Plenary Talk PV XIII Thu 9:15 B Audimax

Device-independent quantum cryptography — •Renato Renner — ETH Zurich, Switzerland

Quantum cryptography provides, in principle, perfect security, based solely on the correctness of physical laws. Nevertheless, recent successful hacking attacks have revealed that such strong security is not warranted by actual implementations. This mismatch between theory and practice is due to a fundamental incompleteness of models for real-world devices such as photon sources and detectors.

A clean and elegant approach to overcome this problem is "device-independent" quantum cryptography. The idea is to establish security claims that hold independently of the details of the devices used for their implementation. This is achieved by the use of techniques originally proposed for experiments on the foundations of quantum theory, such as loophole-free Bell tests.