

A short introduction to Quantum Computing and Quantum Cryptography

Giannicola Scarpa
UCM (Matemáticas)

Facultad de Informática
Sala de Grados - miércoles 10 de abril de 2019 - 16:00
Entrada libre hasta completar el aforo

Resumen:

In the last decades, a new model of computation based on quantum mechanics has gained attention in the computer science community. We give an introduction to this model starting from the basics, with no prerequisites. Then, with the help of some simple examples, we see why quantum computers outperform standard ones in certain tasks. We then move to the topic of quantum entanglement and show how sharing quantum information can create a strong provable correlation among distant parties. With this basic understanding of quantum computation and quantum entanglement, we can already illustrate two interesting cryptographic protocols: quantum key distribution and position verification. Both perform classically impossible tasks: the first allows to detect an intruder intercepting a secret communication, while the second allows certifying somebody's GPS location.

Sobre Giannicola Scarpa:

Giannicola Scarpa is a researcher specialized in the theory of quantum information and computation. His main interests are using computer science tools to discover features of quantum mechanics, and using quantum mechanics to discover new tools in computer science. He holds a Master's degree in Informatics from the University of Salerno, Italy, with a thesis on quantum game theory supervised by Giuseppe Persiano. He obtained a PhD from the University of Amsterdam, the Netherlands, defending a thesis entitled "Quantum entanglement in non-local games, graph parameters and zero-error information theory". His advisor was Ronald de Wolf. He was post-doc in Andreas Winter's group at UAB in Barcelona, and he is now a post-doc with David Pérez-García at UCM.