CV-QKD Applications for Non-deterministic Noiseless Amplification

T.C.Ralph (1), A.P.Lund (2)
1: Department of Physics, The University of Queensland, Brisbane, 4072, QLD Australia.
ralph@physics.uq.edu.au
2: Centre for Quantum Computer Technology, School of Science, Griffith University.

Abstract

We introduce the idea of non-deterministic noiseless linear amplification and propose an explicit realization based on linear optics and photon counting. We discuss applications of the device to cv-qkd both in terms of distilling entanglement and in directly amplifying quantum transmissions.

It is well known that a linear or phase insensitive amplifier acting on a quantum optical field, or more generally on any harmonic oscillator state, must introduce noise [1]. Never-the-less we have recently shown that a non-deterministic, but heralded, linear amplifier can be noiseless [2]. In particular we propose a linear optics circuit, heralded by photon counting outcomes (see Fig.1), that approximately applies the transformation:

$$\hat{T}|\alpha\rangle = c|g\alpha\rangle$$

where g is a real number greater than 1, $|\alpha\rangle$ is a coherent state with complex amplitude α, and c is complex number with absolute value less than 1.

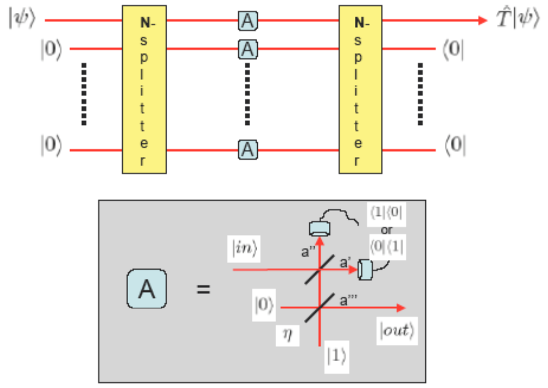

Figure.1 Schematic of the noiseless linear amplifier. The N-splitter is an array of beamsplitters that evenly divides the input beam. The second N-splitter coherently recombines the beams and is considered to have succeeded if no light exits through the other ports, as determined by photon counters. The interaction labelled "A" interacts a single photon ancilla with an input beam as shown in the gray inset. The upper beamsplitter is 50:50 whilst the lower beamsplitter has transmission η as shown. The interaction succeeds if a single count is recorded at a' and no count at a'', or vice versa.

Such a device could have several applications. We consider here its use in extending the range of cv-qkd. Consider first a direct cv-qkd protocol involving the transmission of coherent states from Alice to Bob through a lossy channel. If Bob applies noiseless amplification to the states that arrive then he can postselect an ensemble of states for which the effective channel transmission is higher – increasing security. Similarly for an entanglement based protocol in which Alice keeps one output of an EPR generator (two-mode squeezer) and sends the other to Bob through a lossy channel (see Fig.2), noiseless amplification can distill purer shared entanglement (see Fig.3).

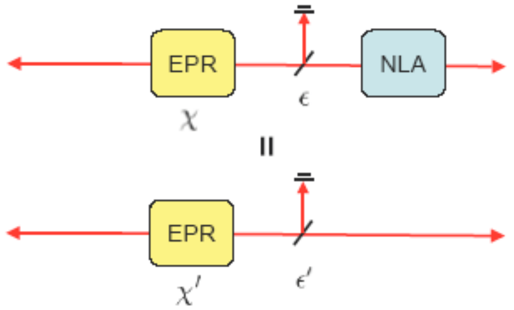

Figure 2: Entanglement distillation using noiseless amplification and the equivalent entanglement produced, where $\chi<\chi'$ and $\varepsilon<\varepsilon'$

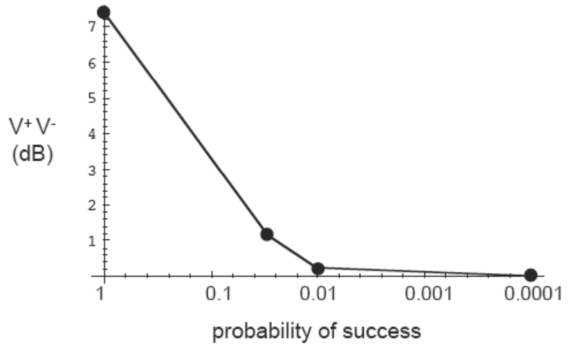

Figure 3: Purity of amplified output states versus probability of success with EPR state inputs where a fixed strength of entanglement is targeted. The purity is quantified by the uncertainty product of the squeezed and anti-squeezed quadrature correlations of the post-selected EPR state.

References

1. C.M.Caves, Phys.Rev.D **23**, 1693 (1981).
2. T.C.Ralph and A.P.Lund, arXiv:0809.0326 (2008).