Entanglement-based QKD from Micius

Juan Yin

CAS Center for Excellence in Quantum Information and Quantum Physics

University of Science and Technology of China

08/27/2018
Team

Jian-Wei Pan
Chief scientist
Quantum Science Satellite

Cheng-Zhi Peng
Chief engineer
The scientific part of
Quantum Science Satellite

Excellence Center for Quantum Information and Quantum Physics
University of Science and Technology of China (USTC)
Shanghai Institute of Technical Physics of the Chinese Academy of Sciences

Shanghai Engineering Center for Microsatellite
The Institute of Optics and Electronics, the Chinese Academy of Sciences
National Astronomical Observatories, Chinese Academy of Sciences
Quantum Communication

Single-particle-based secret key distribution
Bennett & Brassard (1984)

Entanglement-based secret key distribution
Ekert, PRL 67, 661 (1991)

The six “fathers” of quantum teleportation

Bennett et al., Phys. Rev. Lett. 73, 3801 (1993)
Quantum Communication

- Cube-sat
- Montreal, Waterloo, etc.

- United States
- Quantum network (DAPRA)
- Los Alamos, NASA, IBM, MIT, Harvard, Caltech …

- Canada

- Europe
- Space-QUEST for space quantum communication
- Cube-sat

- Japan
- “Socrates” satellite channel test
- Quantum network in Tokyo

- Singapore
- Satellite with entanglement source
Quantum Communication in China

Fiber based Quantum Communication

100km Decoy-QKD
Peng et al., PRL 98, 010505 (2007)

200km Decoy-QKD
Liu et al., Optics Express 18, 8587 (2010)

404km MDI-QKD
Yin, et al., PRL. 117, 190501 (2016)

Free Space Quantum Communication

13km quantum entanglement distribution

16km quantum teleportation

100km quantum entanglement distribution
Yin et al., Nature 488, 185 (2012)

QKD toward satellite
Wang et al., Nature Photonics 7, 387–393 (2013)
The "Quantum Science Satellite" project was officially approved.

2011

The first prototype satellite started.

2012

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

2014

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

2015

Lijiang and Ali was complete.

2016

The satellite was launched.
“Micius” Quantum Science Satellite

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

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

Launched on 16th Aug. 2016
Experiments of “Micius” Quantum Satellite

- Quantum key distribution from satellite to earth [Nature 549, 43 (2017)]
- Entanglement distribution over thousand km [Science 356, 1140 (2017)]
- Quantum teleportation from earth to satellite [Nature 549, 70 (2017)]

“Micius” has already achieved the three main scientific goals
New experiments are in progress
“Micius” Quantum Science Satellite

Telescope 1

Telescope 2

Exp. Control

Entanglement source

Xinglong

Delingha

Nanshan

Lijiang

Ngari
“Micius” Quantum Science Satellite

- 532nm beacon and synchrotron laser source
- 850nm synchrotron laser source
- 850nm decoy state source
- 671nm beacon laser detector
- 1064nm synchrotron laser detector
- 780nm quantum signal detector
Further Experiments with Micius

Collaborations with more countries are ongoing!
Satellite-relayed intercontinental QKD
Satellite-relayed intercontinental QKD

Intercontinental Quantum Key Distribution

Liao et al., PRL 120, 030501 (2018)

Jointly explore the feasibility of global QC
High speed satellite-to-ground QKD

✓ Efficient BB84 QKD/ biased-basis QKD; Sifting efficiency 50% => 77%
✓ Repetition rate 100Mhz => 200Mhz
✓ Improved receiving efficiency 20% => 45%

Ground station upgrade
Micius->NanShan
- Max Sifted key rate ~450kbps
- QBER ~1%
- Final key ~12 Mbits
- Final key rate ~40kbps
High speed satellite-to-ground QKD
Entanglement-based QKD

Quantum cryptography based on Bell’s theorem
Ekert, PRL 67, 661 (1991)

Quantum cryptography without Bell’s theorem
Bennett&Brassard&Mermin, PRL 68, 557 (1992)

Without relying on trustful relay

“Satellite/entangled photon source could even be in the hands of an adversary”

“This would achieve the holy Grail that all cryptographers have been dreaming of for thousands of years”
Entanglement-based QKD

II-type PPKTP in Sagnac

In-orbit test

- Visibility 20:1@2M
- Rate 8 MHz

<table>
<thead>
<tr>
<th>Date</th>
<th>S</th>
<th>σ</th>
<th>S. d.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016.10.19</td>
<td>2.442</td>
<td>0.012</td>
<td>37</td>
</tr>
<tr>
<td>2016.10.20</td>
<td>2.436</td>
<td>0.012</td>
<td>36</td>
</tr>
<tr>
<td>2016.10.21</td>
<td>2.379</td>
<td>0.012</td>
<td>32</td>
</tr>
</tbody>
</table>
Entanglement-based QKD

Satellite-to-ground entanglement-based QKD

- Distance: 530km-1000km
- Channel loss: 29dB-36dB
- Final key: 3.5bits/s (1% sampling)

Yin et al., PRL 119, 200501 (2017)
Remote state preparation

Bennett et al., PRL 87, 077902 (2001)
Some new attempts with satellite-borne entanglement source

The integrated MZI

- Extinction ratio of MZI: > 88:1
- Channel loss: 64 dB - 82 dB
- Average fidelity: > 80%
Address loopholes in Bell Test

✓ Involve human observers for addressing the loopholes.

✗ Freedom of choice loophole: random number generators (RNGs) could be prior correlated ➔ the choice of measurement bases are not truly random

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

✗ 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)

Requirement:
Quantum signal transit time exceeds human reaction 100ms ➔
✓ Entanglement distribution at a distance on the order of one light-second
✓ Ultra-high brightness Entanglement source is needed
Address loopholes in Bell Test

Present a proposal between Earth and Moon to address freedom-of-choice and collapse loopholes.

- Proof-of-principle exp.: Bell test with human supplying random measurement over simulated extremely high loss channel (103dB)

  *Cao et al., PRL 120, 140405 (2018)*

Challenging local realism with human choices

- Generating random numbers with the help of worldwide 100,000 volunteers’ free will
- 12 labs run Bell tests with the human’s random numbers (ICFO, ICREA, ETH Zurich, USTC, et al.)

  *Nature 557, 212-216 (2018)*

GHz entanglement source for the Bell test between Earth and Moon
Future Prospect: Quantum Exp. Between Earth and Moon

- Large-scale Bell test with Human-observer
- Realize the truly loophole-free Bell test between Earth and Moon with quantum memory and event-ready scheme?

Entanglement distribution between Moon and Earth with China’s future Moon landing project!
Future Prospect: Global Quantum Network

- Experiment time is ~ 8 minutes for each pass
- Coverage range is about 500km (Radius)
- Have to be in the shadow of earth
- Weather condition affects

☑ Fiber quantum network
☑ Quantum constellation with LEO nano satellites
☑ GEO satellite
Challenge of global quantum network -- Quantum constellation

**Quantum key satellite network**

- 3-5 nano quantum satellites
- Provide key distribution services to more than 100 ground stations worldwide
Challenge of global quantum network -- Quantum constellation

The movable ground station

The low-cost ground station
Challenge of global quantum network – GEO satellite

Quantum key distribution based on entanglement with GEO satellite

- Wider space scale
  - 10000-36000km (all over)
- Longer experiment duration
  - Form minutes to hours
- Better micro-gravity
  - $10^{-6}$-$10^{-7}$g
Outlook: Global Quantum Network

- Fiber network on earth
- Quantum constellation in space

- letters
- Phone
- Internet
- Quantum internet
Thank you!