PhD Thesis Defense IVAN SUPIC 'Device-Independent Certification of Quantum Resources'

IVAN SUPIC

September 19, 2018

Wednesday, September 19, 11:00. ICFO Auditorium

IVAN SUPIC

Quantum Information Theory

ICFO-The Institute of Photonic Sciences

The last two decades have been a very fruitful period for the fundamental research related to quantum information theory. Today we have a fairly good understanding of how intrinsically quantum properties affect various computational and cryptographic tasks. Practical implementations are advancing as well. Devices performing quantum key distribution or quantum random number generation are already commercially available. As time goes more

resources are being invested in building a device which would demonstrate and exploit quantum computational supremacy. In the context of the impending second quantum revolution it is of crucial importance to build new certification tools, improve the existing ones and understand their limits. When assessing the non-classicality of a given device it is essential to estimate which assumptions about the device are not jeopardizing the certification procedure. Device-independent scenario does not make any assumptions about the inner functioning of devices, but usually only assumes the correctness of quantum theory. It gained a lot of attention because it manages to certify the quantum character of certain devices while giving to potential adversaries all power allowed by the laws of physics. Device-independent certification of various quantum resources is the main subject of the thesis.In the first part of the thesis we focus on self-testing, one of the simplest device-independent protocols. It aims to recover quantum states solely from the observed measurement correlations. It has a fundamental importance for the device-independent paradigm because it shows which quantum states can leave a device-independent ?imprint?. Practically, it bears a significance as a possible first step in more complex protocols such as blind quantum computing, randomness generation or quantum key distribution. In this thesis we present several new self-testing results. Firstly, we provide a proof that chained Bell inequalities can be used to robustly self-test maximally entangled pair of qubits and an arbitrary number of real measurements. As a side result we also present a protocol for randomness generation based on the maximal violation of a chained Bell inequality. Secondly, we provide new self-testing protocols for several classes of multipartite quantum states: Dicke states, graph states and all states of arbitrary finite dimension admitting the Schmidt decomposition. Finally, we extend self-testing to the semi-device-independent scenario and explore its properties.In the second part we move to the certification of several quantum resources and protocols. While the device-independent scenario offers the utmost security, it has a few undesirable properties. Firstly, it is very difficult to implement. In some cases, depending on the scenario, stronger assumptions about the functioning of the devices can be made. Secondly, the scenario relies on the observation of nonlocal measurement correlations, which makes some classes of entangled states useless for device-independent protocols. We address the first difficulty by presenting quantification of entanglement and randomness in quantum networks in the measurement-device-independent scenario, in which parties are assumed to have characterized preparation devices. In this scenario all entangled states can be detected. To address the second issue, we merge measurement-device-independent entanglement detection with self-testing and present the first protocol for a completely device-independent detection of all entangled states. The protocol involves placing an entangled state to be detected in a quantum network. Finally, we identify quantum state teleportation as a representative of one-sided measurement-device-independent protocols, which helps us to propose a new benchmark for certifying the non-classicality of teleportation. By using this new benchmark we show that

all entangled states can lead to a teleportation protocol that cannot be simulated classically.

Wednesday, September 19, 11:00. ICFO Auditorium

Thesis Advisor: Prof Dr Antonio Acin