CLASSICAL AUTHENTICATION IN QUANTUM KEY DISTRIBUTION

Edoardo Signorini

Telsy

Quantum Key Distribution (QKD) is a family of key exchange protocols that base their security on the principles of quantum mechanics. It constitutes a possible response to the quantum computer threat to cryptography and its security is supposed to be inviolable even against an attacker with unlimited computing power. Although QKD is often described in the domain of physics, its realization requires the integration with purely "classical" components of cryptographic and information theory. In particular, it is known that in the absence of an authenticated classic channel, the QKD cannot be performed securely. Ignoring or misinterpreting this aspect is likely to weaken the security of the protocol or to reduce it to a computational form, therefore no better than the completely classic counterparts. In this talk, we will briefly describe QKD and its components, introduce unconditionally secure authentication schemes and analyze their use in combination with QKD protocols. Finally, we will focus on recent literature findings and discuss the risk of possible gaps with commercial implementations.