

Supplementary Information for “Fundamental limits to quantum channel discrimination”

Stefano Pirandola,^{1,2} Riccardo Laurenza,³ Cosmo Lupo,⁴ and Jason Pereira²

¹*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

²*Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK*

³*QSTAR, INO-CNR and LENS, Largo Enrico Fermi 2, 50125 Firenze, Italy*

⁴*Department of Physics and Astronomy, University of Sheffield, Sheffield S3 7RH, UK*

I. DEPOLARIZING PROBABILITY FOR QUBIT PBT

Here we show the formula for the PBT numbers ξ_M given in Eq. (11) of the main text. Define the states

$$|\phi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}, \quad (1)$$

$$\sigma^i = \frac{1}{2^{M-1}} |\phi^-\rangle \langle \phi^-|_{A_i C} \otimes \mathbb{I}_{\mathbf{A}}^{M-1}, \quad (2)$$

$$\rho = \sum_{i=1}^M \sigma^i, \quad (3)$$

where $\mathbb{I}_{\mathbf{A}}^{M-1}$ is the 2^{M-1} -dimensional identity operator acting on the $M-1$ qubits $\mathbf{A} = \mathbf{A} \setminus A_i$ (similarly, we denote $\mathbf{B} = \mathbf{B} \setminus B_i$). Then, in qubit-based PBT with M ports, one uses a POVM with operators

$$\Pi_{C\mathbf{A}}^i = \rho^{-\frac{1}{2}} \sigma^i \rho^{-\frac{1}{2}} + M^{-1} (\mathbb{I}^{M+1} - \rho^{-\frac{1}{2}} \rho \rho^{-\frac{1}{2}}), \quad (4)$$

where $\mathbb{I}^{M+1}$ is the 2^{M+1} -dimensional identity operator acting on the input qubit C and Alice's resource qubits $\mathbf{A}$, while $\rho^{-\frac{1}{2}}$ is taken over the support of ρ [1].

Since the resource state

$$\Phi_{\mathbf{AB}}^{\otimes M} = \bigotimes_{i=1}^M |\phi^-\rangle_i \langle \phi^-| \quad (5)$$

is symmetric under exchange of labels, we can calculate ξ_M assuming that the qubit is teleported to the first port, and hence we only need to consider $\Pi_{C\mathbf{A}}^1$. The PBT channel Γ_M from qubit C to qubit B_1 is a depolarizing channel with isotropic Choi matrix

$$(\rho_{\Gamma_M})_{DB_1} = \begin{pmatrix} \frac{1}{2} - \frac{\xi_M}{4} & 0 & 0 & \frac{1}{2} - \frac{\xi_M}{2} \\ 0 & \frac{\xi_M}{4} & 0 & 0 \\ 0 & 0 & \frac{\xi_M}{4} & 0 \\ \frac{1}{2} - \frac{\xi_M}{2} & 0 & 0 & \frac{1}{2} - \frac{\xi_M}{4} \end{pmatrix}, \quad (6)$$

where ξ_M is the probability of depolarizing and D is the ancillary system not passing through the PBT channel. Note that we can equivalently use a POVM $\{\Pi_{C\mathbf{A}}^i\}$ and a resource state $\Phi_{\mathbf{AB}}^{\otimes M}$ where we replace

$$|\phi^-\rangle \rightarrow |\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}. \quad (7)$$

In order to find ξ_M , it suffices to find any one of the non-zero elements in the output Choi matrix. Selecting

the coefficient of $|01\rangle_{DB_1} \langle 01|$, our expression is

$$\frac{\xi_M}{4M} = \langle 01 | \text{Tr}_{\mathbf{A}\bar{\mathbf{B}}C} [\sqrt{\Pi^1} \Phi_{\mathbf{AB}}^{\otimes M} |\Phi\rangle_{CD} \langle \Phi | \sqrt{\Pi^1}] | 01 \rangle \quad (8)$$

$$= \text{Tr} [\Pi_{C\mathbf{A}}^1 \Phi_{\mathbf{AB}}^{\otimes M} |\Phi\rangle_{CD} \langle \Phi | |01\rangle_{DB_1} \langle 01|] \quad (9)$$

$$= \frac{1}{2} \text{Tr} [\Pi_{C\mathbf{A}}^1 (1|_{B_1} \text{Tr}_{\mathbf{B}} (\Phi_{\mathbf{AB}}^{\otimes M}) |1\rangle_{B_1} \otimes |0\rangle_C \langle 0|)], \quad (10)$$

where the factor of M comes from the fact we have M possible outcomes and where the third line is due to $|\Phi\rangle_{CD}$. Considering the structure of $\Phi_{\mathbf{AB}}^{\otimes M}$, we can write

$$\xi_M = \frac{M}{2^{M-1}} \text{Tr} [\Pi_{C\mathbf{A}}^1 (\mathbb{I}_{\mathbf{A}}^{M-1} \otimes |00\rangle_{A_1 C} \langle 00|)]. \quad (11)$$

Ref. [1] showed that, by using a spinorial basis, the eigenvectors and eigenvalues of ρ can be expressed in a simple form. Defining the basis vectors $\{|\Phi^M(j, m, \alpha)\rangle\}$, where j is the total spin, m is the spin component in the z -basis and α is a degeneracy value, they constructed the eigenvectors of ρ as

$$\begin{aligned} |\Psi(\lambda_j^\mp, m, \alpha)\rangle = & \quad (12) \\ & |\Phi^M(j, m + \frac{1}{2}, \alpha)\rangle_{\mathbf{A}} |0\rangle_C \left\langle j, m + \frac{1}{2}, \frac{1}{2}, -\frac{1}{2} \middle| j \pm \frac{1}{2}, m \right\rangle \\ & + |\Phi^M(j, m - \frac{1}{2}, \alpha)\rangle_{\mathbf{A}} |1\rangle_C \left\langle j, m - \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \middle| j \pm \frac{1}{2}, m \right\rangle, \end{aligned}$$

where the terms in the large, triangular brackets are the Clebsch-Gordan coefficients. They found that these eigenvectors correspond to the eigenvalues

$$\lambda_j^- = \frac{1}{2} \left(\frac{M}{2} - j \right), \quad \lambda_j^+ = \frac{1}{2} \left(\frac{M}{2} + j + 1 \right). \quad (13)$$

(Our expressions differ from those in Ref. [1] by a factor of 2^{M+1} due to including this factor in the definition of the σ^i). Then, Ref. [1] expressed the state ρ as

$$\begin{aligned} \rho = & \sum_{s, m, \alpha} \lambda_j^- |\Psi(\lambda_{s-\frac{1}{2}}^-, m, \alpha)\rangle \langle \Psi(\lambda_{s-\frac{1}{2}}^-, m, \alpha)| \\ & + \lambda_j^+ |\Psi(\lambda_{s+\frac{1}{2}}^+, m, \alpha)\rangle \langle \Psi(\lambda_{s+\frac{1}{2}}^+, m, \alpha)|. \end{aligned} \quad (14)$$

Note that the basis vectors on an M -spin system, $\{|\Phi^M(j, m, \alpha)\rangle\}$, can be divided into two types based on how they are constructed from the basis vectors on an

$(M-1)$ -spin system, $\{|\Phi^{M-1}(j, m, \alpha)\rangle\}$. Specifically

$$\begin{aligned} |\Phi_I^M(j, m)\rangle = & \quad (15) \\ & |\Phi^{M-1}(j + \frac{1}{2}, m + \frac{1}{2})\rangle|0\rangle \left\langle j + \frac{1}{2}, m + \frac{1}{2}, \frac{1}{2}, -\frac{1}{2} \middle| j, m \right\rangle \\ & + |\Phi^{M-1}(j + \frac{1}{2}, m - \frac{1}{2})\rangle|1\rangle \left\langle j + \frac{1}{2}, m - \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \middle| j, m \right\rangle, \end{aligned}$$

and

$$\begin{aligned} |\Phi_{II}^M(j, m)\rangle = & \quad (16) \\ & |\Phi^{M-1}(j - \frac{1}{2}, m + \frac{1}{2})\rangle|0\rangle \left\langle j - \frac{1}{2}, m + \frac{1}{2}, \frac{1}{2}, -\frac{1}{2} \middle| j, m \right\rangle \\ & + |\Phi^{M-1}(j - \frac{1}{2}, m - \frac{1}{2})\rangle|1\rangle \left\langle j - \frac{1}{2}, m - \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \middle| j, m \right\rangle, \end{aligned}$$

where we have omitted the label α , but both component vectors are assumed to have the same degeneracy value. We also divide the eigenvectors $\{|\Psi(\lambda_j^\mp, m, \alpha)\rangle\}$ into types I and II , based on whether they are constructed from the vectors $\{|\Phi_I^M(j, m, \alpha)\rangle\}$ or $\{|\Phi_{II}^M(j, m, \alpha)\rangle\}$. Ref. [1] also used the explicit forms of the Clebsch-Gordon coefficients to calculate the expressions

$$\begin{aligned} \langle \phi^- |_{A_1 C} |\Psi_I(\lambda_s^- - \frac{1}{2}, m, \alpha)\rangle_{\mathbf{A}C} = & \\ \sqrt{\frac{s}{2s+1}} |\Phi^{M-1}(s, m, \alpha)\rangle_{\bar{\mathbf{A}}} & \quad (17) \end{aligned}$$

$$\langle \phi^- |_{A_1 C} |\Psi_I(\lambda_s^+ + \frac{1}{2}, m, \alpha)\rangle_{\mathbf{A}C} = 0, \quad (18)$$

$$\langle \phi^- |_{A_1 C} |\Psi_{II}(\lambda_s^- - \frac{1}{2}, m, \alpha)\rangle_{\mathbf{A}C} = 0, \quad (19)$$

$$\begin{aligned} \langle \phi^- |_{A_1 C} |\Psi_{II}(\lambda_s^+ + \frac{1}{2}, m, \alpha)\rangle_{\mathbf{A}C} = & \\ -\sqrt{\frac{s+1}{2s+1}} |\Phi^{M-1}(s, m, \alpha)\rangle_{\bar{\mathbf{A}}}. & \quad (20) \end{aligned}$$

We can express σ^1 as

$$\begin{aligned} \sigma^1 = |\phi^- \rangle_{A_1 C} \langle \phi^- | \otimes & \\ \sum_{j=j_{min}}^{\frac{M-1}{2}} \sum_{m=-j}^j \sum_{\alpha} |\Phi^{M-1}(j, m, \alpha)\rangle_{\bar{\mathbf{A}}} \langle \Phi^{M-1}(j, m, \alpha)| & \quad (21) \end{aligned}$$

where the term over the $\bar{\mathbf{A}}$ qubits is the identity. We now separate out the contributions from the two terms of Π^1 , writing

$$\Pi^1 = \pi_0 + \pi_1, \quad (22)$$

$$\pi_0 = M^{-1} \left(\mathbb{I}^{M+1} - \rho^{-\frac{1}{2}} \rho \rho^{-\frac{1}{2}} \right), \quad (23)$$

$$\pi_1 = \rho^{-\frac{1}{2}} \sigma^1 \rho^{-\frac{1}{2}}. \quad (24)$$

Here π_0 is simply M^{-1} times the identity over the vector space that does not lie in the support of ρ , and corresponds to those eigenvectors of ρ with eigenvalue 0,

namely $\{|\Psi_{II}(\lambda_{\frac{M}{2}}^-, m)\rangle\}$ (omitting the label α , since the degeneracy is 1 for this choice of j). Consequently, we may write

$$\pi_0 = M^{-1} \sum_{m=-\frac{M+1}{2}}^{\frac{M+1}{2}} |\Psi_{II}(\lambda_{\frac{M}{2}}^-, m)\rangle \langle \Psi_{II}(\lambda_{\frac{M}{2}}^-, m)|. \quad (25)$$

Combining the expressions for ρ and σ^1 in Eqs. (14) and (21) and the expressions in Eqs. (17)-(20), we can write

$$\begin{aligned} \pi_1 = & \sum_{s=s_{min}}^{(M-1)/2} \sum_{m=-s}^s \sum_{\alpha} \quad (26) \\ & \left[(\lambda_{s-\frac{1}{2}}^-)^{-1} \frac{s}{2s+1} |\Psi_I(\lambda_{s-\frac{1}{2}}^-, m, \alpha)\rangle \langle \Psi_I(\lambda_{s-\frac{1}{2}}^-, m, \alpha)| \right. \\ & - (\lambda_{s-\frac{1}{2}}^- \lambda_{s+\frac{1}{2}}^+)^{-\frac{1}{2}} \frac{\sqrt{s(s+1)}}{2s+1} \\ & \left(|\Psi_I(\lambda_{s-\frac{1}{2}}^-, m, \alpha)\rangle \langle \Psi_{II}(\lambda_{s+\frac{1}{2}}^+, m, \alpha)| + \right. \\ & \left. |\Psi_{II}(\lambda_{s+\frac{1}{2}}^+, m, \alpha)\rangle \langle \Psi_I(\lambda_{s-\frac{1}{2}}^-, m, \alpha)| \right) + \\ & \left. (\lambda_{s+\frac{1}{2}}^+)^{-1} \frac{s+1}{2s+1} |\Psi_{II}(\lambda_{s+\frac{1}{2}}^+, m, \alpha)\rangle \langle \Psi_{II}(\lambda_{s+\frac{1}{2}}^+, m, \alpha)| \right], \end{aligned}$$

where $s_{min} = 1/2$ for even M , and 0 for odd M .

By calculating the Clebsch-Gordon coefficients, we find

$$\begin{aligned} \langle \Psi_I(\lambda_{s-\frac{1}{2}}^-, m) | (\mathbb{I}^{M-1} \otimes |00\rangle \langle 00|) | \Psi_I(\lambda_{s-\frac{1}{2}}^-, m) \rangle = & \\ \frac{(s-m)(s+m+1)}{2s(2s+1)}, & \quad (27) \end{aligned}$$

$$\begin{aligned} \langle \Psi_{II}(\lambda_{s+\frac{1}{2}}^+, m) | (\mathbb{I}^{M-1} \otimes |00\rangle \langle 00|) | \Psi_{II}(\lambda_{s+\frac{1}{2}}^+, m) \rangle = & \\ \frac{(s-m)(s+m+1)}{2(s+1)(2s+1)}, & \quad (28) \end{aligned}$$

$$\begin{aligned} \langle \Psi_I(\lambda_{s-\frac{1}{2}}^-, m) | (\mathbb{I}^{M-1} \otimes |00\rangle \langle 00|) | \Psi_{II}(\lambda_{s+\frac{1}{2}}^+, m) \rangle = & \\ \frac{(s-m)(s+m+1)}{2(2s+1)\sqrt{s(s+1)}}, & \quad (29) \end{aligned}$$

$$\begin{aligned} \langle \Psi_{II}(\lambda_{\frac{M}{2}}^-, m) | (\mathbb{I}^{M-1} \otimes |00\rangle \langle 00|) | \Psi_{II}(\lambda_{\frac{M}{2}}^-, m) \rangle = & \\ \frac{M-1-2m}{2M} \left(\frac{1}{2} - \frac{m}{M+1} \right). & \quad (30) \end{aligned}$$

Using Eq. (30) and summing over m , we find

$$\frac{M}{2^{M-1}} \text{Tr} [\pi_0 (\mathbb{I}_{\bar{\mathbf{A}}}^{M-1} \otimes |01\rangle_{A_1 C} \langle 01|)] = \frac{1}{3} \frac{M+2}{2^{M-1}}. \quad (31)$$

Using Eqs. (27)-(29), we find

$$\begin{aligned} \frac{M}{2^{M-1}} \text{Tr} [\pi_1 (\mathbb{I}_{\bar{\mathbf{A}}}^{M-1} \otimes |01\rangle_{A_1 C} \langle 01|)] = & \\ \frac{M}{2^{M-1}} \sum_{s=s_{min}}^{(M-1)/2} \sum_{m=-s}^s \sum_{\alpha} \frac{(s-m)(s+m+1)}{2(2s+1)^2} & \\ \times \left[(\lambda_{s-\frac{1}{2}}^-)^{-1} - 2(\lambda_{s-\frac{1}{2}}^- \lambda_{s+\frac{1}{2}}^+)^{-\frac{1}{2}} + (\lambda_{s+\frac{1}{2}}^+)^{-1} \right]. & \quad (32) \end{aligned}$$

We can simplify the term on the RHS, using

$$\begin{aligned} & \left[(\lambda_{s-\frac{1}{2}}^-)^{-1} - 2(\lambda_{s-\frac{1}{2}}^- \lambda_{s+\frac{1}{2}}^+)^{-\frac{1}{2}} + (\lambda_{s+\frac{1}{2}}^+)^{-1} \right] \\ &= \left[(\lambda_{s-\frac{1}{2}}^-)^{-\frac{1}{2}} - (\lambda_{s+\frac{1}{2}}^+)^{-\frac{1}{2}} \right]^2. \end{aligned} \quad (33)$$

The degeneracy $g[s]$ for a given s -value is given by

$$g[s] = \frac{(2s+1)(M-1)!}{\left(\frac{M-1}{2} - s\right)! \left(\frac{M+1}{2} + s\right)!}, \quad (34)$$

and substituting this into Eq. (32), we get

$$\begin{aligned} & \frac{M}{2^{M-1}} \text{Tr} \left[\pi_1 \left(\mathbb{I}_{\mathbf{A}}^{M-1} \otimes |01\rangle_{A_1 C} \langle 01| \right) \right] = \\ & \sum_{s=s_{\min}}^{(M-1)/2} \sum_{m=-s}^s \frac{(s-m)(s+m+1)}{2^M (2s+1)} \binom{M}{\frac{M-1}{2} - s} \\ & \times 8 \frac{(M+2) - \sqrt{(M+2)^2 - (2s+1)^2}}{(M+2)^2 - (2s+1)^2}, \end{aligned} \quad (35)$$

where we have substituted in the expressions from Eq. (13). Summing over m , we get

$$\begin{aligned} & \frac{M}{2^{M-1}} \text{Tr} \left[\pi_1 \left(\mathbb{I}_{\mathbf{A}}^{M-1} \otimes |01\rangle_{A_1 C} \langle 01| \right) \right] = \\ & \sum_{s=s_{\min}}^{(M-1)/2} \frac{1}{3} \frac{s(s+1)}{2^{M-4}} \binom{M}{\frac{M-1}{2} - s} \\ & \times \frac{(M+2) - \sqrt{(M+2)^2 - (2s+1)^2}}{(M+2)^2 - (2s+1)^2}. \end{aligned} \quad (36)$$

Therefore, by combining Eqs. (31) and (36), we finally get the expression of ξ_M given in Eq. (11) of the main text. We can numerically verify that ξ_M scales as M^{-1} for large M .

One may check that Eq. (11) of the main text can equivalently be obtained by combining Eq. (47) of our Methods section (i.e., Eq. (8) of our Lemma 1) together with the expression of the entanglement fidelity for qubit-based PBT which is given in Eq. (29) of Ref. [1]. The algebraic check is tedious and not reported here.

II. ULTIMATE SINGLE-PHOTON QUANTUM OPTICAL RESOLUTION

Consider the problem of discriminating between the following situations:

- (1) A point-like source emitting light from position $x = s/2$;
- (2) A point-like source emitting light from the shifted position $x = -s/2$.

The discrimination is achieved by measuring the image created by a focusing optical system. More precisely, we consider a linear imaging system in the paraxial approximation that is used to image point-like sources. This is characterized by the Fresnel number

$$\mathcal{F} = \frac{\ell}{x_R}, \quad (37)$$

where ℓ is the size of the object, and

$$x_R = \frac{\lambda}{N_A} \quad (38)$$

is the Rayleigh length. Here λ is the wavelength and $N_A = R/D$ is the numerical aperture, where R is the radius of the pupil and D is the distance from the object. In the far-field regime, light is attenuated by a loss parameter $\eta \simeq \mathcal{F}$ [2–4]. In particular, because we consider point-like sources, we are in the regime $\eta \ll 1$.

First we need to model the imaging system as a quantum channel acting on the *input* state represented by the light emitted by the source. The two cases are described by the following Heisenberg-picture transformations on the input annihilation operator a

$$(1) : a \rightarrow \sqrt{\eta} b_1 + \sqrt{1-\eta} v_1, \quad (39)$$

$$(2) : a \rightarrow \sqrt{\eta} b_2 + \sqrt{1-\eta} v_2, \quad (40)$$

where $b_{1,2}$ are the output operators (encoding the position of the source) and $v_{1,2}$ are associated with a vacuum environment. The modes b_1, b_2 are defined on the image plane and have the form

$$b_j = \int dx \psi_j(x) a(x), \quad (41)$$

where $a(x), a(x)^\dagger$ is a continuous family of canonical operators $[a(x), a(y)^\dagger] = \delta(x-y)$ defined on the image plane (for simplicity, we assume unit magnification factor). In general the image modes b_1, b_2 do satisfy the (non-canonical) commutation relations

$$[b_1, b_2^\dagger] = \int dx \psi_1(x) \psi_2^*(x), \quad (42)$$

where ψ_j is the point-spread function associated to the source being in position j . Then, by setting $\delta = \text{Re} \int dx \psi_1(x) \psi_2^*(x)$, we can define the effective image operators

$$b_\pm := (b_1 \pm b_2) / \sqrt{2(1 \pm \delta)}. \quad (43)$$

The fact that $\delta \neq 0$ means that the two image fields overlap and the sources cannot be perfectly distinguished. This is a manifestation of diffraction through the finite objective of the optical imaging system.

As a result, we can write the action of the channels as

$$(1) : a \rightarrow \sqrt{\eta_+} b_+ + \sqrt{\eta_-} b_- + \sqrt{1-\eta} v_1, \quad (44)$$

$$(2) : a \rightarrow \sqrt{\eta_+} b_+ - \sqrt{\eta_-} b_- + \sqrt{1-\eta} v_2, \quad (45)$$

where $\eta_{\pm} := (1 \pm \delta)\eta/2$. For simplicity, consider a single-photon state at the input. We then have

$$(1) : |1\rangle \rightarrow \eta|\psi_+\rangle\langle\psi_+| + (1-\eta)|0\rangle\langle 0|, \quad (46)$$

$$(2) : |1\rangle \rightarrow \eta|\psi_-\rangle\langle\psi_-| + (1-\eta)|0\rangle\langle 0|, \quad (47)$$

where

$$|\psi_{\pm}\rangle = \frac{\sqrt{\eta_+}|1\rangle_+ - \sqrt{\eta_-}|1\rangle_-}{\sqrt{\eta}}. \quad (48)$$

More generally, the action of the channels on a generic pure input state is given by

$$(1) : \alpha|0\rangle + \beta|1\rangle \rightarrow (|\alpha|^2 + \eta|\beta|^2) \times \quad (49)$$

$$|\psi_+(\alpha, \beta)\rangle\langle\psi_+(\alpha, \beta)| + (1-\eta)|\beta|^2|0\rangle\langle 0|,$$

$$(2) : \alpha|0\rangle + \beta|1\rangle \rightarrow (|\alpha|^2 + \eta|\beta|^2) \times \quad (50)$$

$$|\psi_-(\alpha, \beta)\rangle\langle\psi_-(\alpha, \beta)| + (1-\eta)|\beta|^2|0\rangle\langle 0|,$$

where

$$|\psi_{\pm}(\alpha, \beta)\rangle = \frac{\alpha|0\rangle + \beta\sqrt{\eta_+}|1\rangle_+ \pm \beta\sqrt{\eta_-}|1\rangle_-}{\sqrt{|\alpha|^2 + \eta|\beta|^2}}. \quad (51)$$

As we can see from Eqs. (49) and (50), if we apply a Pauli operator X [5] to the input state $\alpha|0\rangle + \beta|1\rangle$, we have a swap between α and β . This leads to an output state with a different eigenspectrum, so that it cannot be obtained by applying a unitary. This means that the quantum channels are *not* teleportation-covariant.

By limiting ourselves to the space of either no photon or one photon $\mathcal{H}_2 = \text{span}\{|0\rangle, |1\rangle\}$, the the input space of the channels is a qubit, and their output is a qutrit, so that the dimension of the input Hilbert space is $d = 2$. Apart from restricting the input space to qubits, we assume the most general adaptive strategy allowed by quantum mechanics, so that the quantum state of the source may be optimized as a consequence of the output (as generally happens in the adaptive protocol discussed in the main text). In order to compute the ultimate performance, we need to compute the quantum fidelity between the Choi matrices of the two channels in Eqs. (44) and (45) suitably truncated to $\mathcal{H}_2$.

Consider then the maximally entangled state $|\Phi_2\rangle = (|0\rangle|1\rangle + |1\rangle|0\rangle)/\sqrt{2}$. The Choi matrices associated with the two truncated channels are equal to

$$\rho_{(1)} = \frac{1+\eta}{2}|\Psi_+\rangle\langle\Psi_+| + \frac{1-\eta}{2}|0\rangle\langle 0|, \quad (52)$$

$$\rho_{(2)} = \frac{1+\eta}{2}|\Psi_-\rangle\langle\Psi_-| + \frac{1-\eta}{2}|0\rangle\langle 0|, \quad (53)$$

where

$$|\Psi_{\pm}\rangle = \frac{|0\rangle|1\rangle + \sqrt{\eta_+}|1\rangle_+|0\rangle \pm \sqrt{\eta_-}|1\rangle_-|0\rangle}{\sqrt{1+\eta}}. \quad (54)$$

Notice that $\langle\Psi_+|\Psi_-\rangle = (1+\delta\eta)/(1+\eta)$ where $\delta\eta := \eta_+ - \eta_-$. Therefore we obtain the fidelity

$$\begin{aligned} F(\rho_{(1)}, \rho_{(2)}) &= \text{Tr} \sqrt{\sqrt{\rho_{(1)}} \rho_{(2)} \sqrt{\rho_{(1)}}} \\ &= \frac{1+\eta}{2} \left| \frac{1+\delta\eta}{1+\eta} \right| + \frac{1-\eta}{2} = \frac{1-\eta + |1+\delta\eta|}{2}. \end{aligned} \quad (55)$$

Assuming that δ is real, this becomes

$$F[\rho_{(1)}, \rho_{(2)}] = 1 - \frac{\eta(1-\delta)}{2}, \quad (56)$$

which allows us to identify $\epsilon = \eta(1-\delta)/2$. A common way to model diffraction is to consider a Gaussian point-spread function, i.e.

$$\psi_j(s) \simeq e^{-(x-x_j)^2/4}, \quad (57)$$

where x_j is the center of the j th emitter, and the variance of the Gaussian is 1 in units of Rayleigh length. Under this Gaussian model one obtains [6, 7]

$$\delta \simeq e^{-s^2/8}, \quad (58)$$

where s is the separation in unit of wavelength. Therefore

$$\epsilon \simeq \frac{\eta(1-e^{-s^2/8})}{2} \simeq \frac{\eta s^2}{16}. \quad (59)$$

By replacing this quantity in Eq. (27) of the main text with $d = 2$ we obtain the lower bound

$$B \gtrsim \frac{1}{4} \exp(-2ns\sqrt{\eta}). \quad (60)$$

III. ULTIMATE LIMIT OF ADAPTIVE QUANTUM ILLUMINATION

A. Standard (non-adaptive) protocol

In quantum illumination [8–11], we aim at determining whether a low-reflectivity object is present or not in a region with thermal noise. We therefore prepare a signal system s and an idler system i in a joint entangled state ρ_{si} . The signal system is sent to probe the target while the idler system is retained for its measurement together with the potential signal reflection from the target. If the object is absent, the “reflected” system is just thermal background noise. If the object is present, then this is composed of the actual reflection of the signal from the target plus thermal background noise. This object can be modelled by a beam splitter, with very small transmissivity $\eta \ll 1$, which combines the each incoming optical mode (signal system) with a thermal mode with b mean number of photons.

In the discrete-variable version of quantum illumination [8], the signal system is prepared in an ensemble of d optical modes, with 1 photon in one of the modes and vacuum in the others. This is the number of modes which are distinguished by the detector in each detection process. If we introduce the following d -dimensional com-

putational basis

$$|1\rangle := \overbrace{|00\dots 01\rangle}^d, \quad (61)$$

$$|2\rangle := |00\dots 10\rangle, \quad (62)$$

$\vdots$

$$|d-1\rangle := |01\dots 00\rangle, \quad (63)$$

$$|d\rangle := |10\dots 00\rangle, \quad (64)$$

then the entangled signal-idler state can be written as

$$\psi_{si} = |\psi\rangle_{si} \langle\psi|, \quad |\psi\rangle_{si} = d^{-1/2} \sum_{k=1}^d |kk\rangle_{si}. \quad (65)$$

Let us define the d -dimensional identity operator $\mathbb{I}^d := \sum_{k=1}^d |k\rangle \langle k|$ which projects onto the subspace spanned by the 1-photon states, and the $(d+1)$ -dimensional identity operator $\mathbb{I}^{d+1} := \sum_{k=0}^d |k\rangle \langle k|$ which also includes the vacuum state $|0\rangle := |00\dots 00\rangle$. Then, we have the reduced idler state

$$\psi_i := \text{Tr}_s(\psi_{si}) = d^{-1} \mathbb{I}_i^d, \quad (66)$$

and we define the thermal state of the environment as [8]

$$\rho^{\text{th}}(b) := (1 - db)|0\rangle \langle 0| + b\mathbb{I}^d, \quad (67)$$

where b is the mean number of thermal photons per mode. Here $b \ll 1$ and $db \ll 1$, where db is the mean number of thermal photons in each detection event.

The output $(d+1) \times d$ state of the reflected signal and retained idler is given by

$$\begin{aligned} \text{Target absent: } \sigma &= \rho^{\text{th}}(b) \otimes d^{-1} \mathbb{I}_i^d, \\ \text{Target present: } \rho &= (1 - \eta)\sigma + \eta\psi_{si}. \end{aligned} \quad (68)$$

If the target is probed n times, then we may use the QCB to bound Q the error probability p_{err} in the discrimination of ρ and σ . In the regime of signal-to-noise-ratio $\eta d/b \lesssim 1$, one finds [8]

$$Q = 1 - \frac{\eta^2 d}{8b} + \mathcal{O}(b^2, \eta b), \quad (69)$$

which tightens the QCB by a factor d with respect to the unentangled case where $Q \approx 1 - \eta^2/(8b)$. From Eq. (69), we may write the following bound for the error probability of target detection after n probings [8]

$$p_n(\sigma \neq \rho) \leq \frac{1}{2} \exp\left(-\frac{\eta^2 dn}{8b}\right). \quad (70)$$

In particular, for $\eta d/b \simeq 1$, this can be written as

$$p_n(\sigma \neq \rho) \leq \frac{1}{2} \exp\left(-\frac{\eta n}{8}\right). \quad (71)$$

Note that, for the unentangled case, in the same regime $\eta/b \simeq 1/d$ we may write $p_n \leq \frac{1}{2} \exp[-n\eta/(8d)]$.

B. Adaptive protocol

The adaptive formulation of the discrete variable protocol of quantum illumination assumes an unlimited quantum computer with two register **a** and **b**, prepared in an arbitrary joint quantum state. In each probing, a system a is picked from the input register **a** and sent to the target. Its reflection a' is stored in the output register **b**. A adaptive quantum operation (QO) is applied to both the update registers before the next transmission and so on. Therefore any probing is interleaved by the application of adaptive QOs Λ 's to the registers, defining the adaptive protocol $\mathcal{P}_n$ (see also the main text for this description). After n probings, the state of the registers is $\rho_n(u)$ where $u = 0, 1$ is a bit encoding the absence or presence of the target. This state is optimally measured by an Helstrom POVM. By optimizing over all protocol $\mathcal{P}_n$, we define the minimum error probability p_n for adaptive quantum illumination.

Following the constraints and typical regime of DV quantum illumination, we assume that the signal systems are $(d+1)$ -dimensional qudits described by a basis $\{|0\rangle, |1\rangle, \dots, |d\rangle\}$, where $|i\rangle := |0\dots 010\dots 0\rangle$ has one photon in the i th mode. For this reason, the two possible quantum illumination channels, $\mathcal{E}_0$ and $\mathcal{E}_1$, are $(d+1)$ -dimensional channels. In particular, consider as their input the maximally-entangled state

$$\Psi_{si} = \frac{1}{d+1} \sum_{k,j=0}^d |kk\rangle_{si} \langle jj|, \quad (72)$$

which is similar to ψ_{si} in Eq. (65) but also includes the vacuum state. Then, we may write the following two $(d+1) \times (d+1)$ dimensional Choi matrices

$$\begin{aligned} \text{Target absent: } \sigma &:= \rho_{\mathcal{E}_0} = \rho^{\text{th}}(b) \otimes (d+1)^{-1} \mathbb{I}_i^{d+1}, \\ \text{Target present: } \rho &:= \rho_{\mathcal{E}_1} = (1 - \eta)\sigma + \eta\Psi_{si}. \end{aligned} \quad (73)$$

It is clear that $\mathcal{E}_0$ and $\mathcal{E}_1$ are not jointly teleportation-covariant due to the fact that they have different transmissivities ($\eta_0 = 0$ and $\eta_1 = \eta$).

To bound p_n we apply Theorem 3 of the main text and, more specifically, Eq. (27) of the main text, because $\eta \ll 1$ and, therefore, the fidelity between the Choi matrices can be expanded as $F(\sigma, \rho) \simeq 1 - \epsilon$. Thus, let us start by computing this fidelity. Let us set $x = \sqrt{1 - bd}$ and note that we may write

$$\sqrt{\sigma} = (x|0\rangle_s \langle 0| + \sqrt{b}\mathbb{I}_s^d) \otimes (d+1)^{-1/2} \mathbb{I}_i^{d+1}. \quad (74)$$

Then, we may compute

$$\begin{aligned}\Omega^2 &:= \sqrt{\sigma}\rho\sqrt{\sigma} \\ &= \frac{1}{(d+1)^2} \left\{ (1-\eta) [x^4|0\rangle_s\langle 0| + b^2\mathbb{I}_s^d] \otimes \mathbb{I}_i^{d+1} \right. \\ &\quad + \eta \left[x^2|00\rangle_{si}\langle 00| + \sqrt{b}x \sum_{k=1}^d (|00\rangle_{si}\langle kk| + |kk\rangle_{si}\langle 00|) \right. \\ &\quad \left. \left. + b \sum_{j,k=1}^d |kk\rangle_{si}\langle jj| \right] \right\}. \quad (75)\end{aligned}$$

One can check that Ω^2 has d^2 degenerate eigenvalues equal to $b^2(d+1)^{-2}$, d degenerate eigenvalues equal to $(1-\eta)x^4(d+1)^{-2}$, and other $d+1$ eigenvalues $\{\lambda_i\}$ given by the diagonalization of the matrix $(d+1)^{-2}\mathbf{M}$ where

$$\mathbf{M} = \begin{pmatrix} (1-\eta)x^4 + \eta x^2 & \eta x\sqrt{b} & \eta x\sqrt{b} & \cdots & \eta x\sqrt{b} \\ \eta x\sqrt{b} & b(b+\eta) & \eta b & \cdots & \eta b \\ \eta x\sqrt{b} & \eta b & b(b+\eta) & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \eta b \\ \eta x\sqrt{b} & \eta b & \cdots & \eta b & b(b+\eta) \end{pmatrix}. \quad (76)$$

Once we find the eigenvalues of Ω^2 we take their square root so as to compute those of Ω . Finally, their sum provides $\text{Tr}\Omega = F(\sigma, \rho)$. We are interested in the regime of low thermal noise $b \ll 1$ and low reflectivity $\eta \ll 1$. There, we may expand at the leading orders in η and b to get

$$F(\sigma, \rho) = 1 - \frac{\eta d + 2b - 2\sqrt{\eta db}}{2(d+1)} + \mathcal{O}(\eta^2, \eta^{3/2}b^{1/2}, \eta b, b^{3/2}). \quad (77)$$

In the typical signal-to-noise-ratio $\eta d/b \simeq 1$ of quantum illumination [8], we may directly re-write Eq. (77) as $F(\sigma, \rho) \simeq 1 - \epsilon$, where

$$\epsilon := \frac{\eta d + 2b - 2\sqrt{\eta db}}{2(d+1)} \simeq \frac{d\eta}{2(d+1)} < \eta/2, \quad (78)$$

up to orders $\mathcal{O}(\eta^2, \sqrt{\eta b}, b)$. By replacing the latter in Eq. (27) of the main text (and assuming the correct dimension $d \rightarrow d+1$), we get the following lower bound for the minimum error probability p_n of adaptive quantum illumination

$$p_n \geq \frac{1}{4} \exp(-4nd\sqrt{\eta}). \quad (79)$$

IV. ADAPTIVE QUANTUM CHANNEL ESTIMATION

A. Adaptive protocols for parameter estimation

As also described in the main text, consider an adaptive protocol of quantum channel estimation. We want

to estimate a continuous parameter θ encoded in a quantum channel $\mathcal{E}_\theta$ by means of the most general protocols allowed by quantum mechanics, i.e., based on adaptive QOs as described in the main text. After n probings, there is a θ -dependent output state $\rho_n(\theta)$ which is generated by the sequence of QOs $\{\Lambda_0, \Lambda_1, \dots, \Lambda_n\}$ characterizing the adaptive protocol $\mathcal{P}_n$. Finally, the output state is measured by a POVM $\mathcal{M}$ providing an optimal unbiased estimator $\hat{\theta}$ of parameter θ . The minimum error variance $\text{Var}(\hat{\theta}) := \langle (\hat{\theta} - \theta)^2 \rangle$ must satisfy the quantum Cramer-Rao bound (QCRB) [12] $\text{Var}(\hat{\theta}) \geq 1/\text{QFI}_\theta(\mathcal{P}_n)$, where $\text{QFI}_\theta(\mathcal{P}_n)$ is the quantum Fisher information (QFI) associated with n adaptive uses.

Note that the QFI can be computed as

$$\text{QFI}_\theta(\mathcal{P}_n) = \frac{4d_B^2[\rho_n(\theta), \rho_n(\theta + d\theta)]}{d\theta^2}, \quad (80)$$

where $d_B(\rho, \sigma) := \sqrt{2[1 - F(\rho, \sigma)]}$ is the Bures distance, with $F(\rho, \sigma)$ being the Bures fidelity of ρ and σ . The ultimate precision of adaptive quantum metrology is given by optimizing the QFI over all adaptive protocols, i.e.,

$$\overline{\text{QFI}}_\theta^n := \sup_{\mathcal{P}} \text{QFI}_\theta(\mathcal{P}_n). \quad (81)$$

Contrarily to the cases of sequential or parallel strategies, the ultimate performance of adaptive quantum metrology is poorly studied, with limited results for DV programmable channels, and mainly stated for DV and CV teleportation-covariant channels, such as Pauli or Gaussian channels [13].

B. PBT stretching of adaptive quantum metrology

As shown in Ref. [13], the adaptive estimation of a noise parameter θ encoded in a teleportation-covariant channel (i.e., such that the parametrized class of channels $\mathcal{E}_\theta$ is jointly-teleportation covariant) is limited to the standard quantum limit (SQL). More generally, as discussed in Ref. [14], the adaptive estimation of a parameter in a quantum channel cannot beat the SQL if the channel has a single-copy simulation, i.e., of the type

$$\mathcal{E}_\theta(\rho) = \mathcal{S}(\rho \otimes \pi_\theta), \quad (82)$$

where $\mathcal{S}$ is a (parameter-independent) trace-preserving QO and π_θ is a program state (depending on the parameter). To beat the SQL, the channel should not admit a simulation as in Eq. (82) but a multi-copy version

$$\mathcal{E}_\theta(\rho) = \mathcal{S}(\rho \otimes \pi_\theta^{\otimes M}), \quad (83)$$

for some $M > 1$. This is approximately the type of simulation that we can achieve by using PBT.

First of all, we may replace the channel $\mathcal{E}_\theta$ with its M -port approximation $\mathcal{E}_\theta^M := \mathcal{E}_\theta \circ \Gamma_M$, where Γ_M is the M -port PBT channel. Using Lemma 1 of the main text, the simulation error may be bounded as

$$\|\mathcal{E}_\theta - \mathcal{E}_\theta^M\|_\diamond \leq \delta_M := \|\mathcal{I} - \Gamma_M\|_\diamond \leq 2\beta M^{-1}, \quad (84)$$

where we set $\beta := d(d-1)$. By repeating the steps shown in Fig. 2 of the main text, we may write the metrological equivalent of Eq. (13). In other words, for any input state ρ_C , we may write the simulation

$$\mathcal{E}_\theta^M(\rho_C) = \mathcal{T}^M(\rho_C \otimes \rho_{\mathcal{E}_\theta}^{\otimes M}), \quad (85)$$

where $\mathcal{T}^M$ is a trace-preserving LOCC and $\rho_{\mathcal{E}_\theta}$ is the Choi matrix of $\mathcal{E}_\theta$. Then, we may also repeat the PBT stretching in Fig. 3 of the main text. In this way, the n -use output state $\rho_n = \rho_n(\theta)$ of an adaptive parameter estimation protocol can be decomposed as in Lemma 2 of the main text, i.e.,

$$\|\rho_n(\theta) - \bar{\Lambda}(\rho_{\mathcal{E}_\theta}^{\otimes nM})\| \leq n\delta_M. \quad (86)$$

C. PBT implies the Heisenberg scaling

Using the decomposition in Eq. (86), we may write a bound for the optimal quantum Fisher information in Eq. (81). For large n , we obtain the Heisenberg scaling

$$\overline{\text{QFI}}_\theta^n \lesssim n^2 \text{QFI}(\rho_{\mathcal{E}_\theta}), \quad (87)$$

where

$$\text{QFI}(\rho_{\mathcal{E}_\theta}) = \frac{4d_B^2(\rho_{\mathcal{E}_\theta}, \rho_{\mathcal{E}_\theta+d\theta})}{d\theta^2}. \quad (88)$$

In order to show Eq. (87), consider the function

$$q_n(\theta, \delta) = 2 \frac{d_B[\rho_n(\theta), \rho_n(\theta + \delta)]}{\delta}. \quad (89)$$

We set $u_\theta := \bar{\Lambda}(\rho_{\mathcal{E}_\theta}^{\otimes nM})$ and apply twice the triangular inequality, so that we may write

$$d_B[\rho_n(\theta), \rho_n(\theta + \delta)] \leq d_B[\rho_n(\theta), u_\theta] + d_B[u_\theta, u_{\theta+\delta}] + d_B[u_{\theta+\delta}, \rho_n(\theta + \delta)]. \quad (90)$$

Bounding the Bures distance with the trace distance, we get

$$d_B^2[\rho_n(\theta), u_\theta] \leq \frac{\|\rho_n(\theta) - u_\theta\|}{2} \leq \frac{n\delta_M}{2} \leq \frac{\beta n}{M}. \quad (91)$$

Using Eqs. (90) and (91), we may write

$$q_n(\theta, \delta) \leq 2 \frac{d_B[u_\theta, u_{\theta+\delta}]}{\delta} + \frac{4}{\delta} \sqrt{\frac{\beta n}{M}}. \quad (92)$$

We may bound d_B in Eq. (92) as follows

$$\begin{aligned} d_B[u_\theta, u_{\theta+\delta}] &\stackrel{(1)}{\leq} d_B[\rho_{\mathcal{E}_\theta}^{\otimes nM}, \rho_{\mathcal{E}_{\theta+\delta}}^{\otimes nM}] \\ &\stackrel{(2)}{=} \sqrt{2[1 - F(\rho_{\mathcal{E}_\theta}^{\otimes nM}, \rho_{\mathcal{E}_{\theta+\delta}}^{\otimes nM})]} \\ &\stackrel{(3)}{=} \sqrt{2(1 - F^{nM})} \stackrel{(4)}{\leq} \sqrt{2nM(1 - F)} \\ &\stackrel{(2)}{=} \sqrt{nM} d_B[\rho_{\mathcal{E}_\theta}, \rho_{\mathcal{E}_{\theta+\delta}}], \end{aligned} \quad (93)$$

where: (1) we use the monotonicity of the Bures distance under the CPTP map $\bar{\Lambda}$, (2) we use the standard relation between Bures distance and fidelity, (3) we set $F := F(\rho_{\mathcal{E}_\theta}, \rho_{\mathcal{E}_{\theta+\delta}})$ and exploit the multiplicativity of the fidelity over tensor products, and (4) we use the inequality $F^n \geq 1 - n + nF$. Therefore, from Eq. (92), we may derive the inequality

$$q_n(\theta, \delta) \leq 2\sqrt{nM} \frac{d_B[\rho_{\mathcal{E}_\theta}, \rho_{\mathcal{E}_{\theta+\delta}}]}{\delta} + \frac{4}{\delta} \sqrt{\frac{\beta n}{M}}. \quad (94)$$

Now notice that

$$\lim_{\delta \rightarrow 0} 2 \frac{d_B[\rho_{\mathcal{E}_\theta}, \rho_{\mathcal{E}_{\theta+\delta}}]}{\delta} = \sqrt{\text{QFI}(\rho_{\mathcal{E}_\theta})}. \quad (95)$$

This means that for any $\epsilon > 0$, there is $\delta < \delta_\epsilon$ such that

$$q_n(\theta, \delta) \leq \sqrt{nM} \left[\sqrt{\text{QFI}(\rho_{\mathcal{E}_\theta})} + \epsilon \right] + \frac{4}{\delta} \sqrt{\frac{\beta n}{M}}. \quad (96)$$

Setting $M = n^{1+z}$ (for any $z > 0$) implies

$$\begin{aligned} q_n(\theta, \delta) &\leq \kappa_n(\theta, \delta | \epsilon, z) \\ &:= \sqrt{n^{2+z}} \left[\sqrt{\text{QFI}(\rho_{\mathcal{E}_\theta})} + \epsilon \right] + \frac{4}{\delta} \sqrt{\frac{\beta}{n^z}}. \end{aligned} \quad (97)$$

Note that, by definition, $\text{QFI}_\theta(\mathcal{P}_n) := \lim_{\delta \rightarrow 0} q_n(\theta, \delta)^2$. Then, assume that the limit

$$\lim_{n \rightarrow \infty} \lim_{\delta \rightarrow 0} \frac{q_n(\theta, \delta)^2}{n^{2+z}} \quad (98)$$

exists for any $z > 0$. Then, using Eq. (97), which is valid for any n and δ , we may write

$$\begin{aligned} \lim_{n \rightarrow \infty} \lim_{\delta \rightarrow 0} \frac{q_n(\theta, \delta)}{\sqrt{n^{2+z}}} &\leq \liminf_{n \rightarrow \infty, \delta \rightarrow 0} \frac{\kappa_n(\theta, \delta | \epsilon, z)}{\sqrt{n^{2+z}}} \\ &\leq \sqrt{\text{QFI}(\rho_{\mathcal{E}_\theta})} + \epsilon. \end{aligned} \quad (99)$$

The previous inequality leads to

$$\lim_{n \rightarrow \infty} \frac{\text{QFI}_\theta(\mathcal{P}_n)}{n^{2+z}} \leq \left[\sqrt{\text{QFI}(\rho_{\mathcal{E}_\theta})} + \epsilon \right]^2, \quad (100)$$

for any $\epsilon, z > 0$. Now, sending ϵ and z to zero gives the following scaling for large n

$$\text{QFI}_\theta(\mathcal{P}_n) \lesssim n^2 \text{QFI}(\rho_{\mathcal{E}_\theta}). \quad (101)$$

Since this upper bound holds for any protocol $\mathcal{P}_n$ (because $\bar{\Lambda}$ disappears), then the asymptotic scaling in Eq. (101) may be extended to $\overline{\text{QFI}}_\theta^n$ as in Eq. (87). In conclusion we have obtained an upper bound for the quantum Fisher information corresponding to the Heisenberg (quadratic) scaling in the number of uses.

V. CONVERSE BOUNDS FOR ADAPTIVE PRIVATE COMMUNICATION

A. Adaptive protocols for quantum/private communication

Let us assume that the adaptive protocol described in the main text has the task of secret key generation, i.e., to establish a secret key between the register $\mathbf{a}$, owned by Alice, and the register $\mathbf{b}$, owned by Bob. This protocol employs adaptive LOCCs Λ_i interleaved with the transmissions over a d -dimensional quantum channel $\mathcal{E}$. (In this analysis we assume input and output Hilbert spaces with the same dimension d ; if the spaces have different dimensions, we may always pad the one with the lower dimension and formally enlarge the channel to include the extra dimensions.) After n adaptive uses of the channel, the output state ρ_n of the registers is epsilon-close to a target private state [15] ϕ_n with nR_n^ϵ private bits, i.e., $\|\rho_n - \phi_n\| \leq \epsilon$. By taking the limit for large n , small ϵ (weak converse), and optimizing over all asymptotic key-generation adaptive protocols $\mathcal{P}$, we define the secret key capacity of the channel $\mathcal{E}$

$$K(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{\epsilon, n} R_n^\epsilon. \quad (102)$$

It is known that this capacity is greater than other two-way assisted capacities. In fact, we have [15]

$$Q_2(\mathcal{E}) = D_2(\mathcal{E}) \leq P_2(\mathcal{E}) \leq K(\mathcal{E}), \quad (103)$$

where Q_2 is the two-way assisted quantum capacity (qubits per channel use), D_2 is the two-way assisted entanglement distribution capacity (ebits per channel use), and P_2 is the two-way assisted private capacity (private bits per channel use). We now investigate upper bounds for $K(\mathcal{E})$ which are derived by combining PBT stretching with various entanglement measures, therefore extending one of the main insights of Ref. [16].

B. PBT stretching of private communication and single-letter upper bounds

Consider the M -port approximation $\mathcal{E}^M$ of $\mathcal{E}$, as achieved by the PBT simulation with error δ_M . Correspondingly, we have an M -port approximate output state ρ_n^M such that $\|\rho_n - \rho_n^M\| \leq n\delta_M$ as in Eq. (15) of the main text. Then, we may stretch an adaptive n -use protocol $\mathcal{P}_n$ over $\mathcal{E}^M$ and write $\rho_n^M = \bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes nM})$ for a trace-preserving LOCC $\bar{\Lambda}$. Using the triangle inequality, we may write

$$\begin{aligned} \|\rho_n^M - \phi_n\| &\leq \|\rho_n^M - \rho_n\| + \|\rho_n - \phi_n\| \\ &\leq n\delta_M + \epsilon := \gamma. \end{aligned} \quad (104)$$

Now consider an entanglement measure E with the properties listed in Ref. [15, Sec. VIII]. For instance,

E may be the relative entropy of entanglement E_R (REE) [17–19] or the squashed entanglement E_{SE} (SE). In particular, these measures satisfy a suitable continuity property. For d -dimensional states ρ and σ such that $\|\rho - \sigma\| \leq \gamma$, we may write the Fannes-type inequality

$$|E(\rho) - E(\sigma)| \leq g(\gamma) \log_2 d + h(\gamma), \quad (105)$$

where g, h are regular functions going to zero in ϵ' . For the REE and the SE, these functions are [15]

$$\text{REE: } g(\gamma) = 4\gamma, \quad h(\epsilon) = 2H_2(\gamma), \quad (106)$$

$$\text{SE: } g(\gamma) = 16\sqrt{\gamma}, \quad h(\gamma) = 2H_2(2\sqrt{\gamma}), \quad (107)$$

where H_2 is the binary Shannon entropy.

By applying Eq. (105) to Eq. (104), we get

$$|E(\rho_n^M) - E(\phi_n)| \leq g(\gamma) \log_2 d + h(\gamma), \quad (108)$$

where $E(\phi_n) \geq nR_n^\epsilon$ (normalization) and

$$E(\rho_n^M) = E[\bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes nM})] \leq nM E(\rho_{\mathcal{E}}), \quad (109)$$

which exploits the monotonicity of E under trace-preserving LOCCs and the subadditivity over tensor-product states [15]. Therefore, we may write

$$R_n^\epsilon \leq M E(\rho_{\mathcal{E}}) + \frac{g(n\delta_M + \epsilon) \log_2 d + h(n\delta_M + \epsilon)}{n}. \quad (110)$$

Note that for a private state, we may write $\log_2 d \leq cn$ for some constant c [15]. Thus, for any adaptive key generation protocol $\mathcal{P}_n$ over a d -dimensional quantum channel $\mathcal{E}$, the maximum ϵ -secure key rate that can be generated after n uses is bounded as in Eq. (110) where E is an entanglement measure (as the REE or the SE), M is the number of ports, and δ_M is the error of the M -port PBT defined in Lemma 1 of the main text.

We can find alternate bound by extending the definition of channel's REE [16] to a tripartite version. Consider three finite-dimensional systems a', a and b' , and a quantum channel $\mathcal{E} = \mathcal{E}_{a \rightarrow b}$ from a to the output system b . Consider a generic input state $\rho_{a'ab'}$ transformed into an output state $\omega_{a'bb'} := \mathcal{E}_{a \rightarrow b}(\rho_{a'ab'})$ by the action of this channel. Then, one can define a tripartite version of channel's REE as

$$\tilde{E}_R(\mathcal{E}) := \sup_{\rho_{a'ab'}} E_R(a'|bb')_\omega - E_R(a'a|b)_\rho, \quad (111)$$

which satisfies $K(\mathcal{E}) \leq \tilde{E}_R(\mathcal{E})$ [20]. Moreover, if two channels are close in diamond norm $\|\mathcal{E} - \mathcal{E}'\|_\diamond \leq 2\epsilon$, then one may also write the continuity property [20]

$$|\tilde{E}_R(\mathcal{E}) - \tilde{E}_R(\mathcal{E}')| \leq 2\epsilon \log_2 d + f(\epsilon), \quad (112)$$

$$f(\epsilon) := (1 + \epsilon) \log_2(1 + \epsilon) - \epsilon \log_2 \epsilon, \quad (113)$$

where d is the dimension of the Hilbert space. Finally, as a straightforward application of one of the tools established in Ref. [16], i.e., the LOCC simulation of a quantum channel $\mathcal{E}$ via a resource state σ [15], one may write the data-processing upper bound $\tilde{E}_R(\mathcal{E}) \leq E_R(\sigma)$.

In our channel simulation via PBT, we have a multi-copy resource state $\sigma = \rho_{\mathcal{E}}^{\otimes M}$ for the M -port approximation $\mathcal{E}^M$ of the d -dimensional channel $\mathcal{E}$. This means that we may write

$$\tilde{E}_R(\mathcal{E}^M) \leq E_R(\rho_{\mathcal{E}}^{\otimes M}) \leq M E_R(\rho_{\mathcal{E}}). \quad (114)$$

Then, because we have

$$\|\mathcal{E} - \mathcal{E}^M\|_{\diamond} \leq \|\mathcal{I} - \Gamma_M\|_{\diamond} := \delta_M \leq 2d(d-1)M^{-1}, \quad (115)$$

from Eq. (112) we may derive

$$\tilde{E}_R(\mathcal{E}) \leq E_R(\rho_{\mathcal{E}}^{\otimes M}) + \delta_M \log_2 d + f(\delta_M/2). \quad (116)$$

As a result, we may write the upper bound

$$\begin{aligned} K(\mathcal{E}) &\leq E_R(\rho_{\mathcal{E}}^{\otimes M}) + \delta_M \log_2 d + f(\delta_M/2) \\ &\leq M E_R(\rho_{\mathcal{E}}) + \frac{2d(d-1)}{M} \log_2 d + f\left[\frac{d(d-1)}{M}\right] \\ &:= K_{\text{UB}}^M(\mathcal{E}). \end{aligned} \quad (117)$$

The tightest upper bound is obtained by minimizing $K_{\text{UB}}^M(\mathcal{E})$ over M , which is typically a finite value.

Let us apply the bound to channels that are nearly entanglement-breaking, so that $E_R(\rho_{\mathcal{E}}) \ll 1$. In this case, we expect that the optimal value of M is large. It is easy to see that a sub-optimal choice for M is given by

$$\tilde{M} = \sqrt{\frac{2d(d-1) \log_2 d}{E_R(\rho_{\mathcal{E}})}}, \quad (118)$$

which provides the upper bound

$$\begin{aligned} K(\mathcal{E}) &\leq 2\sqrt{2d(d-1) \log_2 d} \sqrt{E_R(\rho_{\mathcal{E}})} \\ &\quad + f\left[\sqrt{\frac{d(d-1)E_R(\rho_{\mathcal{E}})}{2 \log_2 d}}\right]. \end{aligned} \quad (119)$$

The bound in Eq. (119) is particularly interesting for almost entanglement-breaking channels, such that $E_R(\rho_{\mathcal{E}}) \lesssim (\log_2 d)/[8d(d-1)]$.

-
- [1] Ishizaka, S. & Hiroshima, T. Quantum teleportation scheme by selecting one of multiple output ports. *Phys. Rev. A* **79**, 042306 (2009).
 - [2] Shapiro, J. H. The quantum theory of optical communications. *IEEE J. Sel. Top. Quantum Electron.* **15**, 1547-1569 (2009).
 - [3] Lupo, C., Giovannetti, V., Pirandola, S., Mancini, S. & Lloyd, S. Enhanced quantum communication via optical refocusing. *Phys. Rev. A* **84**, 010303(R) (2011).
 - [4] Lupo, C., Giovannetti, V., Pirandola, S., Mancini, S. & Lloyd, S. Capacities of linear quantum optical systems. *Phys. Rev. A* **85**, 062314 (2012).
 - [5] Nielsen, M. A. & Chuang I. L. *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
 - [6] Tsang, M., Nair, R & Lu, X.-M. Quantum Theory of Superresolution for Two Incoherent Optical Point Sources. *Phys. Rev. X* **6**, 031033 (2016).
 - [7] Lupo, C. & Pirandola, S. Ultimate Precision Bound of Quantum and Subwavelength Imaging. *Phys. Rev. Lett.* **117**, 190802 (2016).
 - [8] Lloyd, S. Enhanced sensitivity of photodetection via quantum illumination. *Science* **321**, 1463 (2008).
 - [9] Tan, S.-H. *et al.* Quantum illumination with Gaussian states. *Phys. Rev. Lett.* **101**, 253601 (2008).
 - [10] Barzanjeh, S *et al.* Microwave quantum illumination. *Phys. Rev. Lett.* **114**, 080503 (2015).
 - [11] Weedbrook, C., Pirandola, S., Thompson, J., Vedral, V. & Gu, M. How discord underlies the noise resilience of quantum illumination. *New J. Phys.* **18**, 043027 (2016).
 - [12] Braunstein, S. L. & Caves, C. M. Statistical distance and the geometry of quantum states. *Phys. Rev. Lett.* **72**, 3439 (1994).
 - [13] Pirandola, S. & Lupo, C. Ultimate precision of adaptive noise estimation. *Phys. Rev. Lett.* **118**, 100502 (2017).
 - [14] Laurenza, R., Lupo, C., Spedalieri, G., Braunstein, S. L. & Pirandola, S. Channel simulation in quantum metrology. *Quantum Meas. Quantum Metrol.* **5**, 1-12 (2018).
 - [15] Pirandola, S., Braunstein, S. L., Laurenza, R., Ottaviani, C., Cope, T. P. W., Spedalieri, G. & Banchi, L. Theory of channel simulation and bounds for private communication *Quantum Sci. Technol.* **3**, 035009 (2018).
 - [16] Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017). See also preprint at <https://arxiv.org/abs/1510.08863> (2015).
 - [17] Vedral, V. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.* **74**, 197 (2002).
 - [18] Vedral, V., Plenio, M. B., Rippin, M. A. & Knight, P. L. Quantifying entanglement. *Phys. Rev. Lett.* **78**, 2275-2279 (1997).
 - [19] Vedral, V. & Plenio, M. B. Entanglement measures and purification procedures. *Phys. Rev. A* **57**, 1619 (1998).
 - [20] Kaur, E. & Wilde, M. M. Amortized entanglement of a quantum channel and approximately teleportation-simulable channels. *J. of Phys. A* **51**, 035303 (2018).