

Title: Quantum cryptography with finite resources: Unconditional security bound for discrete variable protocols with one-way postprocessing

Authors: V. Scarani (CQT and Dept Phys, NUS) and R. Renner (ETH Zurich)

Ref: Phys. Rev. Lett.100, 200501 (2008)

Publicity LH11007

QUANTUM CRYPTOGRAPHY IS POSSIBLE WITH FINITE RESOURCES (FORTUNATELY)

The possibility of using quantum physics for secret communication has been noticed more than 20 years ago. "Quantum cryptography" has since been implemented, first in physics laboratories, then in the first commercial devices. In parallel, theoretical tools have been developed to assess the security of these systems in a rigorous way. These, however, are generally only applicable under the (unrealistic) assumption that the cryptographic system runs for an infinite time, thereby exchanging an infinite amount of communication. In this letter, we propose a general method that allows to take into account finite-size effects.

In particular, we prove that a significant amount of bits (approximately 1 million) must be exchanged before any security at all can be guaranteed. Had this value been much larger, quantum cryptography would have been impossible in practice; had it been much smaller, the concern for finite communication would have been proved pointless in practice. As things stand, quantum cryptography can be made secure in practice, but only provided a finite-communication bound like ours is used instead of the usual asymptotic bounds.