Master Seminar: Your passion for physics
Quantum Key Distribution

Kilian Welz
Heidelberg University

December 7, 2021

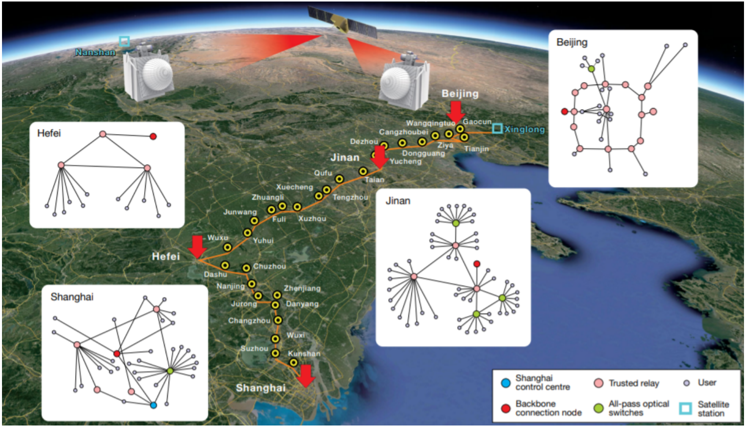


Figure 1: The Shanghai-Beijing integrated space-to-ground quantum network (adapted from [1])

Quantum Key Distribution methods

Bennet-Brassard protocol:

- polarized single photons
- sent via optical fiber
- a lot channel loss

Entanglement distribution protocol:

- entangled pairs of photons
- satellite-to-ground link
- less channel loss

Outline

Bennet-Brassard '84 protocol

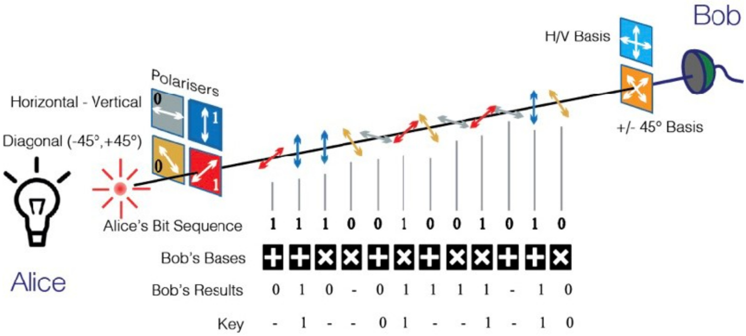


Figure 2: The scheme for the BB'84 protocol (adapted from https://qt.eu/discover-quantum/underlying-principles/quantum-key-distribution-qkd/)

1. Send random key in random bases
2. Compare bases publicly
3. Sift key
4. Error correction and verification

Bennet-Brassard '84 setup

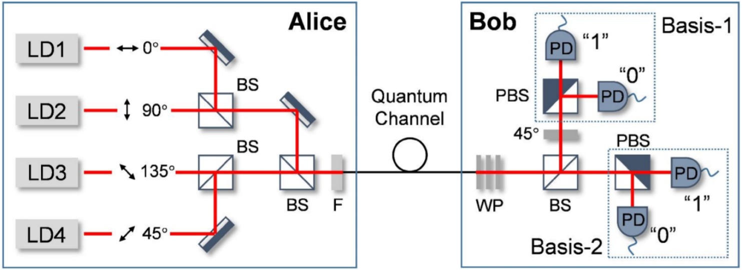


Figure 3: A typical system for BB84 QKD polarization encoding (adapted from http://www.e-jikei.org/Conf/ICMEMIS2017/proceedings/materials/proc_files/GS_papers/GS-03/ICMEMIS2017-GS-03.pdf)

- LD: Laser diode
- BS: Beam splitter
- WP: Wave plate
- PBS: polarizing Beam splitter

Photon number splitting attack

$$-coherent\ laser\ pulse : |\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \qquad (1)$$

$|\alpha|^2$: average photon number
$|n\rangle$: n photon Fock-state

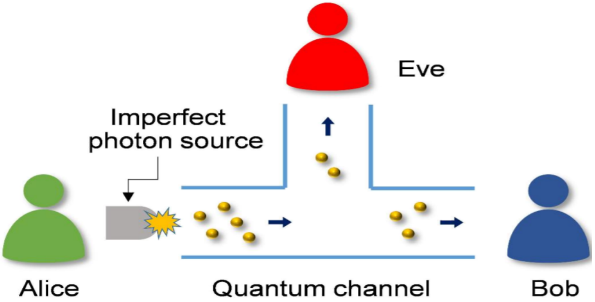
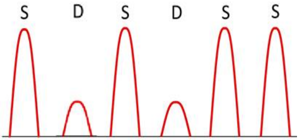


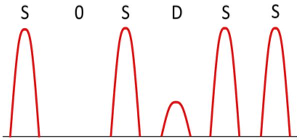
Figure 4: Diagram of Photon Number Splitting attack: PNS attack (adapted from http://www.e-jikei.org/Conf/ICMEMIS2017/proceedings/materials/proc_files/GS_papers/GS-03/ICMEMIS2017-GS-03.pdf)

Decoy state QKD

Alice sends:



Bob receives:



Attenuation with an AOM:

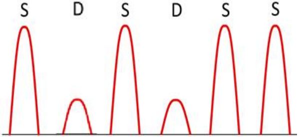
- Signal state
  - $|\alpha_S|^2 = 0.6$
- Decoy state
  - $|\alpha_D|^2 = 0.2$

- Eve requires at least 1 photon

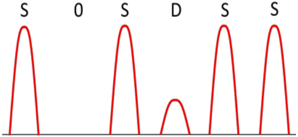
$\rightarrow$ *high decoy error rate*

Practical use of decoy state QKD

Alice sends:



Bob receives:



- Find Eve by comparing error rates (photon number statistics)

Shanghai-Beijing fiber network:
- pulse rate: 625 MHz
- key rate: 10-25 kbps
$\rightarrow$ *only* 1 :10^4 photon used

Micius satellite

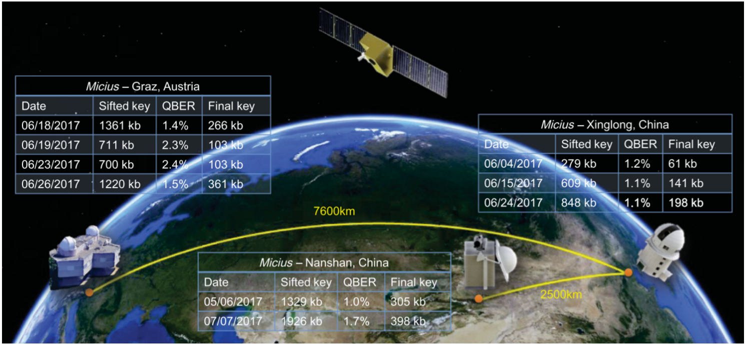


Figure 5: Illustration of the three cooperating ground stations (Graz, Nanshan, and Xinglong) (adapted from `https://arxiv.org/ftp/arxiv/papers/1801/1801.04418.pdf`)

- Launch: August 2016
- ca. $ 100 million
- quantum optics at a space scale

Entanglement distribution

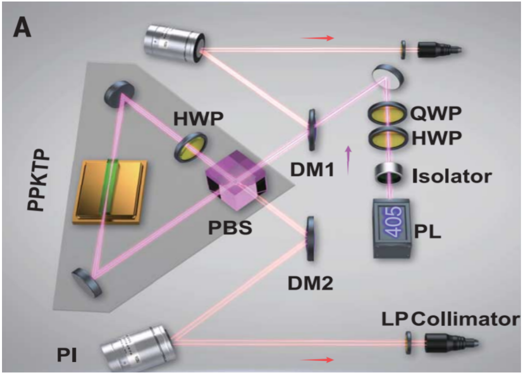


Figure 6: Schematic of the spaceborne entangled-photon source (adapted from [8])

single photon passes through crystal:
- $|\Psi\rangle \rightarrow (|V\rangle_A |H\rangle_B + e^{i\phi} |H\rangle_A |V\rangle_B)/\sqrt{2}$
- 1 photon: 405 nm $\rightarrow 2\ photons:\ 810\ nm$

Ground-to-space key rates

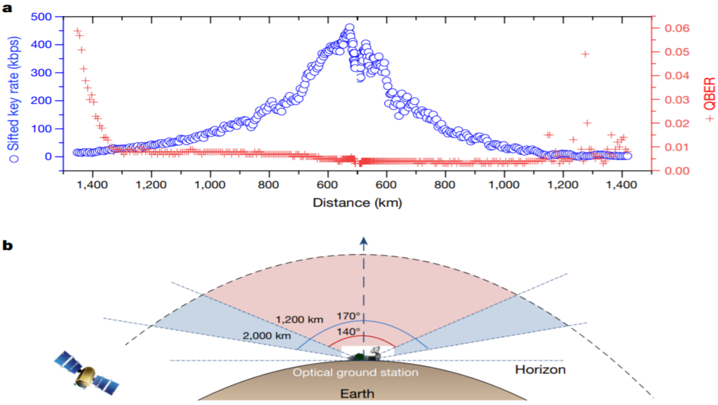


Figure 7: Performance of high-speed satellite-to-ground QKD (adapted from [1])

- pulse rate: 200 MHz
- few photons detected

- sifted key: two-photon coincidence at the ground station
- Quantum bit error rate (QBER): ratio of error rate to key rate

The Beijing-Shanghai network

Figure 8: Illustration of the backbone network (adapted from https://www.photonics.com/Articles/Quantum_Networks_Photons_Hold_Key_to_Data/a60541)

- Megaproject of the 13th five-year plan (2016-2020) of the CCP
- Micius: "*a satellite for the post-Snowden age*" - Popular Science, 2016
- 4 Quantum-metropolitan area networks

Quantum metropolitan-area networks

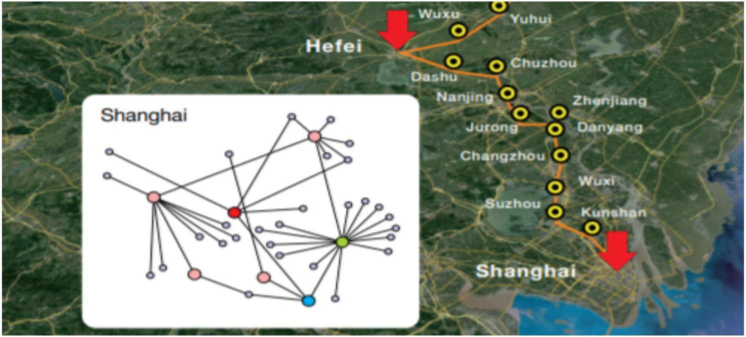


Figure 9: The quantum metropolitan-area network in Shanghai (adapted from [1])

- 700 fibre links, > 150 users, distances over 2000 km
- Average Key rates:

- Metropolitan network: 11.2 - 26.3 kbps
- backbone network: 79.3 kbps
- ground-to-space link: 1.1 - 47.8 kbps

The first setup

Laboratory Implementation achieved in 1992
by Bennet, Brassard et al.

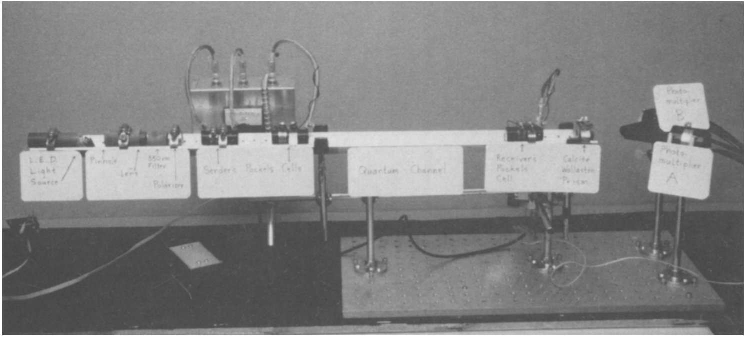


Figure 10: Photograph of the optical setup used in the first QKD experiment (adapted from `https://link.springer.com/content/pdf/10.1007/BF00191318.pdf`)

Challenges

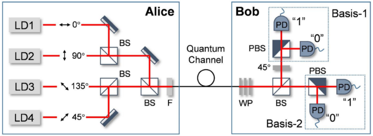
- Costs:
  - QKD transmitter and receiver modules (>US$ 100k)
  - Micius satellite
  - work hours

Figure 11: InGaAs/InP single-photon detection head (adapted from `http://www.micro-photon-devices.com/Products/Photon-Counters/InGaAs-InP`)

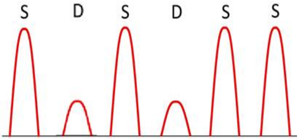
- calibrating/ synchronizing/ testing
- establishing protocols:
  - error correction
  - automated optimal routing
  - attack detection (Photon number splitting, Man-in-the-middle, Trojan-horse, denial of service,...)
  - attack countermeasures

Summary

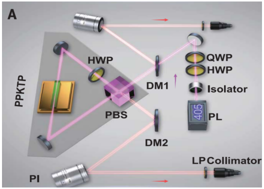
BB84 protocol:



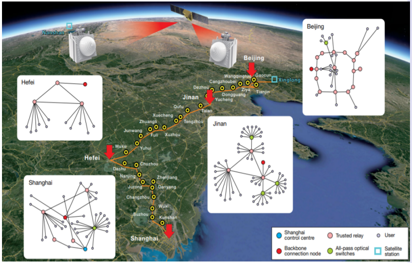
Decoy method:



Entanglement distribution:



Beijing-Shanghai network:



Outlook

- dense wavelength-division multiplexing
- geosynchronous satellite
- weather-independent ground-satellite link
- more efficient protocols
- connecting more national quantum networks

$\rightarrow$ *global quantum network*

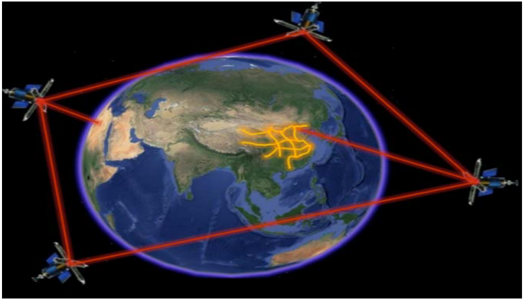


Figure 12: A future global quantum network (adapted from `https://iopscience.iop.org/article/10.1088/2058-9565/ab4bea`)

[1] Yu-Ao Chen et al. "An integrated space-to-ground quantum communication network over 4,600 kilometres". In: *Nature* (2021). DOI: 10.1038/s41586-020-03093-8.

[2] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical Computer Science* 560 (2014). DOI: https://doi.org/10.1016/j.tcs.2014.05.025.

[3] Sergio L. Castro. "Towards a global space-based QKD network". In: *(Master thesis)* (Jan. 2019). URL: https://repository.tudelft.nl/islandora/object/uuid%5C%3Ad8a391e8-d21a-4f37-95ec-467a49d391ea.

[4] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". In: *Phys. Rev. Lett.* 67 (Aug. 1991). DOI: 10.1103/PhysRevLett.67.661.

[5] Kevin Günthner et al. "Quantum-limited measurements of optical signals from a geostationary satellite". In: *Optica* 4 (June 2017). DOI: 10.1364/OPTICA.4.000611.

[6] Won-Young Hwang. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". In: *Phys. Rev. Lett.* 91 (5 Aug. 2003). DOI: 10.1103/PhysRevLett.91.057901.

[7] Xiongfeng Ma et al. “Practical decoy state for quantum key distribution”. In: *Phys. Rev. A* 72 (July 2005). DOI: 10.1103/PhysRevA.72.012326.

[8] Juan Yin et al. “Satellite-based entanglement distribution over 1200 kilometers”. In: *Science* 356 (2017). DOI: 10.1126/science.aan3211.