CV-QUANTUM

Improving Security and Capacity Using Continuous Variables Quantum Communications

Quantum technologies can address two of the more challenging problems that networks face nowadays: Capacity and Privacy. Recently it was proposed that quantum communications systems can be implemented with optical continuous variables. In the framework of this project, we engineered a continuous variable communication system to implement bit commitment and oblivious transfer quantum primitives.

Main Project Team	
Armando Nolasco Pinto	**OCP-Av**
Nelson Muga	OCP-Av
Nuno Silva	OCP-Av
Álvaro Almeida	OCP-Av
Paulo Mateus	SQIG-Lx
Nikola Paunkovic	SQIG-Lx
Ricardo Loura	SQIG-Lx
Indicators	
Funding	30k €
Journal papers	10
Conference papers	12
Concluded PhD	3
Concluded MSc	1

Two Main Publications

Almeida, A. ; Stojanovic, A. ; Paunkovic, N. ; Loura, R. Loura ; Muga, N. J. ; Silva, N. A. ; Mateus, P. ; André, PS ; Pinto, A. N.; "Implementation of a two-state quantum bit commitment protocol in optical fibers". "Journal of Optics" Vol. 18, Nº 1, pp. 015202 - 015202, January, 2016.

A. Souto, P. Mateus, P. Adão, N. Paunkovic; "Bit-string oblivious transfer based on quantum state computational distinguishability". "Physical Review" A, Vol. 91, No. 1, pp. 042306 - 042306, April, 2015.

PROJECT WEBPAGE URL

http://www.av.it.pt/cv-quantum/

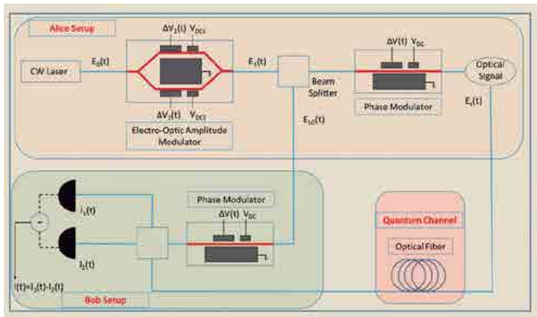

Fig. 1 Setup used to implement a continuous variable system.

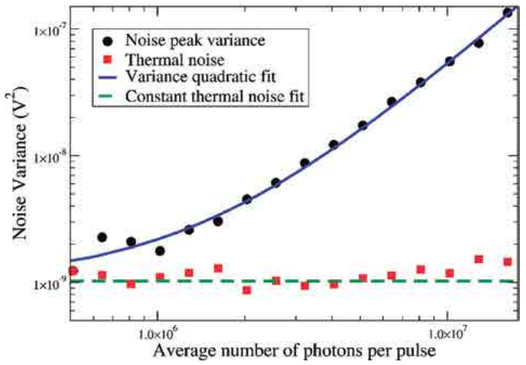

Fig. 2 Characterization of homodyne detector noise variance.

GENERAL MOTIVATION AND OBJECTIVES

Most of the quantum protocols available nowadays encode the information in one of the degrees of freedom of single photons. In that sense, the quantum information used in that protocols is discrete, described by qubits. Recently, an alternative approach to discrete qubits has been suggested, which is based on continuous variables of the electromagnetic field such as phase and amplitude. This new approach has been suggested to replace the single photon detectors with standard telecom detectors, which are faster and more efficient. Moreover, continuous variable protocols can be implemented with weak coherent light fields, which are easy to generate and to practically implement. Quantum continuous variables protocols demands homodyne detection schemes instead of direct detection based on single photon detectors.

The main scientific objectives of this research project are: to propose secure bit commitment and oblivious transfer quantum protocols based on continuous variables. To evaluate the capacity of an optical fibre for low-energy optical signals. To optimize the transmitter and the receiver for weak coherent fields

CHALLENGE

An important advantage of the continuous variables approach, when compared with discrete variables ones, has to do with their simple system architecture that eliminates the need for specific resources such as single-photon sources and detectors, which opens the door to higher modulation rates. Nevertheless, the weak coherent field used as quantum information carrier demands high sensitivity coherent detection. The coherent receiver must be able to reconstruct the amplitude quadrature and/or the phase quadrature of the input signal depending on the relative phase between the signal and the local oscillator, considering that the signal-to-noise ratio at receiver decision circuit input is approximately equal to one. This requires fibre-based homodyne detectors with high stability, low electronic, and high common mode rejection ratio.

Bit commitment and oblivious transfer are two basic quantum primitives can be composed to set up much more complex protocols. Those basic primitives are well stablished in discrete variable quantum systems. To be used in continuous variable systems they must be modified by replacing perfectly distinguishable with quasi-orthogonal partially distinguishable states.

WORK DESCRIPTION AND ACHIEVEMENTS

In this project we design and assemble a balanced homodyne detector for being used in continuous variable quantum communication system. In a homodyne receiver there are two fundamental noise sources, producing fluctuations in the current even if the input optical signal is constant in time, i.E. Shot and thermal noise sources. We perform an experimental and theoretical characterization of the variance of noise sources, including noise due to local oscillator time intensity fluctuation resulting of a not null common mode rejection of the detector. We observe a shot-to-thermal noise higher than 11 db.

The presence of active components such as amplifiers in the networks does not allow to provide to the classical networks quantum security and privacy. We have demonstrated that removing some amplifiers from the end to the beginning of a transmission link does not significantly change the capacity of the link, extending in that sense the reach of unamplified links. Moreover we have demonstrated in that regime that the performance of the communication link is mainly limited by the receiver shot noise, instead by the optical noise due to the amplifiers and nonlinear effects.

We develop two quantum primitives, mainly oblivious transfer and bit commitment, for being used with continuous variable communication system, extending its security proof to the use of weak coherent light fields. Those quantum primitives have the same

Experimental requirements as quantum key distribution, which is already a mature technology. Finally, we develop and validate experimentally a two state quantum bit commitment primitive in optical fibres.