Quantum Key Distribution with Coherent States

Jie Lin, Patrick J. Coles, Adam Winick, and Norbert Lütkenhaus
Institute for Quantum Computing and Department of Physics and Astronomy,
University of Waterloo, N2L3G1 Waterloo, Ontario, Canada

Background.— In practical quantum key distribution (QKD) devices, an attenuated laser source has been commonly used instead of a single-photon source. To counteract more powerful eavedropping attacks allowed by this replacement, techniques such as decoy-state methods[1] and discrete phase randomization[2] have been proposed and implemented to improve the performance of such coherent-state protocols. On the other hand, to use optically integrated sources and to operate at higher clock speed, it is more desirable to utilize coherent state signals without dephasing. Here, we want to balance the tradeoff between the ease of implementation and the performance of a protocol by analyzing how additional states that Alice sends to Bob affect the key-generating rate. In addition, this work demonstrates the applications of the numerical key rate calculation method developed by Coles, Winick, and Lütkenhaus[3].

Methods.—Obtaining a reliable lower bound of the key generation rate is at the heart of the security proof for a QKD protocol. We apply the numerical approach developed by Coles et al.[3] to calculate asymptotic limit of the key rate. It can be summarized as follows: we solve the well-known key rate formula [4] by first performing a convex minimization where the computer terminates at a sub-optimal point, and then by solving the dual problem of a linearization from the sub-optimal point to obtain a reliable lower bound.

Protocols.— We investigate the variations of the protocol proposed in [5]. It involves BB84-type signal states and measurements. The key is encoded in the relative phase between the reference pulse and the signal pulse whose intensities are the same. Each variation involves different additional states that Alice can send to Bob, as illustrated below.

With a non-random phase.— The protocol is simply the original protocol with no additional states. The phase of the coherent states is fixed and known to Eve. As shown in Figure 1, our numerical calculation has provided an improved lower bound compared to the analytical results in [6].

With discrete phase randomization.— Alice performs an active phase randomization via a phase modulator with a finite number of settings. Our numerical calculation demonstrates the increase of key rate as more phases are added. Moreover, the key rate quickly approaches to the asymptotic limit of continuously randomized phases with only a few number of phases. This agrees with [2]. In addition, our numerical calculation has the flexibility to choose which phase choices are included. The key rate calculation can base on the actual phases used in the implementation, thereby imposing less restrictive requirements on the phase modulator.

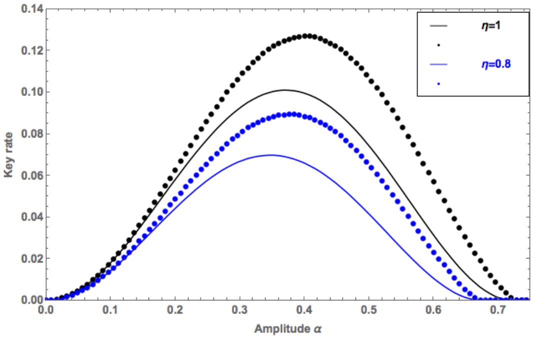

FIG. 1: The key rate as a function of the amplitude of coherent states for the protocol in [5] with single-photon transmission probabilities $\eta = 1$ (black curves) and $\eta = 0.8$ (blue curves). Solid lines are values given by the analytical expression in [6] and solid dots are our numerical results.

With decoy states and a non-random phase.— In this protocol setup, Alice applies the decoy-state methods and modifies the intensity of the coherent states. We adopt the intensity choices in [1]. However, we do not assume a random phase for each pulse. Our numerical calculation demonstrates the ability to handle decoy states, and we are working on incorporating the decoy-state method into this non-random phase coherent state protocol.

With decoy states and discrete phase randomization.— Alice applies both the decoy-state methods and discrete phase randomization. We are currently investigating various combinations of decoy-state settings and choices of phases and trying to understand which states have more significant impacts on the key rate.

Conclusion.— We have demonstrated the ability of applying the new numerical approach [3] for key rate calculation to QKD protocols involving coherent states. With this numerical approach, we have been able to improve some existing theoretical results. More importantly, it enables us to study what additional test states are the most effective in improving the key rate.

[1] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[2] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, New J. Phys. **17**, 053014 (2015).

[3] P. J. Coles, A. Winick, and N. Lütkenhaus (in preparation).

[4] I. Devetak and A. Winter, in *Proceedings of the Royal Society A* (2005), vol. 461, pp. 207–235.

[5] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[6] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 431 (2007).