Are quantum key distribution systems really useful (in practice)?

Hoi-Kwong Lo
Dept. of ECE and Dept. of Physics,
10 King's College Road,
University of Toronto, Toronto, ON Canada, M5S 3G4
hklo@comm.utoronto.ca

Abstract

I discuss some challenges to the widespread deployment of quantum key distribution (QKD) systems. First, I present our recent successful quantum hacking experiment by time-shfit attack against a commercial QKD system [1], thus highlighting the importance of the study of quantum hacking and its counter-measures. Second, I mention our recent security proof of QKD with an unknown and untrusted source [2]. Finally, we recall that the initial shipment of QKD systems requires a trusted courier. So, QKD must compete with the trusted courier solution (who instead ships a large hard-drive containing a one-time-pad) in, for example, speed. This means that we need high-speed QKD.

References

1. Y. Zhao et al., , http://arxiv.org/abs/0704.3253
2. Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A, 77, 052327 (2008), also available on-line http://arxiv.org/abs/0802.2725