Quantum Physics

Multi-mode states in decoy-based quantum key distribution protocols

Wolfram Helwig, Wolfgang Mauerer, Christine Silberhorn

(Submitted on 29 Jan 2009)

Every security analysis of quantum key distribution (QKD) relies on a faithful modeling of the employed quantum states. Many photon sources, like for instance a parametric down conversion (PDC) source, require a multi-mode description, but are usually only considered in a single-mode representation. In general, the important claim in decoy-based QKD protocols for indistinguishability between signal and decoy states does not hold for all sources. We derive new bounds on the single photon transmission probability and error rate for multi-mode states, and apply these bounds to the output state of a PDC source. We observe two opposing effects on the secure key rate. First, the multi-mode structure of the state gives rise to a new attack that decreases the key rate. Second, more contributing modes change the photon number distribution from a thermal towards a Poissonian distribution, which increases the key rate.

Subjects: **Quantum Physics (quant-ph)**
Cite as: **arXiv:0901.4695v1 [quant-ph]**

Submission history

From: Wolfgang Mauerer [view email]
[v1] Thu, 29 Jan 2009 14:49:08 GMT (62kb,D)

Which authors of this paper are endorsers?