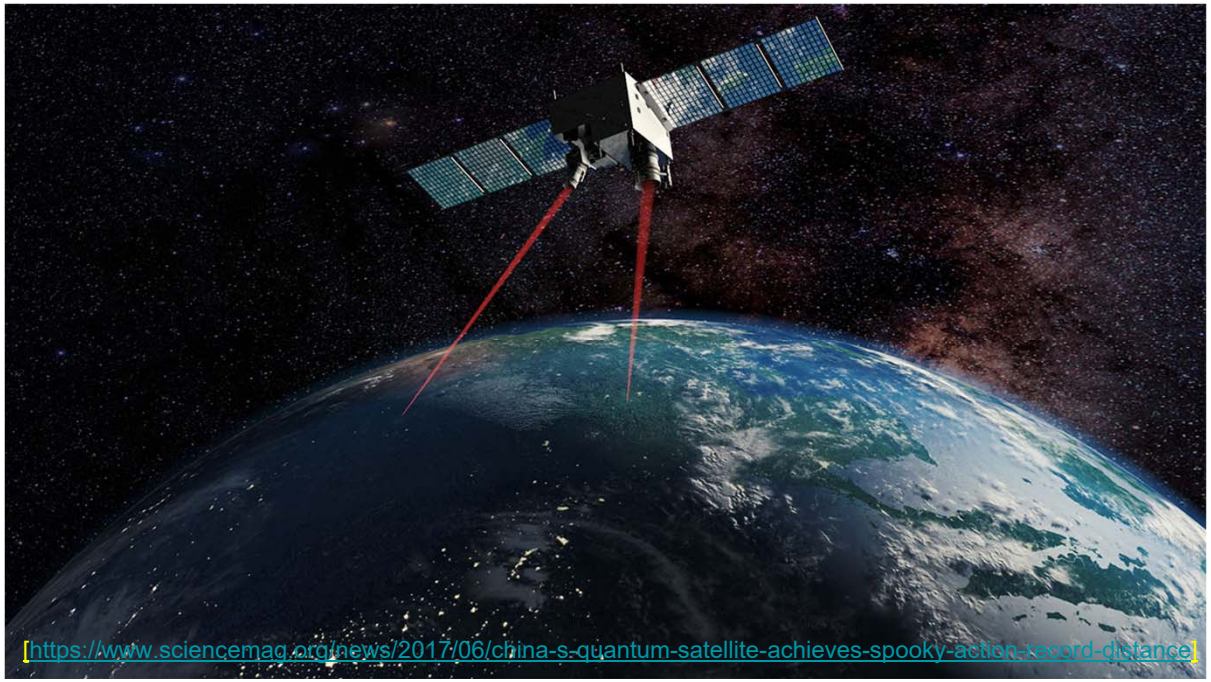
Satellite-Relayed Intercontinental Quantum Network

Rachel Birchmier, Andrew Conrad, Darshan Chalise, Brian Doolittle

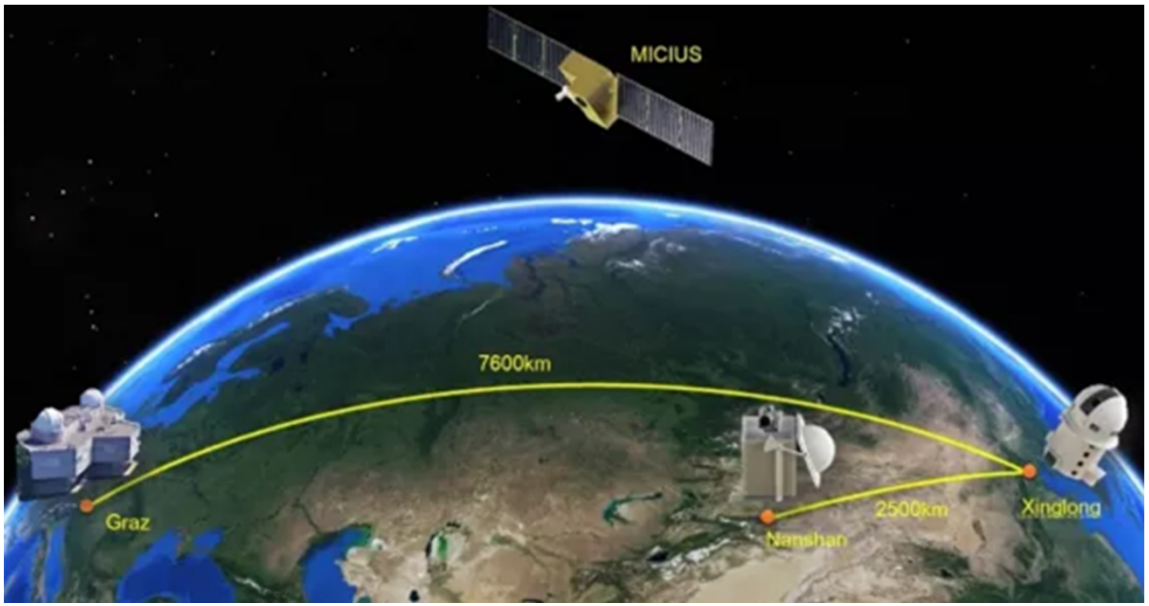
[Sheng-Kai Liao, et al. *Phys. Rev. Lett.* **120**, 030501 (19 January 2018)]



[https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance]

Intercontinental Quantum Key Distribution (QKD)

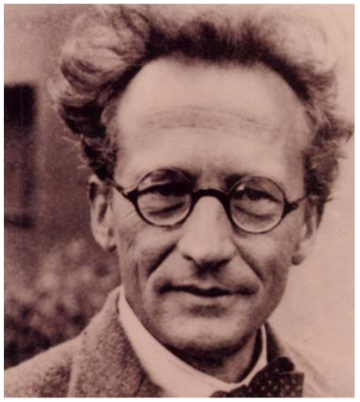
- A satellite, Micius, uses single photon pulses to securely distributes keys to ground stations in Austria and China.
- The keys enable the ground stations to securely encrypt communications.



Keys are successfully distributed over distances of 7600 km between Xinglong and Graz or 2500 km between Xinglong and Nanshan.

[Sheng-Kai Liao, et al. *Phys. Rev. Lett.* **120**, 030501 (19 January 2018)]

Testing the Quantum Network



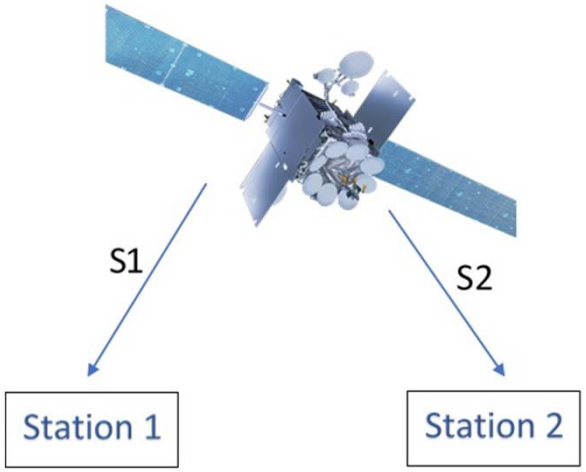
Schrodinger to Xinglong station

Image of Micius to Graz/Vienna

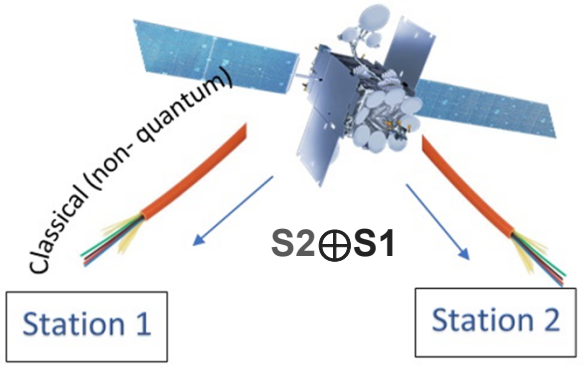
- Micius distributes a ~215 kb key with an error of ~1.5% to each station, daily
- Ground stations use keys to securely communicate
  - Shared images over classical channels
  - Held a 75 min video conference between Austria and China with the help of China’s terrestrial fiber network

Distributing Quantum Keys

- Micius sends different signals or quantum keys to each station

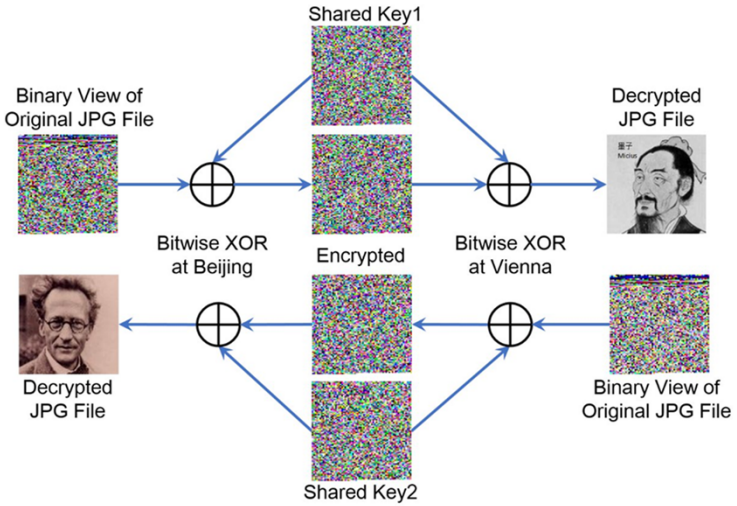


- The signals are mixed using an exclusive or (XOR).
- The XOR'ed signal is sent to each station by classical means.



Sharing Keys Between Ground Stations

- Each ground station determines the other's private key using the XOR'ed signal from the satellite and their own key
  - $S1=(S2 \oplus S1) \oplus S2$
  - $S2=(S2 \oplus S1) \oplus S1$
- The keys are used to securely encrypt communications between ground stations

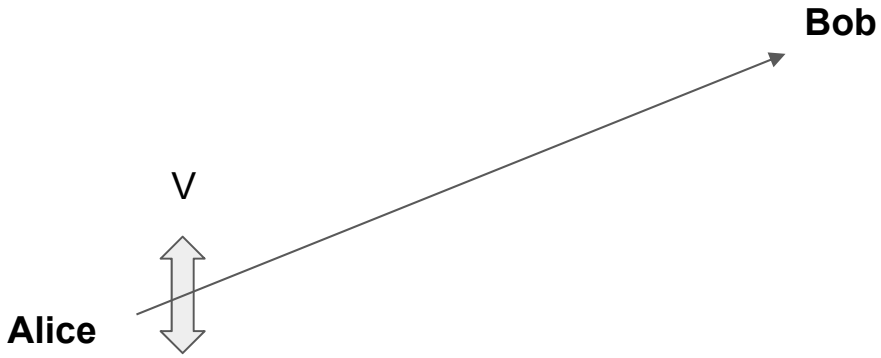


China and Austria securely share pictures of Schrodinger and Micius

[Sheng-Kai Liao, et al. *Phys. Rev. Lett.* **120**, 030501 (19 January 2018)]

How does QKD work?

Bennett and Brassard in 1984



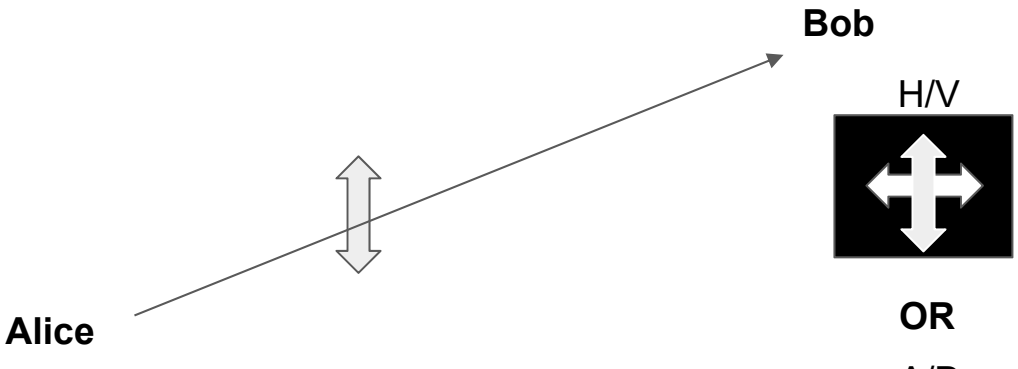
State:	Basis:
↔	Horizontal/Vertical (H/V)
↕	Horizontal/Vertical (H/V)
↘↖	Anti-Diagonal/Diagonal (A/D)
↙↗	Anti-Diagonal/Diagonal (A/D)

Protocol

- Alice sends one of the four polarization states at random to Bob

How does QKD work?

Bennett and Brassard in 1984



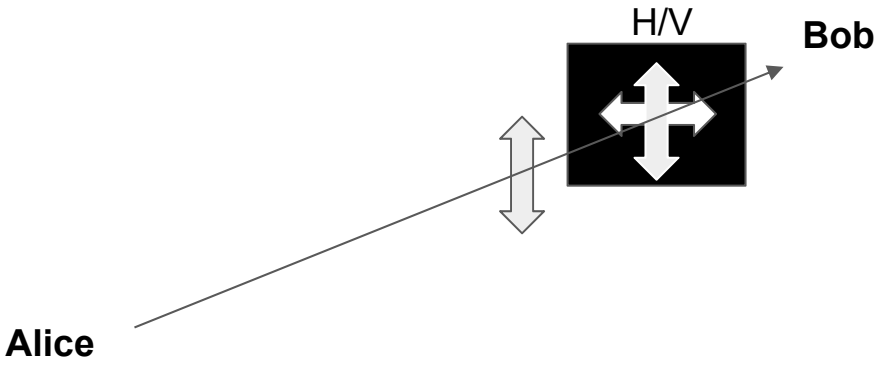
State:	Basis:
↔	Horizontal/Vertical (H/V)
↕	Horizontal/Vertical (H/V)
⤡	Anti-Diagonal/Diagonal (A/D)
⤢	Anti-Diagonal/Diagonal (A/D)

Protocol

- Alice sends one of the four polarization states to Bob
- Bob randomly selects a basis to measure

How does QKD work?

Bennett and Brassard in 1984



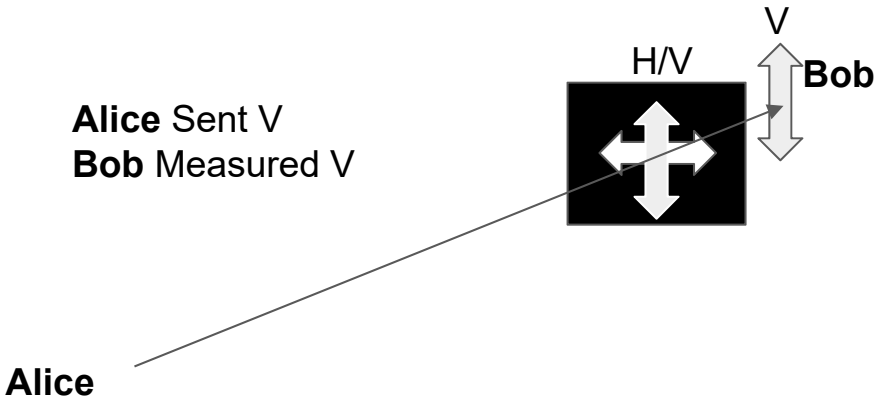
State:	Basis:
↔	Horizontal/Vertical (H/V)
↕	Horizontal/Vertical (H/V)
⤡	Anti-Diagonal/Diagonal (A/D)
⤢	Anti-Diagonal/Diagonal (A/D)

Protocol

- Alice sends one of the four polarization states to Bob
- Bob randomly selects a basis to measure

How does QKD work?

Bennett and Brassard in 1984



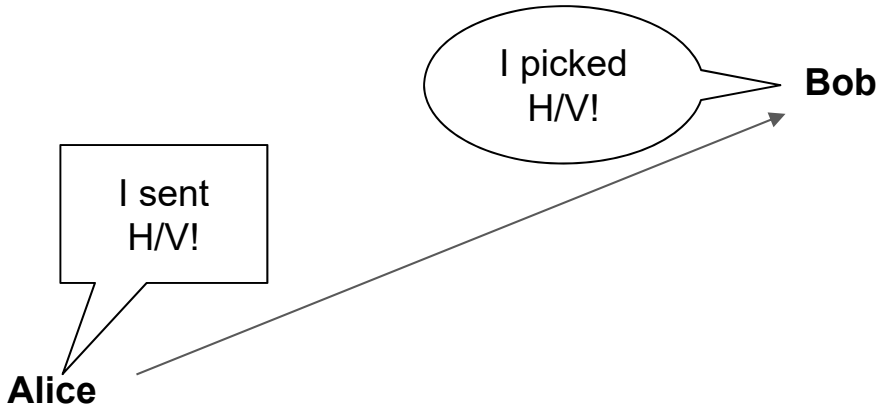
State:	Basis:
↔	Horizontal/Vertical (H/V)
↕	Horizontal/Vertical (H/V)
⤡	Anti-Diagonal/Diagonal (A/D)
⤢	Anti-Diagonal/Diagonal (A/D)

Protocol

- Alice sends one of the four polarization states to Bob
- Bob randomly selects a basis to measure, then records the result

How does QKD work?

Bennett and Brassard in 1984



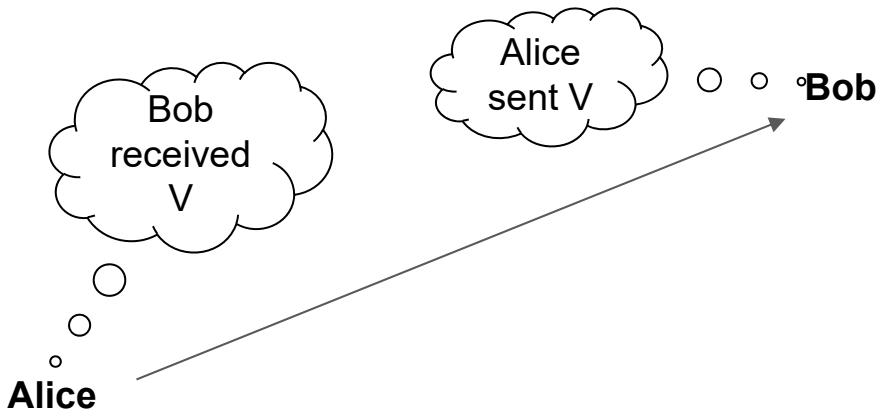
State:	Basis:
↔	Horizontal/Vertical (H/V)
↕	Horizontal/Vertical (H/V)
⤡	Anti-Diagonal/Diagonal (A/D)
⤢	Anti-Diagonal/Diagonal (A/D)

Protocol

- Alice sends one of the four polarization states to Bob
- Bob randomly selects a basis to measure then records the result
- Afterwards Alice and Bob announce which basis they used

How does QKD work?

Bennett and Brassard in 1984



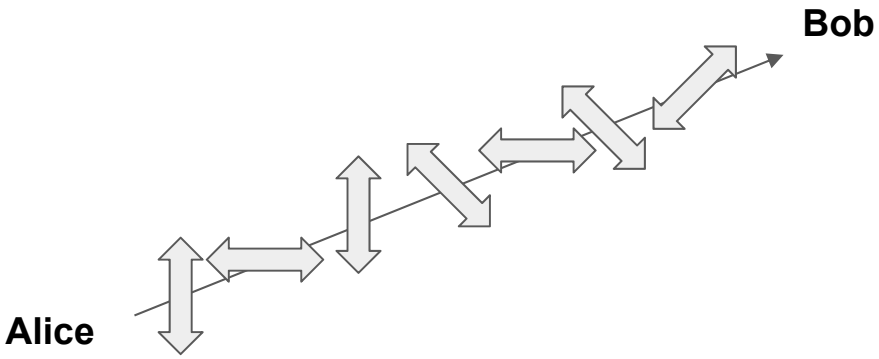
State:	Basis:
↔	Horizontal/Vertical (H/V)
↕	Horizontal/Vertical (H/V)
⤡	Anti-Diagonal/Diagonal (A/D)
⤢	Anti-Diagonal/Diagonal (A/D)

Protocol

- Alice sends one of the four polarization states to Bob
- Bob randomly selects a basis to measure then records the result
- Afterwards Alice and Bob share which basis they used
- If Bob chose the right basis, then their results will match

How does QKD work?

Bennett and Brassard in 1984



State:	Basis:
↔	Horizontal/Vertical (H/V)
↕	Horizontal/Vertical (H/V)
⤡	Anti-Diagonal/Diagonal (A/D)
⤢	Anti-Diagonal/Diagonal (A/D)

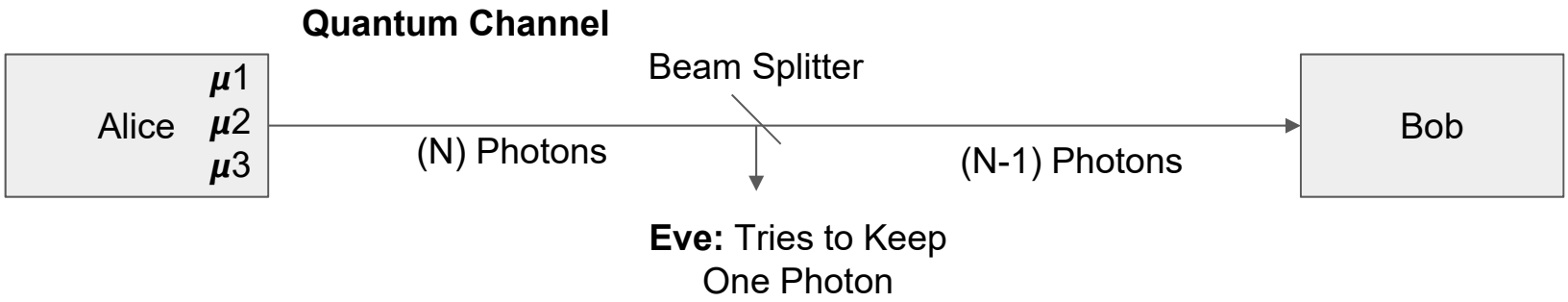
Protocol

- Alice sends one of the four polarization states to Bob
- Bob randomly selects a basis to measure then records the result
- Afterwards Alice and Bob share which basis they used
- If Bob chose the right basis, then their results will match, then repeat

How to Prevent Eavesdropping

Decoy State BB84 - transmits a weak coherent state (WCS) of varying intensities [1]

- Motivation: Decoy State BB84 is used to counter Photon Splitting Attack
- It has been shown that only 3 intensities are required [2]

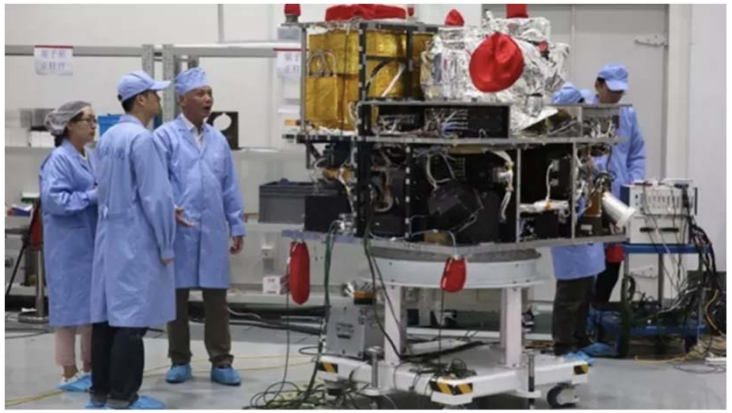


1. Wang, Dong, et al. *Scientific reports* 5 (2015): 15130.
2. Wang, Xiang-Bin. *Physical review letters* 94.23 (2005): 230503.

Hardware Overview

Source:

- Weak Coherent Laser Pulses
- 850 nm Fiber-Coupled Lasers (8 Channels)



Micius Satellite [1]

Optics:

- Photons are sent to an encoder, consisting of a half-wave plate and two polarizing beam splitters (PBS)
- Output is randomly one of the following four polarization states: H, V, A, D

1. https://www.smh.com.au/technology/chinese-quantum-satellite-micius-breaks-record-for-distribution-distance-of-quantum-entangled-photons-20170615-gwrh0u.html

Past Successes in QKD

Fiber Optics

- QKD through 150 Km fiber optic (2006) [1]
- Intercity QKD using trusted relays (2010) [2]

1. Hiskett, P A, et al. *New Journal of Physics*, 8 (9): 193.
2. Chen, Teng-Yun, et al. *Optics Express*, 18 (26): 27217.

Fiber relay stations enable secure keys to be distributed to multiple locations in a city [2]

Free-space transmission is performed by drones in the Kwiat lab.

Free-space transmission

- 144 Km using entanglement (2006) [3]
- Distribution using airplanes and drones [4]

3. Nguyen, Kim-Chi et.al. (2006). *Nature Physics*. **3** (7): 481–486.
4. Pugh, C. J.; Kaiser, et al. *Quantum Science and Technology*. **2** (2): 024009

Critiques of satellite based Quantum Key Distribution

- It may be too expensive to establish in a large scale
- It cannot be used during daytime or bad weather
- Key lengths are too short to practically secure communications
- Satellite is susceptible to classical hacking or physical attacks
- Quantum key distribution networks are susceptible to denial of service attacks

A Race for Quantum Technology has Begun

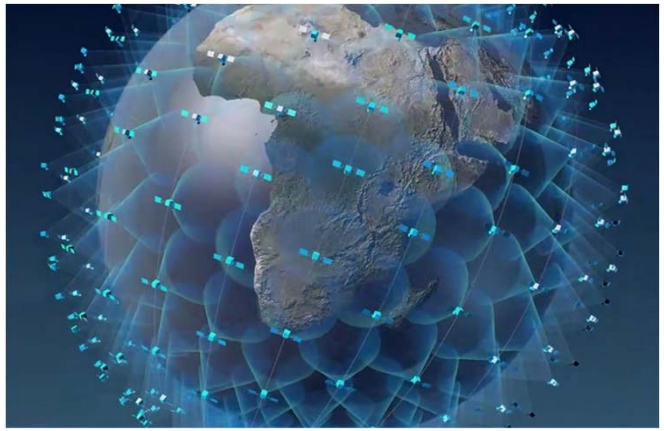
- Quantum key distribution via satellite is a huge accomplishment
- The success of China and Austria motivates other nations to invest in quantum technology [Lin J. et al. “China’s Quantum Satellite Could Change Cryptography Forever.” *Popular Science* (3 March 2016)]

Launch of Micius, China’s quantum-enabled satellite
[https://www.bbc.com/news/world-asia-china-37091833]

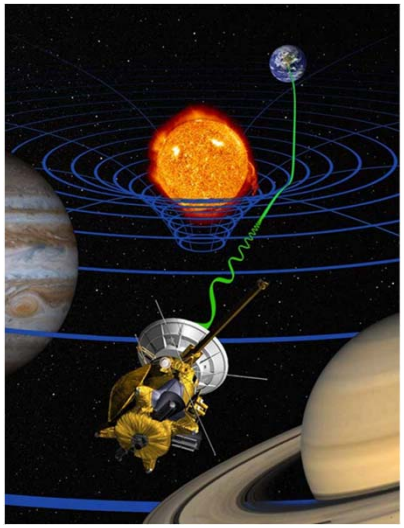
Motivates Future Work

Quantum Internet [Kimble, H. J. *Nature* **453**, 1023-1030]

- Improve performance and scale of satellite key distribution.
- Distribute quantum keys globally.



OneWeb's proposal for an internet satellite network
[https://www.nbcnews.com/science/space/oneweb-wins-500-million-backing-internet-satellite-network-n381691]



Precision measurement of general relativity
[https://solarsystem.nasa.gov/news/12249/saturn-bound-spacecraft-tests-einsteins-theory/]

Quantum Experiments in Space
[Agnesi, C. et al. *Phil. Trans. R. Soc. A 2018* **376** 20170461.]

- Satellites may perform quantum optics experiments over curved spacetime
  - E.g. decoherence due to curved spacetime

Conclusions

- Intercontinental quantum key distribution was successfully performed by satellite.
- Technical improvements are required for practical use.
- Key distribution is secure against eavesdropping, but is not globally secure.

The Austrian ground station receives quantum keys by satellite

[https://www.oeaw.ac.at/en/events-communication/public-relations-communication/public-relations-communication/ausgewaehlte-oeaw-pressemeldungen/press-releases/first-quantum-satellite-successfully-launched/]

Questions?

References

1. Hiskett, P A, et al. “Long-Distance Quantum Key Distribution in Optical Fibre.” *New Journal of Physics*, vol. 8, no. 9, 2006, pp. 193–193., doi:10.1088/1367-2630/8/9/193.
2. Chen, Teng-Yun, et al. “Metropolitan All-Pass and Inter-City Quantum Communication Network.” *Optics Express*, vol. 18, no. 26, Oct. 2010, p. 27217., doi:10.1364/oe.18.027217.
3. Yin, Juan; Cao, Yuan; Li, Yu-Huai; Liao, Sheng-Kai; Zhang, Liang; Ren, Ji-Gang; Cai, Wen-Qi; Liu, Wei-Yue; Li, Bo; Dai, Hui; et al. (2017). "Satellite-based entanglement distribution over 1200 kilometers". *Science*. **356** (6343): 1140–1144. arXiv:1707.01339. doi:10.1126/science.aan3211. PMID 28619937.
4. Nguyen, Kim-Chi; Gilles Van Assche; Cerf, Nicolas J.; Weier, H.; Scheidl, T.; Lindenthal, M.; Blauensteiner, B.; Jennewein, T.; Perdigues, J.; Trojek, P.; Ömer, B.; Fürst, M.; Meyenburg, M.; Rarity, J.; Sodnik, Z.; Barbieri, C.; Weinfurter, H.; Zeilinger, A. (2006). "Free-Space distribution of entanglement and single photons over 144 km". *Nature Physics*. **3** (7): 481–486. arXiv:quant-ph/0607182. doi:10.1038/nphys629.
5. Pugh, C. J.; Kaiser, S.; Bourgoin, J.- P.; Jin, J.; Sultana, N.; Agne, S.; Anisimova, E.; Makarov, V.; Choi, E.; Higgins, B. L.; Jennewein, T. (2017). "Airborne demonstration of a quantum key distribution receiver payload". *Quantum Science and Technology*. **2** (2): 024009. arXiv:1612.06396. Bibcode:2017QS&T....2b4009P. doi:10.1088/2058-9565/aa701f.
6. Grant, A. “Intercontinental Quantum Communication.” *Physics Today* **71**, 3, 24 (2018).
7. Kimble, H. J. “The Quantum Internet.” *Nature* **453**, 1023-1030 (19 June 2008).
8. Rideout, D. et al. “Fundamental Quantum Optics Experiments Conceivable with Satellites--Reaching Relativistic Distances and Velocities.” *Classical and Quantum Gravity.* **29** 22, (18 October 2012).
9. Agnesi, C. et al. “Exploring the Boundaries of Quantum Mechanics: Advances in Satellite Quantum Communications.” *Phil. Trans. R. Soc. A 2018* **376** 20170461. (28 May 2018).
10. Lin J. et al. “China’s Quantum Satellite Could Change Cryptography Forever.” *Popular Science* (3 March 2016)
11. Howarth, F. “The Role of Human Error in Successful Security Attacks.” *Security Intelligence*
12. https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/ (2 September 2014).