International Conference on Space Optics—ICSO 2018

Chania, Greece

9–12 October 2018

Edited by Zoran Sodnik, Nikos Karafolas, and Bruno Cugny

Space-to-ground quantum key distribution

T. Scheidl

J. Handsteiner

D. Rauch

R. Ursin

International Conference on Space Optics — ICSO 2018, edited by Zoran Sodnik, Nikos Karafolas, Bruno Cugny, Proc. of SPIE Vol. 11180, 111801W · © 2018 ESA and CNES · CCC code: 0277-786X/18/$18 · doi: 10.1117/12.2535987

Space-to-Ground Quantum Key Distribution

T.Scheidl*[a,b], J. Handsteiner[a,b], D. Rauch[a,b], R. Ursin[a,b]
[a]Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria;
[b]Vienna Center for Quantum Science & Technology (VCQ), Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria

ABSTRACT

Quantum key distribution (QKD) can in principle offer unconditional security by making use of the fundamental laws of quantum mechanics. In practice, this is typically achieved by preparing individual photons in quantum superposition states and sending them to a remote receiver. To date, most commercially available QKD systems rely on the transmission of the photons via optical fibers, which, due to channel loss and detector noise, limits the distance over which QKD is feasible to a few hundred kilometers. Alternatively, satellite-based QKD facilitates low photon loss and negligible signal disturbance and offers a viable solution for establishing a global scale quantum network. Recently, a quantum science mission of the Chinese Academy of Sciences (CAS) in collaboration with the Austrian Academy of Sciences (AAS) and the University of Vienna aimed at a satellite-based intercontinental quantum-key relay. Using the Chinese Quantum Science Satellite "Micius" as a trusted relay, a quantum network consisting of three optical ground stations located in China (Xinglong, Nanshan) and Austria (Graz-Lustbühel) has been demonstrated successfully. Here we report on the development of a quantum receiving module, installed at the Satellite Laser Ranging Station in Graz (Austria) capable of implementing the so-called decoy-state QKD protocol in a downlink scenario from the LEO satellite "Micius". Furthermore, we will present the experimental results obtained during several downlinks from the Chinese satellite focusing on the performance of the Austrian receiving station.

Keywords: Quantum Key Distribution, Quantum Communication, Decoy-State Protocol, Quantum Internet, Satellite-based Quantum Communication

*thomas.scheidl@univie.ac.at; phone +43-1-4277-29558; www.iqoqi-vienna.at

1. INTRODUCTION

Quantum Key Distribution (QKD) allows two authorized parties, traditionally called Alice and Bob, to establish a secret key at a distance. They need to be connected by two channels: a quantum channel, allowing them to share quantum signals; and a classical channel, on which they can send classical messages forth and back. The classical channel needs to be authenticated: this means that Alice and Bob identify themselves. A third person can listen to the conversation but cannot participate in it. The quantum channel, however, is open to any possible manipulation from a third person. Specifically, the task of Alice and Bob is to guarantee security against an adversarial eavesdropper, usually called Eve, tapping on the quantum channel and listening to the exchanges on the classical channel.

QKD consists of two phases. In the first phase Alice and Bob exchange quantum signals over the quantum channel and perform measurements, obtaining a *raw key* – two strongly correlated but non-identical and only partly secret strings. In the second phase, Alice and Bob use the classical channel to perform an interactive post-processing protocol, which allows them to distil two identical and completely secret strings, which are two identical copies of the generated secure key.

1.1 Decoy-State QKD Protocol

The decoy-state QKD protocol[1] requires four different qubit states that form two complementary bases. These states are usually realized with four linear polarization states of photons, e.g. horizontal (*H*), vertical (*V*), diagonal (*D*) and anti-diagonal (*A*). Ideal QKD systems would utilize true single photon states as qubits, because this reduces the power of a possible eavesdropper. In practice however, true single photon sources are barely available and rather impractical for QKD, thus faint laser pulses are often used as quantum signals. The number of photons contained in faint laser pulses follows a Poissonian distribution with mean photon number μ. The mean photon number can be set via the intensity of the laser.

Consequently, to avoid several powerful eavesdropping attacks (e.g. photon-number-splitting attack[2]) enabled by the fact that faint laser pulses exhibit a non-zero probability of having more than one photons per pulse, the decoy-state protocol implemented in typical QKD systems uses three different intensity levels for the signal pulses ($\mu_s \approx 1$), decoy pulses ($\mu_d < \mu_s$) and vacuum pulses ($\mu_{vac}=0$), respectively. Since an eavesdropper cannot distinguish between signal and decoy pulses, any photon-number dependent eavesdropping strategy has different effects on the signal states and on the decoy states and can thus be detected with high probability (depending on a selectable security parameter).

As depicted in Figure 1, for each laser pulse, Alice randomly selects and records the polarization state as well as the intensity level and sends it to Bob via the quantum channel. Bob receives and analyzes them with a two channel analyzer, again randomly in one of the two complementary measurement bases, *H/V* or *D/A*. He records his measurement results together with the chosen basis. After enough photons have been transmitted, Bob communicates publicly with Alice over the authenticated classical channel and tells her which photons actually arrived and the corresponding analyzing bases. In return, Alice tells Bob when she has used the same basis to prepare them, because only in these cases Bob obtains the correct result. Assigning the binary values "0" to the states *H* and *D* and the value "1" to the states *V* and *A*, leaves Alice and Bob with the so-called *sifted key*.

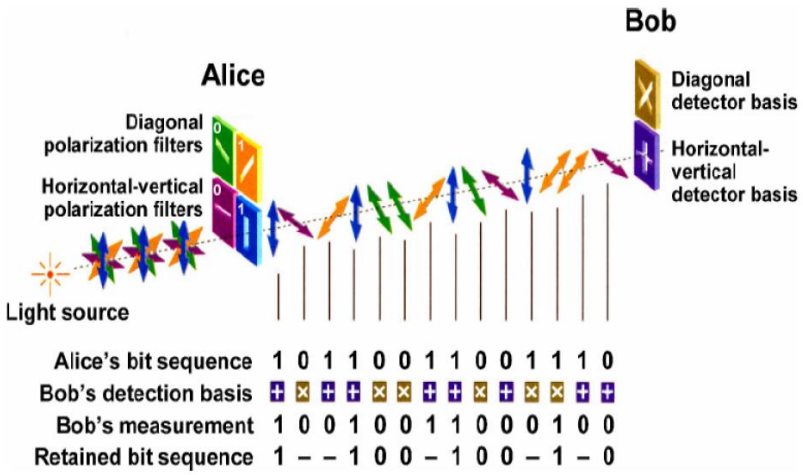

Figure 1 – Scheme of the decoy-state protocol (Figure taken from Ref. [3]). Alice prepares and sends faint laser pulses randomly in one of the four polarization states. Bob measures the photons randomly either in the *H/V* or *D/A* measurement basis. Only photons measured in the correct basis contribute to the key.

Practical systems will always suffer from inherent noise due to detector dark counts, background counts and errors in state preparation, transmission and measurement. The resulting errors in the sifted key are usually quantified as the quantum bit error ratio (QBER). As it cannot be distinguished whether errors come from noise or eavesdropping activities, the most conservative strategy is to attribute them all to a potential eavesdropping attack. Thus, for extracting the final *secure key* from the defective sifted key, classical procedures like *error correction* and *privacy amplification* have to be applied. Finally, the secure key rate R_f is given by

$$R_f = q \cdot R \cdot [-Q_s \cdot f(E) \cdot H_2(E) + Q_1 \cdot (1 - H_2(E)]. \quad (1)$$

Here, q is the basis reconciliation factor, R is the rate of signal pulses, Q_s is the gain of signal states, E is the quantum bit error ratio, f is the error correction efficiency, Q_1 is the (estimated) gain of the signal pulses that contain only one photon and H_2 is the binary Shannon entropy with

$$H_2(x) = -x \cdot log_2(x) - (1 - x) \cdot log_2(1 - x). \quad (2)$$

1.2 Key Relay Protocol

In our experiment, the decoy-state QKD protocol facilitates independent secure key exchanges between the Chinese satellite and several ground stations. Subsequently, these individual keys can be used to obtain a secure key betweeen any two ground stations by following the so-called *key relay protocol* (see Figure 2).

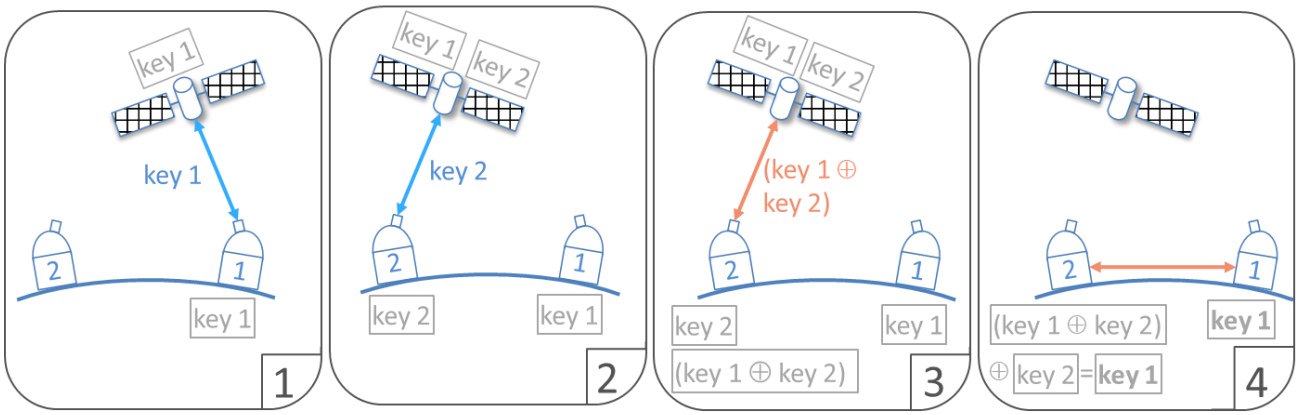

Figure 2 – Key Relay Protocol: a satellite sequentially generates secure quantum keys with two ground-stations (*key 1* and *key 2*) utilizing the decoy-state QKD protocol. Finally, secure communication between the ground stations is possible by logically combining the individual keys (see main text for details).

First, ground station 1 (e.g. in Austria) exchanges a key (*key 1*) via a direct optical link with the Chinese satellite. Sequentially, at some later time, the same satellite exchanges another key (*key 2*) with ground station 2 (e.g. in China). Afterwards, the satellite logically combines both keys (XOR combination) and sends the result to one of the ground stations (e.g. ground station 2) via a classical channel. Finally, using the individual *key 2*, ground-station 2 can now determine the key of the other station such that both ground stations now share *key 1*. Note that in this scenario, the satellite is considered to be a *trusted* relay station.

2. EXPERIMENTAL DETAILS

2.1 The Chinese Satellite "Micius"

As explained in detail in Ref. [4], the satellite was launched into a sun-synchronous low-Earth orbit with an altitude of approximately 500km and is equipped with a decoy-state QKD transmitter operating at a wavelength of 849nm and a pulse repetition rate of 100MHz. Eight laser diodes are combined into a single spatial mode using polarizing and non-polarizing beam splitters, facilitating the generation of the four polarization states at two intensity levels, corresponding to mean photon numbers of μ_s=0.8 and μ_d=0.1 for signal and decoy states, respectively. The probability of sending signal, decoy or vacuum pulses is set to 50%, 25% and 25%, respectively. A 300-mm-aperture Cassegrain telescope is used to transmit the faint laser pulses towards ground. Co-aligned with the quantum signal, a pulsed beacon laser (532nm, 10kHz) is sent towards ground for tracking and time synchronization purposes.

2.2 The Satellite Laser Ranging Station Graz-Lustbühel (Austria)

The ground station in Graz is located on the Lustbühel hill approximately 4 km east of the city center. The ground station consists of an alt-azimuth mechanical mount with an f/11 Cassegrain telescope with an aperture diameter of 0.5 m and a mechanical pointing accuracy of better than 10 µrad. A coarse pointing system (f/7.5 lens plus CCD camera) with field-of-view of 10 mrad is attached to and co-aligned with the optical axis of the main telescope. Additionally, an uplink beacon laser (671 nm, 3 W) with full divergence angle of 3 mrad is required for tracking purposes. The quantum receiver module is installed at the Cassegrain focus of the telescope (see Figure 3). An achromatic lens with f=11 cm collimates the quantum signal and downlink beacon laser beams after the primary focus with a magnification of 50 to beams with 1cm diameter. This is followed by a dichroic mirror separating the quantum signal from the 532nm beacon laser coming from the satellite.

In the beam path of the beacon laser, a 90/10 beam splitter is used to reflect 10% of the signal to a PIN photodiode for time synchronization, while 90% are transmitted and focused onto a fine-pointing camera with a field-of-view of 1.5 mrad. To compensate for inaccurate orbit predictions, coarse- and fine-pointing corrections have been implemented manually based on the spot positions at the coarse- and fine-pointing cameras.

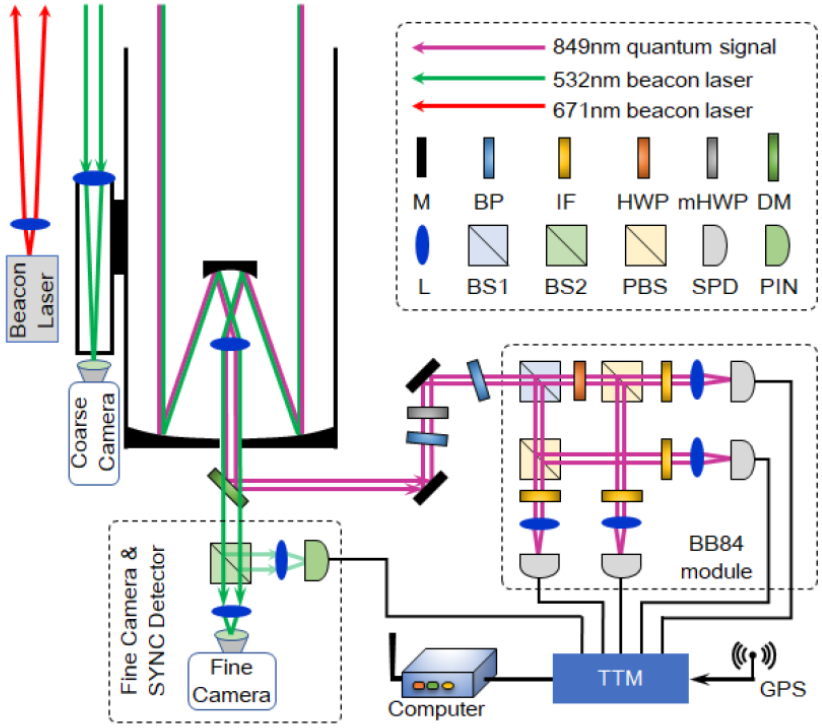

Figure 3 – A schematic of the experimental setup installed at the Satellite Laser Ranging Station Graz-Lustbühel (Austria). For details please refer to the main text. (Figure taken from Supplemental Material of Ref. [5].)

The quantum signal is guided to the quantum receiver box, consisting of a motorized half wave plate (mHWP) placed in between two birefringent plates (BP), a 50/50 beam splitter (BS), two polarizing beam splitters (PBS), another HWP set to 22.5° and four single photon detector (SPD). The detectors facilitate an active area of 500 µm, a timing resolution of < 350ps and a field-of-view of 250µrad. Interference filters at 849 nm with an FWHM bandwidth of 3 nm are placed in front of each single photon detector. The optical axes of the birefringent plates is oriented parallel to horizontal polarization, as defined by the polarizing beam splitter. A one-time adjustment of the tilt of the first birefringent plate enables compensating phase-shifts between s- and p-polarization components introduced by optical elements before that plate, thus ensuring that the linear polarization states of the quantum signal reach the motorized half wave plate without being altered. Doing so, the motorized half wave plate can be used to compensate unwanted relative rotations between the linear-polarization reference frames of the satellite and the ground station that occur during a satellite passage. The time-dependent rotation angle of the motorized half wave plate can be calculated from the orbit prediction data and the exact coordinates of the ground station in advance. Phase-shifts that occur at optical elements between the motorized half wave plate and the polarizing beam splitters are compensated by a one-time adjustment of the tilt of the second birefringent plate. Then, the quantum signal is guided to the 50/50 beam splitter, where reflected photons are analyzed in the *H/V* polarization basis by means of a polarizing beam splitter, while transmitted photons are analyzed in the *D/A* basis by placing a half wave plate with its optical axis set to 22.5° in front of a polarizing beam splitter. Finally, the photons are detected using four single photon detectors placed in the output ports of the two polarizing beam splitters and the detection signals are fed into a time tagging module (TTM).

3. RESULTS

The experimental schedule foresees several performance tests before finally executing the decoy-state QKD protocol. The results of these tests as well as the performance of the quantum ground receiver during the execution of the final experiment are presented in this chapter.

3.1 Satellite Tracking Tests

The first tracking tests were scheduled for the satellite pass on 19th of April 2017 at 23:17h (UTC). The satellite was only sending the green downlink beacon laser towards the ground station and similarly, the uplink beacon laser was fired towards the satellite. As explained above, the downlink beacon laser is observed with a coarse-pointing as well as with a fine-pointing camera.

Figure *4* shows the difference of the observed spot from the reference position at the fine-pointing camera. The black and blue curve correspond to pointing deviations along azimuth and elevation, respectively. For comparison, the red dashed lines indicate the field of view (FoV) of the single photon detectors in the quantum receiver module, which was approximately 250µrad (full angle). One can clearly see that the satellite could be tracked with sufficient precision to stabilize the signal at the active area of the single photon detectors. During the satellite pass, fine-pointing corrections have been constantly applied to correct for small inaccuracies of the orbit predictions. The fine-pointing corrections have been intentionally interrupted twice to check how quickly the spot moves out of the desired field of view.

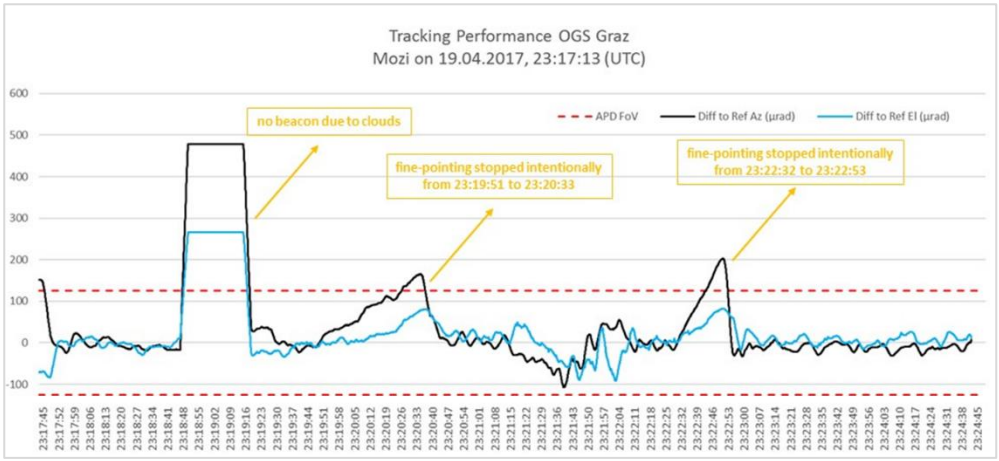

Figure 4 – Results of the satellite tracking tests executed on 19th of April 2017. Please refer to the main text for a detailed discussion.

3.2 Polarization Tests

For investigating the quality of the polarization analyzer system in the quantum receiving module, the satellite was sending a horizontally (*H*) polarized continuous-wave reference laser in parallel to the beacon laser to the ground station. The wavelength of the reference laser matches the wavelength of the quantum signal in the decoy-state QKD transmitter but facilitates higher intensity, making the test procedure more failure safe. After introducing additional neutral density filters at the entrance of the quantum receiver module, we detected on the order of 10^4-10^5 photons per second.

Figure 5 shows the results of this measurement, which was executed during the satellite pass starting on 25th of May 2017 at 22:45h (UTC). Since the reference laser is *H*-polarized, we expected a high contrast in the *H/V* measurement basis (i.e. counts detected at the *H*-detector divided by the counts detected at the *V*-detector). Figure 5 shows the time-dependent contrast during the satellite pass. Once the satellite was captured with the help of the tracking system the signal could be observed at the single photon detectors. At low elevation angles at the beginning of the satellite pass a contrast of approximately 40 was measured and increased to about 140 at the point of highest elevation (approximately 33° for this specific pass). The increase in contrast results from a decreasing link attenuation at higher elevations leading to a higher signal-to-noise ratio at the single photon detectors. A polarization contrast of 140 corresponds to a quantum bit error ratio of only 0.7% when executing a QKD protocol. Consequently, we have demonstrated a high-quality performance of the polarization analyzer including the polarization compensation system utilizing the motorized half wave plate and hence the polarization tests could be considered successful. Note that due to the pulsed nature of the decoy-state QKD transmitter

a further increase in polarization contrast can be expected in the final measurement, since noise photons will be reduced as a consequence of temporal filtering.

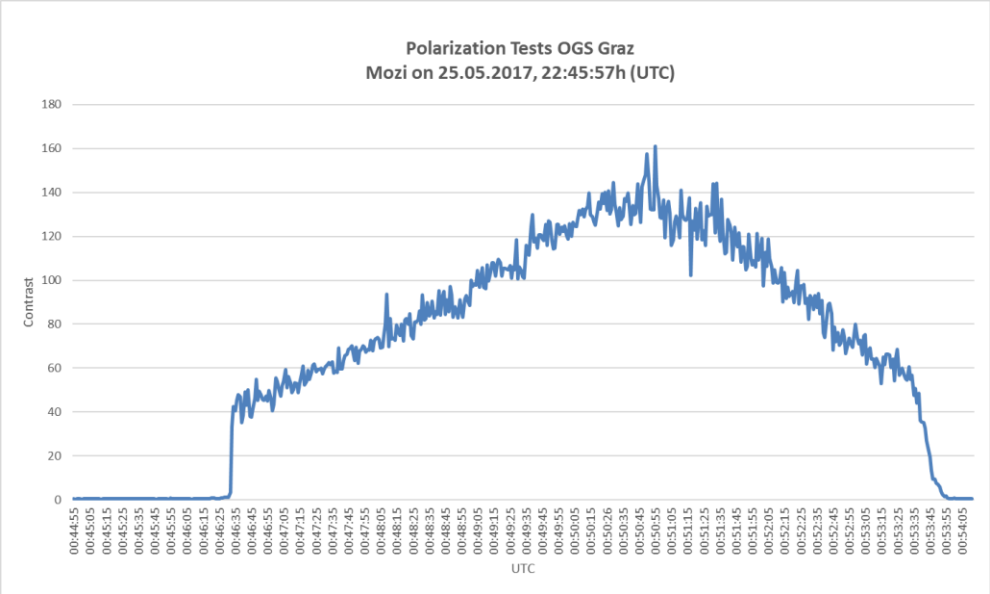

Figure 5 – Results of the polarization tests executed on 25th of May 2017. Please refer to the main text for a detailed discussion.

3.3 Decoy-state QKD protocol

The decoy-state QKD protocol was executed during several satellite passes in the time between 18th and 26th of June 2017. The performance of our quantum receiver module during the execution of the QKD procedure is shown in Figure 6 for a typical pass.

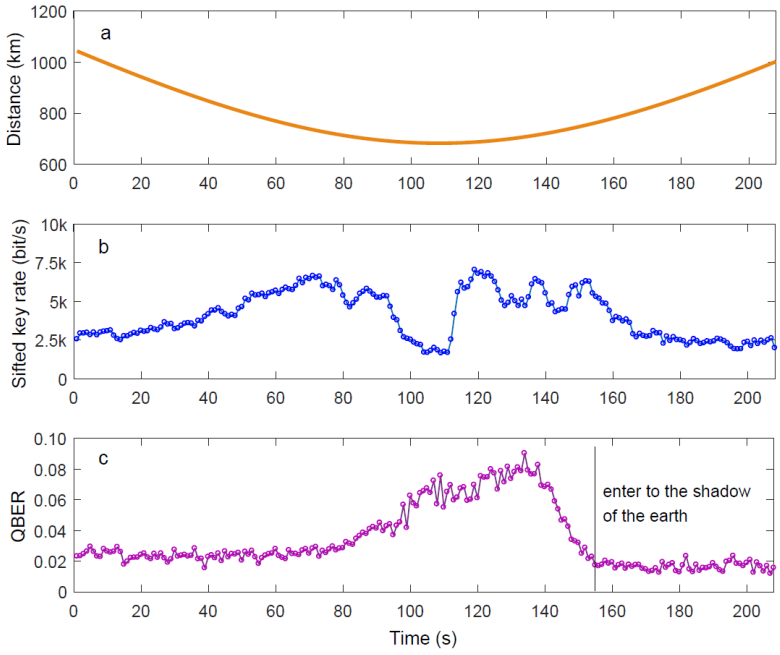

Figure 6 – Results of the decoy-state protocol measurements during a typical satellite pass. Please refer to the main text for a detailed discussion. (Figure taken from Ref. [5] Supplemental Material.)

The time-dependent distance between the satellite and the ground stations (Figure 6a), the sifted-key-rate (Figure 6b) as well as the quantum bit error ratio (Figure 6c) are shown. Since the downlinks to the Graz ground station have been performed around the time of summer solstice, the satellite was illuminated by the sun until approximately the point of highest elevation. Hence, the quantum bit error ratio is increasing until the satellite finally enters the shadow of the earth.

In total we could extract secure keys from 4 satellite passes over Graz with a total length of around 800kbit. Similarly, secure keys have been generated between the satellite and the Chinese ground stations in Xinglong and Nanshan. We then applied the key relay protocol to generate a secure key between the ground stations in Graz and in Xinglong and used the key to mutually transmit pictures of Erwin Schrödinger and Micius between Austria and China (see Figure 7) using one-time pad encryption.

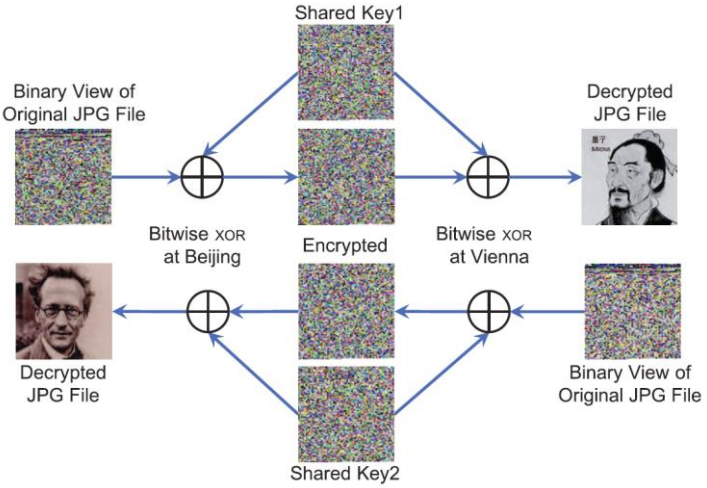

Figure 7 – Schematic of the transmission of two pictures encrypted with the generated secure quantum keys. (Figure taken from Ref. [5].)

4. CONCLUSION

We have summarized the basic concepts of the decoy-state QKD protocol using polarized faint laser pulses and described the key relay protocol that enables generating secure quantum keys between two parties that share only individual keys with a trusted relay station. Furthermore, we have presented the cornerstones and preliminary test results of the Chinese-Austrian collaboration project with a focus at the performance of the quantum receiver module installed at the Austrian Satellite Laser Ranging Station in Graz-Lustbühel. The project aimed at demonstrating an intercontinental quantum key exchange between optical ground stations in China and Austria using the Chinese Quantum Science Satellite "Micius" as a trusted relay station. Downlink experiments from the satellite enabled us to demonstrate QKD utilizing a space-based decoy-state QKD transmitter and to generate secure quantum keys between the Austrian ground station and ground stations in China following the key relay protocol. The generated keys have finally been used to encrypt and decrypt images of Schrödinger and Micius exchanged between Austria and China.

REFERENCES

[1] Lo, H.-K., Ma, X.-F. and Chen, K., "Decoy state quantum key distribution," Physical Review Letters 94(23), 230504 (2005).
[2] Lütkenhaus, N., "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A 61, 052304 (2000).
[3] Sharbaf, M. S., "Quantum cryptography: An emerging technology in network security," IEEE International Conference on Technologies for Homeland Security (HST), 13–19 (2011).
[4] Liao, S.K., *et al.*, "Satellite-to-ground quantum key distribution," Nature 549, 43–47 (2017).
[5] Liao, S.K., *et al.*, "Satellite-Relayed Intercontinental Quantum Network," Physical Review Letters 120, 030501 (2018).