Unconstrained capacities of quantum key distribution and entanglement distillation for pure-loss bosonic broadcast channels

Masahiro Takeoka[1], Kaushik P. Seshadreesan[2], Mark M. Wilde[3],
[1] *National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan*
[2] *Max Planck Institute for the Science of Light, Erlangen 91058, Germany*
[3] *Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, and Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA*

Quantum key distribution (QKD) and entanglement distillation (ED) are two cornerstones of quantum communication. Not only have there been theoretical developments, but also quantum communication technologies have been emerged rapidly in last decades. In particular, QKD has been available commercially and now is expanded to real-world networks, which consists of *point-to-point* QKD links and trusted nodes.

One important direction is to go beyond point-to-point links and make use of single-hop network channel. Single-hop network channels includes a quantum broadcast channel (single-sender and multiple-receiver) and a multiple access channel (multi-sender and single-receiver) for example. In fact, the QKD operation in the latter fiber network has been recently experimentally demonstrated [1], where the link between each sender and receiver is essentially point-to-point quantum communication and multiple users share the channel, each having a given amount of time to use it. This *time-sharing* protocol has a strong limit on the rate of key that can be generated among the parties. Then a natural question arises. Is this a fundamental trade-off limit or can we do better than the time-sharing limit?

In this paper, we answer this question affirmatively by establishing the unconstrained capacity region of a pure-loss bosonic broadcast channel, when used for the distillation of bipartite entanglement and secret key between the sender A and each receiver B_i $(i = 1, \ldots m)$, along with the assistance of unlimited local operations and classical communication (LOCC) [2]. Let $\{\eta_{B_1}, \ldots \eta_{B_m}\}$ be a set of power transmittances of the pure-loss broadcast channel from the sender to the respective receivers. Each η_{B_i} is non-negative and $\sum_{i=1}^{m} \eta_{B_i} \leq 1$. Let $\mathcal{B} = \{B_1, \ldots, B_m\}$, let $\mathcal{T} \subseteq \mathcal{B}$, and let $\overline{\mathcal{T}}$ denote the complement of the set $\mathcal{T}$. Our main result is as follows [2]:

Theorem 1: The LOCC-assisted unconstrained capacity region of the 1-to-m pure-loss bosonic broadcast channel is given by

$$\sum_{B_i \in \mathcal{T}} E_{AB_i} + K_{AB_i} \leq \log_2([1 - \eta_{\overline{\mathcal{T}}}]/[1 - \eta_{\mathcal{B}}]) , \qquad (1)$$

for all non-empty $\mathcal{T} \subseteq \mathcal{B}$, where E_{AB_i} and K_{AB_i} are the entanglement and key rates, respectively, $\eta_{\mathcal{B}} = \sum_{i=1}^{m} \eta_{B_i}$ and $\eta_{\overline{\mathcal{T}}} = \sum_{B_i \in \overline{\mathcal{T}}} \eta_{B_i}$.

Figure 1(a) plots a typical capacity region of ED in the 1-to-2 broadcast channel with sender A and receivers B and C, which is compared with the time sharing of the optimal point-to-point protocol. The capacity clearly outperforms time sharing even on the axes. This rate gain originates from the fact that in the optimal strategy, the third party helps the distillation between the other two [2]. This rate gap is more pronounced when we extend this to the m-receiver scenario. Figure 1(b) compares the sum of the rates in the 1-to-m symmetric pure-loss channel with transmittance η/m for each receiver. The plots show a huge gap between the capacity and the time sharing strategy. Finally, we do not leave this result as a purely theoretical development, but we also consider an example of the broadcast QKD protocol by extending the point-to-point protocol proposed in [3] and show that it overcomes the limit by simple point-to-point protocols for an optical broadcast channel (see [2] for the technical details). This is an important step toward the opening of a new framework of network channel-based quantum communication technology.

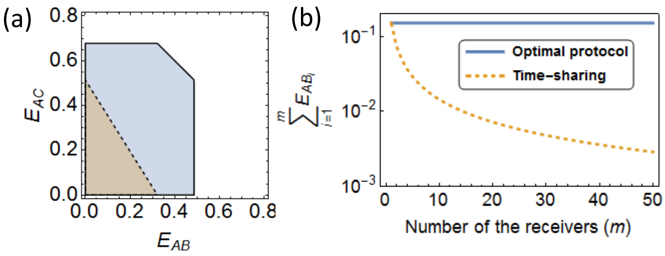

FIG. 1: (a) Comparison of the LOCC-assisted capacity (solid line) and the time sharing of the point-to-point capacity (dashed line) for the 1-to-2 pure-loss broadcast channel with $(\eta_B, \eta_C) = (0.2, 0.3)$. (b) Rate sum comparison for the capacity (optimal protocol) and the time sharing in the 1-to-m pure-loss broadcast channel with $\eta = 0.1$.

[1] B. Fröhlich *et al.*, Nature 501, 69 (2013).
[2] M. Takeoka, K. P. Seshadreesan, and M. M. Wilde, arXiv:1706.06746.
[3] R. García-Patón and N. Cerf, Phys. Rev. Lett. 102, 130501 (2009).