Statistical Fluctuation Analysis for QKD between Micius Satellite and Graz Ground Station

Bo Liu[1,2,3], Thomas Scheidl[2,4], Johannes Handsteiner[2], Dominik Rauch[2], Baokang Zhao[5], Wanrong Yu[5], Bo Jiang[1], Jinfeng Huang[1], Chunqing Wu[6], Rupert Ursin[2,3], Anton Zeilinger[2,4]

[1] College of Advanced Interdisciplinary Research, NUDT, Changsha, 410073, China

[2] Institute for Quantum Optics and Quantum Information - Vienna (IQOQI), Austrian Academy of Sciences, Vienna, Austria

[3] Vienna Center for Quantum Science and Technology (VCQ), Vienna, Austria

[4] Quantum Optics, Quantum Nanophysics and Quantum Information, Faculty of Physics, University of Vienna, Boltzmanngasse 5, Vienna 1090, Austria

[5]College of Computer, NUDT, Changsha, 410073, China

[6]Guangzhou University, Guangzhou, 510006, China

Abstract

We performed decoy-state quantum key distribution (QKD) between a low-Earth-orbit satellite (Micius) and optical ground station located in Graz, which established secure key with kHz rate. With the trusted relay Micius, a secret key is created between China and Europe at locations separated by 7600 km on Earth. Taking care of the finite-size-effects, we made a rigorous statistical fluctuation analysis on the secure key generation procedure of the satellite-to-ground decoy-state QKD, performed between Micius and Graz ground station. Setting the failure probability to $\xi = 10^{-7}$ and the error correction efficiency to $f = 1.35$, the secure final key rate is 1.01 kbps in our actual key extraction system.

Quantum key Distribution (QKD), based on quantum fundamental principles, can generate information-theoretical-secure (ITS) keys for communication parties. We performed decoy-state quantum key distribution (QKD) between a low-Earth-orbit satellite (Micius) and optical ground station located in Xinglong, Nanshan and Graz, which established secure key with kHz rate [1, 2]. Then, upon request from the ground command, "Micius" acts as a trusted relay. It performs bitwise exclusive OR operations between the two keys and relays the result to one of the ground stations. That way, a secret key is created between China and Europe at locations separated by 7600 km on Earth. These keys are then used for intercontinental quantum secured communication. This was, on the one hand, the transmission of images in a one-time pad configuration from China to Austria as well as from Austria to China. Also, a video conference was performed between the Austrian Academy of Sciences and the Chinese Academy of Sciences. Relayed by quantum satellites, a intercontinental quantum secure communication network can be constructed to provide ITS protection for critical applications.

Taking care of the finite-size-effects, we made a rigorous statistical fluctuation analysis on the secure key generation procedure of the satellite-to-ground decoy-state QKD, performed between "Micius" and Graz ground station. For one extraction procedure performed between "Micius" and Graz ground station on 26th June 2017, the satellite sent out 6×10^9 pulses during 120 seconds, we received in total 546998 bits sifted key, the detailed analysis result is shown in Table 1. Setting the failure probability to $\xi = 10^{-7}$ and the error correction efficiency to $f = 1.35$, the secure final key rate is 1.01 kbps in our actual key extraction system.

Table 1: Statistical fluctuation analysis for QKD between "Micius" and Graz ground station

T (s)	Y_0	Q_1^z	Q_1^x	E_μ^z	E_μ^x	$e_1^{ph,z}$	$e_1^{ph,x}$	R_f (bps)
120	4.3×10^{-6}	6.3×10^{-5}	6.1×10^{-5}	1.34%	2.01%	9.87%	8.40%	1014.5

T is the effective time, Y_0 is the yield for the vacuum states, Q_1^i is the gain of single photon, E_μ^i is the overall QBER, $e_1^{ph,i}$ is the estimated single photon phase error rate, R_f is the final secure key rate. Here $i = z$ *or* x, means "Z" basis or "X" basis.

[1] Liao S.-K., Cai W.-Q., Handsteiner J., Liu B., Yin J., Zhang L., Rauch D., Fink M., Ren J.-G., Liu W.-Y., Li Y., Shen Q., Cao Y., Li F.-Z., Wang J.-F., Huang Y.-M., Deng L., Xi T., Ma L., Hu T., Li L., Liu N.-L., Koidl F., Wang P., Chen Y.-A., Wang X.-B., Steindorfer M., Kirchner G., Lu C.-Y., Shu R., Ursin R., Scheidl T., Peng C.-Z., Wang J.-Y., Zeilinger A., Pan J.-W, *Satellite-Relayed Intercontinental Quantum Network*, Physical Review Letters **120**, 030501 (2018).

[2] Liao S.-K., Cai W.-Q., et al., *Satellite-to-ground quantum key distribution*, Nature **549**, 43 (2017).