

## Finite-key analysis for practical implementations of quantum key distribution

Raymond Y Q Cai and Valerio Scarani<sup>1</sup>

Centre for Quantum Technologies and Department of Physics,  
National University of Singapore, Singapore  
E-mail: [physv@nus.edu.sg](mailto:physv@nus.edu.sg)

*New Journal of Physics* **11** (2009) 045024 (20pp)

Received 24 November 2008

Published 30 April 2009

Online at <http://www.njp.org/>

doi:10.1088/1367-2630/11/4/045024

**Abstract.** The lists of bits processed in quantum key distribution are necessarily of finite length. The need for finite-key unconditional security bounds was recognized long ago, but the theoretical tools have become available only very recently. We provide finite-key unconditional security bounds for two practical implementations of the Bennett–Brassard 1984 coding: prepare-and-measure implementations without decoy states and entanglement-based implementations. A finite-key bound for prepare-and-measure implementations with decoy states is also derived under a simplified treatment of the statistical fluctuations. The presentation is tailored to allow direct application of the bounds in experiments. Finally, the bounds are also evaluated on *a priori* reasonable expected values of the observed parameters.

<sup>1</sup> Author to whom any correspondence should be addressed.