Bounds on entanglement distillation and secret key agreement for quantum broadcast channels

Kaushik P. Seshadreesan Masahiro Takeoka Mark M. Wilde

Abstract

The squashed entanglement of a quantum channel finds application as an upper bound on the rate at which secret key and entanglement can be generated when using the quantum channel a large number of times in addition to unlimited classical communication. This quantity has led to an upper bound of $\log((1+\eta)/(1-\eta))$ on the capacity of an optical communication channel for such a task, where η is the average fraction of photons that make it from the input to the output of the channel. In this work, we go beyond the single-sender single-receiver setting and consider a more general scenario involving a quantum broadcast channel between a single sender and multiple receivers. We establish constraints on the rates at which secret key and entanglement can be generated between any subset of the users of such a channel. We do so by employing multipartite generalizations of the squashed entanglement, while along the way developing several new properties of these measures. We apply our results to the case of an optical broadcast channel with one sender and two receivers, and characterize the rate-loss tradeoffs for such a channel.

Background. Quantum mechanics enables both unconditionally secure classical communication as well as faithful quantum communication. The former is made possible by quantum key distribution (QKD) and direct communication via the one-time pad protocol. On the other hand, the latter can be achieved with the help of shared entanglement and classical communication via the quantum teleportation protocol. A general paradigm for generating unconditionally secure secret key in a QKD protocol involves the distillation of the so-called "private states" [2] under unlimited local operations and classical communication (LOCC). Likewise, the most general paradigm for generating shared entanglement is to distill maximally entangled states under unlimited LOCC. The fact that both entanglement distillation and secret-key agreement can be accomplished most generally under the umbrella of LOCC allows for a combined treatment of the two tasks.

Over the years, various optical QKD systems have been developed and implemented, and their security proven. Unfortunately, practical implementations of optical QKD are known to suffer from a rate-loss tradeoff that forces the key distillation rates to decay exponentially with the distance of communication. Recently, this fact was established as a fundamental limitation of the optical communication channel using the squashed entanglement of a channel, which is an upper bound for the entanglement distillation capacity and secret key agreement capacity of a channel [4]. The squashed entanglement upper bound, when evaluated for a pure-loss bosonic point-to-point channel, was shown to be solely a function of the loss parameter of the channel, independent of the transmitted power. Further, the upper bound was shown to be nearly optimal at high loss and to match the rates achieved in current state-of-the-art QKD systems, thereby asserting that no yet-to-be-discovered protocol for QKD could perform any better than the current QKD systems. This development has firmly established the need for quantum repeater technology, which would enable relaying quantum states over long distances, and thereby aid in circumventing the rate-loss tradeoff.

Motivation. One of the main long-term goals of quantum communication and cryptography is to establish quantum networks, which enable secure classical communication as well as the sharing of entanglement between multiple users for various quantum information processing applications. While

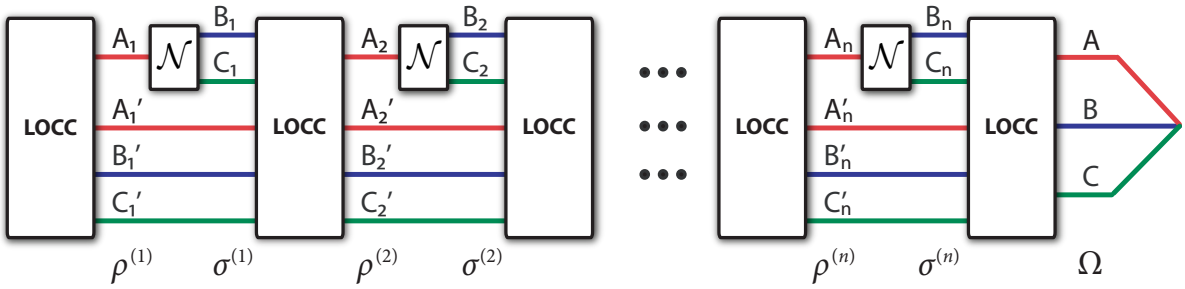

Figure 1: A general protocol for entanglement distillation and secret key agreement using LOCC and a quantum broadcast channel $\mathcal{N}_{A\to BC}$ with one sender and two receivers. The protocol uses the channel n times, and the primed registers represent "scratch" registers that each party uses for local processing. The state Ω_{ABC} at the end is ε-close in trace distance to the ideal state which is a tensor product of maximally entangled states and private states on systems shared between all possible subsets of the three users of the channel.

point-to-point channels certainly are the preferred architecture to establish long distance links in the networks, they are not so favored for the "end-user stage", where the goal is to enable multiple users to access the network for secure communication. This is because, enabling multiple users to use a quantum network via point-to-point channels would require full QKD systems to be installed for each end-user, which could be very expensive. Whereas, architectures based on one-sender multiple-receivers (which can be modeled as broadcast channels) and vice versa (multiple access channels) offer more viable and efficient options for the end-user stage.

In this work, we consider an architecture based on the quantum broadcast channel for multipartite secret-key agreement and entanglement generation. Our goal is to obtain constraints on the achievable rates between any subset of the users of a one-to-many quantum broadcast channel. We analyze a general protocol for entanglement distillation and secret-key agreement over a quantum broadcast channel. Fig. 1 depicts a protocol for the one-sender two-receiver case as an example. The protocol consists of n applications of the broadcast channel, where successive applications of the channel are interleaved by LOCC involving all the three users.

Tools. We use multipartite generalizations of the squashed entanglement quantities defined earlier in [6, 1] to give our constraints on achievable entanglement distillation and secret-key agreement rates over the quantum broadcast channel. Along the way, we develop several new properties of these quantities (see [3, Lemmas 6-8]). Among these, the property perhaps most important is [3, Lemma 6], which is a multipartite generalization of the sub-additivity inequality introduced in [5, Theorem 7]. This property allows us to "peel off" the actions of the channel from the output state of the protocol one by one, thereby allowing us to upper bound the squashed entanglement of the output state in terms of a sum of squashed entanglements on states that result from each successive action of the channel and each round of LOCC.

Main Result. Our main result is a theorem that constrains the rates at which secret key and entanglement can be generated between any subset of users of a one-to-many quantum broadcast channel when assisted by unlimited LOCC between all the users of the channel. The bounds we give are single-letter bounds, i.e., they can be evaluated in terms of the output of a single use of the channel when input with a pure state. Our theorem for a one-sender two-receiver quantum broadcast channel is stated as follows [3, Theorem 11]:

Theorem 1. *Let $\mathcal{N}_{A\to BC}$ be a quantum broadcast channel from a sender Alice to receivers Bob and Charlie. If the rate tuple $(E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})$ is achievable, then there exists a pure state ϕ_{RA} with*

$$\omega_{RBC} \equiv \mathcal{N}_{A\to BC}(\phi_{RA}), \tag{1}$$

such that the following bounds hold

$$E_{AB} + K_{AB} + E_{BC} + K_{BC} + E_{ABC} + K_{ABC} \leq E_{\text{sq}}\left(RC;B\right)_{\omega} \tag{2}$$

$$E_{AC} + K_{AC} + E_{BC} + K_{BC} + E_{ABC} + K_{ABC} \leq E_{\text{sq}}\left(RB;C\right)_{\omega} \tag{3}$$

$$E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{ABC} + K_{ABC} \leq E_{\text{sq}}\left(R;BC\right)_{\omega} \tag{4}$$

$$E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{BC} + K_{BC} + \frac{3}{2}\left(E_{ABC} + K_{ABC}\right) \leq \min\left\{E_{\text{sq}}\left(R;B;C\right)_{\omega}, \widetilde{E}_{\text{sq}}\left(R;B;C\right)_{\omega}\right\}. \tag{5}$$

The dimension of system R need not be any larger than the dimension of the channel input.

We also state and prove a general theorem for a one-sender and m-receiver quantum broadcast channel in [3, Theorem 12].

Application to pure-loss bosonic broadcast channels. We apply our result to the case of a pure-loss bosonic broadcast channel (namely where the environment injects the vacuum state) from a single sender Alice to two receivers Bob and Charlie. The channel is modeled by a three-way beamsplitter transformation

$$\hat{a} \rightarrow \sqrt{\eta_B}\hat{b} + \sqrt{\eta_C}\hat{c} + \sqrt{1-\eta_B-\eta_C}\hat{e}, \tag{6}$$

where $\eta_B, \eta_C \in [0,1]$, $\eta_B + \eta_C \leq 1$, $\hat{a}$, $\hat{b}$, and $\hat{c}$, are mode operators corresponding to the sender Alice's input, Bob's output, and Charlie's output, respectively, and where $\hat{e}$ is the mode operator corresponding to the environment of the channel. Our theorem is stated as follows:

Theorem 2. *Let a pure-loss bosonic broadcast channel from a sender Alice to receivers Bob and Charlie be described by the mode transformation in* (6)*. Then the achievable entanglement distillation and secret key agreement rates* $(E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})$ *between two or more of the three parties involved are bounded as follows:*

$$E_{AB} + K_{AB} + E_{BC} + K_{BC} + E_{ABC} + K_{ABC} \leq \log\left(\frac{1+\eta_B-\eta_C}{1-\eta_B-\eta_C}\right), \tag{7}$$

$$E_{AC} + K_{AC} + E_{BC} + K_{BC} + E_{ABC} + K_{ABC} \leq \log\left(\frac{1+\eta_C-\eta_B}{1-\eta_B-\eta_C}\right), \tag{8}$$

$$E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{ABC} + K_{ABC} \leq \log\left(\frac{1+\eta_B+\eta_C}{1-\eta_B-\eta_C}\right), \tag{9}$$

and

$$E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{BC} + K_{BC} + \frac{3}{2}\left(E_{ABC} + K_{ABC}\right) \leq \frac{1}{2}\left[\log\left(\frac{\eta_B}{(1-\eta)\left(1-\eta^*_{E'}\right)}+1\right) + \log\left(\frac{\eta_C}{(1-\eta)\left(1-\eta^*_{E'}\right)}+1\right) + \log\left(\frac{\eta}{(1-\eta)\,\eta^*_{E'}}+1\right)\right], \tag{10}$$

where $\eta^*_{E'}$ *is the solution of*

$$\frac{1}{\eta^2_{E'}\left(1-\eta\right)/\eta_B + \eta_{E'}} + \frac{1}{\eta^2_{E'}\left(1-\eta\right)/\eta_C + \eta_{E'}} = \frac{1}{\left(1-\eta_{E'}\right)^2\left(1-\eta\right)/\eta + 1 - \eta_{E'}}. \tag{11}$$

References

[1] David Avis, Patrick Hayden, and Ivan Savov. Distributed compression and multiparty squashed entanglement. *Journal of Physics A: Mathematical and Theoretical*, 41(11):115301, March 2008. arXiv:0707.2792. (document)

[2] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, April 2009. arXiv:quant-ph/0506189. (document)

[3] Kaushik P. Seshadreesan, Masahiro Takeoka, and Mark M. Wilde. Bounds on entanglement distillation and secret key agreement for quantum broadcast channels. arXiv:1503.08139 [quant-ph]. (document)

[4] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, 5:5235, October 2014. (document)

[5] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60(8):4987–4998, August 2014. arXiv:1310.0129. (document)

[6] Dong Yang, Karol Horodecki, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Wei Song. Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof. *IEEE Transactions on Information Theory*, 55(7):3375–3387, July 2009. arXiv:0704.2236. (document)