MAR13-2012-004201

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

**Security of continuous-variable quantum key distribution against general attacks**[1]

ANTHONY LEVERRIER, INRIA Rocquencourt

We prove the security of Gaussian continuous-variable quantum key distribution with coherent states against arbitrary attacks in the finite-size regime. In contrast to previously known proofs of principle (based on the de Finetti theorem), our result is applicable in the practically relevant finite-size regime. This is achieved using a novel proof approach, which exploits phase-space symmetries of the protocols as well as the postselection technique introduced by Christandl, Koenig and Renner (*Phys. Rev. Lett.* 102, 020504 (2009)).

[1]This work was supported by the SNF through the National Centre of Competence in Research "Quantum Science and Technology" and through Grant No. 200020-135048, the ERC (grant No. 258932), the Humbolt foundation and the F.R.S.-FNRS under project HIPERCOM.