This is a repository copy of *Converse bounds for quantum and private communication over Holevo-Werner channels*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/137392/

Version: Accepted Version

Converse bounds for quantum and private communication over Holevo-Werner channels

Thomas P. W. Cope,[1] Kenneth Goodenough,[2] and Stefano Pirandola[1]

[1]*Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK*
[2]*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*

Werner states have a host of interesting properties, which often serve to illuminate the unusual properties of quantum information. Starting from these states, one may define a family of quantum channels, known as the Holevo-Werner channels, which themselves afford several unusual properties. In this paper we use the teleportation covariance of these channels to upper bound their two-way assisted quantum and secret-key capacities. This bound may be expressed in terms of relative entropy distances, such as the relative entropy of entanglement, and also in terms of the squashed entanglement. Most interestingly, we show that the relative entropy bounds are strictly subadditive for a sub-class of the Holevo-Werner channels, so that their regularisation provides a tighter performance. These information-theoretic results are first found for point-to-point communication and then extended to repeater chains and quantum networks, under different types of routing strategies.

I. INTRODUCTION

The area of quantum information and computation [1–5] is one of the fastest growing fields. Understanding how quantum information is transmitted is necessary not only for the development of a future quantum Internet [6–13] but also for the construction of practical quantum key distribution (QKD) [14–17] networks. Motived by this, there is much interest in trying to establish the optimal performance in the transmission of quantum bits (qubits), entanglement bits (ebits) and secret bits between two remote users. This is a theoretical framework which is a direct quantum generalization of Shannon's theory of information [18, 19]. In the quantum setting, there are different types of maximum rates, i.e., capacities, that may be defined for a given quantum channel. These include the classical capacity (transmission of classical bits), the entanglement distribution capacity (distribution of ebits), the quantum capacity (transmission of qubits), the private capacity (transmission of private bits), and the secret-key capacity (distribution of secret bits). All these capacities may be defined allowing side local operations (LOs) and classical communication (CC) either one-way or two-way between the remote parties.

We shall focus on the use of LOs assisted by two-way CC, also known as "adaptive LOCCs". The maximization over these types of LOCCs leads to the definition of corresponding two-way assisted capacities. In particular, in this work we are interested in the two-way quantum capacity Q_2 (which is equal to the two-way entanglement distribution capacity D_2) and the secret-key capacity K (which is equal to the two-way private capacity P_2). Generally, these capacities are extremely difficult to calculate because they involve quantum protocols based on adaptive LOCCs, where input states and the output measurements are optimized in an interactive way by the two remote parties. Similar adaptive protocols may be considered in other tasks, such as quantum hypothesis testing [20–22] and quantum metrology [21, 23–29].

Building on a number of preliminary tools [30–43] and generalizing ideas therein to arbitrary dimension and arbitrary tasks, Ref. [44] showed how to use the LOCC simulation [45] of a quantum channel to reduce an arbitrary adaptive protocol into a simpler block version. More precisely, Ref. [44] showed how the suitable combination of an adaptive-to-block reduction (teleportation stretching) with an entanglement measure, such as the relative entropy of entanglement (REE) [46–48], allows one to reduce the expression of Q_2 and K to a computable single-letter version. In this way, Ref. [44] established the two-way capacities of several quantum channels, including the bosonic lossy channel [5], the quantum-limited amplifier, the dephasing and the erasure channel [1]. The secret-key capacity of the erasure channel was also established in a simultaneous work [49] by using a different approach based on the squashed entanglement [50], which also appears to be powerful in the case of the amplitude damping channel [44, 49]. Note that, prior to these results, only the Q_2 of the erasure channel was known [51].

One of the golden rules to apply the previous techniques is teleportation covariance, first considered for discrete variable (DV) channels [41–43] and then extended to any dimension, finite or infinite [44]. This is the property of a quantum channel to "commute" with the random unitaries of quantum teleportation [52–55]. Because the Holevo-Werner (HW) channels [56, 57] are teleportation covariant, we may therefore apply the previous reduction tools and bound their two-way assisted capacities, Q_2 and K, via single-letter quantities. These channels are particularly interesting because the resulting upper bounds, based on relative entropy distances (such as the REE), are generally non-additive. In fact, we show a regime of parameters where a multi-letter bound is strictly tighter than a single-letter one.

As a result of this sub-additivity, the regularisation of the upper bound needs to be considered for the capacities Q_2 and K of these channels. This is a property that the HW channels inherit from their Choi matrices, the Werner states [58]. Recall that these states may be entangled, yet admit a local model for all measure-

ments [58, 59]. They disproved the additivity of REE [60] (which is the main property exploited here), and they are also conjectured to prove the existence of negative partial transpose undistillable states [61].

Another interesting finding is that bounds which are based on the squashed entanglement compete with the REE bounds in a way that there is not a clear preference among them. In fact, we find that the secret-key capacity of an HW channel is better bounded by the REE or the squashed entanglement depending on the value of its main defining parameter. This is a feature which has never been observed for another quantum channel so far.

The structure of this paper is as follows. We begin in Sec. II by introducing the mathematical description of both Werner states and HW channels. In Sec. III we review the notions of relative entropy distance with respect to separable states and partial positive transpose (PPT) states, also discussing their regularised versions. In Sec. IV, we compute the REE for the overall state consisting of two identical Werner states, discussing the strict subadditivity of the REE for a subclass of the family. Then, in Sec. V we give our upper bounds to the Q_2 and K of the HW channels, which too exhibits the subadditivity property. Here we also prove a general upper bound for the Q_2 of any teleportation covariant channel (at any dimension). In Sec. VI we extend the results to repeater chains and quantum networks connected by HW channels. We then conclude and summarize in Sec. VII.

II. WERNER STATES AND HOLEVO-WERNER CHANNELS

Werner states are an important family of quantum states which are generally defined over two qudits of equal dimension d. They have the peculiar property to be invariant under unitaries U_d applied identically to both subsystems, i.e., they satisfy the fixed-point equation

$$(U_d \otimes U_d)\rho(U_d^\dagger \otimes U_d^\dagger) = \rho. \tag{1}$$

There exists several parametrisations of this family as also shown in Fig. 1. We shall use the "expectation representation", where the Werner state $W_{\eta,d}$ is parametrised by $\eta \in [0,1]$ which is defined by the mean value

$$\eta := \text{Tr}[W_{\eta,d}\mathbb{F}], \tag{2}$$

where $\mathbb{F}$ is the flip operator acting on two qudits in the computational basis $\{|i\rangle\}_{i=0}^{d-1}$, i.e.,

$$\mathbb{F} := \sum_{i,j=0}^{d-1} |ij\rangle \langle ji|. \tag{3}$$

If η is negative (non-negative), then the Werner state is entangled (separable). One also has an explicit formula for $W_{\eta,d}$ as a linear combination of the $\mathbb{F}$ operator and the d^2-dimensional identity operator $\mathbb{I}$, i.e.,

$$W_{\eta,d} = \frac{(d-\eta)\mathbb{I} + (d\eta - 1)\mathbb{F}}{d^3 - d}. \tag{4}$$

As already mentioned before, Werner states are of much interest to quantum information theorists due to their properties. For $d \geq 3$ there are Werner states which are entangled, yet admit a local model for all measurements [58, 59]. In particular, the extremal entangled Werner state $W_{-1,d}$ was used to disprove the additivity of the REE [60]. A useful property of the Werner states is that, for a given dimension, they are simultaneously diagonalisable, i.e., they share a common eigenbasis. A Werner state $W_{\eta,d}$ has n_+ (n_-) eigenvectors with eigenvalue γ_+ (γ_-), where $n_\pm := d(d \pm 1)/2$ and $\gamma_\pm := (1 \pm \eta)[d(d \pm 1)]^{-1}$.

Closely linked with Werner states are the HW channels [56, 57]. These are defined as those channels $\mathcal{W}_{\eta,d}$ whose Choi matrices are Werner states $W_{\eta,d}$. In other words, we have

$$W_{\eta,d} := \mathbf{I} \otimes \mathcal{W}_{\eta,d} (|\Phi\rangle \langle\Phi|), \tag{5}$$

where $\mathbf{I}$ is the d-dimensional identity map and $|\Phi\rangle = d^{-1/2} \sum_{i=0}^{d-1} |ii\rangle$ is a maximally-entangled state. This is a family of quantum channels whose action can be expressed as

$$\mathcal{W}_{\eta,d}(\rho) := \frac{(d-\eta)\mathbf{I} + (d\eta - 1)\rho^T}{d^2 - 1}, \tag{6}$$

where T is transposition (see Fig. 2 for a representation in the specific case $d = 2$). It is known that the minimal output entropy of the HW channels is additive [57], and the extremal HW channel (for $\eta = -1$) is a counterexample of the additivity of the minimal Renyí entropy [56]. HW channels were also studied by Ref. [43] in relation to forward-assisted quantum error correcting codes and superactivation of quantum capacity.

An important property of the HW channels is their *teleportation covariance*. A quantum channel $\mathcal{E}$ is called "teleportation covariant" if, for any teleportation unitary U, there exists some unitary V such that [44]

$$\mathcal{E}(U\rho U^\dagger) = V\mathcal{E}(\rho)V^\dagger, \tag{7}$$

for any state ρ. The teleportation unitaries referred to here are the Weyl-Heisenberg generalisation of the Pauli matrices [1]. Note that the output unitary V may belong to a different representation of the input group. For an HW channel $\mathcal{W}_{\eta,d}$, it is easy to see that we may write

$$\mathcal{W}_{\eta,d}(U_d\rho U_d^\dagger) = U_d^* \mathcal{W}_{\eta,d}(\rho)(U_d^*)^\dagger, \tag{8}$$

for an arbitrary unitary U_d. This comes from Eq. (6) and noting that $\mathbf{I} = U_d^*\mathbf{I}(U_d^*)^\dagger$ and $(U_d\rho U_d^\dagger)^T = U_d^*\rho^T(U_d^*)^\dagger$.

III. RELATIVE ENTROPY DISTANCES

An important functional of two quantum states ρ and σ is their relative entropy, which is defined as

$$S(\rho||\sigma) = \text{Tr}(\rho\log_2\rho - \rho\log_2\sigma). \tag{9}$$

Representation	Variable	State	Separable Extreme	Boundary	Entangled Extreme
α-rep	α	$\frac{1}{d^2-d\alpha}\left(\mathbb{I}-\alpha\mathbb{F}\right)$	-1	$\frac{1}{d}$	1
Weighting rep	p	$\frac{1-p}{d^2+d}\left(\mathbb{I}+\mathbb{F}\right)+\frac{p}{d^2-d}\left(\mathbb{I}-\mathbb{F}\right)$	0	$\frac{1}{2}$	1
Expectation rep	$\langle\mathbb{F}\rangle=\eta$	$\frac{1}{d^3-d}\left[(d-\eta)\mathbb{I}+(d\eta-1)\mathbb{F}\right]$	1	0	-1
Anti-rep	t	$t\frac{\mathbb{I}-d\mathbb{F}}{d^2(d-1)}+\frac{\mathbb{I}}{d^2}$	$-\frac{1}{d-1}$	$\frac{1}{d+1}$	1

FIG. 1. The various ways in which the set of Werner states of dimension d may be parametrised. All of these are equivalent and may be transformed between. Here $\mathbb{I}$ is the d^2-dimensional identity operator and $\mathbb{F}$ is the flip operator.
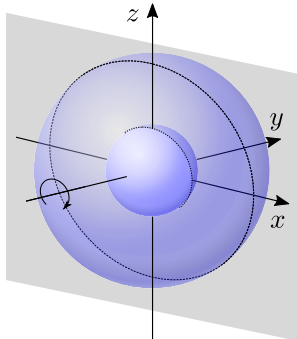

FIG. 2. An illustration of the qubit HW channel ($d=2$). The Bloch sphere is shrunk by a factor of $|\frac{2\eta-1}{3}|$, with the state reflected in the x-z axis for $\frac{2\eta-1}{3}>0$, and rotated by π around the y axis for $\frac{2\eta-1}{3}<0$.

This is the basis for defining relative entropy distances. Given any compact and convex set of states S (containing the maximally mixed state), the relative entropy distance of a state ρ from this set is defined as [62]

$$E_S\left(\rho\right):=\inf_{\sigma\in S}S(\rho||\sigma). \tag{10}$$

This is known to be asymptotically continuous [62, 63]. One possible choice for S is the set of separable (SEP) states, in which case we have the REE [46–48]

$$E_R\left(\rho\right):=\inf_{\sigma\in\mathrm{Sep}}S(\rho||\sigma). \tag{11}$$

Another possible choice is the set of PPT states, in which case we have the relative entropy distance with respect to PPT states, which we denote by RPPT. This is defined as

$$E_P\left(\rho\right):=\inf_{\sigma\in\mathrm{PPT}}S(\rho||\sigma), \tag{12}$$

which coincides with the Rains' bound [64, 65] when ρ is a Werner state, as shown in Ref. [66]. Recall that a PPT state σ is such that σ^{PT} has non-negative eigenvalues (where PT is transposition over the second subsystem only). This is a *necessary* condition for σ to be separable, but is *not sufficient*, unless σ is a 2-qubit or qubit-qutrit state. Thus, in general, we have

$$E_P(\rho)\leq E_R(\rho). \tag{13}$$

Both the measures here defined are subadditive, i.e., they have the following property under tensor product,

$$E^2_{R(P)}(\rho):=\frac{E_{R(P)}\left(\rho^{\otimes 2}\right)}{2}\leq E_{R(P)}\left(\rho\right). \tag{14}$$

It was shown that there exist states which are *strictly* subadditive ($<$). In fact, for $d>2$, Ref. [60] proved that

$$E^2_{R(P)}\left(W_{-1,d}\right)<E_{R(P)}(W_{-1,d}). \tag{15}$$

This motivates the definition of the regularised quantities

$$E^\infty_{R(P)}\left(\rho\right)=\lim_{n\to\infty}\frac{E_{R(P)}\left(\rho^{\otimes n}\right)}{n}\leq E_{R(P)}\left(\rho\right), \tag{16}$$

i.e., the regularised REE E^∞_R and RPPT $E^\infty_P\leq E^\infty_R$.

For an entangled Werner state, the closest separable and PPT state (for one copy) is the boundary Werner separable state $W_{0,d}$, so that [60]

$$E_{R(P)}\left(W_{\eta,d}\right) \tag{17}$$
$$=\begin{cases}0 & \text{if }\eta\geq 0,\\ \frac{1+\eta}{2}\log_2\left(1+\eta\right)+\frac{1-\eta}{2}\log_2\left(1-\eta\right) & \text{if }\eta\leq 0.\end{cases}$$

Note that the one-copy quantity $E_{R(P)}\left(W_{\eta,d}\right)$ does not depend on the dimension d. Then, for Werner states, the regularised RPPT E^∞_P is known [66] and reads

$$E^\infty_P\left(W_{\eta,d}\right) \tag{18}$$
$$=\begin{cases}0 & \text{if }\eta\geq 0,\\ \frac{1+\eta}{2}\log_2\left(1+\eta\right)+\frac{1-\eta}{2}\log_2\left(1-\eta\right) & \text{if }-\frac{2}{d}\leq\eta\leq 0,\\ \log_2\left(\frac{d+2}{d}\right)+\frac{1+\eta}{2}\log_2\left(\frac{d-2}{d+2}\right) & \text{if }\eta\leq -\frac{2}{d}.\end{cases}$$

From the previous equation, we see that we have strict subadditivity $E^\infty_P\left(W_{\eta,d}\right)<E_P\left(W_{\eta,d}\right)$ in the region $\eta<-2/d$. Note that, in the region $-2/d\leq\eta\leq 0$, the REE is additive, and that the REE, the RPPT, and their regularised versions all coincide. In fact, using the previous results, one has

$$E_R\left(W_{\eta,d}\right)=E_P\left(W_{\eta,d}\right)=E^\infty_P\left(W_{\eta,d}\right)$$
$$\leq E^\infty_R\left(W_{\eta,d}\right)\leq E_R\left(W_{\eta,d}\right). \tag{19}$$

IV. RELATIVE ENTOPY DISTANCE OF A TWO-COPY WERNER STATE

One of the results of Ref. [60] was to show that the closest state σ minimizing $E_{R(P)}(W_{\eta,d}^{\otimes n})$ is invariant under the following transformation

$$U_d^1 \otimes U_d^1 \otimes \ldots U_d^n \otimes U_d^n \, (\sigma) \, (U_d^1 \otimes U_d^1 \otimes \ldots U_d^n \otimes U_d^n)^\dagger, \quad (20)$$

where each $U_d^i \otimes U_d^i$ acts on the $d \times d$ Hilbert space occupied by the ith copy of $W_{\eta,d}$. States which are invariant under this action are of the form

$$\begin{aligned}
\sigma_{\mathbf{x}}^n &= x_0 W_{-1,d}^{\otimes n} \\
&+ \frac{x_1}{n}\left(W_{-1,d}^{\otimes n-1} \otimes W_{1,d} + \ldots W_{1,d} \otimes W_{-1,d}^{\otimes n-1}\right) \\
&+ \ldots + \frac{x_k}{\binom{n}{k}}\left(W_{-1,d}^{n-k} \otimes W_{1,d}^k \ldots W_{1,d}^k \otimes W_{-1,d}^{n-k}\right) \\
&+ \ldots + x_n W_{1,d}^{\otimes n},
\end{aligned} \quad (21)$$

where $\mathbf{x} = (x_0, x_1, \ldots, x_n)^T$ is a vector of probabilities, i.e., $x_i \geq 0$ and $\sum_{i=0}^n x_i = 1$. We also have an explicit condition of $\mathbf{x}$ to ensure that $\sigma_{\mathbf{x}}^n$ is PPT. This is [66]

$$\begin{pmatrix} -1 & 1 \\ 1 & \frac{d-1}{d+1} \end{pmatrix}^{\otimes n} \mathbf{x}' \geq 0, \quad (22)$$

where

$$\mathbf{x}' = \left(x_0, \overbrace{\frac{x_1}{n}, \ldots, \frac{x_1}{n}}^{n}, \ldots \overbrace{\frac{x_k}{\binom{n}{k}}, \ldots, \frac{x_k}{\binom{n}{k}}}^{\binom{n}{k}}, \ldots x_n\right)^T. \quad (23)$$

For general n, it is not known if the PPT states $\sigma_{\mathbf{x}}^n$ satisfying Eq. (22) are separable. However, they are known to be equivalent for $n = 2$ [60], in which case Eq. (22) simplifies to

$$1 - 2x_1 \geq 0, \quad (24)$$
$$(d-1) - 2dx_0 + (2-d)x_1 \geq 0, \quad (25)$$
$$(d-1)^2 + 4dx_0 + 2(d-1)x_1 \geq 0, \quad (26)$$

where we have eliminated the dependent variable x_2. This means that, for two copies ($n = 2$), the state $\sigma_{\mathbf{x}}^2$ is the closest state for the minimization of both $E_P(W_{\eta,d}^{\otimes 2})$ and $E_R(W_{\eta,d}^{\otimes 2})$. Let us compute the latter quantity.

Assuming the basis where the single-copy Werner state is diagonal, we may write

$$S\left(W_{\eta,d}^{\otimes n}||\sigma_{\mathbf{x}}^n\right) = \sum_{i=0}^n y_i \log_2\left(\frac{y_i}{x_i}\right), \quad (27)$$

$$y_i = \frac{\binom{n}{i}(1-\eta)^{n-i}(1+\eta)^i}{2^n}. \quad (28)$$

Therefore, for $n = 2$ and in the region $\eta \leq -\frac{2}{d}$, we derive

$$\begin{aligned}
E_R^2(W_{\eta,d}) &:= \frac{E_R\left(W_{\eta,d}^{\otimes 2}\right)}{2} = \min_{x_0,x_1}\left\{\frac{(1-\eta)^2}{8}\log_2\frac{(1-\eta)^2}{4x_0}\right. \\
&+ \frac{(1-\eta)(1-\eta)}{4}\log_2\frac{(1-\eta)(1-\eta)}{2x_1} \\
&\left.+ \frac{(1+\eta)^2}{8}\log_2\frac{(1+\eta)^2}{4(1-x_0-x_1)}\right\},
\end{aligned} \quad (29)$$

where

$$1 - 2x_1 \geq 0, \quad (30)$$
$$(d-1) - 2dx_0 + (2-d)x_1 \geq 0, \quad (31)$$
$$(d-1)^2 + 4dx_0 + 2(d-1)x_1 \geq 0, \quad (32)$$
$$x_0 + x_1 \leq 1. \quad (33)$$

We can use Lagrangian optimisation methods to solve this problem. Let us set

$$\begin{aligned}
\theta &:= d^4(\eta^2+1)^2 - 4d^3\eta(\eta^2-3) \\
&- 4d^2(\eta^4+3\eta^2-1) + 8d\eta(\eta^2-3) + 4(\eta^2+1)^2,
\end{aligned} \quad (34)$$

then we compute

$$x_0 = \frac{d^2(\eta^2+1) + \sqrt{\theta} - 2d(\eta-2) - 2\eta^2 - 2}{8d(d+2)}, \quad (35)$$

$$x_1 = -\frac{d^2(\eta^2-3) + \sqrt{\theta} - 2d\eta - 2\eta^2 + 6}{4(d^2-4)}. \quad (36)$$

The comparison between the one-copy REE $E_R(W_{\eta,d})$ of Eq. (17) and the two-copy REE $E_R^2(W_{\eta,d})$ of Eq. (29) is shown in Fig. 3. While $E_R(W_{\eta,d})$ does not depend on the dimension d, we see that the two-copy REE considerably decreases for increasing $d > 2$.
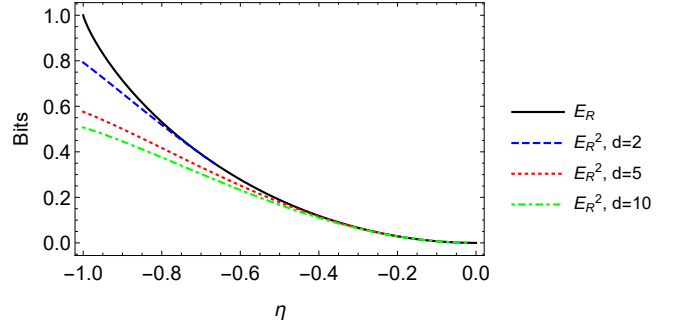

FIG. 3. Comparison between the one-copy REE E_R and the two-copy REE E_R^2 of a Werner state $W_{\eta,d}$, for varying dimension $d > 2$. In particular, we consider here $\eta \leq 0$ which includes the subadditivity region $\eta < -2/d$.

V. TWO-WAY ASSISTED CAPACITIES OF THE HOLEVO-WERNER CHANNELS

A. Weak converse bounds based on the relative entropy distances

We now combine the results in the previous section with the methods of Ref. [44] to bound the two-way capacities of the HW channels. According to Ref. [44], the secret-key capacity K of a teleportation covariant channel $\mathcal{E}$ is upper bounded by the regularised REE of its Choi Matrix $\chi_{\mathcal{E}}$, i.e.,

$$K\left(\mathcal{E}\right) \le E_R^\infty\left(\chi_{\mathcal{E}}\right). \qquad (37)$$

Therefore, for an HW channel $\mathcal{W}_{\eta,d}$, we may write the upper bound

$$K(\mathcal{W}_{\eta,d}) \le E_R^\infty\left(W_{\eta,d}\right), \qquad (38)$$

by using its corresponding Werner state $W_{\eta,d}$. From the previous section, we have that, for $\eta < -2/d$ we may write the following strict inequality

$$K(\mathcal{W}_{\eta,d}) \le E_R^2\left(W_{\eta,d}\right) < E_R\left(W_{\eta,d}\right), \qquad (39)$$

so that the one-copy (single-letter) REE bound is strictly loose. This shows that the regularised REE is needed to tightly bound (and possibly establish) the secret-key capacity of an HW channel. As shown in Fig. 3, the improvement of E_R^2 over E_R is better and better for increasing dimension d.

Let us now consider the two-way quantum capacity Q_2, which is also known to be equal to the channel's two-way entanglement distribution capacity D_2. In Appendix A, we provide a general proof of the following.

Lemma 1 (Channel's RPPT bound) *For a teleportation covariant channel $\mathcal{E}$, we may write*

$$Q_2(\mathcal{E}) \le E_P^\infty\left(\chi_{\mathcal{E}}\right), \qquad (40)$$

where the Choi matrix $\chi_{\mathcal{E}}$ and the RPPT E_P^∞ are meant to be asymptotic if $\mathcal{E}$ is a continuous-variable channel. In particular, $E_P^\infty\left(\chi_{\mathcal{E}}\right)$ becomes the regularisation of

$$E_P\left(\chi_{\mathcal{E}}\right) := \inf_{\sigma^\mu} \liminf_{\mu\to+\infty} S(\chi_{\mathcal{E}}^\mu || \sigma^\mu), \qquad (41)$$

where: $\chi_{\mathcal{E}}^\mu := \mathcal{I}\otimes\mathcal{E}(\Phi^\mu)$ is defined on a two-mode squeezed vacuum state Φ^μ with energy μ, and σ^μ is a sequence of PPT states converging in trace norm, i.e., such that $\|\sigma^\mu - \sigma\| \xrightarrow{\mu} 0$ for some PPT state σ.

By applying the bound of Eq. (40) to an HW channel $\mathcal{W}_{\eta,d}$, we may write

$$Q_2(\mathcal{W}_{\eta,d}) \le E_P^\infty\left(W_{\eta,d}\right), \qquad (42)$$

where the right hand side is computed as in Eq. (18). Of course we may also write

$$Q_2(\mathcal{W}_{\eta,d}) \le E_R^2\left(W_{\eta,d}\right) \le E_R\left(W_{\eta,d}\right) = E_P\left(W_{\eta,d}\right). \qquad (43)$$

The bounds in Eqs. (42) and (43) are shown and compared in Fig. 4 for a HW channel in dimension $d = 5$.
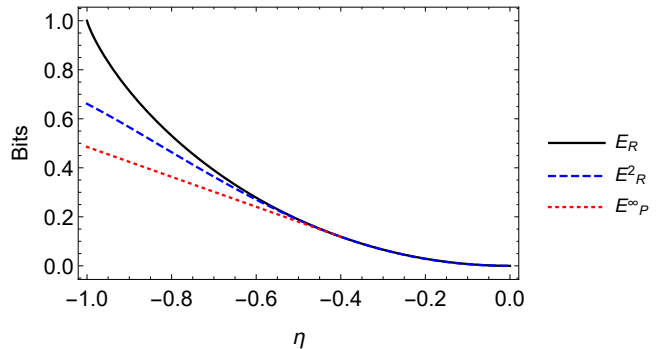

FIG. 4. Weak converse upper bounds for the two-way quantum capacity Q_2 of the HW channel $\mathcal{W}_{\eta,5}$ (dimension $d = 5$). We compare the one-copy REE bound $E_R(= E_P)$, the two-copy REE bound $E_R^2\left(= E_P^2\right)$, and the regularised RPPT bound E_P^∞, which is the tightest. Note that E_R and E_R^2 also bound the secret-key capacity K of the channel.

B. Weak converse bounds based on the squashed entanglement

Whilst the relative entropy distances provide useful upper bounds, we may also consider other functionals. In particular, we may consider the squashed entanglement. For an arbitrary bipartite state ρ_{AB}, this is defined as [2, 50]

$$E_{sq}(\rho_{AB}) := \frac{1}{2} \min_{\rho'_{ABE}\in\Omega_{AB}} S(A : B|E), \qquad (44)$$

where Ω_{AB} is the set of density matrices ρ'_{ABE} satisfying $\text{Tr}_E(\rho'_{ABE}) = \rho_{AB}$, and $S(A : B|E)$ is the conditional mutual information

$$S(A : B|E) := S(\rho'_{AE}) + S(\rho'_{BE}) - S(\rho_E) - S(\rho_{ABE}), \qquad (45)$$

with $S(...)$ being the Von Neumann entropy [1].

The squashed entanglement can be combined with teleportation stretching [44] to provide a single-letter bound to the secret-key capacity. In fact, it satisfies all the required conditions. It normalises, so that $E_{sq}(\phi_m) \ge mR_m$ for a private state ϕ_m with mR_m private bits [50]. It is continuous, and monotonic under LOCC [50]. Furthermore, it is additive over tensor-product states, which means that there is no need to regularize over many copies. For a teleportation covariant dicrete-variable channel $\mathcal{E}$, we may therefore write

$$K(\mathcal{E}) \le E_{sq}(\chi_{\mathcal{E}}). \qquad (46)$$

This is a direct consequence of Proposition 6 of Ref. [44], according to which we may write

$$K(\mathcal{E}) = K(\chi_{\mathcal{E}}), \qquad (47)$$

where the latter is the distillable key of the Choi matrix $\chi_{\mathcal{E}}$. Then, using Ref. [50], we may write $K(\chi_{\mathcal{E}}) \le E_{sq}(\chi_{\mathcal{E}})$, which leads to Eq. (46) [67].

However, there is some difficulty in optimizing over ρ'_{ABE} such that $\mathrm{Tr}_E(\rho'_{ABE}) = \chi_{\mathcal{E}}$, since the dimension of the environment system E is generally unbounded. In order to provide an analytical upper bound, we simply choose the purification $\tilde{\chi}_{\mathcal{E}}$ of $\chi_{\mathcal{E}}$. In the case of an HW channel $\mathcal{E} = \mathcal{W}_{\eta,d}$, we have $\chi_{\mathcal{E}} = W_{\eta,d}$ and we may write

$$K(\mathcal{W}_{\eta,d}) \leq E_{sq}(\mathcal{W}_{\eta,d})$$
$$\leq \tilde{E}_{sq}(\mathcal{W}_{\eta,d}) := \frac{1}{2} S(A:B|E)_{\tilde{W}_{\eta,d}}$$
$$= \log_2 d + \frac{1+\eta}{4} \log_2 \frac{1+\eta}{d(d+1)}$$
$$+ \frac{1-\eta}{4} \log_2 \frac{1-\eta}{d(d-1)}, \tag{48}$$

which is positive only if $\eta \leq 0$.

We can find a further upper bound by exploiting the convexity property of the squashed entanglement. First note that

$$W_{\eta,d} = \frac{(d-\eta)\,\mathbb{I} + (d\eta-1)\,\mathbb{F}}{d^3 - d}$$
$$= (1+\eta)\,W_{0,d} + (-\eta)\,W_{-1,d}, \tag{49}$$

which means that for $-1 \leq \eta \leq 0$ the state $W_{\eta,d}$ can be written as a convex combination of the separable state $W_{0,d}$ and the extremal Werner state $W_{-1,d}$. Second, note that we have $E_{sq}(W_{0,d}) = 0$ (since it is a separable state) and, for the extremal state, we may write [68]

$$E_{sq}(W_{-1,d}) \leq \begin{cases} \log_2\left(\frac{d+2}{d}\right) & \text{if } d \text{ even}, \\ \frac{1}{2}\log_2\left(\frac{d+3}{d-1}\right) & \text{if } d \text{ uneven}. \end{cases} \tag{50}$$

Using the convexity property of the squashed entanglement [50]

$$E_{sq}\left[p\rho_1 + (1-p)\rho_2\right]$$
$$\leq p E_{sq}(\rho_1) + (1-p) E_{sq}(\rho_2), \tag{51}$$

we find that

$$K(\mathcal{W}_{\eta,d}) \leq E_{sq}(\mathcal{W}_{\eta,d}) \leq E_{sq}^*(\mathcal{W}_{\eta,d}), \tag{52}$$

where we define

$$E_{sq}^*(\mathcal{W}_{\eta,d}) = \begin{cases} -\eta \log_2\left(\frac{d+2}{d}\right) & \text{if } d \text{ even}, \\ -\frac{\eta}{2}\log_2\left(\frac{d+3}{d-1}\right) & \text{if } d \text{ uneven}, \end{cases} \tag{53}$$

for $-1 \leq \eta \leq 0$ and zero otherwise.

These bounds are compared in Fig. 5 for the case of an HW channel with dimension $d = 4$. We can see that one bound is better than another depending on the value of η. In particular, the secret-key capacity is in the gray area of Fig. 5(a) or, equivalently, below the composition of bounds shown in Fig. 5(b).

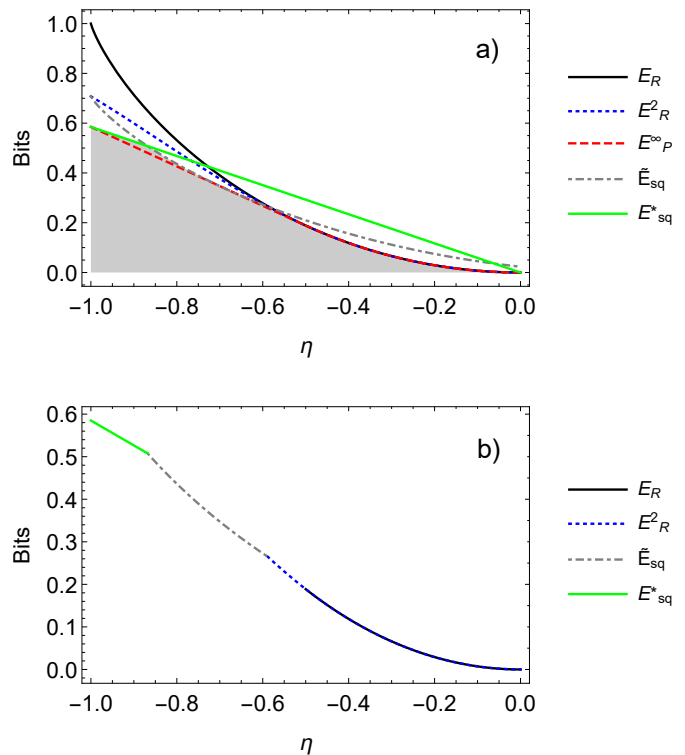FIG. 5. Comparison of the capacity bounds for the HW channel $\mathcal{W}_{\eta,4}$. (a) The regularised RPPT bound E_P^∞ is the lowest (red-dashed) curve and bounds the two-way quantum capacity Q_2 of the channel. The secret-key capacity of the channel K is in the gray area. Depending on the value of η, this is upper-bounded by the two-copy REE bound $E_R^2(= E_P^2)$ (better than $E_R(= E_P)$) or by the squashed entanglement bounds $\tilde{E}_{sq}$ and E_{sq}^*. We see that $\tilde{E}_{sq}$ coincides with E_R^2 for $\eta = -1$. (b) We show the competing upper bounds for the secret-key capacity K of the HW channel $\mathcal{W}_{\eta,4}$, explicitly drawing which bound is better at which value of η. We see that the squashed entanglement bounds perform better at lower η, while the REE bounds are better for higher η.

VI. HOLEVO-WERNER REPEATER CHAINS AND QUANTUM NETWORKS

A. Repeater chains

In this section, we apply the results of Ref. [9] to bound the end-to-end capacities of quantum networks in which the edges between nodes are HW channels. First, we consider the simplest multi-hop quantum network which consists of a linear chain of N repeaters between the two end-parties. Such a set up is depicted in Fig. 6.

For a linear chain of N quantum repeaters, whose $N+1$ connecting channels $\{\mathcal{E}_i\}_{i=0}^N$ are teleportation covariant, we have that the secret capacity K of the chain and its

FIG. 6. Alice (A) and Bob (B) are connected by N quantum repeaters $r_1, \ldots, r_N$ in a linear chain; each connection (edge) in the chain is a d dimension HW channel with a generally-different parameter η_i.

two-way quantum capacity Q_2 are bounded by [9]

$$
\begin{aligned}
Q_2 \leq K &\leq \min_i E_R^\infty \left(\chi_{\mathcal{E}_i} \right) \\
&\leq \min_i E_R^2 \left(\chi_{\mathcal{E}_i} \right) \leq \min_i E_R \left(\chi_{\mathcal{E}_i} \right),
\end{aligned} \tag{54}
$$

with $\chi_{\mathcal{E}_i}$ the Choi matrix of the ith channel. Similarly, we may use the squashed entanglement and write [9]

$$
\begin{aligned}
Q_2 \leq K &\leq \min_i E_{sq} \left(\chi_{\mathcal{E}_i} \right) \\
&\leq \min\{\min_i \tilde{E}_{sq} \left(\chi_{\mathcal{E}_i} \right), \min_i E_{sq}^* \left(\chi_{\mathcal{E}_i} \right)\}.
\end{aligned} \tag{55}
$$

In general, we may write

$$
Q_2 \leq K \leq \min_E \min_i E \left(\chi_{\mathcal{E}_i} \right), \tag{56}
$$

where the bound is also minimized over the type of entanglement measure. In particular, we may consider the "ideal" set $E \in \{E_R^\infty, E_{sq}\}$ or the "computable" one $E \in \{E_R^2 \leq E_R, \tilde{E}_{sq}, E_{sq}^*\}$. Then, if the task of the parties is to transmit qubits (or distill ebits), we may use the regularised RPPT and write [9]

$$
Q_2 = D_2 \leq \min_i E_P^\infty \left(\chi_{\mathcal{E}_i} \right). \tag{57}
$$

Let us apply these results to a linear repeater chain connected by $N + 1$ iso-dimensional HW channels $\{\mathcal{W}_{\eta_i, d}\} = \{\mathcal{W}_{\eta_0, d}, \ldots, \mathcal{W}_{\eta_N, d}\}$, i.e., with the same dimension d but generally different η's. We may simplify the previous bounds (E_R, E_R^2, $\tilde{E}_{sq}$, E_{sq}^*, and E_P^∞) by exploiting the fact that they are monotonically decreasing in η, so that the maximum value $\eta_{\max} := \max\{\eta_i\}$ determines the bottleneck of the chain, i.e., $\min_i E = E(\mathcal{W}_{\eta_{\max}, d})$. In particular, for $\eta_{\max} \geq 0$, we certainly have $Q_2 = D_2 = K = 0$ because $E_R(\mathcal{W}_{\eta_{\max} \geq 0, d}) = 0$ from Eq. (17). By contrast, if $\eta_{\max} \leq 0$, then we may write the following bounds for the secret-key capacity and two-way quantum capacity of the repeater chain

$$
K \left(\{\mathcal{W}_{\eta_i, d}\} \right) \leq \min_E E \left(\mathcal{W}_{\eta_{\max}, d} \right), \tag{58}
$$

$$
Q_2 \left(\{\mathcal{W}_{\eta_i, d}\} \right) \leq E_P^\infty \left(\mathcal{W}_{\eta_{\max}, d} \right). \tag{59}
$$

In Eq. (58), the optimal entanglement measure E can be computed from the set $\{E_R^2 \leq E_R, \tilde{E}_{sq}, E_{sq}^*\}$, where E_R is given in Eq. (17), E_R^2 in Eq. (29), $\tilde{E}_{sq}$ in Eq. (48), E_{sq}^* in Eq. (53). In Eq. (59), we compute E_P^∞ from Eq. (18).

B. Single-path routing in quantum networks

We may then extend the results to an arbitrary quantum network, where there exist many possible paths between the two end-parties, Alice and Bob. Assuming single-path routing, a single chain of repeaters is used for each use of the network and this may differ from use to use. For a network connected by teleportation covariant channels, we may bound the single-path secret-key capacity of the network as [9]

$$
K \leq \min_C E(C), \ E(C) := \max_{\mathcal{E} \in \tilde{C}} E(\chi_{\mathcal{E}}), \tag{60}
$$

where E is a suitable entanglement measure, here to be optimized in $\{E_R, E_{sq}\}$ [69], and $\tilde{C}$ is a "cut-set" associated with the cut [70, 71].

The cut-set $\tilde{C}$ can be described as a set of channels such that, if those channels were removed by the cut, then the network would be bi-partitioned, with Alice and Bob in separate sets of nodes. Therefore the meaning of Eq. (60) is that: (i) we perform an arbitrary cut C of the network; (ii) we consider the channels $\mathcal{E}$ in the cut-set $\tilde{C}$; (iii) we compute the entanglement measure E of their Choi matrices $\chi_{\mathcal{E}}$; (iv) we take the maximum so as to compute $E(C)$; (v) we finally minimize over all the possible Alice-Bob cuts C of the network.

In the case of a quantum network connected by HW channels, we may the following bound for the single-path secret-key capacity

$$
K \leq \min_C \max_{\mathcal{W}_{\eta, d} \in \tilde{C}} E(\mathcal{W}_{\eta, d}). \tag{61}
$$

If the HW channels are iso-dimensional (as in the example of Fig. 7), then we may simplify the previous bound into the following

$$
K \leq \min_C E(\mathcal{W}_{\eta_{\min(C)}, d}), \tag{62}
$$

where $\eta_{\min(C)}$ is the smallest expectation parameter belonging to the cut-set $\tilde{C}$. In particular, we may also minimize E over $\{E_R, \tilde{E}_{sq}, E_{sq}^*\}$ by computing E_R as in Eq. (17), $\tilde{E}_{sq}$ as in Eq. (48), and E_{sq}^* as in Eq. (53).

C. Multi-path routing in quantum networks

Finally we may also consider multipath routing. In this case, each use of the network corresponds to a simultaneous use of all the channels, allowing for simultaneous pathways between Alice and Bob (e.g., see Fig. 8). This is also known as a flooding protocol [72] and represents a crucial requirement in order to extend the max-flow/min-cut theorem [73–75] to the quantum setting [9].

For a network connected by teleportation-covariant channels, the multi-path secret-key capacity $K^{\mathrm{m}} \geq K$
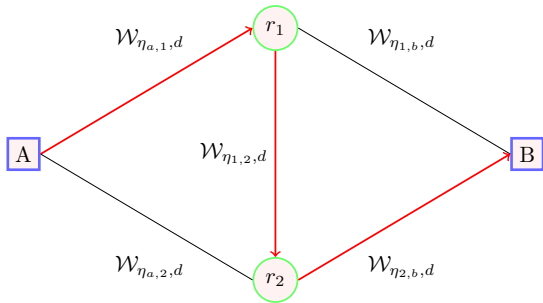
FIG. 7. Alice (A) and Bob (B) as end-nodes of a diamond network connected by iso-dimensional HW channels with generally-different expectation parameters η. In red we show a possible path between the end-nodes.
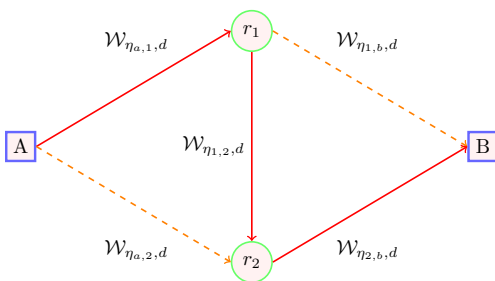

FIG. 8. Example of multipath routing in a diamond network (with iso-dimensional HW channels). With respect to Fig. 7 all the channels are used in a single use of the network (flooding protocol). Dashed lines represent the advantage over the previous single-path routing protocol.

is bounded as [9]

$$
\begin{aligned}
K^{\mathrm{m}} \leq \min_C \Sigma^\infty(C) & \leq \cdots \leq \min_C \Sigma^r(C) \\
& \leq \cdots \leq \min_C \Sigma^1(C),
\end{aligned}
\tag{63}
$$

where, for any integer $r = 1, \cdots, \infty$,

$$
\Sigma^r(C) := \sum_{\mathcal{E} \in \tilde{C}} E^r(\chi_{\mathcal{E}}).
\tag{64}
$$

and E^r is a suitable r-copy entanglement measure. In particular, we may optimize over the multi-copy REE $E^r = E_R^r$ or the squashed entanglement $E^r = E_{sq}$ (the latter being additive). For the multipath two-way quantum capacity, we may correspondingly write

$$
Q_2^{\mathrm{m}} \leq \min_C \Sigma_P^\infty(C) \leq \cdots \leq \min_C \Sigma_P^1(C),
\tag{65}
$$

where

$$
\Sigma_P^r(C) := \sum_{\mathcal{E} \in \tilde{C}} E_P^r(\chi_{\mathcal{E}}),
\tag{66}
$$

and E_P^r is the r-copy RPPT.

For a network connected by HW channels $\mathcal{W}_{\eta,d}$, we may specify the previous bounds to one- and two-copy REE, so that we may write

$$
K^{\mathrm{m}} \leq \min_C \sum_{\mathcal{W}_{\eta,d} \in \tilde{C}} E_R^2(W_{\eta,d}) \leq \min_C \sum_{\mathcal{W}_{\eta,d} \in \tilde{C}} E_R(W_{\eta,d}),
\tag{67}
$$

where E_R is in Eq. (17), and E_R^2 in Eq. (29). The first bound in Eq. (67) is certainly tighter than the second one if the channels have $\eta < -2/d$. More generally, we write

$$
K^{\mathrm{m}} \leq \min_E \min_C \sum_{\mathcal{W}_{\eta,d} \in \tilde{C}} E(W_{\eta,d}),
\tag{68}
$$

where E is minimized in the computable set $\{E_R^2 \leq E_R, \tilde{E}_{sq}, E_{sq}^*\}$. Finally, we may write

$$
Q_2^{\mathrm{m}} \leq \min_C \sum_{\mathcal{W}_{\eta,d} \in \tilde{C}} E_P^\infty(W_{\eta,d}) \leq \min_C \sum_{\mathcal{W}_{\eta,d} \in \tilde{C}} E_P(W_{\eta,d}),
\tag{69}
$$

where E_P is in Eq. (17) and E_P^∞ in Eq. (18). The first bound in Eq. (69) is computable from the regularised RPPT in Eq. (18) and is certainly strictly tigther than the second bound if the channels have $\eta < -2/d$.

VII. CONCLUSIONS

In this work we have considered quantum and private communication over the class of (teleportation-covariant) Holevo-Werner channels. We have computed suitable upper bounds for their two-way assisted capacities in terms of relative entropy distances, i.e., the relative entropy of entanglement (REE) and its variant with respect to PPT states (RPPT), and also in terms of the squashed entanglement (using the identity isometry and then the convexity property).

We have shown that there is a general competing behaviour between these bounds, so that an optimization over the entanglement measure is in order. These calculations were done not only for point-to-point communication, but also for chains of quantum repeaters and, more generally, quantum networks under different types of routings.

In all cases, we have also pointed out the subadditivity behaviour of the REE and RPPT bounds, so that their two-copy and regularised versions perform strictly better than their simpler one-copy expressions, under suitable conditions of the parameters. From this point of view, our paper clearly shows how the subadditivity properties of the Werner states can be fully mapped to the corresponding Holevo-Werner channels in configurations of adaptive quantum and private communication.

Appendix A: Proof of the RPPT bound in Lemma 1 at any dimension

1. Discrete-variable channels

To get the result for finite dimension, we may apply an heuristic argument of reduction into entanglement distillation [30] (suitably extended from Pauli channels to teleportation-covariant channels). This gives $Q_2(\mathcal{E}) = D_2(\chi_\mathcal{E})$, where the latter is the two-way distillability of the Choi matrix $\chi_\mathcal{E}$. Then, we may use the fact that $D_2(\chi_\mathcal{E}) \leq E_P^\infty(\chi_\mathcal{E})$ [2, Sec. 8.10], therefore deriving the bound in Eq. (40) for discrete variable channels.

This bound can be proven more rigorously (and also extended to bosonic channels), by resorting to teleportation stretching [44], where the n-use output of a quantum protocol ρ^n is directly expressed in terms of the resource states $(\chi_\mathcal{E}^{\otimes n})$ via a single but complicated trace-preserving LOCC Λ, i.e.,

$$\rho^n = \Lambda\left(\chi_\mathcal{E}^{\otimes n}\right). \tag{A1}$$

Recall that, for any channel $\mathcal{E}$, we may consider an adaptive entanglement-distillation protocol $\mathcal{P}$ such that, after n uses, Alice and Bob share an output state ρ^n satisfying the trace-distance condition $||\rho^n - \Phi_2^{\otimes nR_n}||_1 \leq \varepsilon$, where $\Phi_2^{\otimes nR_n}$ are nR_n ebits. By taking the limit in n and optimizing over $\mathcal{P}$, we write

$$Q_2(\mathcal{E}) = D_2(\mathcal{E}) = \sup_\mathcal{P} \lim_{n\to\infty} R_n. \tag{A2}$$

Then recall the asymptotic continuity: For any pair of finite-dimensional bipartite states, ρ and σ, such that $||\rho - \sigma||_1 \leq \varepsilon$, we may write $|E_P(\rho) - E_P(\sigma)| \leq f(\varepsilon, d)$, where [62, 63, 76]

$$f(\varepsilon, d) := \frac{\varepsilon}{2}\log_2 d + \left(1 + \frac{\varepsilon}{2}\right) H_2\left(\frac{\varepsilon}{2+\varepsilon}\right), \tag{A3}$$

with H_2 being the binary Shannon entropy [19] and d the smaller of the two subsystems' dimensions. For any finite d, this function f disappears as $\varepsilon \to 0$. Using this property and the normalization [64] $E_P(\Phi_2^{\otimes nR_n}) \geq nR_n$, we may write

$$nR_n \leq E_P(\Phi_2^{\otimes nR_n}) \leq E_P(\rho^n) + f(\varepsilon, d^{nR_n}). \tag{A4}$$

Next step is to apply teleportation stretching to reduce the output state ρ^n. For an adaptive protocol over a finite-dimensional teleportation-covariant channel, we may write Eq. (A1) where $\chi_\mathcal{E}$ is the channel's Choi matrix and Λ is a trace-preserving LOCC [44]. Because the RPPT is monotonic under PPT operations, it is so under the more restrictive LOCCs as Λ. Therefore, we may write $E_P(\rho^n) \leq E_P(\chi_\mathcal{E}^{\otimes n})$ and Eq. (A4) becomes

$$nR_n \leq E_P\left(\chi_\mathcal{E}^{\otimes n}\right) + f(\varepsilon, d^{nR_n}) \tag{A5}$$

$$= E_P\left(\chi_\mathcal{E}^{\otimes n}\right) + \frac{\varepsilon nR_n}{2}\log_2 d$$

$$+ \left(1 + \frac{\varepsilon}{2}\right) H_2\left(\frac{\varepsilon}{2+\varepsilon}\right). \tag{A6}$$

By re-organizing the terms in the previous inequality, we may write

$$R_n \leq \frac{E_P\left(\chi_\mathcal{E}^{\otimes n}\right) + \left(1 + \frac{\varepsilon}{2}\right) H_2\left(\frac{\varepsilon}{2+\varepsilon}\right)}{n\left(1 - \frac{\varepsilon}{2}\log_2 d\right)}. \tag{A7}$$

Taking the limit in n, we therefore get

$$\lim_{n\to\infty} R_n \leq \frac{E_P^\infty(\chi_\mathcal{E})}{1 - \frac{\varepsilon}{2}\log_2 d}. \tag{A8}$$

For $\varepsilon \to 0$ (weak converse), we obtain $\lim_{n\to\infty} R_n \leq E_P^\infty(\chi_\mathcal{E})$ and the optimization over the protocols $\mathcal{P}$ automatically leads to the upper bound $Q_2(\mathcal{E}) \leq E_P^\infty(\chi_\mathcal{E})$ as promised in Eq. (40).

2. Continuous-variable channels

Thanks to the latter derivation, we can extend the bound to continuous-variable (bosonic) channels, for which the output state ρ^n is infinite-dimensional. Following Ref. [44], we apply a truncation LOCC $\mathbb{T}_d$ at the output of the protocol $\mathcal{P}$ so that $\rho^{n,d} = \mathbb{T}_d(\rho^n)$ is a finite dimensional state, epsilon-close to $nR_{n,d}$ ebits. We may then repeat the previous steps and modify Eq. (A4) into

$$nR_{n,d} \leq E_P(\rho^{n,d}) + f(\varepsilon, d^{nR_{n,d}}) \tag{A9}$$

$$\leq E_P(\rho^n) + f(\varepsilon, d^{nR_{n,d}}), \tag{A10}$$

where we exploit the monotonicity $E_P(\rho^{n,d}) \leq E_P(\rho^n)$ in the second inequality.

Now we use the asymptotic stretching $\rho^n = \lim_\mu \Lambda(\chi_\mathcal{E}^{\mu\otimes n})$ in terms of the quasi-Choi matrix $\chi_\mathcal{E}^\mu := \mathcal{I} \otimes \mathcal{E}(\Phi^\mu)$, with Φ^μ being a two-mode squeezed vacuum state with energy μ. More precisely, we write

$$\left\|\rho^n - \Lambda(\chi_\mathcal{E}^{\mu\otimes n})\right\| \leq n\varepsilon_{\mu,N}, \tag{A11}$$

where $\varepsilon_{\mu,N} := \|\mathcal{E} - \mathcal{E}^\mu\|_{\diamond N}$ is the channel simulation error expressed in terms of energy-constrained diamond distance between the channel $\mathcal{E}$ and its teleportation simulation $\mathcal{E}^\mu$ [44]. For any finite energy N of the input alphabet, we have the bounded-uniform convergence of the Braunstein-Kimble protocol, so that $\lim_\mu \varepsilon_{\mu,N} = 0$. As a result for any N, we have the asymptotic convergence in trace distance

$$\lim_\mu \left\|\rho^n - \Lambda(\chi_\mathcal{E}^{\mu\otimes n})\right\| = 0. \tag{A12}$$

We may therefore use the lower semi-continuity of the

relative entropy [4]. In fact, we may write

$$
\begin{aligned}
E_P(\rho^n) &= \inf_{\sigma \in \text{PPT}} S(\rho^n || \sigma) \\
&\overset{(1)}{\leq} \inf_{\sigma^\mu} S\left[\lim_\mu \Lambda(\chi_{\mathcal{E}}^{\mu \otimes n}) \,||\, \lim_\mu \sigma^\mu \right] \\
&\overset{(2)}{\leq} \inf_{\sigma^\mu} \liminf_{\mu \to +\infty} S\left[\Lambda(\chi_{\mathcal{E}}^{\mu \otimes n}) \,||\, \sigma^\mu \right] \\
&\overset{(3)}{\leq} \inf_{\sigma^\mu} \liminf_{\mu \to +\infty} S\left[\Lambda(\chi_{\mathcal{E}}^{\mu \otimes n}) \,||\, \Lambda(\sigma^\mu) \right] \\
&\overset{(4)}{\leq} \inf_{\sigma^\mu} \liminf_{\mu \to +\infty} S\left(\chi_{\mathcal{E}}^{\mu \otimes n} \,||\, \sigma^\mu \right) \\
&\overset{(5)}{=} E_P(\chi_{\mathcal{E}}^{\otimes n}), \qquad\qquad\qquad\qquad \text{(A13)}
\end{aligned}
$$

where: (1) σ^μ is a sequence of PPT states such that $\|\sigma - \sigma^\mu\| \overset{\mu}{\to} 0$ for some PPT σ; (2) we use the lower semi-continuity of the relative entropy [4]; (3) we use that $\Lambda(\sigma^\mu)$ are specific types of converging PPT sequences; (4) we use the monotonicity of the relative entropy under trace-preserving LOCCs; and (5) we use the definition of

RPPT for asymptotic states of Eq. (41).

Combining Eqs. (A10) and (A13), we then derive

$$
nR_{n,d,N} \leq E_P(\chi_{\mathcal{E}}^{\otimes n}) + f(\varepsilon, d^{nR_{n,d,N}}), \qquad \text{(A14)}
$$

for any n, d and N. We can compute the extension of Eq. (A8), which is

$$
\lim_{n \to \infty} R_{n,d,N} \leq \frac{E_P^\infty(\chi_{\mathcal{E}})}{1 - \frac{\varepsilon}{2} \log_2 d}. \qquad \text{(A15)}
$$

For $\varepsilon \to 0$ (weak converse), we obtain $\lim_{n \to \infty} R_{n,d,N} \leq E_P^\infty(\chi_{\mathcal{E}})$ and the optimization over the original protocols $\mathcal{P}$ automatically leads to the upper bound

$$
Q_2(\mathcal{E}|d, N) := \sup_{\mathcal{P}} \lim_{n \to \infty} R_{n,d,N} \leq E_P^\infty(\chi_{\mathcal{E}}) . \qquad \text{(A16)}
$$

Since the right hand side does not depend on the input energy constraint N and the output truncated dimension d, we may extend it to the supremum, i.e.,

$$
Q_2(\mathcal{E}) = \sup_{d,N} Q_2(\mathcal{E}|d, N) \leq E_P^\infty(\chi_{\mathcal{E}}). \qquad \text{(A17)}
$$

[1] M. A. Nielsen, and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).

[2] M. Hayashi, *Quantum Information: An introduction* (Springer-Verlag Berlin Heidelberg, 2006).

[3] M. Hayashi, *Quantum Information Theory: Mathematical Foundation* (Springer-Verlag Berlin Heidelberg, 2017).

[4] A. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction* (De Gruyter, Berlin-Boston, 2012).

[5] C. Weedbrook *et al.,* Rev. Mod. Phys. **84**, 621 (2012).

[6] H. J. Kimble, Nature **453**, 1023–1030 (2008).

[7] R. Van Meter, *Quantum Networking* (Wiley, 2014).

[8] S. Pirandola, and S. L. Braunstein, Nature **532**, 169–171 (2016).

[9] S. Pirandola, arXiv:1601.00966 (2016).

[10] E. Schoute, L. Mancinska, T. Islam, I. Kerenidis, and S. Wehner, arXiv:1610.05238 (2016).

[11] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, arXiv:1708.07142 (2017).

[12] F. Rozpedek, K. Goodenough, J. Ribeiro, N. Kalb, V. Caprara Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, arXiv:1705.00043 (2017).

[13] L. Rigovacca, G. Kato, S. Bäuml, M. S. Kim, W. J. Munro, K. Azuma, New J. Phys. **20**, 013033 (2018).

[14] C. H. Bennett and G. Brassard. *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, **175** (1984).

[15] A. K. Ekert, Phys. Rev. Lett. **67**, 661-663 (1991).

[16] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, Rev. Mod. Phys. **81** 1391-1350 (2009).

[17] R. Colbeck, *Quantum And Relativistic Protocols For Secure Multi-Party Computation* (University of Cambridge, 2006).

[18] C. E. Shannon, *The Mathematical Theory of Communication* (University of Illinois Press, 1949).

[19] T. M. Cover, and J. A. Thomas, *Elements of Information Theory* (Wiley, New Jersey, 2006).

[20] A. W. Harrow, A. Hassidim, D. W. Leung, and J. Watrous, Phys. Rev. A **81**, 032339 (2010).

[21] S. Pirandola, and C. Lupo, Phys. Rev. Lett. **118**, 100502 (2017).

[22] S. Pirandola, R. Laurenza, and C. Lupo, *Fundamental limits to quantum channel discrimination*, arXiv:1803.02834 (2018).

[23] K. Kravtsov *et al.*, Phys. Rev. A **87**, 062122 (2013).

[24] D. H. Mahler *et al.*, Phys. Rev. Lett. **111**, 183601 (2013).

[25] R. Demkowicz-Dobrzański, and L. Maccone, Phys. Rev. Lett. **113**, 250801 (2014).

[26] A. A. Berni *et al.,* Nature Photon. **9**, 577 (2015).

[27] Z. Hou, H. Zhu, G.-Y. Xiang, C.-F. Li, and G.-C. Guo, npj Quantum Information **2**, 16001 (2016).

[28] T. P. W. Cope, and S. Pirandola, Quantum Meas. Quantum Metrol. **4**, 44-52 (2017).

[29] R. Laurenza, C. Lupo, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Quantum Meas. Quantum Metrol. **5**, 1-12 (2018).

[30] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824-3851 (1996).

[31] M. A. Nielsen, and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).

[32] G. Brassard, S. L. Braunstein, and R. Cleve, Physica D **120**, 43–47 (1998).

[33] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **99**, 1888–1898 (1999).

[34] D. Gottesman, and I. L. Chuang, Nature **402**, 390–393

(1999).

[35] G. Bowen, and S. Bose, Phys. Rev. Lett. **87**, 267901 (2001).

[36] E. Knill, R. Laflamme, and G. Milburn, Nature **409**, 46–52 (2001).

[37] R. F. Werner, J. Phys. A **34**, 7081–7094 (2001).

[38] G. Giedke, and J. I. Cirac, Phys. Rev. A **66**, 032316 (2002).

[39] P. Aliferis, and D. W. Leung, Phys. Rev. Lett. **70**, 062314 (2004).

[40] J. Niset, J. Fiurasek, and N. J. Cerf, Phys. Rev. Lett. **102**, 120501 (2009).

[41] A. Müller-Hermes, *Transposition in quantum information theory* (Master's thesis, Technical University of Munich, 2012).

[42] M. M. Wolf, Notes on "Quantum Channels & Operations" (see page 35). Available at https://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/ Michael-Wolf/QChannelLecture.pdf.

[43] D. Leung, and W. Matthews, IEEE Trans. Info. Theory **61**, 4486-4499 (2015).

[44] S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi, Nat. Commun. **8**, 15043 (2017). See also arXiv:1510.08863 and arXiv:1512.04945 (2015).

[45] In general, a LOCC simulation of a channel is a representation of the channel $\mathcal{E}$ where it is replaced by an LOCC (or a sequence of LOCCs) applied to the input state ρ and a suitable resource state σ (which may be finite or infinite dimensional) [44]. A preliminary version of the LOCC simulation was proposed in Ref. [33]. However, because the latter does not involve sequences of LOCCs and only considers finite dimensional σ, it cannot simulate the amplitude damping channel, i.e., it cannot cover all the DV channels.

[46] V. Vedral, Rev. Mod. Phys. **74**, 197 (2002).

[47] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275-2279 (1997).

[48] V. Vedral, and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[49] K. Goodenough, D. Elkouss, and S. Wehner, New J. Phys. **18**, 063005 (2016).

[50] M. Christandl, *The Structure of Bipartite Quantum States: Insights from Group Theory and Cryptography* (PhD thesis, University of Cambridge, 2006).

[51] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, Phys. Rev. Lett. **78**, 3217-3220 (1997).

[52] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[53] S. L. Braunstein, and H. J. Kimble, Phys. Rev. Lett. **80**, 869–872 (1998).

[54] S. L. Braunstein, G. M. D'Ariano, G. J. Milburn, and M. F. Sacchi, Phys. Rev. Lett. **84**, 3486-3489 (2000).

[55] S. Pirandola *et al.*, Nat. Photon. **9**, 641-652 (2015).

[56] R. F. Werner, and A. S. Holevo, J. Mat. Phys. **43**, 4353 (2002).

[57] M. Fannes, B. Haegeman, M. Mosonyi and D. Vanpeteghem, arXiv:quant-ph/0410195 (2004).

[58] R. F. Werner, Phys. Rev. A **40**, 4277–4281 (1989).

[59] F. Barrett, Phys. Rev. A **65**, 042302 (2002).

[60] K. G. H. Vollbrecht, and R. F. Werner, Phys. Rev. A **64**, 062307 (2001).

[61] D. Z. Djokovic, Entropy **18**, 216 (2016).

[62] K. Horodecki, M. Horodecki, P. Horodecki, and J. Op-penheim, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[63] M. Donald, and M. Horodecki, Phys. Lett. A **264**, 257-260 (1999).

[64] E. Rains, Phys. Rev. A **60**, 179 (1999).

[65] E. M. Rains, IEEE Trans. Inf. Theory **47**, 2921–2933 (2001).

[66] K. Audenaert, J. Eisert, E. Jané, M. B. Plenio, S. Virmani, and B. De Moor, Phys. Rev. Lett. **87**, 217902 (2001).

[67] The proof for continuous-variable channels is more complicated and is not reported here. It is based on a suitable extension of the squashed entanglement functional to account for asymptotic states.

[68] M. Christandl, N. Schuch, and A. Winter, Communications in Mathematical Physics **311**, 397-422 (2012).

[69] For technical reasons connected with the proof of the single-path bound, we cannot consider multi-copy REE quantities or the regularisation E_R^∞ in Eq. (60).

[70] P. Slepian, *Mathematical Foundations of Network Analysis* (Springer-Verlag, New York, 1968).

[71] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin, *Network Flows: Theory, Algorithms and Applications* (Prentice Hall, 1993).

[72] A. S. Tanenbaum, and D. J. Wetherall, *Computer Networks* (5th Edition, Pearson, 2010).

[73] T. E. Harris, and F. S. Ross, Research Memorandum, Rand Corporation (1955).

[74] L. R. Ford, and D. R. Fulkerson, Canadian Journal of Mathematics **8**, 399 (1956).

[75] P. Elias, A. Feinstein, and C. E. Shannon, IRE Trans. Inf. Theory **2**, 117–119 (1956).

[76] A. Winter, Commun. Math. Phys **347**, 291-313 (2016).