Security proof of quantum key distribution with detection-efficiency mismatch

Yanbao Zhang,[1,2,3,4] Patrick Coles,[3,4,5] Adam Winick,[3] and Norbert Lütkenhaus[3,4]

[1]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[2]*NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[3]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[4]*Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[5]*Theoretical Division, Los Alamos National Laboratory, Los Alamos, NM 87545, US*

Security proof of quantum key distribution (QKD) usually assumes that all threshold detectors involved have the same efficiency. Under this assumption, one cannot distinguish no-detection events due to detection inefficiency from those due to transmission loss. For simplicity, in the security proof of QKD people usually lump these two kinds of loss together as a new increased transmission loss followed by ideal threshold detectors with perfect efficiency.

However, in practice it is hard to build two detectors that have exactly the same efficiency. Furthermore, as demonstrated in recent experiments [1, 2], efficiency mismatch can be induced by an adversary using the fact that a detector can respond to a photon differently depending on degrees of freedom (for example, spatial mode) rather than those employed to encode information. In the presence of efficiency mismatch, one cannot treat detection inefficiency in the same way as transmission loss. So, current security-proof techniques cannot be applied.

Here we present a numerical method to prove security in the presence of detection-efficiency mismatch. The method works as long as the efficiency mismatch is characterized, even if the mismatch depends on degrees of freedom of a photon that are not employed to encode information. Our method can also be applied when the optical signal lives in the infinite-dimensional mode space with no limit on the number of photons contained in that space. In addition, with our method we can study the individual effects of transmission loss and detection inefficiency on the secret key rate.

The method presented here is based on our previous work [3], where the security proof of a general QKD protocol is formulated as a convex optimization problem. Here we extend this numerical method to QKD protocols with detection-efficiency mismatch. To study the case where the number of photons arriving at Bob is not limited, we bound the distribution of the number of photons directly from experimental observations using the method developed in our previous work [4].

To illustrate our method, we study an implementation of the BB84-QKD protocol with polarization encoding. We model the channel connecting Alice and Bob as a depolarizing channel where with probability p the input Bell state gets depolarized; additionally, the transmission efficiency (i.e., the single-photon transmission probability) over the channel is t; and Eve intercepts the single photon and resends a randomly-depolarized two-photon state to Bob with probability r. Moreover, we consider the case that Bob measures the polarization states of incoming photons using the active-detection scheme where the efficiencies of the two detectors can be mismatched.

First, we consider the case where both detectors have the same efficiency η. The typical results, as shown in Fig. 1, suggest that the traditional security proof by lumping detection inefficiency and transmission loss together is conservative. By treating these two kinds of loss separately, we can distill more secret keys.

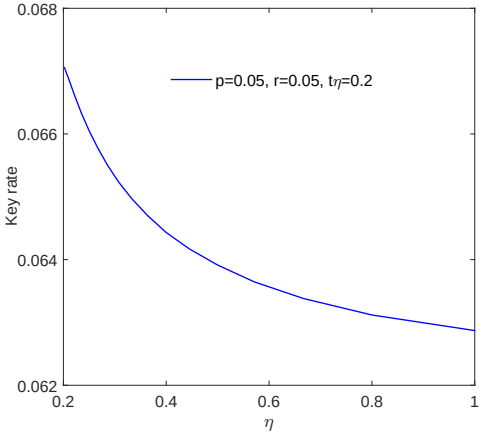

FIG. 1: Key rate as a function of the detection efficiency η of each detector. Here we keep the product of detection efficiency η and transmission efficiency t fixed, so the observed distribution is the same for all values of η plotted.

Second, we study the effect of detection-efficiency mismatch. We consider two scenarios: 1) All the optical signals stay in the same spatial mode, and the two detectors in the active-detection scheme have efficiencies η_1 and η_2 respectively; 2) The optical signals arriving at Bob can be in two different spatial modes. In the first spatial mode the two detectors' efficiencies are η_1 and η_2 respectively, while in the second spatial mode the two detectors exchange their efficiencies. In the security proof we can assume that the number of photons arriving at Bob is no more than 2, or we can prove security without such assumption. The typical results are shown in Fig. 2. These results suggest that the stronger the efficiency mismatch, the lower the secret key rate becomes.

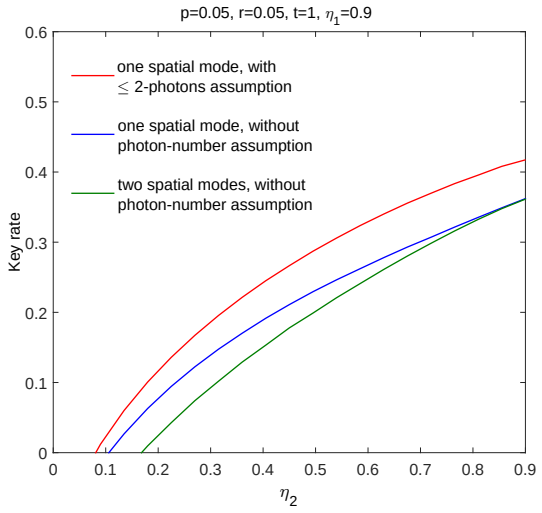

FIG. 2: Key rate as a function of the detection efficiency η_2 of the second detector (for the optical signals in the first spatial mode) in the active-detection scheme. Here we fix the efficiency of the first detector (for the optical signals in the first spatial mode) to $\eta_1 = 0.9$. See the text for other details.

[1] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, IEEE J. Quantum Electron. **21**, 1 (2014).

[2] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Phys. Rev. A **91**, 062301 (2015).

[3] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Nature Commu. **7**, 11712 (2016).

[4] Y. Zhang and N. Lütkenhaus, Phys. Rev. A **95**, 042319 (2017).