MAR13-2012-020749

Abstract for an Invited Paper
for the MAR13 Meeting of
the American Physical Society

Fully device-independent quantum key distribution

THOMAS VIDICK, Massachusetts Institute of Technology (MIT)

The laws of quantum mechanics allow unconditionally secure key distribution protocols. Nevertheless, security proofs of traditional quantum key distribution (QKD) protocols rely on a crucial assumption, the trustworthiness of the quantum devices used in the protocol. In device-independent QKD, even this last assumption is relaxed: the devices used in the protocol may have been adversarially prepared, and there is no a priori guarantee that they perform according to specification. Proving security in this setting had been a central open problem in quantum cryptography. We give the first device-independent proof of security of a protocol for quantum key distribution that guarantees the extraction of a linear amount of key even when the devices are subject to a constant rate of noise. Our only assumptions are that the laboratories in which each party holds his or her own device are spatially isolated, and that both devices, as well as the eavesdropper, are bound by the laws of quantum mechanics. All previous proofs of security relied either on the use of many independent pairs of devices, or on the absence of noise.