

Security of quantum key distribution with bit and basis dependent detector flaws

Lars Lydersen and Johannes Skaar

Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway, lars.lydersen@iet.ntnu.no

Abstract

We consider the security of the Bennett-Brassard 1984 (BB84) protocol for Quantum Key Distribution (QKD), in the presence of bit and basis dependent detector flaws. We suggest a powerful attack that can be used in systems with detector efficiency mismatch, even if the detector assignments are chosen randomly by Bob. A security proof is provided, valid for any basis dependent, linear optical imperfections in the receiver/detectors.

Introduction

Quantum mechanics makes it possible to exchange a secret random bit string at a distance. In theory, the key distribution is secure, even if an eavesdropper Eve can do anything allowed by the currently known laws of nature.

In practical QKD systems there will always be imperfections. The security of QKD systems with a large variety of imperfections has been proved. However, a QKD system is relatively complex, and loopholes and imperfections exist that are not covered by existing security proofs.

Detector efficiency mismatch

We consider detector efficiency mismatch (DEM) [2]. If an apparatus has DEM, Eve can control the efficiencies of Bob's detectors by choosing a parameter t in some external domain. Examples of such domains can be the timing, polarization, or frequency of the photons [2,3].

The DEM loophole can be utilised to compromise the security of the Scarani-Acin-Ribordy-Gisin 2004 (SARG04), Ekert, and Differential Phase Shift Keying (DPSK) protocols, in addition to BB84 [4]. The loophole has also been used to compromise the security of a commercial QKD system [5,6].

A powerful attack

A frequently suggested patch is to let Bob choose from four different phase settings instead of only two,

called the four-state Bob patch. This randomly maps the bit values to the two detectors.

Nevertheless, powerful attacks exist, that compromise the security even in the presence of the four-state Bob patch. We suggest and analyse such a specific attack; a combination of an optimal individual attack, the time-shift attack, and a large pulse attack.

Securing QKD systems with DEM

A security loophole can be dealt with in two different ways: Either you modify the implementation, or you increase the amount of privacy amplification required to remove Eve's information about the key.

In QKD-systems with DEM we argue that the amount of privacy amplification should be increased. We establish the secret key rate which we have been able to improve since our first results [1]. Further we argue that to secure QKD systems with gated detectors, it is necessary to make some changes to the implementations.

References

1. Lydersen et al. arXiv:0807.0767 [quant-ph]
2. Makarov et al. Phys. Rev. A, 74 (2006), 022313
3. Fung et al. arXiv:0802.3788v1 [quant-ph]
4. Makarov et al. Quant. Inf. Comp., 8 (2008), 0622
5. Qi et al. Quant. Inf. Comp., 7 (2007), 73
6. Zhao et al. arXiv:/0704.3253v1 [quant-ph]