Secure key rate improvement methods in DI-QKD protocols

Maryam Afsary
Morteza Moradi, Magdalena Stobińska

Institute of Informatics, Faculty of Mathematics, Informatics and Mechanics, University of Warsaw, Banacha 2c, 02--097 Warsaw, Poland

m.afsary@uw.edu.pl

Abstract

Secure communication is of paramount importance in various fields, ranging from government and military to financial and healthcare. Quantum Key Distribution (QKD) leverages the unique properties of quantum mechanics to offer a promising solution. In conventional QKD protocols, the security relies on the specific implementation of the devices used by the legitimate parties. However, device-independent QKD (DI-QKD) protocols offer a more robust security guarantee by eliminating the need for trusted devices. DI-QKD protocols are based on the violation of Bell inequalities, which ensures security against any eavesdropping attempt, irrespective of the devices employed.

Two key factors in any QKD protocol are the distance over which secure keys can be distributed and the rate at which keys can be generated. The distance is limited by the attenuation of quantum signals, while the key rate is affected by various factors, including the channel noise and the efficiency of the detector. On the other side, by optimizing the post-processing stage, we can improve the key rate and distance of existing protocols, making DI-QKD more practical for real-world applications. These techniques involve manipulating the raw data generated by the protocol to extract a secure key, like what happens in post-selection [1] and noisy pre-processing [2].

In this work, we employed post-processing techniques to improve key rate in the DI-QKD protocol based on photon number counting [3]. We investigate three different methods to fulfill this goal.

In the first method, we leverage the CHSH inequality to calculate an analytical lower bound on the key rate[4], reaching approximately to 0.71 for the specified protocol. While simple, this method often underestimates the full existing correlations. To improve the results, we explore other methods. A more sophisticated approach numerically calculates a reachable lower bound on the key rate by considering conditional von Neumann entropy [5]. It significantly improves the rate to around 0.95, demonstrating substantial potential. However, this method may not always be feasible depending on numeric complexity, requiring alternative approaches in such cases. This method focuses on the entire raw key statistics to establish a lower bound on the key rate based on Eve's guessing probability. While the obtained rate of 0.93 is slightly lower than the numerical method, this approach guarantees its validity regardless of the parameters. Both numerical methods employed optimization techniques such as the NPA hierarchy and Semidefinite Programming (SDP) to further refine the results.

Overall, our analysis demonstrates that post-processing techniques can significantly boost the key rate of the photon-counting DI-QKD protocol. Each method offers distinct advantages and drawbacks, allowing researchers to choose the most suitable approach depending on their specific needs and priorities.

References

[1] F. Xu, Y. Zhang, Q. Zhang, and J. Pan, PRL, 128 (2022) 110506
[2] M. Ho, P. Sekatski, E. Tan, R. Renner, J. Bancal, and N. Sangouard, PRL, 124 (2020) 230502
[3] M. Mycroft, T. McDermott, A. Buraczewski, and M. Stobińska, PRA, 107 (2023) 012607
[4] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, V. Scarani, New Journal of Physics, 11 (2009) 045021
[5] P. Brown, H. Fawzi, and O. Fawzi, arXiv preprint arXiv:2106.13692 (2021)