PhD Thesis Defense ALEJANDRO MATTAR 'Quantum Information with Black Boxes - Lifting Protocols from Theory to Implementation'

ALEJANDRO MATTAR

October 17, 2017

Tuesday October 17, 12:00. ICFO Auditorium

ALEJANDRO MATTAR

Quantum Information Theory

ICFO-The Institute of Photonic Sciences

According to recent estimates, 10^18 bytes of data are generated on a daily basis around the globe. Our information society urges for radical solutions to treat such data deluge. By exploiting fundamental key elements of quantum theory ---arguably the most probed theory

of modern physics--- quantum information science is nowadays revolutionizing the way in which we acquire, process, store and transmit information. In the midst of the information era, the potential of quantum technologies is being recognized by the industry sector, and in turn, new capabilities for quantum information processing keep driving exciting discoveries related to more fundamental aspects of science.

There are several research programs all around the world fostering the development and commercialization of quantum technologies, mostly for cryptographic and randomness generation duties. Thus, the technological limitations that today step us aside from the quantum information era are gradually being overcome. But there is a fundamental issue that still needs to be faced: the impossibility to know what is really going on in quantum experiments, due to their atomic-scale dimensions.
Indeed, how will an average user guarantee the proper functioning of a quantum device that has been purchased from an external company? To his eyes, the device will merely look like a black box. Even if the customer holds a PhD in quantum science, the issue will remain fundamentally cumbersome because of the impossibility to fully control, i.e. monitor, all the physical processes occurring in any quantum experiment. Furthermore, the situation turns even more dramatic when considering adversarial applications, where a malicious eavesdropper could break the devices to manipulate their internal working, turning the protocol insecure and hence irrelevant as well.

Therefore, it is the purpose of this Thesis to contribute to the experimental development of quantum information protocols with uncharacterized devices, namely, device-independent quantum information protocols. These protocols are naturally immune to any attack or failure related to mismatches between protocol theory and its actual implementation. This is achieved throughout the different Chapters by pursuing the following three overlapping duties: (i) To broaden theoretic capabilities by establishing a richer understanding of relevant fundamental resources lying at the basis of the theory of quantum information with uncharacterized devices. (ii) To develop competitive quantum information protocols by finding an adequate trade-off between high-performance and practicability; between the power of the device-independent framework and its less demanding, so-called semi-device-independent, relaxations. (iii) To analyze and improve experimental conditions of diverse physical setups in order to carry out implementations in proof-of-principle experiments demonstrating quantum information protocols with black boxes.

Our objective of turning the theory of quantum information into a graspable technology for

our society through the development and implementation of protocols based on the minimalist, user-friendly, black-box paradigm contributes not only to the technological development of these protocols, but it also offers valuable insights on more fundamental aspects of quantum theory. In this sense, we contribute to the characterization and quantification of entanglement ---the pivotal quantum resource at the basis of most testable phenomena without classical account--- in scenarios of practical interest where uncharacterized devices are used. From the more applied perspective, we contribute to the development of two specific information tasks: the certification of genuinely random numbers in device-independent and semi-device-independent scenarios, and the generation of a shared secret key among two parties in a full device-independent manner.

Tuesday October 17, 12:00. ICFO Auditorium

Thesis Director: Prof Dr. Antonio Acin dal Maschio