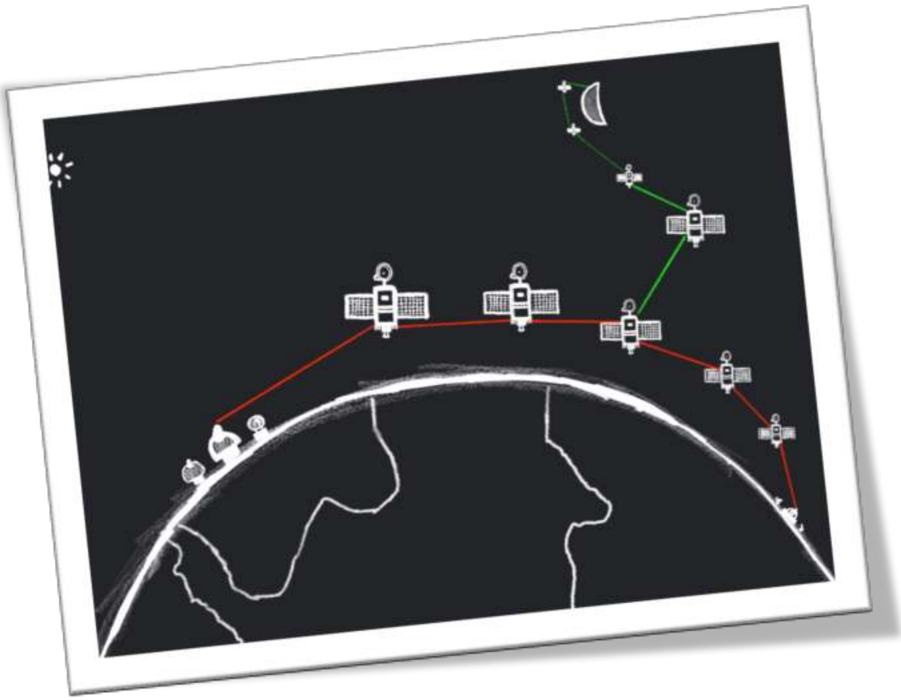
# Quantum-Enabled
# Secure Communications in Space



IFT-6155 Quantum Computing

Research Presentation

Ayoub & Nassim

Université de Montréal

# Plan of the presentation

**1) Conceptual Background**

- Quantum key distribution (QKD) Protocols
- Entanglement distribution
- Quantum teleportation

**2) MICIUS Experimentations**

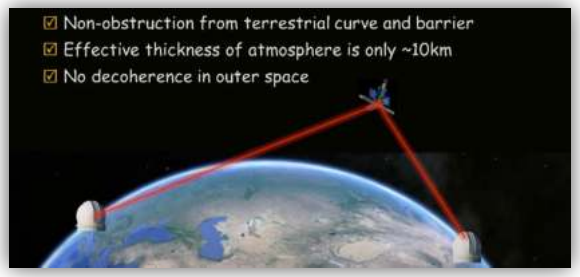
- Overview
- Challenges in large-scale applications
- Quantum repeaters
- Satellite-based free-space channels
- Key technologies
- Satellite payloads
- Satellite-based quantum experiments with Micius

**3) Outlook for the future**

- Other Quantum Satellite Projects
- Challenges, Solutions, and Satellite Constellations
- Quantum communication across interstellar distances

## ➢ <u>Utility of Secure Space Communications?</u>


- **Secure Communications?**
  - "Guaranteed" Privacy between Alice and Bob
  - Secure Internet, banking system, transactions, business secrets, government secrets, Military…




- **Why Space?**
  - Required when communicating with spacecrafts, astronauts, …
  - Key option when it comes to **long communicating distances** (> 1000 kms)
  - Available everywhere on earth's surface in the presence of a satellite constellation (Scalable)
  - Circumvent the inevitable large photon loss in fiber optic and atmospheric free space channels… Almost 0 absorption and decoherence compared to those
  - ***At 1000 km, even with a perfect single-photon source of 10 GHz, ideal photon detectors, and 0.2 dB/km fiber losses, one would detect only 0.3 photons on average per <u>century</u> (Gisin and Thew, 2010)***

# Section 1
# Conceptual Background

# 1) Background -- Quantum Key Distribution (QKD)

- **Quantum Key Distribution (QKD)**

- Method for **establishing secure communication channels between two parties** based on the principles of quantum mechanics.

- Relies on the fundamental properties of quantum mechanics for security (**Heisenberg uncertainty principle** and the **no-cloning theorem)**

- Basic idea: Use the properties of quantum states to transmit information in a way that is **intrinsically secure against eavesdropping**.

- Initially developed by Bennett & Brassard (1984) [1] via the first QKD protocol known as BB84

- This protocol **permits two distant communicating parties to produce a common, random string of secret bits, called a secret key**.

- It is NOT an encryption protocol

- The shared secret key **can then be used alongside the one-time pad encryption**
  - **Which was proved** secure by Shannon in 1949 (Shannon, 1949)
  - Key as a truly random sequence of 0s and 1s of the same length as the message

# 1) Background -- Quantum key distribution (QKD)

- **2 types of QKD protocols :**

**1) Non-Entangled based:**

- These protocols are using photons that are not entangled for communicating the secret key from Alice to Bob.
- This is the case for the **BB84 protocol** theorized by Charles Bennett and Gilles Brassard in 1984.

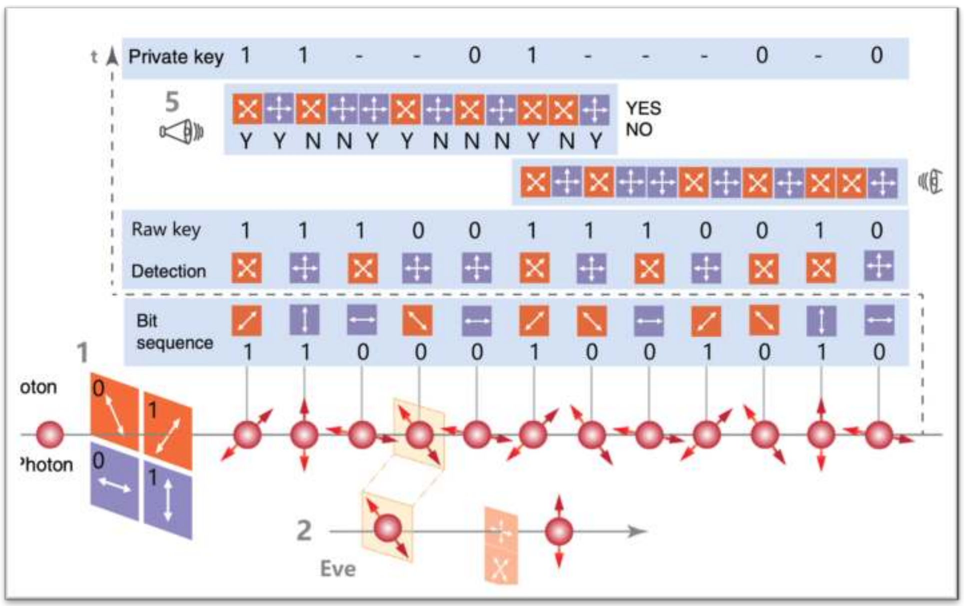
**2) Entanglement based protocols:**

- These protocols are using entangled pairs of qubits which are distributed to Alice and Bob, who then extract key bits by measuring their qubits.
- We can name the **E91 protocol** theorized by Artur Ekert in 1991.

*Both of these approach have advantages and disadvantages that we will discuss later in the presentation.*

# 1) Background -- Quantum key distribution (QKD)

- **BB84 Protocol**




**This protocol exploits four polarization states of photons that span two bases.**

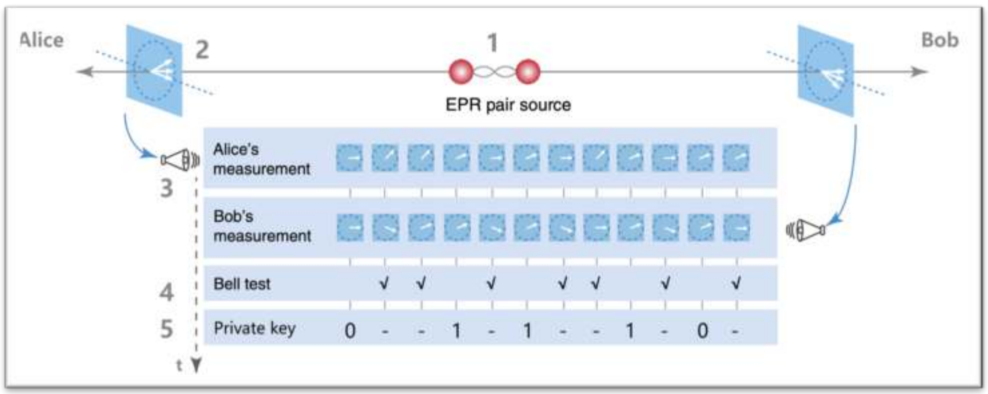
**(such as the horizontal polarization $|H\rangle$ , the vertical polarization $|V\rangle$ , the diagonal polarization $|45°\rangle$ , and the antidiagonal polarization $|-45°\rangle$**

**Procedure :**

1. Alice randomly generates a sequence of bits (this sequence will contain the secret key)
2. Alice encodes the sequence of bits in terms of polarized photons (**basis randomly chosen**)
3. Alice sends these photons to Bob through a **quantum channel**
4. Bob receives those polarized photons and measures them using a **random detection scheme**
5. Bob **broadcasts** his choice of **measurement** basis for each photon through a **classical information channel**
6. **Alice responds Yes or No** for the same or different basis that they used**.**
7. **They discard the bits that are a result of different basis measurement and emission.**

# 1) Background -- Quantum key distribution (QKD)

- **E91 Protocol**




**This protocol operates by sharing secret keys between Alice and Bob by distributing EPR pairs.**

**Procedure :**

1. Alice and Bob first **share an entangled photon** pair in the singlet state **|Ψ−⟩** .
2. Alice and Bob receive the photon then **randomly and independently choose their measurement** bases, obtained by rotating the basis.
3. They measure and register a series of photon pairs. After that, they **broadcast the measurement bases** they have used while **keeping the outcomes secret**
4. They **use the measurement outcomes with the same angles as raw keys** and use the **others for the Bell inequality test**.

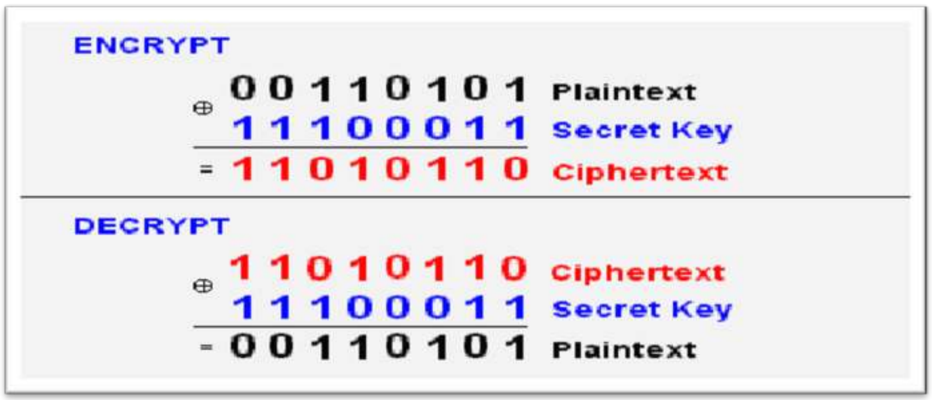
# 1) Background -- Quantum key distribution (QKD)

**Estimating Eve's information**

Alice and Bob share a small part of their secret keys publicly and **check for errors above a certain threshold**

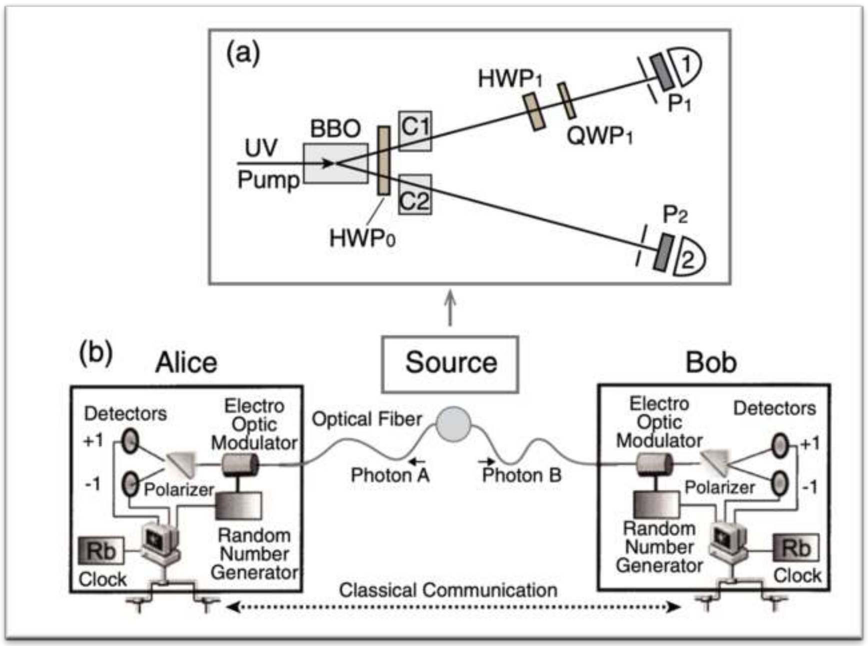
Note that in Ekert91, Alice and Bob estimate the Eve's information based on the Bell's inequality test; whereas in BBM92, as in the case of BB84, Alice and Bob make use of the privacy amplification to eliminate Eve's information regarding the final key (Lo and Chau, 1999)

**Usage in terms of One-time Pad**



# 1) Background -- Entanglement distribution

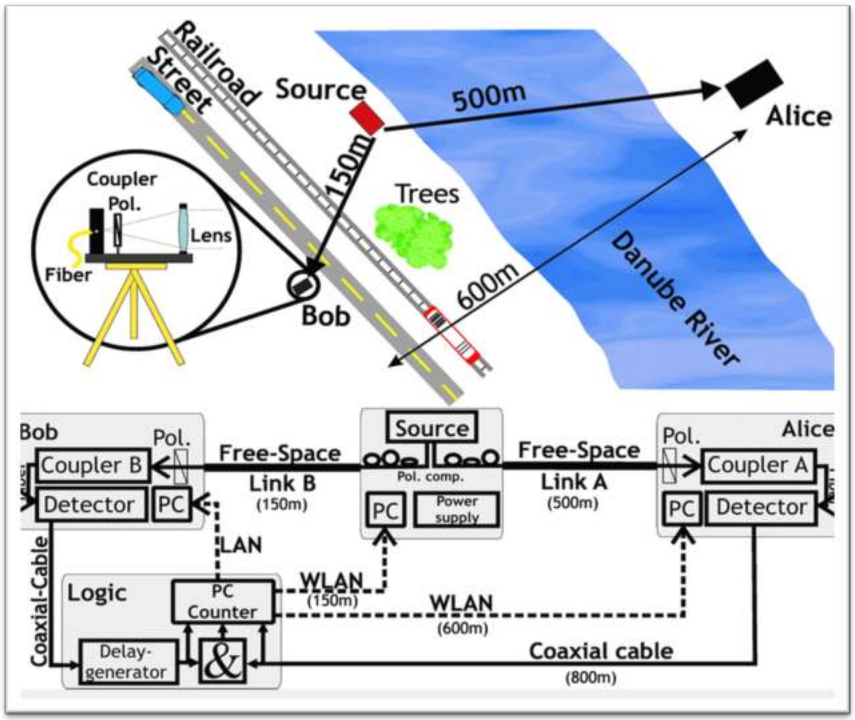
**Entanglement distribution**




- One of the **most important concept** and tool of Quantum Theory
  - Bell's Inequality
  - Quantum Teleportation
  - Entanglement Swapping
- Type-II noncollinear phase matching in β-barium borate (BBO)

# 1) Background -- Entanglement distribution

**Entanglement distribution (Experiment)**




**In 2003**:

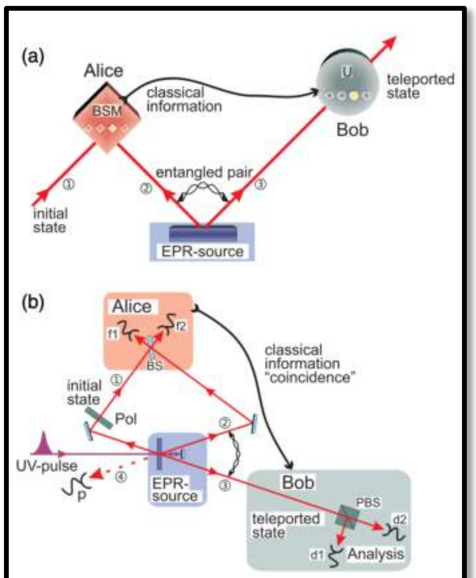
**First entanglement distribution outside** of a laboratory over free-space (Vienna) (600 meters distance)

**In 2004 :**

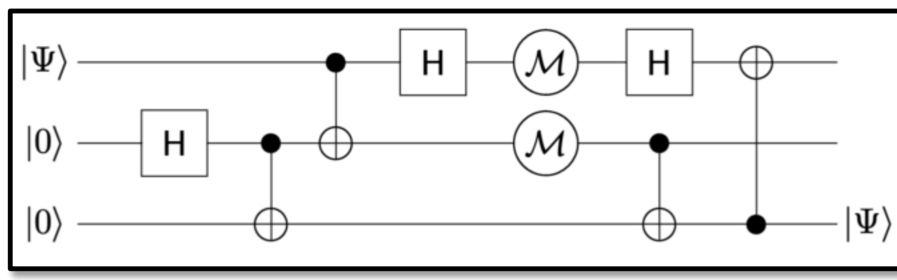
*Poppe et al.* demonstrated a successful run of a quantum cryptography system where a produced key was directly sent through a quantum secured on-line wire from the city hall to headquarters of Bank-Austria, **showing a real-world application scenario outside of ideal laboratory condition**.

# 1) Background -- Quantum teleportation

**Quantum teleportation**



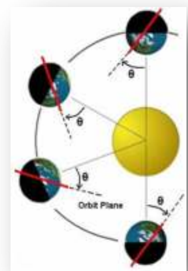

- Discovered in 1993 by C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters
- First demonstration 1997 by Bouwmeester

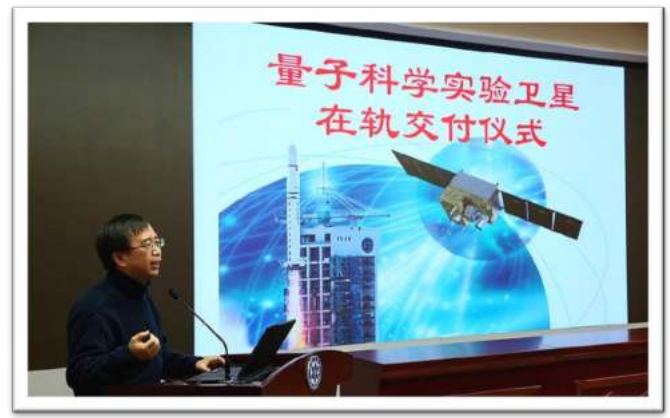


# Section 2
# MICIUS Experimentations

# 2) MICIUS Experimentations -- Overview

- Experiment conducted by **Jian-Wei Pan and his team at the University of Science and Technology of China**
- Satellite launched from China in August 2016 which is dedicated to quantum science experiments (via a Long March 2D)
- Micius etymology: Named after the 4th century BCE Chinese philosopher Micius




- Orbital Parameters:
  - ➢ Regime: Sun-synchronous Circular Orbit
  - ➢ Perigee altitude: 468km
  - ➢ Apogee altitude: 482km
  - ➢ Inclination: 97.4 degrees

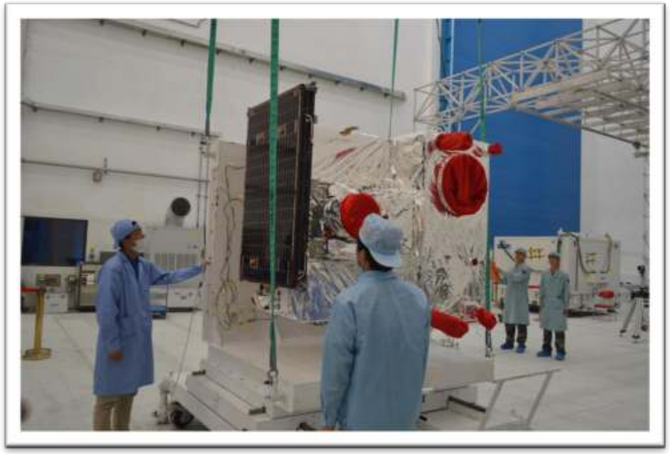
- 5 ground stations in China:
  - Four are for receiving via downlink channels. One is for transmitting via uplink channels
- The University of Vienna and the Austrian Academy of Sciences are running the satellite's European receiving stations

| NORAD CAT ID | SATNAME | INTLDES | TYPE | COUNTRY | LAUNCH | SITE | DECAY | PERIOD | INCL | APOGEE | PERIGEE | RCS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 41731 | QSS | 2016-051A | PAYLOAD | PRC | 2016-08-15 | JSC | | 94.10 | 97.33 | 482 | 468 | LARGE |

# 2) MICIUS Experimentations -- Overview

- The mission cost was around US$100 million in total

- Within a year of the launch, three key milestones for a global-scale quantum communication network were achieved:
  - **(1) Satellite-to-ground decoy-state QKD with KHz rate over a distance of up to 1200 km and satellite-replayed intercontinental key exchange**
  - **(2) Satellite-based entanglement distribution to two locations on the Earth separated by 1205 km and subsequent Bell test**
  - **(3) Ground-to-satellite quantum teleportation**



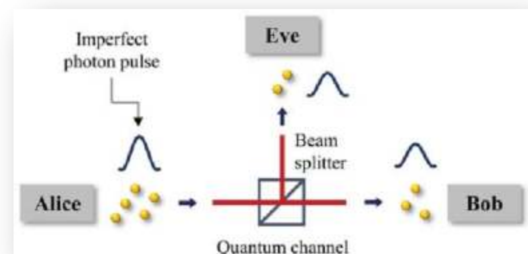
- Experiments established the possibility of effective link efficiencies through satellite
- **12-20 orders of magnitudes** greater than direct transmission through optical fibers
- Distance of ~1200 km

# 2) MICIUS -- Challenges in large-scale applications

- **Security Loopholes**

- **Imperfections of realistic QKD** implementations might introduce **deviations** (or **side channels**) from the idealized models used for security analysis
- Ideally, only when perfect single-photon sources and detectors are utilized, quantum cryptography can be considered secured.
- Unfortunately, **ideal devices do not exist in practice**.

- Different type of attacks exist :
  - Photon number splitting (**PNS**) attack, *(Brassard et al., 2000; Lutkenhaus, 2000)*
  - ***Blinding attacks**, (Makarov, 2009)*




- Solutions:
  - For **PNS attacks (Photon Source Loophole)** → Decoy State QKD (choosing randomly intensity levels)
  - For **Blinding attacks (Detector Loophole)** → Measure-Device-Independent QKD (**MDI-QKD**)

# 2) MICIUS -- Challenges in large-scale applications

**Long Distances**

- **What limits the distance of quantum communications?**
- In both the fiber optics and terrestrial free space channels, there are inevitable **photon losses**, which **scale exponentially** up with the transmission length in optical fibers.
- ***Gisin et al. highlighted that at 1000 km, even with a perfect single-photon source of 10 GHz, ideal photon detectors, and 0.2 dB/km fiber losses, one would detect only 0.3 photons on average per century (Gisin and Thew, 2010)***
- Unlike classical bits, the quantum signal of QKD cannot be noiselessly amplified (**No Cloning Theorem**)
- Hence what makes the security of QKD is also what excludes the possibility of amplifying quantum signals for longer distances communications.

# 2) MICIUS -- Quantum repeaters

- Quantum repeaters combine **entanglement swapping**, **entanglement purification**, and **light storage**, and in principle, can enable quantum communication at arbitrarily large scales

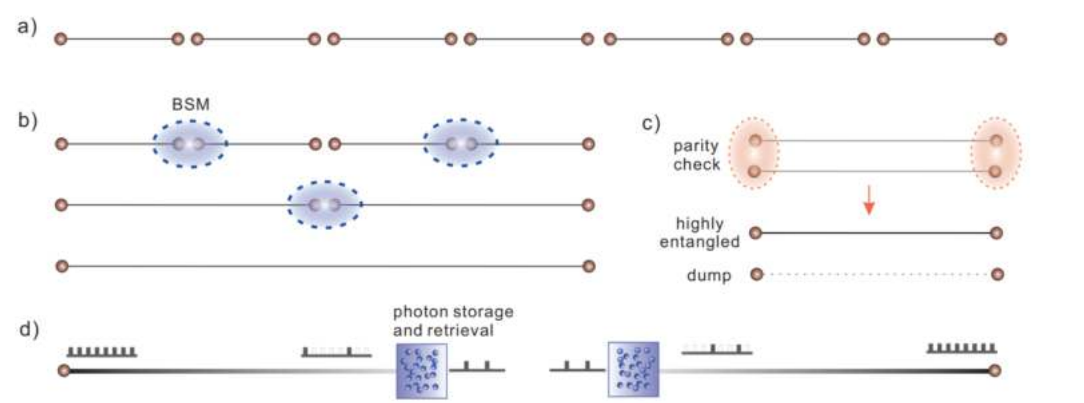



FIG. 8 Principle of quantum repeaters (Briegel *et al.*, 1998; Duan *et al.*, 2001). (a) Dividing the communication channel into $N$ segments. (b) Using entanglement swapping to establish entanglement between remote nodes. (c) Using entanglement purification to distill highly entangled pairs between remote nodes. (d) Using quantum memory to store single photons for a sufficiently long time and retrieve the single photon for time synchronized two-photon interference.

# 2) MICIUS -- Satellite-based free-space channels

**Why choosing free-space channels ?**

- The attenuation in free space is **lower than that in fiber** for optical signals.
- **For instance, values of 0.07 dB=km can be achieved at 2400 m above sea level (Schmitt- Manderbach et al., 2007) with higher absorption attenuations at lower altitudes.**
- In the vacuum above Earth's atmosphere, the absorption attenuations are reduced to **almost zero**.
- Nonbirefringent character of the atmosphere guarantees the **preservation of polarization state to a high degree.**

**Why choosing satellite-based ?**

- Terrestrial free-space suffer from obstruction from :
    - Objects in the line of sights
    - Weather conditions
    - Earth curvature
- Thickness of the atmosphere is approximately **5–10 km**, most of the photon's propagation path is in empty space with negligible absorption and turbulence, which is **crucial for transmitting single photons that cannot be amplified.**

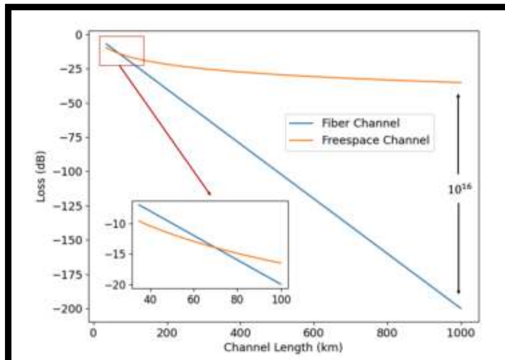



FIG. 10 Typical losses in fiber and free-space channels. The attenuation parameter of fiber is $\sim 0.2\ dB/km$. The parameters of free-space channel are based on the design of Micius satellite. The free-space channel shows advantage for a distance over $\sim 70$ km

# 2) MICIUS -- Satellite-based free-space channels

**A) Analysis of space-ground links**

- **Several factors influence the attenuation of quantum communication channels** when photons travel between a ground station and a satellite.

- Mainly affected by the efficiencies of :
  - **Optical transmitting system $\eta_t$**
  - **Receiving system $\eta_r$**

- During transmission, the optical beam will be **broadened or deflected by diffraction**, **air turbulence** and **mispointing (pointing error)**, which will induce **losses $\eta_d$**, **$\eta_{at}$**, and **$\eta_p$**, respectively. Atmospheric absorption brings the attenuation **$\eta_{as}$**

$$\eta = \eta_t \eta_r \eta_d \eta_{\mathrm{at}} \eta_p \eta_{\mathrm{as}}$$

# 2) MICIUS -- Satellite-based free-space channels

A) **Analysis of space-ground links**

- **Beam diffraction $\eta_d$** (Ex: can be mitigated by choosing relatively shorter photon wavelengths)
  - Diffraction of an optical beam depends mainly on its spatial mode, its wavelength, and the telescope aperture.
  - The diffraction loss in long-distance quantum communications can be mitigated by choosing relatively shorter photon wavelengths or a large waist radius

- **Air turbulence $\eta_{at}$**
  - This is one of the main factors limiting the channel efficiency in free-space quantum communication
  - Changes the direction of the propagating beam (due to atmospheric refractive index inhomogeneity)
  - Large-scale turbulence causes beam deflection, while small-scale turbulence induces beam broadening (Vasylyev, Semenov, and Vogel, 2016)

# 2) MICIUS -- Satellite-based free-space channels

## A) Analysis of space-ground links

- **Pointing error $\eta_p$**
  - To establish the link between the ground and the high-speed moving satellite, a **high-precision** and **high-bandwidth APT system**, should be developed.

- **Atmosphere transmittance $\eta_{as}$**
  - The particles in the atmosphere are distributed **mainly on the ground surface**, with a **decreasing concentration as the altitude increases**.
  - The **transmittance is good at a high altitude angle** because of the relatively short propagation time in the atmosphere.

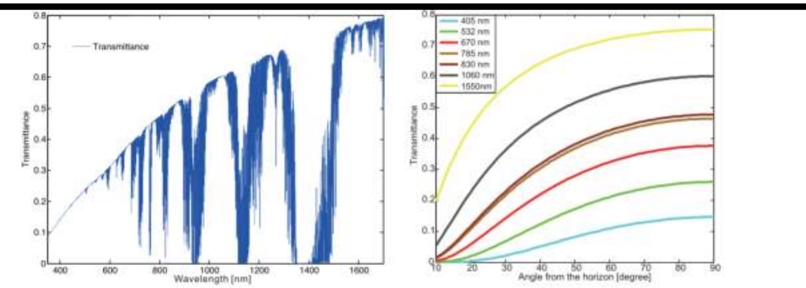



FIG. 11 The simulated atmospheric transmittance for zenith with different wavelengths (left) and different altitude angles (right).

### Characteristics of the two types of transmissions :

- **Downlink** : the beam reaches air turbulence with a large size and is received immediately after the atmosphere is crossed; thus, the **impacts are marginal on the beam broadening and deflection** induced by turbulence.

- **Uplink** : photons encounter air turbulence at the beginning of propagation and subsequently transmit to the satellite. Therefore, turbulence-induced **distortion will significantly increase the beam divergence angle** and result in a **larger channel attenuation** than that in the case of the downlink transmission

# 2) MICIUS -- Satellite-based free-space channels

## B) Feasible channel parameters for the low-Earth orbit satellite

**Downlink experiment preferred :**

- Satellite-based QKD
- Entanglement distribution

**Uplink experiment preferred :**

- Quantum Teleportation

*Downlink is more challenging as your satellite is less flexible and much more limited than the ground station.*

***Using the estimated total channel loss and the requirements of the satellite mission as the input condition, one can output the specifications of key technologies. Cf. Table II***

| **List of feasible design baseline:** | |
|---|---|
| Satellite operating lifetime | $\geqslant$ 2 years |
| Time synchronization accuracy | $\leqslant$ 1 ns (1 $\sigma$) |
| **Satellite-to-ground QKD** | |
| Raw key rate | $\geqslant$ 1 kbps |
| QBER | $\leqslant$ 3.5% |
| Total experimental time | $\geqslant$ 20000 s |
| Total Channel loss | $\leqslant$ 40 dB |
| **Satellite-based entanglement distribution** | |
| Received coincident count | $\geqslant$ 1000 |
| Effective fidelity | $\geqslant$ 85% |
| Total experimental time | $\geqslant$ 10000 s |
| Total Channel loss | $\leqslant$ 80 dB |
| **Ground-to-satellite quantum teleportation** | |
| Received coincident count | $\geqslant$ 400 |
| Effective fidelity | $\geqslant$ 75% |
| Total experimental time | $\geqslant$ 40000 s |
| Total Channel loss | $\leqslant$ 55 dB |

TABLE II Main practical requirements of satellite-based quantum science experiments.

# 2) MICIUS – Feasibility Studies & Key Technologies

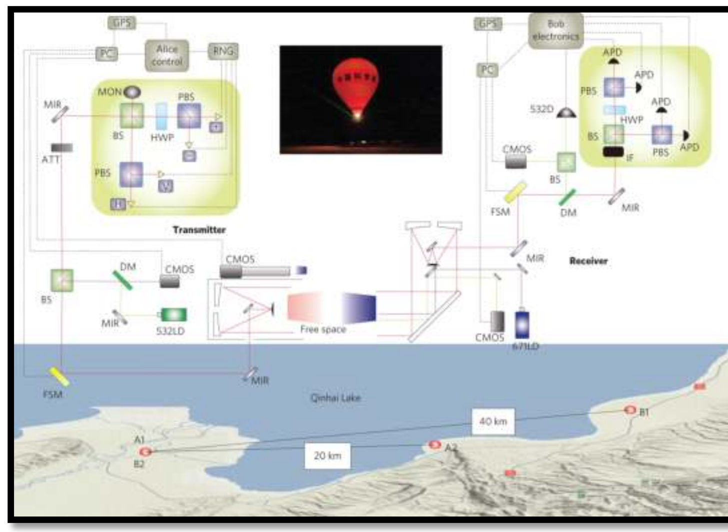
## - Five aspects:

### 1) Overcoming the effective atmospheric thickness

- In 2005, entangled photon pairs were bidirectionally distributed over Hefei, China

### 2) Testing the feasibility of satellite- ground channels

- Wang et al. (2013) conducted a full verification study of the decoy-state QKD over a 97 km free-space link and demonstrated the possibility of achieving a high signal-to-noise ratio and overcoming the obstacle of a high-loss environment




### 3) Testing moving objects

- Simulation experiments with a turntable and a hot-air balloon were implemented to simulate the platform in a rapidly moving orbit as well as the vibration, random motion, and attitude change related to the LEO Satellite.

### 4) Time synchronization

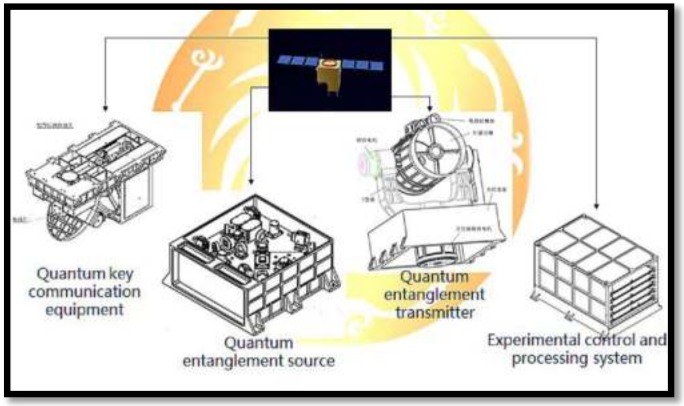
- As the distance between the transmitter and receiver changes all the time when the satellite passes over the ground station, both the Global Positioning System (GPS) pulse-per-second (PPS) signal and an assistant pulse laser are employed in the typical synchronization scheme.

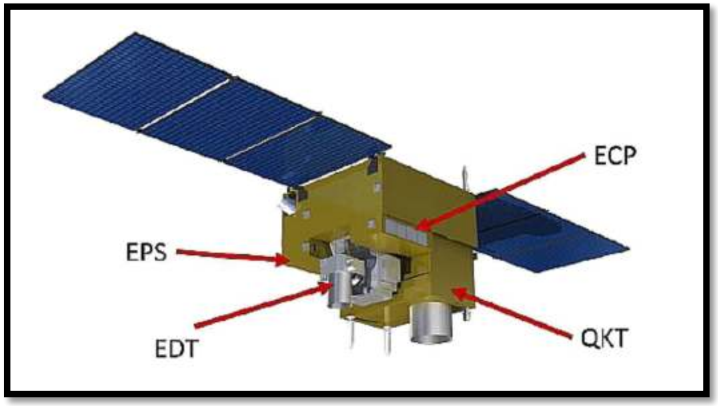
### 5) Polarization maintenance and compensation

- Polarization compensation in real time : inputting the real-time data of the orbit prediction into an auto rotatable half-wave-plate (HWP) for polarization tracking
- Polarization maintenance : while the optical system was set up, a polarization extinction ratio of 200:1 was obtained for both the transmitter and receiver systems Wang et al. (2013)

# 2) MICIUS -- Satellite payloads

- Weight: 635 kg
- The satellite carries four devices:
    - Quantum key distributor
    - Quantum entanglement transmitter
    - Quantum entanglement generator
    - Quantum test control processor.
- It has two separate antennas to simultaneously establish quantum communications with two ground stations on Earth.



# 2) MICIUS -- Satellite payloads

**1) Two optical transmitter**

- Transmitter 1 : for QKD, entanglement distribution and Teleportation
    - 8 laser diodes with drivers
    - BB84 polarization encoding module
    - Telescope
    - Receiving module

- Transmitter 2 : for entanglement distribution
    - Can serve as transmitter 1's backup for the satellite-based QKD

**2) Spaceborne entangled-photon source**

- Create $|+\rangle$ , $|-\rangle$

**3) Experimental control processor**

- Experimental Process management
- Random-number generation and storage
- Modulation of the decoy-state photon source
- Synchronization-pulse recording
- QKD postprocessing

**4) Two APT control box**

- Control electronics for the coarse tracking loop and the fine tracking loop


FIG. 18 The full view of the Micius satellite and main payloads. (a) The photograph of the Micius satellite before launching. (b) The transmitter 1 for QKD, entanglement distribution and teleportation. (c) The transmitter 2 specially for entanglement distribution. (d) The experimental control box. (e) The entangled-photon source.

# 2) MICIUS -- Satellite payloads

**B) Testing the payload under various conditions**

In general, there are three main types of space environment tests:

- **Vibration** : sinusoidal, random vibration, and impact tests
- **Thermal** : thermal-vacuum, thermal cycling, and thermal-vacuum-optical measurements
- **Vacuum** : thermal-vacuum, thermal-vacuum-optical measurements

After every payload has passed the test separately, all the payloads are combined for the final test in the thermal-vacuum environment.

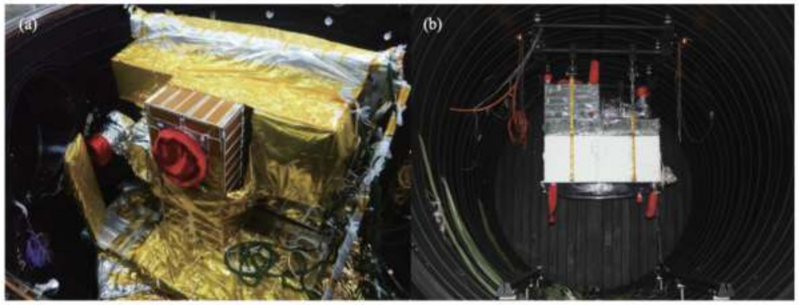



FIG. 21 The thermal-vacuum-optical measurement (a) and the thermal balancing testing (b) for payload combination.

# 2) MICIUS -- Satellite-based Quantum Experiments

## A) Satellite-to-ground quantum key distribution

- Establish a space-ground quantum link and perform QKD from satellite to ground

- The satellite passes each ground station with a sun synchronous orbit every midnight local time for a duration of about 5 minutes (clear nighttime skies are forecast)

- The attitude of the satellite is adjusted to point at the ground station 10 min before the satellite enters the shadow zone.

- Its attitude control system ensures that the transmitter is pointing to the ground station with a coarse orientation accuracy of better than 0.5°. The closed-loop APT systems then start bidirectional tracking and pointing (a tracking accuracy of ~1.2 μrad through the entire orbit)


FIG. 45 Experimentally demonstrating the feasibility of satellite-to-ground QKD with compact ground stations. Up to 2020, QKD with Micius satellite and the compact ground station, in many cities of China, such as Beijing, Jinan, Weihai, Lijiang, Mohe, and so on. The typical sifted key rate is ~ 2 kbps.

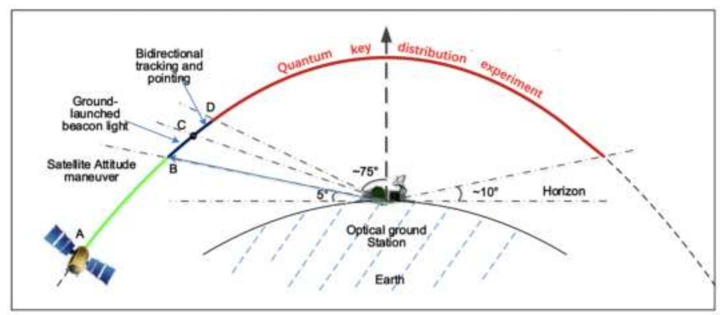



FIG. 27 Tracking and QKD processes during an orbit. (Liao *et al.*, 2017a)

# 2) MICIUS -- Satellite-based Quantum Experiments

## A) Satellite-to-ground quantum key distribution

- A decoy-state BB84 protocol, a form of QKD that uses weak coherent pulses at high channel loss is used in this experience.

- The experiment collected 3 551 136 detection events in the ground station after 273 s and 1 671 072 bits of sifted keys

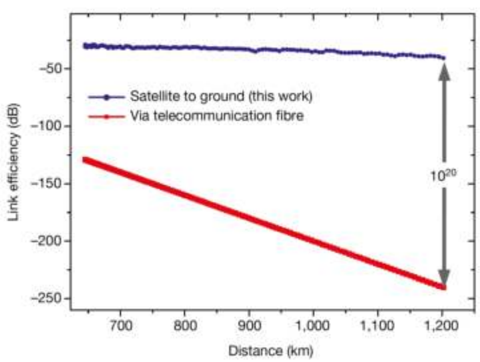



FIG. 29 Link efficiencies are shown for direct transmission through telecommunication optical fibers (red) and the satellite-to-ground approach (blue). The link efficiencies for the latter were calculated by dividing the photon intensity that arrived in front of the detectors at the ground station by that at the output of the satellite's transmitter. (Liao *et al.*, 2017a)

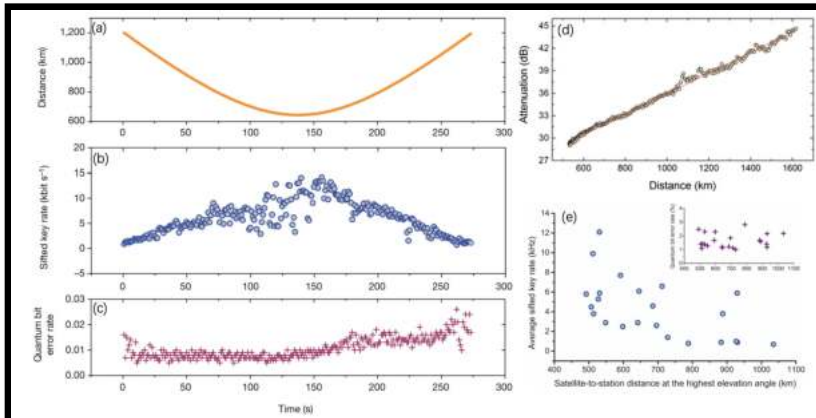



FIG. 28 Performance of satellite-to-ground QKD during one orbit. (Liao *et al.*, 2017a) (a) The trajectory of the Micius satellite measured from Xinglong ground station. (b) The sifted key rate as a function of time and physical distance from the satellite to the station. (c) Observed quantum bit error rate. (d) The attenuation of the down-link channel with different distances between the satellite and the ground. (e) Summary of the QKD data obtained for 23 different days. The $x$ axis is the shortest satellite-to-station distance, which occurs at the highest elevation angle and varies for different days. The $y$ axis is the average sifted key rate.

# 2) MICIUS -- Satellite-based Quantum Experiments

**B) Satellite-based entanglement distribution**

- The **second planned mission** of the MICIUS satellite was a **bidirectional distribution of its spaceborne entangled photons** to two distant locations on Earth (Yin et al., 2017a)
- Owing to channel loss, however, the previously achieved distance was limited to **~300 km**
- The entanglement distribution was achieved both between Delingha and Lijiang and between Delingha and Nanshan.
- The satellite (Fig. 20) emits 5.9 million entangled photon pairs per second, which are then sent out using two telescopes.

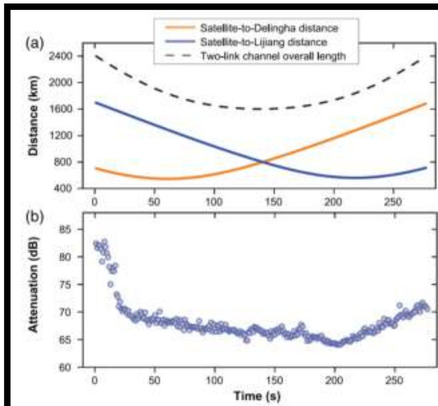



FIG. 31. (a) Typical two-downlink transmission from the satellite to Delingha and Lijiang that lasted for about 275 s in one orbit. The distance from the satellite to Delingha varies from 545 to 1680 km. The distance from the satellite to Lijiang varies from 560 to 1700 km. The overall length of the two-downlink channel varies from 1600 to 2400 km. (b) Measured two-downlink channel attenuation in one orbit using the high-intensity reference laser coaligned with the entangled photons. The highest loss is 82 dB at a total distance of 2400 km, when the satellite has just reached a 10° elevation angle observed from Lijiang station. Since its telescope (the largest) has a diameter of 1.8 m and thus has a higher receiving efficiency than other stations, when the satellite flies over Lijiang at an elevation angle of more than 15°, the channel loss remains relatively stable (from 64 to 68.5 dB). From Yin *et al.*, 2017a.

# 2) MICIUS -- Satellite-based Quantum Experiments

## C. Entanglement-based quantum key distribution

The key rate and the quantum bit error rate there (8.1%) were insufficient for performing entanglement-based quantum cryptography (Ekert, 1991)

The receiving efficiencies were considerably improved using a higher efficiency telescope and follow-up optics. Both ground stations used newly built telescopes with diameters of 1.2 m.

With these technical improvements, Yin et al. observed an average two-photon count **rate of 2 Hz** (corresponding to an increase of the two-photon link efficiency by a factor of 4), which significantly increased the obtained key rate and decreased the **quantum bit error rate from 8.1% to 4.5%.**

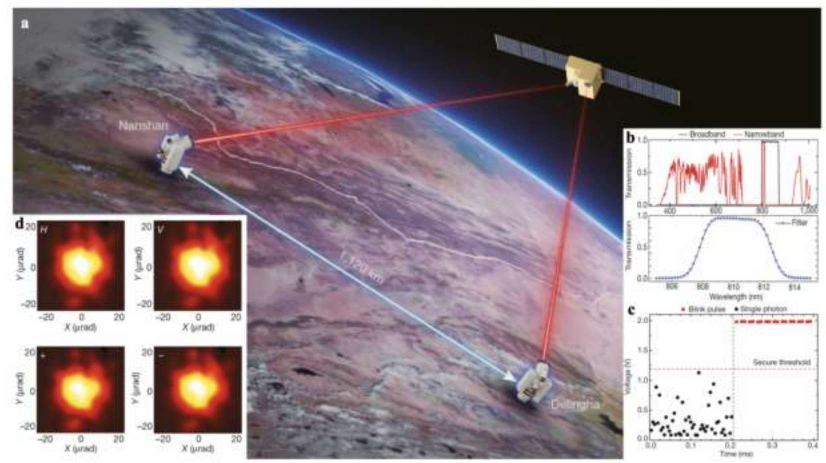



FIG. 33 Overview of the experimental set-up of quantum key distribution based on the entanglement distribution. (Yin *et al.*, 2020) (a) An illustration of the Micius satellite and two ground stations. Image credit: Fengyun-3C/Visible and Infrared Radiometer, with permission (2020). (b), (c), and (d) are monitoring and filtering against side channels. (b) The transmission of broad-bandwidth and narrow-bandwidth filters. (c) The output of monitoring circuit with/without blinding attack. Without blinding attack, the outputs are random avalanching single-photon-detection signals (black dots). With blinding attack (starting from 0.2 ms), the output signals are at around 2 V, which is clearly above the security threshold, thus triggering the security alarm. (d) The system detection efficiency of the four polarizations in the spatial domain. With the spatial filter, the four efficiencies are identical.

# 2) MICIUS -- Satellite-based Quantum Experiments

## D) Ground-to-satellite quantum teleportation

**Experiment:**

- Perform Quantum Teleportation of a single photon from an observatory ground station in Ngari to the satellite

**Challenges:**

- Loss of entangled photons during transmission through the Earth's atmosphere
    - Absorption and scattering of photons by the atmosphere
    - Can cause the entangled state to degrade and become unusable for teleportation

- Requires a multi-photon interferometry with a coincidence count rate several orders of magnitude lower than typical single or two-photon experiments.

**Additional challenges for uplink transmission:**

- Atmospheric turbulence in the uplink channel occurs at the **beginning of the transmission path**,

- Causes beam wandering and broadening that increases the amount of spreading of the traveling beams.

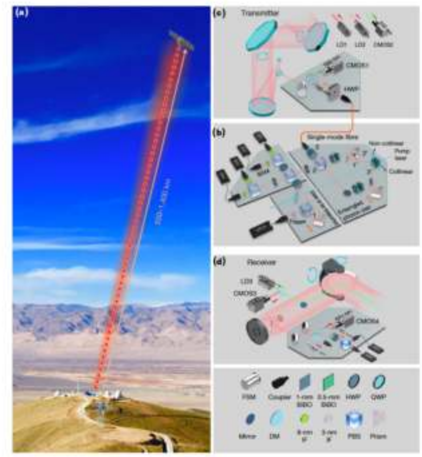
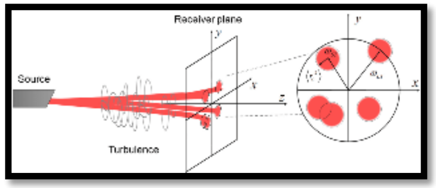


FIG. 34 Overview of the set-up for ground-to-satellite quantum teleportation of a single photon over distances of up to 1,400 km. (Ren *et al.*, 2017) (a) A schematic of the satellite is overlaid on a photograph of the Ngari ground station in Tibet. The separation between the satellite and the ground station varies from about 500 km to 1,400 km during quantum teleportation. (b) The compact multi-photon set-up for teleportation at the ground station. (c) The transmitter at the ground station. (d) The receiver on the satellite.



# 2) MICIUS -- Satellite-based Quantum Experiments

## E) Satellite-relayed intercontinental quantum key distribution


FIG. 37 Schematic of key exchange procedure between Graz and Xinglong with the satellite as a trusted relay (Liao et al., 2018). After Micius distributed a key with Graz (MG) and Xinglong (MX), it performs a bitwise exclusive OR between those keys (MX ⊕ MG) and sends this combined key via a classical channel towards Xinglong station. Combining the XORed key at Xinglong with MX leads to the same key (MG) on both sides.

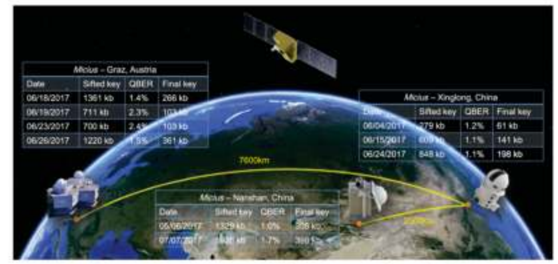


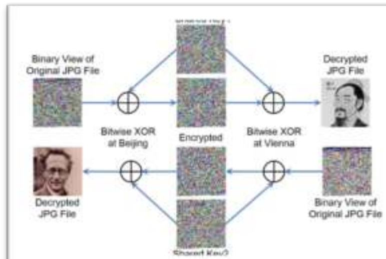

FIG. 36 Illustration of the three cooperating ground stations (Graz, Nanshan, and Xinglong). Listed are all paths used for key generation and the corresponding final key length. (Liao et al., 2018)

**- Goal:**

- Satellite acting as a trustful relay to connect points on Earth to form a network for high-security key exchange

**- Example:**

- Satellite establishes a secure key between itself and city A (MA key)
- Satellite establishes another key between itself and city B (MB key)
- Micius can act as a trusted relay by simply performing bitwise exclusive OR operations between the two keys
- Which then yields a new string: MA⊕MB
- The new string can be sent through a classical communications channel to city A or B
- Which decodes other original keys using another exclusive OR (i.e. MA=(MB⊕MA)⊕MB)




**- Experimentation:**

- 100 kB secure key was established between Xinglong and Graz.
- 10 kB of the key was used to transmit a picture of **Micius** from Beijing to Vienna, and a picture of **Schrodinger** the other way (One-time-pad)
- The other 70 kB of the secure key was:
    - Combined with the advanced encryption standard (AES)-128 protocol
    - Then used in a **video conference** between Beijing and Vienna for 75 minutes with total data transmission of about 2 GB.

# Section 3
# Outlook for the future

# 3) Outlook

- **Other Quantum Satellite Projects**

**Canada**: Quantum Encryption and Science Satellite (QEYSSat) (2024–2025)

$1.5 million funding (2017)

$30 million funding (2019)

**USA/Europe**: NASA quantum satellite link: "Marconi 2.0".

**Europe**: Nanobob, ESA's Eagle-1 quantum key distribution satellite (2024)

**Singapore**: 3U CubeSat involving an entangled photon source

**International**: CubeSat Quantum Communications Mission (CQuCoM)

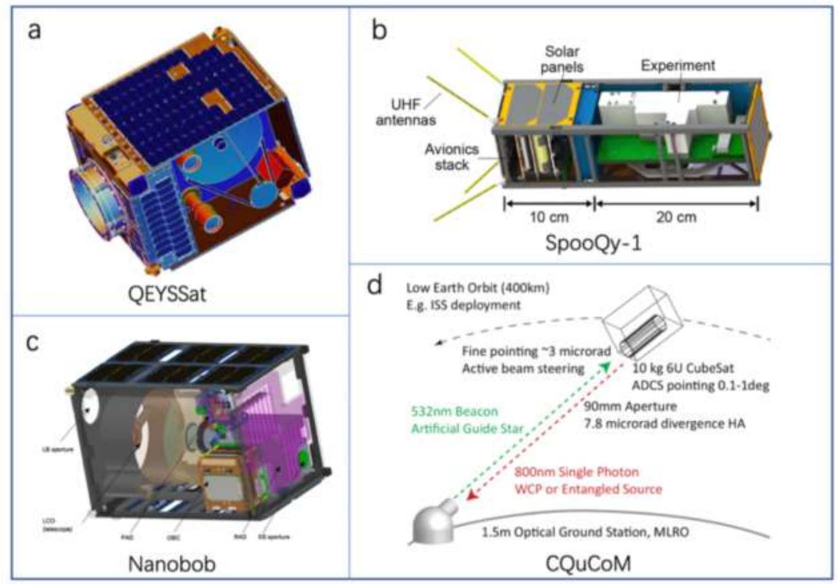
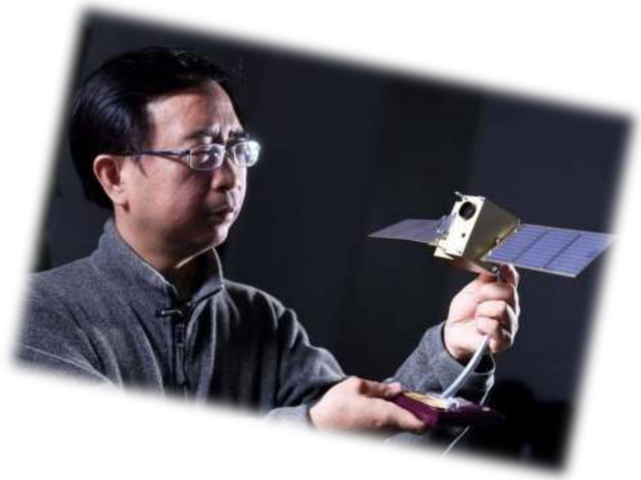



FIG. 40 Other quantum satellite plans besides Micius. (a) The Quantum Encryption and Science Satellite (QEYSSat) project in Canada (Jennewein *et al.*, 2014; Pugh *et al.*, 2017). (b) The 3U Cubesat involving an entangled photon source developed by the group in National University of Singapore (Villar *et al.*, 2020). (c) The CubeSat-based mission concept Nanobob proposed by researchers of France and Austria (Kerstel *et al.*, 2018). (d) The CubeSat Quantum Communications Mission (CQuCoM) jointly undertaking by a joint research team (Oi *et al.*, 2017).

# 3) Outlook



- **Outlook for the Chinese Team**

- Micius is only the beginning according to them

- Two goals in the next 5 to 10 years (2022):

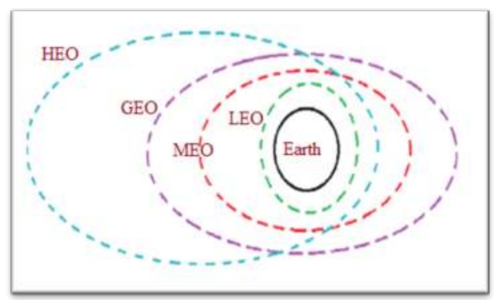
**1)** Develop 3 to 5 small LEO satellites dedicated to QKD missions, which will provide more practical and efficient QKD services.

**2)** Develop a medium-Earth orbit (MEO)-to-geosynchronous-orbit (GEO) quantum science satellite that involves ambitious scientific goals.

- Why?

- LEO vs Higher orbit satellites → Much longer **service time** and **wider coverage**

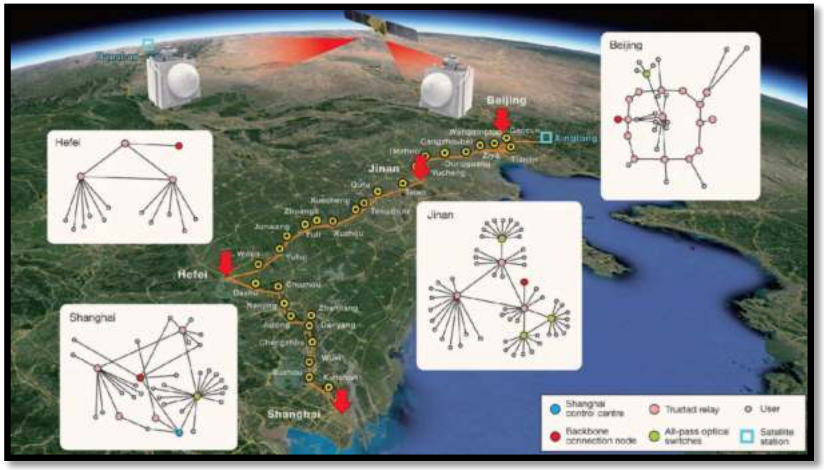
- High-orbit satellite + LEO satellites → Quantum Constellation for **Global Services**



# 3) Outlook

- **Other achievement from their team**

- **World's first integrated quantum communication network**
- Combining over **700 optical fibers** on the ground with 2 ground-to-satellite links
- Network can achieve quantum key distribution over a total distance of **4.600 km**



# 3) Outlook

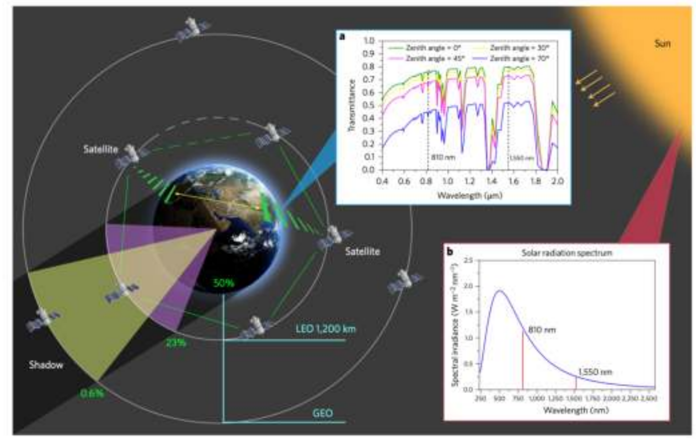



**Figure 1 | Satellite-constellation-based global quantum network.** A global quantum network needs many LEO satellites or several geosynchronous orbit satellites to create a satellite constellation. The time that a satellite is in the Earth shadow zone, which we call night, is inversely proportional to the orbit height of the satellite. **a**, Transmittance spectra from visible to near-infrared light in the atmosphere at selected zenith angles. **b**, Solar radiation spectrum from visible to near-infrared light.

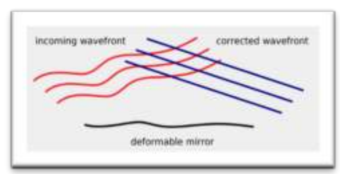
- **Daytime quantum communications**

- **Some Major Drawbacks of MICIUS**:
  - Limited capacity at Night (Requires Earth's Shadow)
  - Limited availability (8 minutes per experimentations)
  - Limited coverage (500km radius)
  - Weather conditions are important

- **Main challenge of daytime operations → Strong Background Noise from the Scattered Sunlight**
  - Typically **five orders of magnitude greater** than the background noise during night time
  - More serious problem for higher orbit satellites → Time spent in Earth's shadow zone is inversely proportional to the orbit height of the satellite
  - A LEO satellite system has a ~ 70% probability of being in the sunlight area, and for GEO satellites, this probability increases to ~ 99% (Gilmore, 2002).

- Some methods can be used to improve LEO satellites performances
  - Ex: Improved Filtering, Wavelength changes, …
  - Sun is 1/5 as bright at 1,550 nm as it is at 800 nm… And 1,550-nm light has reduced atmospheric interference

- For higher-orbit satellites working in day time:
  - Due to the **longer distances** and the **associated diffraction loss (beam spreading in free space)**
  - New techniques are needed for better link efficiency
  - Ex: Large-size telescopes, better APT systems, and wavefront correction through **adaptive optics**…



# 3) Outlook

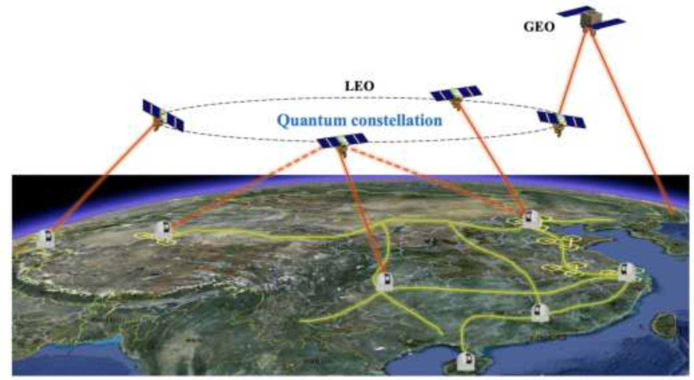



FIG. 46 The roadmaps towards the global quantum communication network. Intra-city metropolitan networks will be created using fibers. Quantum repeaters can connect the metropolitan networks. Long-distance and intercontinental quantum communication will be realized via satellite-based quantum channels.

- **Satellite-Constellation-based Quantum Networks**

- Solution to previous drawback → **Satellite constellations**
- A mix of LEO and high-Earth-orbit (HEO) satellites are necessary

- What is needed?
    - Increasing the number of satellites
    - Raising the orbital altitudes
    - Miniaturization and low-cost designs for satellites
        - LEO satellites / ground stations are more concerned (large margin in channel efficiency)
        - Higher channel losses of HEO-satellite-based QKD will limit their design sacrifices

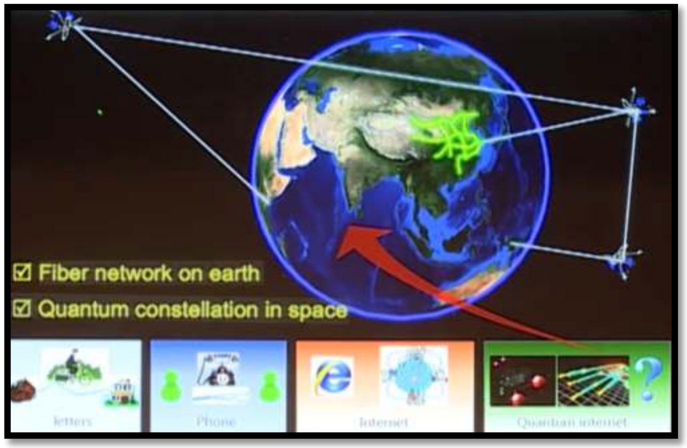
- Limitations of each regime:
    - LEO systems: Limited by ground contact duration
    - GEO systems: Better lifetime (4x), better contact duration (18x), but benefits almost cancelled by decreased key rates due to the increased distance (1/100)

# 3) Outlook

- Their vision: **Global Quantum Network**

- Combination of:
    - Fiber networks on Earth
    - Quantum satellite constellations in space

- According to them, this could allow the **Quantum Internet**



# 3) Outlook

- ## Quantum Communication across Interstellar Distances

- For the curious ones… Could we achieve quantum-enabled secure communications across interstellar distances?

- Article [4] demonstrated that:
    - Quantum communication signal can propagate through large interstellar distances without decoherence
    - X-rays have mean free paths long enough to even cross galactic distances without interactions
    - The same applies for radiation at radio frequencies and up to the microwave region

*- Across interstellar distances, can the quantum coherent state of a photon be sustained? What are the **relevant factors to consider which could induce decoherence** of the traveling photon?*
    - Gravitational field of astrophysical bodies
    - The local environment of the Solar System
    - Magnetic fields in galaxies
    - Particle content in the interstellar medium
        - Distribution of hydrogen, electrons, protons and photons from the cosmic microwave background (CMB), as well as some other heavier elements
        - The interstellar medium is dominated by electrons, protons and CMB photons… interactions with this background is negligible
        - However, gas and dust are also present in the interstellar medium of the galaxy, with traces of heavier elements… Photons will interact with them through photo absorption and photoionization

- How to quantify the effect of gravity on the quality of a quantum channel?

See *"**Probing gravity-induced decoherence**"* in [1] (MICIUS experimentation not covered in this presentation)

# References


[1] Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." arXiv preprint arXiv:2003.06557 (2020).

[2] Liao, Sheng-Kai, et al. "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication." Nature Photonics 11.8 (2017): 509-513.

[3] Lu, Chao-Yang, et al. "Micius quantum experiments in space." Reviews of Modern Physics 94.3 (2022): 035001.

[4] Berera, Arjun, and Jaime Calderón-Figueroa. "Viability of quantum communication across interstellar distances." Physical Review D 105.12 (2022): 123033.

[5] Liao, Sheng-Kai, et al. "Satellite-to-ground quantum key distribution." Nature 549.7670 (2017): 43-47.

# Thank you

- Questions ?