Role of syndrome information on a one-way quantum repeater using teleportation-based error correction

Ryo Namiki and Norbert Lütkenhaus
Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo ON, Canada N2L 3G1

We investigate a quantum repeater scheme for QKD based on the work by Muralidharan *et al.,* Phys. Rev. Lett. 112, 250501 (2014). Our scheme extends that work by making use of error syndrom measurement results available at the repeater stations. We calculate the increase of key rate and show that these key rates surpass the Takeoka-Guha-Wilde bound on secret key rates of direct transmission over lossy bosonic channels.

Recently, an approach to establish a long distance entanglement by using middle stations and one-way classical communication has been proposed [1]. It employs a teleportation-based error correction (TEC) protocol within the stations and potentially gives a higher quantum key generation rate compared with the other quantum repeater protocols. In this scheme, the syndrome information of each middle stations is available for optimizing the key rate. However, the analysis in [1] is based on the key rate with a set of averaged success probability and error rates of TEC. This implies subsets of syndrome events are averaged out and some of useful information is discarded. Hence, the key generation rate would increase when we keep the syndrome information instead of coarse graining the success and error distributions. In this poster, we show how much the key rate increases by using the syndrome information in the one-way quantum communication scheme.

To explore the possibility of quantum communication schemes over a long distance, an essential question is whether the key generation with a use of middle stations could be better than *any* key generation scheme without middle stations. A clear criterion for this is to surpass Takeoka-Guha-Wilde (TGW) bound [2], which determines an upper bound of the secret key rate over pure lossy channels, hence, an ideal key generation without middle stations. As a no-go theorem on a type of middle stations, untamed Gaussian operations have been shown to be useless to beat TGW bound [3]. Thereby, it is natural to ask what type of structure for middle stations are sufficient to overcome TGW bound. We will address this question by showing a parametric regime where our key rate (per use of the channel) becomes higher than TGW bound.

[1] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).
[2] M. Takeoka, S. Guha, and M. Wilde, IEEE Trans. Inf. Theory **60**, 4987 (2013).
[3] R. Namiki, O. Gittsovich, S. Guha, and N. Lütkenhaus, Phys. Rev. A **90**, 062316 (2014).