Comparison of Discrete and Continuous Variable Quantum Key Distribution Protocols over a Thermal-Loss Channel

Sebastian P. Kish, Ping Koy Lam and Syed M. Assad

[a]*Centre of Excellence for Quantum Computation and Communication Technology, Department of Quantum Science and Technology, Research School of Physics, The Australian National University, Canberra, ACT, Australia.*

Quantum key distribution (QKD) enables the sharing of keys between two parties, Alice and Bob. Once a quantum secret key is established, it can later be used by both parties to unlock encrypted communication with total confidentiality. In fact, this form of communication is guaranteed to be secure against an eavesdropper, Eve, by the laws of quantum physics. The first proposed QKD protocol based on discrete-variables (DV), which was named after the authors Bennett & Brassard, is BB84. This protocol relies on the use of single-photon states and remains a robust QKD protocol to this day [1]. Fifteen years afterwards, QKD was extended to continuous-variables (CV), which was initially based on entangled multi-photon two-mode squeezed states (TMSV) and use of low-noise coherent detection [2, 3, 4]. An equivalent scheme—the squeezed-state protocol—only requiring preparation of modulated squeezed states was proposed shortly afterwards [5].

In a thermal-loss channel, it is uncertain whether a discrete-variable (DV) or a continuous-variable (CV) quantum key distribution (QKD) protocol is more optimal. In this work, we investigate common DV-QKD and CV-QKD protocols, including the BB84 and squeezed-state protocols, in a thermal-loss setting but with the assumed availability of perfect sources and detectors. We find that in an intermediate-noise regime, the BB84 protocol attains positive key rates higher than any known CV protocol. On the other hand, the squeezed-state protocol can outperform the BB84 protocol in a high thermal noise regime. Our analysis addresses the question of which QKD platform and their respective protocols can perform optimally for different thermal-loss channel parameters assuming the protocols run perfectly.

[1] Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. Theor. Comput. Sci. **560** 7–11 (2014).

[2] Ralph, T. C. Continuous variable quantum cryptography. Phys. Rev. A **61**, 010303 (1999).

[3] Ralph, T. C. Security of continuous-variable quantum cryptography. Phys. Rev. A **62**|, 062306 (2000).

[4] Hillery, M. Quantum cryptography with squeezed states. Phys. Rev. A **61**, 022309 (2000).

[5] Cerf, N. J., Lévy, M. & Assche, G. V. Quantum distribution of gaussian keys using squeezed states. Phys. Rev. A **63** 052311 (2001).