Fully device independent quantum key distribution

Sun, 2015-04-05 15:26 - admin
U. Vazirani, T. Vidick
Phys. Rev. Lett. 113, 140501 (2014)

Although quantum key distribution (QKD) is one of the major achievements of quantum information science, its security proofs rely on certain assumptions on the devices used in the protocol. To overcome this serious limitation, device-independent QKD (DIQKD) has been developed as a method to guarantee security even in the case the devices are uncharacterized. Much effort has been devoted in devising DIQKD protocols that extract an amount of key that is linear in the number of uses of the devices, which are secure against increasingly general eavesdropping strategies and are robust to the presence of noise. However, the best known protocols were either based on the assumption that the devices had no internal memory or were polynomially inefficient and unable to tolerate noisy devices. This raised an essential question: is device- independent QKD even possible without independence assumptions in a realistic, noise-tolerant scenario?

In their work, Vazirani and Vidick give a positive answer to this important question. They provide the first complete device-independent proof of security of quantum key distribution that tolerates a constant noise rate and guarantees the generation of a linear amount of key.

- FP7
- QUTE-EUROPE
- Work Package 2
- Highlight
- Quantum Information Theory

Source URL: http://qurope.eu/content/fully-device-independent-quantum-key-distribution