Enhancing free space DI QKD via employing NPA hierarchy method

Magdalena Stobinska
Morteza Moradi, Maryam Afsary

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

mstobinska@mimuw.edu.pl

Introduction. Recently, there has been a growing focus on quantum communication due to its inherent security advantages [1,2]. However, there are still many challenges that need to be addressed, such as the distribution of entangled states over long distances, closing the Bell test loopholes, and increasing the key rate [3]. In this work, we present an innovative device-independent quantum key distribution (DI-QKD) protocol based on the distribution of near-maximally entangled multiphoton states across long distances. Our proposed strategy employs the resources available within the current landscape of integrated quantum photonic technology, including the utilization of squeezed vacuum states and photon-number-resolving detectors. Besides, this protocol enables entanglement sharing and quantum communication in free space.

Entanglement distribution. The distributed state using multi-photon bipartite entanglement is the Generalized Holland-Burnett (GHB) states, while the losses are due to quantum optical systems modelled with beam splitters [3].
Alice and Bob locally generate a photon-number-entangled two-mode squeezed vacuum state each, obtained by spontaneous parametric down-conversion (SPDC). They send their idler modes to a remote station Charlie, who holds a balanced beam splitter (BS), where the two modes interfere, and performs a photon-number-resolving (PNR) detection on the BS output modes. The state and the amount of shared entanglement are parametrized by the outcomes of Charlie's measurement. After Charlie informs the parties classically of the measurement outcome, Alice and Bob know which state they possess and may employ it for quantum applications.

Key generation and extraction. Alice and Bob interfere their signal with the coherent states. To this end, they use variable beam splitters. Alice repeatedly chooses between three coherent states as her setting while Bob uses two. In the homodyne limit, this setup allows them to perform a displacement operator on their modes. They interpret the readout obtained with photon-number-resolved (PNR) detectors as binary outcomes.

Alice and Bob apply post-selection on their key generation rounds in which they randomly and independently retain bits "0" with probability p and keep all bits "1". Then, they announce the discarded rounds through an authenticated classical channel.

Finally, they apply error correction and privacy amplification procedures. To find the key rate using the Devetak-Winter formula, they need to calculate their conditional entropy and maximize Eve's guessing probability based on the full behaviour of their statistics. This can be done by certifying quantum correlations leveraging SDP (i.e. NPA hierarchy method [4]).

References

[1] Ch. Portmann and Renato Renner, Reviews of Modern Physics 94 (2022) 025008.
[2] A. Acín et al., Physical Review Letters 98 (2007) 230501.
[3] M. Mycroft et al., Physical Review A 107 (2023) 012607.
[4] M. Navascués, S. Pironio, and A. Acín, New Journal of Physics 10 (2008) 073013.