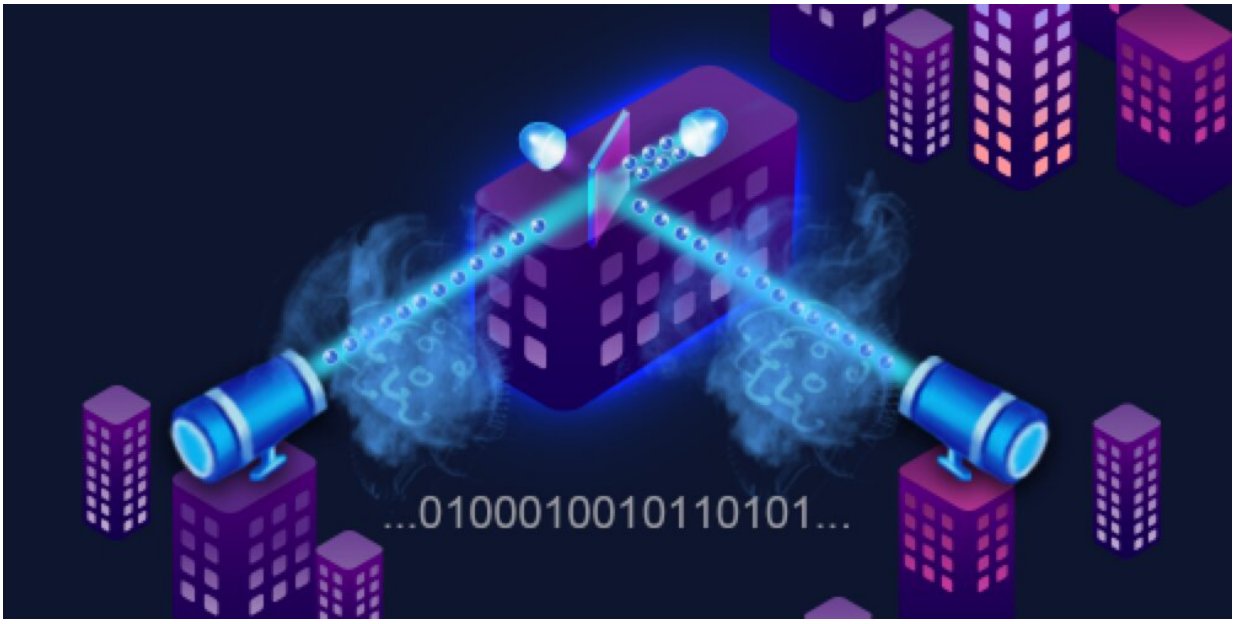
Long-distance and secure quantum key distribution (QKD) over a free-space channel

January 25 2021, by Ingrid Fadelli



A concept figure of the MDI-QKD experiment in a city. Telescopes are located in high-rise buildings for transmitting encoded photons. The turbulence of the atmosphere, which exists everywhere in the transmission channel, is the main challenge for the photons to maintain the spatial mode in the detection terminal. Credit: Yao Zheng/Micius Salon.

Quantum key distribution (QKD) is a technique that enables secure communications between devices using a cryptographic protocol that is partly based on quantum mechanics. This communication method ultimately allows two parties to encrypt and decrypt messages they send

to each other using a unique key that is unknown to other parties.

Measurement-device-independent quantum key distribution (MDI-QKD) is a unique protocol that facilitates the creation of more secure QKD networks with untrusted devices. This protocol can enable QKD-based communication over longer distances, as well as higher key production rates and more reliable network verification.

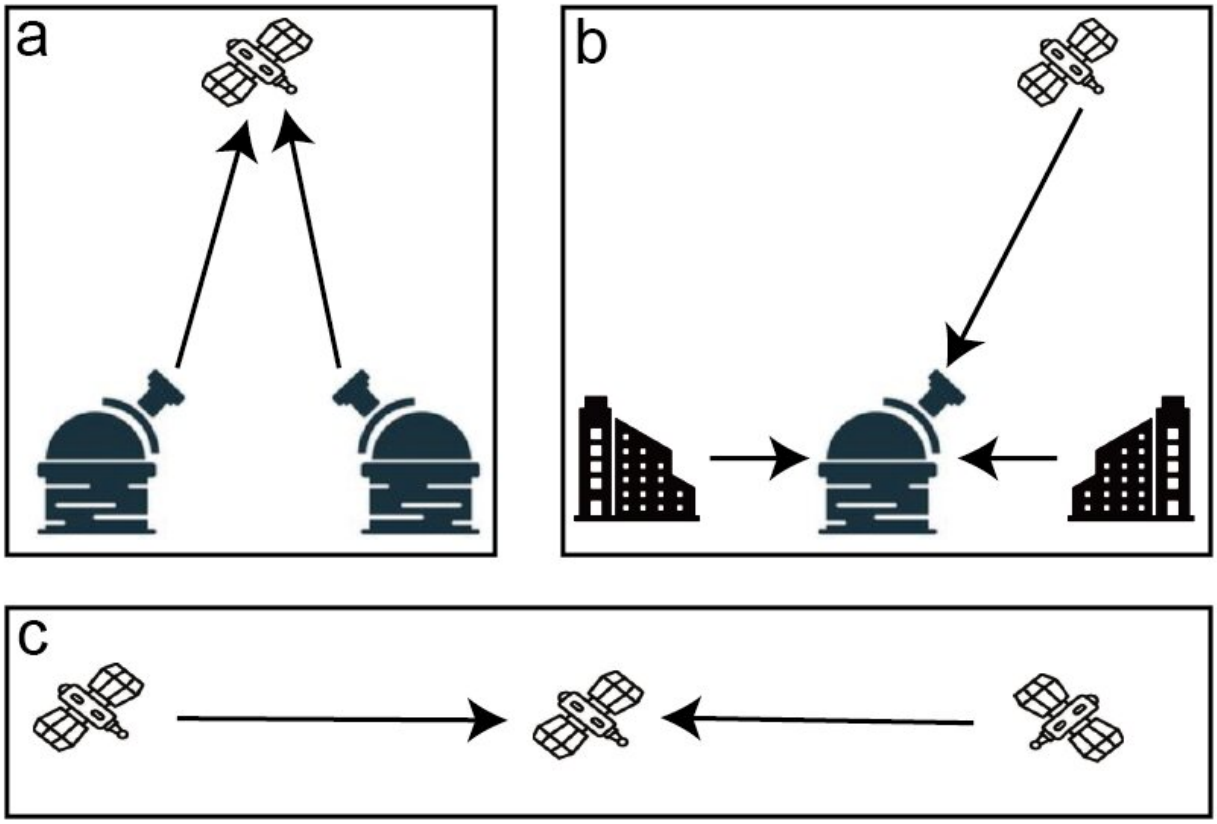
So far, MDI-QKD has only been successfully implemented using fiber optics. Implementing the protocol across free-space channels, on the other hand, has proved significantly challenging.

A research group led by Jian-Wei Pan, from the University of Science and Technology in China, has recently demonstrated long-distance and secure MDI-QKD over a free-space channel for the very first time. Their paper, published in *Physical Review Letters*, could pave the way to satellite-based MDI-QKD implementations.

"The final goal of QKD is to realize a global-scale quantum secure communication network," Qiang Zhang, one of the researchers who carried out the study, told Phys.org. "In order to achieve this ambitious goal, two main challenges need to be addressed. One is to reduce the gap between theory and practice of QKD, and the other one is to extend the distance of QKD. The goal of our recent work was to solve these two difficulties."

Theoretically, QKD offers greater security in communications leveraging physics laws. However, imperfections and vulnerabilities of real devices could result in deviations from the models used to carry out security analyses. The MDI-QKD protocol can help to tackle this challenge by closing all loopholes on detection at once. Moreover, it can improve the performance and security of QKD implementations on real devices, by including decoy states.

Satellite-based QKD implementations could extend the distance across which this secure communication can take place, as they would enable lower transmission losses and negligible decoherence in space. By extending MDI-QKD from fiber to free-space channels, the work by Pan and his colleagues could be a first step toward implementing MDI-QKD protocols on a large scale using satellites.



Possible configurations of satellite-based MDI-QKD. (a) the satellite plays the role of the detection terminal, while two ground stations send photons via the up-link to the satellite. (b) A ground station plays the role of the detection terminal. Users in the ground fiber-based network share secret keys with the satellite via the ground station. (c) MDI-QKD between three satellites. Credit: Cao et al.

"Although several fiber-based MDI-QKD experiments have been performed before our study, none of them have demonstrated the feasibility of the protocol with a free-space channel," Zhang said. "The main reason is that the amplitude and phase fluctuation induced by atmospheric turbulence makes it difficult to maintain the indistinguishability in terms of spatial, timing and spectral modes between independent photons."

As atmospheric turbulence typically destroys the spatial mode between independent photons, MDI-QKD implementations typically require the use of single-mode fiber to perform spatial filtering before applying interferometry techniques. Using single-mode fiber to couple photons, however, generally leads to a low coupling efficiency and intensity fluctuation. To solve this problem, the researchers developed a new adaptive optics system that improves the channel's overall efficiency.

"As the rapid fluctuation of light intensity makes sharing the time-frequency reference difficult, we developed new technologies to achieve high-precision time synchronization and frequency locking between independent photon sources located far apart in order to maintain the indistinguishability of the timing and spectral modes," Zhang explained. "Thanks to these technical breakthroughs, we completed a task that seemed impossible to complete before."

The study is an important milestone in the path toward implementing QKD on a large scale and using it to secure communications over longer distances. Moreover, the researchers were the first to realize photon interference in long-distance atmospheric channels. This could open up exciting possibilities for the development of complex types of quantum information processing involving quantum interference, such as quantum entanglement swapping and quantum teleportation. It could also offer new ways of testing the interface of quantum mechanics and gravity.

The researchers' long-term goal is to demonstrate satellite-based MDI-QKD and eventually to build a global quantum network. To achieve this, however, they will first need to overcome a number of additional challenges.

"One of these challenges is the high loss mainly induced by the atmospheric fluctuation," Zhang explained. "In the most straightforward configuration of satellite-based MDI-QKD, a satellite plays the role of the detection terminal (i.e., two ground stations send photons via the 'up-link' to the satellite). The channel loss measured by the Micius satellite is about 41 ~ 52 dB from a ground station with altitude of 5,100 miles. The loss is likely to be much higher from ground stations at a lower altitude. The single mode fiber coupling efficiency is another source of loss, which is also very significant with existing MDI-QKD systems."

In order to enable effective satellite-based MDI-QKD implementations, therefore, the researchers will first need to advance existing methods to transit photons across free-space channels. To do this, they have so far developed an adaptive optics system and an algorithm that increases the efficiency of free-space channels. In their next studies, they plan to create other algorithms and techniques for improving the overall transmission channel.

"The second challenge we hope to overcome is associated with the motion of satellites," Zhang added. "Since the signal pulses are expected to be overlapped in the time domain at the detection terminal, a very accurate prediction of a satellite's orbit is required, and the emission time of each encoded pulse should also be accurately timed, so that they can finally overlap well in the detection terminal. The Doppler frequency shift, on the other hand, is an important source of frequency mismatch that is annoying for HOM interference. The frequency of each encoded pulse should also be accurately shifted for compensation. After solving all of these technical challenges, we believe that we will be able to

realize satellite-based MDI-QKD."

More information: Long-distance free-space measurement-device-independent quantum key distribution. *Physical Review Letters*(2021). DOI: 10.1103/PhysRevLett.125.260503.