INSTITUTE
OF COMMUNICATION,
INFORMATION
AND PERCEPTION
TECHNOLOGIES

Sant'Anna
School of Advanced Studies – Pisa

HYBRID QUANTUM KEY DISTRIBUTION using coherent states and photon-number-resolving detectors

TeCIP Institute - Blue Room - 3 p.m.

6th June 2018

Stefano OLIVARES

Abstract:

Protocols for quantum key distribution (QKD) exploit the very laws of quantum mechanics to establish a shared secret key between two (or more) parties. In this lecture, we briefly review some basic elements of quantum optics and their application to continuous-variable QKD protocols based on Gaussian modulation of coherent fields and homodyne detection. Then, we present a hybrid QKD protocol where we still use a modulation of coherent states, but the detection stage is replaced by photon-number-resolving (PNR) detectors. Since our scheme exploits both the wave-like properties (amplitude and phase) of the signals together with a detection stage that highlights the particle-like nature of the radiation, we refer to this protocol as "hybrid". When reverse reconciliation is considered, the hybrid scheme outperforms the homodyne one both for individual and collective attacks. In the presence of direct reconciliation, the PNR strategy turns out to be the best one against individual attacks, but, for the collective ones, the homodyne-based scheme is still to be preferred as the channel transmissivity decreases.

Short bio:

Stefano Olivares received the Ph.D. degree in physics from the University of Milan and is currently Assistant professor at the Department of Physics, University of Milan, Italy. He is a theoretician and works in quantum optics and quantum information and communication with emphasis on the optical implementation of quantum information processing. Although his research activity is mainly theoretical, he is an active collaborator in many experimental groups