# Unconstrained Capacities of Quantum Key Distribution and Entanglement Distillation for Pure-Loss Bosonic Broadcast Channels

Masahiro Takeoka, Kaushik P. Seshadreesan, and Mark M. Wilde

Phys. Rev. Lett. **119**, 150501 — Published 13 October 2017
DOI: 10.1103/PhysRevLett.119.150501

# Unconstrained Capacities of Quantum Key Distribution and Entanglement Distillation for Pure-Loss Bosonic Broadcast Channels

Masahiro Takeoka,[1] Kaushik P. Seshadreesan,[2] and 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, Staudtstr. 2, 91058 Erlangen, 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*

We consider quantum key distribution (QKD) and entanglement distribution using a single-sender multiple-receiver pure-loss bosonic broadcast channel. We determine the unconstrained capacity region for the distillation of bipartite entanglement and secret key between the sender and each receiver, whenever they are allowed arbitrary public classical communication. A practical implication of our result is that the capacity region demonstrated drastically improves upon rates achievable using a naive time-sharing strategy, which has been employed in previously demonstrated network QKD systems. We show a simple example of the broadcast QKD protocol overcoming the limit of the point-to-point strategy. Our result is thus an important step toward opening a new framework of network channel-based quantum communication technology.

*Introduction*. Quantum key distribution (QKD) [1, 2] and entanglement distillation (ED) [3, 4] are two cornerstones of quantum communication. QKD enables two or more cooperating parties to distill and share unconditionally secure, random bit sequences, which could then be used for secure classical communication. ED, on the other hand, allows them to distill pure maximal entanglement from a quantum state shared via a noisy communication channel, which could then be used to faithfully transfer quantum states by means of quantum teleportation [5]. In both protocols, the parties are allowed to perform (in principle) an unlimited amount of local operations and classical communication (LOCC).

Not only have there been theoretical developments, but also quantum communication technologies have matured tremendously in recent years. In particular, QKD has been available commercially for a number of years and has now expanded to real-world networks [6–8], which consist of point-to-point QKD links and trusted nodes.

Another important direction is to go beyond point-to-point links and make use of network channels. In fact the operation of QKD has been proposed for a broadcast channel (single-sender and multiple-receiver) [9] and recently experimentally demonstrated for a multiple access channel [10] (multiple-sender and single-receiver). In [10], the developed system is based on conventional optical-access network protocols, in which 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: when one sender and one receiver use the channel most of the time, the key or entanglement rates for the other users decrease. 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 and each receiver, along with the assistance of unlimited LOCC [11]. Even though communication tasks in various network scenarios have been examined [12–17], there has been limited work on the capacity of entanglement and secret key distillation assisted by unlimited LOCC. Only recently in [18] were outer bounds on the achievable rates established for multipartite secret-key agreement and entanglement generation between any subset of the users of a general single-sender $m$-receiver quantum broadcast channel (QBC) (for any $m \geq 1$), assisted by unlimited LOCC. The main idea was to employ multipartite generalizations of the squashed entanglement [19, 20] and the methods of [21, 22].

We break the proof of the capacity region into two parts. The upper bound (converse) is established by combining the method in [18] and the point-to-point upper bound based on relative entropy of entanglement [23, 24], first discussed in [23] and rigorously proven in [24]. The lower bound (achievability) is proved by employing the quantum state merging protocol [25, 26]. Our result clearly shows that the rate region considerably improves upon the time-sharing limit, and at the same time, it proves that this is the fundamental limit that cannot be overcome within the same framework. Moreover, we do not leave this result as a purely theoretical development, but we also consider the possible implementation of a QKD protocol overcoming the limit by simple point-to-point protocols for an optical broadcast channel. Our result is thus an important step toward the opening of a new framework of network channel-based quantum communication technology.

*LOCC-assisted distillation in a linear-optical network.* We consider the following general distillation protocol which uses a quantum broadcast channel [18]. The sender $A$ prepares some quantum systems in an initial quantum state and successively sends some of these systems to the receivers $B_1$, $B_2$, $\ldots$, $B_m$ by interleaving $n$ channel uses of the 1-to-$m$ broadcast channel with rounds of LOCC. The goal of the protocol is to distill bipartite maximally entangled states $\Phi_{AB_i}$ and private states $\gamma_{AB_i}$ (equivalently, a secret key [27, 28]). After each channel use, they can perform an arbitrary number of rounds of LOCC (in any direction with any number of parties). The quantity $E_{AB_i}$ denotes the rate of entanglement that can be established between $A$ and $B_i$ (i.e., the logarithm of the Schmidt rank of $\Phi_{AB_i}$ normalized by the number of channel uses) and $K_{AB_i}$ denotes the rate of secret key that can be established between $A$ and $B_i$ (i.e., the number of secret-key bits in $\gamma_{AB_i}$ normalized by the number of channel uses). The parameter $\varepsilon \in (0,1)$ is such that the fidelity [29] between the ideal state at the end of the protocol and the actual state is not smaller than $1-\varepsilon$. The protocol considered here is similar to the one described in [18], except that here the goal is *not* to establish bipartite entanglement or key among the receivers or multipartite entanglement or key among more than two parties. A rate tuple $(E_{AB_1},\ldots,E_{AB_m}, K_{AB_1},\ldots,K_{AB_m})$ is achievable if for all $\varepsilon \in (0,1)$ and sufficiently large $n$, there exists an $(n, E_{AB_1},\ldots,E_{AB_m}, K_{AB_1},\ldots,K_{AB_m},\varepsilon)$ protocol of the above form. The capacity region is the closure of the set of all achievable rates.

The quantum channel we consider here is a general 1-to-$m$ bosonic broadcast channel $\mathcal{L}_{A'\to B_1\cdots B_m}$ consisting of passive linear optical elements (beam splitters and phase shifters) [30]. An isometric extension of the channel (see, e.g., [31]), denoted by $U^{\mathcal{L}}$, is then given by an $l$-input $l$-output linear optical unitary transformation (see Fig. 1(a)). For $U^{\mathcal{L}}$, one of the inputs is the sender $A$'s input and the others are prepared as vacuum states. Also, $m$ of the outputs ($m \le l$) are given to the legitimate receivers $\{B_1,\ldots,B_m\}$ (one per receiver), and the rest of the outputs are for the environment, which we allow the eavesdropper to access during the protocol. Let $\{\eta_{B_1},\ldots,\eta_{B_m}\}$ be a set of power transmittances from the sender to the respective receivers. Each $\eta_{B_i}$ is nonnegative and $\sum_{i=1}^m \eta_{B_i} \le 1$. 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 $\mathcal{T}$. Then our main result is as follows:

*Theorem 1:* The LOCC-assisted unconstrained capacity region of the pure-loss bosonic QBC $\mathcal{L}_{A'\to B_1\cdots B_m}$ is given by

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

for all non-empty $\mathcal{T} \subseteq \mathcal{B}$, where $\eta_{\mathcal{B}} = \sum_{i=1}^m \eta_{B_i}$ and $\eta_{\overline{\mathcal{T}}} = \sum_{B_i\in\overline{\mathcal{T}}} \eta_{B_i}$.

The proof of Theorem 1 consists of three steps:

*(1) Decomposition of $U^{\mathcal{L}}$.* First we argue that $U^{\mathcal{L}}$ can be rewritten as an equivalent and simpler QBC (see [30] as well for the reduction outlined here). The isometric extension $U^{\mathcal{L}}$ can be represented by an $l\times l$ unitary matrix describing the input-output relation of a set of annihilation operators $\{\hat{a}_1,\ldots\hat{a}_l\}$ for $l$ input modes. In [32], it was shown that any such $l\times l$ unitary matrix can be decomposed as a sequence of $2\times 2$ matrices, each realized by a beam splitter and phase shifters combining any two of the $l$ modes (see Fig. 1(b), which contains at most ${}_lC_2$ beam splitters). Recall that all the inputs except for the sender's are prepared as vacuum states. Then we can remove all the beam splitters that have both inputs set to vacuum states because their outputs are vacuum states as well. In addition, by grouping together all of the eavesdropper's modes, the channel is simplified to just a sequence of $m$ beam splitters (Fig. 1(c)). In what follows, we consider this simplified, equivalent channel model.

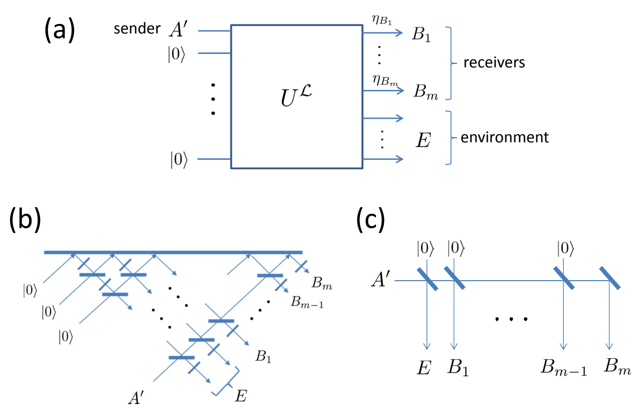


FIG. 1. (a) Single-sender $m$-receiver pure-loss linear optics quantum broadcast channel. $U^{\mathcal{L}}$ is a unitary operator of an arbitrary linear optics circuit. (b), (c) Reductions to an equivalent channel.

*(2) Achievability part.* To achieve the rate region in (1), we consider a distillation protocol which employs quantum state merging. State merging was introduced in [25, 26] and provides an operational meaning for the conditional quantum entropy. For a state $\rho_{AB}$, its conditional quantum entropy is defined as $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$ where $H(AB)_\rho$ and $H(B)_\rho$ are the quantum entropies of $\rho_{AB}$ and its marginal $\rho_B$, respectively. For many copies of $\rho_{AB}$ shared between Alice and Bob, $H(A|B)_\rho$ is the optimal rate at which two-qubit maximally entangled states need to be consumed to transfer Alice's systems to Bob's side via LOCC. If $H(A|B)_\rho$ is negative, the result is that after transferring Alice's systems, they can gain (i.e., distill) entanglement at rate $-H(A|B)_\rho$. State merging also yields a quantum analog of the Slepian-Wolf theorem concerning classical distributed compression and has been applied to the QBC in [16, 17].

Here we consider the following alternative state-merging-based protocol. Alice first prepares $n$ copies of a two-mode squeezed vacuum (TMSV) state, defined as $|\Psi(N_S)\rangle_{AA'} = \sum_{m=0}^\infty \sqrt{\lambda_m(N_S)}|m\rangle_A|m\rangle_{A'}$, where $|m\rangle$ is an $m$-photon state, $\lambda_m(N_S) = N_S^m/\left(N_S+1\right)^{m+1}$, and $N_S$ is the average photon number of one mode of the state. She sends system $A'$ to $B_1\cdots B_m$ through the broadcast channel in Fig. 1(a). After $n$ uses of the channel, they share $n$ copies of the state $\phi_{AB_1\cdots B_m} = \mathcal{L}_{A'\to B_1\cdots B_m}(|\Psi(N_S)\rangle\langle\Psi(N_S)|_{AA'})$.

Then by using $\phi_{AB_1\cdots B_m}^{\otimes n}$, they perform state merging to establish entanglement. More precisely, all the receivers successively transfer their systems back to Alice by LOCC and at the same time generate entanglement with her in the process This can be accomplished by applying the point-to-point state merging protocol successively [25, 26].

Then we obtain the achievable rate region as

$$\sum_{B_i\in\mathcal{T}} E_{AB_i} \leq -H(\mathcal{T}|A\overline{\mathcal{T}})_\phi, \tag{2}$$

where $\phi_{AB_1\cdots B_m} = \mathcal{L}_{A'\to B_1\cdots B_m}(|\Psi(N_S)\rangle\langle\Psi(N_S)|_{AA'})$. The right-hand side of the inequalities in (2) can be explicitly calculated. Recall that the marginal of the TMSV $\Psi_{A'}(N_S) = \mathrm{Tr}_A[|\Psi(N_S)\rangle\langle\Psi(N_S)|_{AA'}]$ is a thermal state with mean photon number $N_S$. Its entropy is equal to $H(A')_\Psi = g(N_S)$, where $g(x) = (x+1)\log_2(x+1) - x\log_2 x$. Also a pure-loss channel with transmittance $\eta$ maps a thermal state to another thermal state with reduced average photon number. Then the right-hand side of (2) is calculated as

$$\begin{aligned}-H(\mathcal{T}|A\overline{\mathcal{T}})_\phi &= H(A\overline{\mathcal{T}})_\phi - H(A\mathcal{T}\overline{\mathcal{T}})_\phi \\ &= H(\mathcal{T}E)_\phi - H(E)_\phi \\ &= g((1-\eta_{\overline{\mathcal{T}}})N_S) - g((1-\eta_{\mathcal{B}})N_S).\end{aligned}$$

By taking $N_S \to \infty$ in the last line above, the limit is equal to $\log_2([1-\eta_{\overline{\mathcal{T}}}]/[1-\eta_{\mathcal{B}}])$. Since one ebit of entanglement can generate one private bit of key, we can replace $E_{AB_i}$ with $E_{AB_i} + K_{AB_i}$, which completes the achievability part.

*(3) Converse part*. The converse relies upon several tools and is given in terms of the one-shot variant [33] of the relative entropy of entanglement (REE) [34]. The $\varepsilon$-REE for a quantum state $\rho_{AB}$ is defined by

$$E_R^\varepsilon(A;B)_\rho = \inf_{\sigma_{AB}\in\mathrm{SEP}} D_H^\varepsilon(\rho_{AB}\|\sigma_{AB}), \tag{3}$$

where $D_H^\varepsilon(\rho\|\sigma) = -\log_2 \inf_{0\leq\Lambda\leq I, \mathrm{Tr}[\Lambda\rho]\geq 1-\varepsilon} \mathrm{Tr}[\Lambda\sigma]$ is the hypothesis testing quantum relative entropy [35–37] and SEP denotes the set of separable states. The original LOCC-assisted communication protocol can equivalently be rewritten by using a teleportation simulation argument [4, Section V] (see also [38]) suitably extended to continuous-variable bosonic channels [39]. Teleportation simulation in the case of a point-to-point channel can be understood as a way of reducing a sequence of adaptive protocols involving two-way LOCC to a sequence of non-adaptive protocols followed by a final LOCC [4, 38]. For all 'teleportation-simulable channels' that allow for such a reduction, an upper bound on the entanglement and secret key agreement capacity can be given by the $\varepsilon$-REE [24], because the $\varepsilon$-REE is an upper bound on the one-shot distillable key of a bipartite state [24]. Furthermore, for pure-loss bosonic channels, one can use a concise formula for the REE identified in [23]. With these techniques, an upper bound on the unconstrained capacity of a point-to-point pure-loss channel is given by the REE of the state resulting from sending an infinite-energy TMSV through the channel, explicitly calculated to be $-\log_2(1-\eta)$ [23, 24].

Following [24], suppose that the original protocol generates a state $\omega_{AB_1\cdots B_m}$ which is $\varepsilon$-close to $\tilde{\Phi}_{AB_1\cdots B_m}$:

$$1-\varepsilon \leq F(\omega_{AB_1\cdots B_m}, \tilde{\Phi}_{AB_1\cdots B_m}) \tag{4}$$

$$\tilde{\Phi}_{AB_1\cdots B_m} = \Phi_{A^1B_1^1}^{\otimes nE_{AB_1}} \otimes \cdots \otimes \Phi_{A^mB_m^1}^{\otimes nE_{AB_m}} \otimes \gamma_{A^{m+1}B_1^2}^{\otimes nK_{AB_1}} \otimes \cdots \otimes \gamma_{A^{2m}B_m^2}^{\otimes nK_{AB_m}}, \tag{5}$$

where $A^j$ and $B_i^j$ are subsystems of $A$ and $B_i$, respectively. Since the pure-loss bosonic QBC is covariant with respect to displacement operations (which are the teleportation corrections for bosonic channels [40]), it is teleportation-simulable [39]. Then the original broadcasting protocol described above can be replaced by the distillation of $n$ copies of $\phi_{AB_1\cdots B_m} = \mathcal{N}_{A'\to B_1\cdots B_m}(|\Psi(N_S)\rangle\langle\Psi(N_S)|_{AA'})$ via a single LOCC. This simulation incurs an additional error that depends on the energy $N_S$ of the state $|\Psi(N_S)\rangle_{AA'}$ and which vanishes in the limit $N_S \to \infty$. Let us denote the total error by $\varepsilon(N_S)$ and note that $\lim_{N_S\to\infty}\varepsilon(N_S) = \varepsilon$. Then by using the arguments of [24], we find that

$$\sum_{B_i\in\mathcal{T}} (E_{AB_i} + K_{AB_i}) \leq \frac{1}{n} E_R^{\varepsilon(N_S)}(\mathcal{T}^n; A^n\overline{\mathcal{T}}^n)_{\phi^{\otimes n}} \tag{6}$$

for all $\mathcal{T}$, where $E_R^{\varepsilon(N_S)}$ denotes the $\varepsilon$-relative entropy of entanglement recalled above.

To find an upper bound on $\frac{1}{n}E_R^{\varepsilon(N_S)}(\mathcal{T}^n; A^n\overline{\mathcal{T}}^n)_{\phi^{\otimes n}}$ for each $\mathcal{T}$, we use a calculation from [23, 24] for a point-to-point pure-loss bosonic channel with transmittance $\eta$. In [24], it was shown that the $\varepsilon$-relative entropy of entanglement for a pure-loss channel is bounded from above by $-\log_2(1-\eta) + C(\varepsilon)/n$, where $C(\varepsilon) = \log_2 6 + 2\log_2([1+\varepsilon]/[1-\varepsilon])$. Also it is critical to observe that the order of the beam splitters in Fig. 1(c) is reconfigurable by properly commuting the beam splitting operators. By using this observation and some properties of the TMSV, we obtain the following upper bound on (6):

$$\log_2([1-\eta_{\overline{\mathcal{T}}}]/[1-\eta_{\mathcal{B}}]) + C(\varepsilon)/n. \tag{7}$$

The converse proof is completed by taking the limit $n \to \infty$. Note that our converse is a *strong converse* because there is no need to take the limit $\varepsilon \to 0$ in order to get the upper bound of $\log_2\left(\frac{1-\eta_{\overline{\mathcal{T}}}}{1-\eta_{\mathcal{B}}}\right)$. See Supp. Mat. 1 [41] for detailed calculations. Since the converse bound coincides with the achievable rate region, this completes the proof of Theorem 1.

*Discussion.* The simplest pure-loss broadcast channel is a 1-to-2 broadcast channel with one sender, Alice, and two receivers, Bob and Charlie. The capacity region implied by Theorem 1 is explicitly given by

$$E_{AB} + K_{AB} \leq \log_2([1-\eta_C]/[1-\eta_B-\eta_C]), \tag{8}$$

$$E_{AC} + K_{AC} \leq \log_2([1-\eta_B]/[1-\eta_B-\eta_C]), \tag{9}$$

$$E_{AB} + K_{AB} + E_{AC} + K_{AC} \leq -\log_2(1-\eta_B-\eta_C), \tag{10}$$

where $\eta_B$ and $\eta_C$ are the transmittances from Alice to Bob and Charlie, respectively.

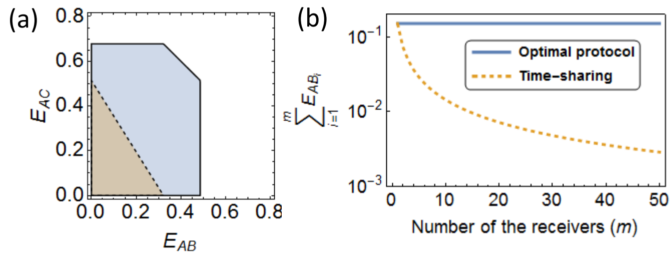


FIG. 2. Comparison of the LOCC-assisted capacity (solid line) and the time sharing of the point-to-point capacity (dashed line). (a) Capacity region for the 1-to-2 QBC with $(\eta_B,\ \eta_C) = (0.3,\ 0.3)$. (b) Rate sum comparison for the 1-to-$m$ QBC with $\eta = 0.1$.

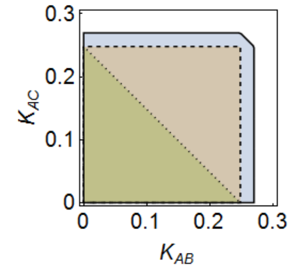


FIG. 3. Secret key rate region of the GC09 based CVQKD in a 1-to-2 pure-loss bosonic QBC, with $(\eta_B, \eta_C) = (0.3, 0.3)$. The squeezing parameter is $v = 40$ (see Supp. Mat. 3 [41]). The BC-CVQKD (solid line), simultaneous application of point-to-point protocol (dashed line), and time sharing of the point-to-point protocol (dotted line).

It is interesting to compare the capacity with a point-to-point protocol based approach. To do so, we discuss ED and QKD scenarios separately. A naive ED protocol in QBC is the time sharing of the optimal point-to-point protocol (i.e., they split $n$ uses of the quantum channel into two parts: distill $E_{AB}$ with rate $-\log_2(1-\eta_B)$ in the first part and $E_{AC}$ with rate $-\log_2(1-\eta_C)$ in the second part). Figure 2(a) compares the capacity region and the time-sharing strategy. The capacity (optimal strategy) clearly outperforms time sharing and the gap is observed 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 through a sequence of successive state merging [26] (for example, Charlie helps to increase $E_{AB}$ and vice versa).

The rate gap is more pronounced when we extend this to the $m$-receiver scenario. Consider the 1-to-$m$ symmetric pure-loss channel where each receiver has equal transmittance $\eta/m$ and the distillation scenario such that all receivers achieve the same rate. Then the sum of the rates for the optimal protocol based on state merging is $-\log_2(1-\eta)$ whereas that for time sharing of the point-to-point optimal protocol is $-\log_2(1-\eta/m)$ (see Supp. Mat. 2 [41]). The plots in Fig. 2(b) show a huge gap between time sharing and the optimal key distillation strategy.

Let us turn to the QKD scenario. The experimental demonstration in [10] utilizes the time (or frequency) sharing due to technical reasons [42]. In principle, however, one can overcome this by still a point-to-point based protocol. In QKD, the purpose of quantum communication is to hold correlated classical data and then the key distilled classically. Thus, the sender Alice can copy her data and make point-to-point key distillation simultaneously with each receiver (a related idea is in [9]) which can overcome the tradeoff by time sharing. The question is then: can we even outperform this no tradeoff rate region? Here we show that it is possible by describing an explicit example based on a point-to-point continuous variable QKD protocol proposed in [43] (GC09), which uses squeezed state and reverse reconciliation (see Supp. Mat. 3 [41]).

In the 1-to-2 QBC setting, the simultaneous operation of the point-to-point GC09 protocol generates a pair of key rates $(K_{AB}, K_{AC}) = (I(X;Y) - I(Y;C')_\rho, I(X;Z) - I(Z;B')_\rho)$, where $X$, $Y$, and $Z$ are the classical data shared by Alice, Bob, and Charlie after $n$ uses of the quantum channel, $B'$ and $C'$ are the quantum systems for possible eavesdroppers which may contain the environment (usually called Eve) and the receiver who is not involved in the key (for example, $C'$ includes Charlie). $I(X;Z)$ and $I(Z;C')_\rho$ denote classical and quantum mutual information, respectively. As discussed above, these two rates are simultaneously achievable.

Now we show how to overcome this by using a trick inspired by the successive state merging. Suppose Alice and Charlie first conduct point-to-point key distillation. This operation achieves the key rate $K_{AC} = I(X;Z) - I(Z;B')_\rho$ and also reconstructs Charlie's classical system $Z$ at Alice's side. After that, Bob distills the key with Alice, where Alice holds $X$ and $Z$ and Bob holds $Y$. Thus, they can achieve the key rate $K_{AB} = I(XZ;Y) - I(Y;C')_\rho$, which can be larger than that in the simple point-to-point protocol. Similarly, by changing the order of distillation, they can achieve the rate pair $(K_{AB}, K_{AC}) = (I(X;Y) - I(Y;C')_\rho, I(XY;Z) - I(Z;B')_\rho)$. Thus the achievable rate region is given by time sharing of these two rate pairs. We refer to this protocol as the broadcast-CVQKD (BC-CVQKD). Figure 3 shows the key rate region for BC-CVQKD, which outperforms the rate regions for the simultaneous point-to-point protocol and the simple time sharing (Supp. Mat. 3 [41] gives an explicit key rate expression). Since the original GC09 is a noise-immune CVQKD protocol [43] (see also [44]), it is an interesting future work to extend our analysis to a noisy bosonic QBC. Also there still remains a huge gap between the key rate region in Fig. 3 and the capacity region in Fig. 2, suggesting that there may exist yet-to-be discovered clever broadcast QKD protocols.

*Conclusion.* We have established the unconstrained capacity region of a pure-loss bosonic broadcast channel for LOCC-assisted entanglement and secret key distillation. The channel we considered here is general in the sense that it includes any (no-repeater) linear optics network as its isometric extension. It could provide a useful benchmark for the broadcasting of entanglement and secret key through such channels. Furthermore, our result stimulates practical protocols for QKD or entanglement distillation over broadcast channels which overcome the time-sharing bound. As an example, we show the BC-CVQKD approach that can outperform a simple application of the point-to-point strategy.

We thank Saikat Guha, Michael Horodecki, Haoyu Qi, and John Smolin. MT acknowledges the Open Partnership Joint Projects of JSPS Bilateral Joint Research Projects and the ImPACT Program of Council for Science, Technology, and Innovation, Japan. MMW thanks NICT for hosting him during Dec. 2015 and acknowledges NSF and ONR. KPS thanks the Max Planck Society.

[1] C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing , 175 (1984).
[2] A. K. Ekert, Physical Review Letters **67**, 661 (1991).
[3] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Physical Review Letters **76**, 722 (1996).
[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Physical Review A **54**, 3824 (1996), arXiv:9604024 [quant-ph].
[5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Physical Review Letters **70**, 1895 (1993).
[6] M. Peev, C. Pacher, and R. Alléaume, New Journal of Physics **11**, 075001 (2009).
[7] M. Sasaki et al., Optics Express **19**, 10387 (2011), arXiv:quant-ph/1103.3566.
[8] S. Wang et al., Optics Express **22**, 21739 (2014).
[9] P. D. Townsend, Nature **385**, 47 (1997).
[10] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, Nature **501**, 69 (2013).
[11] Here "unconstrained capacity" means the capacity without any energy constraint on the input quantum states.
[12] A. E. Allahverdyan and D. B. Saakian, (1998), arXiv:9805067 [quant-ph].
[13] A. Winter, IEEE Transactions on Information Theory **47**, 3059 (2001).
[14] S. Guha, J. H. Shapiro, and B. I. Erkmen, Physical Review A **76**, 032303 (2007).
[15] J. Yard, P. Hayden, and I. Devetak, IEEE Transactions on Information Theory **54**, 3091 (2008), arXiv:0501045 [quant-ph].
[16] J. Yard, P. Hayden, and I. Devetak, IEEE Transactions on Information Theory **57**, 7147 (2011).
[17] F. Dupuis, P. Hayden, and K. Li, IEEE Transactions on Information Theory **56**, 2946 (2010).
[18] K. P. Seshadreesan, M. Takeoka, and M. M. Wilde, IEEE Transactions on Information Theory **62**, 2849 (2016), arXiv:1503.08139.
[19] D. Avis, P. Hayden, and I. Savov, Journal of Physics A: Mathematical and Theoretical **41**, 115301 (2008), arXiv:0707.2792.
[20] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, IEEE Transactions on Information Theory **55**, 3375 (2009).
[21] M. Takeoka, S. Guha, and M. M. Wilde, Nature Communications **5**, 5235 (2014).
[22] M. Takeoka, S. Guha, and M. M. Wilde, IEEE Transactions on Information Theory **60**, 4987 (2014), arXiv:1310.0129.
[23] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, (2015), arXiv:1510.08863v5.
[24] M. M. Wilde, M. Tomamichel, and M. Berta, IEEE Transactions on Information Theory **63**, 1792 (2017), arXiv:1602.08898.
[25] M. Horodecki, J. Oppenheim, and A. Winter, Nature **436**, 673 (2005).
[26] M. Horodecki, J. Oppenheim, and A. Winter, Communications in Mathematical Physics **136**, 107 (2007).
[27] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Physical Review Letters **94**, 160502 (2005), arXiv:quant-ph/0309110.
[28] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Transactions on Information Theory **55**, 1898 (2009), arXiv:quant-ph/0506189.
[29] A. Uhlmann, Reports on Mathematical Physics **9**, 273 (1976).
[30] S. Guha, *Multiple-User Quantum Information Theory for Optical Communication Channels*, Ph.D. thesis, Massachusetts Institute of Technology (2008).
[31] M. M. Wilde, *From Classical to Quantum Shannon Theory* (2016) arXiv:1106.1445v7.
[32] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Physical Review Letters **73**, 58 (1994).
[33] F. G. S. L. Brandao and N. Datta, IEEE Transactions on Information Theory **57**, 1754 (2011), arXiv:0905.2673.
[34] V. Vedral and M. B. Plenio, Physical Review A **57**, 1619 (1998), arXiv:quant-ph/9707035.
[35] F. Hiai and D. Petz, Communications in Mathematical Physics **143**, 99 (1991).
[36] F. Buscemi and N. Datta, IEEE Transactions on Information Theory **56**, 1447 (2010), arXiv:0902.0158.
[37] L. Wang and R. Renner, Physical Review Letters **108**, 200501 (2012), arXiv:1007.5456.
[38] A. Müller-Hermes, *Transposition in Quantum Information Theory*, Master's thesis (2012).
[39] J. Niset, J. Fiurášek, and N. Cerf, Physical Review Letters **102**, 1 (2009).
[40] S. L. Braunstein and H. J. Kimble, Physical Review Letters **80**, 869 (1998).
[41] See Supplemental Material [url] which includes Refs. [24, 43, 45, 46].
[42] In this experiment, the multiple access configuration is chosen to reduce the number of single photon detectors, which is the most expensive component in their protocol, where the simultaneous point-to-point protocol does not work.
[43] R. García-Patrón and N. J. Cerf, Physical Review Letters **102**, 130501 (2009).
[44] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nature communications **3**, 1083 (2012).
[45] R. Renner and J. I. Cirac, Physical Review Letters **102**, 1 (2009), arXiv:arXiv:0809.2243v1.
[46] M. Takeoka, R.-b. Jin, and M. Sasaki, New Journal of Physics **17**, 43030 (2015).