Quantum Secure Direct Communication Using Differential Quadrature Phase-Shift Quantum Key Distribution

Ranara L. C. Damasceno, Antônio Geovan de A. H. Guerra and Rubens Viana Ramos

ranaralouise@gmail.com geovanguerra@gmail.com rubens.viana@pq.cnpq.br

Lab. of Quantum Information Technology, Teleinformatic Engineering Department, Federal University of Ceara, Fortaleza, Brazil

In this work, firstly an optical setup for quantum secure direct communication (QSDC) using differential quadrature phase-shift quantum key distribution (DQPS-QKD) is presented. The advantages of the proposed setup are:

1) It is fully implementable with current technology.
2) Its security comes from the security of the DQPS-QKD [1,2]. Hence, it is resistant to all attacks that DQPS-QKD is resistant.
3) At the end of the protocol, besides the message sent deterministically from Alice to Bob, they also share a key that can be used latter for cryptographic tasks. Hence, the optical setup permits QSDC and QKD simultaneously. The last protects the former.

The disadvantages are:

1) The protocol proposed does not prevent Eve of knowing the information sent from Alice to Bob. Although Alice and Bob will know when Eve attacked, the information sent during an attack must be discarded. This limitation reduces the possible practical applications of the first QSDC setup proposed.

2) It employs weak coherent states, hence the transmission of the full information will require multiple runs of the protocol since many optical pulses will have no photons. On the other hand, a simple codification can be used to simplify the protocol realization: each logical '0' ('1') is represented by a sequence of *n* physical zeros (ones). This repetition code does not decrease the security since it implies in a longer running of the DQPS-QKD protocol.

Aiming to solve the first limitation, a second optical setup is proposed. In order to prevent Eve of obtaining useful information, frequency-dependent phase modulation, coherent and thermal light states are used [3]. Hence, there is an increase of the complexity of the optical setup but it is still feasible with current technology.

[1] K. Inoue, Y. Iwai, "Differential-quadrature-phase-shift quantum key distribution", Phys. Rev. A, 79, 022319, 2009.
[2] S. Kawakami, T. Sasaki and M. Koashi, "Security of differential quadrature phase shift quantum key distribution", xxx.lanl.gov 1512.08129v2, 2015. Available on http://arxiv.org/pdf/1512.08129v2.pdf.
[3] P. V. P. Pinheiro and R. V. Ramos, "Two layer quantum key distribution", Quant. Inf. Process., 14, 6, 2111, 2015.