POLITECNICO DI TORINO

PHOTONEXT

Seminars on Photonics organized by the PhotoNext Center

www.photonext.polito.it

Introduction to Quantum Cryptography: from the lab to the practical applications

Dr. Ivo Pietro Degiovanni - *INRIM, Torino, Italy*

Wednesday 27 April 2022 - 16:00 – 17:30 Classroom 8I

Telecom

Sensors

Components

Secure communications for personal, commercial and governmental use are fundamental to the way we live. Today, our cybersecurity infrastructure is based on the exchange and use of digital cryptographic keys. Recently, the perceived threat of the quantum computer to modern cryptographic standards in widespread use has increased dramatically. Government security agencies have called for a move to a quantum-safe cryptographic solution. The solution is a combination of algorithmic encryption aimed to be secure against a quantum computer (dubbed post-quantum cryptography), and quantum cryptography, more correctly referred to as quantum key distribution (QKD). QKD can distribute secret digital keys over optical links. Uniquely, it provides protocols whose security can be proven by the laws of nature, rather than computational complexity, and does not require assumptions about the resources available to an adversary. QKD was originated by the 1984 paper by Bennet and Brassard, but is no longer limited to research laboratories: QKD networks are under development worldwide. Commercial products and industrial prototypes for QKD are available from SMEs and large companies. Although QKD protocols can be proven unconditionally secure in theory, in practice any deviations of the real system from the idealised model could introduce vulnerabilities. The security of real systems requires physical characterisation and certification. Despite this strong industrial drive, the development of a certification infrastructure to support the widespread adoption and commercialisation of QKD has just begun. The establishment of standards will be key for addressing a global market and support the emergence of supply chains and quantum technology eco-systems. The aim of this lesson is briefly presenting the QKD idea and the status of the art of its practical implementations.

Dr. Ivo Pietro Degiovanni is Senior Researcher ("Primo Ricercatore") at Istituto Nazionale di Ricerca Metrologica (INRIM). He has developed his scientific competences in the fields of Quantum Metrology, Quantum Communication and Quantum Optics. Regarding quantum Communication, he has mainly worked on quantum cryptography and quantum communication, in the context of Italian, NATO and European projects. In particular, he has worked on metrology supporting quantum communication such as e.g. on single photon sources based on parametric down conversion, and color centers in (nano)diamonds, as well as single photon detectors calibration. He also has worked on several aspects on quantum optics ranging from quantum-enhanced measurement, to quantum sensors, to quantum imaging, to quantum state tomography, and state "quantumness" quantifiers. He has been the Chairman of the EURAMET European Metrology Network for Quantum Technologies (EMN-Q) since 2019, and he has served as a member of the Strategic Research Agenda Working Group (SRA-WG) of the EU Quantum Flagship (team: "Sensing and Metrology") since 2018. He is Associate Editor of the European Physical Journal D (EPJ D) and of the European Physical Journal Quantum Technology (EPJ QT). He is Lecturer of the course "Quantum Communication" at University of Torino (Torino Graduate School in Physics and Astrophysics), and he is the INRIM representative in the ETSI ISG-QKD (European Telecommunication Standard Institute – Industry Specification Group on Quantum Key Distribution).

For further information: info.photonext@polito.it