THESIS DEFENSE | Certification in quantum information theory: key distribution, self-testing and entanglement

MARIA BALANZO JUANDO

September 12, 2024

10:00

ICFO Auditorium and Online (Teams)

In the beginning of the last century, we witnessed a change of paradigm in how physics described the world with the formulation of quantum mechanics. This new theory shook the pillars of science by setting fundamental limits on our ability to describe nature. It was able to explain the laws that govern physics at the microscopic level, which could not be explained by means of the existing laws. The behavior at such small scales differs significantly from our daily experience. For instance, exotic phenomena such as entanglement or nonlocality are exclusively observed at the microscale. Entanglement and nonlocal correlations represent two essential resources in quantum information processing, enabling novel tasks that are

unattainable within a classical framework.

The end of the twentieth century has seen a wave of studies on the fundamental properties of quantum theory. Nowadays, as a consequence of these advances in quantum theory and experiments, various companies are selling devices claimed to perform a quantum information task with no classical analog, such as quantum random number generators, prototypes of quantum computers, or quantum key distribution devices. Since quantum devices cannot be simulated classically, it is hard to verify them using only classical resources, which are the ones available to the average user. Hence, a natural question to ask ourselves is how we can verify the properties and functioning of quantum devices in an efficient way.

In this context, device-independent protocols have been developed in quantum information theory over the past decade. The main advantage of such protocols is that users do not have to make any assumption about the inner workings of their devices, considering them as black boxes. The security and success of a device-independent protocol relies on the observation of nonlocal correlations in a Bell experiment.

This thesis is dedicated to provide tools to achieve the certification of quantum information devices or tasks in a device-independent way.

In the first part of this thesis, we focus on certifying the security of device-independent quantum key distribution. To this end, we first study whether Bell nonlocality is a sufficient condition for security in the most used protocols, proving that there exist nonlocal correlations that are not useful for secure device-independent quantum key distribution using these protocols. Moreover, we study noisy scenarios, that is when experimental imperfections are present, and derive upper bounds on the two-way and one-way key rates for this kind of protocols.

In the second part, we study self-testing, which is one of the simplest device-independent protocols. Its goal is to recover quantum states solely from the observed measurement correlations. In the majority of quantum information processing tasks one needs to consider a particular quantum state, making the certification of quantum states of great importance in the device-independent paradigm. We prove that all multipartite states of qubits can be self-tested. Moreover, we study self-testing in higher-dimensional systems.

Finally, in the third part of this thesis, we tackle the problem of certification of entanglement. It is well known that certifying the presence of entanglement in a system is a hard task. The key methods for entanglement detection, entanglement witnesses and positive maps, rely on our understanding of the mathematical features of multilinear algebra. By using the fact that any separable state is one to one related to a matrix inequality, we port previously known results on the entanglement of states with positive partial transpose into the domain of matrix inequalities, which also allow us to translate multilinear positive maps back into entanglement witnesses. This approach leads to a unified treatment of a large class of matrix inequalities, allowing us to find new inequalities on the basis of advances in entanglement

theory.

Thursday September 12, 10:00 h. ICFO Auditorium and Online (Teams)
Thesis Director: Prof. Dr. Antonio Acin
Hosted by: Prof. Dr. Antonio Acin