Contribution ID: **1089** Type: **Talk**

Invisible Trojan-horse attack

Friday 25 August 2017 14:30 (30 minutes)

Quantum key distribution (QKD) allows two remote parties, Alice and Bob, to obtain symmetric keys –random but correlated sequence of bits –by exchanging quantum states [1]. The security relies on the fact that an adversary Eve cannot eavesdrop without introducing noticeable errors. However, due to gaps existing between theory and practice, it is often possible for an eavesdropper, Eve to implement some attacks to extract information about the keys without introducing noticable errors. Such gaps can arise due to imperfections in the physical devices and/or incorrect assumptions in the theoretical security proofs [2,3]. Hence, before trying to promote and commercialize QKD, it is of utmost importance to identify these gaps and evaluate their effects on the security.

This is where security evaluation of QKD comes in. It involves investigating practical QKD implementations to identify such theory-practice deviations, demonstrate the resultant vulnerability, and propose countermeasures to protect Alice and Bob from Eve. In this work, we have done such a security evaluation of the practical QKD system Clavis2 [4] running the Scarani-Acin-Ribordy-Gisin QKD protocol [5]. We evaluated security against the so- called Trojan-horse attack (THA) [6].

In a THA, Eve can probe the properties of a component inside Alice or Bob by sending in a bright pulse into the system and analyzing a suitable back-reflected portion of it. This attack was previously attempted [7] at telecom wavelength with the intention to breach the security of a similar system and was successful in remotely reading the phase modulator settings in Bob via a homodyne measurement. However, the resultant increase in afterpulsing [8] at Bob's InGaAs single-photon detectors (SPDs) led to an elevated quantum bit error rate (QBER) which disclosed the presence of Eve.

In this work, we have tested the experimental feasibility of a Trojan-horse attack that remains nearly invisible and evaluated the security of Clavis2 system against it. The invisibility has been achieved by using a different wavelength where detectors are expected to be less sensitive. To quantify the decrease in afterpulsing probabilities, we have compared the afterpulsing at λl = 1924 nm with that at λs = 1536 nm.

From Eve's point of view, the benefit of reduced afterpulsing at λl comes at the expense of a much higher attenuation inside Bob. Additionally, the degree of modulation received at λl differs from that at λs substantially. We quantify the increased optical attenuation and the suboptimal modulator response by means of further experimental measurements. Taking all these factors into account as well as optimizing the attack path through Bob, we evaluate the attack performances in the long wavelength regime. By means of a numerical simulation, we conclude that a Trojan- horse attack at λl can extract keys from the system at the same time being invisible to Alice and Bob. The invisible nature of the current attack poses a threat to the security of practical QKD if proper countermeasures are not adopted. We end by remarking that the attack can be mitigated by using a wavelength filter at the input of the QKD device.

[1] C. H. Bennett and G. Brassard, in Proceedings of IEEE In- ternational Conference on Computers, Systems, and Sig- nal Processing (IEEE Press, New York, Bangalore, India, 1984) pp. 175–179.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du˘sek, N. Lu¨tkenhaus, and M. Peev, Rev. Mod. Phys. 81, 1301 (2009).

[3] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, Contemporary Physics 57, 366 (2016), http://dx.doi.org/10.1080/00107514.2016.1148333.

[4] Clavis2 specification sheet, http://www. idquantique.com/images/stories/PDF/
clavis2- quantum- key- distribution/clavis2- specs.

pdf, visited 28 May 2016.

[5] V. Scarani, A. Ac´ın, G. Ribordy, and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004).

[6] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A 73, 022320 (2006).

[7] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, New J. Phys. 16, 123030 (2014).

[8] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. 13, 013043 (2011).

Topic:

Topic: Quantum Physics, Quantum Optics and Quantum Information

Summary

Authors: Mr SAJEED, shihan (university of waterloo); MINSHULL, Carter; Dr JAIN, nitin; Dr MAKAROV, vadim

Presenter: Mr SAJEED, shihan (university of waterloo)

Session Classification: Parallel session

Track Classification: C Quantum Physics, Quantum Optics and Quantum Information