Quantum Physics

Upper bounds for the secure key rate of decoy state quantum key distribution

Marcos Curty, Tobias Moroder, Xiongfeng Ma, Hoi-Kwong Lo, Norbert Lütkenhaus

(Submitted on 29 Jan 2009)

The use of decoy states in quantum key distribution (QKD) has provided a method for substantially increasing the secret key rate and distance that can be covered by QKD protocols with practical signals. The security analysis of these schemes, however, leaves open the possibility that the development of better proof techniques, or better classical post-processing methods, might further improve their performance in realistic scenarios. In this paper, we derive upper bounds on the secure key rate for decoy state QKD. These bounds are based basically only on the classical correlations established by the legitimate users during the quantum communication phase of the protocol. The only assumption about the possible post-processing methods is that double click events are randomly assigned to single click events. Further we consider only secure key rates based on the uncalibrated device scenario which assigns imperfections such as detection inefficiency to the eavesdropper. Our analysis relies on two preconditions for secure two-way and one-way QKD: The legitimate users need to prove that there exists no separable state (in the case of two-way QKD), or that there exists no quantum state having a symmetric extension (one-way QKD), that is compatible with the available measurements results. Both criteria have been previously applied to evaluate single-photon implementations of QKD. Here we use them to investigate a realistic source of weak coherent pulses. The resulting upper bounds can be formulated as a convex optimization problem known as a semidefinite program which can be efficiently solved. For the standard four-state QKD protocol, they are quite close to known lower bounds, thus showing that there are clear limits to the further improvement of classical post-processing techniques in decoy state QKD.

Comments:	10 pages, 3 figures
Subjects:	**Quantum Physics (quant-ph)**
Journal reference:	Phys. Rev. A 79, 032335 (2009)
DOI:	10.1103/PhysRevA.79.032335
Cite as:	**arXiv:0901.4669v1 [quant-ph]**

Submission history

From: Marcos Curty [view email]
[v1] Thu, 29 Jan 2009 12:56:55 GMT (44kb)

Which authors of this paper are endorsers?