UNIVERSITÀ DEGLI STUDI DI TORINO

Dipartimento di Fisica

Seminar

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

Dr. Ivo Degiovanni

Istituto Nazionale di Ricerca Metrologica

Quantum Cryptography (Quantum Key Distribution)

Friday, May 14th h 14:00

WEBEX link:

https://unito.webex.com/unito/j.php?MTID=m7f874eda85a490966dd197fea9216c53

Secure communications are fundamental in the modern world. The actual cybersecurity infrastructure is based substantially on the public key cryptographic solution. 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, 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.

QKD originated from the 1984 paper by Bennet and Brassard, but is no longer limited to research laboratories: demonstrational QKD networks has been built in several places around the world. Although QKD protocols can be proven to be unconditionally secure in theory, the development of a certification infrastructure to support their widespread adoption and commercialisation 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 Seminar is presenting the QKD idea and the status of the art of its practical implementations.

UNIVERSITÀ DEGLI STUDI DI TORINO

Dipartimento di Fisica

The speaker

Dr Ivo Pietro Degiovanni is Senior Researcher at INRIM. He developed his scientific competences in the fields of Quantum Metrology with photons, Quantum Information and Quantum Optics (>90 co-authored ISI papers on these topics). He has been Project and/or INRIM Local Coordinator of several European and National research projects related to quantum (communication) technologies.

Since 2017 he has served as a member of the INRiM Scientific Governing Board, and of the Strategic Research Agenda Working Group (SRA-WG) of the EU Quantum Flagship (team: "Sensing and Metrology") since 2017.

He is the INRIM representative in the ETSI ISG-QKD (European Telecommunication Standard Institute – Industry Specification Group on Quantum Key Distribution).

He is contributor of the white-book on cybersecurity in Italy: "Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici Progetti e Azioni per difendere al meglio il Paese dagli attacchi informatici" published by Laboratorio Nazionale di Cybersecurity and CINI - Consorzio Interuniversitario Nazionale per l'Informatica (Roberto Baldoni, Rocco De Nicola, Paolo Prinetto Ed.s).

He is contributor of the ETSI White Paper No. 27: "Implementation Security of Quantum Cryptography; introduction, challenges, solutions" (First edition – July 2018 ISBN No. 979-10-92620-21-4) published by ETSI (European Telecommunications Standards Institute).