PhD Thesis Defense ELSA PASSARO 'Impact of Imperfections on Correlation-Based Quantum Information Protocols'

ELSA PASSARO

May 30, 2016

Monday, May 30, 11:00. ICFO Auditorium

ELSA PASSARO

Quantum information science is a rapidly evolving field both from the theoretical and the experimental viewpoint, motivated by the fact that protocols exploiting quantum resources can perform tasks that are unfeasible in classical information theory. Interestingly, the trustworthiness of quantum information protocols can be certified relying upon as few assumptions as possible adopting the "device-independent" (DI) framework. In this scenario no assumption is made on the internal working of the involved devices, which are treated as black boxes. The quantum certification of DI protocols is guaranteed by the nonlocal character of the correlations between the inputs and outputs of those boxes. Unfortunately,

demonstrating nonlocality is highly demanding from the implementation point of view, since low levels of experimental imperfections are tolerated. Those imperfections (e.g.noise and losses) may alter the input/output statistics, thus undermining the reliability of DI protocols. The experimental requirements for the security of DI protocols can be relaxed considering partly-DI scenarios, in which additional assumptions on the devices or the systems used in the protocols are made. Indeed, partly-DI protocols offer two main advantages: First, they are more secure than standard device-dependent protocols; second, they are more robust to experimental imperfections than their fully-DI counterparts. The general aim of this Thesis is to provide bounds on imperfections and losses arising in experimental implementations of DI and partly-DI protocols that are necessary or sufficient for security.

In the first part, we tackle the problem of secure implementation of quantum key distribution protocols in the DI and partly-DI scenarios. The goal is to establish conditions on the detection efficiency necessary for the security of those protocols. To this aim, we present a general attack on the detectors from which we derive bounds on the critical detection efficiency that do not depend on the number of measurements applied nor on the number of outcomes.

In the second part, we study randomness certification in the steering and the prepare-and-measure scenarios. We devise an optimal method for quantifying the local and global randomness that can be extracted in both scenarios. Applying this method we provide sufficient conditions for randomness certification in the presence of noise and losses. Moreover, we present a method that for any fixed state gives the optimal measurements and steering inequality that certify the most randomness.

The next question we address is the secure implementation of semi-device-independent (SDI) protocols, whose quantum certification is provided by dimension witnesses. We study the problem of the robustness of DI dimension witnesses to loss, in the case in which shared randomness is allowed between the preparing and measuring devices. The main result in this part is to provide thresholds for the critical detection efficiency necessary to perform reliable dimension witnessing. Furthermore, we study detection loophole attacks on SDI quantum and classical protocols in the case in which the preparing and measuring devices do not share correlations. We determine general conditions under which a potential eavesdropper cannot exploit the experimental losses to hack such protocols.

Finally, we focus on a recently demonstrated quantum process and its inverse, namely the quantum state joining and splitting processes. We prove that a linear-optical realization of the quantum state joining of two photons relying only on postselection -and thus simpler than

the implementation originally proposed- is not possible, implying that it requires at least one ancilla photon. Furthermore, we demonstrate that the quantum joining process is equivalent to the preparation of a particular class of three-qubit entangled states, showing that this process can also find application for generating complex cluster states of entangled photons.

Monday, May 30, 11:00. ICFO Auditorium

Thesis Director: Prof. Dr. Antonio Acin