Device-independent Secret Key Rates for Quantum Repeater Setups

Timo Holz, Hermann Kampermann, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-University, D-40225 Duesseldorf, Germany

July 7, 2016

Quantum key distribution (QKD) is a central task in quantum cryptography. To achieve a secure distribution of a key between two or more parties, it is desirable to not trust any device involved in the QKD-protocol. This is due to the fact that the complete characterisation of the apparatuses for measurement and state preparation is very difficult, if not impossible. In the device-independent approach, one relies solely on fundamental assumptions, namely that the laws of quantum mechanics hold true and that every involved party works in an isolated laboratory, meaning that there is no uncontrolled leakage of information to the environment during the QKD-process. In particular one drops the assumption of having perfect control over the devices.
The figure of merit in QKD is the secret key rate R, given by the product of the raw key R_{raw} and the secret fraction r. The possibility of generating a secure key from the measurement results crucially relies on the violation of some Bell-inequality. Depending on this violation, one can impose a lower bound on the achievable secret fraction in the device-independent scenario [1]. With h, Q and S denoting the binary entropy, the quantum bit error rate between the two parties and the violation of the CHSH-inequality, respectively, the bound is given by $r \geq 1 - h\big(Q\big) - h\big(\big(1+\sqrt{(S/2)^2-1}\big)/2\big)$. However, there exist other device-independent QKD-protocols (e.g. [2]) with different lower bounds on the secret fraction, which we also investigate.
Entanglement is the main resource of secure quantum communication. Unfortunately, photon losses scale exponentially with the length of the fiber, making it impossible to reliably distribute entangled photon pairs among two distant parties. To extend the distance one can use quantum repeaters. We study achievable secret key rates in the device-independent bipartite case for different quantum repeater setups and compare them to the device-dependent case [3]. The quantum repeater protocols under consideration are the original protocol by Briegel *et al.* [4], the hybrid quantum repeater protocol by van Loock *et al.* [5] and the Duan-Lukin-Cirac-Zoller-setup based on atomic ensembles and linear optics [6]. The secret key rate R is an explicit function of the used protocol. A variety of parameters, such as gate quality, detector efficiency or the purity of initially distributed states have an impact on the achievable key rate. We optimize the strategy in order to maximize the secret key rate.
Finally, we also consider device-independent quantum cryptography in the multipartite case, with the graph state repeater setup by Epping *et al.* [7]. Motivated by the methods of the bipartite case, we investigate the possibility to connect the violation of an appropriate inequality with the achievable secret key rate.

Reference

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007)
[2] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014)
[3] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Phy. Rev. A **87**,052315 (2013)
[4] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998)
[5] P. van Loock, T.D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W.J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006)
[6] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001)
[7] M. Epping, H. Kampermann, and D. Bruß, New J. Phys. **18**, 053036 (2016)