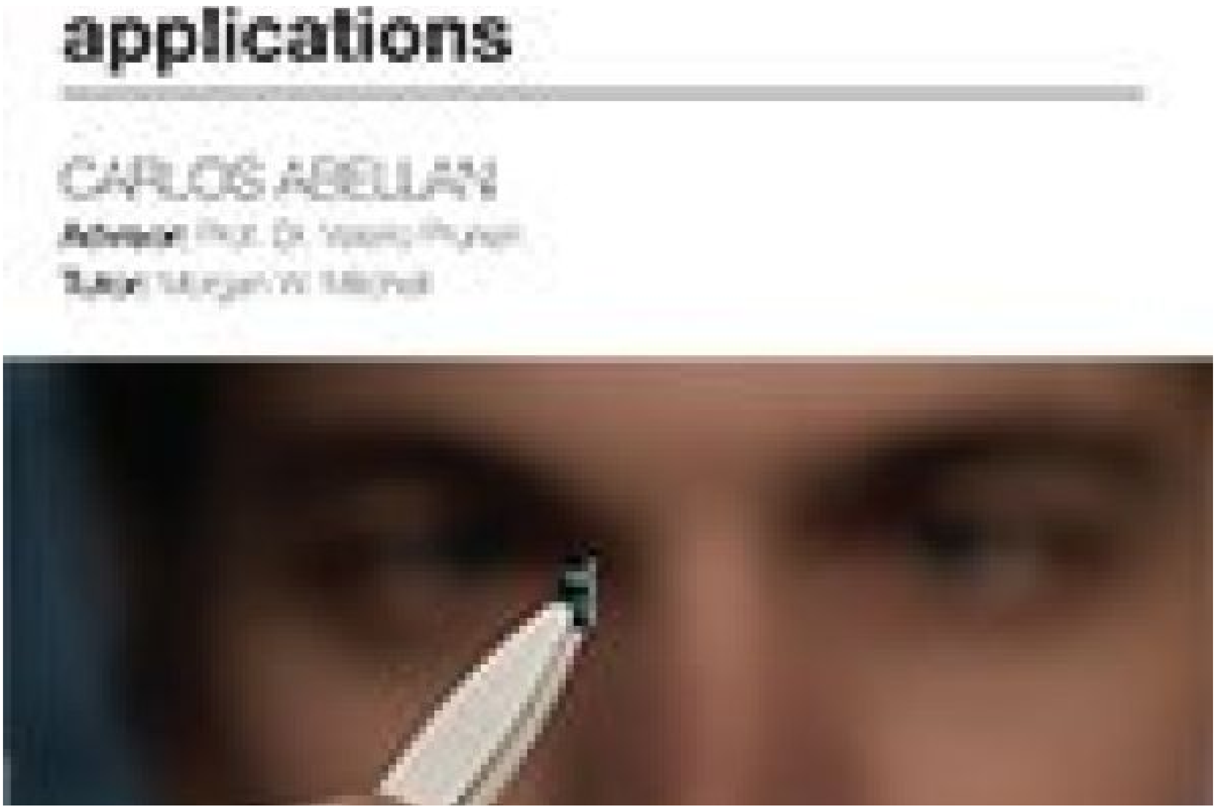
ICFO



PhD Thesis Defense CARLOS ABELLAN 'Quantum Random Number Generators for Industrial Applications'

CARLOS ABELLAN

June 19, 2018

Tuesday June 19, 15:00. ICFO Auditorium

CARLOS ABELLAN

Optoelectronics

ICFO-The Institute of Photonic Sciences

Randomness is one of the most intriguing, inspiring and debated topics in the history of the world. It appears every time we wonder about our existence, about the way we are, e.g. Do we have free will? Is evolution a result of chance? It is also present in any attempt to understand our anchoring to the universe, and about the rules behind the universe itself, e.g. Why are we here and when and why did all this start? Is the universe deterministic or does unpredictability exist? Remarkably, randomness also plays a central role in the information era and technology. Random digits are used in communication protocols like Ethernet, in search engines and in processing algorithms as page rank. Randomness is also widely used in so-called Monte Carlo methods in physics, biology, chemistry, finance and mathematics, as well as in many other disciplines. However, the most iconic use of random digits is found in cryptography. Random numbers are used to generate cryptographic keys, which are the most basic element to provide security and privacy to any form of secure communication.

This thesis has been carried out with the following questions in mind: Does randomness exist in photonics? If so, how do we mine it and how do we mine it in a massively scalable manner so that everyone can easily use it? Addressing these two questions lead us to combine tools from fundamental physics and engineering. The thesis starts with an in-depth study of the phase diffusion process in semiconductor lasers and its application to random number generation. In contrast to other physical processes based on deterministic laws of nature, the phase diffusion process has a pure quantum mechanical origin, and, as such, is an ideal source for generating truly unpredictable digits.

First, we experimentally demonstrated the fastest quantum random number generation scheme ever reported (at the time), using components from the telecommunications industry only. Up to 40 Gb/s were demonstrated to be possible using a pulsed scheme. We then moved towards building prototypes and testing them with partners in supercomputation and fundamental research. In particular, the devices developed during this thesis were used in the landmark loophole- free Bell test experiments of 2015. In the process of building the technology, we started a new research focus as an attempt to answer the following question: How do we know that the digits that we generate are really coming from the phase diffusion process that we trust? As a result, we introduced the randomness metrology methodology, which can be used to derive quantitative bounds on the quality of any physical random number generation device. Finally, we moved towards miniaturisation of the technology by leveraging techniques from the photonic integrated circuits technology industry. The first fully integrated quantum random number generator was demonstrated using a novel two-laser scheme on an Indium Phosphide platform. In addition, we also demonstrated the integration of part of the technology on a Silicon Photonics platform, opening the door towards manufacturing in the most advanced semiconductor industry.

Tuesday June 19, 15:00. ICFO Auditorium

Thesis Advisor: Prof Dr Valerio Pruneri