Quantum hacking of free-space QKD system by wavelength control with an external laser

Min-Soo Lee, Min Ki Woo, Jisung Jung, Il Young Kim, Yong-Su Kim, Sang-Wook Han, and Sung Moon

Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, South Korea

Fax: +82-(031)-546-7472 E-mail address: swhan@kist.re.kr

Quantum key distribution (QKD) systems have developed to securely share quantum keys between Alice and Bob [1]. The QKD systems can be divided into fiber-based QKD and free-space QKD. Although fiber-based QKD systems are more mature in terms of commercialization, free-space QKD systems using satellites, aircrafts, and balloons have been actively studied because the QKD systems could potentially solve the transmission distance problem [2]. Risks of quantum hacking exist in the both of QKD systems due to the incompleteness of hardware. While fiber-based QKD system attacks focus on detector attacks, free-space QKD system hacking studies typically consider the imperfections of the quantum light source as major attack paths. An eavesdropper can detect marginal characteristic differences of the photons from the four laser diodes (LDs) used in free-space QKD systems, such as the spatial, spectral, and temporal modes of the photons. The eavesdropper can infer the quantum state of the photon from these detected results. Although these methods successfully demonstrate the risk of quantum hacking, they are easily prevented by methods to make the four LDs indistinguishable, such as the temperature control of the laser diodes [3].

However, we develop a way to hack free-space quantum key distribution (QKD) systems by changing the wavelength of the indistinguishable quantum signal laser using an external laser [4]. Most free-space QKD systems use four distinct lasers for each polarization, thereby making the characteristics of each laser indistinguishable. We discover a side-channel that can distinguish the lasers by using an external laser. Our hacking scheme identifies the lasers by automatically applying the external laser to each signal laser at different intensities and detecting the wavelength variation according to the amount of incident external laser power. We conduct a proof-of-principle experiment to verify the proposed hacking structure and confirm that the wavelength varies by several gigahertzes to several nanometers, depending on the intensity of the external laser. The risk of hacking is successfully proven through the experimental results. Details will be provided in the conference.

References

1. C. H. Bennett, and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Theoretical computer science, 560, 7–11 (2014).

2. R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night,” New J. Phys. 4, 43 (2002).

3. M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, “Spatial mode side channels in free-space QKD implementations,” IEEE J. Sel. Top. Quantum Electron. 21, 187–191 (2015).

4. Min Soo Lee, Min Ki Woo, Jisung Jung, Yong-Su Kim, Sang-Wook Han, and Sung Moon, "Free-space QKD system hacking by wavelength control using an external laser," Opt. Express 25, 11124-11131 (2017).