Entanglement verification with detection efficiency mismatch

Yanbao Zhang[1, 2] and Norbert Lütkenhaus[1, 2]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada*
[2] *Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada*

For quantum key distribution (QKD), we usually use optical signals, which are naturally described in an infinite dimensional Hilbert space, to encode information. To measure optical signals, we tend to use threshold detectors, which do not provide any refined knowledge about the photon number of an incoming signal. Often, there is a detection efficiency mismatch between the various detectors in a setup, either intrinsically, or induced by an adversary. Such a mismatch affects the security of the QKD system. For example, if the adversary can control the efficiency of each detector used and the efficiency mismatch introduced is large enough, successful intercept-resend attacks exist, as demonstrated in the recent work [1].

As entanglement, either physical or hypothetical, is a necessary condition for secure quantum key distribution [2] and also implies the absence of any intercept-resend attack, it is important for the sender and receiver in QKD to learn whether or not they can effectively share entanglement. If there is no detection efficiency mismatch, entanglement can be verified via applying squashing maps [3] which reduces the problem to a finite dimensional problem. However, in the efficiency mismatch case, no method is known so far to verify entanglement efficiently. Note that one can use Bell inequalities for this purpose, but they are too restrictive in practice.

Here, given that the detection efficiency mismatch is characterized and known, we present a method to verify entanglement in the implementation of the BB84 protocol with polarization encoding. (The method can be extended to other QKD protocols.) The main idea is to construct an expectation-value matrix (EVM) [4, 5] using a finite number of real measurements which contain the efficiency mismatch information. In this way, we map an infinite dimensional density matrix into a finite dimensional EVM.

To illustrate our method, we study a toy channel connecting the sender and the receiver, where with probability ω it depolarizes the input Bell state and then with probability p it intercepts the single photon and resends multiple photons to the receiver. The receiver can measure the polarization state of incoming photons using either the active or passive detection scheme. We would like to know, for which values of ω and p the sender and receiver can verify entanglement. For this particular situation, the results using the active detection scheme are shown in Fig. 1. The results suggest that, the larger the mismatch is, the smaller the set of quantum channels that can be verified to transmit quantum information becomes. Similar results are obtained for the passive detection scheme. We also compare our method with the method based on squashing maps [3] when there is no mismatch, and the results as in Fig. 2 show that our method gives a stronger criterion.

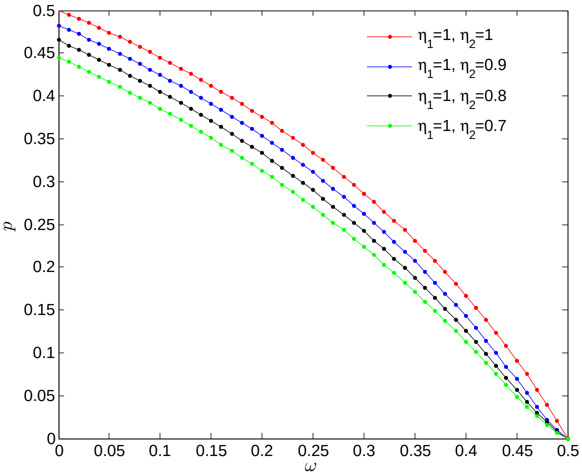

FIG. 1: Results in the active detection scheme. Different curves are for different mismatches as labeled. For each mismatch, when the noise parameters ω and p in the transmission are below the curve, one can verify entanglement. See the text for more details.

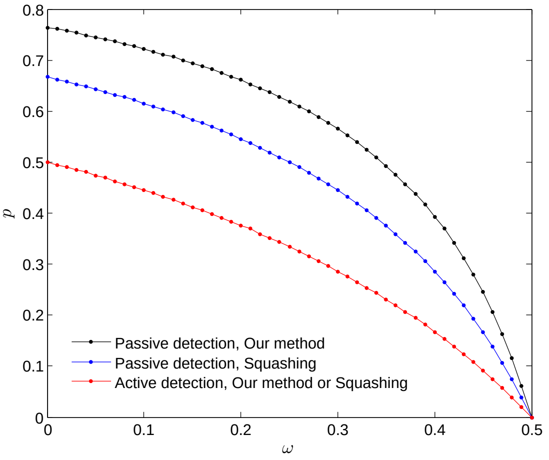

FIG. 2: Comparison of our method with the method based on squashing maps, when all detectors are perfect. Different curves are for different detection schemes and methods as labeled. For each case, when the noise parameters ω and p in the transmission are below the curve, one can verify entanglement. See the text for more details.

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

[2] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[3] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[4] J. Rigas, O. Gühne, and N. Lütkenhaus, Phys. Rev. A **73**, 012341 (2006).

[5] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007).