

Title:

Implementation of an attack scheme on a practical QKD system

Abstract:

The stated goal of quantum key distribution (QKD) is to grow a secret key securely between two parties with a minimum of additional assumptions. The number of assumptions has been continuously reduced, from requiring the validity of quantum mechanics in early QKD, to more general constraints on the laws of physics in device-independent QKD.

Despite steady theoretical progress in dealing with known limitations of current technology, in practice the security of QKD relies not only on the quantum protocol but on the physical implementation. We demonstrated a full implementation of an eavesdropper attacking an established QKD connection. The eavesdropper obtains the complete 'secret' key, while none of the results measured by the legitimate parties indicate a breach in security. This confirms that non-idealities in physical implementations of QKD can be fully exploitable.

Authors:

Ilja Gerhardt

<http://lanl.arxiv.org/find/quant-ph/1/au:+Gerhardt_I/0/1/0/all/0/1>,

Qin Liu <http://lanl.arxiv.org/find/quant-ph/1/au:+Liu_Q/0/1/0/all/0/1>,

Vadim Makarov

<http://lanl.arxiv.org/find/quant-ph/1/au:+Makarov_V/0/1/0/all/0/1>,

Johannes Skaar

<http://lanl.arxiv.org/find/quant-ph/1/au:+Skaar_J/0/1/0/all/0/1>,

Valerio Scarani, Antia Lamas-Linares

<http://lanl.arxiv.org/find/quant-ph/1/au:+Lamas_Linares_A/0/1/0/all/0/1>,

Christian Kurtsiefer

<http://lanl.arxiv.org/find/quant-ph/1/au:+Kurtsiefer_C/0/1/0/all/0/1>

arXiv references:

arXiv:1011.0105 <<http://lanl.arxiv.org/abs/1011.0105>>,

arXiv:0906.4547 <<http://lanl.arxiv.org/abs/0906.4547>>