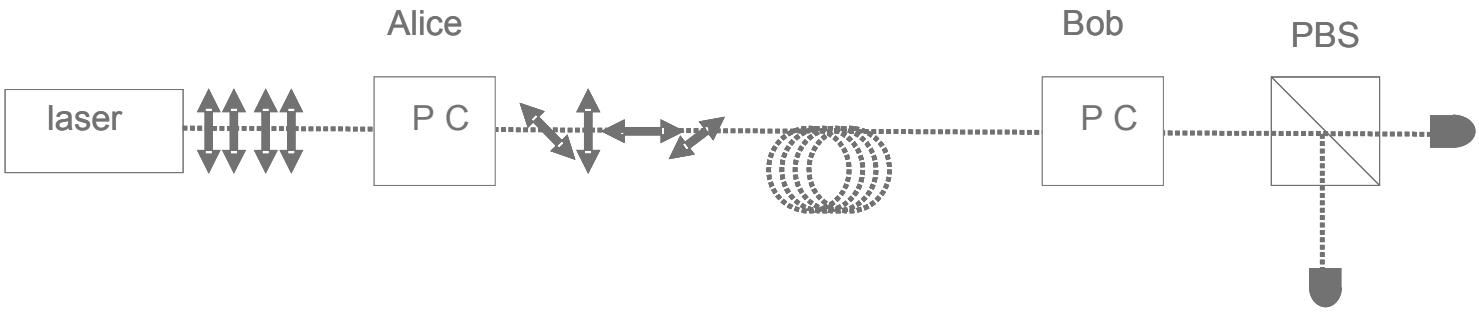
From Classical to Quantum Cryptography



Lecturer

Stefano Mancini
Università Camerino

21-22 February, 2019

Sala Verde
10:30-12:30

Abstract

Information science is undergoing a quantum revolution and cryptography is the cutting edge of this revolution.
There, quantum key distribution solves the longstanding problem of distributing random sequence of bits between authorized users with unconditionally (information-theoretic) security. Eavesdropper's attack is in fact bounded by fundamental laws of quantum physics: any information gained by it disturbs the quantum channel between the legitimate users.
However, all that glitters is not gold. In fact, it is exactly quantum features, like entanglement, that prevent the security of other important cryptographic primitives like the bit commitment.

I will review these concepts (from an information theoretic perspective) by addressing in sequence: Classical cryptosystems (Vernam and Public key); Quantum key distribution protocols (BB84, B92, E91); Quantum security (Quantum entropy and uncertainty relation, Privacy, Key rate); Quantum bit commitment.