

Congratulations to New ICFO PhD Graduate

Dr. Carlos Pascual graduated with a thesis entitled "Continuous Variable Quantum Communications: Technologies and Security"

April 07, 2025

We congratulate Dr. Carlos Pascual who defended his thesis this morning in ICFO's Auditorium.
Dr. Pascual obtained his MSc in Quantum Science and Technology from the UPV/EHU (University of the Basque Country), before joining the Quantum Information Theory research group led by ICREA professor at ICFO Dr. Antonio Acin. His thesis titled "Continuous Variabl Quantum Communications: Technologies and Security" was supervised by Prof. Dr. Antoni Acin and Dr. Stefan Bauml

ABSTRACT:

With this Thesis, we will focus on diverse technologies as well as techniques relevant for the development of secure communication systems based on Quantum Mechanics. This

theoretical analysis involves the application of diverse methodologies, which represent formidable challenges from a purely analytical perspective, as well as from a numerical stance. The contents of this manuscript are divided according to the nature of the particular technology under scrutiny.

As a first step, we will provide a study of Quantum Key Distribution based on continuous variable states and coarse-grained measurements. This inquiry is split according to two chapters. In the first one, a thorough description of our approach will be provided, as well as diverse outcomes regarding the addition of postselection techniques for an improved perfomance; a study of optimization in infinite dimensions, as well as results in the finite regime under collective attacks. In the second part, we will observe how performing a full discretization on the measurements grants not only full security against any adversary allowed by Quantum Mechanics, but also a new formalism via entropy accumulation approaches that permits the analysis of the statistical fluctuations that emerge when only finite statistics are accessible.

This discussion will be followed by a study of Quantum Random Number Generation according to a semi Device Independent perspective where the assumptions on the experimental setups are limited. Our discussion will be based on using a trusted measurement and imposing a bound on the corresponding expectation value -- which requires an adaption from the well-known asymptotic limit to the the finite case in order to prevent emerging security pitfalls. This examination is completed with a thorough security proof against general attacks and diverse results in the finite regime.

To conclude, this Thesis finishes with an assessment of Quantum Key Distribution for large networks based on classical Internet models, which provides insights on the scalability and optimality conditions of Quantum Communications according to the density of users and their connections. In particular, this indagation is mainly based on continuous variable systems, albeit another approach grounded on discrete variables is also added to the model in order to enhance its performance.

Thesis Committee:

Dr. Eleni Diamanti, Centre National de la Recherche Scientifique

Prof. Dr. Valerio Pruneri, ICFO

Assoc. Prof. Dr. Peter Brown, Telecom SudParis



Thesis Committee