TOWARD A GLOBAL QUANTUM NETWORK

Jian-Wei Pan – DOI: https://doi.org/10.1051/epn/2023104
University of Science and Technology of China

About 90 years ago, Albert Einstein complained about the "spooky action at a distance" of quantum entanglement and questioned the completeness of quantum mechanics [1]. This year, the Nobel Prize is awarded to three pioneers that put Einstein's curiosity under experimental tests based on Bell's inequality [2]. The fundamentals of quantum mechanics are not of just theoretical or philosophical interest. Rather, worldwide efforts are harnessing these quantum weirdness to develop emerging technologies.

The goal is to build a large-scale and fully functional quantum networks both for the exploration of new frontier of physics and the implementations of quantum computation, communication, and metrology.

The near-term application of such a quantum network is to establish secure quantum-encrypted communications, because privacy and security rooted in human being since the ancient time. Traditional public-key cryptography usually relies on the perceived computational intractability of certain mathematical functions. However, history has shown that nearly all advances in classical cryptography were subsequently defeated by advances in cracking. It has long been suspected that, "Human ingenuity cannot concoct a cipher which human ingenuity cannot resolve".

It might come as a surprise that the very fundamental principle of quantum mechanics was exploited to solve this long-standing problem on information security which the mathematicians have struggled with for centuries. In the 1980s, Bennett and Brassard presented a feasible protocol of quantum key distribution (QKD), known as BB84 [3]. Independently, in 1991, Ekert discovered that quantum entanglement can be used for unconditionally secure information transfer [4]. Their invented quantum cryptography is a fundamentally new way—and the only known approach—that allows distant parties to communicate safely under the nose of an eavesdropper endowed with unlimited computational power.

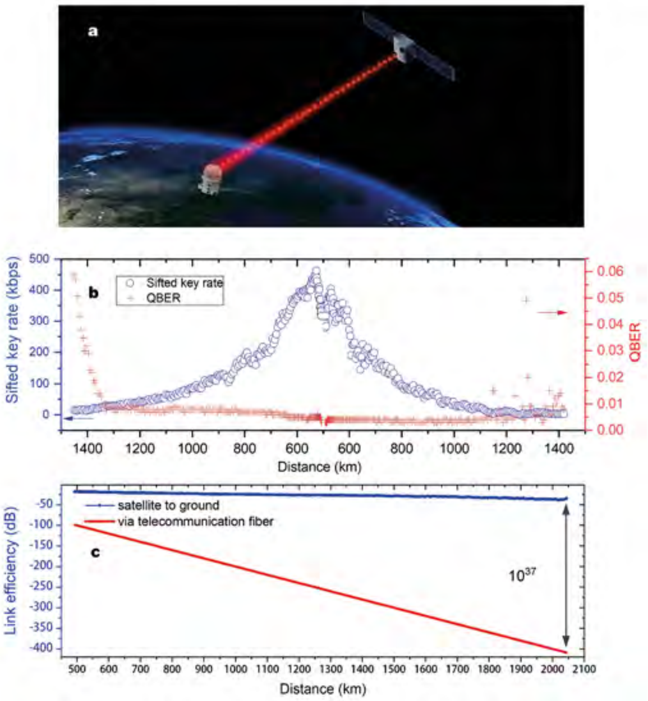
The first table-top proof-of-concept QKD experiment was done in 1989 by Bennett and his co-workers using an attenuated LED with a distance of 32 cm, followed by many similar small-scale demonstrations in optical fibres or terrestrial free space up to a distance of a few tens of kilometres. However, these communication distances, which were within half an hour drive, were far from a practical scale. More importantly, there existed serious loopholes in the early work, which can be used for eavesdropping. For example, Brassard recalled that in their work they "could literally hear the photons as they flew, and zeroes and ones made different noises".

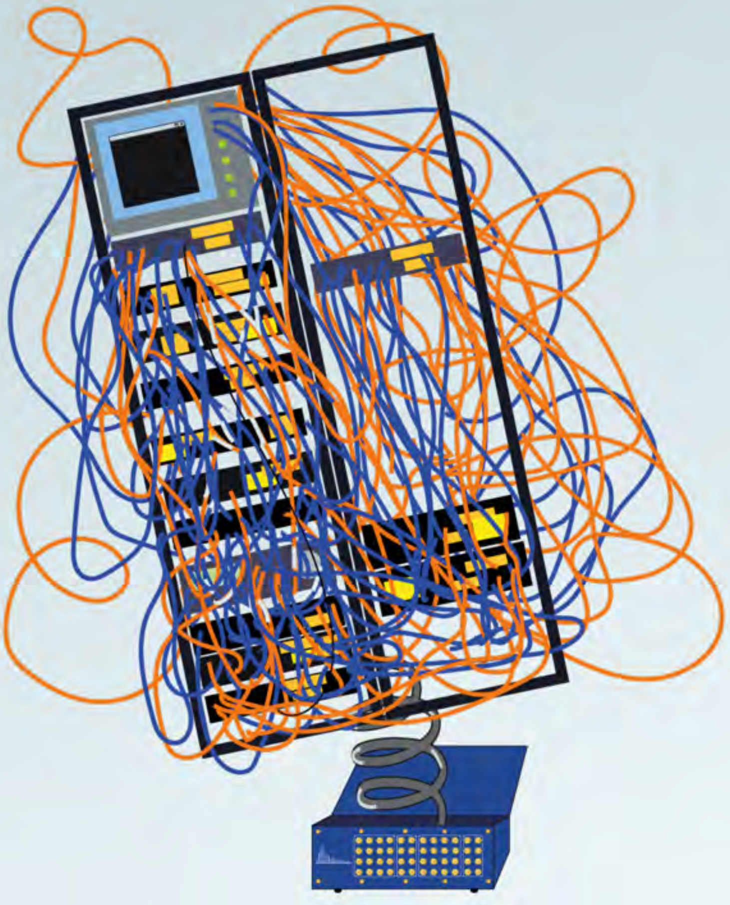
Quantum cryptography is ideally secure only when perfect single-photon sources and detectors are employed. Unfortunately, ideal devices never exist. To solve the problems related to source and detector, respectively, decoy-state and measurement-device-independent QKD was proposed and experimentally realized. These works made QKD a viable technology under realistic conditions and kick-started worldwide engineering efforts of practical QKD networks.

The most important challenge of quantum networks is to go long distance to be useful at a global scale. In both fiber optics and terrestrial free space, there is inevitable photon loss exponentially at an increasing channel length. At 1000 km, even with a perfect GHz rate single-photon source, ideal photon detectors and the best commercial optical fibres, one can detect only 0.3 photons per century. Moreover, the quantum no-cloning theorem, which underpins the security of QKD, also excludes the possibility of simply amplifying quantum signals as in classical repeaters.

Due to these problems, quantum repeaters will play a key role in future quantum network to extend to a scalable range, by combining the functionalities of entanglement swapping, entanglement purification, and quantum memory. While these key parameters keep improving in ongoing experiments, significant engineering efforts remain to be done for • • •

▼ FIG. 1: (a) Establishing a reliable space-to-ground link for the quantum state transfer; (b)&(c) Performance of satellite-to-ground QKD during one orbit. QBER: quantum bit error rate.





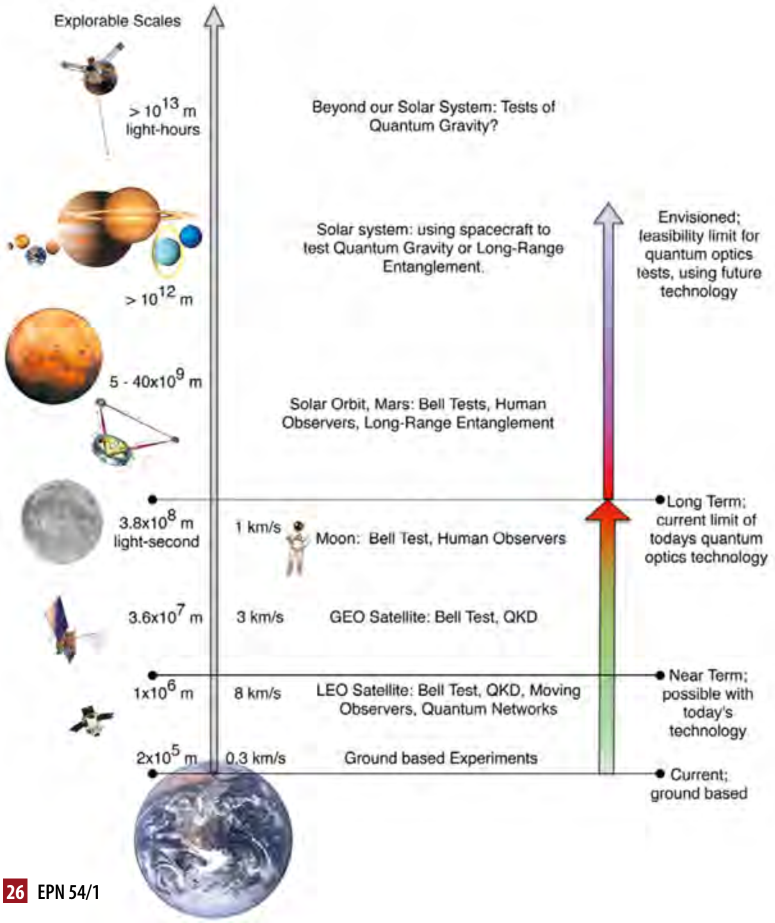
the quantum repeaters to go to 1000 km scale.

On the other hand, satellite-based free-space quantum link offers a unique and more efficient approach for global quantum networks, by taking advantage of the negligible photon loss in the atmosphere. The first quantum satellite, Micius, was successfully launched in August 16, 2016, in Jiuquan, China, orbiting at an altitude of ~500 km.

The satellite sends two entangled photon beams from two telescopes in the satellite to separate ground stations, with two independent satellite-to-ground quantum links established simultaneously. As the entangled photons propagate from the flying satellite (with a speed of 8 km/s) through the atmosphere to the two ground stations thousands of km apart, extremely demanding techniques are needed to be developed to overcome the detrimental effects of beam diffraction, pointing error, atmospheric turbulence and absorption. To put it in a non-technical way, the necessary technical ability is equivalent to: clearly seeing and tracking a moving single human hair at a distance of 300 meters away (in terms of pointing and tracking ability), and detecting a single photon in the Earth from a single match's fire lighted at the Moon (in terms of single-photon detection sensitivity and isolation from background noise).

Three key milestones have been in a few months after the launch: satellite-to-ground decoy-state quantum key distribution over a distance of 1200 km generating a final key rate of 1.1 kbits/s [5], which was recently improved to 47.8 kbits/s; satellite-based entanglement distribution to two locations on the Earth separated by 1200 km and test of Bell inequality [6], and ground-to-satellite quantum teleportation over 1400 km [7]. Remarkably, the effective link efficiency of the satellite-based channel is ~37 orders of magnitudes larger than direct transmission through optical fibres at the same length of ~2000 km.

▾ FIG. 2: Overview of the distance scales and the corresponding conceived quantum experiments reviewed in ref. [8].



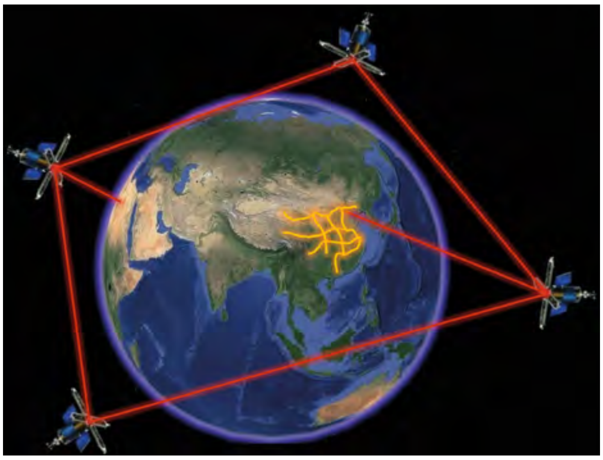
The two-link efficiency was further improved in 2020, and the satellite was utilized to perform quantum cryptography between two ground stations over 1120 km based on Ekert's entanglement-based protocol, where the unconditional security is ensured even if the satellite is controlled by an adversary. The satellite has now been combined with metropolitan fibre networks to form a space-ground integrated quantum network. Using the satellite as a trustful relay, two team achieved intercontinental quantum communications between Beijing and Vienna with a record distance of 7600 km.

Meanwhile, the methods developed in the quantum science satellite opens new paths to high-precision measurement and foundational tests. For instance, using satellite-based entanglement distribution, it is possible to entangled remote N atomic clocks and improve the time measurement accuracy by √N times, as proposed by Lukin and Ye *et al.* Combining the quantum teleportation with the distributed telescopes will create an effective aperture with the size of Earth and an enormous resolution that would allow in principle reading licence plates on Jupiter's moons as pointed by Kwiat.

In general, the space-based platform is also a first step toward fundamental quantum optics experiments at distances that are inaccessible previously on the ground. A wide variety of potential tests have been conceived using increasingly distant satellites, as sketched in Fig. 2. Examples include probing the gravity-induced decoherence and the interface between gravity (the theory of very large) and quantum (the theory of very small). These tests have the potential to determine the applicability of quantum theory at larger length scales, eliminate various alternative physical theories, and place bounds on phenomenological models motivated by ideas about spacetime microstructure from quantum gravity.

Micius only marks the beginning. For the Chinese quantum satellite plans, there are two goals in the next 5 to 10 years. The first one is to develop 3 to 5 small LEO satellites dedicated to QKD missions, which will provide more practical and efficient QKD services. The second goal is to develop a medium-Earth-orbit to geosynchronous-orbit satellite, which can provide longer service time and wider coverage. The combination of a high-orbit satellite and multiple LEO satellites can form a quantum constellation for global services, as shown in Fig. 3. Furthermore, with such a new generation space platform, we plan to realize the high-precision satellite-ground time-frequency transfer and GEO satellite-based optical clocks to verify the technology of wide-area optical frequency standard.

Another important element in quantum networks is quantum computers, with various qubit candidates including



▲ **FIG. 3:** Road maps for the global quantum communication network. Intracity 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.

superconducting circuits, trapped ions, atom arrays in optical tweezers, and single photons. To link the distant qubits, quantum interface is required to coherently mapping a single photon qubit in and out of the stationary qubits. Optical quantum computers have the unique advantage to be naturally integrated in the photonic networks. As a non-universal model of quantum computing, boson sampling has been demonstrated with up to 113 photon clicks out of a 144-mode interferometer, which yields a Hilbert state space dimension of 1043 and a sampling rate ten order of magnitudes faster than using the state-of-the-art simulation strategies on supercomputers [9]. Just as Bell experiments refute Einstein's local hidden variable models, the quantum computational experiments have provided strong evidence against the Extended Church-Turing Thesis. These work marks the dawn of the quantum era in computation. ■

About the Author

Jian-Wei Pan received his Bachelor (1992) and Master (1995) in Physics from the University of Science and Technology of China, Hefei, and his PhD (1999) from the University of Vienna. He is currently a Professor of Physics of the University of Science and Technology of China.

References

[1] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935)

[2] J. S. Bell, *Physics* **1**, 195 (1964)

[3] C. H. Bennett, and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE Press, New York) pp. 175-179 (1984)

[4] Artur K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991)

[5] S.-K. Liao, *et al.*, *Nature* **549**, 43 (2017)

[6] J. Yin, *et al.*, *Science* 356, 1140-1144 (2017)

[7] J.-G. Ren, *et al.*, *Nature* **549**, 70 (2017)

[8] D. Rideout, *et al.*, *Classical Quantum Gravity* **29**, 224011 (2012)

[9] H.-S. Zhong, *et al.*, *Science* **370**, 1460 (2020)