Universal Limitations on Quantum Key Distribution over a Network

Siddhartha Das,[1,*] Stefan Bäuml,[2,†] Marek Winczewski,[3,4] and Karol Horodecki[4,5]

[1]*Centre for Quantum Information & Communication (QuIC), École polytechnique de Bruxelles, Université libre de Bruxelles, Brussels, B-1050, Belgium*

[2]*ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Avinguda Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain*

[3]*Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland*

[4]*International Centre for Theory of Quantum Technologies (ICTQT), University of Gdańsk, 80-308 Gdańsk, Poland*

[5]*Institute of Informatics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland*

(Received 30 September 2020; revised 15 July 2021; accepted 23 July 2021; published 22 October 2021)

We consider the distribution of secret keys, both in a bipartite and a multipartite (conference) setting, via a quantum network and establish a framework to obtain bounds on the achievable rates. We show that any multipartite private state—the output of a protocol distilling secret key among the trusted parties—has to be genuinely multipartite entangled. In order to describe general network settings, we introduce a multiplex quantum channel, which links an arbitrary number of parties where each party can take the role of sender only, receiver only, or both sender and receiver. We define asymptotic and nonasymptotic local quantum operations and classical communication-assisted secret-key-agreement (SKA) capacities for multiplex quantum channels and provide strong and weak converse bounds. The structure of the protocols we consider, manifested by an adaptive strategy of secret-key and entanglement [Greenberger–Horne–Zeilinger (GHZ) state] distillation over an arbitrary multiplex quantum channel, is generic. As a result, our approach also allows us to study the performance of quantum key repeaters and measurement-device-independent quantum key distribution (MDI-QKD) setups. For teleportation-covariant multiplex quantum channels, we get upper bounds on the SKA capacities in terms of the entanglement measures of their Choi states. We also obtain bounds on the rates at which secret key and GHZ states can be distilled from a finite number of copies of an arbitrary multipartite quantum state. We are able to determine the capacities for MDI-QKD setups and rates of GHZ-state distillation for some cases of interest.

DOI: 10.1103/PhysRevX.11.041016

Subject Areas: Atomic and Molecular Physics, Photonics, Quantum Physics, Quantum Information

I. INTRODUCTION

Quantum communication over a network is a pertinent issue from both fundamental and application aspects [1–7]. With technological advancement [8–11], and concerns for privacy [7,12], there is a need for determining protocols and criteria for secret communication among multiple trusted parties in a network. Quantum key distribution (QKD) provides unconditional security for generating secure, random bits among trusted parties against a quantum eavesdropper, i.e., an eavesdropper that is only limited by the laws of quantum mechanics. Secret key agreement (SKA) among multiple allies is called conference key agreement [13,14]. Conference key agreement can be achieved if all parties involved share a Greenberger–Horne–Zeilinger (GHZ) state [15]. As in the case of bipartite QKD, however, there exists a larger class of states, known as multipartite private states [14], which can provide conference keys by means of local measurements by the parties.

Given the global efforts towards a so-called quantum internet [3,16,17], as well as quantum key distribution over long distances [18,19], it is thus pertinent to establish security criteria and benchmarks on key distribution and entanglement generation capabilities over a quantum network. A quantum network is a complex structure as it

*das.seed@gmail.com
†stefan.baeuml@icfo.eu

inherits various setups of different quantum channels with particular alignment due to local environmental conditions. One of the biggest obstacles in building this structure is the attenuation of the signal, which cannot be amplified by cloning or broadcasting because of its inherent quantum nature. The signal decays exponentially with distance over an optical fiber [20], and also, the interaction with the environment makes it difficult to preserve entanglement for a long time [10]. Hence, even obtaining a metropolitan-scale quantum network remains a challenge. To overcome these problems, there is a global effort in building technology of quantum repeaters [11,21–23] that could act as relay stations for long-distance quantum communication [7,19].

Some of the first protocols to be performed once a quantum network is available will likely be bipartite as well as multipartite secret key agreement. Securing the network is a necessity for these QKD protocols to be free of loopholes. A number of spectacular attacks on implementations are based on inaccuracy (inefficiency) of detectors of polarized light [24–26]. Based on the idea of entanglement swapping, a novel protocol known as measurement-device-independent QKD (MDI-QKD) [27,28] was introduced, which does not require the honest parties to detect an incoming quantum signal, thus avoiding the problem of detector inefficiencies. This idea has drawn enormous theoretical and experimental attention over the last few years in terms of analyzing achievable key rates for such a scheme with various noise models and performing experiments with current technologies [29–39].

Given the broad interest in implementing such technologies, understanding the fundamental limitations on the key rates achievable in scenarios such as quantum networks and quantum repeaters, as well as setups for MDI-QKD, is an important task. Seminal papers [40,41] on upper bounds on secret key distillation from states, along with results from Refs. [42–46], have led to notable recent progress in the aforementioned direction, for two parties over point-to-point channels assisted by local quantum operations and classical communication (LOCC) [47–50]. Building upon these works, further progress has been made in restricted network settings, e.g., between two parties over bidirectional [51–53], broadcast [54–56], multiple access, and interference quantum channels [54], as well as quantum repeaters [50,57] and networks consisting of point-to-point [58–60] or broadcast channels [61].

In this work, we aim to provide a unifying framework to derive upper bounds on the key rates, both in bipartite and conference settings, achievable in a broad range of different scenarios, including but not limited to broadcast, multiple access, interference channels, repeaters, some MDI-QKD setups, and more general network scenarios. For that purpose, we introduce a multiplex quantum channel, i.e., a multipartite quantum process that connects parties, each playing one of three possible roles—both sender and receiver, only sender, or only receiver. A multiplex

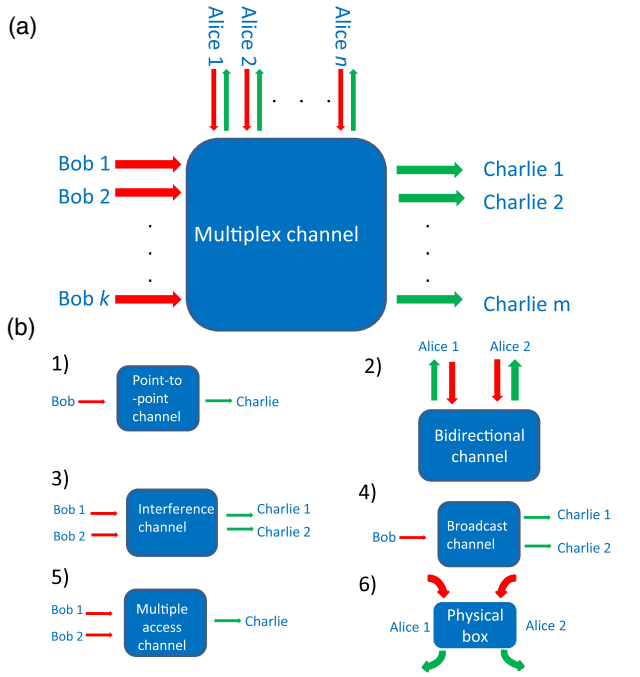

FIG. 1. Pictorial illustration of the universal nature of a multiplex quantum channel from which all other network quantum channels arise, where red and green arrows show inputs and outputs to channels, respectively; see Sec. III B for definitions.

quantum channel is the most general form of a memoryless multipartite quantum channel in a communication network setting. All other network quantum channels can be seen as a special case of this channel (see Fig. 1 for certain common examples). Even the physical setups of MDI-QKD and key repeaters can be described as special cases of multiplex quantum channels (see Fig. 2). In general, the input and output systems on which such a channel acts can be discrete

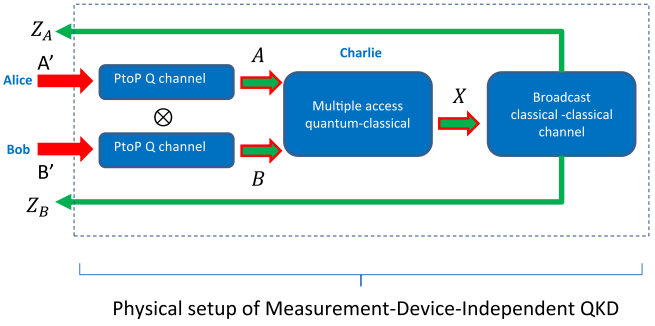

FIG. 2. Graphical depiction of a quantum-to-classical multiplex channel $\mathcal{N}^{\mathrm{MDI}}_{A'B'\to Z_A Z_B}$ as a bidirectional channel, which is a composition of three elementary multiplex channels. We show a pair of point-to-point channels from Alice to Charlie, and from Bob to Charlie composed of a multiple access quantum-to-classical channel (quantum instrument) performed by Charlie, followed by a broadcast classical channel back to Alice and Bob. The green arrows with red boundaries are the outputs of one multiplex channel, which are, at the same time, inputs to the other channel, hence the coloring.

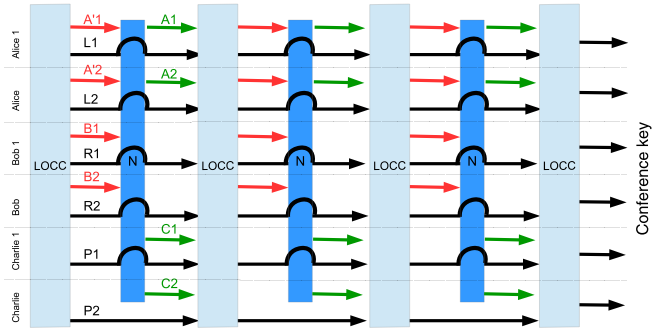

FIG. 3. Example of an LOCC-assisted secret-key-agreement protocol among six parties—Alice 1, Alice 2, Bob 1, Bob 2, Charlie 1, and Charlie 2—using the multiplex channel $\mathcal{N}$ three times. Inputs into $\mathcal{N}$ are depicted in red, outputs in green, and reference systems in black. Alice 1 and 2 enter systems into and receive systems from $\mathcal{N}$, Bob 1 and 2 only enter systems, and Charlie 1 and 2 only receive systems. In the end, the six parties obtain a six-partite conference key.

(finite-dimensional) or continuous variable (infinite-dimensional) quantum systems.

Next, we introduce secret-key-distribution protocols over multiplex quantum channels with LOCC assistance between users, as shown in Fig. 3, which provides a unifying framework to evaluate performances of various seemingly different QKD protocols. In particular, we describe a general paradigm of QKD protocols where a fixed number of trusted allies are connected over a multiplex quantum channel $\mathcal{N}$. In these protocols, the allies are allowed to perform LOCC between each use of $\mathcal{N}$ to generate, in the end, a key that is secure against any eavesdropper that satisfies the laws of quantum mechanics. This so-called quantum eavesdropper can have access to all environment parts, including the isometric extension to channel $\mathcal{N}$.

Our main technical result consists of a metaconverse bound on the one-shot conference key agreement capacity of a multiplex quantum channel, from which we can obtain a number of weak as well as strong converse bounds for the many uses of the multiplex quantum channel, including adaptive and nonadaptive strategies. As our results work in the nonasymptotic setting of a finite number of channel uses, we believe them to be of wide practical interest.

In particular, as an important observation, we show that key repeater protocols, as well as commonly used setups for MDI-QKD, are special cases of LOCC-assisted secret key agreement via a multiplex quantum channel. Whereas bounds on the key rates in such scenarios can also be obtained from a number of earlier results—e.g., from Refs. [50,58,60]—our framework allows for a higher level of specificity in the setups, e.g., by taking into consideration the lack of quantum memory or a particular kind of noisy measurement that is performed in the relay station. Thus, our framework allows us to obtain tighter bounds than those in Refs. [50,58,60] and even to compute MDI-QKD capacities of certain photon-based practical prototypes that use the so-called dual-rail encoding scheme. This approach provides important tools for benchmarking the performance of such experimentally relevant protocols.

When considering conference key agreement, the pivotal observation we arrive at is that multipartite quantum states with directly accessible secret bits, also called (multipartite) private states [14,62], are genuinely multipartite entangled. This fact also allows us to derive nonasymptotic upper bounds on the secret key distillation from a finite number of copies of a multipartite quantum state.

Our work showcases the topology-dependent and yet universal nature of entanglement measures based on sandwiched Rényi relative entropies [63,64], of which relative entropy is a special case. These entanglement measures provide upper bounds on the secret key rate over an arbitrary multiplex quantum channel, which was first shown for bipartite states in Ref. [40]. The entanglement measures are topology dependent because the upper bound's argument depends (only) on the partition of quantum systems held by trusted allies based on their roles in the network channel. The results are based on the observation that multipartite private states are necessarily genuinely multipartite entangled.

The structure of this paper is as follows. We begin with a brief overview of the main results and briefly mention some important prior results along the direction of our work in Sec. II, respectively. We introduce notations and review basic definitions and relevant prior results in Sec. III. In Sec. IV, we introduce and discuss the properties of entanglement measures for the multiplex quantum channel. We show that genuine multipartite entanglement is a necessary criterion for secrecy. In Sec. V, we introduce LOCC-assisted secret-key-agreement protocols over an arbitrary multiplex quantum channel. We derive upper bounds on the maximum achievable rate for conference key agreement over finite uses of multiplex quantum channels. In Sec. VI, we leverage our bounds to provide nontrivial upper bounds on other quantum key distribution schemes such as measurement-device-independent quantum key distribution and quantum key repeaters. In Sec. VII, we derive lower bounds on the secret-key-agreement capacity over an arbitrary multiplex quantum channel. In Sec. VIII, we derive upper bounds on the number of secret key bits that can be distilled via LOCC among trusted parties sharing a finite number of copies of multipartite quantum states. We provide concluding remarks and open questions in Sec. IX.

II. SUMMARY OF THE MAIN RESULTS

In the following, we provide a brief overview of our main results. Regarding technique, our focus is on multipartite private states, which are the most general class of states that provide the quantum conference key directly (i.e., without

distillation) by local measurements. Such states are of the form [14]

$$\gamma_{\overrightarrow{SK}} := U^{\mathrm{tw}}_{\overrightarrow{SK}}(\Phi^{\mathrm{GHZ}}_{\vec{K}} \otimes \omega_{\vec{S}})(U^{\mathrm{tw}}_{\overrightarrow{SK}})^{\dagger}, \tag{1}$$

where $\vec{K} = K_1, \ldots, K_N$ denotes the so-called key part—i.e., the systems that the N parties involved have to measure in order to obtain conference—and $\vec{S} = S_1, \ldots, S_N$ denotes the so-called shield systems, which the parties have to keep secure from the eavesdropper. Also, Φ^{GHZ} is an N-partite GHZ state, ω is some density operator, and U^{tw} is a specifically constructed bipartite unitary operation known as twisting.

We show that states of this form are necessarily genuinely multipartite entangled (GME); i.e., they cannot be expressed as a convex sum of product states no matter with respect to which partition the states are products. To show this, we define a multipartite privacy test, i.e., a dichotomic measurement $\{\Pi^{\gamma}, \mathbb{1} - \Pi^{\gamma}\}$ such that any ϵ-approximate multipartite private state ρ with fidelity $F(\rho, \gamma) \geq 1 - \epsilon$ passes the test with success probability $\mathrm{Tr}[\Pi^{\gamma}\rho] \geq 1 - \epsilon$. We then show that any biseparable state σ cannot pass the privacy test with probability larger than $1/K$, where $\log K$ is the number of conference key bits obtainable by measuring (the key part of) γ. Namely, we show that $\mathrm{Tr}[\Pi^{\gamma}\sigma] \leq 1/K$ for all biseparable σ.

As a means of distributing bipartite or multipartite private states among the users, e.g., in a future quantum version of the internet [3,17], we introduce multiplex quantum channels that connect a number of parties that have one of three possible roles—that of only sender, only receiver, or both sender and receiver. We denote senders as Bob 1,..., Bob k, and their inputs as $B_1, \ldots, B_k$; receivers as Charlie 1,..., Charlie m, and their inputs as $C_1, \ldots, C_m$; and parties that are both senders and receivers as Alice 1,..., Alice n, with respective inputs $A'_1, \ldots, A'_n$ and outputs $A_1, \ldots, A_n$. See also Fig. 1. To describe such channels, we use the notation $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$, where, for sake of brevity, we have introduced $\vec{A} := A_1, \ldots, A_n$, etc. Furthermore, $:\vec{A}:$ denotes the partition $A_1 : \ldots : A_n$ and $:\vec{A}:\vec{B}:$ stands for $A_1 : \ldots : A_n : B_1 : \ldots : B_k$, etc.

By interleaving the uses of a multiplex quantum channel with LOCC among the parties, we provide a general framework to describe a number of different quantum protocols. The idea is to construct a multiplex quantum channel in such a way that its use, interleaved by LOCC, simulates the protocol. For example, in a MDI-QKD setup, where Alice 1 and Alice 2 send states to the central measurement unit using respective channels $\mathcal{N}^{1,2}$, we can define a (bipartite) multiplex quantum channel of the form

$$\mathcal{N}^{\mathrm{MDI}}_{A'_1A'_2\to A_1A_2} := \mathcal{B}_{X\to A_1A_2} \circ \mathcal{M}_{A''_1A''_2\to X} \circ \mathcal{N}^1_{A'_1\to A''_1} \otimes \mathcal{N}^2_{A'_2\to A''_2}. \tag{2}$$

Here, $\mathcal{M}_{A''_1A''_2\to X}$ is the quantum channel performing the central measurement, and $\mathcal{B}_{X\to A_1A_2}$ is a classical broadcast channel sending the result back to Alice 1 and Alice 2. Other examples include multipartite MDI-QKD and secret-key-agreement protocols over quantum network laced with key repeaters [50,57].

Generalizing results for point-to-point [48–50] and bidirectional [51–53] channels, we derive divergence-based measures for the entangling abilities of multiplex quantum channels and show that they provide upper bounds on their secret-key-agreement capacities. The measures we introduce are of the following form:

$$\mathbf{E}_r(\mathcal{N}) := \sup_{\tau\in\mathrm{FS}(:\overrightarrow{LA'}:\overrightarrow{RB}:)} \mathbf{E}_r(:\overrightarrow{LA}:\vec{R}:\vec{C}:)_{\mathcal{N}(\tau)}, \tag{3}$$

where $r = \mathrm{E}$ or $r = \mathrm{GE}$ (E and GE denote entanglement and genuine entanglement, respectively) and FS denotes the set of fully separable states (see Secs. IV A and IV B). Here, $\vec{L}, \vec{R}$ denote ancillary systems that are kept by the respective parties. For any partition $:\vec{X}:$, we have defined $\mathbf{E}_r$ as the divergence from the convex set $\mathbf{S}_E$ of fully separable or the convex set $\mathbf{S}_{\mathrm{GE}}$ of biseparable states, measured by some divergence $\mathbf{D}$:

$$\mathbf{E}_r(:\vec{X}:)_{\rho} := \inf_{\sigma\in\mathbf{S}_r(:\vec{X}:)} \mathbf{D}(\rho\|\sigma). \tag{4}$$

Our main results are the following upper bounds on secret-key-agreement capacities of a multiplex quantum channel, i.e., on the maximum rates at which multipartite private states can be obtained by using the channel as well as some free operations. In the one-shot case of a multiplex quantum channel with classical preprocessing and post-processing (cppp), we have the following weak converse result: For any fixed $\varepsilon \in (0, 1)$, the achievable region of cppp-assisted secret key agreement over a multiplex channel $\mathcal{N}$ satisfies

$$P^{(1,\varepsilon)}_{\mathrm{cppp}}(\mathcal{N}) \leq E^{\varepsilon}_{h,\mathrm{GE}}(\mathcal{N}), \tag{5}$$

where $E^{\varepsilon}_{h,\mathrm{GE}}(\mathcal{N})$ is the ε-hypothesis-testing relative entropy of genuine multipartite entanglement of the multiplex channel $\mathcal{N}$, which is based on the ε-hypothesis-testing divergence [65]. In the case of many channel uses, interleaved by LOCC, we can also show the following strong converse bound:

$$P_{\mathrm{LOCC}}(\mathcal{N}) \leq E_{\max,E}(\mathcal{N}), \tag{6}$$

where $E_{\max,E}(\mathcal{N})$ is the max-relative entropy of entanglement of the multiplex channel $\mathcal{N}$, which is based on the max-relative entropy [46]. In the case of finite-dimensional Hilbert spaces, we can also get a strong converse result in terms of the regularized relative entropy,

$$P_{\mathrm{LOCC}}(\mathcal{N}) \leq E^{\infty}_{R,E}(\mathcal{N}). \tag{7}$$

If $\mathcal{N}$ is teleportation-simulable [48,66]—i.e., it can be simulated by a resource state and an LOCC operation—the bounds on $P_{\mathrm{LOCC}}(\mathcal{N})$ reduce to the relative entropy of entanglement of the resource state. Our upper bounds on the secret-key-agreement capacities are also upper bounds on the multipartite quantum capacities, where our goal is to distill GHZ states.

Our technique allows us to compute upper bounds on the rates achievable in MDI-QKD scenarios. For instance, we consider a dual-rail scheme based on single photons [67] to determine bounds on the MDI-QKD rates for two users. In this case, the channels between the users and the relay station are describable by erasure channels $\mathcal{E}_i$. We obtain the MDI-QKD capacity

$$\tilde{P}_{\mathrm{LOCC}}(\mathcal{N}^{\mathrm{MDI},\mathcal{E}}_{\vec{A}\to\vec{Z}}) = q\eta_1\eta_2, \tag{8}$$

where η_i's are the parameters of the erasure channels connecting users to the relay station and q is the probability of success of the Bell measurement at the relay station (see Sec. VI D for a precise model of the MDI-QKD setup). Dependence on η_i allows us to consider the rate-distance trade-off. We also determine upper bounds on the maximum rates for the MDI-QKD setups, where the quantum channels from the users to the relay station are depolarizing and dephasing channels.

We also provide lower bounds on the secret-key-agreement rates of multiplex quantum channels that can be achieved by cppp. Our protocols are based on Devetak-Winter (DW) [68] and generalize the lower bound for multipartite states presented in Ref. [14], as well as the bound for point-to-point quantum channels presented in Ref. [69] to multiplex quantum channels. Our first lower bound is a direct extension of the result for states given in Ref. [14]. The idea is to choose a so-called distributing party that performs the (directed) DW protocol with all remaining parties. The achievable rate is then the worst-case DW rate achievable between the distributing party and any other party. Furthermore, we maximize over all choices for the distributing party. Our second protocol is a variation, where we have a directed chain of parties in which each party performs the DW protocol with the next party in the chain. The obtainable rate is given by the "weakest link," i.e., the lowest DW rate, in the chain, and we maximize over all possible permutations of the parties in the chain.

In the case of a bidirectional network, i.e., a network in which all nodes are connected with their neighbors by a product of point-to-point channels in opposite directions, we provide a tighter bound based on spanning trees. The idea is to find the lowest DW rate in a spanning tree among any pair of the parties and maximize this quantity among all spanning trees. We provide an example where this protocol achieves a higher rate than the previous ones and show that the lower bound can be computed with polynomial complexity.

Finally, we show that the techniques developed in previous sections can also be applied to upper bound the rates at which the conference key can be distilled from multipartite quantum states. In particular, we provide an upper bound on the one-shot distillable conference key in terms of the hypothesis-testing relative entropy with respect to biseparable states. Our bound reads

$$K^{(1,\varepsilon)}_{\mathrm{D}}(\rho) \leq E^{\varepsilon}_{h,\mathrm{GE}}(\rho). \tag{9}$$

Using a particular construction of biseparable states, we provide bounds on this quantity for a number of examples, such as (multiple copies of) GHZ and W states, as well as dephased or depolarized GHZ and W states. We also provide an upper bound on the asymptotic distillable conference key, which is given by the regularized relative entropy with respect to biseparable states,

$$K_D(\rho) \leq E^{\infty}_{\mathrm{GE}}(\rho), \tag{10}$$

which is a generalization of the bipartite bound given in Ref. [62].

A. Relation to prior works

We briefly sketch some of the major developments that provide upper bounds on the key distillation capacities from states or via an LOCC-assisted secret-key-agreement protocol over a quantum channel. We then compare our bounds on the SKA capacities with those mentioned in prior works.

Conditions and bounds on the distillable key of bipartite states were provided in Refs. [40,41,62]. The former is in terms of the relative entropy of entanglement [43,44], and the latter is in terms of the squashed entanglement [70] (cf. Refs. [71,72]). These results were generalized to the conference key in Refs. [14,73], respectively.

For an LOCC-assisted secret-key-agreement protocol over a point-to-point channel, Ref. [47] provides a weak converse bound in terms of the squashed entanglement, which is generalized to the distribution of bipartite and multipartite private states via broadcast channels in Ref. [55]. In the case of tele-covariant channels (see Sec. V C), Ref. [48] provides a weak converse bound and Ref. [49] a strong converse bound in terms of the relative entropy of entanglement. This bound has been generalized to the distribution of multiple pairs of bipartite private states via broadcast channels [54,56], as well as multiple-access and interference channels [54].

For arbitrary point-to-point channels, a strong converse bound in terms of the max-relative entropy of entanglement [46] is provided in Ref. [50]. Recently, another strong converse bound in terms of the regularized relative entropy was provided in Ref. [74]. For bidirectional channels,

strong converse bounds in terms of the max-relative entropy of entanglement, which reduce to the relative entropy of entanglement for tele-covariant channels, have been provided in Refs. [51–53].

In the case where the bipartite key is distributed between two parties using a quantum key repeater, bounds have been provided in Ref. [50] when quantum communication takes place over a point-to-point channel. Bounds on rates, at which bipartite and multipartite keys for networks of point-to-point or broadcast channels can be obtained, have been provided in Refs. [58–60,75,76] and [61], respectively. Also, bounds on the rates obtainable in key repeaters that are in terms of entanglement measures of the input states have been obtained in Refs. [57,77].

In an LOCC-assisted conference key agreement protocol, the use of a multiplex quantum channel is interleaved with LOCC among trusted parties. For this scenario, we derive strong converse bounds in terms of the max-relative entropy entanglement for arbitrary multiplex channels. In the case of finite channel dimensions, we also derive bounds in terms of the regularized relative entropy of entanglement. In the case of tele-covariant channels, we obtain bounds in terms of the relative entropy of entanglement. In general, our bounds are not comparable with the squashed entanglement bounds provided in Refs. [47,55]. We are able to retain the results of Refs. [48–50,74] when multiplex channels are assumed to be point-to-point channels. Our bounds in terms of the max-relative entropy are a direct generalization of the bounds on bidirectional channels presented in Refs. [51–53]; thus, we retain those results. By using the recent results in Ref. [74], we further provide bounds in terms of the regularized relative entropy of entanglement, which can provide an improvement.

Concerning quantum key repeaters as well as setups of MDI-QKD, upper bounds on the achievable key rates can be obtained from results bounding key rates achievable in quantum networks, e.g., the one presented in Ref. [60] and subsequently used in Ref. [78] or the ones presented in Refs. [50,58]. However, we note that by designing the right kind of multiplex channel, we can make more specific assumptions on the operations performed at the relay stations and thus obtain tighter bounds. For example, we could design a multiplex channel for a protocol that does not use a quantum memory at the relay station or that performs a particular imperfect measurement at the relay station. The bounds given in Refs. [50,58,60], on the other hand, would bound the key rates of a repeater or MDI-QKD setup by finding the weakest link between the nodes, i.e., only taking into consideration limitations arising from imperfect point-to-point channels linking Alice and Bob with the central relay station, while assuming unlimited quantum memory at the nodes as well as the possibility to perform perfect measurements, resulting in looser bounds. Hence, the bounds given in Refs. [50,58,60] basically reduce to the minimum of the capacities of the two point-to-point channels, whereas our bounds represent the limitation arising from both imperfect channels and imperfect node operations, which is an important factor when benchmarking experimental implementations.

As for conference key distillation from multipartite states, we provide tighter bounds than those presented in Ref. [14]. As a GHZ state is a special case of a multipartite private state, our bounds can also be applied to the distillation of GHZ states from any pure or mixed multipartite entangled state, both in the asymptotic and finite copies regimes. There are a number of results concerned with computing and bounding rates of multipartite entanglement transformation, including those in Refs. [79–87]. As an example, we consider the nonasymptotic distillation of a tripartite conference key from noisy and noiseless W states and compare our results with Ref. [80].

III. PRELIMINARIES

In this section, we introduce notations and review basic concepts and standard definitions to be used frequently in later sections.

A. Notations and definitions

We consider quantum systems associated with separable Hilbert spaces. We study both discrete and continuous variable quantum systems; therefore, the associated Hilbert spaces can be finite or infinite dimensional. For a composite quantum system AB in a state ρ_{AB}, the reduced state $\mathrm{Tr}_B[\rho_{AB}]$ of system A is denoted as ρ_A. We denote the identity operator as $\mathbb{1}$. Let $\vec{A}' \coloneqq \{A'_a\}_{a\in\mathcal{A}}$, $\vec{A} \coloneqq \{A_a\}_{a\in\mathcal{A}}$, $\vec{B} = \{B_b\}_{b\in\mathcal{B}}$, $\vec{C} = \{C_c\}_{c\in\mathcal{C}}$, $\vec{K} = \{K_i\}_{i=1}^{M}$ denote sets (compositions) of quantum systems, where $\mathcal{A}, \mathcal{B}, \mathcal{C}$ are finite sets of symbols such that $|\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}| = M$ for some natural number $M \geq 2$. We consider M trusted allies $\{\mathbf{X}_i\}_{i=1}^{M} \coloneqq \{\mathbf{A}_a\}_{a\in\mathcal{A}} \cup \{\mathbf{B}_b\}_{b\in\mathcal{B}} \cup \{\mathbf{C}_c\}_{c\in\mathcal{C}}$. Also, $\overrightarrow{LA}$ denotes the set $\{L_aA_a\}_{a\in\mathcal{A}}$, where L_a is a reference system of A_a held by $\mathbf{A}_a$, and the same follows for $\overrightarrow{RB}$, $\overrightarrow{PC}$, and $\overrightarrow{SK}$. A quantum state $\rho_{\vec{A}}$ denotes a joint state of a system formed by composition of all A_a. We use $:\vec{A}:$ to denote partition with respect to each system in the set $\vec{A}$ as they are held by separate entities, and the same follows for $:\overrightarrow{LA}:\overrightarrow{RB}:$. Each separate element in a set is held by a separate party, in general. For example, let us consider $\vec{A} = \{A_1, A_2, A_3\}$ for $|\mathcal{A}| = 3$; then, $\vec{A}$ also depicts the composite system $A_1A_2A_3$, and $:\vec{A}:$ denotes the partition $A_1:A_2:A_3$ between each subsystem A_a of $\vec{A}$. In a conference key agreement protocol, each pair K_i, S_i of key and shield systems belongs to the respective trusted party $\mathbf{X}_i$ fully secure from Eve, while all $A'_a, A_a, B_b, C_c, K_i, S_i$ are physically inaccessible to Eve.

Let $\Phi^{\mathrm{GHZ}}_{\vec{K}}$ denote an M-partite GHZ state and $\Phi^{+}_{\vec{L}|\vec{A}}$ an Einstein–Podolsky–Rosen (EPR) state [88], also called a

maximally entangled state, where maximal entanglement is between $\vec{L}$ and $\vec{A}$. It should be noted that $\Phi^{+}_{\vec{L}|\vec{A}} = \bigotimes_{a\in\mathcal{A}} \Phi^{+}_{L_a|A_a}$, where

$$\Phi^{+}_{L_a|A_a} = \frac{1}{d}\sum_{i,j=0}^{d-1} |i,i\rangle\langle j,j|_{L_aA_a} \tag{11}$$

for an orthonormal basis $\{|i\rangle\}_i$, where $d = \min\{|L_a|, |A_a|\}$. (Without loss of generality, one may assume an EPR state of an even-dimensional qudit system to be a tensor product of EPR states of qubit systems.)

A quantum channel $\mathcal{M}_{B\to C}$ is a completely positive, trace-preserving map that acts on trace-class operators defined on the Hilbert space $\mathcal{H}_B$ and uniquely maps them to trace-class operators defined on the Hilbert space $\mathcal{H}_C$. For a channel $\mathcal{M}_{A\to B}$ with A and B as input and output systems, its Choi state $J^{\mathcal{M}}_{LB}$ is equal to $\mathcal{M}(\Phi^{+}_{LA})$.

A measurement channel $\mathcal{M}_{A'\to AX}$ is a quantum instrument whose action is expressed as

$$\mathcal{M}_{A'\to AX}(\cdot) = \sum_x \mathcal{E}^x_{A'\to A}(\cdot)\otimes|x\rangle\langle x|_X, \tag{12}$$

where each $\mathcal{E}^x$ is a completely positive, trace-nonincreasing map such that $\mathcal{M}$ is a quantum channel and X is a classical register that stores measurement outcomes. A classical register (system) X can be represented with a set of orthogonal quantum states $\{|x\rangle\langle x|_X\}_{x\in\mathcal{X}}$ defined on the Hilbert space $\mathcal{H}_X$.

An LOCC channel $\mathcal{L}_{\vec{A'}\to\vec{B}}$ can be written as $\sum_{x\in\mathcal{X}}(\bigotimes_{y\in\mathcal{Y}} \mathcal{E}^{y,x}_{A'_y\to B_y})$, where $\vec{A'} = \{A'_y\}_y$ and $\vec{B} = \{B_y\}_y$ are sets of inputs and outputs, respectively, and $\{\mathcal{E}^{y,x}\}_x$ is a set of completely positive, trace-nonincreasing maps for each y such that $\mathcal{L}$ is a quantum channel (cf. Ref. [89]). A LOCC channel does not increase the value of entanglement monotones and is deemed as a free operation in the resource theory of entanglement [14,62,89].

A quantity is called a generalized divergence [90,91] if it satisfies the following monotonicity (data-processing) inequality for all density operators ρ and σ and quantum channels $\mathcal{N}$:

$$\mathbf{D}(\rho\|\sigma) \geq \mathbf{D}(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)). \tag{13}$$

Examples include the quantum relative entropy [92]

$$D(\rho\|\sigma) := \mathrm{Tr}[\rho\log_2(\rho-\sigma)], \tag{14}$$

for $\mathrm{supp}(\rho)\subseteq\mathrm{supp}(\sigma)$—otherwise it is ∞—as well as the sandwiched Rényi relative entropy [63,64], which is denoted as $\tilde{D}_\alpha(\rho\|\sigma)$ and defined for states ρ, σ, and $\forall\,\alpha\in(0,1)\cup(1,\infty)$ as

$$\tilde{D}_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\log_2\mathrm{Tr}[(\sigma^{(1-\alpha)/2\alpha}\rho\sigma^{(1-\alpha)/2\alpha})^\alpha], \tag{15}$$

but it is set to $+\infty$ for $\alpha\in(1,\infty)$ if $\mathrm{supp}(\rho)\not\subseteq\mathrm{supp}(\sigma)$. In the limit $\alpha\to1$, the sandwiched Rényi relative entropy converges to the quantum relative entropy; in the limit $\alpha\to\infty$, it converges to the max-relative entropy [64], which is defined as [46,93]

$$D_{\max}(\rho\|\sigma) := \inf\{\lambda\in\mathbb{R}:\rho\leq 2^\lambda\sigma\}, \tag{16}$$

and if $\mathrm{supp}(\rho)\not\subseteq\mathrm{supp}(\sigma)$, then $D_{\max}(\rho\|\sigma)=\infty$. Another generalized divergence is the ε-hypothesis-testing divergence [65,94], defined as

$$D^\varepsilon_h(\rho\|\sigma) := -\log_2\inf_{\Lambda:0\leq\Lambda\leq\mathbb{1}}\{\mathrm{Tr}[\Lambda\sigma]:\mathrm{Tr}[\Lambda\rho]\geq1-\varepsilon\}, \tag{17}$$

for $\varepsilon\in[0,1]$ and density operators ρ,σ. For a more detailed description and other examples of the generalized divergences like the trace distance $\|\rho-\sigma\|_1$ and negative of fidelity $-F(\rho,\sigma)$ and their properties, see the Appendix A.

B. Multiplex quantum channels

We now formally define a general form of network channel that encompasses all other known multiplex quantum channels possible in communication or information processing settings [see Fig. 1(a) and Appendix B]. To the best of our knowledge, there is not such a general form of network channel in the literature of quantum communication and computation.

Definition 1: Consider the multipartite quantum channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$, where each pair A'_a, A_a is held by a respective party $\mathbf{A}_a$ and each B_b, C_c are held by parties $\mathbf{B}_b$, $\mathbf{C}_c$, respectively. While $\mathbf{A}_a$ is both the sender and receiver to the channel, $\mathbf{B}_b$ is only a sender, and $\mathbf{C}_c$ is only a receiver to the channel. Such a quantum channel is referred to as the multiplex quantum channel. Any two different systems need not be of the same size, in general. The sets $\mathcal{A}$, $\mathcal{B}$, or $\mathcal{C}$ can be empty in such a way that there is at least one input to the channel and one output from the channel.

Definition 1 includes all scenarios depicted in Fig. 1 (see Appendix B). For example, for a point-to-point channel from Bob to Charlie the set $\mathcal{A}=\varnothing$ and the sets $\mathcal{B}$ and $\mathcal{C}$ are singleton sets.

Also, any physical box with quantum or classical inputs and quantum or classical outputs is a type of multiplex quantum channel. We may not have an exact description of what is going on inside the box except that the undergoing process is physical, i.e., described by quantum mechanics. Physical computational devices like a physical black box (oracle) and quantum circuit [95] are also examples of multiplex quantum channels.

C. Conference key and private states

There are two usual approaches to studying secret key distillation. A direct approach is to consider purifications of states where the purifying system is accessible to Eve and all allied parties are allowed to perform local operations and public communication (LOPC). In this approach, we have Eve and M allied parties. Another approach is to consider the private states defined below, where all allied parties perform LOCC. We need not consider Eve explicitly in the paradigm of private states, and it is assumed that purifications of states are accessible to Eve. Both approaches are known to be equivalent [40]. We discuss the equivalence of these two approaches in more detail in Sec. V.

We now review the properties of conference key states discussed in Ref. [14]. Conference key states are a multipartite generalization of the secret key shared between two parties.

Definition 2: A conference key state $\gamma^c_{\vec{K}E}$, with $|K_i| = K$ for all $i \in [M] \coloneqq 1, \ldots, M$, is defined as

$$\mathcal{D}_{K_1} \otimes \mathcal{D}_{K_2} \otimes \cdots \otimes \mathcal{D}_{K_M}(\gamma^c_{\vec{K}E}) \coloneqq \frac{1}{K}\sum_{k\in\mathcal{K}} |k\rangle\langle k|_{K_1} \otimes |k\rangle\langle k|_{K_2} \otimes \cdots \otimes |k\rangle\langle k|_{K_M} \otimes \sigma_E, \tag{18}$$

where σ_E is a state of the system E, which is accessible to an eavesdropper Eve, $\mathcal{D}(\cdot) = \sum_{k\in\mathcal{K}} |k\rangle\langle k|(\cdot)|k\rangle\langle k|$ is a projective measurement channel, and $\{|k\rangle_{K_i}\}_{k\in\mathcal{K}}$ forms an orthonormal basis for each $i \in [M]$.

A conference key state $\gamma^c_{\vec{K}E}$ has $\log_2 K$ secret bits (key) that are readily accessible.

A state $\rho_{\vec{K}E}$ is called an ε-approximate conference key state, for $\varepsilon \in [0, 1]$, if there exists a conference key state $\gamma^c_{\vec{K}E}$ such that [14]

$$F(\gamma^c_{\vec{K}E}, \rho_{\vec{K}E}) \geq 1 - \varepsilon. \tag{19}$$

Definition 3: A state $\gamma_{\overrightarrow{SM}}$, with $|K_i| = K$ for all $i \in [M]$, is called a (M-partite) private state if and only if

$$\gamma_{\overrightarrow{SK}} \coloneqq U^{\mathrm{tw}}_{\overrightarrow{SK}}(\Phi^{\mathrm{GHZ}}_{\vec{K}} \otimes \omega_{\vec{S}})(U^{\mathrm{tw}}_{\overrightarrow{SK}})^\dagger, \tag{20}$$

where $U^{\mathrm{tw}}_{\overrightarrow{SK}} \coloneqq \sum_{\vec{k}\in\mathcal{K}^{\times M}} |\vec{k}\rangle\langle\vec{k}|_{\vec{K}} \otimes U^{\vec{k}}_{\vec{S}}$ is called a twisting unitary operator for some unitary operator $U^{\vec{k}}_{\vec{S}}$ and ω is some density operator [14].

It should be noted that $\gamma_{\overrightarrow{SK}}$ has at least $\log_2 K$ secret (key) bits (see Ref. [62] for a discussion of when the private state has exactly $\log_2 K$ bits). Similar to a conference key state, a state $\rho_{\overrightarrow{SK}}$ is called an ε-approximate private state for $\varepsilon \in [0, 1]$ if there exists a private state $\gamma_{\overrightarrow{SK}}$ such that [14]

$$F(\gamma_{\overrightarrow{SK}}, \rho_{\overrightarrow{SK}}) \geq 1 - \varepsilon. \tag{21}$$

Any state extension (including purification) $\gamma_{\overrightarrow{SKE}}$ of such a private state (20) necessarily has the following form [14]:

$$\gamma_{\overrightarrow{SKE}} \coloneqq U^{\mathrm{tw}}_{\overrightarrow{SKE}}(\Phi_{\vec{K}} \otimes \omega_{\vec{S}E})(U^{\mathrm{tw}}_{\overrightarrow{SKE}})^\dagger, \tag{22}$$

where $\omega_{\vec{S}E}$ is a state extension of the density operator $\omega_{\vec{S}}$.

It follows from Theorem IV.1 of Ref. [14] that $F(\gamma^c_{\vec{K}E}, \rho_{\vec{K}E}) \geq 1 - \varepsilon$ implies $F(\gamma_{\overrightarrow{SK}}, \rho_{\overrightarrow{SK}}) \geq 1 - \varepsilon$, and the converse is also true; i.e., $F(\gamma_{\overrightarrow{SK}}, \rho_{\overrightarrow{SK}}) \geq 1 - \varepsilon$ implies $F(\gamma^c_{\vec{K}E}, \rho_{\vec{K}E}) \geq 1 - \varepsilon$.

It is known that all perfect private states have nonlocal correlations [96].

IV. ENTANGLEMENT AND PRIVACY TEST

This section introduces frameworks for the resource theories of multipartite entanglement for the multipartite quantum channels (see Refs. [51,53,97,98] for the discussion on bipartite channels).

A. Multipartite entanglement

Here, we provide a short overview of the relevant definitions. For a detailed review of the topic, see Ref. [99]. A pure n-partite state that can be written as a tensor product $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_m\rangle$ is called m-separable. If $m < n$, there are partitions of the set of all the parties into two, with respect to which the state is entangled. If $n = m$, the pure state is said to be fully separable. If there is no bipartition with respect to which the pure state is a product state, it is called genuinely n-partite entangled.

An arbitrary n-partite state is m-separable if it can be written as the following convex composition:

$$\rho_{m-\mathrm{sep}} = \sum_{x\in\mathcal{X}} p_X(x)|\psi^x_1\rangle\langle\psi^x_1| \otimes |\psi^x_2\rangle\langle\psi^x_2| \otimes \ldots \otimes |\psi^x_m\rangle\langle\psi^x_m|, \tag{23}$$

where $p_X(x)$ is a probability distribution. The m-separable states form a convex set. Note, however, that the subsystems with respect to which the elements of the decomposition have to be products can differ.

A mixed n-partite state is considered GME if any decomposition into pure states contains at least one genuinely n-partite entangled pure state; i.e., the state is not biseparable. Let a free set $\mathbf{F}(:\vec{A}:)$ denote the set of all fully separable and biseparable states of system $\vec{A}$ for $\mathbf{F} =$ FS and $\mathbf{F} =$ BS, respectively. Both the sets FS and BS are convex. We note that while FS is preserved under an LOCC operation and tensor product, BS is preserved under LOCC but not under the tensor product, i.e., $\rho^{(x)}_{\overrightarrow{A^{(x)}}} \in \mathrm{BS}(:\overrightarrow{A^{(x)}}:)$

for $x \in [2]$ but $\rho^{(1)} \otimes \rho^{(2)}$ need not belong to $\mathrm{BS}(:\overrightarrow{A^{(1)}A^{(2)}}:)$. We refer to biseparable quantum states whose biseparability is preserved under tensor products, i.e., $\rho^{(x)}_{\underrightarrow{A^{(x)}}} \in \mathrm{BS}(:\overrightarrow{A^{(x)}}:)$ and $\rho^{(1)} \otimes \ldots \otimes \rho^{(n)} \in \mathrm{BS}(:\overrightarrow{A^{(1)}\ldots A^{(n)}}:)$ for all $n \in \mathbb{N}$, as tensor-stable biseparable states.

B. Entanglement measures

It is pertinent to quantify the resourcefulness of states and channels. The bounds on the capacities that we obtain are in terms of these quantifiers. It is desirable for entanglement quantifiers to be non-negative, to attain their minimum for the free states (and separable channels, respectively), and to be monotone under the action of LOCC.

Definition 4: The generalized divergence of entanglement $\mathbf{E}_{\mathrm{E}}$ or GME $\mathbf{E}_{\mathrm{GE}}$ of an arbitrary state $\rho_{\vec{A}}$ is defined as [100]

$$\mathbf{E}_r(:\vec{A}:)_\rho := \inf_{\sigma \in \mathbf{F}(:\vec{A}:)} \mathbf{D}(\rho_{\vec{A}} \| \sigma_{\vec{A}}), \tag{24}$$

when $\mathbf{F} = \mathrm{FS}$ or $\mathbf{F} = \mathrm{BS}$ for $r = \mathrm{E}$ or $r = \mathrm{GE}$, respectively, where $\mathbf{D}(\rho\|\sigma)$ denotes the generalized divergence.

The following definition of the entanglement measure of a multiplex channel generalizes the notion of entangling power of bipartite quantum channels [101] (see also Refs. [51,53,102]).

Definition 5: The entangling power of a multiplex channel $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$ with respect to entanglement measure $\mathbf{E}_r$ [Eq. (24)] is defined as the maximum possible gain in the entanglement $\mathbf{E}_r$ when a quantum state is acted upon by the given channel $\mathcal{N}$,

$$\mathbf{E}^p_r(\mathcal{N}) := \sup_\rho [\mathbf{E}_r(:\overrightarrow{LA}:\vec{R}:\overrightarrow{PC}:)_{\mathcal{N}(\rho)} - \mathbf{E}_r(:\overrightarrow{LA'}:\overrightarrow{RB}:\vec{P}:)_\rho], \tag{25}$$

where optimization is over all possible input states $\rho_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}}$.

Another way to quantify the entanglement measure of a multiplex channel is the following (see Ref. [53] for the bidirectional channel).

Definition 6: The generalized divergence of entanglement $\mathbf{E}_{\mathrm{E}}(\mathcal{N})$ or GME $\mathbf{E}_{\mathrm{GE}}(\mathcal{N})$ of a multiplex channel $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$ is

$$\mathbf{E}_r(\mathcal{N}) := \sup_{\rho \in \mathrm{FS}(:\overrightarrow{LA'}:\overrightarrow{RB}:)} \mathbf{E}_r(:\overrightarrow{LA}:\vec{R}:\vec{C}:)_{\mathcal{N}(\rho)}, \tag{26}$$

for $r = \mathrm{E}$ or $r = \mathrm{GE}$, respectively, where $\mathbf{E}_r(:\vec{A}:)_\rho$ is defined in Eq. (24) and GME stands for genuinely multipartite entanglement.

For $r = \mathrm{E}$, the entanglement measure in Eq. (24) is called ε-hypothesis-testing relative entropy of entanglement $E^\varepsilon_{h,E}$, max-relative entropy of entanglement $E_{\max,E}$, sandwiched Rènyi relative entropy of entanglement $\tilde{E}_{\alpha,E}$, or relative entropy of entanglement E_E when the generalized divergence is the ε-hypothesis-testing relative entropy, max-relative entropy, sandwiched Rényi relative entropy, or relative entropy, respectively. For $r = \mathrm{GE}$, the entanglement measure in Eq. (24) is called ε-hypothesis-testing relative entropy of GME $E^\varepsilon_{h,\mathrm{GE}}$, max-relative entropy of GME $E_{\max,\mathrm{GE}}$, sandwiched Rènyi relative entropy of GME $\tilde{E}_{\alpha,\mathrm{GE}}$, or relative entropy of GME when the generalized divergence E_{GE} is the ε-hypothesis-testing relative entropy, max-relative entropy, sandwiched Rényi relative entropy, or relative entropy, respectively. We follow the same procedure for the nomenclature of entanglement measures of channels.

We note that the sets FS, BS are convex. Using the data-processed triangle inequality [50] and the argument from the proof of Proposition 2 in Ref. [51], we arrive at the following lemma.

Lemma 1: The entangling power of a multiplex channel $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$ with respect to the max-relative entropy of entanglement $E_{\max,E}$ is equal to the max-relative entropy of entanglement of the channel $\mathcal{N}$,

$$E^p_{\max,E}(\mathcal{N}) = E_{\max,E}(\mathcal{N}). \tag{27}$$

Using a recent result on relative entropies [103], we can also obtain a result for the relative entropy of entanglement. Let us first define the regularized relative entropy of entanglement of a multiplex channel $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$ as

$$E^\infty_R(\mathcal{N}) := \inf_{\Lambda \in \mathrm{LOCC}} D^\infty(\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}} \| \Lambda_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}), \tag{28}$$

where $D^\infty(\mathcal{N}\|\mathcal{M}) := \lim_{n\to\infty}(1/n) D(\mathcal{N}^{\otimes n}\|\mathcal{M}^{\otimes n})$ and

$$D(\mathcal{N}\|\mathcal{M}) := \max_{\phi_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}}} D(\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}(\phi) \| \mathcal{M}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}(\phi)), \tag{29}$$

where $L \simeq A'$, $R \simeq B$ and $P \simeq C$. We now show the following relation between the regularized relative entropy of entanglement and the relative entropy of entanglement.

Lemma 2: For finite-dimensional Hilbert spaces, the entangling power of a multiplex channel $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$ with respect to the relative entropy of entanglement E_E is less than or equal to the regularized relative entropy of entanglement of the channel $\mathcal{N}$,

$$E^p_E(\mathcal{N}) \le E^\infty_E(\mathcal{N}). \tag{30}$$

Proof.—Let $\rho_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}}$ be a state and let $\sigma' \in \mathrm{FS}(:\overrightarrow{LA'}:\overrightarrow{RB}:\vec{P}:)$. Let $\Lambda_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$ be an LOCC channel. Then, the following inequality holds:

$$E_E(:\overrightarrow{LA}:\vec{R}:\overrightarrow{PC}:)_{\mathcal{N}(\rho)} \leq D\left(\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}(\rho_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}})\|\Lambda_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}(\sigma'_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}})\right). \quad (31)$$

Applying the chain rule from Ref. [103], we find that

$$D\left(\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}(\rho_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}})\|\Lambda_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}(\sigma'_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}})\right) \leq D\left(\rho_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}}\|\sigma'_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}}\right) + D^{\infty}(\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}\|\Lambda_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}).$$

Since the above holds for arbitrary, fully separable states $\sigma'_{\overrightarrow{LA'}\overrightarrow{RB}\vec{P}}$ and arbitrary LOCC channels $\Lambda_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$, we arrive at

$$E_E(:\overrightarrow{LA}:\vec{R}:\overrightarrow{PC}:)_{\mathcal{N}(\rho)} \leq E_E(:\overrightarrow{LA'}:\overrightarrow{RB}:\vec{P}:)_{\rho} + E_E^{\infty}(\mathcal{N}), \quad (32)$$

finishing the proof. ∎

Remark 1: It suffices to optimize $E^{\varepsilon}_{h,E}(\mathcal{N})$, $E^{\varepsilon}_{h,\mathrm{GE}}(\mathcal{N})$, $E_{\max,E}(\mathcal{N})$, $E_{E,E}(\mathcal{N})$, and $E_{\max,\mathrm{GE}}(\mathcal{N})$ of a multiplex channel $\mathcal{N}$ over all pure input states; i.e., $\rho \in \mathrm{FS}(:\overrightarrow{LA'}:\overrightarrow{RB}:)$ is a pure state in Eq. (26) for $E^{\varepsilon}_{h,E}(\mathcal{N})$, $E^{\varepsilon}_{h,\mathrm{GE}}(\mathcal{N})$, $E_{\max,E}(\mathcal{N})$, $E_{E,E}(\mathcal{N})$, $E_{\max,\mathrm{GE}}(\mathcal{N})$. This reduction follows from the quasiconvexity of the max-relative entropy [93] and ε-hypothesis-testing relative entropy [104], as well as the convexity of the relative entropy of entanglement [44]. Namely, the maximum of a (quasi)convex function over a convex set will be attained on a boundary point. The boundary points of the set of fully separable density matrices are given by the fully separable pure states.

C. Multipartite privacy test

A γ-privacy test corresponding to $\gamma_{\overrightarrow{SK}}$ is defined as the dichotomic measurement [49] $\{\Pi^{\gamma}_{\overrightarrow{SK}}, \mathbb{1} - \Pi^{\gamma}_{\overrightarrow{SK}}\}$, where $\Pi^{\gamma}_{\overrightarrow{SK}} \coloneqq U^{\mathrm{tw}}_{\overrightarrow{SK}}(\Phi_{\vec{K}} \otimes \mathbb{1}_{\vec{S}})(U^{\mathrm{tw}}_{\overrightarrow{SK}})^{\dagger}$.

Using the properties of fidelity and form of the test measurement, we arrive at the following proposition.

Proposition 1: If a state $\rho_{\overrightarrow{SK}}$ is ε approximate to $\gamma_{\overrightarrow{SK}}$, i.e., $F(\rho_{\overrightarrow{SK}}, \gamma_{\overrightarrow{SK}}) \geq 1 - \varepsilon$, then $\rho_{\overrightarrow{KS}}$ passes the γ-privacy test with success probability $1 - \varepsilon$, i.e.,

$$\mathrm{Tr}[\Pi^{\gamma}_{\overrightarrow{SK}}\rho_{\overrightarrow{SK}}] \geq 1 - \varepsilon. \quad (33)$$

Proof.—

$$\mathrm{Tr}[\Pi^{\gamma}_{\overrightarrow{SK}}\rho_{\overrightarrow{SK}}] = \langle\Phi^{\mathrm{GHZ}}|_{\vec{K}}\mathrm{Tr}_{\vec{S}}[(U^{\mathrm{tw}}_{\overrightarrow{SK}})^{\dagger}\rho_{\overrightarrow{SK}}U^{\mathrm{tw}}_{\overrightarrow{SK}}]|\Phi^{\mathrm{GHZ}}\rangle_{\vec{K}} \quad (34)$$

$$= F(\Phi^{\mathrm{GHZ}}_{\vec{K}}, \mathrm{Tr}_{\vec{S}}[(U^{\mathrm{tw}}_{\overrightarrow{SK}})^{\dagger}\rho_{\overrightarrow{SK}}U^{\mathrm{tw}}_{K_1\ldots K_M S_1\ldots S_M}]) \quad (35)$$

$$\geq F(\Phi^{\mathrm{GHZ}}_{\vec{K}} \otimes \omega_{\vec{S}}, (U^{\mathrm{tw}}_{\overrightarrow{SK}})^{\dagger}\rho_{\overrightarrow{SK}}U^{\mathrm{tw}}_{\overrightarrow{SK}}) \quad (36)$$

$$= F(U^{\mathrm{tw}}_{\overrightarrow{SK}}\Phi^{\mathrm{GHZ}}_{\vec{K}} \otimes \omega_{\vec{S}}(U^{\mathrm{tw}}_{\overrightarrow{SK}})^{\dagger}, \rho_{\overrightarrow{SK}}) \quad (37)$$

$$= F(\gamma_{\overrightarrow{SK}}, \rho_{\overrightarrow{SK}}) \geq 1 - \varepsilon. \quad (38)$$

∎

We employ proof arguments similar to the bipartite case of Eq. (281) in Ref. [62] to arrive at the following theorem, which implies that all private states are necessarily GME states. This is a strict generalization of Eq. (281) in Ref. [62], as a direct generalization would be the same statement for fully separable states instead of biseparable states (cf. Ref. [14]). See Appendix C for the proof.

Theorem 1: A biseparable state $\sigma_{\overrightarrow{SK}} \in \mathrm{BS}(:SK:)$ can never pass any γ-privacy test with probability greater than $1/K$, i.e.,

$$\mathrm{Tr}[\Pi^{\gamma}_{\overrightarrow{SK}}\sigma_{\overrightarrow{SK}}] \leq \frac{1}{K}. \quad (39)$$

V. CONFERENCE KEY AGREEMENT PROTOCOL

In this section, we give a formal description of a secret-key-agreement protocol for multiple trusted parties, i.e., a conference key agreement protocol.

We consider an LOCC-assisted secret-key-agreement protocol among M trusted allies $\{\mathbf{X}_i\}_{i=1}^{M}$ over a multiplex quantum channel $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$, where each pair A'_a, A_a is held by trusted party $\mathbf{A}_a$ and each B_b, C_c is held by trusted parties $\mathbf{B}_b$, $\mathbf{C}_c$, respectively. The environment part E of an isometric extension $U^{\mathcal{N}}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}E}$ of the channel $\mathcal{N}$ is accessible to Eve, along with all classical information communicated among $\mathbf{X}_i$ while performing LOCC. All other quantum systems that are locally available to $\mathbf{X}_i$ are said to be secure from Eve; i.e., even if local operations during LOCC are noisy, purifying quantum systems are still within labs of trusted allies, which are off limits for Eve. This assumption is justifiable because $\mathbf{X}_i$'s can always abandon performing local operations that would leak information to Eve. In an LOCC-assisted protocol, the uses of the multiplex channel $\mathcal{N}$ are interleaved with LOCC channels.

In the first round, all $\mathbf{X}_i$ perform LOCC $\mathcal{L}^1$ to generate a state $\rho_1 \in \mathrm{FS}(:\overrightarrow{L^{(1)}A^{(1)'}}:\overrightarrow{R^{(1)}B^{(1)}}:\overrightarrow{P^{(1)}})$. All $\mathbf{A}_a$ and $\mathbf{B}_b$ input respective systems to multiplex channel $\mathcal{N}^1_{\overrightarrow{A^{(1)'}}\overrightarrow{B^{(1)}}\to\overrightarrow{C^{(1)}}}$ and let $\tau_1 := \mathcal{N}^1(\rho)$ be the output state after the first use $\mathcal{N}^1$ of the multiplex channel. In the second round, an LOCC $\mathcal{L}^2$ is performed on τ_1, and then, the second use $\mathcal{N}^2$ of the multiplex channel is employed on $\rho_2 := \mathcal{L}^2(\tau_1)$. In the third round, an LOCC $\mathcal{L}^3$ is performed on $\tau_2 := \mathcal{N}^2(\rho_2)$, and then, the third use $\mathcal{N}^3$ of the multiplex channel is employed on $\rho_3 := \mathcal{L}^3(\tau_2)$. Successively, we continue this procedure for n rounds, where an $\mathcal{L}$ acts on the output state of the previous round, after which the multiplex channel is performed on the resultant state. Finally, after the nth round, an LOCC $\mathcal{L}^{n+1}$ is performed as a decoding channel, which generates the final state $\omega_{\overrightarrow{SK}}$.

It can be concluded from the equivalence between private states and CK states that any protocol of the above form can be purified, i.e., by considering isometric extensions of all channels (LOCC and $\mathcal{N}$) (the proof arguments are the same as for the purified protocol for LOCC-assisted secret key agreement [51]). At the end of the purified protocol, Eve possesses all the environment systems E^n from isometric extension $U^{\mathcal{N}}$ of each use of the multiplex channel $\mathcal{N}$ along with coherent copies Y^{n+1} of the classical data exchanged among trusted parties $\mathbf{X}_i$ during performances of $n+1$ LOCC channels, whereas each trusted party $\mathbf{X}_i$ possesses the key system K_i and the shield system S_i, which consist of all local reference systems, after the action of the decoder. The state at the end of the protocol is a pure state $\omega_{\overrightarrow{SKY^{n+1}E^n}}$ with $F(\gamma_{\overrightarrow{SK}}, \omega_{\overrightarrow{SK}}) \geq 1-\varepsilon$. Such a protocol is called an (n, K, ε) LOCC-assisted secret-key-agreement protocol. The rate P of a given (n, K, ε) protocol is equal to the number of conference (secret) bits generated per channel use:

$$P := \frac{1}{n}\log_2 K. \tag{40}$$

A rate P is achievable if for $\varepsilon \in (0,1), \delta > 0$, and sufficiently large n, there exists an $(n, 2^{n(P-\delta)}, \varepsilon)$ LOCC-assisted secret-key-agreement protocol. The LOCC-assisted secret-key-agreement capacity $\hat{P}_{\mathrm{LOCC}}(\mathcal{N})$ of a multiplex quantum channel $\mathcal{N}$ is defined as the supremum of all achievable rates.

A rate P is called a strong converse rate for LOCC-assisted secret key agreement if for all $\varepsilon \in [0,1), \delta > 0$, and sufficiently large n, there does not exist an $(n, 2^{n(P+\delta)}, \varepsilon)$ LOCC-assisted secret-key-agreement protocol. The strong converse LOCC-assisted secret-key-agreement capacity $\tilde{P}_{\mathrm{LOCC}}(\mathcal{N})$ is defined as the infimum of all strong converse rates.

The following inequality is a direct consequence of the definitions:

$$\hat{P}_{\mathrm{LOCC}}(\mathcal{N}) \leq \tilde{P}_{\mathrm{LOCC}}(\mathcal{N}). \tag{41}$$

We can also consider the whole development discussed above for conference key agreement assisted only by cppp communication; i.e., all parties are allowed only two LOCC channels, one for encoding and the other for decoding. A (n, K, ε) cppp-assisted secret-key-agreement protocol over $\mathcal{N}$ is the same as a $(1, K, \varepsilon)$ LOCC-assisted secret-key-agreement protocol over channel $\mathcal{N}^{\otimes n}$, and for $n = 1$, both protocols are the same. The cppp-assisted secret-key-agreement capacity $\hat{P}_{\mathrm{cppp}}$ of the channel $\mathcal{N}$ is always less than or equal to $\hat{P}_{\mathrm{LOCC}}$,

$$\hat{P}_{\mathrm{cppp}}(\mathcal{N}) \leq \hat{P}_{\mathrm{LOCC}}(\mathcal{N}). \tag{42}$$

Let $\hat{P}^{\mathcal{N}}_{\mathrm{cppp}}(n, \varepsilon)$ be the maximum rate such that $(n, 2^{nP}, \varepsilon)$ cppp-assisted secret key agreement is achievable for any given $\mathcal{N}$.

Remark 2: It should be noted that the maximum rate at which secret keys can be distilled using the LOCC- or cppp-assisted protocol over a multiplex channel $\mathcal{N}$ is never less than the maximum rate at which the GHZ state can be distilled using the LOCC- or cppp-assisted protocol over a given channel $\mathcal{N}$, respectively. This statement holds because the GHZ state is a special private state from which secret bits are readily accessible to trusted allies.

Remark 3: Different physical constraints can be invoked in communication protocols to define constrained protocols and associated capacities. For instance, we can invoke energy constraints on input states and detectors to get energy-constrained protocols and respective capacities (cf. Refs. [105,106]).

A. Privacy from a single use of a multiplex channel

Let $\hat{P}^{\mathcal{N}}_{\mathrm{cppp}}(n, \varepsilon)$ denote the maximum rate P such that the (n, K, ε) conference key agreement protocol is achievable for any $\mathcal{N}$ using cppp. The following bound holds for the one-shot secret-key-agreement rate of a multiplex quantum channel $\mathcal{N}$ (see Appendix D 1 for the proof).

Theorem 2: For any fixed $\varepsilon \in (0,1)$, the achievable region of cppp-assisted secret key agreement over a single use of the multiplex channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ satisfies

$$\hat{P}^{\mathcal{N}}_{\mathrm{cppp}}(1, \varepsilon) \leq E^{\varepsilon}_{h,\mathrm{GE}}(\mathcal{N}), \tag{43}$$

where

$$E^{\varepsilon}_{h,\mathrm{GE}}(\mathcal{N}) \coloneqq \sup_{\psi\in \mathrm{FS}(:\overrightarrow{LA'}:\overrightarrow{RB}:)} \inf_{\sigma\in \mathrm{BS}(:\overrightarrow{LA}:\vec{R}:\vec{C}:)} D^{\varepsilon}_{h}(\mathcal{N}(\psi)\|\sigma) \tag{44}$$

is the ε-hypothesis-testing relative entropy of genuine entanglement of the multiplex channel $\mathcal{N}$. It suffices to optimize over pure input states $\psi \in \mathrm{FS}(:\overrightarrow{LA'}:\overrightarrow{RB}:)$.

We can conclude from the above theorem that

$$\hat{P}^{\mathcal{N}}_{\mathrm{cppp}}(n,\varepsilon) \leq \frac{1}{n} E^{\varepsilon}_{h,\mathrm{GE}}(\mathcal{N}^{\otimes n}), \tag{45}$$

which leads to the following corollaries.

Corollary 1: A weak converse bound on the cppp-assisted secret-key-agreement capacity of a multiplex channel $\mathcal{N}$ is given by

$$\hat{P}_{\mathrm{cppp}}(\mathcal{N}) = \inf_{\varepsilon\in(0,1)} \liminf_{n\to\infty} \hat{P}^{\mathcal{N}}_{\mathrm{cppp}}(n,\varepsilon) \tag{46}$$

$$\leq E^{\infty}_{\mathrm{GE}}(\mathcal{N}). \tag{47}$$

Corollary 2: Consider a class of multiplex channels $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ such that for all pure input states $\psi \in \mathrm{FS}(\overrightarrow{LA'}:\overrightarrow{RB}:\vec{P})$, the output states $\mathcal{N}(\psi)$ are tensor-stable biseparable states with respect to the partition $\overrightarrow{LA}:\overrightarrow{RB}:\overrightarrow{PC}$. The cppp-assisted secret-key-agreement capacities for such a class of multiplex channels are zero.

B. Strong converse bounds on LOCC-assisted private capacity of multiplex channel

We now derive converse and strong converse bounds on an LOCC-assisted secret-key-agreement protocol over a multiplex channel $\mathcal{N}$.

For an LOCC-assisted secret-key-agreement protocol, by employing Theorem 1 and generalizing the proof arguments of Theorem 2 in Ref. [51] (see also Ref. [50]) to the multiplex scenario, we get the following converse bound (proof in Appendix D 2).

Theorem 3: For a fixed $n, K \in \mathbb{N}, \varepsilon \in (0,1)$, the following bound holds for an (n,K,ε) protocol for LOCC-assisted secret key agreement over a multiplex $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$:

$$\frac{1}{n}\log_2 K \leq E_{\max,E}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right), \tag{48}$$

where the max-relative entropy of entanglement $E_{\max,E}(\mathcal{N})$ of the multiplex channel $\mathcal{N}$ is

$$E_{\max,E}(\mathcal{N}) \coloneqq \sup_{\psi\in \mathrm{FS}(:\overrightarrow{LA'}:\overrightarrow{RB}:)} \inf_{\sigma\in \mathrm{FS}(:\overrightarrow{LA}:\vec{R}:\vec{C}:)} D_{\max}(\mathcal{N}(\psi)\|\sigma)$$

and it suffices to optimize over pure states ψ.

Remark 4: The bound in Eq. (48) can also be rewritten as

$$1-\varepsilon \leq 2^{-n(P-E_{\max,E}(\mathcal{N}))}, \tag{49}$$

where we have $P = (1/n)\log_2 K$. Thus, if the secret-key-agreement rate P is strictly greater than the max-relative entropy of entanglement $E_{\max,E}(\mathcal{N})$ of the (multiplex) channel $\mathcal{N}$, then the fidelity of the distillation $(1-\varepsilon)$ decays exponentially fast to zero in the number of channel uses.

An immediate corollary of the above remark is the following strong converse statement.

Corollary 3: The strong converse LOCC-assisted secret-key-agreement capacity of a multiplex channel $\mathcal{N}$ is bounded from above by its max-relative entropy of entanglement:

$$\tilde{P}_{\mathrm{LOCC}}(\mathcal{N}) \leq E_{\max,E}(\mathcal{N}). \tag{50}$$

We also have another upper bound on the private capacity of a multiplex channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ with finite-dimensional input and output systems in terms of the regularized relative entropy instead of the max-relative entropy (proof in Appendix D 3).

Theorem 4: For finite Hilbert space dimensions, the asymptotic LOCC-assisted secret-key-agreement capacity of a multiplex channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ is bounded by its regularized relative entropy of entanglement:

$$\tilde{\mathcal{P}}_{\mathrm{LOCC}}(\mathcal{N}) \leq E^{\infty}_{E}(\mathcal{N}). \tag{51}$$

C. Teleportation-simulable and tele-covariant multiplex channels

For a class of multipartite quantum channels obeying certain symmetries, such as teleportation-simulability [66], the LOCC assistance does not enhance secret-key-agreement capacity, and the original protocol can be reduced to a cppp-assisted secret-key-agreement protocol. This observation for secret communication between two parties over the point-to-point teleportation-simulable channel was first made in Ref. [48].

Definition 7: A multipartite quantum channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ is teleportation simulable with the associated resource state $\theta_{\overrightarrow{LA}\vec{R}\vec{C}}$, where $R_b \simeq B_b$ for all $b \in \mathcal{B}$ and $L_a \simeq A'_a$ for all $a \in \mathcal{A}$, if for all input states $\rho_{\vec{A'}\vec{B}}$ the following identity holds:

$$\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}(\rho_{\vec{A'}\vec{B}}) = \mathcal{T}_{\overrightarrow{A'LA}\,\overrightarrow{\mathrm{BR}}\vec{C}\to\vec{A}\vec{C}}(\rho_{\vec{A'}\vec{B}}\otimes\theta_{\overrightarrow{LA}\vec{R}\vec{C}}) \quad (52)$$

for some LOCC channel $\mathcal{T}$ with input partition $:\overrightarrow{A'LA}:\overrightarrow{\mathrm{BR}}:\vec{C}:$ and output partition $:\vec{A}:\vec{C}:$.

Covariant channels.—For each $a\in\mathcal{A}$ and $b\in\mathcal{B}$, let $\mathcal{G}_a$ and $\mathcal{G}_b$ be finite groups of respective sizes G_a and G_b with respective unitary representations $g_a\to U_{A'_a}(g_a)$ and $g_b\to U_{B_b}(g_b)$ for all group elements g_a and g_b. Let $W^{\vec{g}}_{A_a}$ and $W^{\vec{g}}_{C_c}$ be unitary representations for all $a\in\mathcal{A}$ and $c\in\mathcal{C}$, where $\vec{g}=\{g_a,g_b\}_{a,b}$. A multiplex quantum channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ is *covariant* with respect to these representations if the following relation holds for all input states $\rho_{\vec{A'}\vec{B}}$ and group elements $g_a\in\mathcal{G}_a$ and $g_b\in\mathcal{G}_b$ for all $a\in\mathcal{A}$ and $b\in\mathcal{B}$:

$$\begin{aligned}&\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}\Big(\Big(\bigotimes_{a\in\mathcal{A}}\mathcal{U}^{g_a}_{A'_a}\otimes\bigotimes_{b\in\mathcal{B}}\mathcal{U}^{g_b}_{B_b}\Big)(\rho_{\vec{A'}\vec{B}})\Big)\\&\quad=\Big(\bigotimes_{a\in\mathcal{A}}\mathcal{W}^{\vec{g}}_{A_a}\otimes\bigotimes_{c\in\mathcal{C}}\mathcal{W}^{\vec{g}}_{C_c}\Big)\big(\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}(\rho_{\vec{A'}\vec{B}})\big),\end{aligned} \quad (53)$$

where we have used the notation $\mathcal{U}(\cdot):=U(\cdot)U^\dagger$ for unitaries U.

Definition 24: A quantum channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ is called tele-covariant if it is covariant with respect to groups $\{\mathcal{G}_a\}_{a\in\mathcal{A}}$ and $\{\mathcal{G}_b\}_{b\in\mathcal{B}}$ that have representations as unitary one-designs; i.e., for all $a\in\mathcal{A}$ and $b\in\mathcal{B}$ as well as states $\rho_{A'_a}$ and ρ_{B_b}, it holds that $(1/G_a)\sum_{g_a\in\mathcal{G}_a}\mathcal{U}^{g_a}_{A'_a}(\rho_{A'_a})=\mathbb{1}/|A_a|$ and $(1/G_b)\sum_{g_b\in\mathcal{G}_b}\mathcal{U}^{g_b}_{B_b}(\rho_{B_b})=\mathbb{1}/|B_b|$, respectively.

The following observation follows from the definition of tele-covariant channels.

Remark 5: Tele-covariance of a channel is with respect to the groups and their unitary representations on the input and output Hilbert spaces of the channel. If associated unitary representations for the tele-covariant channels $\mathcal{N}^1$ and $\mathcal{N}^2$ are, respectively, the same on the output Hilbert spaces of $\mathcal{N}^1$ that are also the input Hilbert spaces for $\mathcal{N}^2$, then the composition channel $\mathcal{N}=\mathcal{N}^2\circ\mathcal{N}^1$ is also tele-covariant.

A quantum channel obtained by the tensor product (superoperation "⊗," which physically means parallel uses) of tele-covariant channels is also a tele-covariant channel.

The following theorem generalizes the developments in Refs. [51,107–109] (see Appendix D 4 for the proof):

Theorem 5: If a multipartite channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ is tele-covariant, then it is teleportation-simulable with resource state (52) as its Choi state, i.e., $\theta_{\overrightarrow{LA}\vec{R}\vec{C}}=\mathcal{N}(\Phi^+_{\vec{L}\vec{R}|\vec{A'}\vec{B}})$.

Following the approach in Refs. [48,62], we obtain the following theorem:

Theorem 6: The LOCC-assisted secret-key-agreement capacity of a multiplex quantum channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$, which is teleportation-simulable with resource state $\theta_{\overrightarrow{LA}\vec{R}\vec{C}}$, is upper bounded as

$$\hat{P}_{\mathrm{LOCC}}(\mathcal{N})\le E^{\infty}_{\mathrm{GE}}(:\overrightarrow{LA}:\vec{R}:\vec{C}:)_\theta, \quad (54)$$

where $E^\infty(:\vec{A}:)_\rho$ is the regularized relative entropy of entanglement of state $\rho_{\vec{A}}$.

For the proof, see Appendix D 4. Using the above theorem, we immediately get the following.

Corollary 4: For a multiplex quantum channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$, which is teleportation-simulable with a tensor-stable biseparable resource state, it holds that $\hat{P}_{\mathrm{LOCC}}(\mathcal{N})=0$.

Let us note that unlike in Refs. [48,62], which deals with the bipartite relative entropy of entanglement, we do not trivially get a nonregularized bound, which is due to the fact that the definition of biseparability is not tensor stable. If we consider the relative entropy of entanglement with respect to fully separable states, however, we can employ the proof argument of Theorem 4 in Ref. [51] and arrive at the following theorem:

Theorem 7: For a fixed $n,K\in\mathbb{N},\varepsilon\in(0,1)$, the following bound holds for an (n,M,ε) protocol for LOCC-assisted secret key agreement over a multiplex teleportation-simulable quantum channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ with the associated resource state $\theta_{\overrightarrow{LA}\vec{R}\vec{C}}$, $\forall\,\alpha>1$,

$$\frac{1}{n}\log_2 K\le\tilde{E}_{\alpha,E}(:\overrightarrow{LA}:\vec{R}:\vec{C}:)_\theta+\frac{\alpha}{n(\alpha-1)}\log_2\left(\frac{1}{1-\varepsilon}\right). \quad (55)$$

For the proof, see Appendix D 4. Setting $\alpha=1+(1/\sqrt{n})$ and letting $n\to\infty$, we obtain the following:

Corollary 5: The LOCC-assisted secret-key-agreement capacity of a multiplex channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$, which is teleportation-simulable with the resource state $\theta_{\overrightarrow{LA}\vec{R}\vec{C}}$, is upper bounded as

$$\hat{P}_{\mathrm{LOCC}}(\mathcal{N})\le E_E(:\overrightarrow{LA}:\vec{R}:\vec{C}:)_\theta, \quad (56)$$

where $E(:\vec{A}:)_\rho$ is the relative entropy of entanglement of state $\rho_{\vec{A}}$; this bound is also a strong converse bound.

VI. APPLICATION TO OTHER PROTOCOLS

In this section, we exploit the general nature of an LOCC-assisted secret-key-agreement protocol over a multiplex quantum channel. We derive upper bounds on the rates for two-party and conference key distribution for a number of seemingly different protocols that are of wide interest. Such seemingly different quantum key distribution and conference key agreement protocols can be shown to be special types of LOCC-assisted secret-key-agreement protocol over some particular multiplex quantum channels. In particular, we identify protocols like measurement-device-independent quantum key distribution, both in the

bipartite [27,28] and conference setting [30,110,111], as well as for quantum key repeaters, i.e., generalized quantum repeaters with the goal of distributing private states [50,57,77] to be special types of LOCC-assisted secret-key-agreement protocol over some particular multiplex quantum channels. We are able to derive upper bounds on the rates achieved in these protocols by exploiting our results in the previous section. Furthermore, as EPR or GHZ states are special cases of bipartite or multipartite private states, respectively, the same holds for LOCC-assisted quantum communication protocols, where the goal is to distill EPR or GHZ states. By providing a unified approach to such a diverse class of private communication setup, we contribute to a better understanding of limitations on respective protocols. These limitations provide benchmarks on experimental realizations of private communication protocols.

A. Measurement-device-independent QKD

Measurement-device-independent (MDI) QKD is a form of QKD, where the honest parties, Alice and Bob, trust their state preparation but do not trust the detectors [27,28]. In a typical setup of MDI-QKD, such as the ones described in Refs. [27,28], Alice and Bob locally prepare states that they send to a relay station, which might be in the hands of Eve, using channels $\mathcal{N}^1_{A'\to A}$ and $\mathcal{N}^2_{B'\to B}$. At the relay station, a joint measurement of the systems AB is performed, e.g., in the Bell basis, the results of which are classical values that are then communicated to Alice and Bob. Alice and Bob use the relay many times and perform classical postprocessing.

A way to incorporate such protocols in our scenario is to identify Alice and Bob as two trusted parties and include the measurement performed by the relay, as well as channels $\mathcal{N}^{1,2}$, into a bipartite quantum-classical (qc) channel

$$\mathcal{N}^{\mathrm{MDI}}_{A'B'\to Z_A Z_B} \coloneqq \mathcal{B}_{X\to Z_A Z_B}\circ\mathcal{M}_{AB\to X}\circ\mathcal{N}^1_{A'\to A}\otimes\mathcal{N}^2_{B'\to B}, \quad (57)$$

where $\mathcal{M}_{AB\to x}$ is the quantum instrument (channel) performing a POVM $\{\Lambda^x\}_x$ and writing the output x into a classical register X and $\mathcal{B}_{X\to Z_A Z_B}$ a classical broadcast channel sending input x to Z_A and Z_B. Registers Z_A and Z_B are received by Alice and Bob, respectively. The channel $\mathcal{N}^{\mathrm{MDI}}_{A'B'\to Z_A Z_B}$ is a multiplex channel that is a composition of multiplex channels (see Fig. 2).

Application of Theorem 3 for arbitrary systems and Theorem 4 for finite-dimensional systems (as well as the results of Ref. [51–53]) then provides bounds on the achievable key rate in terms of $E_{\max,E}(\mathcal{N}^{\mathrm{MDI}}_{A'B'\to Z_A Z_B})$ and $E^{\infty}_{E}(\mathcal{N}^{\mathrm{MDI}}_{A'B'\to Z_A Z_B})$, respectively, which can be seen as measures of the entangling capabilities of the measurement $\{\Lambda^x\}_x$. The multiplex quantum channel $\mathcal{N}^{\mathrm{MDI}}_{A'B'\to Z_A Z_B}$ is tele-covariant if $\mathcal{N}_{1,2}$ as well as $\mathcal{M}$ are tele-covariant, and the bound reduces to the relative entropy of entanglement of the Choi state of $\mathcal{N}^{\mathrm{MDI}}_{A'B'\to Z_A Z_B}$.

B. Measurement-device-independent conference key agreement

The concept of MDI-QKD has also been generalized to the multipartite setting [30,110,111]. We assume a setup of MDI conference agreement, where a number of trusted parties $\mathbf{A}_i$, for $i\in[n]$, locally prepare states that they send to a central relay via channels $\mathcal{N}^1_{A'_1\to A_1},\ldots,\mathcal{N}^n_{A'_n\to A_n}$. At the relay, a joint measurement is performed on $A_1A_2\ldots A_n$, the result of which is broadcast back to the trusted parties. It is straightforward to generalize Eq. (57) to the multipartite case and apply Theorems 3 and 4 (or Theorem 5 for tele-covariant channels) to obtain bounds on the conference key rates.

C. Quantum key repeater

Let us now consider the quantum key repeater. In its simplest setup, there are three parties: Alice, Bob, and Charlie. Alice and Bob are trusted parties who wish to establish a cryptographic key, whereas Charlie is assumed to be cooperative but is not trusted. One could think of Charlie as a telecom provider. There are two quantum channels, $\mathcal{N}^{A\to C_A}_1$ from Alice to Charlie and $\mathcal{N}^{B\to C_B}_2$ from Bob to Charlie. Alice and Bob are not connected by a quantum channel and are assumed not to have any pre-shared entanglement. Instead, Alice and Bob locally prepare quantum states, e.g., two singlets $\Phi^+_{AR_A}$ and $\Phi^+_{BR_B}$, and both send a subsystem to Charlie, using the respective channels. This is then followed by an entanglement swapping operation [112], where Charlie performs a joint measurement on the C_AC_B subsystem and communicates the result to Bob, who then performs a unitary on his reference system R_B, which should create entanglement that can be used for a cryptographic key, between Alice and Bob. The key has to be secure even in the case where Charlie's information falls into the hands of Eve.

If the channels $\mathcal{N}^{A\to C_A}_1$ and $\mathcal{N}^{B\to C_B}_2$ are too noisy, it might be necessary to use them multiple times and perform an entanglement purification or error-correction protocol before applying the swapping operation. Whereas early quantum repeater protocols [21,22] make use of entanglement purification protocols that require two-way classical communication, between Alice and Charlie and between Charlie and Bob, it is also possible to use error correction that only requires one-way classical communication. Such protocols are known as second- and third-generation repeater protocols (see Ref. [23] and references therein).

By using a large enough number of repeater stations, the key can, in principle, be distributed across arbitrarily long distances. A way to extend a basic three-party repeater protocol to arbitrarily long repeater chains is known as

nested purification [22]. More advanced schemes using error correction and one-way communication have also been developed [23].

As in Refs. [50,57,77], we want to find upper bounds on the rates at which the key can be distributed. Depending on the repeater protocol, there are different ways in which we can describe a quantum key repeater as a multipartite channel and use our results to obtain such bounds. We now describe how a repeater can be described by a bipartite channel. For an alternative way to describe a repeater, we refer to Appendix E.

In order to describe a repeater as a bipartite channel, we consider two trusted parties, Alice and Bob, and a bipartite quantum-to-classical (qc) channel that takes two quantum (and possibly also classical) inputs from Alice and Bob and returns two classical outputs to Alice and Bob, respectively. Such an operation could include the channels from Alice to Charlie and from Bob to Charlie, the measurement performed by Bob, as well as classical communication of the measurement result from Charlie to Alice and Bob. It could also include an error-correction protocol that uses the channels from Alice to Charlie and from Bob to Charlie multiple times and makes use of one-way classical communication from Alice to Charlie and from Bob to Charlie. It is then followed by Charlie's measurement and classical communication to Alice and Bob. Alice and Bob are then allowed to perform LOCC among them but not including Charlie. In the case without error correction, we can define

$$\mathcal{N}^{\text{repeater}}_{AB\to XY} := \mathcal{M}_{C_AC_B\to XY}\circ\mathcal{N}_1^{A\to C_A}\otimes\mathcal{N}_2^{B\to C_B}, \quad (58)$$

where $\mathcal{M}_{C_AC_B\to XY}$ describes the measurement and sending of classical messages X and Y to Alice and Bob, respectively. If we add one-way error correction, we get a bipartite channel of the form

$$\mathcal{N}^{\text{repeater}}_{A^kB^kX'Y'\to XY} := \mathcal{M}_{\tilde{C}_A\tilde{C}_B\to XY}\circ\mathcal{E}_1^{X'A^k\to\tilde{C}_A}\otimes\mathcal{E}_2^{Y'B^k\to\tilde{C}_B}, \quad (59)$$

where $\mathcal{E}_1^{A^k\to\tilde{C}_A}$ includes k instances of the channel $\mathcal{N}_1^{A\to C_A}$, the transmission of the classical data X' obtained by Alice's part of the one-way error-correction protocol to Charlie, as well as Charlie's part of the error-correction protocol (Alice's part of the one-way error-correction protocol is included in the LOCC). Note that $\mathcal{E}_2^{Y'B^k\to\tilde{C}_B}$ is defined in the same way.

By recursively combining the bipartite channels $\mathcal{N}^{\text{repeater}}$, it is possible to derive a bipartite channel $\mathcal{N}^{\text{repeater chain}}$ between Alice and Bob that includes a repeater chain with an arbitrary amount of repeater stations.

Using the results of Refs. [51–53], or Theorem 4, we can obtain upper bounds for key repeater protocols that only involve one-way classical communication from Charlie to Alice and Bob, as considered in Refs. [57,77]. The bounds are given by $\min\{E_{\max,E}(\mathcal{N}^{\text{repeater (chain)}}), E_E^{\infty}(\mathcal{N}^{\text{repeater (chain)}})\}$. By Remark 5, if $\mathcal{N}_{1,2}$ as well as $\mathcal{M}$ are tele-covariant, so is $\mathcal{N}^{\text{repeater (chain)}}$. Hence, by Theorem 5, the bound reduces to the relative entropy of entanglement of the Choi state of $\mathcal{N}^{\text{repeater (chain)}}$. Note that, whereas the bounds in Refs. [57,77] only depend on the initial states shared by Alice and Charlie as well as Bob and Charlie, the formulation in terms of a bipartite channel can provide bounds that also depend on the measurement performed by Charlie, as well as operations performed during error correction. The new bounds take into account imperfect measurements and error correction, which provide an additional limitation on the obtainable rate in practical implementations. Our bounds can at least be shown to be comparable with the results of Refs. [57,77] under certain situations of practical interest. For example, our bound is certainly better when $\mathcal{N}_1^{A\to C_A}$ and $\mathcal{N}_2^{B\to C_B}$ are identity channels, allowing Alice and Charlie as well as Bob and Charlie to share maximally entangled states, whereas Charlie's measurement is noisy.

D. Limitations on some practical prototypes

In this section, we explore fundamental limitations on some practical prototypes for MDI-QKD protocols between two trusted parties. We first begin by considering photon-based prototypes for which a detailed discussion of the quantum system and transmission noise model can be found in Ref. [67]. In Appendix F, we consider MDI-QKD prototypes with qubit systems and transmission noise models depicted by dephasing or depolarizing channels.

We begin by considering a dual-rail scheme based on single photons to encode the qubits [113]. The dual-rail encoding of a qubit in two orthogonal optical modes can be represented in the computational basis of the qubit system, where only one of the two modes is occupied by a single photon and another mode is vacuum. When these optical modes are two polarization modes—horizontal and vertical—of the light, then we express eigenstates in the computational basis as $|H\rangle$ and $|V\rangle$ for horizontal and vertical polarization. It is also possible to consider frequency-offset modes instead of polarization modes for dual-rail encodings. We assume a noise model for the transmission of a photon through the optical fiber to be a pure-loss bosonic channel with transmissivity η. The inputs to the optical fiber are restricted to a single-photon subspace that is spanned by $|H\rangle$ and $|V\rangle$. The action of this pure-loss channel on a qubit encoded with our dual-rail scheme is identical to an erasure channel [114] $\mathcal{E}$ with erasure parameter $1-\eta$ and erasure state $|e\rangle$, where $|e\rangle$ is the vacuum state, i.e., zero photon in both modes. We note that an erasure channel is tele-covariant.

Two trusted parties $\mathbf{A}_i$, $i\in[2]$, use the above-mentioned polarization-based dual-rail photons to transmit their qubit systems to Charlie at the measurement-relay station, through the optical fibers with respective transmissivities

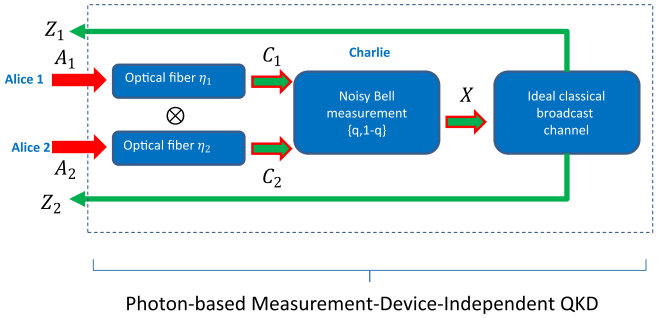

FIG. 4. Pictorial illustration of our photon-based MDI-QKD between two parties using the dual-rail encoding scheme.

η_i (see Fig. 4 for MDI-QKD). We make a simplistic noise model assumption on the measurement channel $\mathcal{M}_{\vec{C}_i\to X}$ by Charlie: It can perform perfect qubit Bell measurement for bipartite MDI-QKD, respectively, with probability q, whereas with probability $1-q$ for the failed measurement, we assume the relay station signals $|\perp\rangle\langle\perp|_X$ to the users. In addition, we can safely assume classical communication $X\to\vec{Z}$ among all parties to be clean (noiseless) as they do not require any quantum resource. Finally, for simplicity, we assume that error-correcting local operations for all parties can be made perfectly.

To calculate the upper bound on the MDI-QKD capacity, it suffices to consider the relative entropy of entanglement of the Choi state of the associated multiplex channel $\mathcal{N}^{\mathrm{MDI},\mathcal{E}}_{\vec{A}\to\vec{Z}}$ as it is tele-covariant. Notice that the action of the erasure channel $\mathcal{E}_{A_i\to C_i}$ on $D_i\in\{|H\rangle\langle H|_{A_i},|H\rangle\langle V|_{A_i},|V\rangle\langle H|_{A_i},|V\rangle\langle V|_{A_i}\}$ is given as

$$\mathcal{E}_{A_i\to C_i}(D_i)=\eta_i D_i+(1-\eta_i)\mathrm{Tr}[D_i]|e\rangle\langle e|_{C_i}. \quad (60)$$

Then, the Choi state $J^{\mathcal{E}}_{\vec{L}\vec{C}}$ of $\bigotimes_{i=1}^{2}\mathcal{E}_{A_i\to C_i}$ is

$$J^{\mathcal{E}}_{\vec{L}\vec{C}}=\bigotimes_{i=1}^{2}\left(\eta_i\Phi^{+}_{L_iC_i}+(1-\eta_i)\frac{\mathbb{1}_{L_i}}{2}\otimes|e\rangle\langle e|_{C_i}\right). \quad (61)$$

For the bipartite MDI-QKD,

$$\mathcal{M}_{C_1C_2\to X}(\cdot)=q\sum_{j=1}^{4}\mathrm{Tr}[\Phi^{(j)}(\cdot)\Phi^{(j)}]|j\rangle\langle j|_X + (1-q)\mathrm{Tr}[\cdot]\otimes|\perp\rangle\langle\perp|_X, \quad (62)$$

where $\{\Phi^{(j)}_{C_1C_2}\}_{j=1}^{4}$ is the Bell measurement, which is a projective measurement. Here, $\{\Phi^{(j)}_{C_1C_2}\}_{j=1}^{4}$ represents the set of maximally entangled states $\{\Phi^{+},\Phi^{-},\Psi^{+},\Psi^{-}\}$ for two-qubit systems and $|\perp\rangle\perp|j\rangle$. We note that the Bell measurement is tele-covariant. Upon action of the measurement channel $\mathcal{M}_{C_1C_2\to X}$ on the state $J^{\mathcal{E}}_{L_1L_2C_1C_2}$ [Eq. (61)], the output state is essentially of the form (see Ref. [67])

$$q\eta_1\eta_2\frac{1}{4}\sum_{j=1}^{4}\Phi^{(j)}_{L_1L_2}\otimes|j\rangle\langle j|_X+(1-q\eta_1\eta_2)\frac{\mathbb{1}_{L_1L_2}}{4}\otimes|\perp\rangle\langle\perp|_X, \quad (63)$$

which implies that the relative entropy of entanglement of the Choi state of $\mathcal{N}^{\mathrm{MDI},\mathcal{E}}_{A_1A_2\to Z_1Z_2}$ is $q\eta_1\eta_2$. Employing Theorem 7, the bipartite MDI-QKD capacity for the given MDI-QKD prototype with erasure channels is

$$\tilde{P}_{\mathrm{LOCC}}(\mathcal{N}^{\mathrm{MDI},\{\mathcal{E}_i\}_{i=1}^{2}})=q\eta_1\eta_2, \quad (64)$$

as $q\eta_1\eta_2$ bits is an achievable rate for the given setup (see Refs. [48,49,105] for the private capacities of $\mathcal{E}_{A_i\to C_i}$). Notice that $q\eta_1\eta_2$ is a strong converse bound.

For bipartite MDI-QKD (see Fig. 4), using the results of Ref. [48,105], we get upper bound (RB) on the bipartite MDI-QKD capacity as $\min\{\eta_1,\eta_2\}$ (e.g., see Refs. [50,60]). This bound is always looser than our strong converse upper bound $q\eta_1\eta_2$ bits, for all practical purposes. In Fig. 5, we plot the rate-distance trade-off (secret key capacity versus distance L in km) for our bound in Eq. (64) when $n=2$, $\eta_1=\eta_2=\exp(-\alpha L)$, and $\alpha=(1/22\ \mathrm{km})$ and compare it with the upper bound (RB) η_1 (since $\eta_1=\eta_2$).

We note that, whereas there now exist variants of MDI-QKD schemes or setups that can achieve the repeaterless bound, e.g., Refs. [31,32,34], the dual-rail protocols we consider here, while being suboptimal, may be easier to implement practically. In particular, implementation of a

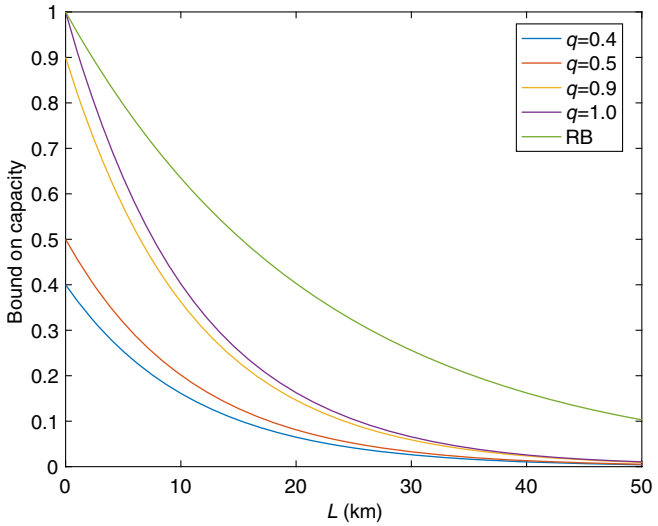

FIG. 5. Rate-distance trade-off comparison between our bound (64) (blue, red, yellow, and purple lines) and the RB bound (green line) for the MDI-QKD protocol for our photon-based prototype.

twin-field protocol requires long-distance phase stabilization, which can be challenging [115]. We showcase here the ability to get nontrivial upper bounds for a specific, suboptimal implementation of QKD schemes. These nontrivial upper bounds are derived from a universal framework, which illustrates the usefulness of the framework we have proposed.

VII. LOWER BOUNDS ON PRIVACY

In this section, we derive lower bounds on the secret-key-agreement rate of a multiplex channel achievable by means of cppp, in the sense of Ref. [68]. This is a generalization of the lower bound presented in Ref. [14] from multipartite states to multiplex channels, as well as a generalization of the lower bounds on one-to-one channels presented in Ref. [69] to the multiplex case.

The DW protocol [68], which is considered with bipartite states, only uses one-way communication from Alice to Bob. In Ref. [69], which is concerned with one-to-one channels, direct and reverse scenarios are considered. The former corresponds to the case where the quantum channel and the classical communication are oriented in the same direction. The latter corresponds to the case where the two are oriented in opposite directions. In Ref. [14], the DW protocol is generalized to multipartite states by selecting one distributing party, which performs the DW protocol with all remaining parties simultaneously.

We now generalize this result to the setting of multiplex channels. We begin with a fully separable pure state $\phi^n \in \mathrm{FS}(:\overrightarrow{A'^nL}:\overrightarrow{B^nR}:\vec{P}:)$. Here, the notation $\overrightarrow{X^n}$ means we consider n copies of all subsystems $X_1,\ldots,X_M$. Application of n copies of the isometric extension of the multiplex channel $\mathcal{N}_{\overrightarrow{A'B}\to\overrightarrow{AC}}$ results in a pure state $\psi^n_{:\overrightarrow{A^nL}:\vec{R}:\overrightarrow{C^nP}:E^n}$. Let us now choose one party, $\mathbf{X}_i$, $i\in\{1,\ldots,M\}$, as the distributing party. Party $\mathbf{X}_i$ performs a POVM $\mathcal{Q}=\{Q_x\}$ with a corresponding random variable $X=\{x,p(x)\}$ on her subsystem, resulting in a classical-quantum-...-quantum (c$\mathbf{q}$) state

$$\omega_{c\mathbf{q}}=\sum_x p(x)|x\rangle\langle x|_X\otimes\omega^x, \tag{65}$$

where ω^x is the post-measurement state of the remaining parties and Eve. Party $\mathbf{X}_i$ then processes X using classical channels $X\to Y$ and $Y\to Z$, where $Y=\{y,q(y)\}$ and $Z=\{z,r(z)\}$ are classical random variables. Here, Y is kept by party $\mathbf{X}_i$ (to be used for the key), and Z is broadcast to all other trusted parties (and Eve). Upon receiving Z, the other parties then perform their respective POVMs, with the goal of estimating the key variable Y. Thus, as shown in Ref. [68], every trusted party $\mathbf{X}_j$, where $i\neq j\in\{1,\ldots,M\}$, obtains a common key with $\mathbf{X}$ at a rate $r_n^{i\to j}$ of

$$r_n^{i\to j}=\frac{1}{n}\left(I(Y:\mathbf{X}_j|Z)_{\tilde{\omega}_{c\mathbf{q}}}-I(Y:E^n|Z)_{\tilde{\omega}_{c\mathbf{q}}}\right), \tag{66}$$

where, in a slight abuse of notation, we use $\mathbf{X}_j$ as a placeholder for $A_j^nL_j$, R_j, or $C_j^nP_j$, depending if $\mathbf{X}_j$ is in $\{\mathbf{A}_a\}_a$, $\{\mathbf{B}_b\}_b$, or $\{\mathbf{C}_c\}_c$, respectively. The second and third cases correspond to the reverse and direct scenarios in Ref. [69], respectively, whereas

$$\tilde{\omega}_{c\mathbf{q}}=\sum_{xyz} r(z|y)q(y|x)p(x)|xyz\rangle\langle xyz|\otimes\omega^x. \tag{67}$$

Equation (66) has to be maximized over all free input states $\phi^n\in\mathrm{FS}(:\overrightarrow{A'^nL}:\overrightarrow{B^nR}:\vec{P}:)$, POVMs $\mathcal{Q}$, as well as classical channels $X\to Y$ and $Y\to Z$. As discussed in Ref. [14], a conference key among all trusted parties can be obtained at the worst-case rate between any pair $(\mathbf{X}_i,\mathbf{X}_j)$. We also have the freedom to choose the distributing party. Putting it all together, we can achieve the following rate of the conference key:

$$\hat{P}^{\mathcal{N}}_{\mathrm{cppp}}\geq\max_i\min_j\lim_{n\to\infty}\max_{\substack{\phi^n,\mathcal{Q}\mathrm{POVM}\\ X\to Y,Y\to Z}} r_n^{i\to j}, \tag{68}$$

with $\phi^n\in\mathrm{FS}(:\overrightarrow{A'^nL}:\overrightarrow{B^nR}:\vec{P}:)$. Note that in the case of a single-sender–single-receiver channel $\mathcal{N}:B\to C$, this reduces to the maximum of the direct and reverse key rates presented in Ref. [69].

Next, we propose an alternative generalization of the DW protocol to the case of multipartite states and multiplex channels. The rough idea is that, instead of performing the DW protocol simultaneously with all other parties after her measurement, the distributing party performs a one-way protocol with a second party, who then performs a one-way protocol with a third party, and the iteration continues. In particular, the random variables obtained in all previous measurements can be passed on in every classical communication step, so a party can adapt her measurement depending on all previous measurements instead of the first measurement as in the protocol described in Ref. [14].

We now describe the protocol in detail: As before, we begin with a fully separable pure state $\phi^n\in\mathrm{FS}(:\overrightarrow{A'^nL}:\overrightarrow{B^nR}:\vec{P}:)$ and apply n copies of the isometric extension of the multiplex channel $\mathcal{N}_{\overrightarrow{A'B}\to\overrightarrow{AC}}$, resulting in a pure state $\psi^n_{:\overrightarrow{A^nL}:\vec{R}:\overrightarrow{C^nP}:E^n}$.

Now, assume that we are given some permutation $\sigma:\{1,\ldots,M\}\to\{\sigma(1),\ldots,\sigma(M)\}$, which determines the order in which the parties participate in the protocol. Party $\mathbf{X}_{\sigma(1)}$ begins by performing a POVM $\mathcal{Q}^{(1)}$ on her share of ψ^n, i.e., on subsystem $A^n_{\sigma(1)}L_{\sigma(1)}$, $R_{\sigma(1)}$, or $C^n_{\sigma(1)}P_{\sigma(1)}$, depending on which kind of party $\mathbf{X}_{\sigma(1)}$ is. This results in a random variable $X^{(1)}=\{p_1(x_1),x_1\}$. The corresponding classical-quantum-...-quantum (c$\mathbf{q}$) state is

$$\omega_{c\mathbf{q}}^{(1)} = \sum_{x_1} p_1(x_1)|x_1\rangle\langle x_1|_{X^{(1)}} \otimes \omega^{x_1}. \tag{69}$$

Party $\mathbf{X}_{\sigma(1)}$ then performs classical channels $X^{(1)} \to Y^{(1)} \to Z^{(1)}$, keeping the random variable $Y^{(1)}$ and sending $Z^{(1)}$ to party $\mathbf{X}_{\sigma(2)}$. The corresponding c$\mathbf{q}$ state is then given by

$$\tilde{\omega}_{c\mathbf{q}}^{(1)} = \sum_{x_1 y_1 z_1} r_1(z_1|y_1) q_1(y_1|x_1) p_1(x_1) |x_1 y_1 z_1\rangle\langle x_1 y_1 z_1| \otimes \omega^{x_1}, \tag{70}$$

where ω^{x_1} is the state of the remaining parties and Eve. Next, party $\mathbf{X}_{\sigma(2)}$ performs a POVM $\mathcal{Q}_{Z^{(1)}}^{(2)}$ on her share of ω^{x_1}, which provides the random variable $X^{(2)}$. Party $\mathbf{X}_{\sigma(2)}$ then performs classical channels $Z^{(1)}X^{(2)} \to Y^{(2)} \to Z^{(2)}$, keeps $Y^{(2)}$ for herself, and sends $Z^{(2)}$ to the next party $\mathbf{X}_{\sigma(3)}$, who applies the same procedure. The protocol is repeated until party $\mathbf{X}_{\sigma(M)}$ receives $Z^{(M-1)}$, followed by her POVM and postprocessing. The c$\mathbf{q}$ after $k \in \{1, \ldots, M\}$ measurements and postprocessing steps is given by

$$\tilde{\omega}_{c\mathbf{q}}^{(k)} = \sum_{\substack{x_1 \ldots x_k \\ y_1 \ldots y_k \\ z_1 \ldots z_k}} \tilde{p}_{x_1 y_1 z_1 \ldots x_k y_k z_k} \times |x_1 y_1 z_1 \ldots x_k y_k z_k\rangle\langle x_1 y_1 z_1 \ldots x_k y_k z_k| \otimes \omega^{x_1 \ldots x_k}, \tag{71}$$

where we have defined, recursively,

$$\tilde{p}_{x_1 y_1 z_1 \ldots x_k y_k z_k} = r_k(z_k|y_k) q_k(y_k|x_k z_{k-1}) p_k(x_k) \times \tilde{p}_{x_1 y_1 z_1 \ldots x_{k-1} y_{k-1} z_{k-1}}. \tag{72}$$

Parties $\mathbf{X}_{\sigma(k)}$ and $\mathbf{X}_{\sigma(k+1)}$ can establish a key rate of [68]

$$r^{\sigma(k)\to\sigma(k+1)} = \frac{1}{n}\left(I(Y^{(k)}:\mathbf{X}_{\sigma(k+1)}|Z^{(k)})_{\tilde{\omega}_{c\mathbf{q}}^{(k)}} - I(Y^{(k)}:E^n|Z^{(k)})_{\tilde{\omega}_{c\mathbf{q}}^{(k)}}\right). \tag{73}$$

We can again maximize over all free input states, POVMs, as well as classical channels and consider the worst-case rate between any pair $(\mathbf{X}_i, \mathbf{X}_j)$. Furthermore, we have the freedom to choose the order of the parties. Putting it all together, we can achieve the following rate of the conference key:

$$\hat{P}_{\text{cppp}}^{\mathcal{N}} \geq \max_{\sigma\in\text{perm}} \min_k \lim_{n\to\infty} \max_{\substack{\phi^n, \mathcal{Q}^{(1)}, \ldots, \mathcal{Q}^{(k)} \text{POVM} \\ X^{(1)}\to Y^{(1)}\to Z^{(1)} \\ X^{(2)}Z^{(1)}\to Y^{(2)}\to Z^{(2)} \\ \ldots \\ X^{(k)}Z^{(k-1)}\to Y^{(k)}\to Z^{(k)}}} r^{\sigma(k)\to\sigma(k+1)}, \tag{74}$$

with $\phi^n \in \text{FS}(:\overrightarrow{A'^n L}:\overrightarrow{B^n R}:\vec{P}:)$.

A. Lower bound for bidirectional network via spanning tree

In this section, we observe that one can tighten the lower bounds presented in the previous section for a particular multiplex channel called the bidirectional network (BN). In the BN, each of the nodes is connected with its neighbors by product bidirectional channels, which are specific bidirectional channels that is a tensor product of two point-to-point channels directed in opposite ways from each other.

We first observe that BN is a particular case of a multiplex channel (call it $\mathcal{N}$). Indeed, in this case, all the parties are of type $\mathcal{A}$; i.e., they can read and write. The rule is that each party represented in the network as a vertex v has $\deg(v)$ of neighbors (see Ref. [116] for an introduction to graph theory). Each party is assumed to write to her neighbors and also receive from these neighbors some quantum data. We now present a tighter bound on the private capacity of $\mathcal{N}$ based on the above exemplary graph.

To be more specific, the BN can be represented by a weighted, directed multigraph $G = (E, V)$ in which each edge $e_{ij} = (v_i, v_j) \in E$ represents a product bidirectional channel $\Lambda_{ij} = \Lambda_{i\to j} \otimes \Lambda_{j\to i}$ with weight $W: E \mapsto R_+$ such that $W(e_{ij}) = W(e_{ji}) = \mathcal{P}(\Lambda_{i\to j}) = \mathcal{P}(\Lambda_{j\to i})$ (this edge can be represented by two directed edges: one from v_i to v_j and the other vice versa; hence, the structure is directed multigraph). Each product bidirectional channel has in both directions the same private capacity (that, however, may differ for different channels). By convention, we consider edges with index $i > j$ only. The number of nodes in the network is denoted as $|V| := n$ and the number of edges as $|E| := m$.

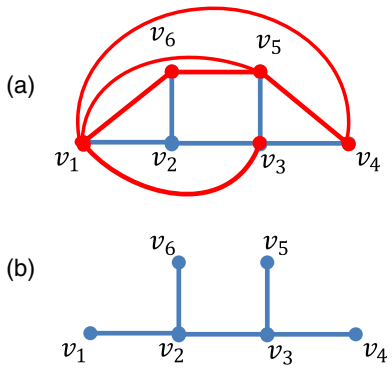

FIG. 6. (a) Exemplary graph. Red edges correspond to private capacity 1 and blue to private capacity 2. The first strategy for obtaining the conference key uses a vertex connected to all others and reaches the suboptimal rate $\min\{w(e_{ij}):(v_1, v_6), (v_1, v_5), (v_1, v_4), (v_1, v_3), (v_1, v_2)\} = 1$. The same happens for any path, which inevitably has to pass through some red edge. The solution is a tree, which is a spanning tree of this graph, and it contains no red edge (b). Traversing the edges of this tree is equivalent to the breadth-first search.

As a motivation for the next consideration, for such multiplex channels, the bounds given in inequalities (68) and (74) above are not tight. We exemplify this on the graph presented in Fig. 6(a). Namely, we assume that each red edge of the graph G depicted there represents a (bidirectional) channel with private capacity 1, while each blue edge is with capacity equal to 2. We do not depict all other edges (connections) as they have zero private capacity by assumption. We now make two observations: (i) The approach of inequality (68) would yield overall secret key agreement at rate 1, as the only node connected to all others in G (v_1) contains (in fact, more than one) red edge. (ii) We observe, by direct inspection, that every path connecting all vertices also contains at least one red edge. On the other hand, there is a set of vertices [depicted with edges in Fig. 6(b)] that forms the so-called spanning tree $T \coloneqq (V_T, E_T) \subset G$ of the graph G. The spanning tree is an acyclic connected subgraph of G, and the word "spanning" refers to the fact that all the vertices of the graph G belong to V_T. It is easy to see that starting from any vertex of this tree, by the breadth-first search algorithm, one can visit all its edges, and one can obtain the conference key at rate 2 (see Ref. [117] for an introduction to algorithms).

As a generalization of this idea, one easily comes up with the following lower bound, which is the main result of this section:

$$\hat{P}^{\mathcal{N}}_{\mathrm{cppp}} \geq \max_{T\subseteq G} \min_{t\in V_T, t'\in N[t]} \lim_{n\to\infty} \max_{\substack{\phi^n, \mathcal{Q}^{(1)},\ldots,\mathcal{Q}^{(|V_T|)}\mathrm{POVM} \\ X^{(v_1)}\to Y^{(v_1)}\to Z^{(v_1)}, \\ X^{(N[v_1])}Z^{(v_1)}\to Y^{(N[v_1])}\to (Z^{(N[v_1])})|_{\deg\geq 2}, \\ X^{(N_2[v_1])}Z^{(N[v_1])}\to Y^{(N_2[v_1])}\to (Z^{(N_2[v_1])})|_{\deg\geq 2}, \\ X^{N_l[v_1]}Z^{N_l[v_1]}\to Y^{N_l[v_1]}}} r^{\sigma(t)\to\sigma(t')}, \tag{75}$$

where $1 \leq l \leq n$ is an index that counts how many times the breadth-first search needs to be invoked in order to traverse all the edges of the spanning tree T. For ease of notation, T is meant to be a rooted, without loss of generality, at vertex v_1. By $N[v]$, we mean the proper neighborhood of the node v (i.e., the set of all vertices that are connected by a single edge with v). In a rooted tree, every vertex is reachable from the root vertex by a path. By $N_i[v_1]$, we mean the set of vertices reachable from vertex v_1 by a path of length i. Owing to this notation, $N[v_1] \equiv N_1[v_1]$, while all vertices achievable from v_1 by traversing two edges belong to $N_2[v_1]$ and so on.

The first inner maximization needs to be understood inductively. The first step is obvious: We begin with an arbitrary vertex $v_1 \in V_T$. The party X_{v_1} who is at node v_1 performs a POVM Q_1, which produces a random variable $X^{(v_1)}$. She processes this variable further to obtain $Y^{(v_1)}$ and sends a communication in the form of a variable $Z^{(v_1)}$. The latter variable is broadcast to all the next neighbors of v_1, i.e., $N[v_1]\backslash\{v_1\}$. Furthermore, if at step $m-1$ the form of operations and communication between the nodes has concise notation $X^{S_m}Z^{S_{m-1}} \to Y^{S_m} \to Z^{S_m}|_{\deg\geq 2}$, then the next level of nesting, i.e.,

$$X^{N[S_m]}Z^{S_m} \to Y^{N[S_m]} \to (Z^{N[S_m]})|_{\deg\geq 2}, \tag{76}$$

has to be understood as a short notation of the following postprocessing at a number of nodes from the set $N[S_m] = \{s_1, \ldots, s_r\}$ with $r = |N[S_m]|$:

$$\forall_{s_i\in N[S_m]}\colon \deg(s_i) \geq 2^{X^{(s_i)}Z^{N[s_i]\cap p(s_i)}\to Y^{(s_i)}\to Z^{(s_i)}}$$
$$\forall_{s_i\in N[S_m]}\colon \deg(s_i) = 1^{X^{(s_i)}Z^{N[s_i]\cap p(s_i)}\to Y^{(s_i)}},$$

where $p(s_i)$ denotes the parent vertex of the vertex s_i, that is, the unique vertex belonging to the neighborhood that is the closest to the root v_1 in terms of traversed edges.

The above description means that if some vertex of the tree is of degree equal to 1, it has no further children in the tree to pass useful information contained in the Z-type variable, while all vertices with larger degree than 1 need to broadcast appropriate data to their further neighbors in the tree.

We exemplify the lower bound given in inequality (75) with the broadcast network depicted on Fig. 6. Let us first focus on involved sets of vertices in the process of the breadth-first search over the tree T. The set of vertices of the spanning tree T reads $\{v_1, \ldots, v_6\}$. As the root vertex, we choose v_1. Next, $N_1[v_1] = \{v_2\}$, $N_2[v_1] = \{v_3, v_6\}$ and $N_3[v_1] = \{v_4, v_5\}$. In this case, the presented lower bound reads

$$\hat{P}^{\mathcal{N}}_{\mathrm{cppp}} \geq \max_{T\subseteq G} \min_{t\in V_T, t'\in N[t]} \lim_{n\to\infty} \max_{\substack{\phi^n, \mathcal{Q}^{(1)},\ldots,\mathcal{Q}^{(6)}\mathrm{POVM} \\ X^{(v_1)}\to Y^{(v_1)}\to Z^{(v_1)}, \\ X^{(v_2)}Z^{(v_1)}\to Y^{(v_2)}\to Z^{(v_2)}, \\ X^{(v_3)}Z^{(v_2)}\to Y^{(v_3)}\to Z^{(v_3)}, \\ X^{(v_6)}Z^{(v_2)}\to Y^{(v_6)}, \\ X^{(v_5)}Z^{(v_3)}\to Y^{(v_5)}, \\ X^{(v_4)}Z^{(v_3)}\to Y^{(v_4)}}} r^{\sigma(t)\to\sigma(t')}. \tag{77}$$

In Appendix G, we briefly comment on the complexity of finding a subgraph, which allows us to realize the

conference key agreement with the capacity indicated by the inequality (75).

VIII. KEY DISTILLATION FROM STATES

In this section, we concentrate on the subject of the distillation of secret keys from quantum states. An (n, K, ε) LOCC conference key distillation begins with M parties $\mathbf{A}_i$ for $i \in [M]$ sharing n copies of the M-partite quantum state $\rho_{\vec{A}}$, to which they apply an LOCC channel $\mathcal{L}_{\overrightarrow{A^{\otimes n}} \to \overrightarrow{SK}}$. The resulting output state satisfies the following condition:

$$F(\mathcal{L}_{\overrightarrow{A^{\otimes n}} \to \overrightarrow{SK}}(\rho_{\vec{A}}^{\otimes n}), \gamma_{\overrightarrow{KS}}) \geq 1 - \varepsilon. \tag{78}$$

The one-shot secret-key-distillation rate from a single copy of a multipartite quantum state $K_{\mathrm{D}}^{(1,\varepsilon)}$ is upper bounded as follows (cf. Sec. V).

Theorem 8: For any fixed $\varepsilon \in (0, 1)$, the achievable region of secret key agreement from a single copy of an arbitrary multipartite quantum state $\rho_{\vec{A}}$ satisfies

$$K_{\mathrm{D}}^{(1,\varepsilon)}(\rho) \leq E_{h,\mathrm{GE}}^{\varepsilon}(:\vec{A}:)_{\rho}, \tag{79}$$

where

$$E_{h,\mathrm{GE}}^{\varepsilon}(:\vec{A}:)_{\rho} := \inf_{\sigma \in \mathrm{BS}(:\vec{A}:)} D_h^{\varepsilon}(\rho \| \sigma) \tag{80}$$

is the ε-hypothesis-testing relative entropy of genuine entanglement of multipartite state $\rho_{\vec{A}}$.

Proof.—The proof argument is the same as that of Theorem 2, so we omit the proof here. ∎

In the asymptotic limit, the rate $K_{\mathrm{D}}^{(n,\varepsilon)}$ satisfies

$$\inf_{\varepsilon > 0} \limsup_{n \to \infty} \frac{1}{n} K_{\mathrm{D}}^{(n,\varepsilon)}(\rho^{\otimes n}) = K_{\mathrm{D}}(\rho), \tag{81}$$

which follows directly from the definition of the secret key rate K_{D} [14].

Using the same argument as in the proof of Theorem 6 in Sec. V C, we can also get the following asymptotic bound, which is generalized in Theorem 9 of Ref. [62]:

Proposition 2: For an m-partite state $\rho_{\vec{A}}$, it holds that

$$K_D(\rho_{\vec{A}}) \leq E_{\mathrm{GE}}^{\infty}(\rho_{\vec{A}}). \tag{82}$$

In general, to share the conference key, it is necessary for the honest parties to distill genuine multipartite entanglement.

Corollary 6: For a tensor-stable biseparable state $\rho_{\vec{A}}$, it holds that $K_D(\rho_{\vec{A}}) = 0$.

The above Corollary of Theorem 8 is precisely due to the infimum over biseparable states. However, already in the tripartite setting, there are two nonequivalent families of three-partite genuinely entangled states, that is, Φ_M^{GHZ}-type and Φ_M^{W}-type states [79,85,118–121]. Both families of states contain states that are maximally entangled; however, they cannot be transformed with LOCC one into another at unit rate [81,84,86,87,122,123]. As the perfect Φ_M^{GHZ} state plays a role of the honest (or perfect) implementation of conference quantum key agreement protocols, the distillation of Φ_3^{GHZ} states from Φ_3^{W} states has been intensively studied [80–84,86]. In particular, recalling Example 11 of Ref. [80], it is known that one cannot transform a single Φ_3^{W} state into a Φ_3^{GHZ} state even in a probabilistic manner. However, according to Theorem 2 of Ref. [80], the calculated asymptotic rate for conversion from Φ_3^{W} to Φ_3^{GHZ} due to certain protocols is approximately 0.643 (per copy), which constitutes a lower bound for the general case. Another complementary lower bound has been provided in Ref. [86].

Surprisingly, in the one-shot regime, distillation of Φ_3^{GHZ} states from Φ_3^{W} states, and therefore of the secret key, is still possible. To accomplish this task, it is sufficient to consider the initial state as being made up of two copies of the Φ_3^{W} state. Then, using results in Ref. [81], it follows that we can obtain two Φ_2^+ states in two distinct bipartite systems with a probability that is arbitrarily close to $\frac{2}{3}$; having this in mind, one can obtain Φ_3^{GHZ} by employing ancilla and the entanglement swapping protocol [112]. In this way, we calculate a lower bound on the distillation of Φ_3^{GHZ} states from two copies of the Φ_3^{W} state in a one-shot regime (one Φ_3^{GHZ} state with probability $\frac{2}{3}$ from two Φ_3^{W} states). This lower bound can be compared with the upper bound in Theorem 8 given above.

Nevertheless, distillation of Φ_M^{GHZ} states is only an example of a key distillation technique [13,14,84,86,124–127]. A more general conference key agreement scenario of our interest incorporates distillation of twisted Φ_M^{GHZ} states (see Definition 3) [14,61,119,128,129]. In that case, an approach for upper bounding conference key rates that is different than the estimation of Φ_M^{W} to Φ_M^{GHZ} conversion rates is required. This approach corresponds to a possible gap between rates of Φ_M^{GHZ} (that can be distilled) and secret key distillation. Since the Φ_M^{GHZ} state is an instance of a private state, an upper bound on the conference key rate is also an upper bound on the distillation rate from any state. For plotting our numerical results, we concentrate on secret key distillation from n copies of the Φ_M^{W} state in order to compare with other limitations discussed in this section.

The upper bound in Theorem 8 has optimization over all possible biseparable states. Computation of the exact value of the bound given in Eq. (79) need not be feasible in general. As we take the infimum in Eq. (80), we can obtain non-trivial upper bounds on the upper bound given in Eq. (79) by considering optimization over suitable subsets of biseparable states. We make an educated guess for the

form of biseparable state to yield a non-trivial upper bound. We remark here that the set of biseparable states is not closed under a tensor product, so we have to find different states for any tensor power n of Φ_M^{W} or Φ_M^{GHZ} states. We devise two families of biseparable states, $\pi_{\mathrm{W}}^{n,M}$ and $\pi_{\mathrm{GHZ}}^{n,M}$, adjusted to both number of copies, n, and number of parties, M,

$$\pi_{\mathrm{GHZ}}^{n,M} := \frac{1}{M}\sum_{i=1}^{M}\left[\mathcal{S}_{1,i}\left(\frac{I}{2}\otimes\Phi_{M-1}^{\mathrm{GHZ}}\right)\right]^{\otimes n}, \tag{83}$$

$$\pi_{\mathrm{W}}^{n,M} := \frac{1}{M}\sum_{i=1}^{M}\left(\mathcal{S}_{1,i}(|0\rangle\langle 0|\otimes\Phi_{M-1}^{\mathrm{W}})\right)^{\otimes n}, \tag{84}$$

where the operator $\mathcal{S}_{1,i}$ swaps the qubit of the first party with the qubit of the ith party. The choice of $\pi_{\mathrm{GHZ}}^{n,M}$ and $\pi_{\mathrm{W}}^{n,M}$ states is motivated by keeping the correlation between $M-1$ parties most similar to those in Φ_M^{GHZ} or Φ_M^{W} states while keeping one party explicitly separated. Additionally, $\pi_{\mathrm{GHZ}}^{n,M}$ and $\pi_{\mathrm{W}}^{n,M}$ states, by definition, are symmetric with respect to permutation of parties because of permutations with $\mathcal{S}_{1,i}$.

We would like to point out that the $\pi_{\mathrm{W}}^{1,3}$ presented here is closer to the Φ_3^{W} state in the Hilbert-Schmidt norm than the state (let us call it Υ) in Ref. [130], even though the state constructed there was supposed to be the biseparable state closest to Φ_3^{W} in the Hilbert-Schmidt norm. This result is due to different definitions of biseparability; the state in Ref. [130] is a tensor product with respect to one of the cuts, whereas we make use of the convexity of the set of biseparable states. Indeed, our states are biseparable by construction (see Sec. IV A).

The upper bound on the asymptotic secret key rate can be compared with the lower bound on asymptotic Φ_3^{GHZ} states from Φ_3^{W} state distillation [80] in the following way. First, we notice that if two parties unite, then the $M-1$-partite key is no less than the initial M-partite key because the set of operations of the M-partite LOCC protocol is a strict subset of the set of operations for the case in which two parties, i and j, are in the same laboratory. We have the following Proposition:

Proposition 3: For any M-partite state $\rho_{[M]}$, the asymptotic secret-key-agreement rate satisfies the following inequality:

$$\max_k K_D(\rho_{[M+1]_k}) \le K_D(\rho_{[M]}) \le \min_{i,j} K_D(\rho_{[M-1]_{ij}}), \tag{85}$$

where $[M]=[1,\ldots,M]$ and $[M-1]_{ij}=[1,\ldots,i-1,(i,j),i+1,\ldots,j-1,j+1,\ldots,M]$ indicate a state $\rho_{[M-1]}$ in which subsystems i and j are merged. Analogously, $[M+1]_k=[1,\ldots,k-1,k_1,k_2,k+1,\ldots,M+1]$ indicates the state in which subsystem k is split into systems k_1 and k_2.

Proof.—It is enough to notice that the class of LOCC protocols involved in the definition of $K_D(\rho_{[M]})$ is strictly contained in the class of protocols involved in the definition of $K_D(\rho_{[M-1]_{ij}})$. Indeed, the merged parties can still simulate any operation from the former class; however, together, they can perform many more operations, including global quantum operations on all merged subsystems together. Since K_D is defined as the supremum of the key rate over such protocols, the upper bound follows. For the lower bound, it is enough to notice that by splitting subsystem(s) of ρ, we restrict the class of operations that can be used to distill the key. ∎

We immediately observe that Proposition 3 provides a whole family of nonequivalent upper bounds. To see this, one can consider a state that is not invariant under permutations. What is more, one can continue merging as long as there is still two or more subsystems left.

Corollary 7: For any M-partite state $\rho_{[M]}$ defined on the Hilbert space $\mathcal{H}$, the asymptotic secret-key-agreement rate satisfies the following inequality:

$$\max_L K_D(\rho_{[L]}) \le K_D(\rho_{[M]}) \le \min_N K_D(\rho_{[N]}), \tag{86}$$

where the state $\rho_{[L]}$ is obtained from the state $\rho_{[M]}$ by splitting its subsystems so that $L \ge \log\dim(\mathcal{H})$. Analogously, the state $\rho_{[N]}$ is obtained via any merging of subsystems of $\rho_{[M]}$, such that $\rho_{[N]}$ has at least two subsystems.

Hence, in the particular case of the Φ_3^{W} state, we can also skip minimization with respect to i, j since the state is symmetric. Using properties of entanglement measures [131–133], we have

$$K_D(\Phi_3^{\mathrm{W}}) \le K_D(\Phi_{2+1}^{\mathrm{W}}) \le E_r^{\infty}(\Phi_{2+1}^{\mathrm{W}}) \tag{87}$$

$$= h_2\left(\frac{1}{3}\right) \approx 0.9183 \text{ bit}, \tag{88}$$

where $h_2(x)$ is the binary entropy function.

The asymptotic key rate and bounds on it are usually noninteger real numbers. In the one-shot regime, expressing these quantities in a similar manner, instead of integers obtained with floor or ceiling functions, is no less meaningful because the amount of secret key and the value of bounds are functions of privacy test parameter ε, which can vary, yielding, in general, different values of these quantities. Therefore, dependence of the scenario on the privacy parameter ε is interesting on its own. See Appendix H and Ref. [134].

Remark 6: It is natural that the analogies of Proposition 3 and Corollary 7 hold for the multiplex quantum channel $\mathcal{N}$. The upper bound on the M-partite multiplex quantum channel takes the form of the $M-1$-partite multiplex channel, where the new party's type is determined according to the following rule: If the two parties are of the same

type (say, B), then the new type is the same (B in that case). If the types are different, then the new type always becomes A because, e.g., when B and C are merged, they have the ability to both read and write.

IX. DISCUSSION

We have provided universal limits on the rates at which one can distribute the conference key over a quantum network described by a multiplex quantum channel. We have shown that multipartite private states are necessarily genuine multipartite entangled. As a consequence, it is not possible to distill multipartite private states from tensor-stable biseparable states. We have obtained an upper bound on the single-shot, classical preprocessing and postprocessing assisted secret-key-agreement capacity. The bound is in terms of the hypothesis-testing divergence with respect to biseparable states of the output state of the multiplex channel, maximized over all fully separable input states. We have further provided strong-converse bounds on the LOCC-assisted private capacity of multiplex channels that are in terms of the max-relative entropy of entanglement as well as the regularized relative entropy of entanglement. In the case of tele-covariant multiplex channels, we have also obtained bounds in terms of the relative entropy of entanglement of the resource state. We have shown the versatility of our bounds by applying it to several communication scenarios, including measurement-device-independent QKD and conference key agreement as well as quantum key repeaters. In addition to our upper bounds, we have also provided lower bounds on asymptotic conference key rates, which are asymptotically achievable in Devetak-Winter-like protocols. We also derived an upper bound on the secret key that can be distilled from finite copies of multipartite states via LOCC, and we showed some numerical examples. The task of distillation of Φ_3^{GHZ} from Φ_3^{W} was extensively studied in the literature [81,122,123]. Here, we initiate the study on the distillation of the key rather than Φ_3^{GHZ} distillation from the Φ_3^{W} state. This is the rate of the distillation of "twisted" Φ_3^{GHZ} being private states—a class to which Φ_3^{GHZ} belongs. It would be interesting to find if the distillation of the key from Φ_3^{W} is just equivalent to the distillation of Φ_3^{GHZ} (see recent result on this topic [127]).

Distillation of the secret key allows trusted parties to access private random bits. Our lower bound on an asymptotic LOCC-assisted secret-key-agreement capacity over a multiplex channel also provides an asymptotic achievable rate of private random bits for trusted parties over a multiplex channel with classical preprocessing and postprocessing.

Our work also provides frameworks for the resource theories of multipartite entanglement for quantum multipartite channels (analogous to bipartite channels as discussed in Refs. [51,53,97,98]). In this context, it is natural to extend the results of Ref. [135], where the so-called layered QKD is considered, to the noisy case of multipartite private states. It would be interesting to systematically consider other frameworks in the resource theory of multipartite entanglement. An important future direction for application purposes is to identify new information processing tasks and determine bounds on the rate regions of classical and quantum communication protocols over a multiplex channel (e.g., see Refs. [53,136–142]).

ACKNOWLEDGMENTS

S. D. is grateful to Jonathan P. Dowling (3 April 1955–5 June 2020) for insightful discussions. The authors thank Koji Azuma, Nicolas Cerf, Marcus Huber, Liang Jiang, Sumeet Khatri, Glaucia Murta, Mark M. Wilde, and Paweł Żyliński for valuable discussions. S. D. acknowledges individual fellowships at Université Libre de Bruxelles; this project received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement No. 801505. S. B. acknowledges funding from the European Union's Horizon 2020 research and innovation program, Grant Agreement No. 820466 (project CiViQ), the postdoctoral fellowships program Beatriu de Pinós, funded by the Secretary of Universities and Research (Government of Catalonia), and by the Horizon 2020 program of research and innovation of the European Union under the Marie Sklodowska-Curie Grant Agreement No. 801370 (2019 BP 00097), as well as from the Government of Spain (FIS2020-TRANQI and Severo Ochoa CEX2019-000910-S), Fundació Cellex, Fundació Mir-Puig, Generalitat de Catalunya (CERCA, AGAUR SGR 1381, and Quantum-CAT). K. H. and M. W. acknowledge support from the grant Sonata Bis 5 (Grant No. 2015/18/E/ST2/00327) from the National Science Center. We acknowledge partial support by the Foundation for Polish Science (IRAP project, ICTQT, Contract No. MAB/2018/5, co-financed by the EU within Smart Growth Operational Programme). The "International Centre for Theory of Quantum Technologies" project (Contract No. MAB/2018/5) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3).

APPENDIX A: GENERALIZED DIVERGENCES AND THEIR PROPERTIES

Any generalized divergence $\mathbf{D}(\cdot\|\cdot)$ satisfies the following two properties for an isometry U and a state τ [63]:

$$\mathbf{D}(\rho\|\sigma) = \mathbf{D}(U\rho U^\dagger\|U\sigma U^\dagger), \tag{A1}$$

$$\mathbf{D}(\rho\|\sigma) = \mathbf{D}(\rho\otimes\tau\|\sigma\otimes\tau). \tag{A2}$$

The sandwiched Rényi relative entropy obeys the following "monotonicity in α" inequality [64]:

$$\tilde{D}_\alpha(\rho\|\sigma) \leq \tilde{D}_\beta(\rho\|\sigma) \quad \text{if } \alpha \leq \beta, \quad \text{for } \alpha,\beta \in (0,1)\cup(1,\infty). \tag{A3}$$

The following inequality states that the sandwiched Rényi relative entropy $\tilde{D}_\alpha(\rho\|\sigma)$ between states ρ, σ is a particular generalized divergence for certain values of α [143,144]. For a quantum channel $\mathcal{N}$,

$$\tilde{D}_\alpha(\rho\|\sigma) \geq \tilde{D}_\alpha(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)), \quad \forall\ \alpha \in [1/2,1)\cup(1,\infty). \tag{A4}$$

In the limit $\alpha \to 1$, the sandwiched Rényi relative entropy $\tilde{D}_\alpha(\rho\|\sigma)$ between quantum states ρ, σ converges to the quantum relative entropy [63,64]:

$$\lim_{\alpha\to 1}\tilde{D}_\alpha(\rho\|\sigma) = D(\rho\|\sigma), \tag{A5}$$

and the quantum relative entropy [92] between states is

$$D(\rho\|\sigma) \coloneqq \mathrm{Tr}[\rho\log_2(\rho-\sigma)] \tag{A6}$$

for $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$ and otherwise it is ∞.

In the limit $\alpha \to 1/2$, the sandwiched Rényi relative entropy $\tilde{D}_\alpha(\rho\|\sigma)$ converges to $-\log_2 F(\rho,\sigma)$, where $F(\rho,\sigma)$ is the fidelity between ρ, σ defined as

$$F(\rho,\sigma) \coloneqq \left[\mathrm{Tr}\left[\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right]\right]^2. \tag{A7}$$

The following inequality relates $D_h^\varepsilon(\rho\|\sigma)$ to $\tilde{D}_\alpha(\rho\|\sigma)$ for density operators ρ, σ, $\alpha \in (1,\infty)$ and $\varepsilon \in (0,1)$ (see Refs. [145–147] and Lemma 5 in Ref. [148]):

$$D_h^\varepsilon(\rho\|\sigma) \leq \tilde{D}_\alpha(\rho\|\sigma) + \frac{\alpha}{\alpha-1}\log\left(\frac{1}{1-\varepsilon}\right). \tag{A8}$$

The following inequality also holds [94]:

$$D_h^\varepsilon(\rho\|\sigma) \leq \frac{1}{1-\varepsilon}\left(D(\rho\|\sigma) + h_2(\varepsilon)\right), \tag{A9}$$

where $h_2(\varepsilon) \coloneqq -\varepsilon\log_2\varepsilon - (1-\varepsilon)\log_2(1-\varepsilon)$ is the binary entropy function.

In a specific case, ε-hypothesis-testing relative entropy can be calculated exactly.

Lemma 3: If ρ is a pure state and it is one of the eigenvectors of σ, i.e., there exists decomposition $\sigma = p_0\rho + \sum_{i=1} p_i\gamma_i^\perp$, with $\sum_{i=0} p_i = 1$, $0 \leq p_i \leq 1$, $p_0 \neq 0$ and states $\gamma_i^\perp$ orthogonal to ρ, then for any $\epsilon \in [0,1]$,

$$D_h^\epsilon(\rho\|\sigma) = -\log_2 \mathrm{Tr}[\Omega\sigma], \tag{A10}$$

with $\Omega = (1-\varepsilon)\rho$.

APPENDIX B: MULTIPLEX QUANTUM CHANNELS

All network channels that are possible in a communication setting are special cases of multiplex quantum channels $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ (see Fig. 1):

(1) Point-to-point quantum channel: This is a quantum channel of the form $\mathcal{N}_{B_b\to C_c}$ with a single sender and a single receiver. When a multiplex quantum channel has the form $\mathcal{N}_{B_b\to C_c}$ then $\mathcal{A} = \varnothing$ and $|\mathcal{B}| = 1 = |\mathcal{C}|$. This is arguably the simplest form of a communication (network) channel as it involves only two parties with one party sending input to the channel and the other receiving the output from the channel.

(2) Bidirectional quantum channel: This is a multiplex quantum channel of the form $\mathcal{N}_{A_1'A_2'\to A_1A_2}$ with two parties who are both senders and receivers, i.e., $|A| = 2$ and $B = \varnothing = C$ (cf. Refs. [53,101]).

(3) Quantum interference channel: This is a bipartite quantum channel of the form $\mathcal{N}_{B_1B_2\to C_1C_2}$ with two senders and two receivers (cf. Ref. [149]). We may also call $\mathcal{N}_{\vec{B}\to\vec{C}}$, with an equal number of senders and receivers, as the quantum interference channel.

(4) Broadcast quantum channel: This is a multipartite quantum channel of the form $\mathcal{N}_{B_b\to\vec{C}}$ with a single sender and multiple receivers (cf. Refs. [150,151]). We may also call $\mathcal{N}_{\vec{B}\to\vec{C}}$ as a broadcast channel if the number of senders is less than the number of receivers.

(5) Multiple access quantum channel: This is a multipartite quantum channel of the form $\mathcal{N}_{\vec{B}\to C_c}$ with multiple senders and a single receiver (cf. Ref. [152]). We may also call $\mathcal{N}_{\vec{B}\to\vec{C}}$ as a multiple access channel if the number of senders is more than the number of receivers.

(6) Physical box: Any physical box with quantum or classical inputs and quantum or classical outputs.

(7) Network quantum channels of types $\mathcal{N}_{\vec{A'}\to\vec{A}\vec{C}}$ and $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}}$.

If inputs and outputs to a multiplex channel are classical systems and underlying processes are governed by classical physics, then the channel is called a classical multiplex channel (see Ref. [137] for examples of such network channels). If inputs and outputs to the channel are quantum and classical systems, respectively, then the channel is called a quantum-to-classical channel. If inputs and outputs to the channel are classical and quantum systems, respectively, then the channel is called a classical to a quantum channel.

APPENDIX C: PRIVACY TEST

Recall the definition of the twisting operation

$$U^{\mathrm{tw}}_{\overrightarrow{KS}} = \sum_{i_1,\ldots,i_M=0}^{K-1} |i_1\ldots i_M\rangle\langle i_1\ldots i_M|_{\vec{K}} \otimes U_{\vec{S}}^{(i_1\ldots i_M)} \tag{C1}$$

and a privacy test as

$$\Pi^{\gamma,K}_{\overrightarrow{KS}} = U^{\mathrm{tw}}_{\overrightarrow{KS}}(\Phi^{\mathrm{GHZ}}_{\vec{K}} \otimes \mathbb{1}_{\vec{S}})U^{\mathrm{tw}\dagger}_{\overrightarrow{KS}} \tag{C2}$$

$$= \frac{1}{K}\sum_{i,k=0}^{K-1}(|i\rangle\langle k|)^{\otimes M}_{\vec{K}} \otimes U^{(i^M)}_{\vec{S}}U^{(k^M)\dagger}_{\vec{S}}, \tag{C3}$$

where we have defined the notation $i^M \coloneqq \underbrace{i\ldots i}_{M\text{times}}$. We now provide the proof of Theorem 1:

Proof of Theorem 1.—We begin by showing the bound for pure biseparable states $|\varphi\rangle_{\overrightarrow{KS}}$. For such a state, there exists a bipartition of the parties, defined by nonempty index sets $I \subset \{1,\ldots,M\}$ and $J = \{1,\ldots,M\}\backslash I$, such that the state is a product with respect to that bipartition. Namely, $|\varphi\rangle_{\overrightarrow{KS}} = |\tilde{\varphi}\rangle_{S_IK_I} \otimes |\bar{\varphi}\rangle_{S_JK_J}$, where we have defined $\mathcal{H}_{S_IK_I} = \bigotimes_{i\in I}\mathcal{H}_{S_iK_i}$ and $\mathcal{H}_{S_JK_J} = \bigotimes_{j\in J}\mathcal{H}_{S_jK_j}$. Let us also define $m \coloneqq |I|$ and $n \coloneqq |J|$ and note that $M = m + n$. We can expand

$$|\tilde{\varphi}\rangle_{S_IK_I} = \sum_{i_1,\ldots,i_m=0}^{K-1}\tilde{\alpha}_{i_1\ldots i_m}|i_1\ldots i_m\rangle_{K_I} \otimes |\tilde{\phi}_{i_1\ldots i_m}\rangle_{S_I}, \tag{C4}$$

$$|\bar{\varphi}\rangle_{S_JK_J} = \sum_{j_1,\ldots,j_n=0}^{K-1}\bar{\alpha}_{j_1\ldots j_n}|j_1\ldots j_n\rangle_{K_J} \otimes |\bar{\phi}_{j_1\ldots j_n}\rangle_{S_J}. \tag{C5}$$

Here, $\tilde{\alpha}_{i_1\ldots i_m} \in \mathbb{C}$ such that $\sum_{i_1,\ldots,i_m=0}^{K-1}|\tilde{\alpha}_{i_1\ldots i_m}|^2 = 1$ and $\bar{\alpha}_{j_1\ldots j_n} \in \mathbb{C}$ such that $\sum_{j_1,\ldots,j_n=0}^{K-1}|\bar{\alpha}_{j_1\ldots j_n}|^2 = 1$. Furthermore, it holds that

$$\mathrm{Tr}[\Pi^{\gamma,K}_{\overrightarrow{KS}}\varphi_{\overrightarrow{KS}}] = \mathrm{Tr}\left[\left(\frac{1}{K}\sum_{i,k=0}^{K-1}(|i\rangle\langle k|)^{\otimes M}_{\vec{K}} \otimes U^{(i^M)}_{\vec{S}}U^{(k^M)\dagger}_{\vec{S}}\right)\tilde{\varphi}_{K_IS_I} \otimes \bar{\varphi}_{K_JS_J}\right] \tag{C6}$$

$$= \frac{1}{K}\sum_{i,k=0}^{K-1}\tilde{\alpha}_{i^m}\bar{\alpha}_{i^n}(\tilde{\alpha}_{k^m})^*(\bar{\alpha}_{k^n})^*\mathrm{Tr}[U^{(i^M)\dagger}|\tilde{\phi}_{i^m}\rangle\langle\tilde{\phi}_{k^m}|_{S_I} \otimes |\bar{\phi}_{i^n}\rangle\langle\bar{\phi}_{k^n}|_{S_J}U^{(k^M)}] \tag{C7}$$

$$= \frac{1}{K}\sum_{i,k=0}^{K-1}\tilde{\alpha}_{i^m}\bar{\alpha}_{i^n}(\tilde{\alpha}_{k^m})^*(\bar{\alpha}_{k^n})^*\langle\zeta_k||\zeta_i\rangle, \tag{C8}$$

where we have defined the state

$$|\zeta_i\rangle_{\vec{S}} \coloneqq U^{(i^M)\dagger}|\tilde{\phi}_{i^m}\rangle_{S_I} \otimes |\bar{\phi}_{i^n}\rangle_{S_J}. \tag{C9}$$

We note that Eq. (C8) is a probability; in particular, it is real and non-negative. Hence, it holds that

$$\frac{1}{K}\sum_{i,k=0}^{K-1}\tilde{\alpha}_{i^m}\bar{\alpha}_{i^n}(\tilde{\alpha}_{k^m})^*(\bar{\alpha}_{k^n})^*\langle\zeta_k||\zeta_i\rangle \tag{C10}$$

$$= \left|\frac{1}{K}\sum_{i,k=0}^{K-1}\tilde{\alpha}_{i^m}\bar{\alpha}_{i^n}(\tilde{\alpha}_{k^m})^*(\bar{\alpha}_{k^n})^*\langle\zeta_k||\zeta_i\rangle\right| \tag{C11}$$

$$\leq \frac{1}{K}\sum_{i,k=0}^{K-1}|\tilde{\alpha}_{i^m}||\bar{\alpha}_{i^n}||\tilde{\alpha}_{k^m}||\bar{\alpha}_{k^n}||\langle\zeta_k||\zeta_i\rangle|, \tag{C12}$$

where in the first inequality, we have used the subadditivity and multiplicity of the absolute value of complex numbers. We note that for all i, k in the sum, $|\langle\zeta_k||\zeta_i\rangle| \leq 1$. Let us define $p_i = |\tilde{\alpha}_{i^m}|^2$ and note that $p_i \geq 0$ and $\sum_{i=0}^{K-1}p_i \leq 1$. Let us also define $q_i = |\bar{\alpha}_{i^n}|^2$ and note that $q_i \geq 0$ and $\sum_{i=0}^{K-1}q_i \leq 1$. Hence, there exist respective probability distributions $\{\hat{p}_i\}$ and $\{\hat{q}_i\}$ over $\{0,\ldots,K-1\}$ such that $p_i \leq \hat{p}_i$ and $q_i \leq \hat{q}_i$ for all $i = 0,\ldots,K-1$. We then obtain

$$\frac{1}{K}\sum_{i,k=0}^{K-1}|\tilde{\alpha}_{i^m}||\bar{\alpha}_{i^n}||\tilde{\alpha}_{k^m}||\bar{\alpha}_{k^n}||\langle\zeta_k||\zeta_i\rangle| \tag{C13}$$

$$\leq \frac{1}{K}\sum_{i,k=0}^{K-1}\sqrt{p_iq_ip_kq_k} = \frac{1}{K}\left[\sum_{i=0}^{K-1}\sqrt{p_iq_i}\right]^2 \tag{C14}$$

$$\leq \frac{1}{K}\left[\sum_{i=0}^{K-1}\sqrt{\hat{p}_i\hat{q}_i}\right]^2 \leq \frac{1}{K}, \tag{C15}$$

where we have used the fact that the classical fidelity between two probability distributions is upper bounded by 1. This establishes the theorem for pure biseparable states with respect to arbitrary bipartitions. Noting that every mixed biseparable state $\sigma_{\overrightarrow{KS}} \in \mathrm{BS}(:\overrightarrow{KS}:)$ can be expressed as a convex sum of pure biseparable states finishes the proof. ∎

APPENDIX D: UPPER BOUNDS ON THE CKA RATES OF MULTIPLEX CHANNELS

1. Proof of Theorem 2

Proof.—Let us consider any cppp-assisted protocol that achieves a rate $\hat{P}^{\mathcal{N}}_{\text{cppp}} \equiv \hat{P}$. Let $\rho^{(1)} \in \text{FS}(:\overrightarrow{LA'}:\overrightarrow{RB}:\vec{P}:)$ be a fully separable state generated by the first use of LOCC among all spatially separated allies. Let

$$\tau^{(1)}_{\overrightarrow{LA}\,\vec{R}\,\overrightarrow{PC}} := \mathcal{N}(\rho^{(1)}_{\overrightarrow{LA}\,\overrightarrow{RB}\,\vec{P}}). \tag{D1}$$

We note that $\tau^{(1)}$ is a separable state with respect to bipartition $\overrightarrow{LA}\,\vec{R}\,\vec{C}:\vec{P}$. The action of the decoder channel $\mathcal{D} := \mathcal{L}^{(2)}_{\overrightarrow{LA}\,\vec{R}\,\overrightarrow{PC}\to\overrightarrow{SK}}$ on $\tau^{(1)}$ yields the state

$$\omega_{\overrightarrow{SK}} := \mathcal{L}^{(2)}(\tau^{(1)}_{\overrightarrow{LA}\,\vec{R}\,\overrightarrow{PC}}). \tag{D2}$$

By assumption, we have that

$$F(\gamma_{\overrightarrow{SK}}, \omega_{\overrightarrow{SK}}) \geq 1-\varepsilon, \tag{D3}$$

for some (M-partite) private state γ, which implies that there exists a projector $\Pi^{\gamma}_{\overrightarrow{SK}}$ corresponding to a γ-privacy test such that (see Proposition 1)

$$\text{Tr}[\Pi^{\gamma}_{\overrightarrow{SK}}\omega_{\overrightarrow{SK}}] \geq 1-\varepsilon. \tag{D4}$$

From Theorem 1,

$$\text{Tr}[\Pi^{\gamma}_{\overrightarrow{SK}}\sigma'_{\overrightarrow{SK}}] \leq \frac{1}{K} = 2^{-\hat{P}}, \tag{D5}$$

for any $\sigma' \in \text{BS}(:\overrightarrow{SK}:)$.

Let us suppose a state $\sigma_{\overrightarrow{LA}\,\vec{R}\,\overrightarrow{PC}} \in \text{BS}(:\overrightarrow{LA}:\vec{R}:\overrightarrow{PC}:)$ of the form $\sigma_{\overrightarrow{LA}\,\vec{R}\,\overrightarrow{PC}} = \sigma_{\overrightarrow{LA}\,\vec{R}\,\vec{C}} \otimes \sigma_{\vec{P}}$, where $\sigma_{\overrightarrow{LA}\,\vec{R}\,\vec{C}}$ is arbitrary. It holds that $\sigma_{\overrightarrow{SK}} := \mathcal{L}^{(2)}(\sigma_{\overrightarrow{LA}\,\vec{R}\,\overrightarrow{PC}}) \in \text{BS}(:\overrightarrow{SK}:)$. Thus, the privacy test is feasible for $D^{\varepsilon}_h(\omega\|\sigma)$, and we find that

$$\hat{P} \leq D^{\varepsilon}_h(\omega_{\overrightarrow{SK}}\|\sigma_{\overrightarrow{SK}}) \tag{D6}$$

$$\leq D^{\varepsilon}_h(\tau^{(1)}_{\overrightarrow{LA}\,\vec{R}\,\overrightarrow{PC}}\|\sigma_{\overrightarrow{LA}\,\vec{R}\,\overrightarrow{PC}}) \tag{D7}$$

$$\leq \sup_{\psi\in\text{FS}(\overrightarrow{LA'}:\overrightarrow{RB}:\vec{P})} D^{\varepsilon}_h(\mathcal{N}(\psi_{\overrightarrow{LA'}:\overrightarrow{RB}:\vec{P}})\|\sigma_{\overrightarrow{LA}\,\vec{R}\,\overrightarrow{PC}}) \tag{D8}$$

$$= \sup_{\psi\in\text{FS}(\overrightarrow{LA'}:\overrightarrow{RB})} D^{\varepsilon}_h(\mathcal{N}(\psi_{\overrightarrow{LA'}:\overrightarrow{RB}})\|\sigma_{\overrightarrow{LA}\,\vec{R}\,\vec{C}}). \tag{D9}$$

The second inequality follows from the data-processing inequality. The third inequality follows from the quasiconvexity of D^{ε}_h. The equality follows from Eq. (A2) and a suitable choice of $\sigma_{\vec{P}}$ that always exists because, for any pure state $\psi \in \text{FS}(\overrightarrow{LA'}:\overrightarrow{RB}:\vec{P})$, the output state $\mathcal{N}(\psi)$ is separable with respect to the bipartition $\overrightarrow{LA}\,\vec{R}\,\vec{C}:\vec{P}$.

Since inequality (D9) also holds for an arbitrary $\sigma \in \text{BS}(:\overrightarrow{LA}:\vec{R}:\vec{C}:)$, we can conclude that

$$\hat{P} \leq E^{\varepsilon}_{h,\text{GE}}(\mathcal{N}). \tag{D10}$$

■

2. Proof of Theorem 3

Proof.—The following inequality holds for an (n, K, ε) LOCC-assisted secret-key-agreement protocol over a multiplex channel $\mathcal{N}$:

$$F(\omega_{\overrightarrow{SK}}, \gamma_{\overrightarrow{SK}}) \geq 1-\varepsilon. \tag{D11}$$

For any $\sigma_{\overrightarrow{SK}} \in \text{FS}(:\overrightarrow{SK}:)$, we have the following bound due to inequality (D11) and Theorem 1:

$$\log_2 K \leq D^{\varepsilon}_h(\omega_{\overrightarrow{SK}}\|\sigma_{\overrightarrow{SK}}). \tag{D12}$$

Employing inequality (A8) in the limit $\alpha \to +\infty$, we obtain

$$\log_2 K \leq D^{\varepsilon}_h(\omega_{\overrightarrow{SK}}\|\sigma_{\overrightarrow{SK}}) \tag{D13}$$

$$\leq D_{\max}(\omega_{\overrightarrow{SK}}\|\sigma_{\overrightarrow{SK}}) + \log_2\left(\frac{1}{1-\varepsilon}\right). \tag{D14}$$

The above inequality holds for arbitrary $\sigma \in \text{FS}(:\overrightarrow{SK}:)$; therefore,

$$\log_2 K \leq E_{\max,E}(:\overrightarrow{SK}:)_{\omega} + \log_2\left(\frac{1}{1-\varepsilon}\right), \tag{D15}$$

where $E_{\max,E}(:\overrightarrow{SK}:)_{\omega}$ is the max-relative entropy of entanglement of the state $\omega_{\overrightarrow{SK}}$.

The max-relative entropy of entanglement $E_{\max,E}$ of a state is monotonically nonincreasing under the action of LOCC channels, and it is zero for states that are fully separable. Using these facts, we get that

$$E_{\max,E}(:\overrightarrow{SK}:)_\omega$$

$$\leq E_{\max,E}(:\overrightarrow{L^{(n)}A^{(n)}}:\overrightarrow{R^{(n)}}:\overrightarrow{P^{(n)}C^{(n)}}:)_{\tau_n} \tag{D16}$$

$$= E_{\max,E}(:\overrightarrow{L^{(n)}A^{(n)}}:\overrightarrow{R^{(n)}}:\overrightarrow{P^{(n)}C^{(n)}}:)_{\tau_n} - E_{\max,E}(:\overrightarrow{L^{(1)}A^{(1)'}}:\overrightarrow{R^{(1)}B^{(1)}}:\overrightarrow{P^{(1)}}:)_{\rho_1} \tag{D17}$$

$$= E_{\max,E}(:\overrightarrow{L^{(n)}A^{(n)}}:\overrightarrow{R^{(n)}}:\overrightarrow{P^{(n)}C^{(n)}}:)_{\tau_n} + \left[\sum_{i=2}^{n} E_{\max,E}(:\overrightarrow{L^{(i)}A^{(i)'}}:\overrightarrow{R^{(i)}B^{(i)}}:\overrightarrow{P^{(i)}}:)_{\rho_i} - \sum_{i=2}^{n} E_{\max,E}(:\overrightarrow{L^{(i)}A^{(i)'}}:\overrightarrow{R^{(i)}B^{(i)}}:\overrightarrow{P^{(i)}}:)_{\rho_i}\right] - E_{\max,E}(:\overrightarrow{L^{(1)}A^{(1)'}}:\overrightarrow{R^{(1)}B^{(1)}}:\overrightarrow{P^{(1)}}:)_{\rho_1} \tag{D18}$$

$$\leq \sum_{i=1}^{n} [E_{\max,E}(:\overrightarrow{L^{(i)}A^{(i)}}:\overrightarrow{R^{(i)}}:\overrightarrow{P^{(i)}C^{(i)}}:)_{\tau_i} - E_{\max,E}(:\overrightarrow{L^{(i)}A^{(i)'}}:\overrightarrow{R^{(i)}B^{(i)}}:\overrightarrow{P^{(i)}}:)_{\rho_i}] \tag{D19}$$

$$\leq nE_{\max,E}(\mathcal{N}). \tag{D20}$$

The first equality follows because $E_{\max,E}(:\overrightarrow{L^{(1)}A^{(1)'}}:\overrightarrow{R^{(1)}B^{(1)}}:\overrightarrow{P^{(1)}}:)_{\rho_1} = 0$. The second inequality follows because $E_{\max,\mathrm{GE}}$ is monotone under LOCC channels and $\rho_i = \mathcal{L}^i(\tau_{i-1})$ for all $i \in \{2,3,\ldots,n\}$. The final inequality follows from Lemma 1.

From inequalities (D15) and (D20), we conclude that

$$\log_2 K \leq nE_{\max,E}(\mathcal{N}) + \log_2\left(\frac{1}{1-\varepsilon}\right). \tag{D21}$$

■

3. Proof of Theorem 4

Proof.—For an (n, K, ε) LOCC-assisted secret-key-agreement protocol over a multiplex channel $\mathcal{N}$, such that $F(\omega_{\overrightarrow{SK}}, \gamma_{\overrightarrow{SK}}) \geq 1-\varepsilon$, due to inequality (D11) and Theorem 1, it holds for any $\sigma_{\overrightarrow{SK}} \in \mathrm{FS}(:\overrightarrow{SK}:)$: that

$$\log_2 K \leq D_h^\varepsilon(\omega_{\overrightarrow{SK}} \| \sigma_{\overrightarrow{SK}}). \tag{D22}$$

Using the fact that [94]

$$D_h^\varepsilon(\omega_{\overrightarrow{SK}} \| \sigma_{\overrightarrow{SK}}) \leq \frac{1}{1-\varepsilon}\left[D(\omega_{\overrightarrow{SK}} \| \sigma_{\overrightarrow{SK}}) + h(\varepsilon)\right], \tag{D23}$$

where h is the binary entropy function, and that the bound (D22) holds for arbitrary $\sigma \in \mathrm{FS}(:\overrightarrow{SK}:)$, we obtain

$$\log_2 K \leq \frac{1}{1-\varepsilon}[E_E(:\overrightarrow{SK}:)_\omega + h(\varepsilon)]. \tag{D24}$$

As the relative entropy of entanglement of a state is monotonically nonincreasing under the action of LOCC channels and vanishes for states that are fully separable, we can repeat the argument in inequalities (D16)–(D20) and obtain

$$E_E(:\overrightarrow{SK}:)_\omega \leq nE_E^p(\mathcal{N}) \leq nE_E^\infty(\mathcal{N}), \tag{D25}$$

where the second inequality follows from Lemma 2. Taking the limits $\varepsilon \to 0$ and $n \to \infty$, we obtain

$$\hat{\mathcal{P}}_{\mathrm{LOCC}}(\mathcal{N}) \leq E_E^\infty(\mathcal{N}), \tag{D26}$$

showing the converse. As for the strong converse, we follow the argument used in Ref. [49]: From inequalities (D22) and (A8), we obtain

$$\log_2 K \leq \tilde{E}_{\alpha,E}(:\overrightarrow{SK}:)_\omega + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right), \tag{D27}$$

where $\alpha \in (1,\infty)$ and $\tilde{E}_{\alpha,E}(:\overrightarrow{SK}:)_\omega$ is the sandwiched Rényi relative entropy of entanglement of the state $\omega_{\overrightarrow{SK}}$. Rewriting inequality (D27), we obtain

$$\epsilon \geq 1 - 2^{-n\frac{\alpha-1}{\alpha}\left(\frac{\log_2 K}{n} - \frac{1}{n}\tilde{E}_{\alpha,E}(:\overrightarrow{SK}:)_\omega\right)}. \tag{D28}$$

Assuming that the rate $\log_2 K/n$ exceeds $E_E^\infty(\mathcal{N})$, by inequality (D25), it will be larger than $(1/n)E_E(:\overrightarrow{SK}:)_\omega$. Hence, there exists an $\alpha > 1$, such that $(\log_2 K/n) - (1/n)\tilde{E}_{\alpha,E}(:\overrightarrow{SK}:)_\omega > 0$, and the error increases to 1 exponentially. ■

4. Proof of Theorem 5

Let $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$ be a multipartite quantum channel that is tele-covariant with respect to groups $\{\mathcal{G}_a\}_{a\in\mathcal{A}}$ and $\{\mathcal{G}_b\}_{b\in\mathcal{B}}$ as defined in Sec. V C. By definition, for all $a \in \mathcal{A}$ and $b \in \mathcal{B}$, we have

$$\frac{1}{G_a}\sum_{g_a} \mathcal{U}_{A_a''}^{g_a}(\Phi^+_{A_a''L_a}) = \frac{\mathbb{1}_{A_a''}}{|A_a''|} \otimes \frac{\mathbb{1}_{L_a}}{|L_a|}, \tag{D29}$$

$$\frac{1}{G_b}\sum_{g_b} \mathcal{U}_{B_b'}^{g_b}(\Phi^+_{B_b'R_b}) = \frac{\mathbb{1}_{B_b'}}{|B_b'|} \otimes \frac{\mathbb{1}_{R_b}}{|R_b|}, \tag{D30}$$

respectively, where $A''_a \simeq L_a$, $B'_b \simeq R_b$, and Φ^+ denotes an EPR state. Note that in order for each $\{U^{g_a}_{A''_a}\}$ and $\{U^{g_b}_{B'_b}\}$ to be one-designs, it is necessary that $|A''_a|^2 \leq G_a$ and $|B'_b|^2 \leq G_b$ [153].

For every $a \in \mathcal{A}$ and every $b \in \mathcal{B}$, we can now define $\{E^{g_a}_{A''_a L_a}\}_{g_a}$ and $\{E^{g_b}_{B'_b R_b}\}_{g_b}$, with respective elements defined as

$$E^{g_a}_{A''_a L_a} := \frac{|A'_a|^2}{G_a} U^{g_a}_{A''_a} \Phi^+_{A''_a L_a} (U^{g_a}_{A''_a})^\dagger, \tag{D31}$$

$$E^{g_b}_{B'_b R_b} := \frac{|B_b|^2}{G_b} U^{g_b}_{B'_b} \Phi^+_{B'_b R_b} (U^{g_b}_{B'_b})^\dagger, \tag{D32}$$

where $A'_a \simeq A''_a$ and $B_b \simeq B'_b$. It follows from the fact that $|A'_a|^2 \leq G_a$ and $|B_b|^2 \leq G_b$ as well as Eqs. (D29) and (D30) that $\{E^{g_a}_{A''_a L_a}\}_{g_a}$ and $\{E^{g_b}_{B'_b R_b}\}_{g_b}$ are valid POVMs for all $a \in \mathcal{A}$ and $b \in \mathcal{B}$.

The simulation of the channel $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$ via teleportation begins with a state $\rho_{\vec{A}''\vec{B}'}$ and a shared resource $\theta_{\overrightarrow{LA}\vec{R}\vec{C}} = \mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}(\Phi^+_{\vec{L}\vec{R}|\vec{A}'\vec{B}})$. The desired outcome is for the receivers to receive the state $\mathcal{N}(\rho_{\vec{A}''\vec{B}'})$ and for the protocol to work independently of the input state $\rho_{\vec{A}''\vec{B}'}$. The first step is for senders $\mathbf{A}_a$ and $\mathbf{B}_b$ to locally perform the measurement $\{\bigotimes_{a\in\mathcal{A}} E^{g_a}_{A''_a L_a} \otimes \bigotimes_{b\in\mathcal{B}} E^{g_b}_{B'_b R_b}\}_{\vec{g}}$ and then send the outcomes $\vec{g}$ to the receivers. Based on the outcomes $\vec{g}$, the receivers $\mathbf{A}_a$ and $\mathbf{C}_c$ then perform $W^{\vec{g}}_{A_a}$ and $W^{\vec{g}}_{C_c}$, respectively. The following analysis demonstrates that this protocol works by simplifying the form of the postmeasurement state:

$$\left(\prod_{a\in\mathcal{A}} G_a \prod_{b\in\mathcal{B}} G_b\right) \mathrm{Tr}_{\overrightarrow{A''L}\,\overrightarrow{B'R}} \left[\left(\bigotimes_{a\in\mathcal{A}} E^{g_a}_{A''_a L_a} \otimes \bigotimes_{b\in\mathcal{B}} E^{g_b}_{B'_b R_b}\right)\left(\rho_{\vec{A}\vec{B}'} \otimes \theta_{\overrightarrow{LA}\vec{R}\vec{C}}\right)\right]$$

$$= \left(\prod_{a\in\mathcal{A}} |A'_a|^2 \prod_{b\in\mathcal{B}} |B_b|^2\right) \mathrm{Tr}_{\overrightarrow{A''L}\,\overrightarrow{B'R}} \left\{\left[\bigotimes_{a\in\mathcal{A}} U^{g_a}_{A''_a} \Phi^+_{A''_a L_a} U^{g_a\,\dagger}_{A''_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{B'_b} \Phi^+_{B'_b R_b} U^{g_b\,\dagger}_{B'_b}\right](\rho_{\vec{A}\vec{B}'} \otimes \theta_{\overrightarrow{LA}\vec{R}\vec{C}})\right\} \tag{D33}$$

$$= \left(\prod_{a\in\mathcal{A}} |A'_a|^2 \prod_{b\in\mathcal{B}} |B_b|^2\right) \langle\Phi^+|_{\overrightarrow{A''}\,\overrightarrow{B'}|\vec{L}\vec{R}} \left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{A''_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{B'_b}\right)^\dagger \rho_{\vec{A}\,\overrightarrow{B'}} \otimes \theta_{\overrightarrow{LA}\vec{R}\vec{C}} \left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{A''_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{B'_b}\right) |\Phi^+\rangle_{\overrightarrow{A''}\,\overrightarrow{B'}|\vec{L}\vec{R}} \tag{D34}$$

$$= \left(\prod_{a\in\mathcal{A}} |A'_a|^2 \prod_{b\in\mathcal{B}} |B_b|^2\right) \langle\Phi^+|_{\overrightarrow{A''}\,\overrightarrow{B'}|\vec{L}\vec{R}} \left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{A''_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{B'_b}\right)^\dagger \rho_{\vec{A}\,\overrightarrow{B'}} \left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{A''_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{B'_b}\right) \otimes \theta_{\overrightarrow{LA}\vec{R}\vec{C}} |\Phi^+\rangle_{\overrightarrow{A''}\,\overrightarrow{B'}|\vec{L}\vec{R}} \tag{D35}$$

$$= \left(\prod_{a\in\mathcal{A}} |A'_a|^2 \prod_{b\in\mathcal{B}} |B_b|^2\right) \langle\Phi^+|_{\overrightarrow{A''}\,\overrightarrow{B'}|\vec{L}\vec{R}} \left[\left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{L_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{R_b}\right)^\dagger \rho_{\vec{L}\vec{R}} \left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{L_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{R_b}\right)\right]^* \theta_{\overrightarrow{LA}\vec{R}\vec{C}} |\Phi^+\rangle_{\overrightarrow{A''}\,\overrightarrow{B'}|\vec{L}\vec{R}}. \tag{D36}$$

The first three equalities follow by substitution and some rewriting. The fourth equality follows from the fact that

$$\langle\Phi|_{A'A} M_{A'} = \langle\Phi|_{A'A} M^*_A \tag{D37}$$

for any operator M, where $*$ denotes the complex conjugate, taken with respect to the basis in which $|\Phi\rangle_{A'A}$ is defined. Continuing, we have that

$$\text{Eq. (D36)} = \left(\prod_{a\in\mathcal{A}} \left|A'_a\right| \prod_{b\in\mathcal{B}} \left|B_b\right|\right) \mathrm{Tr}_{\vec{L}\vec{R}} \left\{\left[\left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{L_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{R_b}\right)^\dagger \rho_{\vec{L}\vec{R}} \left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{L_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{R_b}\right)\right]^* \mathcal{N}_{\overrightarrow{A'}\vec{B}\to\vec{A}\vec{C}} \left(\Phi^+_{\vec{L}\vec{R}|\overrightarrow{A'}\vec{B}}\right)\right\} \tag{D38}$$

$$= \left(\prod_{a\in\mathcal{A}} \left|A'_a\right| \prod_{b\in\mathcal{B}} \left|B_b\right|\right) \mathrm{Tr}_{\vec{L}\vec{R}} \left[\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}} \left(\left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{A'_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{B_b}\right)^\dagger \rho_{\vec{A}'\vec{B}} \left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{A'_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{B_b}\right) \Phi^+_{\vec{L}\vec{R}|\overrightarrow{A'}\vec{B}}\right)\right] \tag{D39}$$

$$= \mathcal{N}_{\overrightarrow{A'}\vec{B}\to\vec{A}\vec{C}} \left(\left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{A'_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{B_b}\right)^\dagger \rho_{\overrightarrow{A'}\vec{B}} \left(\bigotimes_{a\in\mathcal{A}} U^{g_a}_{A'_a} \otimes \bigotimes_{b\in\mathcal{B}} U^{g_b}_{B_b}\right)\right) \tag{D40}$$

$$= \left(\bigotimes_{a\in\mathcal{A}} W^{\vec{g}}_{A_a} \otimes \bigotimes_{c\in\mathcal{C}} W^{\vec{g}}_{C_c}\right)^\dagger \mathcal{N}_{\overrightarrow{A'}\vec{B}\to\vec{A}\vec{C}} \left(\rho_{\overrightarrow{A'}\vec{B}}\right) \left(\bigotimes_{a\in\mathcal{A}} W^{\vec{g}}_{A_a} \otimes \bigotimes_{c\in\mathcal{C}} W^{\vec{g}}_{C_c}\right). \tag{D41}$$

The first equality follows because $|A|\langle\Phi|_{A'A}(\mathbb{1}_{A'} \otimes M_{AB})|\Phi\rangle_{A'A} = \mathrm{Tr}_A\{M_{AB}\}$ for any operator M_{AB}. The second equality follows by applying the conjugate transpose of Eq. (D37). The final equality follows from the covariance property of the channel.

Thus, if the receivers finally perform the unitaries $\bigotimes_{a\in\mathcal{A}} W^{\vec{g}}_{A_a} \otimes \bigotimes_{c\in\mathcal{C}} W^{\vec{g}}_{C_c}$ upon receiving $\vec{g}$ via a classical channel from the senders, then the output of the protocol is $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}(\rho_{\vec{A}'\vec{B}})$, so this protocol simulates the action of the multipartite channel $\mathcal{N}$ on the state ρ. ∎

5. Proof of Theorem 6

Before proving Theorem 6, we need the following lemma, which generalizes Lemma 7 in Ref. [62]:

Lemma 4: Let $\mathcal{T} = \{U^{tw\dagger}\rho_{\overrightarrow{SK}}U^{tw} : \rho_{\overrightarrow{SK}} \in \mathrm{BS}(:\overrightarrow{SK}:)\}$ be the set of twisted biseparable states. Then, for any $\sigma_{\overrightarrow{SK}} \in \mathcal{T}$, it holds that

$$D(\Phi_{\vec{K}}||\sigma_{\vec{K}}) \geq \log K. \tag{D42}$$

Proof.—Let $\sigma_{\overrightarrow{SK}} \in \mathcal{T}$, i.e., $\sigma_{\overrightarrow{SK}} = U^{tw\dagger}\rho_{\overrightarrow{SK}}U^{tw}$ for some twisting unitary U^{tw} and biseparable $\rho_{\overrightarrow{SK}}$. Here, U^{tw} defines a privacy test $\Pi^{\gamma}_{\overrightarrow{SK}} = U^{tw}(\Phi_{\vec{K}} \otimes \mathbb{1}_{\vec{S}})U^{tw\dagger}$. By Theorem 6, it then holds that

$$\mathrm{Tr}[\Phi_{\vec{K}}\sigma_{\vec{K}}] = \mathrm{Tr}[\Pi^{\gamma}_{\overrightarrow{SK}}\rho_{\overrightarrow{SK}}] \leq \frac{1}{K}. \tag{D43}$$

By the concavity of the logarithm, it then holds that

$$D(\Phi_{\vec{K}}||\sigma_{\vec{K}}) = -S(\Phi_{\vec{K}}) - \mathrm{Tr}[\Phi_{\vec{K}}\log\sigma_{\vec{K}}] \tag{D44}$$

$$\geq -\log\mathrm{Tr}[\Phi_{\vec{K}}\sigma_{\vec{K}}] \tag{D45}$$

$$\geq \log K, \tag{D46}$$

finishing the proof. ∎

Now, we can follow Ref. [48] to prove Theorem 6:

Proof of Theorem 6.—Let $\epsilon > 0$ and $n \in \mathbb{N}$. We begin by noting that in the case of teleportation-simulable multiplex channels, LOCC assistance does not enhance secret-key-agreement capacity, and the original protocol can be reduced to a cppp-assisted secret-key-agreement protocol [48]. Namely, in every round $1 \leq i \leq n$, it holds that

$$\rho_i = \mathcal{L}^i(\tau_i) = \mathcal{L}^i(\mathcal{N}_{\overrightarrow{A'^{(i-1)}B^{(i-1)}}\to\overrightarrow{A^{(i-1)}C^{(i-1)}}}(\rho_{i-1})) \tag{D47}$$

$$= \mathcal{L}^i(\mathcal{T}_{\overrightarrow{A'^{(i-1)}LAB^{(i-1)}R\,C}\to\overrightarrow{A^{(i-1)}C^{(i-1)}}}(\theta_{\overrightarrow{LAR}\vec{C}}\otimes\rho_{i-1})), \tag{D48}$$

where $\mathcal{L}^i$ and $\mathcal{T}$ are LOCC. As the initial state ρ_0 is assumed to be fully separable, we find that the final state $\omega_{\overrightarrow{SK}} = \rho_n$ of an adaptive LOCC CKA protocol, involving n uses of the teleportation-simulable multiplex channel $\mathcal{N}_{\vec{A}'\vec{B}\to\vec{A}\vec{C}}$, can be expressed as

$$\omega_{\overrightarrow{SK}} = \mathcal{L}_{\overrightarrow{L^nA^n}\,\overrightarrow{R^n}\,\overrightarrow{C^n}\to\overrightarrow{SK}}(\theta^{\otimes n}_{\overrightarrow{LA}\vec{R}\vec{C}}), \tag{D49}$$

where $\mathcal{L}$ is an LOCC operation with respect to the partition $:\overrightarrow{L^nA^n}:\overrightarrow{R^n}:\overrightarrow{C^n}:$. By assumption, it holds that $\|\omega_{\overrightarrow{SK}} - \gamma_{\overrightarrow{KS}}\|_1 \leq \epsilon$ for some m-partite private state $\gamma_{\overrightarrow{KS}} = U^{tw}(\Phi_{\vec{K}} \otimes \tau_{\vec{S}})U^{tw\dagger}$, where m is the number of parties. Let $\tilde{\sigma}_{\overrightarrow{L^nA^n}\,\overrightarrow{R^n}\,\overrightarrow{C^n}} \in \mathrm{BS}(:\overrightarrow{L^nA^n}:\overrightarrow{R^n}:\overrightarrow{C^n}:)$. Following the proof of Theorem 9 in Ref. [62], we obtain

$$D(\theta^{\otimes n}_{\overrightarrow{LA}\vec{R}\vec{C}}||\tilde{\sigma})$$

$$\geq D(\omega_{\overrightarrow{SK}}||\mathcal{L}(\tilde{\sigma}_{\overrightarrow{L^nA^n}\,\overrightarrow{R^n}\,\overrightarrow{C^n}})) \tag{D50}$$

$$= D(U^{tw\dagger}\omega_{\overrightarrow{SK}}U^{tw}||U^{tw\dagger}\mathcal{L}(\tilde{\sigma}_{\overrightarrow{L^nA^n}\,\overrightarrow{R^n}\,\overrightarrow{C^n}})U^{tw}) \tag{D51}$$

$$\geq \inf_{\sigma_{\overrightarrow{SK}}\in\mathcal{T}} D(\mathrm{Tr}_{\vec{S}}[U^{tw\dagger}\omega_{\overrightarrow{SK}}U^{tw}]||\sigma_{\vec{K}}) \tag{D52}$$

$$\geq \inf_{\sigma_{\overrightarrow{SK}}\in\mathcal{T}} D(\Phi_{\vec{K}}||\sigma_{\vec{K}}) - 4m\epsilon\log K - h(\epsilon) \tag{D53}$$

$$\geq (1 - 4m\epsilon)\log K - h(\epsilon), \tag{D54}$$

where, in the last two inequalities, we have used the asymptotic continuity of the relative entropy and Lemma 4, respectively. Letting $n \to \infty$ and $\epsilon \to 0$, we finish the proof. ∎

6. Proof of Theorem 7

As in the proof of Theorem 6, we have

$$\omega_{\overrightarrow{SK}} = \mathcal{L}_{\overrightarrow{L^nA^n}\,\overrightarrow{R^n}\,\overrightarrow{C^n}\to\overrightarrow{SK}}(\theta^{\otimes n}_{\overrightarrow{LA}\vec{R}\vec{C}}), \tag{D55}$$

where $\mathcal{L}$ is an LOCC operation with respect to the partition $:\overrightarrow{L^nA^n}:\overrightarrow{R^n}:\overrightarrow{C^n}:$. Now, following the proof of Theorem 2, we have that

$$F(\gamma_{\overrightarrow{SK}}, \omega_{\overrightarrow{SK}}) \geq 1 - \varepsilon, \tag{D56}$$

for some private state γ; hence, there exists a projector $\Pi^{\gamma}_{\overrightarrow{SK}}$ corresponding to a γ-privacy test such that (see Proposition 1)

$$\mathrm{Tr}[\Pi^{\gamma}_{\overrightarrow{SK}}\omega_{\overrightarrow{SK}}] \geq 1 - \varepsilon. \tag{D57}$$

On the other hand, from Theorem 1, we have

$$\mathrm{Tr}[\Pi^{\gamma}_{\overrightarrow{SK}}\sigma_{\overrightarrow{SK}}] \leq \frac{1}{K}, \tag{D58}$$

for any $\sigma \in \mathrm{FS}(:\overrightarrow{SK}:)$. Let us suppose a state $\sigma'_{\overrightarrow{LA}\vec{R}\vec{C}} \in \mathrm{FS}(:\overrightarrow{LA}:\vec{R}:\vec{C}:)$, and let us define $\sigma_{\overrightarrow{SK}} = \mathcal{L}_{\overrightarrow{L^nA^n}\overrightarrow{R^n}\overrightarrow{C^n}\to\overrightarrow{SK}}(\sigma'^{\otimes n}_{\overrightarrow{LA}\vec{R}\vec{C}})$, which is in $\mathrm{FS}(:\overrightarrow{SK}:)$. Hence, for all $\alpha > 1$, it holds that

$$\log_2 K \leq D^{\varepsilon}_h\left(\omega_{\overrightarrow{SK}}\middle\|\sigma_{\overrightarrow{SK}}\right) \tag{D59}$$

$$\leq D^{\varepsilon}_h\left(\theta^{\otimes n}_{\overrightarrow{LA}\vec{R}\vec{C}}\middle\|\sigma'^{\otimes n}_{\overrightarrow{LA}\vec{R}\vec{C}}\right) \tag{D60}$$

$$\leq \tilde{D}_{\alpha}\left(\theta^{\otimes n}_{\overrightarrow{LA}\vec{R}\vec{C}}\middle\|\sigma'^{\otimes n}_{\overrightarrow{LA}\vec{R}\vec{C}}\right) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\epsilon}\right) \tag{D61}$$

$$= n\tilde{D}_{\alpha}\left(\theta_{\overrightarrow{LA}\vec{R}\vec{C}}\middle\|\sigma'_{\overrightarrow{LA}\vec{R}\vec{C}}\right) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\epsilon}\right). \tag{D62}$$

The first inequality holds for any $\sigma \in \mathrm{FS}(\overrightarrow{SK})$. The second inequality follows from the data-processing inequality. The third inequality follows from Eq. (A8). The equality is due to the additivity of $\tilde{D}_{\alpha}$ [64]. As the above holds for any $\sigma'_{\overrightarrow{LA}\vec{R}\vec{C}} \in \mathrm{FS}(:\overrightarrow{LA}:\vec{R}:\vec{C}:)$, we obtain Theorem 7.

APPENDIX E: REPEATER AS A MULTIPARTITE CHANNEL

In order to provide bounds for more repeater protocols that involve two-way communication between Alice and Charlie or between Bob and Charlie before Charlie's measurement, we have to slightly generalize our results in Sec. V. Namely, in addition to trusted parties $\{\mathbf{X}_i\}_{i=1}^{M} = \{\mathbf{A}_a\}_a \cup \{\mathbf{B}_b\}_b \cup \{\mathbf{C}_c\}_c$, we can add a number of cooperative but untrusted parties $\{\tilde{\mathbf{X}}_i\}_{i=1}^{\tilde{M}} := \{\tilde{\mathbf{A}}_{\tilde{a}}\}_{\tilde{a}\in\tilde{\mathcal{A}}} \cup \{\tilde{\mathbf{B}}_{\tilde{b}\in\tilde{\mathcal{B}}}\}_{\tilde{b}} \cup \{\tilde{\mathbf{C}}_{\tilde{c}\in\tilde{\mathcal{C}}}\}_{\tilde{c}}$. Let us denote the quantum systems hold by respective untrusted parties as $\widetilde{A'}_{\tilde{a}}, \tilde{L}_{\tilde{a}}, \tilde{A}_{\tilde{a}}, \tilde{B}_{\tilde{b}}, \tilde{R}_{\tilde{b}}, \tilde{C}_{\tilde{c}}, \tilde{P}_{\tilde{c}}$ and redefine

$$\vec{A'} := \{A'_a\}_{a\in\mathcal{A}} \cup \{\widetilde{A'}_{\tilde{a}}\}_{\tilde{a}\in\tilde{\mathcal{A}}}, \vec{A} := \{A_a\}_{a\in\mathcal{A}} \cup \{\tilde{A}_{\tilde{a}}\}_{\tilde{a}\in\tilde{\mathcal{A}}},$$
$$\vec{L} := \{L_a\}_{a\in\mathcal{A}} \cup \{\tilde{L}_{\tilde{a}}\}_{\tilde{a}\in\tilde{\mathcal{A}}},$$
$$\vec{B} := \{B_b\}_{b\in\mathcal{B}} \cup \{\tilde{B}_{\tilde{b}}\}_{\tilde{b}\in\tilde{\mathcal{B}}}, \vec{R} := \{R_b\}_{b\in\mathcal{B}} \cup \{\tilde{R}_{\tilde{b}}\}_{\tilde{b}\in\tilde{\mathcal{B}}},$$
$$\vec{C} := \{C_c\}_{c\in\mathcal{C}} \cup \{\tilde{C}_{\tilde{c}}\}_{\tilde{c}\in\tilde{\mathcal{C}}}, \vec{P} := \{P_c\}_{c\in\mathcal{B}} \cup \{\tilde{P}_{\tilde{c}}\}_{\tilde{c}\in\tilde{\mathcal{C}}},$$

while keeping the old definitions for $\vec{K}$ and $\vec{S}$. We then assume that we have a multiplex channel $\mathcal{N}_{\vec{A'}\vec{B}\to\vec{A}\vec{C}}$ and LOCC operations $\mathcal{L}^i$, for $i = 1, \ldots, n$, among trusted and untrusted parties. However, we assume that as part of the last round of LOCC, $\mathcal{L}^{n+1}$, all subsystems belonging to untrusted parties are traced out, resulting in a state $\omega_{\overrightarrow{SK}}$ among the trusted parties only. It is now easy to show that the proofs of Theorems 3 and 4 also go through in this slightly generalized scenario. Namely, tracing out parties in a fully separable state results in a fully separable state on the remaining parties, and by the monotonicity of the generalized divergences, inequalities (D16) and (D25) also hold if we trace out the untrusted parties in order to obtain ω. Note that the same does not hold true in the case of Theorem 2, where we have the distance to the set of biseparable states, which is not preserved under the trace-out.

Returning to the quantum key repeater, we can now identify Alice and Bob as two trusted parties and Charlie as an untrusted party and define a multiplex channel as the tensor product of the two channels from Alice to Charlie and Bob to Charlie, namely, $\mathcal{N}^{\mathrm{repeater}}_{AB\to C} := \mathcal{N}^{1}_{A\to C_A} \otimes \mathcal{N}^{2}_{B\to C_B}$, with $C := C_A C_B$. We include the local state preparation by Alice and Bob; the LOCC performed by Alice, Charlie, and Bob during key distillation protocols; and Bob's entanglement-swapping measurement and subsequent classical communication into the LOCC operations that interleave the uses of $\mathcal{N}^{\mathrm{repeater}}_{AB\to C}$. Crucially, the final LOCC operation has to include the trace-out of Charlie's system, as he is an untrusted party. Application of the generalized versions of Theorem 3 or Theorem 4 then provides us with an upper bound on the achievable key rate in terms of $\min\{E_{\max,E}(\mathcal{N}^{\mathrm{repeater}}_{AB\to C}), E^{\infty}_{E}(\mathcal{N}^{\mathrm{repeater}}_{AB\to C})\}$. As has been shown in Ref. [74], there are examples of channels acting on finite-dimensional systems where the regularized relative entropy of entanglement is strictly less than max-relative entropy of entanglement, in which case, Theorem 4 provides tighter bounds than the ones provided in Ref. [50]. For tele-covariant channels, we can invoke Remark 5 and Theorem 5 to obtain bounds in terms of the relative entropy of entanglement.

Let us now consider repeater chains with more than a single repeater station. We assume a protocol where each channel has to be used the same number of times to get the desired fidelity. We consider Alice and Bob as trusted parties and the repeater stations $C_1, \ldots, C_l$ as cooperative but untrusted parties. Defining a multiplex channel $\mathcal{N}^{\mathrm{repeater\ chain}}_{AC'_1,\ldots,C'_l\to C_1,\ldots,C_lB} := \mathcal{N}^{1}_{A\to C_1} \otimes \mathcal{N}^{2}_{C'_1\to C_2} \otimes \ldots \otimes \mathcal{N}^{l}_{C'_{l-1}\to C'_l} \otimes \mathcal{N}^{l+1}_{C'_l\to B}$ and including entanglement purification and swapping operations of all nesting levels into the LOCC operations, we then apply Theorem 3 or Theorem 4 to bound the achievable key rate between Alice and Bob by $\min\{E_{\max,E}(\mathcal{N}^{\mathrm{repeater\ chain}}), E^{\infty}_{E}(\mathcal{N}^{\mathrm{repeater\ chain}})\}$. If involved channels are tele-covariant, then we obtain bounds in terms of the relative entropy of entanglement.

APPENDIX F: LIMITATIONS ON SOME MDI-QKD PROTOTYPES

Following the discussion in Sec. VI D, let us now consider MDI-QKD settings with the noise model for transmission of qubit systems from both $\mathbf{A}_{a_1}$ and $\mathbf{A}_{a_2}$ to Charlie through qubit channels given by either the depolarizing channel $\mathcal{D}^l_{A_i\to C_i}$ or the dephasing channel $\mathcal{D}^s_{A_i\to C_i}$:

$$\mathcal{D}^l_{A_i\to C_i}(\rho_{A_i}) = \lambda_l \rho_{C_i} + \frac{1-\lambda_l}{2}\mathbb{1}_{C_i}, \tag{F1}$$

$$\mathcal{D}^s_{A_i\to C_i}(\rho_{A_i}) = \lambda_s \rho_{C_i} + (1-\lambda_s)\hat{Z}\rho_{C_i}\hat{Z}^\dagger, \tag{F2}$$

where

$$-\frac{1}{3} \le \lambda_l \le 1, \qquad 0 \le \lambda_s \le 1, \tag{F3}$$

$\hat{Z}$ is a Pauli-Z operator, and ρ is an arbitrary input state. Like the MDI-QKD setup with erasure channels discussed earlier, we assume that Charlie can perform a perfect Bell measurement $\mathcal{M}_{\vec{C}\to X}$ with probability q and failure probability $1-q$. We notice that the multiplex channels $\mathcal{N}^{\mathrm{MDI},\mathcal{D}^l}_{\vec{A}\to\vec{Z}}, \mathcal{N}^{\mathrm{MDI},\mathcal{D}^s}_{\vec{A}\to\vec{Z}}$ for these MDI-QKD prototypes are also tele-covariant, which implies that the MDI-QKD capacities for respective MDI-QKD settings, i.e., with depolarizing channels and dephasing channels, are upper bounded as (see following subsections for proofs and plots (Figs. 7 and 8) for some values of q:

(1) MDI-QKD with depolarizing channels $\mathcal{D}^l$ [Eq. (F2)], where $-\frac{1}{3} \le \lambda_l \le 1$,

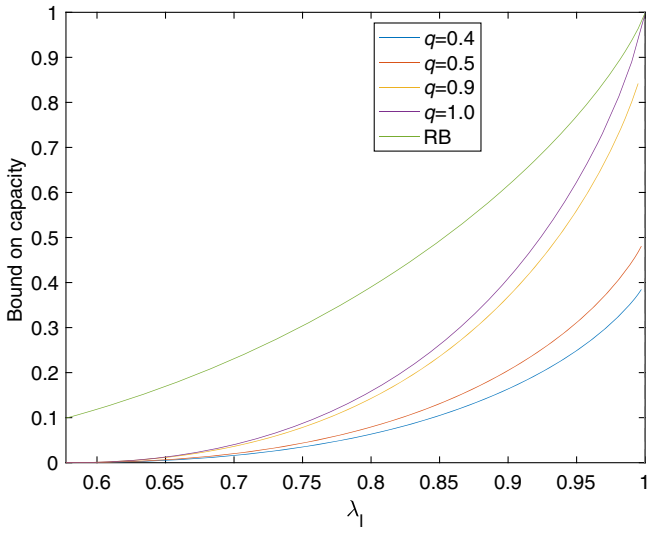

FIG. 7. Upper bounds [Eq. (F4)] on the secret key capacities for the MDI-QKD protocol with depolarizing channels for different values of parameters q and λ_l, in comparison to the RB bound [48].

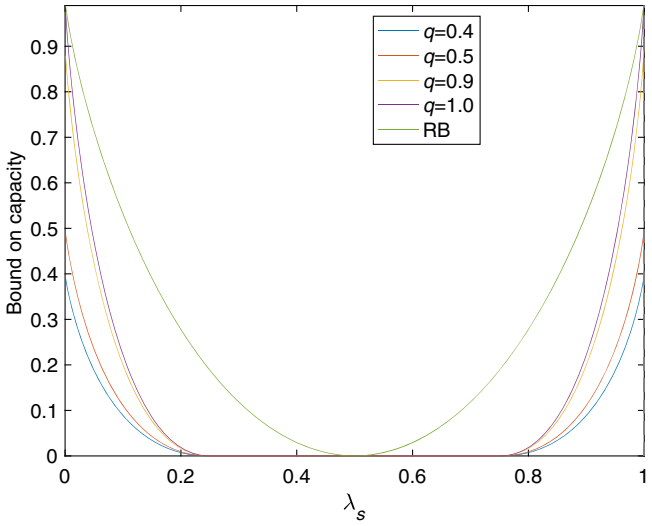

FIG. 8. Upper bounds [Eq. (F5)] on the secret key capacities for the MDI-QKD protocol with dephasing channels for different values of parameters q and λ_s, in comparison to the RB bound [48].

$$\tilde{P}_{\mathrm{LOCC}}(\mathcal{N}^{\mathrm{MDI},\mathcal{D}^l}) \le q\left[1 - h_2\left(\frac{3}{4}\lambda_l^2 + \frac{1}{4}\right)\right] \tag{F4}$$

for $\frac{1}{\sqrt{3}} < \lambda_l \le 1$, and 0 otherwise.

(2) MDI-QKD with dephasing channels $\mathcal{D}^s$ [Eq. (F1)], where $0 \le \lambda_s \le 1$,

$$\tilde{P}_{\mathrm{LOCC}}(\mathcal{N}^{\mathrm{MDI},\mathcal{D}^s}) \le \begin{cases} q(1 - h_2(\frac{1}{2}p_-(\lambda_s)) & \text{for } \lambda_s > \frac{3}{4} \\ 0 & \text{for } \frac{1}{4} \le \lambda_s \le \frac{3}{4} \\ q(1 - h_2(\frac{1}{2}p_-(1-\lambda_s)) & \text{for } \lambda_s < \frac{1}{4}, \end{cases} \tag{F5}$$

where $p_-(x) := 4x^2 - 3x + 1$.

1. MDI-QKD via depolarizing channels

In this section, we show a bound on MDI-QKD (or, equivalently, on a particular type of quantum repeater). In the latter setup, there are three stations: A, B, and an intermediate one $C \equiv C_A C_B$. We consider the links AC_A and $C_B B$ to be depolarizing channels $\mathcal{D}^s$, both with the same parameter λ_l [see Eq. (F2)]. We also consider that the Bell measurement, followed by communication of the results to both the parties, happens only with probability q. With probability $(1-q)$, the state of C is just traced out. We call the multiplex channel for a given MDI-QKD setup composed of depolarizing channels $\mathcal{D}^l$ with Bell measurement, which happens with probability q in total, a q-depolarizing-MDIQKD channel.

The upper bound that we derive below quantitatively demonstrates that the operation of distillation of entanglement along the links does not commute with the operation of entanglement swapping. Indeed, even for $q = 1$, if one does the Bell measurement first, the output key is zero for $\lambda_l \leq (1/\sqrt{3})$.

We are interested in the Choi-Jamiolkowski state of the q-depolarizing-MDIQKD channel, which we obtain from the Choi states (up to local unitary as the input state is Ψ^-) of the two depolarizing channels. The latter two states read $\lambda_l \Psi^- + (1-\lambda_l)\frac{\mathbb{1}}{4}$. The Choi state ρ_{AB}^{out} reads

$$\begin{aligned}\rho_{AB}^{\text{out}} \coloneqq \frac{\lambda_l^2 q}{4}[&\Psi_{AB}^- \otimes |00\rangle\langle 00|_{I_A I_B} + \Psi_{AB}^+ \otimes |11\rangle\langle 11|_{I_A I_B} \\ &+ \Phi_{AB}^- \otimes |22\rangle\langle 22|_{I_A I_B} + \Phi_{AB}^+ \otimes |33\rangle\langle 33|_{I_A I_B}] \\ &\otimes |00\rangle\langle 00|_{I'_A I'_B} \\ &+ (1-\lambda_l^2) q \frac{\mathbb{1}_{AB}}{4} \otimes \frac{1}{4}\sum_{i=0}^{3} |ii\rangle\langle ii|_{I_A I_B} \otimes |00\rangle\langle 00|_{I'_A I'_B} \\ &+ (1-q)\frac{\mathbb{1}_{AB}}{4} \otimes |\perp\rangle\langle\perp|_{I_A I_B} \otimes |11\rangle\langle 11|_{I'_A I'_B}. \end{aligned} \tag{F6}$$

Let us examine this case. First, with probability $(1-q)$, the parties are left with the initial state on AB, which is $\frac{\mathbb{1}}{4}$, and the "flag" $|11\rangle\langle 11|_{I'_A I'_B}$ reporting error in the Bell measurement. With probability q, they obtain a flag $|00\rangle\langle 00|_{I'_A I'_B}$, which informs us that the Bell measurement was successful. They also receive the classical result of the Bell measurement: $\{|ii\rangle\langle ii|_{I_A I_B}\}_{i=0}^3$. Only with probability λ_l^2 does this measurement result in the output of the appropriate Bell state on AB. With probability $(1-\lambda_l^2) = (1-\lambda_l)\lambda_l + \lambda_l(1-\lambda_l) + (1-\lambda_l)^2$, we have one of three possibilities with respective probabilities: (i) teleportation of $\mathbb{1}_{C_B}/2$ from C_A to A with probability $\lambda_l(1-\lambda_l)$, (ii) teleportation of $\mathbb{1}_{C_A}/2$ from C_B to B with probability $(1-\lambda_l)\lambda_l$, and (iii) a Bell measurement on systems $C_A C_B$ of the state $(\mathbb{1}_{AC_A}/4) \otimes (\mathbb{1}_{C_B B}/4)$ followed by communication of the outcomes [with probability $(1-\lambda_l)^2$]. As one can check by inspection, all three operations result in the state $\frac{\mathbb{1}}{4}$ on system AB.

The relative entropy of ρ_{AB}^{out} reads

$$E_R(\rho_{AB}^{\text{out}}) \leq q E_R(\rho_{AB|00}^{\text{out}}) + (1-q) E_R(\rho_{AB|11}^{\text{out}}) \tag{F7}$$

$$= q E_R(\rho_{AB|00}^{\text{out}}), \tag{F8}$$

where $\rho_{AB|11}^{\text{out}} = (\mathbb{1}_{AB}/4) \otimes |\perp\rangle\langle\perp|_{I_A I_B} \otimes |11\rangle\langle 11|_{I'_A I'_B}$ and $\rho_{AB|00}^{\text{out}}$ is such that $(1-q)\rho_{AB|11} + q\rho_{AB|00} = \rho_{AB}$. We have used the convexity of the relative entropy and the fact that it is zero for a maximally mixed state. We then observe that

$$E_R(\rho_{AB|00}^{\text{out}}) = E_R\left(\left(\sum_{i=0}^{3} \lambda_l^2 |\psi_i\rangle\langle\psi_i|_{AB} + (1-\lambda_l^2)\frac{\mathbb{1}_{AB}}{4}\right) \otimes |ii\rangle\langle ii|_{I_A I_B} \otimes |00\rangle\langle 00|_{I'_A I'_B}\right), \tag{F9}$$

where $|\psi_i\rangle\langle\psi_i|$ are the Bell states. Next, we use the fact that for each i, the state $\lambda_l^2|\psi_i\rangle\langle\psi_i|_{AB} + (1-\lambda_l^2)\frac{\mathbb{1}}{4}$ is a Bell diagonal state. A Bell diagonal state of the form $\sum_j p_j |\psi_j\rangle\langle\psi_j|$ has E_R equal to $1 - h(p_{\max})$, where $p_{\max} = \max_j p_j$ is the maximal of the weights of the Bell state $|\psi_j\rangle\langle\psi_j|$ in the mixture, or 0 if $p_{\max} \leq \frac{1}{2}$. In our case, $p_{\max} = \lambda_l^2 + (1-\lambda_l^2)/4$. Thus, via convexity and Eq. (F8), we obtain that

$$E_R(\rho_{AB}^{\text{out}}) \leq q\left[1 - h_2\left(\lambda_l^2 + \frac{(1-\lambda_l^2)}{4}\right)\right] \tag{F10}$$

for $\lambda_l^2 + (1-\lambda_l^2)/4 > 1/2$, and 0 otherwise. The condition $\lambda_l^2 + (1-\lambda_l^2)/4 > 1/2$ on λ_l is equivalent to $\lambda_l > (1/\sqrt{3})$. This implies that for $q = 1$, the bound is zero for $\lambda_l \in (\frac{1}{3}, (1/\sqrt{3})]$, for which the depolarizing channel is nonzero, and hence, its private capacity is nonzero as well. We interpret this as the noncommutativity of the independent and identically distributed (i.i.d.) Bell measurement and entanglement distillation. Indeed, for this range of λ_l, given access to an isotropic state $\rho(\lambda_l)$, one can distill $E_D(\rho(\lambda_l)) = (1 - h_2(\lambda_l))$ of entanglement, and hence, the quantum capacity $\mathcal{Q}(\mathcal{D}^l) = 1 - h_2(\lambda_l)$ (or zero for $\lambda_l \leq 1/3$). On the other hand, this amount of key becomes inaccessible when the Bell measurement is done first.

2. MDI-QKD via dephasing channels

In this section, we consider two dephasing channels [Eq. (F1)] between Alice and Charlie and Bob and Charlie. We again observe that the operation of distillation and i.i.d. entanglement swapping via the Bell measurement do not commute. Altering them leads to different amounts of key in the output. We use the fact that MDI-QKD via the dephasing channel is teleportation covariant.

Note that the Choi-Jamiolkowski state (up to local unitary operations as the input state is Ψ^-) of the dephasing channel equals $\lambda_s \Psi^- + (1-\lambda_s)\Psi^+ = (2\lambda_s - 1)\Psi^- + (2 - 2\lambda_s)\rho_{cl}$, with $\rho_{cl} = \frac{1}{2}(|01\rangle\langle 01| + |10\rangle\langle 10|)$. Hence, the Choi-Jamiolkowski state of the dephasing-MDIQKD channel reads

$$\rho_{AB}^{\text{out}} := (2\lambda_s-1)^2 q\Psi_{AB}^{-}\otimes\sum_{i=0}^{3}|ii\rangle\langle ii|_{I_AI_B}\otimes|00\rangle\langle 00|_{I'_AI'_B} + (2-2\lambda_s)(2\lambda_s-1)q\rho_{cl}^{AB} \otimes\frac{1}{4}\sum_{i=0}^{3}|ii\rangle\langle ii|_{I_AI_B}\otimes|00\rangle\langle 00|_{I'_AI'_B} + (2-2\lambda_s)q\frac{\mathbb{1}_{AB}}{4}\otimes\frac{1}{4}\sum_{i=0}^{3}|ii\rangle\langle ii|_{I_AI_B}\otimes|00\rangle\langle 00|_{I'_AI'_B} + (1-q)\frac{\mathbb{1}_{AB}}{4}\otimes|\perp\rangle\langle\perp|_{I_AI_B}\otimes|11\rangle\langle 11|_{I'_AI'_B}, \quad \text{(F11)}$$

given that Alice has performed the control-Pauli operations on her systems AI_A. We can safely assume that this decoding has been done because the local unitary operation does not change the relative entropy of entanglement. The first case is a straightforward result of correct entanglement swapping. Regarding the next term, with probability $(2-2\lambda_s)\times(2\lambda_s-1)$, a subsystem C_A of the state ρ_{cl} gets correctly teleported to A, and hence, finally, ρ_{cl}^{AB} is shared by Alice and Bob. However, with probability $(2-2\lambda_s)=(2-2\lambda_s)^2+(2-2\lambda_s)(2\lambda_s-1)$, the resulting state is maximally mixed because, with probability $(2-2\lambda_s)^2$, the state on system C is traced out; hence, a product of subsystems of ρ_{cl}^{AB} is an output. On the other hand, with probability $(2-2\lambda_s)\times(2\lambda_s-1)$, subsystem C_B of the state ρ_{cl} is teleported to Bob; however, Bob does not do the decoding. It is then straightforward to check that $\frac{1}{4}\sum_{i=0}^{1}\sigma_i^B\otimes\mathbb{1}_A\rho_{cl}^{AB}\hat{\sigma}_i^B\otimes\mathbb{1}_A$, with $\hat{\sigma}_i$ being Pauli operators, is the maximally mixed state of two qubits.

The relative entropy of ρ_{AB}^{out} reads

$$E_R(\rho_{AB}^{\text{out}}) \le qE_R(\rho_{AB|00}^{\text{out}})+(1-q)E_R(\rho_{AB|11}^{\text{out}}) \quad \text{(F12)}$$

$$= qE_R(\rho_{AB|00}^{\text{out}}), \quad \text{(F13)}$$

where $\rho_{AB|11}^{\text{out}}=(\mathbb{1}_{AB}/4)\otimes|\perp\rangle\langle\perp|_{I_AI_B}\otimes|11\rangle\langle 11|_{I'_AI'_B}$ and $\rho_{AB|00}^{\text{out}}$ is such that $(1-q)\rho_{AB|11}+q\rho_{AB|00}=\rho_{AB}$. We have again used the convexity of the relative entropy and the fact that it is zero for a maximally mixed state. We then observe that

$$E_R(\rho_{AB|00}^{\text{out}})=E_R\left((2\lambda_s-1)^2|\Psi^-\rangle\langle\Psi^-|_{AB}+(2-2\lambda_s)(2\lambda_s-1)\rho_{cl}^{AB}+(2-2\lambda_s)\frac{\mathbb{1}_{AB}}{4}\right), \quad \text{(F14)}$$

where we have neglected systems I_AI_B and $I'_AI'_B$ due to subadditivity of E_R and the fact that it is zero for both the states $\sum_{i=0}^{3}|ii\rangle\langle ii|_{I_AI_B}$ and $|00\rangle\langle 00|_{I'_AI'_B}$. The resulting state is Bell diagonal [note that $\rho_{cl}^{AB}=\frac{1}{2}(|\Psi^-\rangle\langle\Psi^-|+|\Psi^+\rangle\langle\Psi^+|)$]; it is thus sufficient to find the largest weight of a Bell state to compute its relative entropy. Bell diagonal states are separable if the largest weight is less than or equal to half, i.e., when none of the Bell states $(\Phi^+,\Phi^-,\Psi^+,\Psi^-)$ has weight greater than $1/2$.

For the case $\lambda_s\ge\frac{1}{2}$, the state $|\Psi^-\rangle\langle\Psi^-|$ is in the mixed state $\rho_{AB|00}^{\text{out}}$ with probability $(2\lambda_s-1)^2+(2-2\lambda_s)(2\lambda_s-1)+(2-2\lambda_s)/4=\frac{1}{2}(4\lambda_s^2-3\lambda_s+1)$.

Thus, keeping the structure of the Choi state of the dephasing channel in mind, we arrive at the following bound:

$$E_R(\rho_{AB}^{\text{out}})\le\begin{cases} q(1-h_2(\frac{1}{2}p_-(\lambda_s))) & \text{for } \lambda_s>\frac{3}{4}\\ 0 & \text{for } \frac{1}{4}\le\lambda_s\le\frac{3}{4}\\ q(1-h_2(\frac{1}{2}p_-(1-\lambda_s))) & \text{for } \lambda_s<\frac{1}{4},\end{cases} \quad \text{(F15)}$$

where $p_-(x):=4x^2-3x+1$.

APPENDIX G: COMPLEXITY OF FINDING LOWER BOUNDS OF THE SKA RATE FOR THE BIDIRECTIONAL NETWORK

Here, we briefly comment on the complexity of finding a subgraph, which allows us to realize the conference key agreement with the capacity indicated by the inequality (75). As we show, the complexity is a polynomial of low degree $O(n^2)$. In what follows, a minimum spanning tree is a tree with a minimal sum of the weights of its edges. A minimum bottleneck spanning tree is the one in which the edge with the highest weight has the lowest possible value for the considered graph.

The algorithm of finding the maximal of the minimal edges over all spanning trees of the graph is as follows.

(1) Find the maximal weight of the edges of G (denoted as M).
(2) Find the minimum spanning tree T_{MST} in the graph $G'=(V_G,E_G)$, which is the same as G but with the weights of the edges changed from $w(e)$ to $M-w(e)$, where $M\equiv\max_{e'\in E_G}w(e')$.
(3) Find the minimal weight of the edges in T, denoted $w_{\min}$. Return $M-w_{\min}$.

The correctness of this algorithm follows from the fact that every minimum spanning tree is a minimal bottleneck spanning tree. Finding the highest weight of the edges of this tree that is as low as possible is the opposite task from

ours. Indeed, we aim at finding trees with the lowest weight over its edges to be as high as possible, which is why we search for the minimal spanning tree in the graph with converted edges to $M \equiv \max_{e' \in E_G} w(e') - w(e)$. Next, we use the fact that $\min_{T \subseteq G} \max_{e \in E_T} [M - w(e)] = M - \max_{T \subseteq G} \min_{e \in E_T} w(e)$, so $M - w_{\min}$ is the solution. The overall time complexity of this algorithm is $O(m + n \log n)$. Indeed, the first step takes $O(m)$ time. The next two take $O(m + n \log n)$, where finding the minimum spanning tree is via Prim's algorithm based on the data structure called the Fibonacci heap [117]. The final step takes $O(n \log n)$, which is the time for sorting the weights of edges (e.g., by the QuickSort algorithm). Taking into account that m scales pessimistically as n^2, we obtain $O(n^2)$ as the worst-case complexity.

To summarize, the value of the lower bound can be found efficiently on a classical computer, given that all the capacities describing the bidirectional network are known and represented in the form of a graph.

APPENDIX H: KEY DISTILLATION FROM STATES—PLOTS

To calculate our upper bounds, we utilize the technique of semidefinite programming (SDP) with MATLAB (version) library "SDPT3 4.0" [154], see Ref. [134]. We calculate upper bounds for several cases, incorporating both Φ_M^{GHZ} states and Φ_M^{W} states. First, we vary the number of copies of the state that enter the protocol; second, we make calculations for multipartite states with the number of parties exceeding three. Finally, we extend our consideration to states subjected to dephasing or depolarizing noises characterized in Eq. (H1) (each qubit is subjected to noise separately). We investigate the effect of noise in the case of a different number of copies and different number of parties:

$$\rho_{\mathrm{noisy}} = \mathcal{D}^{\otimes M}(\rho), \tag{H1}$$

for $\mathcal{D}$ given by

$$\mathcal{D}^q_{\mathrm{deph}}(\omega) = q\omega + (1-q)\sigma_z \omega \sigma_z, \tag{H2}$$

$$\mathcal{D}^q_{\mathrm{depol}}(\omega) = q\omega + (1-q)\frac{\mathbb{1}}{2}, \tag{H3}$$

where σ_z is the Pauli Z matrix and q is the noise parameter.

We present the plots for the upper bound on the key rate distilled from both Φ_M^{GHZ} and Φ_M^{W} states and tensor powers of them. The plots are a function of the ε parameter controlling the fidelity of the target state $\rho_{\vec{A}}$ with respect to a private state.

We compare the performance of our upper bound and choice of biseparable states for a tripartite single copy state in Figs. 9 and 10. In the control plot in Fig. 9, for the noiseless Φ_M^{GHZ} state, the upper bound, as expected, exhibits the value to be just above 1 for the chosen range of ε, which indicates that the ε-hypothesis-testing upper bound is not too loose. For the single copy tripartite Φ_M^{W} state, the value of the upper bound in Fig. 10 for $\varepsilon \approx 0$ is below 0.6, which is below the value of the rate of the optimal LOCC asymptotic protocol, approximately 0.643 per copy [80]. In the case of two copies of bipartite Φ_M^{W} in Fig. 11, we obtain an upper bound that for $\varepsilon \approx 0$ has a value of around 1.18, which is significantly above the $\frac{2}{3}$ achieved by the protocol described earlier in this Appendix, and 1.286, which is an asymptotic limit for the state being two copies of the Φ_M^{W} state (Theorem 2 in Ref. [80]). Both of these results are in agreement with the fact that single-copy and two-copy one-shot protocols constitute a very

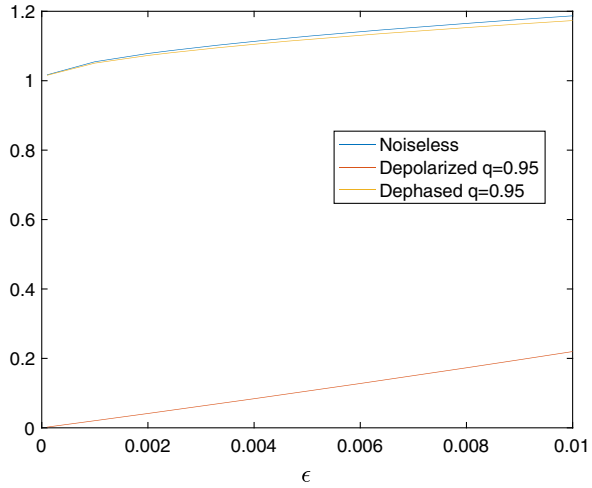

FIG. 9. Plot of ε-hypothesis-testing upper bound on conference key rate for a single copy of the Φ_3^{GHZ} state, for noiseless, dephased, and depolarized cases.

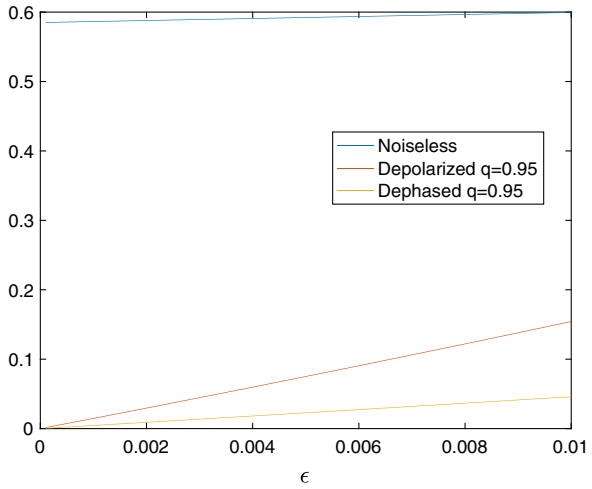

FIG. 10. Plot of ε-hypothesis-testing upper bound on the conference key rate for a single copy of the Φ_3^{W} state, for noiseless, dephased, and depolarized cases.

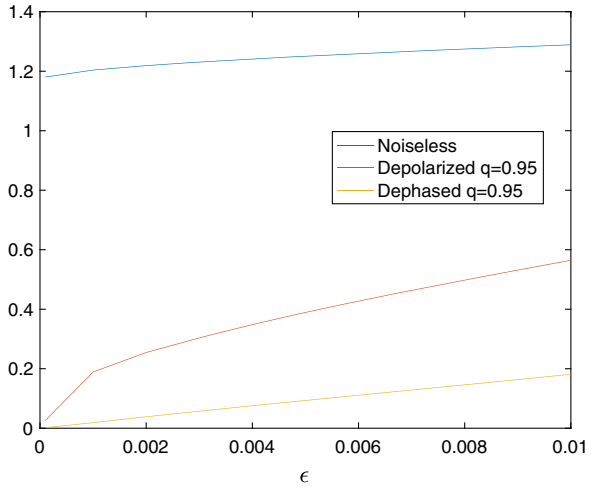

FIG. 11. Plot of ε-hypothesis-testing upper bound on the conference key rate for two copies of the Φ_3^{W} state, for noiseless, dephased, and depolarized cases.

limited class of protocols compared to those available for calculating the asymptotic limit. For two copies of the Φ_M^{W} state, the large gap between our upper bound for the conference key rate and the rate of the Φ_M^{GHZ} state distillation protocol makes us think that, indeed, the former is larger than the latter. However, a formal proof is still missing. Moreover, we notice that the optimal protocol Φ_M^{W} to Φ_M^{GHZ} conversion has to incorporate at least three copies of the Φ_M^{W} state because our ε-hypothesis-testing upper bound is smaller than the asymptotic limit for Φ_M^{GHZ} distillation.

[1] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, in *International Conference on Computer System and Signal Processing, 1984* (IEEE, New York, 1984), Vol. 175, p. 8.

[2] A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. **67**, 661 (1991).

[3] J. P. Dowling and G. J. Milburn, *Quantum Technology: The Second Quantum Revolution*, Phil. Trans. R. Soc. A **361**, 1655 (2003).

[4] R. Renner, Ph.D. thesis, ETH Zürich (2005), https://arxiv.org/abs/quant-ph/0512258.

[5] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, *Field Test of a Practical Secure Communication Network with Decoy-State Quantum Cryptography*, Opt. Express **17**, 6540 (2009).

[6] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, *Experimental Satellite Quantum Communications*, Phys. Rev. Lett. **115**, 040502 (2015).

[7] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, *Large Scale Quantum Key Distribution: Challenges and Solutions*, Opt. Express **26**, 24260 (2018).

[8] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, *Loophole-Free Bell Inequality Violation Using Electron Spins Separated by 1.3 Kilometres*, Nature (London) **526**, 682 (2015).

[9] S. J. Pauka, K. Das, R. Kalra, A. Moini, Y. Yang, M. Trainer, A. Bousquet, C. Cantaloube, N. Dick, G. C. Gardner, M. J. Manfra, and D. J. Reilly, *A Cryogenic Interface for Controlling Many Qubits*, arXiv:1912.01299.

[10] C. E. Bradley, J. Randall, M. H. Abobeih, R. C. Berrevoets, M. J. Degen, M. A. Bakker, M. Markham, D. J. Twitchen, and T. H. Taminiau, *A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute*, Phys. Rev. X **9**, 031045 (2019).

[11] Y.-A. Chen *et al.*, *An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres*, Nature (London) **589**, 214 (2021).

[12] P. W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, California, 1994), pp. 124–134.

[13] K. Chen and H.-K. Lo, *Conference Key Agreement and Quantum Sharing of Classical Secrets with Noisy GHZ States*, in *Proceedings of the International Symposium on Information Theory, 2005* (IEEE, New York, 2005), pp. 1607–1611.

[14] R. Augusiak and P. Horodecki, *Multipartite Secret Key Distillation and Bound Entanglement*, Phys. Rev. A **80**, 042307 (2009).

[15] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Going Beyond Bell's Theorem*, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos, Fundamental Theories of Physics Vol. 37 (Springer, Dordrecht, 1989), https://doi.org/10.1007/978-94-017-0849-4_10.

[16] H. J. Kimble, *The Quantum Internet*, Nature (London) **453**, 1023 (2008).

[17] S. Wehner, D. Elkouss, and R. Hanson, *Quantum Internet: A Vision for the Road Ahead*, Science **362**, eaam9288 (2018).

[18] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, *Quantum Teleportation over 143 Kilometres Using Active Feed-Forward*, Nature (London) **489**, 269 (2012).

[19] S.-K. Liao *et al.*, *Satellite-to-Ground Quantum Key Distribution*, Nature (London) **549**, 43 (2017).

[20] K. Azuma, K. Tamaki, and H.-K. Lo, *All-Photonic Quantum Repeaters*, Nat. Commun. **6**, 6787 (2015).

[21] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, Phys. Rev. Lett. **81**, 5932 (1998).

[22] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, *Quantum Repeaters Based on Entanglement Purification*, Phys. Rev. A **59**, 169 (1999).

[23] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside Quantum Repeaters*, IEEE J. Sel. Top. Quantum Electron. **21**, 78 (2015).
[24] V. Makarov, A. Anisimov, and J. Skaar, *Effects of Detector Efficiency Mismatch on Security of Quantum Cryptosystems*, Phys. Rev. A **74**, 022313 (2006).
[25] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, *Time-Shift Attack in Practical Quantum Cryptosystems*, Quantum Inf. Comput. **7**, 073 (2007).
[26] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, *Practical Challenges in Quantum Key Distribution*, npj Quantum Inf. **2**, 16025 (2016).
[27] H.-K. Lo, M. Curty, and B. Qi, *Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **108**, 130503 (2012).
[28] S. L. Braunstein and S. Pirandola, *Side-Channel-Free Quantum Key Distribution*, Phys. Rev. Lett. **108**, 130502 (2012).
[29] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, *High-Rate Measurement-Device-Independent Quantum Cryptography*, Nat. Photonics **9**, 397 (2015).
[30] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, *Long-Distance Measurement-Device-Independent Multiparty Quantum Communication*, Phys. Rev. Lett. **114**, 090501 (2015).
[31] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters*, Nature (London) **557**, 400 (2018).
[32] X. Ma, P. Zeng, and H. Zhou, *Phase-Matching Quantum Key Distribution*, Phys. Rev. X **8**, 031043 (2018).
[33] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, *Information Theoretic Security of Quantum Key Distribution Overcoming the Repeaterless Secret Key Capacity Bound*, arXiv:1805.05511.
[34] J. Lin and N. Lütkenhaus, *Simple Security Analysis of Phase-Matching Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. A **98**, 042332 (2018).
[35] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, *Twin-Field Quantum Key Distribution without Phase Postselection*, Phys. Rev. Applied **11**, 034053 (2019).
[36] M. Curty, K. Azuma, and H.-K. Lo, *Simple Security Proof of Twin-Field Type Quantum Key Distribution Protocol*, npj Quantum Inf. **5**, 1 (2019).
[37] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H.-K. Lo, T.-Y. Chen, F. Xu, and J.-W. Pan, *Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum Key Distribution over Asymmetric Channels*, Phys. Rev. Lett. **122**, 160501 (2019).
[38] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, *Experimental Quantum Key Distribution Beyond the Repeaterless Secret Key Capacity*, Nat. Photonics **13**, 334 (2019).
[39] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, *Versatile Security Analysis of Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. A **99**, 062332 (2019).
[40] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, *Secure Key from Bound Entanglement*, Phys. Rev. Lett. **94**, 160502 (2005).
[41] M. Christandl and A. Winter, *Squashed Entanglement: An Additive Entanglement Measure*, J. Math. Phys. (N.Y.) **45**, 829 (2004).
[42] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-State Entanglement and Quantum Error Correction*, Phys. Rev. A **54**, 3824 (1996).
[43] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, *Quantifying Entanglement*, Phys. Rev. Lett. **78**, 2275 (1997).
[44] V. Vedral and M. B. Plenio, *Entanglement Measures and Purification Procedures*, Phys. Rev. A **57**, 1619 (1998).
[45] M. Horodecki, P. Horodecki, and R. Horodecki, *General Teleportation Channel, Singlet Fraction, and Quasidistillation*, Phys. Rev. A **60**, 1888 (1999).
[46] N. Datta, *Max-Relative Entropy of Entanglement, Alias Log Robustness*, Int. J. Quantum. Inform. **07**, 475 (2009).
[47] M. Takeoka, S. Guha, and M. Wilde, *Fundamental Rate-Loss Tradeoff for Optical Quantum Key Distribution*, Nat. Commun. **5**, 5235 (2014).
[48] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental Limits of Repeaterless Quantum Communications*, Nat. Commun. **8**, 15043 (2017); see also, arXiv:1512.04945.
[49] M. M. Wilde, M. Tomamichel, and M. Berta, *Converse Bounds for Private Communication over Quantum Channels*, IEEE Trans. Inf. Theory **63**, 1792 (2017).
[50] M. Christandl and A. Müller-Hermes, *Relative Entropy Bounds on Quantum, Private and Repeater Capacities*, Commun. Math. Phys. **353**, 821 (2017).
[51] S. Das, S. Bäuml, and M. M. Wilde, *Entanglement and Secret-Key-Agreement Capacities of Bipartite Quantum Interactions and Read-Only Memory Devices*, Phys. Rev. A **101**, 012344 (2020).
[52] S. Bäuml, S. Das, and M. M. Wilde, *Fundamental Limits on the Capacities of Bipartite Quantum Interactions*, Phys. Rev. Lett. **121**, 250504 (2018).
[53] S. Das, Ph.D. thesis, Louisiana State University (2018), https://arxiv.org/abs/1901.05895.
[54] R. Laurenza and S. Pirandola, *General Bounds for Sender-Receiver Capacities in Multipoint Quantum Communications*, Phys. Rev. A **96**, 032318 (2017).
[55] K. P. Seshadreesan, M. Takeoka, and M. M. Wilde, *Bounds on Entanglement Distillation and Secret Key Agreement for Quantum Broadcast Channels*, IEEE Trans. Inf. Theory **62**, 2849 (2016).
[56] M. Takeoka, K. P. Seshadreesan, and M. M. Wilde, *Unconstrained Capacities of Quantum Key Distribution and Entanglement Distillation for Pure-Loss Bosonic Broadcast Channels*, Phys. Rev. Lett. **119**, 150501 (2017).
[57] S. Bäuml, M. Christandl, K. Horodecki, and A. Winter, *Limitations on Quantum Key Repeaters*, Nat. Commun. **6**, 6908 (2015).

[58] K. Azuma, A. Mizutani, and H.-K. Lo, *Fundamental Rate-Loss Tradeoff for the Quantum Internet*, Nat. Commun. **7**, 13523 (2016).

[59] L. Rigovacca, G. Kato, S. Bäuml, M. Kim, W. J. Munro, and K. Azuma, *Versatile Relative Entropy Bounds for Quantum Networks*, New J. Phys. **20**, 013033 (2018).

[60] S. Pirandola, *End-to-End Capacities of a Quantum Communication Network*, Commun. Phys. **2**, 51 (2019)

[61] S. Bäuml and K. Azuma, *Fundamental Limitation on Quantum Broadcast Networks*, Quantum Sci. Technol. **2**, 024004 (2017).

[62] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, *General Paradigm for Distilling Classical Key from Quantum States*, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[63] M. M. Wilde, A. Winter, and D. Yang, *Strong Converse for the Classical Capacity of Entanglement-Breaking and Hadamard Channels via a Sandwiched Rényi Relative Entropy*, Commun. Math. Phys. **331**, 593 (2014).

[64] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, *On Quantum Rényi Entropies: A New Definition and Some Properties*, J. Math. Phys. (N.Y.) **54**, 122203 (2013).

[65] F. Buscemi and N. Datta, *The Quantum Capacity of Channels with Arbitrarily Correlated Noise*, IEEE Trans. Inf. Theory **56**, 1447 (2010),

[66] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, *Concentrating Partial Entanglement by Local Operations*, Phys. Rev. A **53**, 2046 (1996).

[67] S. Das, S. Khatri, and J. P. Dowling, *Robust Quantum Network Architectures and Topologies for Entanglement Distribution*, Phys. Rev. A **97**, 012335 (2018).

[68] I. Devetak and A. Winter, *Distillation of Secret Key and Entanglement from Quantum States*, Proc. R. Soc. A **461**, 207 (2005).

[69] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, *Direct and Reverse Secret-Key Capacities of a Quantum Channel*, Phys. Rev. Lett. **102**, 050503 (2009).

[70] M. Christandl and A. Winter, *Squashed Entanglement: An Additive Entanglement Measure*, J. Math. Phys. (N.Y.) **45**, 829 (2004).

[71] R. R. Tucci, *Quantum Entanglement and Conditional Information Transmission*, arXiv:quant-ph/9909041.

[72] R. R. Tucci, *Entanglement of Distillation and Conditional Mutual Information*, arXiv:quant-ph/0202144.

[73] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, *Squashed Entanglement for Multipartite States and Entanglement Measures Based on the Mixed Convex Roof*, IEEE Trans. Inf. Theory **55**, 3375 (2009).

[74] K. Fang and H. Fawzi, *Geometric Rényi Divergence and Its Applications in Quantum Channel Capacities*, arXiv: 1909.05758.

[75] K. Azuma and G. Kato, *Aggregating Quantum Repeaters for the Quantum Internet*, Phys. Rev. A **96**, 032332 (2017).

[76] S. Bäuml, K. Azuma, G. Kato, and D. Elkouss, *Linear Programs for Entanglement and Key Distribution in the Quantum Internet*, Commun. Phys. **3**, 55 (2020).

[77] M. Christandl and R. Ferrara, *Private States, Quantum Data Hiding, and the Swapping of Perfect Secrecy*, Phys. Rev. Lett. **119**, 220506 (2017).

[78] P. van Loock, W. Alt, C. Becher, O. Benson, H. Boche, C. Deppe, J. Eschner, S. Höfling, D. Meschede, P. Michler *et al.*, *Extending Quantum Links: Modules for Fiber-and Memory-Based Quantum Repeaters*, Adv. Quantum Technol. **3**, 1900141 (2020).

[79] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, *Exact and Asymptotic Measures of Multipartite Pure-State Entanglement*, Phys. Rev. A **63**, 012307 (2000).

[80] J. A. Smolin, F. Verstraete, and A. Winter, *Entanglement of Assistance and Multipartite State Distillation*, Phys. Rev. A **72**, 052317 (2005).

[81] B. Fortescue and H.-K. Lo, *Random Bipartite Entanglement from W and W-Like States*, Phys. Rev. Lett. **98**, 260501 (2007).

[82] S. Kıntaş and S. Turgut, *Transformations of W-Type Entangled States*, J. Math. Phys. (N.Y.) **51**, 092202 (2010).

[83] W. Cui, E. Chitambar, and H. K. Lo, *Randomly Distilling W-Class States into General Configurations of Two-Party Entanglement*, Phys. Rev. A **84**, 052301 (2011).

[84] P. Vrana and M. Christandl, *Asymptotic Entanglement Transformation between W and GHZ States*, J. Math. Phys. (N.Y.) **56**, 022204 (2015).

[85] C. Spee, J. I. de Vicente, D. Sauerwein, and B. Kraus, *Entangled Pure State Transformations via Local Operations Assisted by Finitely Many Rounds of Classical Communication*, Phys. Rev. Lett. **118**, 040503 (2017).

[86] P. Vrana and M. Christandl, *Distillation of Greenberger–Horne–Zeilinger States by Combinatorial Methods*, IEEE Trans. Inf. Theory **65**, 5945 (2019).

[87] A. Streltsov, C. Meignant, and J. Eisert, *Rates of Multipartite Entanglement Transformations*, Phys. Rev. Lett. **125**, 080502 (2020).

[88] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**, 777 (1935).

[89] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, *Everything You Always Wanted to Know about LOCC (but Were Afraid to Ask)*, Commun. Math. Phys. **328**, 303 (2014).

[90] Y. Polyanskiy and S. Verdú, *Arimoto Channel Coding Converse and Rényi Divergence*, in *Proceedings of the 48th Annual Allerton Conference on Communication, Control, and Computation* (2010), pp. 1327–1333, https://ieeexplore.ieee.org/document/5707067.

[91] N. Sharma and N. A. Warsi, *On the Strong Converses for the Quantum Channel Capacity Theorems*, Phys. Rev. Lett. **110**, 080501 (2013).

[92] H. Umegaki, *Conditional Expectations in an Operator Algebra, IV (Entropy and Information)*, Kodai Math. Sem. Rep. **14**, 59 (1962).

[93] N. Datta, *Min- and Max-Relative Entropies and a New Entanglement Monotone*, IEEE Trans. Inf. Theory **55**, 2816 (2009).

[94] L. Wang and R. Renner, *One-Shot Classical-Quantum Capacity and Hypothesis Testing*, Phys. Rev. Lett. **108**, 200501 (2012).

[95] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[96] R. Augusiak, D. Cavalcanti, G. Prettico, and A. Acín, *Perfect Quantum Privacy Implies Nonlocality*, Phys. Rev. Lett. **104**, 230401 (2010).

[97] S. Bäuml, S. Das, X. Wang, and M. M. Wilde, *Resource Theory of Entanglement for Bipartite Quantum Channels*, arXiv:1907.04181.

[98] G. Gour and C. M. Scandolo, *The Entanglement of a Bipartite Channel*, Phys. Rev. A **103**, 062422 (2021).

[99] N. Friis, G. Vitagliano, M. Malik, and M. Huber, *Entanglement Certification from Theory to Experiment*, Nat. Rev. Phys. **1**, 72 (2019).

[100] P. Contreras-Tejada, C. Palazuelos, and J. I. de Vicente, *Resource Theory of Entanglement with a Unique Multipartite Maximally Entangled State*, Phys. Rev. Lett. **122**, 120503 (2019).

[101] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin, *On the Capacities of Bipartite Hamiltonians and Unitary Gates*, IEEE Trans. Inf. Theory **49**, 1895 (2003).

[102] E. Kaur and M. M. Wilde, *Amortized Entanglement of a Quantum Channel and Approximately Teleportation-Simulable Channels*, J. Phys. A **51**, 035303 (2018).

[103] K. Fang, O. Fawzi, R. Renner, and D. Sutter, *A Chain Rule for the Quantum Relative Entropy*, Phys. Rev. Lett. **124**, 100501 (2020).

[104] M. Tomamichel and V. Y. F. Tan, *Second-Order Asymptotics for the Classical Capacity of Image-Additive Quantum Channels*, Commun. Math. Phys. **338**, 103 (2015).

[105] K. Goodenough, D. Elkouss, and S. Wehner, *Assessing the Performance of Quantum Repeaters for All Phase-Insensitive Gaussian Bosonic Channels*, New J. Phys. **18**, 063005 (2016).

[106] M. M. Wilde and H. Qi, *Energy-Constrained Private and Quantum Capacities of Quantum Channels*, IEEE Trans. Inf. Theory **64**, 7802 (2018).

[107] D. Gottesman and I. L. Chuang, *Demonstrating the Viability of Universal Quantum Computation Using Teleportation and Single-Qubit Operations*, Nature (London) **402**, 390 (1999).

[108] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, *Entangling Operations and Their Implementation Using a Small Amount of Entanglement*, Phys. Rev. Lett. **86**, 544 (2001).

[109] W. Dür, M. J. Bremner, and H. J. Briegel, *Quantum Simulation of Interacting High-Dimensional Systems: The Influence of Noise*, Phys. Rev. A **78**, 052325 (2008).

[110] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, *Continuous-Variable Measurement-Device-Independent Multipartite Quantum Communication*, Phys. Rev. A **93**, 022325 (2016).

[111] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, *Modular Network for High-Rate Quantum Conferencing*, Commun. Phys. **2**, 118 (2019).

[112] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, *Event-Ready-Detectors Bell Experiment via Entanglement Swapping*, Phys. Rev. Lett. **71**, 4287 (1993).

[113] T. C. Ralph and G. J. Pryde, *Optical Quantum Computation*, in *Progress in Optics* (Elsevier, New York, 2010), pp. 209–269.

[114] M. Grassl, T. Beth, and T. Pellizzari, *Codes for the Quantum Erasure Channel*, Phys. Rev. A **56**, 33 (1997).

[115] F.-Y. Lu, Z.-Q. Yin, R. Wang, G.-J. Fan-Yuan, S. Wang, D.-Y. He, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, *Practical Issues of Twin-Field Quantum Key Distribution*, New J. Phys. **21**, 123030 (2019).

[116] R. J. Wilson, *Introduction to Graph Theory* (Longman, England, 1996).

[117] C. E. Leiserson, R. L. Rivest, T. H. Cormen, and C. Stein, *Introduction to Algorithms* (MIT Press, Cambridge, MA, 2001), Vol. 6.

[118] W. Dür, G. Vidal, and J. I. Cirac, *Three Qubits Can Be Entangled in Two Inequivalent Ways*, Phys. Rev. A **62**, 062314 (2000).

[119] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum Entanglement*, Rev. Mod. Phys. **81**, 865 (2009).

[120] L. Amico, R. Fazio, A. Osterloh, and V. Vedral, *Entanglement in Many-Body Systems*, Rev. Mod. Phys. **80**, 517 (2008).

[121] D. Home, D. Saha, and S. Das, *Multipartite Bell-Type Inequality by Generalizing Wigner's Argument*, Phys. Rev. A **91**, 012102 (2015).

[122] B. Fortescue and H.-K. Lo, *Random-Party Entanglement Distillation in Multiparty States*, Phys. Rev. A **78**, 012348 (2008).

[123] W. Cui, W. Helwig, and H.-K. Lo, *Bounds on Probability of Transformations between Multipartite Pure States*, Phys. Rev. A **81**, 012111 (2010).

[124] A. Cabello, *Multiparty Key Distribution and Secret Sharing Based on Entanglement Swapping*, arXiv:quant-ph/0009025.

[125] V. Scarani and N. Gisin, *Quantum Key Distribution Between N Partners: Optimal Eavesdropping and Bell's Inequalities*, Phys. Rev. A **65**, 012311 (2001).

[126] R. Augusiak and P. Horodecki, *W-Like Bound Entangled States and Secure Key Distillation*, Europhys. Lett. **85**, 50001 (2009).

[127] F. Grasselli, H. Kampermann, and D. Bruß, *Conference Key Agreement with Single-Photon Interference*, New J. Phys. **21**, 123002 (2019).

[128] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, *Low-Dimensional Bound Entanglement with One-Way Distillable Cryptographic Key*, IEEE Trans. Inf. Theory **54**, 2621 (2008).

[129] Ł. Pankowski and M. Horodecki, *Low-Dimensional Quite Noisy Bound Entanglement with a Cryptographic Key*, J. Phys. A **44**, 035301 (2010).

[130] F. Verstraete, J. Dehaene, and B. de Moor, *On the Geometry of Entangled States*, J. Mod. Opt. **49**, 1277 (2002).

[131] M. Horodecki, P. Horodecki, and R. Horodecki, *Limits for Entanglement Measures*, Phys. Rev. Lett. **84**, 2014 (2000).

[132] S. Ishizaka and M. B. Plenio, *Publishers Note: Multiparticle Entanglement under Asymptotic Positive-Partial-Transpose-Preserving Operations*, Phys. Rev. A **72**, 059907 (2005).
[133] M. B. Plenio and S. Virmani, *An Introduction to Entanglement Measures*, Quantum Inf. Comput. **7**, 1 (2007).
[134] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevX.11.041016 for codes to get plots.
[135] M. Pivoluska, M. Huber, and M. Malik, *Layered Quantum Key Distribution*, Phys. Rev. A **97**, 032312 (2018).
[136] C. E. Shannon, *Two-Way Communication Channels*, in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics* (University of California Press, Berkeley, California, 1961), pp. 611–644.
[137] A. El Gamal and Y.-H. Kim, *Network Information Theory* (Cambridge University Press, Cambridge, England, 2012), p. 709.
[138] K. Brádler, P. Hayden, D. Touchette, and M. M. Wilde, *Trade-off Capacities of the Quantum Hadamard Channels*, Phys. Rev. A **81**, 062312 (2010).
[139] Q. Wang, S. Das, and M. M. Wilde, *Hadamard Quantum Broadcast Channels*, Quantum Inf. Process. **16**, 248 (2017).
[140] F. Leditzky, M. A. Alhejji, J. Levin, and G. Smith, *Playing Games with Multiple Access Channels*, Nat. Commun. **11**, 1497 (2020).
[141] S.-H. Tan and P. P. Rohde, *The Resurgence of the Linear Optics Quantum Interferometer—Recent Advances & Applications*, Rev. Phys. **4**,100030 (2019).
[142] S. Das and M. M. Wilde, *Quantum Rebound Capacity*, Phys. Rev. A **100**, 030302(R) (2019).
[143] R. L. Frank and E. H. Lieb, *Monotonicity of a Relative Rényi Entropy*, J. Math. Phys. (N.Y.) **54**, 122201 (2013).
[144] S. Beigi, *Sandwiched Rényi Divergence Satisfies Data Processing Inequality*, J. Math. Phys. (N.Y.) **54**, 122202 (2013).
[145] F. Hiai and D. Petz, *The Proper Formula for Relative Entropy and Its Asymptotics in Quantum Probability*, Commun. Math. Phys. **143**, 99 (1991).
[146] H. Nagaoka, *Strong Converse Theorems in Quantum Information Theory*, in *Proceedings of ERATO Workshop on Quantum Information Science* (2001), p. 33; also appeared in *Asymptotic Theory of Quantum Statistical Inference*, edited by M. Hayashi (World Scientific, Singapore, 2005).
[147] T. Ogawa and H. Nagaoka, *Strong Converse and Stein's Lemma in Quantum Hypothesis Testing*, IEEE Trans. Inf. Theory **46**, 2428 (2000).
[148] T. Cooney, M. Mosonyi, and M. M. Wilde, *Strong Converse Exponents for a Quantum Channel Discrimination Problem and Quantum-Feedback-Assisted Communication*, Commun. Math. Phys. **344**, 797 (2016).
[149] O. Fawzi, P. Hayden, I. Savov, P. Sen, and M. M. Wilde, *Classical Communication over a Quantum Interference Channel*, IEEE Trans. Inf. Theory **58**, 3670 (2012).
[150] I. Devetak, *The Private Classical Capacity and Quantum Capacity of a Quantum Channel*, IEEE Trans. Inf. Theory **51**, 44 (2005).
[151] J. Yard, P. Hayden, and I. Devetak, *Quantum Broadcast Channels*, IEEE Trans. Inf. Theory **57**, 7147 (2011).
[152] J. Yard, P. Hayden, and I. Devetak, *Capacity Theorems for Quantum Multiple-Access Channels: Classical-Quantum and Quantum-Quantum Capacity Regions*, IEEE Trans. Inf. Theory **54**, 3091 (2008).
[153] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, *Private Quantum Channels*, *Proceedings of the IEEE 41st Annual Symposium on Foundations of Computer Science* (2000), pp. 547–553, https://ieeexplore.ieee.org/document/892142.
[154] K. C. Toh, M. J. Todd, and R. H. Tütüncü, *SDPT3—A Matlab Software Package for Semidefinite Programming, Version 1.3*, *Optim. Methods Software* 11, 545 (1999).