Enhancing the Viable Distance of Quantum Key Distribution by Recycling Information from Unambiguous Discrimination of Discrete-Modulated Coherent States

L. F. Melo[1,2]

[1] *Department of Physics, Universidade Federal de Minas Gerais, Belo Horizonte, Brazil*
[2] *SENAI CIMATEC, Salvador, Brazil*
Contact Email: lucas.felipe@fbter.org.br

Quantum key distribution (QKD) aims at sharing a secret key among distant parties, Alice and Bob, in such a way that an eavesdropper, Eve, cannot acquire any information about the key. Such task can be done by using a discrete set of phase-symmetrically distributed coherent states that have same mean photon number; such realization is called a phase-shift-keying (PSK) constellation, which includes binary (BPSK), ternary (TPSK) and quatenary (QPSK) modulations. For the reading step, Bob is confined by the laws of quantum mechanics, which prohibit perfect distinction of nonorthogonal states. Under such prerogative, the minimum-error discrimination (MED) was designed to minimize the error probability given that a conclusive answer is always obtained; whereas the optimal unambiguous discrimination (UD), which received notable attention in the field of quantum cryptography, was derived for allowing error-free results with the cost of discarding some trials at optimized rate. One unpleasant aspect of probabilistic discrimination strategies like UD is the potentially useful information that may be present on the failure outputs of the measurement, which are usually discarded. One interesting question, and the main purpose of this work, is how such remaining information can be useful in the field of QKD.

In this work, we consider a QKD scheme where Alice uses a discrete PSK constellation of coherent states and Bob may perform standard UD or a version where a MED is performed on the failure outputs of the former, which we refer to as discrimination with information recycling. We consider beam-splitter attacks and pure-loss channel transmission and show that Alice and Bob can share a secret key using reverse reconciliation. We consider binary, ternary and quaternary PSK constellations (e.g., $N = 2, 3, 4$) and show that for $N > 2$ the protocol with information recycling is more robust with respect to distances than standard UD, providing good performance above 250 km. Differently from standard UD, which is less efficient for greater N, the protocol with information recycling provides higher key rates for TPSK and QPSK constellations. In particular, we find that the ternary configuration saturates the key rate if the distance between Alice and Bob is larger than ~ 100 km.