators could be prior correlated ➡ the choice of measurement bases are not truly random

Brunner *et al.*, RMP 86, 419 (2014)

Schrödinger's cat

☒ Collapse locality loophole: measurement outcome is not defined until it is registered by a human consciousness ➡

Realized "events" have never been space-like separated

Kent, PRA 72, 012107 (2005)

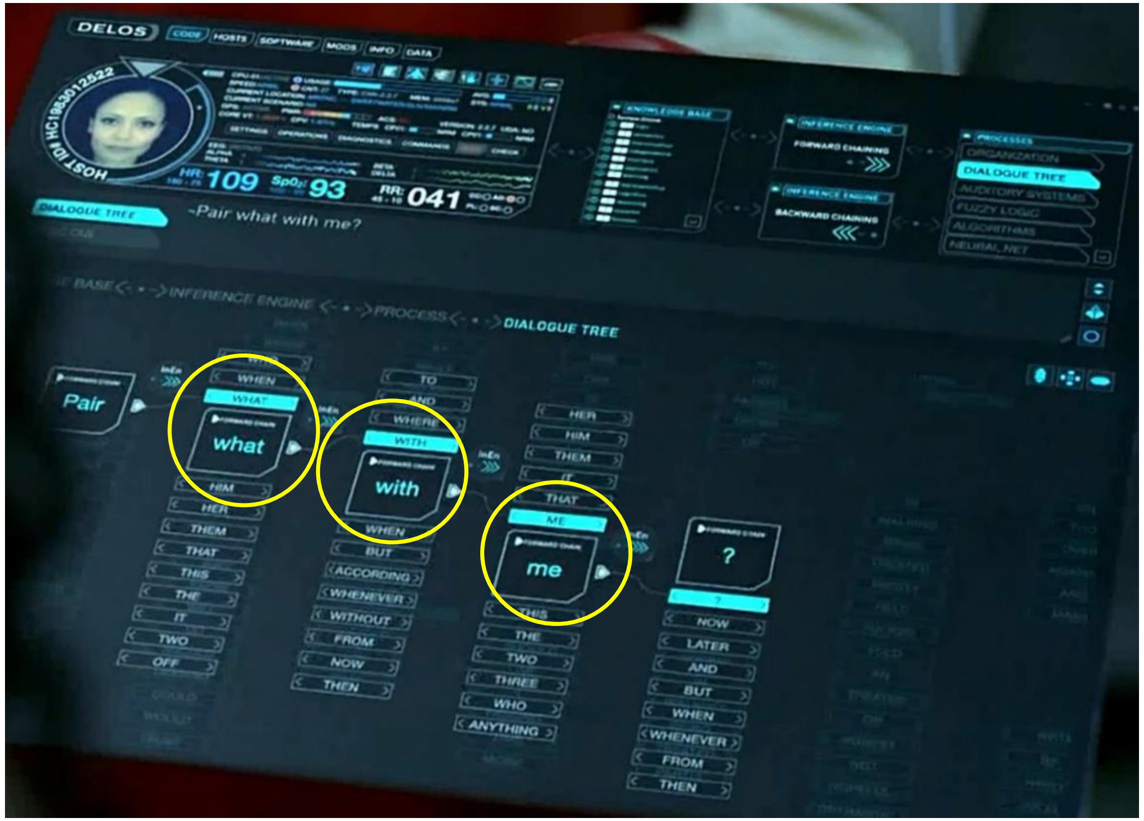
Leggett, Compendium of Quantum Physics (Springer, 2009)

Solution: Bell-test experiment with human-observer!

Why need human-observer?

Though in "Westworld" : AI "thinks" she has free consciousness

☒ Her every actions in future have been indeed priori determined by the remote control station……



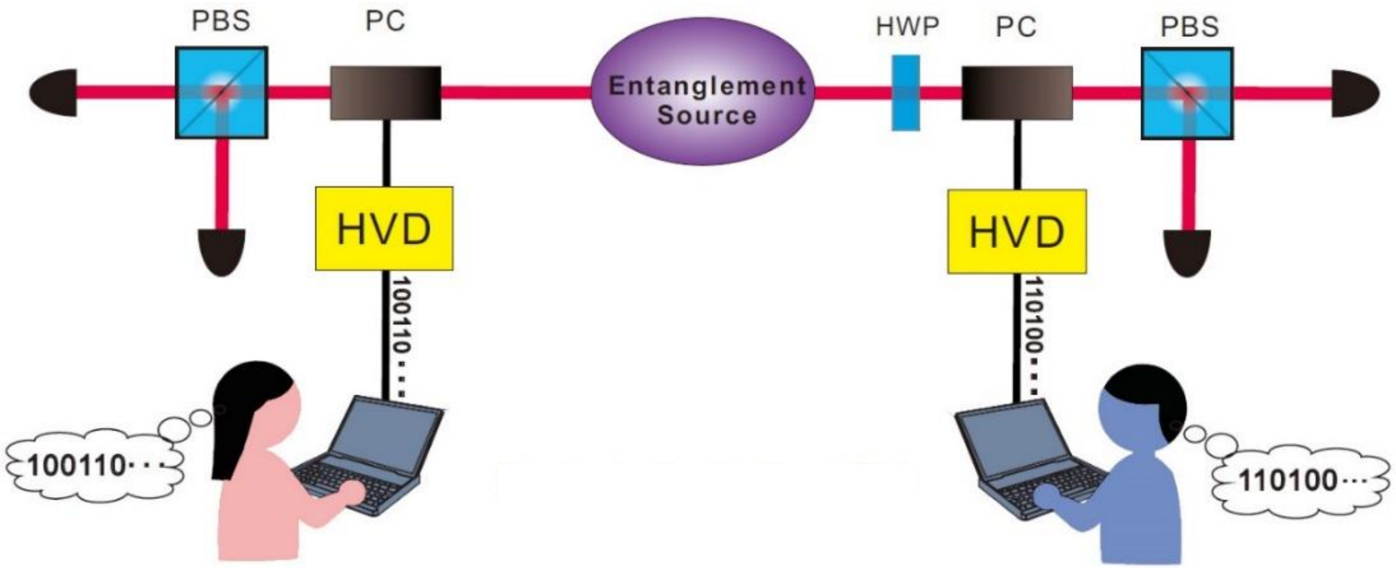
Bell's Inequality: Testing the Battle

☑ Basis choice by free will

☑ Measurement outcomes defined by consciousness

Kent, PRA 72, 012107 (2005)

Leggett, Compendium of Quantum Physics (Springer, 2009)



Requirement:

Quantum signal transit time exceeds human reaction (100ms) ➡ entanglement distribution at a distance on the order of one light-second (e. g., between Earth and Moon, 1.28 ls)

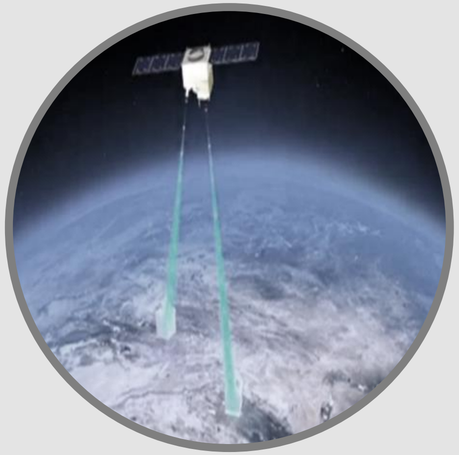
Quantum Information Processing (QIP)

Test of quantum nonlocality

Coherent manipulation of quantum systems

Quantum information processing

Unconditional security



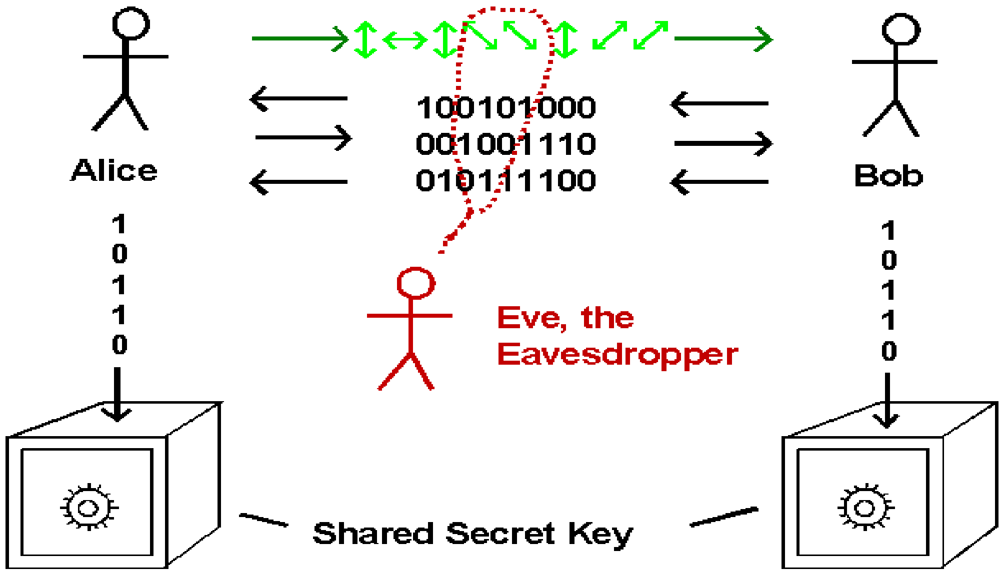
Quantum communication

Computational capacities

Quantum computation and simulation

Quantum Key Distribution (QKD)

- Single-photon-based key distribution: [Bennett & Brassard 1984 protocol]



Unconditional secure in principle

Any eavesdropping will be detected

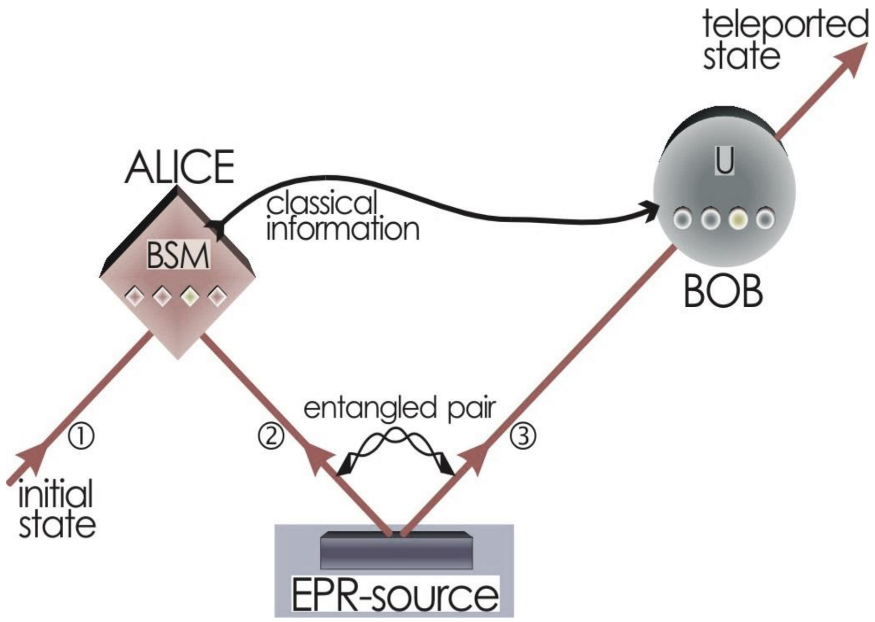
➡ Secure key!

One-time pad encryption

➡ Unhackable!

- Entanglement-based key distribution: [Ekert, PRL 67, 661 (1991)]

Quantum Teleportation



Bennett *et al.*, PRL 70, 1895 (1993)

Initial state

$$|\Phi\rangle_1 = \alpha |H\rangle_1 + \beta |V\rangle_1$$

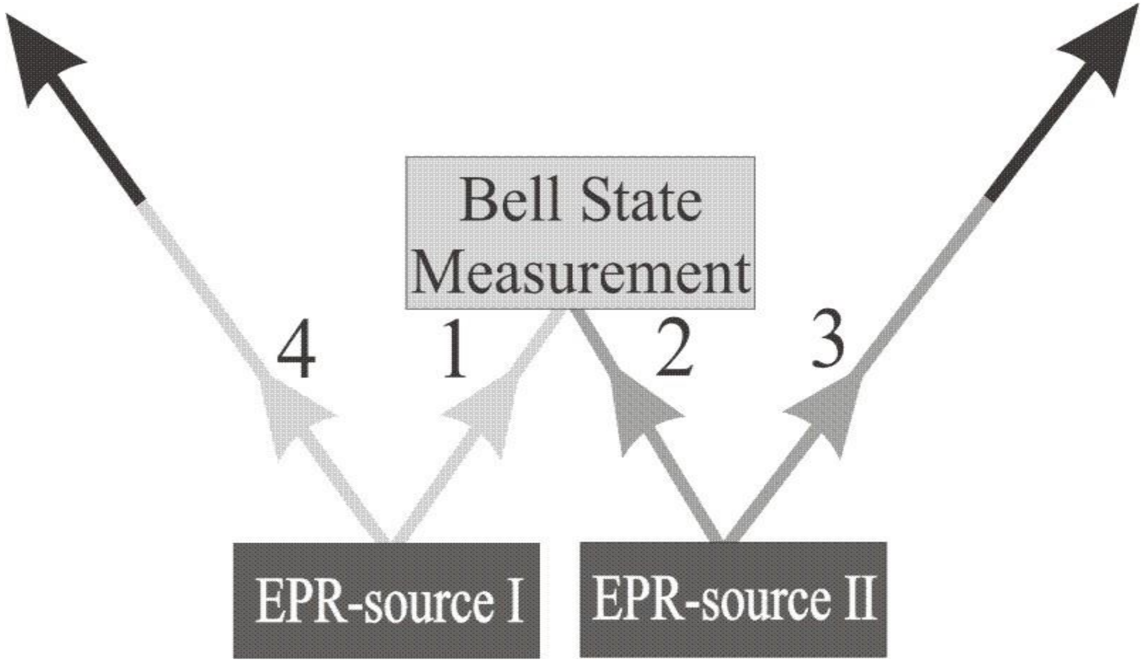
The shared entangled pair

$$|\Phi^+\rangle_{23} = \frac{1}{\sqrt{2}}\left(|H\rangle_2 |H\rangle_3 + |V\rangle_2 |V\rangle_3\right)$$

$$\begin{aligned}
|\Psi\rangle_{123} &= |\Phi\rangle_1 \otimes |\Phi^+\rangle_{23} \\
&= |\Phi^+\rangle_{12} \otimes \left(\alpha |H\rangle_3 + \beta |V\rangle_3\right) + \\
&\quad |\Phi^-\rangle_{12} \otimes \left(\alpha |H\rangle_3 - \beta |V\rangle_3\right) + \\
&\quad |\Psi^+\rangle_{12} \otimes \left(\alpha |V\rangle_3 + \beta |H\rangle_3\right) + \\
&\quad |\Psi^-\rangle_{12} \otimes \left(\alpha |V\rangle_3 - \beta |H\rangle_3\right)
\end{aligned}$$

Essential ingredient for distributed quantum network

Entanglement Swapping



$$|\Psi\rangle_{1234} = |\Phi^+\rangle_{14} \otimes |\Phi^+\rangle_{23}$$

$$= |\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34} + |\Phi^-\rangle_{12} \otimes |\Phi^-\rangle_{34} + |\Psi^+\rangle_{12} \otimes |\Psi^+\rangle_{34} + |\Psi^-\rangle_{12} \otimes |\Psi^-\rangle_{34}$$

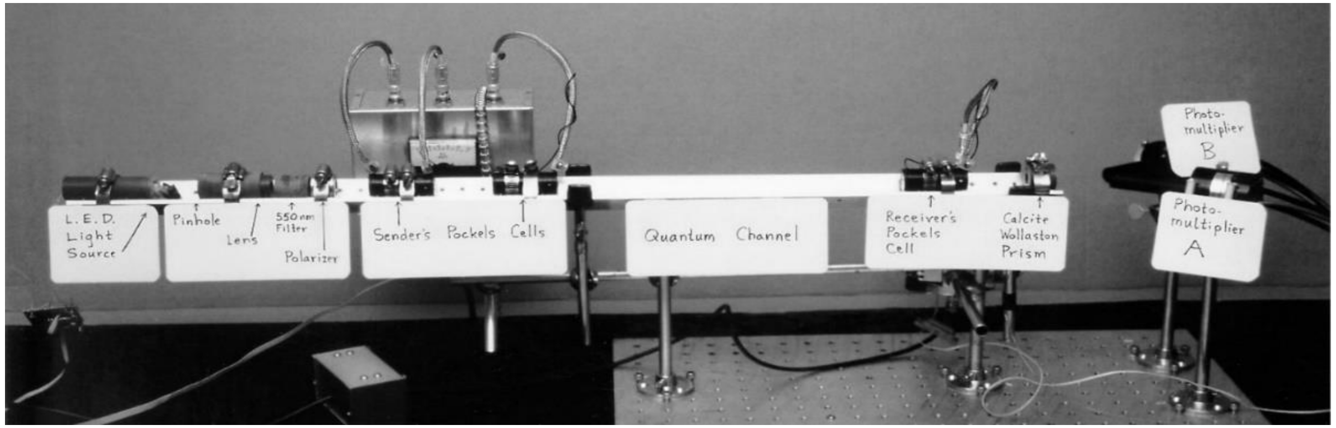
Zukowski *et al.*, PRL 71, 4287 (1993)

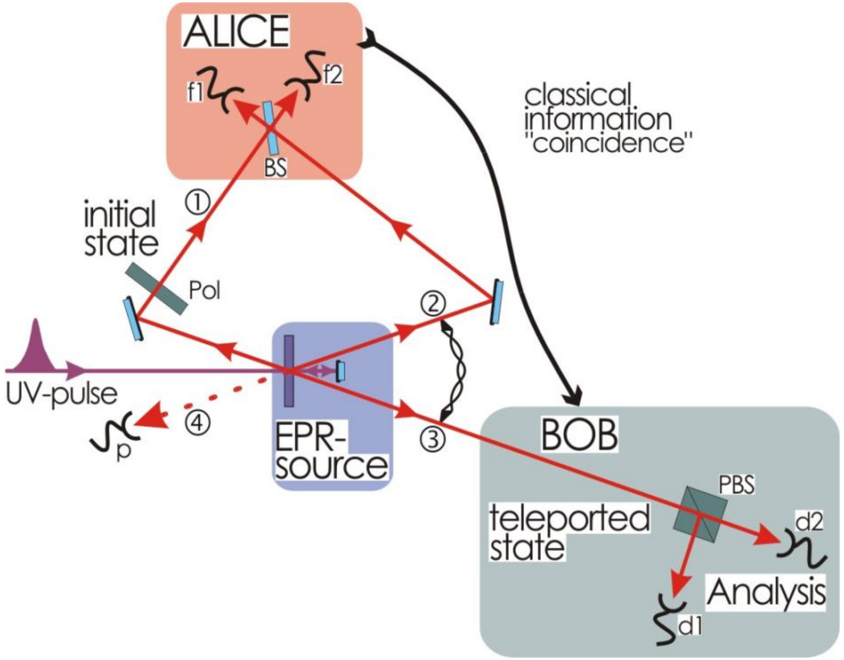
Bennett *et al.*, PRL 70, 1895 (1993)

Proof of Concept Demostrations

First demonstration of QKD (32 cm)

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





First demonstration of quantum teleportation (~30cm)

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

Security Loophole of QKD with Realistic Devices

Probabilistic quasi single photon: weak coherence pulse

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

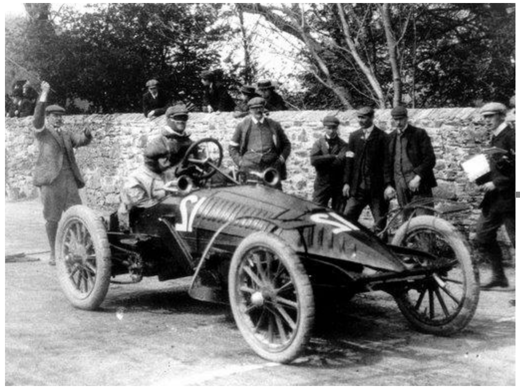
Eavesdrop the keys with two photon events (Photon number splitting attack)

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

Lütkenhaus, PRA 61, 052304 (2000)

Due to imperfect single-photon source:

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



~10km

If so, why we need QKD?

Challenges for Large-scale Secure Quantum Communication

Security ?

Long distance ?

Applications ?

- ☒ Absorption ➡ photon loss
- ☒ Decoherence ➡ degrading entanglement quality
- ☒ Probabilistic entangled photons and single photon source ➡ exponential resource cost

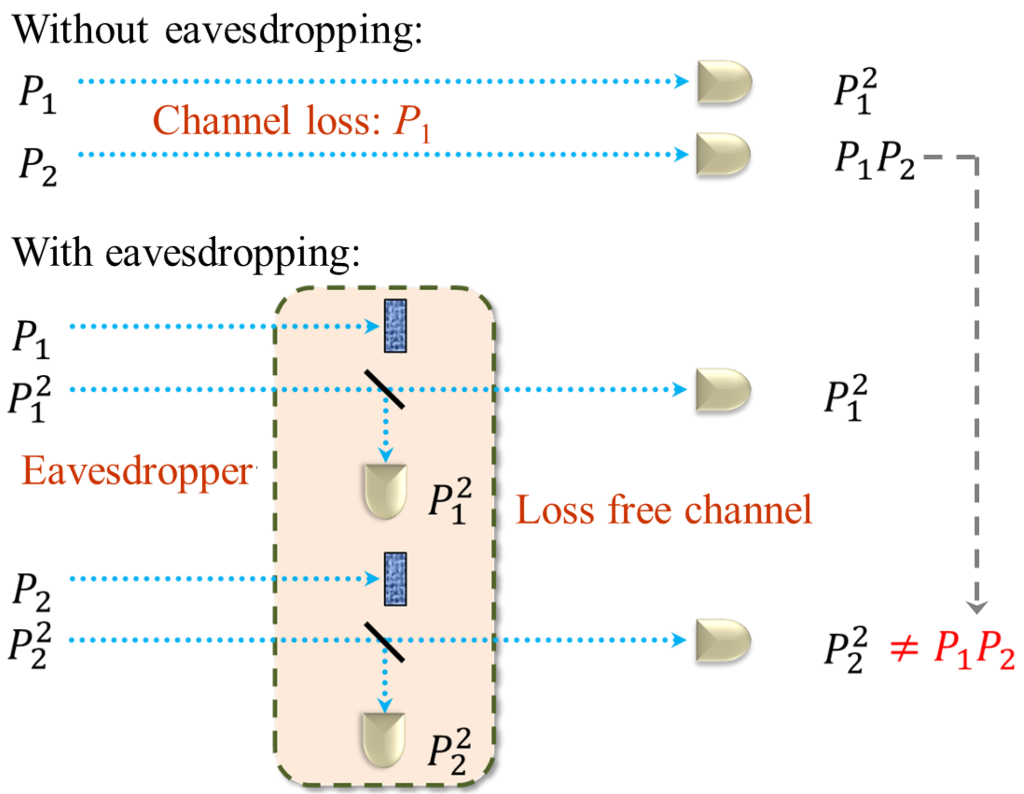
For 1000 km commercial fiber, even with a perfect 10 GHz single-photon source and ideal detectors, only 0.3 photon can be transmitted on average per century!

Security of QKD with Realistic Devices

Solution to imperfect single-photon source:

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

- Hwang, PRL 91, 057901(2003)
- 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)

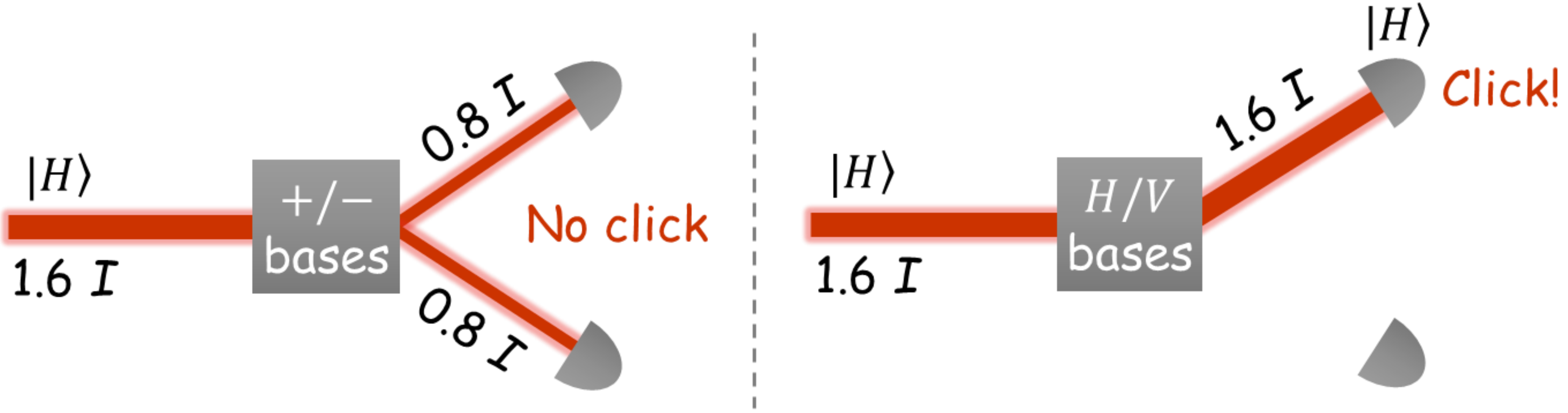
200km:

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

Security of QKD with Realistic Devices

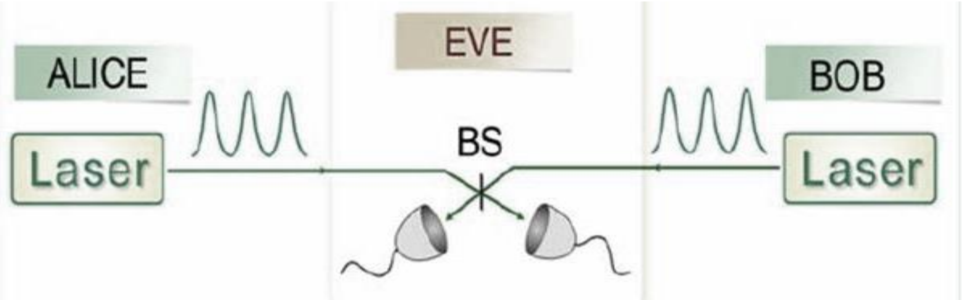
NEW found security loophole : imperfect single-photon detectors

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 (MDI) QKD: immune to any attack on detection [Scheme: Lo *et al.*, PRL 108, 130503 (2012)]



Requirement: 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)

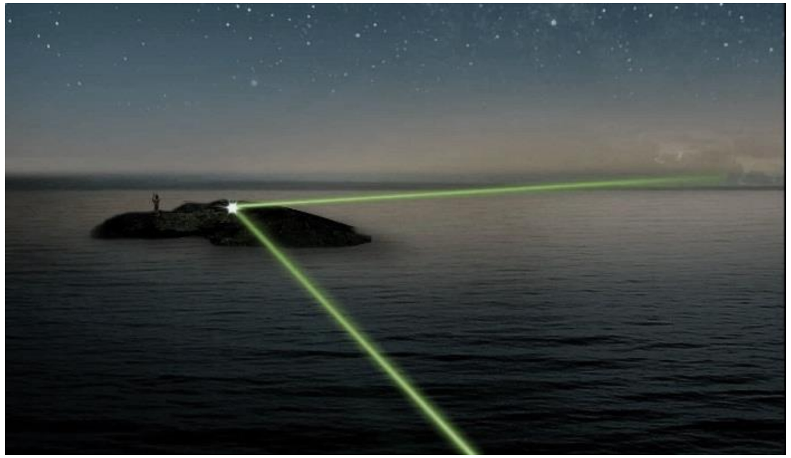
Extended distance:

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

Information-theoretically secure QKD with realistic devices can be achieved!

Towards Long-distance Quamtum Communication

- Longest distance of MDI-QKD in fiber: ~400km
  - Yin *et al.*, PRL 117, 190501 (2016)
- Longest distance of quantum teleportation: ~100km
  - Yin *et al.*, Nature 488, 185 (2012), by Chinese group
  - Ma *et al.*, Nature 489, 269 (2012), by Austrian group



Solution: Quantum Repeater

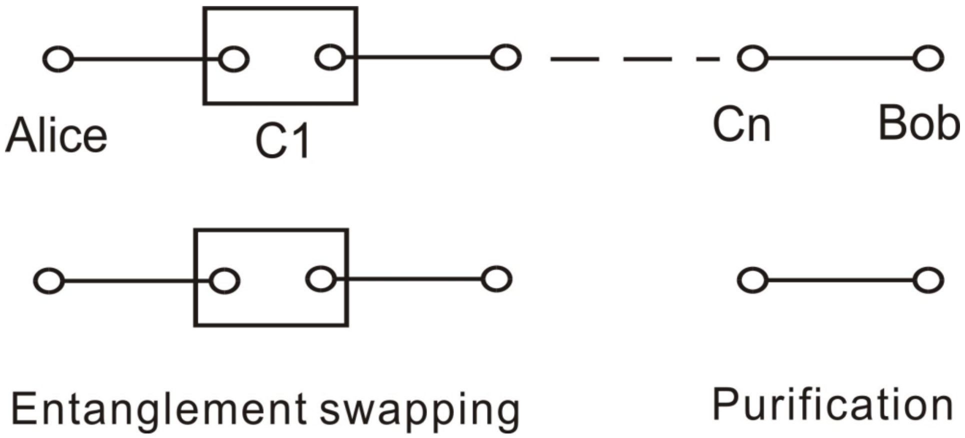
Solution to photon loss: Entanglement swapping !

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

Solution to decoherence: Entanglement purification!

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

Deutsch *et al.*, PRL 77, 2818 (1996)

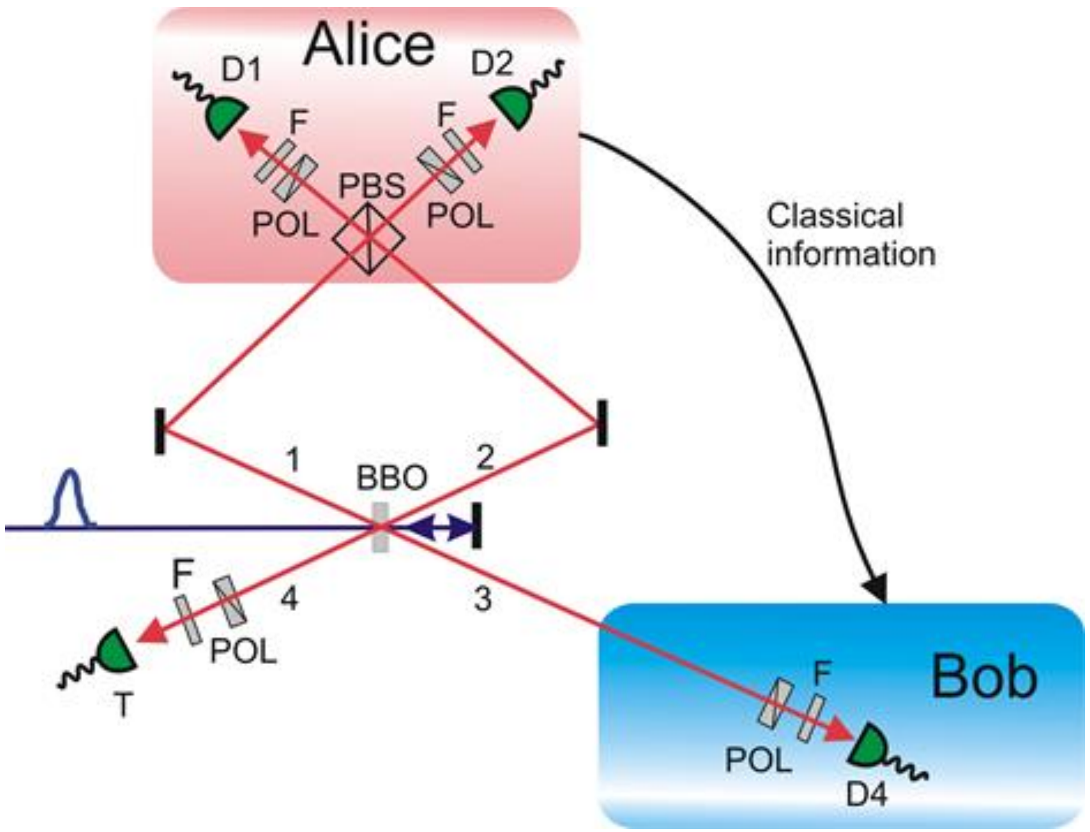


Require

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

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

High Precision Entanglement Swapping



First demonstration with beam splitter

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

High precision fault-tolerable entanglement swapping

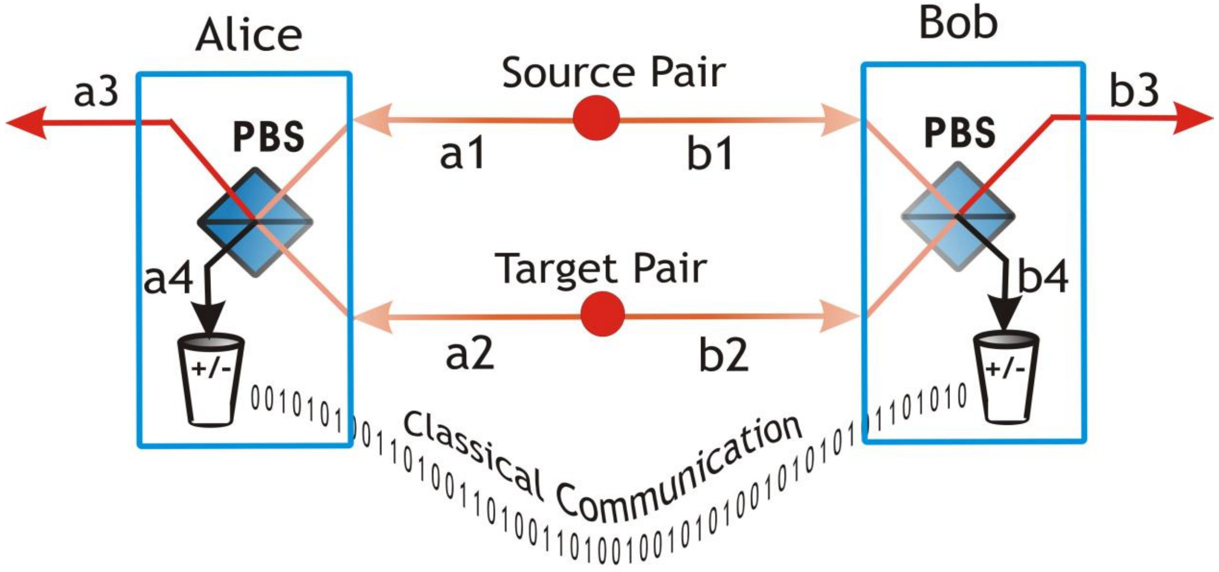
Pan *et al.*, Nature 421, 721 (2003)

High Precision Entanglement Purification

☒ Original entanglement purification scheme requires CNOT operation between independent particles

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

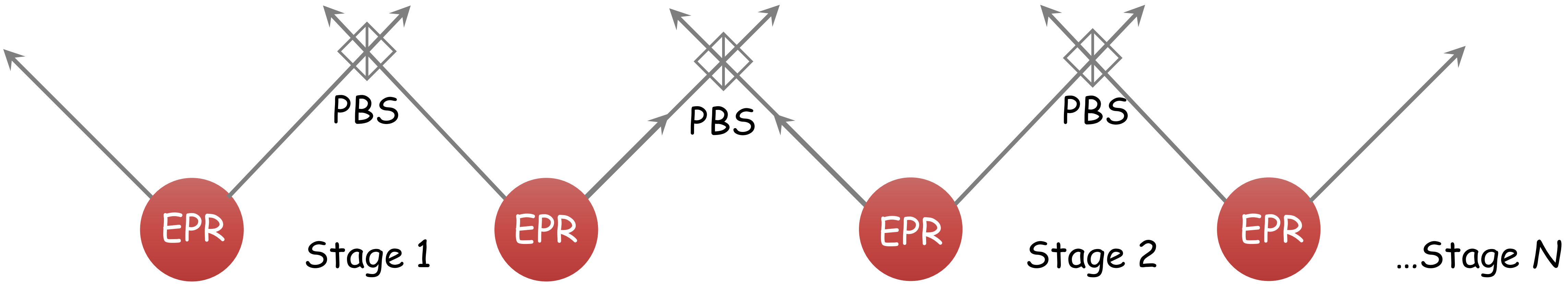
Pan *et al.*, Nature 410, 1067 (2001)



☑ High precision fault-tolerable entanglement purification

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

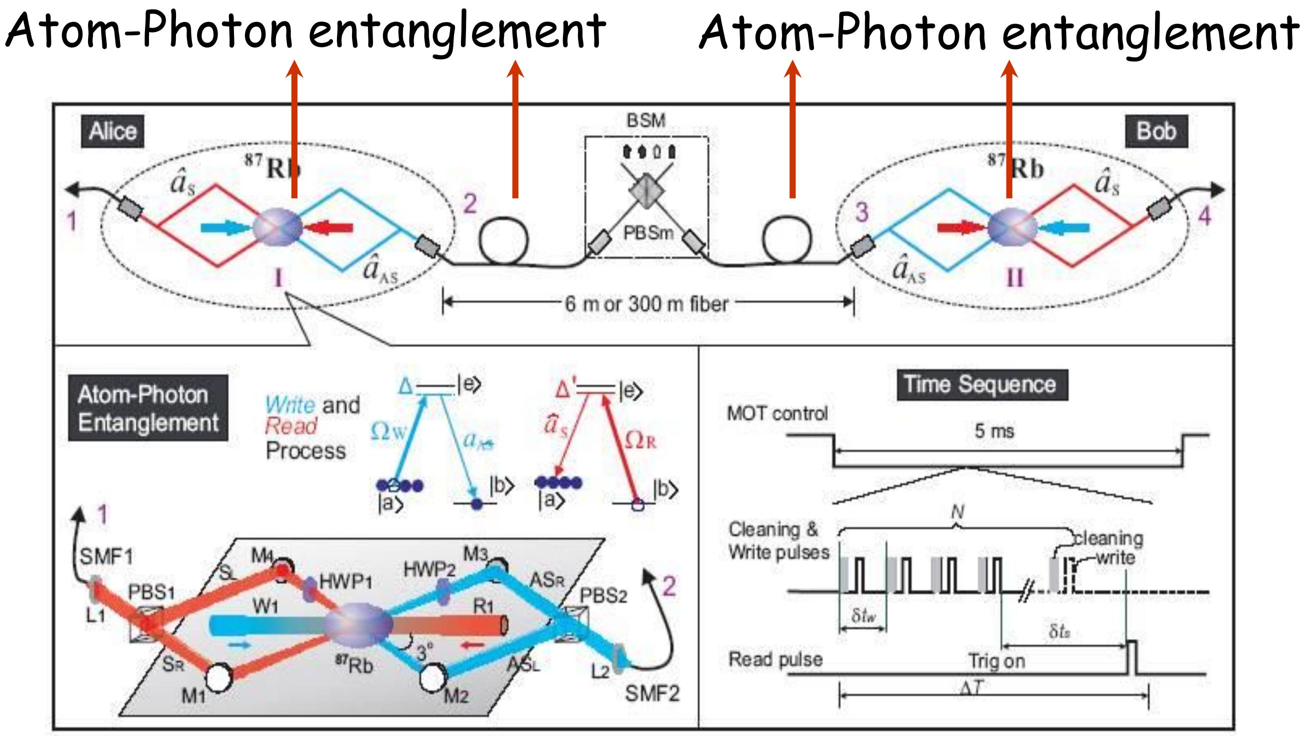
Quantum Memory



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

➡ Efficient distribution of quantum entanglement between distant locations

Quantum Repeater Nodes



Robust BDCZ quantum repeater with atomic quantum memories

- Scheme: Zhao *et al.*, PRL 98, 240502 (2007)
- Experiment: Yuan *et al.*, Nature 454, 1098 (2008)

Other approaches from the groups of Kimble, Kuzmich, Lukin, Harris, Polzik etc.

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

Efficient and Long-lived Quantum Memory

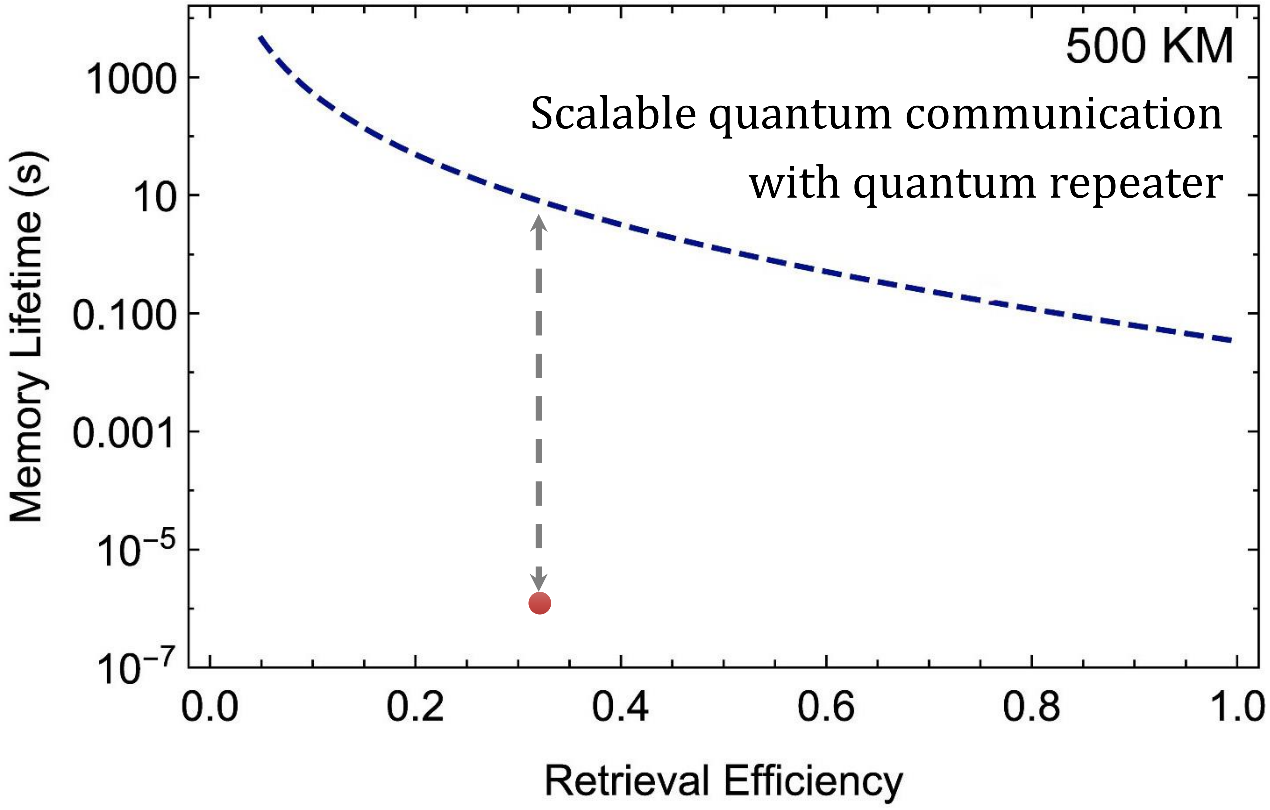
Long lifetime: storage time must be long enough to ensure every node creates an entangled pair

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

In 2008 experiment,

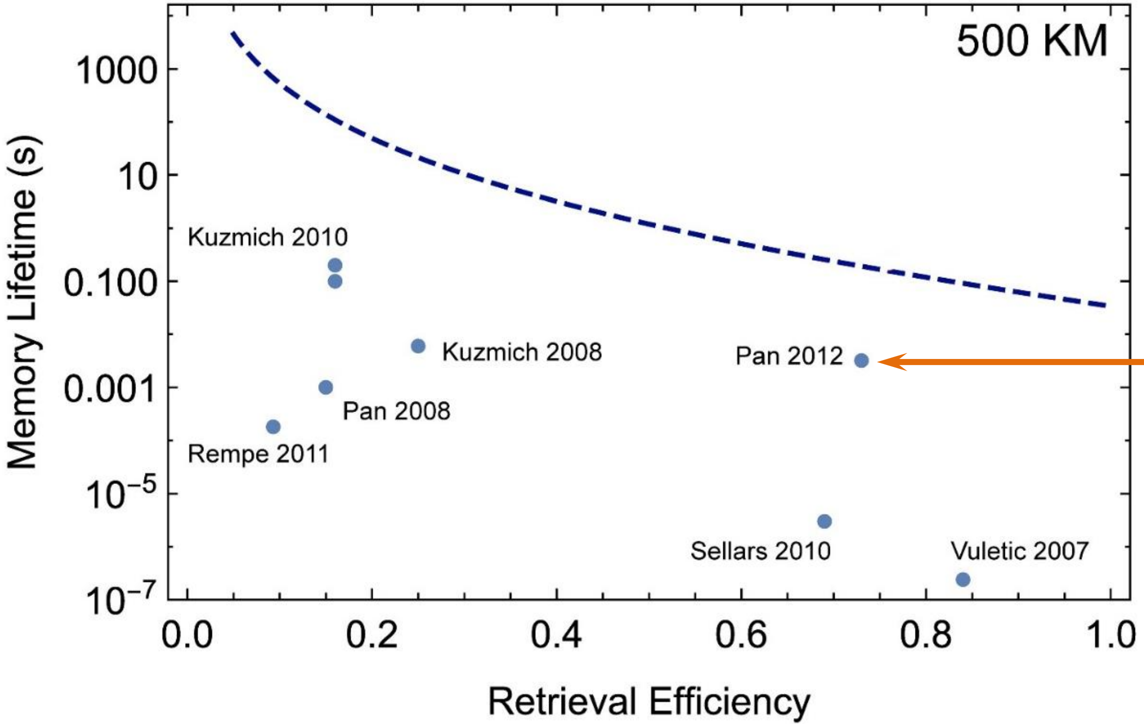
- Life time: 1μs
- Retrieve efficiency: 35%

Require lifetime to be extended about 8 orders of magnitude!



Efficient and Long-lived Quantum Memory

- Clock state: insensitive to magnetic field
- Collinear recoil: minimize phase evolution of spin-wave
- Optical molasses: suppress atomic thermal motion
- Write/Read along the gravity direction: enhance light-atom interaction time
- Ring cavity: increase retrieve efficiency



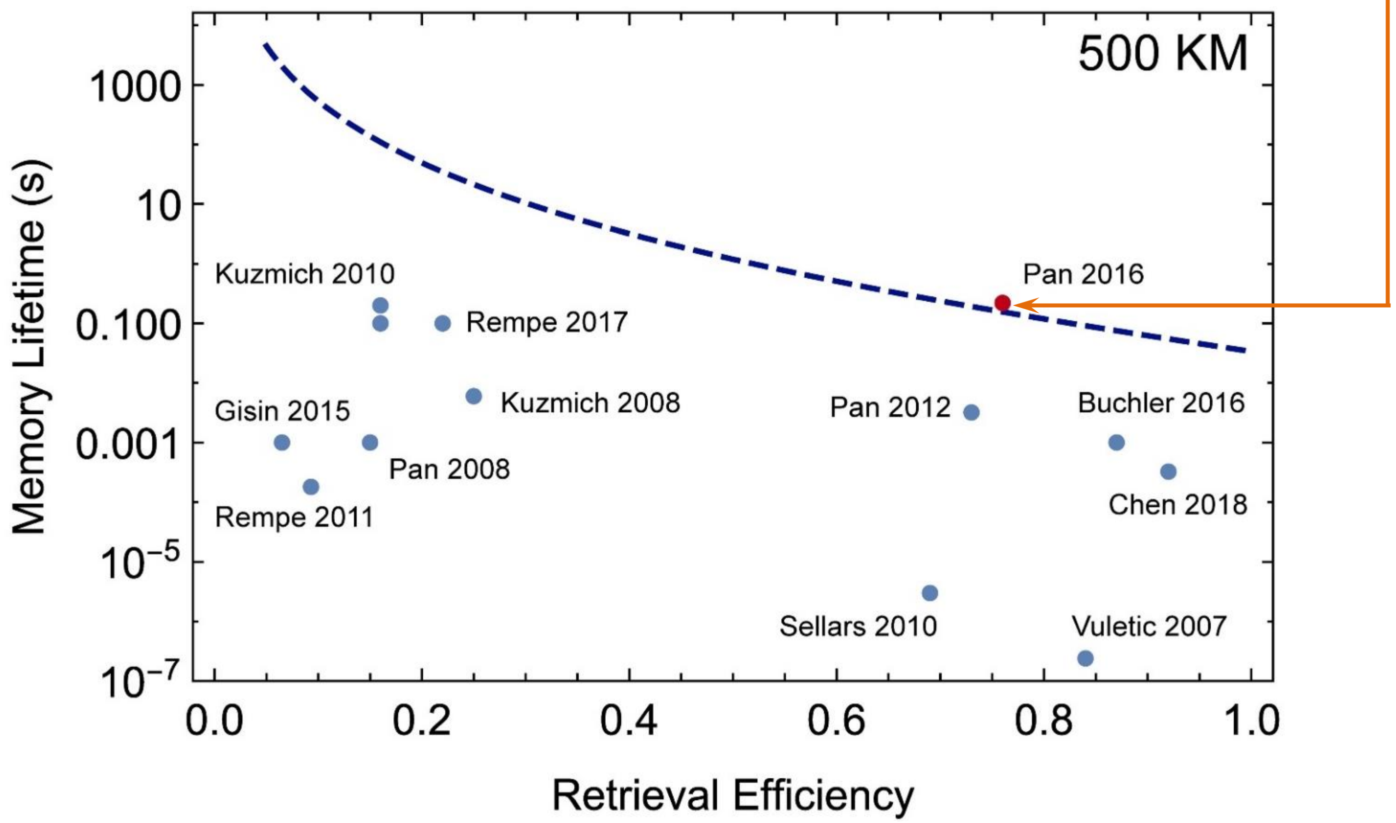
Life time 3ms, retrieve efficiency 73%

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

Require lifetime to be ~2 orders of magnitude

Efficient and Long-lived Quantum Memory

Ring cavity + optical lattice confinement: suppress atomic collision-induced decoherence
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

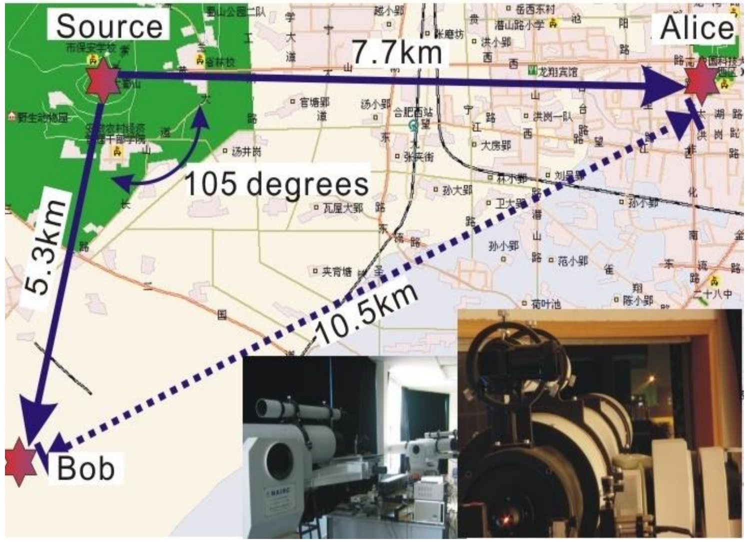
A practical quantum repeater might still need 10 more years

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

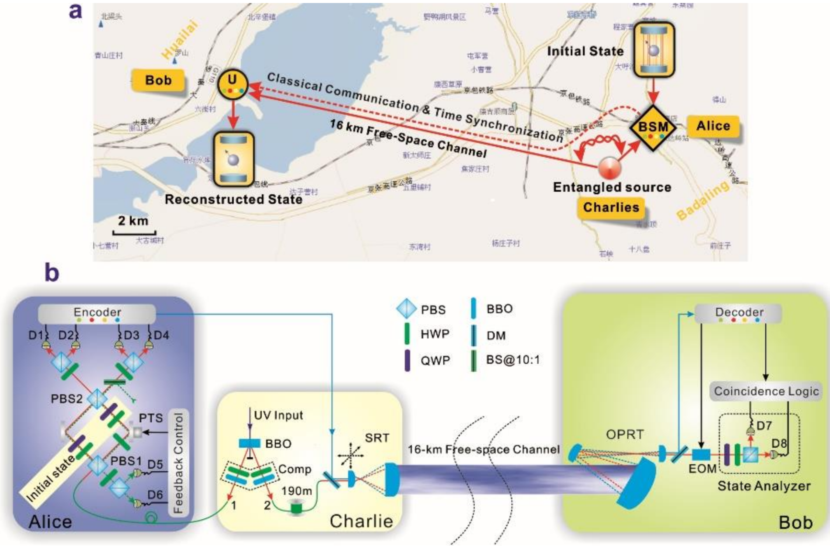
Ground Tests for Satellite-based Quantum Communication

Phase 1: Test the possibility of single photon and entangled photons passing through atmosphere



Free-space quantum entanglement distribution ~13km

Peng *et al.*, PRL 94, 150501 (2005)



Free-space quantum teleportation (16km)

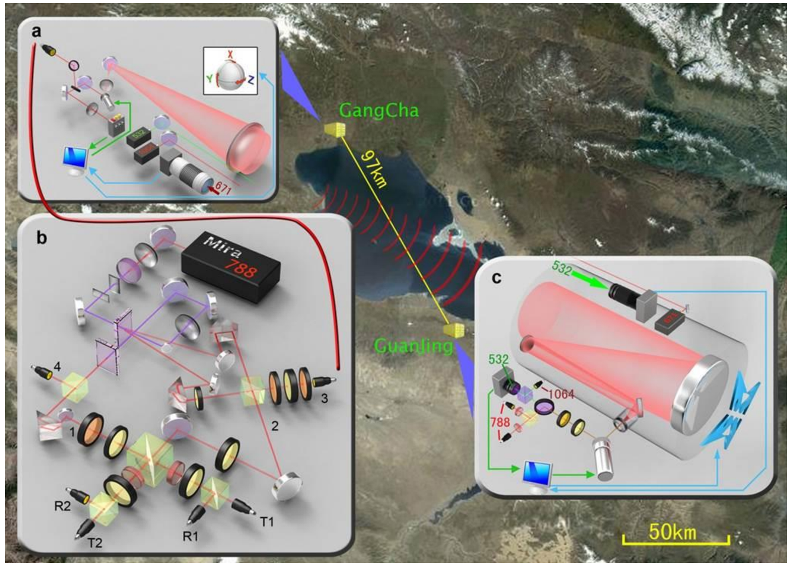
Xin *et al.*, Nature Photonics 4, 376 (2010)

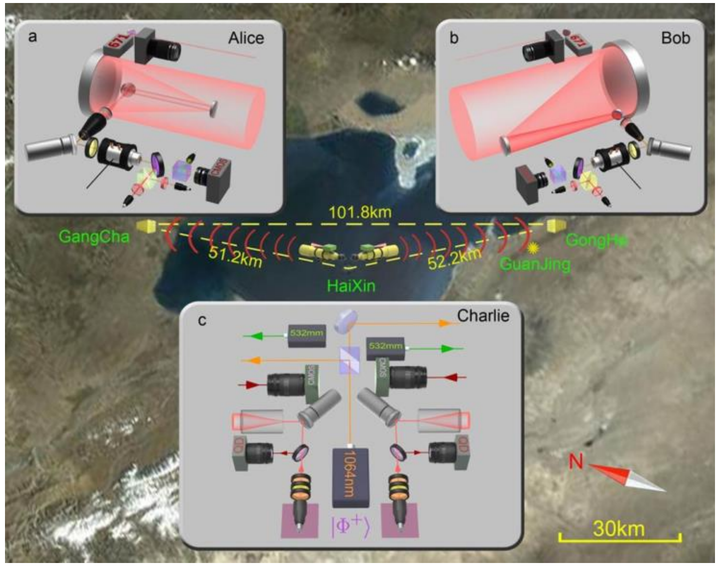
Well beyond the effective thickness of the aerosphere!

Ground Tests for Satellite Quantum Communication

Phase 2: Test the feasibility of quantum communication via high-loss satellite-to-ground channel

Free-Space Quantum Teleportation and entanglement distribution (~100km)





Channel loss: 35-53dB V. S. Loss for an uplink of ground to satellite: 45dB

Channel loss: 66-85dB V. S. Loss for two-downlink between satellite and two ground stations: 75dB

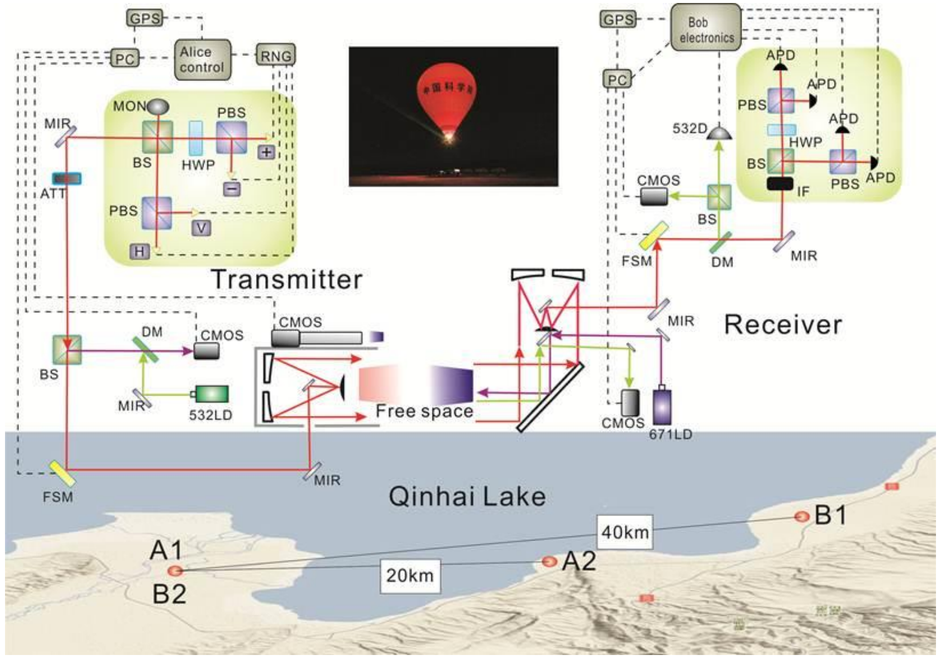
Yin *et al.*, Nature 488, 185 (2012)

Ground Tests for Satellite Quantum Communication

Phase 3: Direct and full-scale verifications towards satellite-to-ground quantum key distribution

- ☑ Mimicking the satellite's angular motion
- ☑ Mimicking the satellite's attitude change
- ☑ A huge loss channel (about 50 dB loss, 97 km)

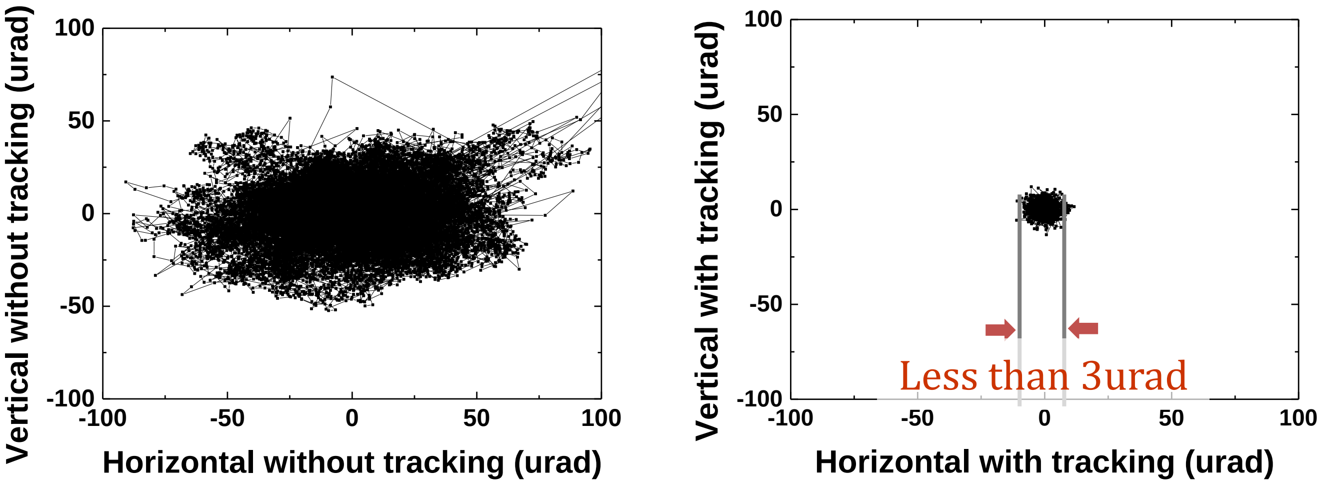
Wang *et al.*, Nature Photonics 7, 387 (2013)



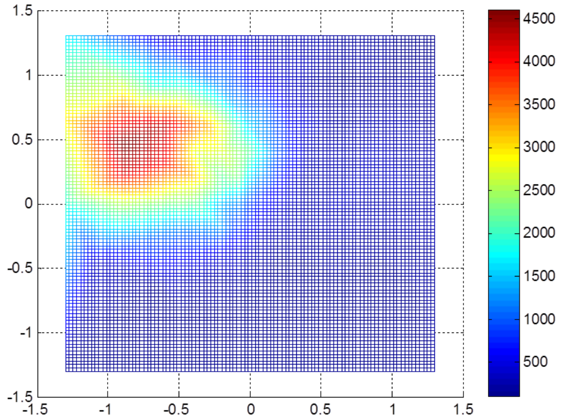
Overcoming all the demanding conditions for ground-satellite QKD

Ground Tests for Satellite Quantum Communication

☑ High precision Acquiring, Pointing and Tracking (APT)

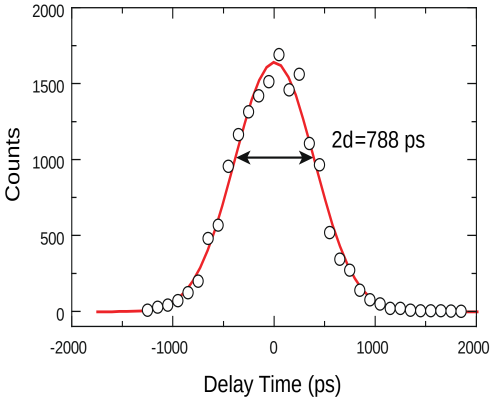


☑ Near-diffraction-limited far-field divergence angle



- Diffraction-limited divergence angles: 8μrad
- Divergence angle ~10μrad@140mm

☑ High precision synchronization

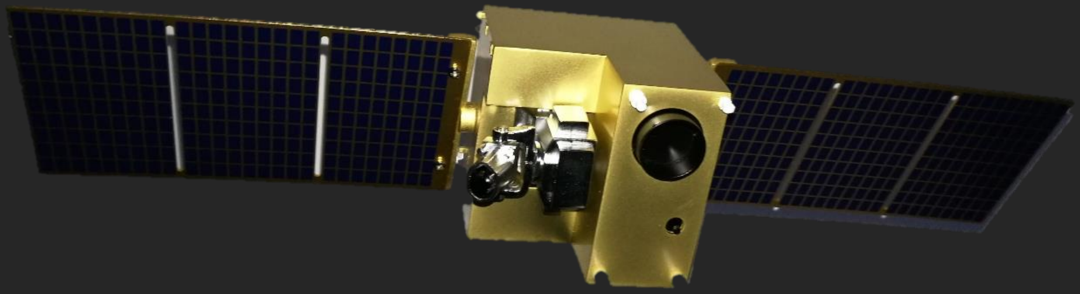


- Hundreds of kilometers
- Rapid motion
- Random movement
- Vibration

☑ Ultra-high energy resolution: detecting from the earth a single match fire lighted on the Moon

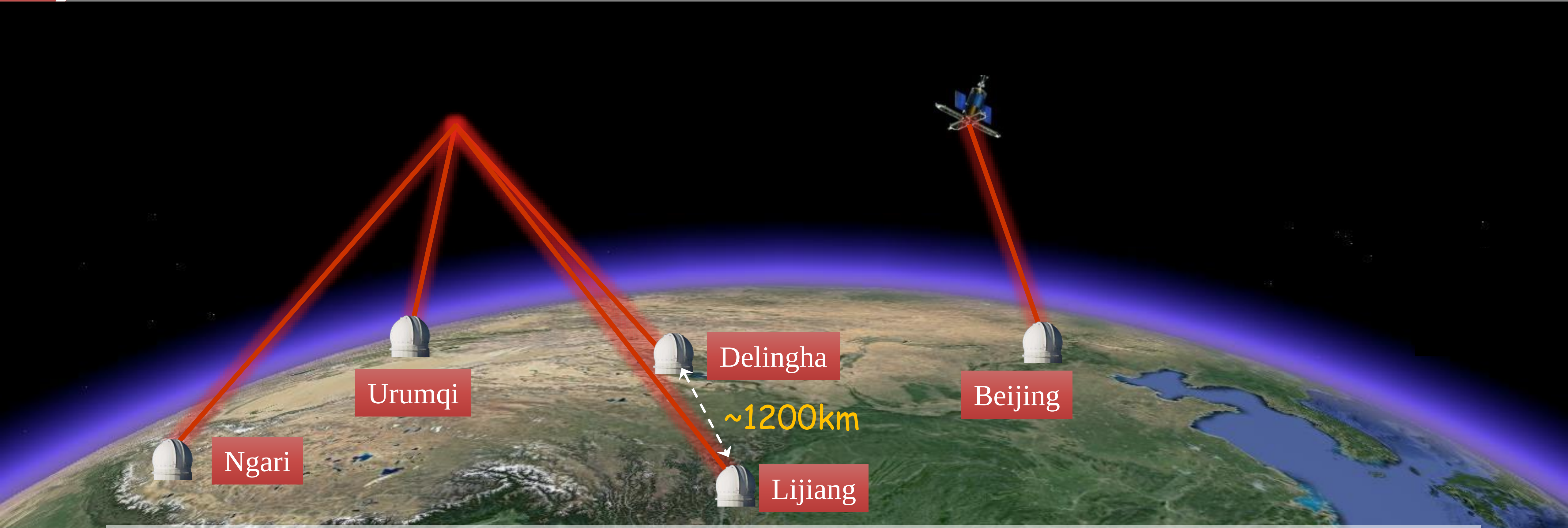
Quantum Science Satellite "Micius"

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



- Weight: ~640kg
- Power: 560W
- Sun-synchronous orbit, altitude 500km

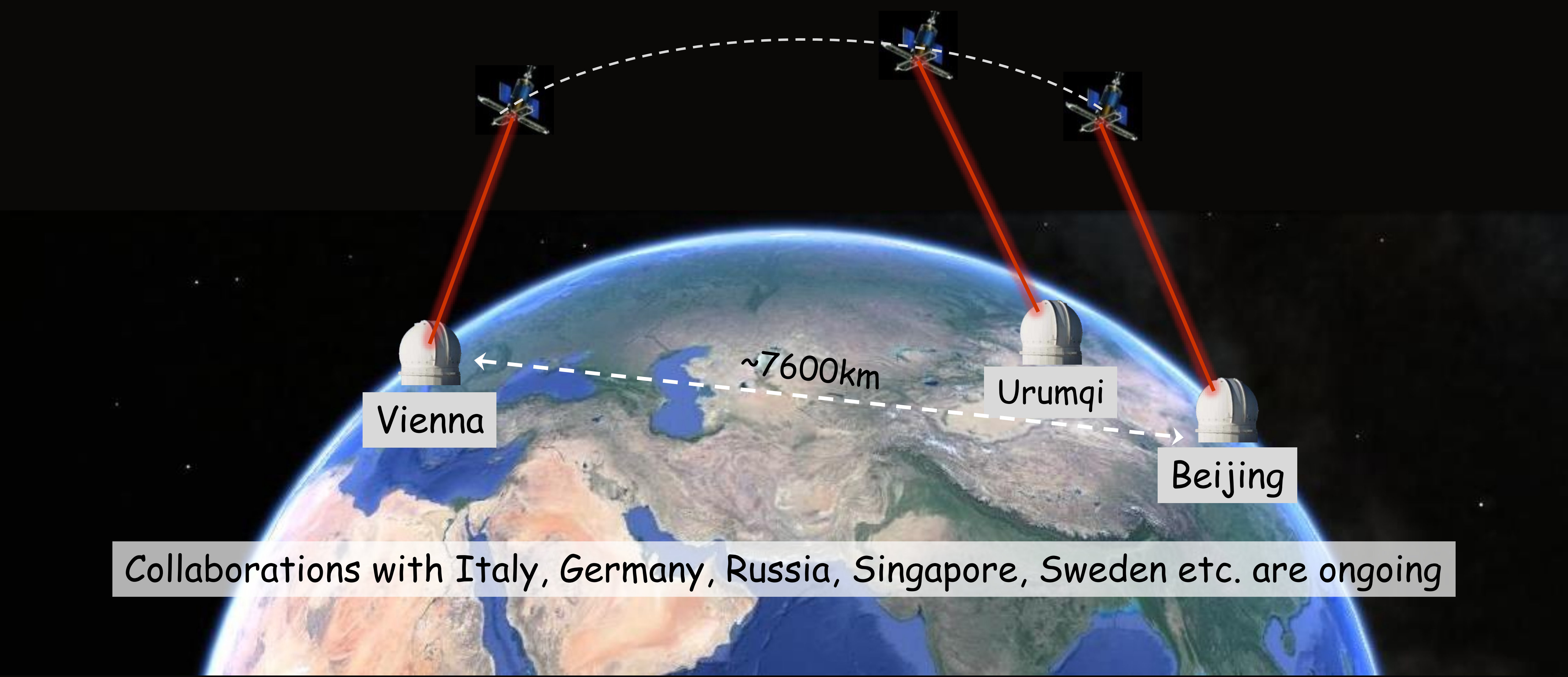
Micius' Three Missions



- QKD between satellite and ground, key rate ~1kbps (recently ~400kbps) ➡ 20 orders of magnitudes higher than using fiber channel at 1200 km [Nature 549, 43 (2017)]
- Quantum entanglement distribution from satellite, test of quantum nonlocality under strict Einstein's locality condition [Science 356, 1140 (2017)]
- Quantum teleportation between ground and satellite [Nature 549, 70 (2017)]

Intercontinental Quantum Key Distribution

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

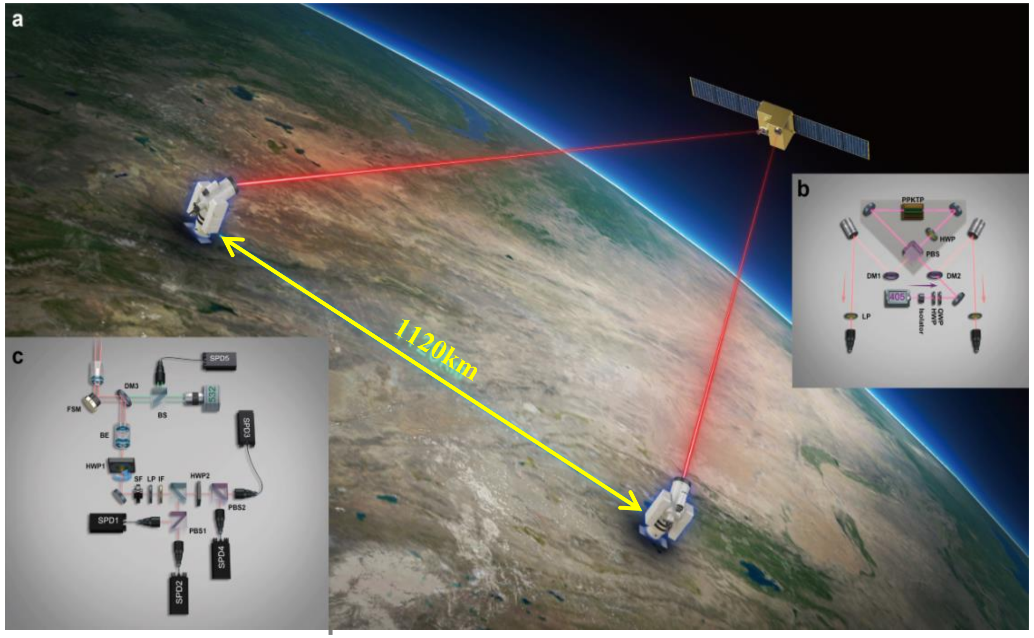


Collaborations with Italy, Germany, Russia, Singapore, Sweden etc. are ongoing

In Progress

Entanglement-based QKD

Even the satellite is controlled by your enemy, once Bell inequality is violated, the security of QKD can still be ensured!



- **Scheme:** Ekert, PRL 67, 661 (1991)
  Bennett *et al.*, PRL 68, 557 (1992)
- **Experiment:**
  over 1120 km [manuscript in preparation (2019)]
  - Channel Loss: 56~71dB, received 2 pairs/s
  - Final key: 0.43 bps
  - QBER: 4.51%±0.37%

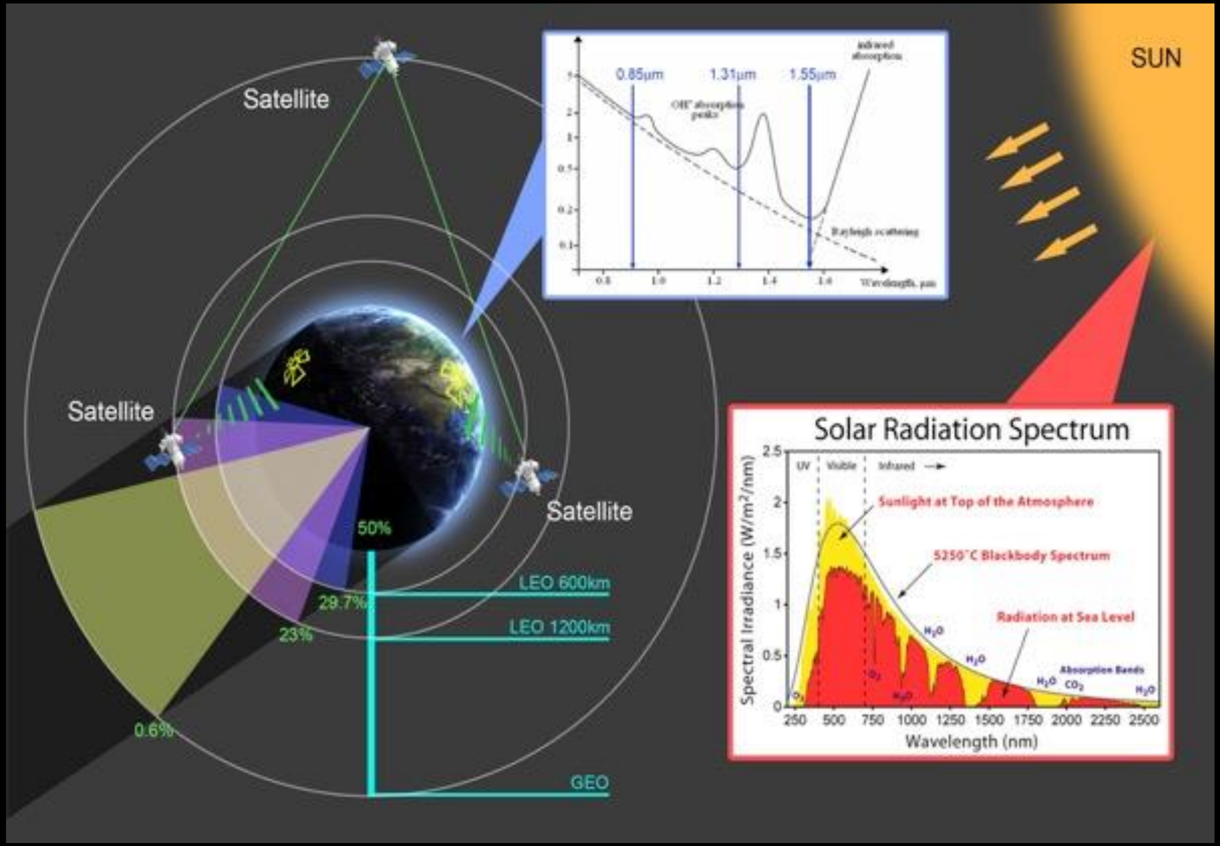
  ➡ If load GHz entanglement source, up to 10kbits per orbit

This would thus achieve the Holy Grail that all cryptographers have been dreaming of for thousands of years

--G. Brassard

- ☒ LEO orbit can not cover the whole earth directly
- ☒ Only working in earth's shadow
- ☑ Solution: Quantum Constellation!

  A pre-requirement: work in solar radiation background

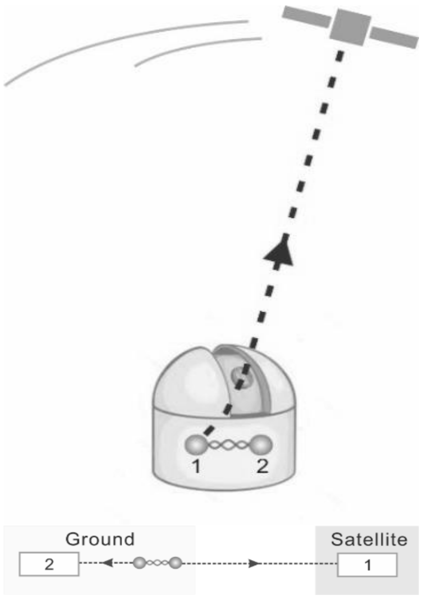


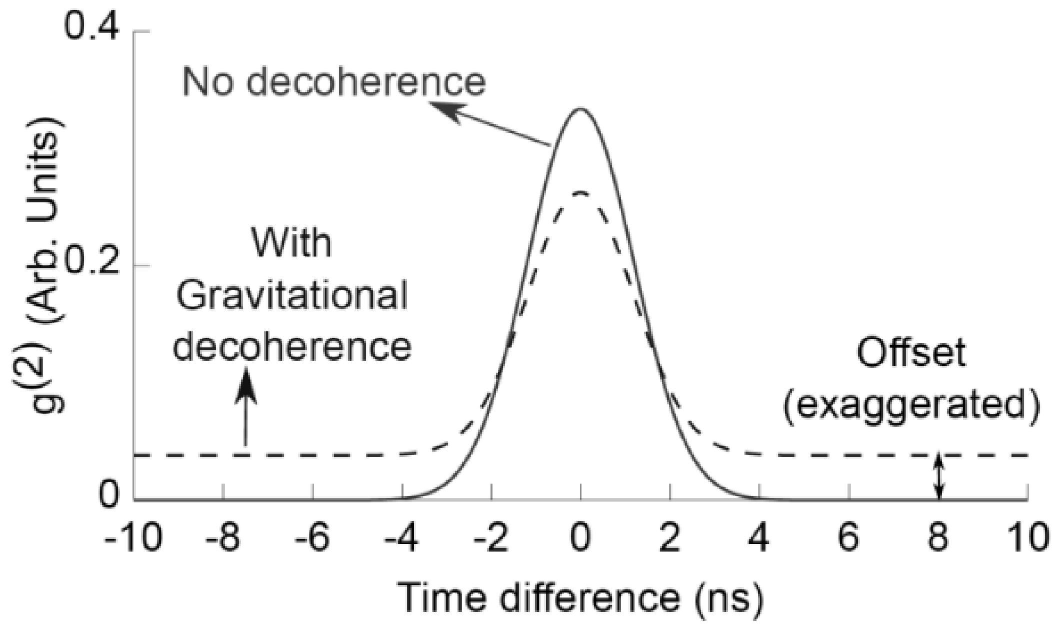
Long-distance free-space QKD in daylight

Liao *et al.*, Nature Photonics 11, 509 (2017)

In Progress

Searching for interface of quantum physics and gravity



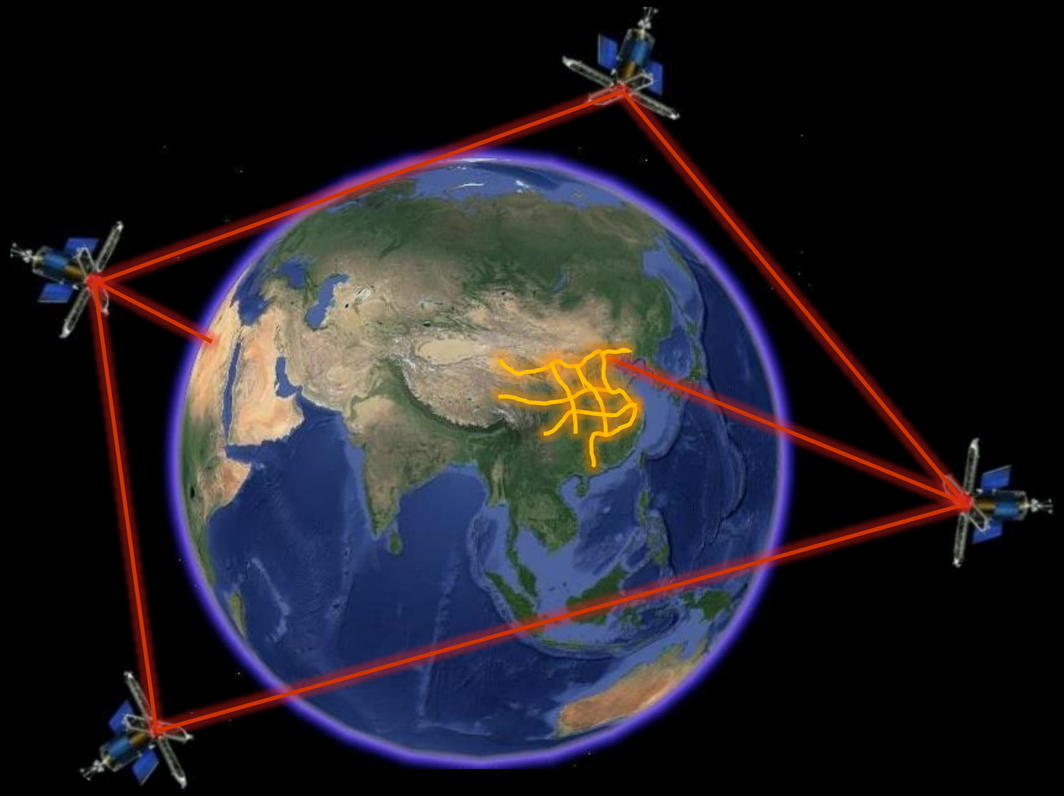


Gravitationally induced decorrelation of entanglement

Scheme: Ralph *et al.*, PRA 79, 022121 (2009)

Experiment: Xu *et al.*, manuscript in preparation (2019)

Future Prospects



Quantum Constellation + Fiber quantum communication infrastructure

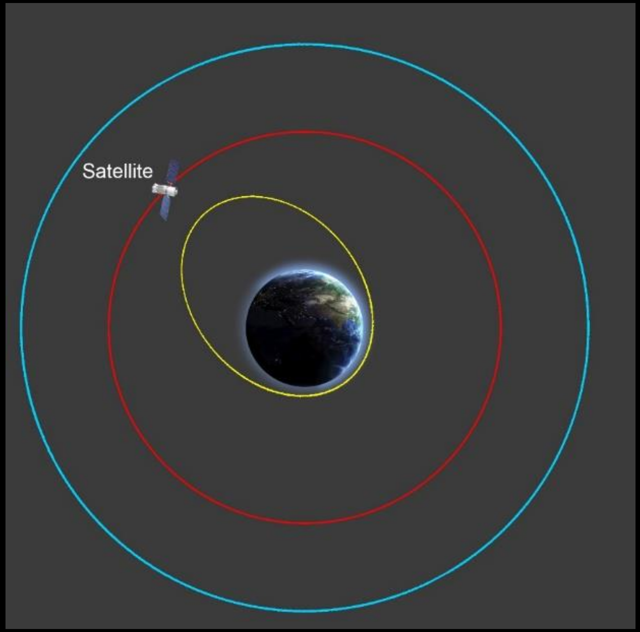
↓

"Quantum Internet"

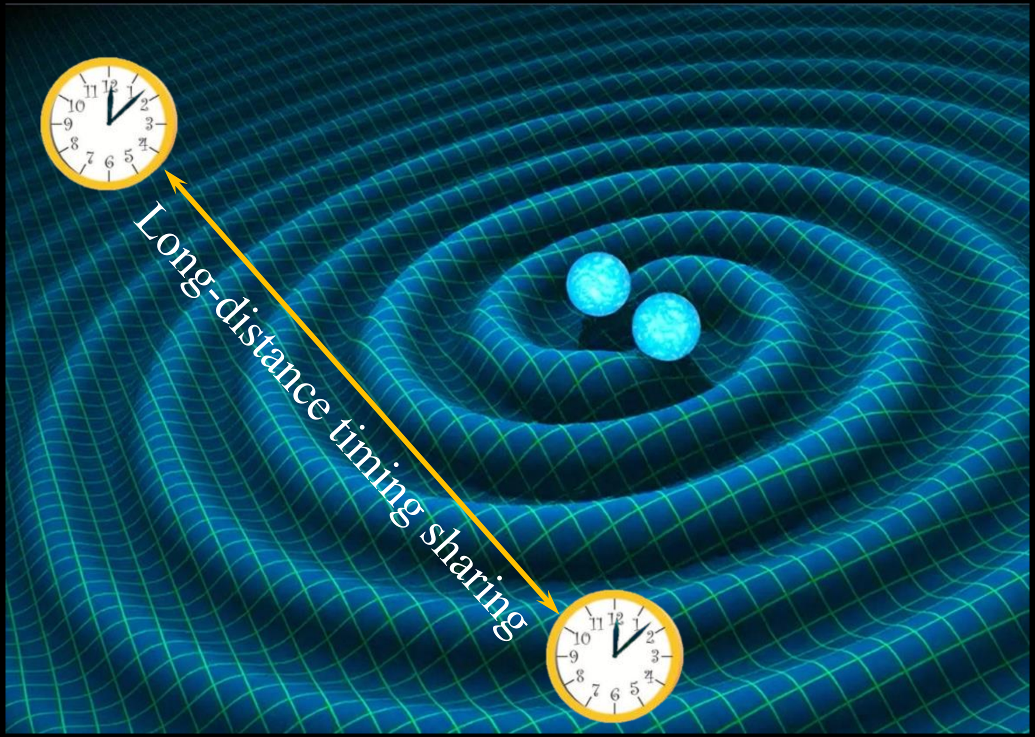
Future Prospects

Ultra-precise optical clocks in outer space

Negligible magnetic and gravitational noise ➡ Fractional instability ~10^{-21}



- Precisely detecting gravitational red shift at different altitude of orbits



- Detecting gravitational wave signal with lower frequency to 0.1Hz ➡ revealing more kinds of astronomical events! (LIGO: ~100Hz)

Future Prospects

Large-scale Bell test with Human-observer

Channel loss of entanglement distribution between Earth and Moon: 100 dB

- Bell test with human supplying random measurement over simulated high loss channel (103dB) [PRL 120, 140405 (2018)]

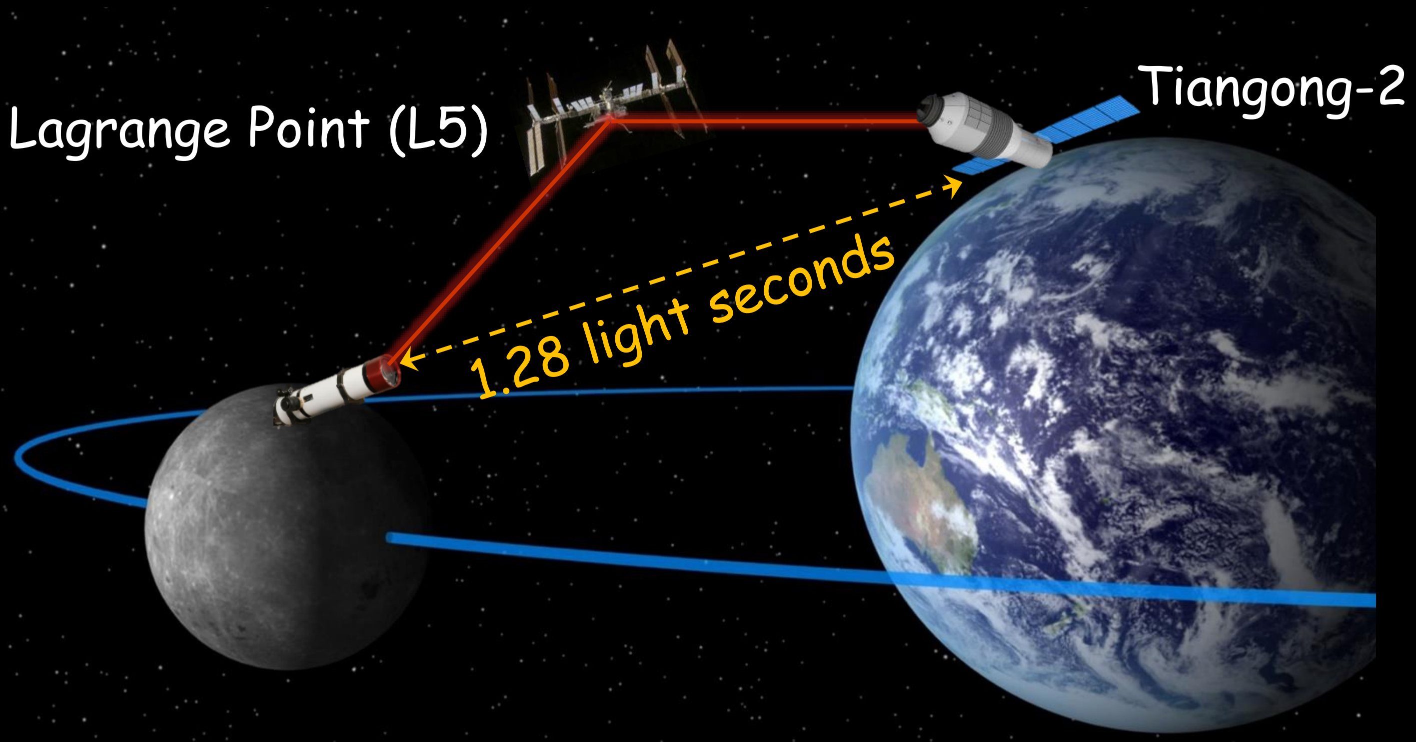
Challenging local realism with human choices

- Generating random numbers with help of worldwide 100k volunteers' free will
- 12 labs run Bell tests with the random numbers

  [*The BIG Bell Test Collaboration*, Nature 557, 212 (2018)]

Future Prospects

Large-scale Bell test with Human-observer



Entanglement distribution between Moon and Earth with China's future Moon landing project

Thanks for your attention!