Energy-constrained two-way capacities of the pure-loss channel

Alessandro Falco[1,*] Francesco Anna Mele[2] Ludovico Lami[1] Vittorio Giovannetti[3]

[1] *Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy*

[2] *Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California 91125, USA*

[3] *NEST, Scuola Normale Superiore and Istituto Nanoscienze-CNR, Piazza dei Cavalieri 7, I-56126 Pisa, Italy*

Abstract

We determine the two-way quantum and secret-key capacities of the pure-loss channel under an average input photon-number constraint. For transmissivity η and photon budget N, both capacities equal $g(N) - g((1-\eta)N)$, where g is the entropy of a thermal state. This coincides with the rate achieved by the known reverse coherent information of a two-mode squeezed vacuum. Our result provides the last missing capacity formula for the celebrated pure-loss channel, completing the picture of bosonic quantum communication under pure loss.

1 Main result

The single-mode pure-loss channel $\mathcal{L}_\eta$, with transmissivity $\eta \in [0,1]$, mixes the input with a vacuum environment on a beam splitter [HW01, WPG+12]. We use its dilation

$$V_\eta|k\rangle = \sum_{j=0}^{k} \sqrt{\binom{k}{j}\eta^{k-j}(1-\eta)^j}\,|k-j\rangle_B|j\rangle_E, \qquad \mathcal{L}_\eta(\rho) = \mathrm{Tr}_E\, V_\eta \rho V_\eta^\dagger. \tag{1}$$

Thus j is the number of photons lost. The complementary channel is $\mathcal{L}_{1-\eta}$, up to the choice of an environment phase.

We consider the standard energy-constrained, two-way-assisted communication model [DSW18, MLG25]. Alice and Bob start with local states and may share public randomness, but no entanglement or secret key. They alternate n uses of $\mathcal{L}_\eta$ with arbitrary local operations and classical communication (LOCC) [CLMOW14]. At each fixed blocklength, a code uses finitely many local rounds and finite or countable classical message alphabets; no uniform bound on the number of rounds is imposed as n grows. All operations act on trace-class states on separable Hilbert spaces; their adjoints are normal. The classical channel is authenticated and public. Eve receives the channel environments and the public transcript. The only energy constraint is

$$\frac{1}{n}\sum_{i=1}^{n} \mathrm{Tr}[\hat{n}\,\bar{\rho}_{S_i}] \le N, \qquad \hat{n} = a^\dagger a, \tag{2}$$

where $\bar{\rho}_{S_i}$ is the unconditional input state at use i: previous measurement outcomes have already been averaged over. Local ancillas and memories are unrestricted.

The capacities $Q_2(\mathcal{L}_\eta, N)$ and $K(\mathcal{L}_\eta, N)$ are the supremal asymptotic rates of entanglement and secret-key generation, respectively, with error tending to zero. Rates are measured in ebits and secret bits per channel use. With free classical communication, entanglement generation and quantum transmission have the same capacity by teleportation [BBC+93, DSW18]. For secret-key generation, we use the standard correctness and secrecy error [PR22]. For entanglement generation, the error is the infidelity with a maximally entangled state. Both errors are evaluated on the unconditional output.

* alessandro.falco@sns.it

Theorem 1.1 (Energy-constrained two-way capacities)**.** *For every $\eta \in [0,1]$ and every finite $N \geq 0$,*

$$\boxed{Q_2(\mathcal{L}_\eta, N) = K(\mathcal{L}_\eta, N) = g(N) - g((1-\eta)N),} \tag{3}$$

where $g(x) = (x+1)\log_2(x+1) - x\log_2 x$ and $0\log_2 0 = 0$. The optimization includes all adaptive LOCC protocols satisfying (2).

Throughout, logarithms are in base 2, and all Hilbert spaces are separable. We write $S(\rho) = -\operatorname{Tr}\rho\log_2\rho$ for von Neumann entropy and $H(p) = -\sum_a p_a \log_2 p_a$ for Shannon entropy. Identity maps on untouched systems are implicit. We abbreviate

$$q := 1-\eta, \qquad f_\eta(x) := g(x) - g(qx). \tag{4}$$

The formula gives 0 at $N = 0$ or $\eta = 0$, and $g(N)$ at $\eta = 1$. For $0 \leq \eta < 1$, it also gives $\lim_{N\to\infty} f_\eta(N) = -\log_2(1-\eta)$, recovering the unconstrained capacity [PLOB17]. Earlier upper bounds for two-way bosonic communication were obtained from squashed entanglement; see [TGW14, GEW16, DSW18]. The achievable function f_η comes from reverse reconciliation and reverse coherent information [PGBL09, GPLS09].

Figure 1 compares these rates with the other capacities of the pure-loss channel at $N = 1$. For $0 < \eta \leq 1/2$, the unassisted quantum and private classical capacities vanish [WHG12, WQ18], whereas Q_2 and K remain positive. At $\eta = 1/2$, for example, $Q_2 = K \simeq 0.6226$.

Proof outline. The lower bound is reverse hashing [DW05, GPLS09]; we recall it in Section 5.3. For finite input energy and finite input relative entropy of entanglement, the central converse statement is

$$E_R^\infty(X:BY)_{(\mathrm{id}\otimes\mathcal{L}_\eta)(\rho)} \leq E_R^\infty(XS:Y)_\rho + f_\eta(\operatorname{Tr}[\hat{n}\rho_S])\,. \tag{5}$$

Here XS belongs to Alice before transmission, Y belongs to Bob, and E_R^∞ is the regularized relative entropy of entanglement. The inequality allows arbitrary correlations with both memories. It can therefore be summed over the uses of an adaptive protocol. We prove it by grouping independent copies, resolving their total photon number, and bounding the relative entropy of entanglement of the sector Choi states. The remaining dephasing cost grows only logarithmically with the number of copies. Finally, a privacy test converts the entanglement bound into a bound on secret-key length that is independent of the size of the shield systems.

2 Relative entropy tools

For states ρ, σ, their quantum relative entropy is $D(\rho\|\sigma) = \operatorname{Tr}\rho(\log_2\rho - \log_2\sigma)$, with its usual extended-value interpretation. We use its data-processing inequality, $D(\rho\|\sigma) \geq D(\mathcal{T}(\rho)\|\mathcal{T}(\sigma))$ for every quantum channel $\mathcal{T}$ [Lin75], with the separable-Hilbert-space formulation covered by [MR17].

For a bipartite state, the relative entropy of entanglement and its regularization are [VPRK97, VP98]

$$E_R(A:B)_\rho := \inf_{\sigma\in\mathrm{SEP}(A:B)} D(\rho\|\sigma), \qquad E_R^\infty(A:B)_\rho := \lim_{r\to\infty}\frac{1}{r}E_R(A^r:B^r)_{\rho^{\otimes r}}. \tag{6}$$

The separable states form the trace-norm closed convex hull of product states. The second limit exists whenever $E_R(\rho) < \infty$, by subadditivity. We omit the bipartition when it is clear.

We use three standard properties of E_R: convexity, subadditivity on tensor products, and monotonicity on average under local instruments and LOCC [VP98]. For completeness, the last

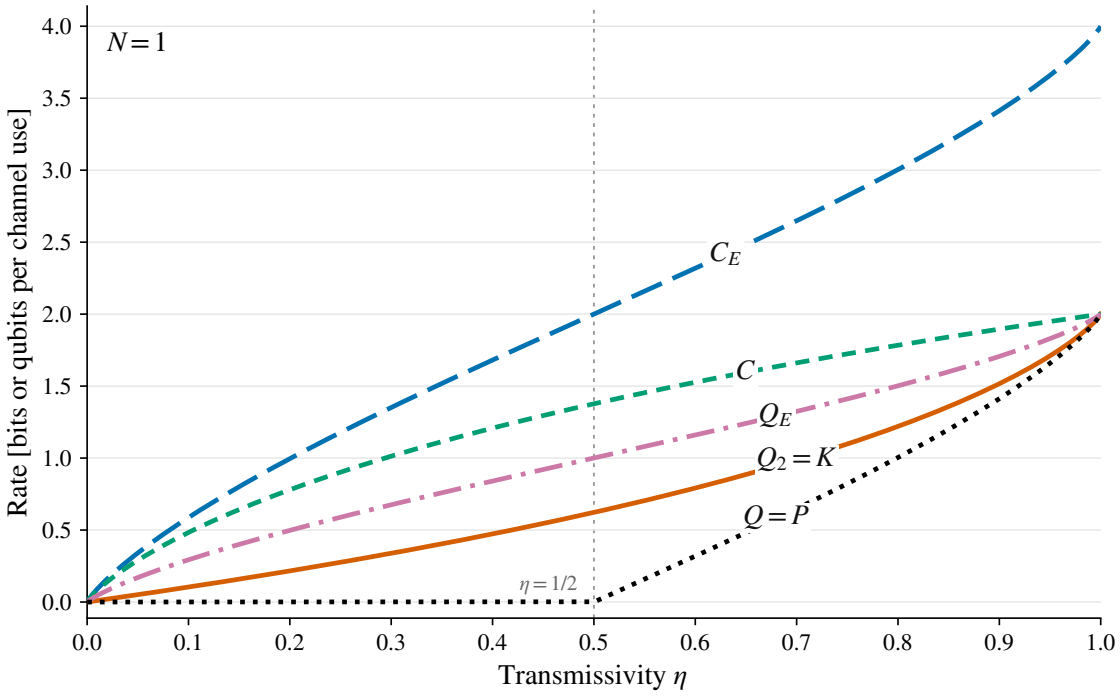


Figure 1: Capacities of the single-mode pure-loss channel as functions of transmissivity η, for an average input photon budget $N = 1$. All rates are asymptotic, with error tending to zero. The two-way quantum and secret-key capacities are $Q_2 = K = g(N) - g((1-\eta)N)$ (solid), by Theorem 1.1. The unassisted classical capacity is $C = g(\eta N)$ (short-dashed) [GGL+04]. With unlimited preshared entanglement, the classical capacity is $C_E = g(N) + g(\eta N) - g((1-\eta)N)$ (long-dashed) [GLMS03], and the quantum capacity is $Q_E = C_E/2$ (dash-dotted) [BSST02]. The unassisted quantum and private classical capacities are $Q = P = \max\{0, g(\eta N) - g((1-\eta)N)\}$ (dotted) [WHG12, WQ18]. The vertical guide marks $\eta = 1/2$; $Q = P = 0$ at and below this value. Classical and key rates are in bits per channel use; quantum rates are in qubits per channel use.

property follows by applying data processing to an instrument with its outcome retained. For any separable comparison state, the resulting relative entropy is a classical relative entropy plus an average of conditional relative entropies. Dropping the first term and optimizing gives $\sum_a p_a E_R(\rho_a) \leq E_R(\rho)$. Convexity follows from joint convexity of relative entropy, and subadditivity follows by taking product comparison states. These arguments also apply on separable infinite-dimensional Hilbert spaces. We will use that E_R is lower semicontinuous in trace norm [LS23, Corollary 20]. The regularized quantity is monotone under LOCC because this holds for every tensor power before taking the limit.

2.1 The cost of local dephasing

The following finite-dimensional observation is the form of non-lockability that we need; see also [HHHO05a].

Lemma 2.1 (Local dephasing)**.** *Let $\Delta(\rho) = \sum_a P_a \rho P_a$ be a projective dephasing on one party of a finite-dimensional bipartite system, and let $p_a = \mathrm{Tr}(P_a \rho)$. Then*

$$E_R(\rho) \le E_R(\Delta\rho) + D(\rho\|\Delta\rho), \qquad D(\rho\|\Delta\rho) \le H(p). \tag{7}$$

Proof. In minimizing $D(\Delta\rho\|\sigma)$ over separable σ, we may dephase σ: separability is preserved and data processing cannot increase the objective. For $\Delta\sigma = \sigma$, block diagonality gives

$$D(\rho\|\sigma) = D(\rho\|\Delta\rho) + D(\Delta\rho\|\sigma).$$

Optimizing proves the first inequality. For the second, purify ρ to $|\psi\rangle$. The nonzero vectors $P_a|\psi\rangle/\sqrt{p_a}$ are orthonormal, so the relative entropy of $|\psi\rangle\langle\psi|$ from its dephased state is $-\sum_a p_a \log_2 p_a = H(p)$. Tracing out the purification and applying data processing proves the claim. □

2.2 Simulation from an irreducible symmetry

Write $|\Phi_d\rangle = d^{-1/2}\sum_{a=1}^{d}|a\rangle|a\rangle$ and $\Phi_d = |\Phi_d\rangle\langle\Phi_d|$. A finite-dimensional channel $\mathcal{T}$ is simulable by LOCC using its normalized Choi state $\Omega_{\mathcal{T}} = (\mathrm{id}\otimes\mathcal{T})(\Phi_d)$ whenever it is covariant under a compact group whose input representation is irreducible:

$$\mathcal{T}(U_g \rho U_g^\dagger) = W_g \mathcal{T}(\rho) W_g^\dagger. \tag{8}$$

The required simulation is given in [GBW21, Proposition 24]. To check its normalization, Alice measures the input and her half of $\Omega_{\mathcal{T}}$ with the Bell POVM, with normalized Haar measure μ,

$$d^2 (I \otimes \bar{U}_g)\Phi_d(I \otimes \bar{U}_g)^\dagger \, \mathrm{d}\mu(g).$$

Schur's lemma makes its integral the identity. Finite-dimensional convexity also allows a finite weighted sum with the same operator average, so finitely many measurement outcomes suffice. Conditional on g, Bob's unnormalized state is $\mathcal{T}(U_g\rho U_g^\dagger)\mathrm{d}\mu(g)$; he applies $W_g^\dagger$. This implements $\mathcal{T}$ exactly, also on inputs correlated with other systems. Consequently, for any such input ρ,

$$E_R(\text{output}) \le E_R(\text{input}) + E_R(\Omega_{\mathcal{T}}). \tag{9}$$

Indeed, the simulation is LOCC, and its initial state is the product of ρ with $\Omega_{\mathcal{T}}$. The resource term in (9) is independent of the local memories.

3 A fixed number of photons

Fix $m \ge 1$ modes. The sector with k photons is

$$\mathcal{H}_{m,k} = \mathrm{Sym}^k(\mathbb{C}^m), \qquad d_k := \dim \mathcal{H}_{m,k} = \binom{m+k-1}{k}, \qquad \pi_k := \frac{\Pi_{m,k}}{d_k}. \tag{10}$$

Here $\Pi_{m,k}$ is the projector onto that sector; m is suppressed in d_k and π_k. The binomial coefficient counts the ways to distribute k photons among m occupation numbers. Passive mode transformations $U \in U(m)$ act as $U^{\otimes k}$ restricted to $\mathrm{Sym}^k(\mathbb{C}^m)$, an irreducible representation [Har13].

For a unit vector $u \in \mathbb{C}^m$, let

$$|u;k\rangle := \frac{\left(\sum_{a=1}^m u_a a_a^\dagger\right)^k}{\sqrt{k!}}|0\rangle. \tag{11}$$

This is the normalized state of k photons in the same mode u. Averaging uniformly over u gives

$$\int |u;k\rangle\langle u;k|\,\mathrm{d}\mu(u) = \pi_k. \tag{12}$$

The integral is invariant under every mode transformation, so irreducibility makes it proportional to $\Pi_{m,k}$; its trace fixes the factor $1/d_k$. This is the standard symmetric-subspace resolution [Har13].

3.1 Conditioning on the number lost

With k input photons, the total number J lost has distribution

$$b_{k,j} := \Pr(J = j \mid k) = \binom{k}{j} q^j \eta^{k-j}, \qquad 0 \le j \le k, \tag{13}$$

independently of the state within the sector. Here and below endpoint probabilities are understood by continuity. To verify this for arbitrary inputs, write a Fock occupation vector as $\mathbf{a} = (a_1, \dots, a_m)$ with $|\mathbf{a}| = k$. The normalized isometry for the branch with j losses is

$$V_{k,j}|\mathbf{a}\rangle = \sum_{\substack{\mathbf{t}\le\mathbf{a}\\ |\mathbf{t}|=j}} \sqrt{\frac{\prod_{s=1}^m \binom{a_s}{t_s}}{\binom{k}{j}}}\,|\mathbf{a}-\mathbf{t}\rangle_B|\mathbf{t}\rangle_E. \tag{14}$$

Different $\mathbf{a}$ give orthogonal outputs. Their squared norms are one by Vandermonde's identity, $\sum_{|\mathbf{t}|=j}\prod_s \binom{a_s}{t_s} = \binom{k}{j}$. Expanding (1) on all m modes therefore gives the branch amplitude $\sqrt{b_{k,j}}V_{k,j}$, proving (13). Expanding (11) also gives the useful identity

$$V_{k,j}|u;k\rangle = |u;k-j\rangle_B|u;j\rangle_E. \tag{15}$$

Together with (12), this implies that the environment marginal of $V_{k,j}\pi_k V_{k,j}^\dagger$ is π_j.

3.2 An explicit separable comparison state

Let $\mathcal{T}_{m,k}$ be $\mathcal{L}_\eta^{\otimes m}$ restricted to $\mathcal{H}_{m,k}$, and let $\Omega_{m,k}$ be its normalized Choi state. Its output lies in the finite-dimensional space $\bigoplus_{\ell=0}^k \mathcal{H}_{m,\ell}$. The channel is covariant under passive mode transformations, with an irreducible input representation. Section 2 therefore gives an exact simulation using $\Omega_{m,k}$.

Lemma 3.1 (Relative entropy of the sector Choi state)**.** *For all $m \ge 1$ and $k \ge 0$,*

$$E_R(\Omega_{m,k}) \le c_m(k), \qquad c_m(k) := \log_2 d_k - \sum_{j=0}^k b_{k,j}\log_2 d_j. \tag{16}$$

Proof. Fix j and put $\ell = k - j$. Let

$$|\Psi_{k,j}\rangle = (I_R \otimes V_{k,j})|\Phi_{d_k}\rangle, \qquad \Omega_{k,j} = \mathrm{Tr}_E|\Psi_{k,j}\rangle\langle\Psi_{k,j}|.$$

The environment marginal is π_j, by (15). Choose an orthonormal basis $\{|t\rangle\}_{t=1}^{d_j}$ of $\mathcal{H}_{m,j}$ and set

$$C_t = (I_B \otimes \langle t|_E)V_{k,j}, \qquad |\chi_t\rangle = \sqrt{d_j}(I_R \otimes C_t)|\Phi_{d_k}\rangle. \tag{17}$$

Since the environment marginal is π_j, these vectors are orthonormal. Thus, with $P_{k,j} := \sum_t |\chi_t\rangle\langle\chi_t|$,

$$\Omega_{k,j} = \frac{P_{k,j}}{d_j}. \tag{18}$$

Consider the separable state

$$\sigma_{k,j} := \int |\bar{u};k\rangle\langle\bar{u};k|_R \otimes |u;\ell\rangle\langle u;\ell|_B \, \mathrm{d}\mu(u), \tag{19}$$

where conjugation is in the Fock basis. We claim that

$$\sigma_{k,j} P_{k,j} = \frac{1}{d_k} P_{k,j}. \tag{20}$$

Indeed, (15) gives $C_t|u;k\rangle = \langle t|u;j\rangle|u;\ell\rangle$ and hence

$$(\langle\bar{u};k| \otimes \langle u;\ell|)|\chi_t\rangle = \sqrt{\frac{d_j}{d_k}}\,\langle t|u;j\rangle.$$

Using this in (19),

$$\begin{aligned}\sigma_{k,j}|\chi_t\rangle &= \sqrt{\frac{d_j}{d_k}} \int |\bar{u};k\rangle \otimes C_t|u;k\rangle \, \mathrm{d}\mu(u) \\ &= \frac{\sqrt{d_j}}{d_k}(I \otimes C_t)|\Phi_{d_k}\rangle = \frac{1}{d_k}|\chi_t\rangle. \end{aligned} \tag{21}$$

For the second equality, vectorizing (12) gives $\int |\bar{u};k\rangle \otimes |u;k\rangle \, \mathrm{d}\mu(u) = d_k^{-1/2}|\Phi_{d_k}\rangle$.

Equations (18) and (20) now imply

$$E_R(\Omega_{k,j}) \le D(\Omega_{k,j}\|\sigma_{k,j}) = \log_2 d_k - \log_2 d_j. \tag{22}$$

Finally, $\Omega_{m,k} = \sum_j b_{k,j}\Omega_{k,j}$, with the different output sectors embedded in the same space. Convexity of E_R and (22) prove (16). □

4 Entanglement increase under an energy constraint

We now allow superpositions of different photon numbers and correlations with either party's memory.

Lemma 4.1 (Block bound)**.** *Let ρ_{XS^mY} be a state on separable Hilbert spaces with $E_R(XS^m : Y)_\rho < \infty$ and $\mathrm{Tr}[\widehat{N}_{S^m}\rho] = m\nu < \infty$, where $\widehat{N}_{S^m} = \sum_{a=1}^m \hat{n}_{S_a}$. Set $\omega = (\mathrm{id}_{XY} \otimes \mathcal{L}_\eta^{\otimes m})(\rho)$. Then*

$$E_R(X : B^mY)_\omega \le E_R(XS^m : Y)_\rho + m f_\eta(\nu) + g(qm\nu). \tag{23}$$

Proof. We first suppose that X, Y are finite-dimensional and that ρ has finite photon-number support. All subsequent entropies are then ordinary finite quantities. The infinite-dimensional extension is given at the end of the proof.

Step 1: pay for coherences between sectors. Let Δ_S and Δ_B dephase the total photon number of the m input and output modes, respectively. Phase covariance gives

$$\Delta_B \circ \mathcal{L}_\eta^{\otimes m} = \mathcal{L}_\eta^{\otimes m} \circ \Delta_S. \tag{24}$$

For example, both dephasings are averages over $e^{i\theta\widehat{N}}$, and the channel intertwines these phase rotations. Let K be the input total photon number, with probabilities p_k, and write $\Delta_S\rho = \sum_k p_k \rho_k$

for the normalized conditional states. Put $\omega_k = (\mathrm{id} \otimes \mathcal{L}_\eta^{\otimes m})(\rho_k)$. Lemma 2.1, data processing, and (24) yield

$$E_R(\omega) \le E_R(\Delta_B \omega) + H(K). \tag{25}$$

Explicitly, the additional term is bounded as $D(\omega \| \Delta_B \omega) \le D(\rho \| \Delta_S \rho) \le H(K)$. By convexity, the sector simulation, and average LOCC monotonicity,

$$\begin{aligned} E_R(\Delta_B \omega) &\le \sum_k p_k E_R(\omega_k) \\ &\le \sum_k p_k (E_R(\rho_k) + c_m(k)) \le E_R(\rho) + \mathbb{E} c_m(K). \end{aligned} \tag{26}$$

Here the bipartition is $XS^m : Y$ before transmission and $X : B^m Y$ after transmission. In particular, measuring K is a local instrument on Alice's side. Combining the two bounds gives

$$E_R(\omega) - E_R(\rho) \le H(K) + \mathbb{E} \log_2 d_K - \mathbb{E} \log_2 d_J, \tag{27}$$

where the joint law is $\Pr(K = k, J = j) = p_k b_{k,j}$.

Step 2: express the photon bound as an entropy difference. Introduce the auxiliary states

$$\zeta := \sum_k p_k \pi_k, \qquad \zeta' := \mathcal{L}_q^{\otimes m}(\zeta) = \sum_j \Pr(J = j) \pi_j. \tag{28}$$

The output identity follows from (12) and (15). Orthogonality of the sectors gives

$$S(\zeta) = H(K) + \mathbb{E} \log_2 d_K, \qquad S(\zeta') = H(J) + \mathbb{E} \log_2 d_J. \tag{29}$$

Therefore the right-hand side of (27) is $S(\zeta) - S(\zeta') + H(J)$.

Step 3: compare with thermal states. The one-mode thermal state with mean photon number x is

$$\tau_x = \frac{1}{x+1} \sum_{k \ge 0} \left(\frac{x}{x+1} \right)^k |k\rangle\langle k|, \qquad S(\tau_x) = g(x). \tag{30}$$

For $x > 0$ and any m-mode state θ of total mean photon number mx, the logarithm of the thermal reference gives

$$D(\theta \| \tau_x^{\otimes m}) = m g(x) - S(\theta). \tag{31}$$

In particular, positivity of relative entropy proves $S(\theta) \le m g(x)$. Binomial thinning of the geometric distribution in (30) gives $\mathcal{L}_q(\tau_x) = \tau_{qx}$. The states in (28) have total means $m\nu$ and $qm\nu$, respectively. For $q > 0$ and $\nu > 0$, data processing gives

$$\begin{aligned} m g(\nu) - S(\zeta) &= D(\zeta \| \tau_\nu^{\otimes m}) \\ &\ge D(\zeta' \| \tau_{q\nu}^{\otimes m}) = m g(q\nu) - S(\zeta'). \end{aligned} \tag{32}$$

It follows that $S(\zeta) - S(\zeta') \le m f_\eta(\nu)$. If $q\nu = 0$, the state ζ' is vacuum, and the same inequality follows from the entropy bound just proved; if $\nu = 0$, both states are vacuum. Finally, J is a nonnegative integer with mean $qm\nu$. Comparing its distribution with the geometric distribution of that mean gives $H(J) \le g(qm\nu)$, again by nonnegativity of relative entropy. Substitution in (27) proves (23).

Step 4: remove all cutoffs. Choose increasing finite-rank projections $P_L^X \to I_X$ and $P_L^Y \to I_Y$ strongly, and define the product projection

$$T_L = P_L^X \otimes \Pi_{m,\le L}^{S^m} \otimes P_L^Y, \qquad p_L = \mathrm{Tr}(T_L\rho), \qquad \rho_L = T_L\rho T_L/p_L.$$

For sufficiently large L, $p_L > 0$. We have $p_L \to 1$ and $\rho_L \to \rho$ in trace norm. The projections commute with the photon number, so monotone convergence gives $\nu_L := m^{-1}\,\mathrm{Tr}(\widehat{N}\rho_L) \to \nu$. The successful projection is a local filtering outcome; hence $p_L E_R(\rho_L) \le E_R(\rho)$. Writing $\omega_L = (\mathrm{id}\otimes\mathcal{L}_\eta^{\otimes m})(\rho_L)$ and applying the finite-dimensional bound,

$$E_R(\omega_L) \le \frac{E_R(\rho)}{p_L} + m f_\eta(\nu_L) + g(qm\nu_L).$$

Now $\omega_L \to \omega$ in trace norm. By lower semicontinuity of E_R [LS23, Corollary 20],

$$E_R(\omega) \le \liminf_{L\to\infty} E_R(\omega_L) \le E_R(\rho) + m f_\eta(\nu) + g(qm\nu),$$

where the last inequality uses $p_L \to 1$, $\nu_L \to \nu$, and continuity of f_η, g. No entropy assumption on X or Y is needed. □

Corollary 4.2 (Amortized regularized bound)**.** *Let ρ_{XSY} satisfy $E_R(XS:Y)_\rho < \infty$ and $\mathrm{Tr}(\hat{n}\rho_S) = \nu < \infty$. For $\omega = (\mathrm{id}_{XY}\otimes\mathcal{L}_\eta)(\rho)$,*

$$E_R^\infty(X:BY)_\omega \le E_R^\infty(XS:Y)_\rho + f_\eta(\nu). \tag{33}$$

Proof. Apply Lemma 4.1 to r copies of ρ, grouping all of Alice's memories and all of Bob's memories. Their r input modes have total mean photon number $r\nu$, so

$$E_R(\omega^{\otimes r}) \le E_R(\rho^{\otimes r}) + r f_\eta(\nu) + g(qr\nu).$$

Divide by r and take $r \to \infty$. The last term divided by r tends to zero, since $g(x) = O(\log(x+1))$ as $x \to \infty$. The single-copy block bound also ensures $E_R(\omega) < \infty$, so both regularizations exist. This proves (33). □

5 Private states and the capacity theorem

We next relate E_R^∞ to an approximate secret key. This step keeps the local shield systems and places no bound on their dimensions.

5.1 A privacy test that survives regularization

A private state with key dimension d has the form [HHHO05b, HHHO09, WTB17]

$$\gamma_{AA'BB'} = U(\Phi_{d,AB}\otimes\theta_{A'B'})U^\dagger, \qquad U = \sum_{a,b=1}^{d} |a,b\rangle\langle a,b|_{AB}\otimes U_{ab}, \tag{34}$$

where the U_{ab} are unitaries and A', B' are the shields. Measuring A, B in the displayed basis gives a uniform common key, independent of every purifying system. Its privacy test is the projector

$$\Pi_\gamma = U(\Phi_{d,AB}\otimes I_{A'B'})U^\dagger. \tag{35}$$

We use squared fidelity, $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$. The standard privacy-test properties are [WTB17, Lemmas 9–10]

$$\mathrm{Tr}(\Pi_\gamma \omega) \geq F(\omega,\gamma), \qquad \mathrm{Tr}(\Pi_\gamma \sigma) \leq \frac{1}{d} \quad \text{for every } \sigma \in \mathrm{SEP}(AA' : BB'). \tag{36}$$

The first inequality follows by applying the test to both states and using fidelity monotonicity. To check the second, take a normalized product vector $|\alpha\rangle_{AA'}|\beta\rangle_{BB'}$ and write $|\alpha\rangle = \sum_a |a\rangle|\alpha_a\rangle$ and $|\beta\rangle = \sum_a |a\rangle|\beta_a\rangle$. Then

$$\langle \alpha,\beta|\Pi_\gamma|\alpha,\beta\rangle = \frac{1}{d}\|\sum_a U_{aa}^\dagger(|\alpha_a\rangle \otimes |\beta_a\rangle)\|^2 \leq \frac{1}{d}\left(\sum_a \|\alpha_a\|\|\beta_a\|\right)^2 \leq \frac{1}{d}. \tag{37}$$

The triangle and Cauchy–Schwarz inequalities give the two bounds. Convexity and trace-norm closure extend them to every separable state, including infinite-dimensional shields.

Lemma 5.1 (Regularized privacy bound)**.** *Suppose $d \geq 2$, $0 \leq \varepsilon \leq \frac{1}{2}$, and $F(\omega,\gamma) \geq 1-\varepsilon$ for a private state of key dimension d. If $E_R(\omega) < \infty$, then*

$$E_R^\infty(\omega) \geq (1-\varepsilon)\log_2 d - h_2(\varepsilon), \tag{38}$$

where $h_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$.

Proof. Put $\Pi = \Pi_\gamma$ and $p = \mathrm{Tr}(\Pi\omega) \geq 1-\varepsilon$. For any state σ_r separable between all of Alice's systems and all of Bob's systems, and any subset $S \subseteq \{1,\dots,r\}$,

$$\mathrm{Tr}\left[\sigma_r \prod_{a\in S} \Pi_a\right] \leq d^{-|S|}. \tag{39}$$

Indeed, the marginal on S is separable, and the product test is itself a privacy test with key dimension $d^{|S|}$. For $t \geq 0$, expansion with nonnegative coefficients therefore gives

$$\mathrm{Tr}\left[\sigma_r \prod_{a=1}^r (I + (2^t-1)\Pi_a)\right] \leq \sum_{S\subseteq\{1,\dots,r\}} (2^t-1)^{|S|} d^{-|S|} = \left(1 + \frac{2^t-1}{d}\right)^r. \tag{40}$$

Measure the r tests separately, and let Z count their successes. Let P, Q be the resulting distributions for $\omega^{\otimes r}$ and σ_r. Then $\mathbb{E}_P Z = rp$, and (40) bounds $\mathbb{E}_Q 2^{tZ}$. Data processing and the classical variational inequality $D(P\|Q) \geq t\mathbb{E}_P Z - \log_2 \mathbb{E}_Q 2^{tZ}$ yield

$$D(\omega^{\otimes r}\|\sigma_r) \geq r\left[tp - \log_2\left(1 + \frac{2^t-1}{d}\right)\right]. \tag{41}$$

The classical inequality follows by comparing P with the probability distribution proportional to $2^{tZ}Q$ and using nonnegativity of relative entropy. Since $p \geq 1-\varepsilon \geq 1/d$, the supremum of the bracket over $t \geq 0$ is the binary relative entropy $d_2(p\|1/d)$. Moreover,

$$d_2(p\|1/d) = p\log_2 d + (1-p)\log_2\frac{d}{d-1} - h_2(p) \geq (1-\varepsilon)\log_2 d - h_2(\varepsilon).$$

Taking the infimum over σ_r in (41), dividing by r, and then taking $r \to \infty$ proves (38). □

5.2 Converse for adaptive protocols

To apply the privacy bound to an actual key protocol, keep the systems that each local operation would otherwise discard, and postpone the final key measurements. Public messages are still sent to Eve, and local copies of their values are retained. Tracing out these extra local systems recovers the original protocol after every step: all transmitted states, and hence all their mean energies, are unchanged. This is the usual private-state representation [HHHO09]; its energy-preserving implementation on separable Hilbert spaces is described in [DSW18, Sections II.F and IV].

Here is the error conversion. Let $|\Psi\rangle_{ABA'B'E_{\mathrm{all}}}$ be the resulting pure state, with A, B the unmeasured key registers, and let $\omega = \mathrm{Tr}_{E_{\mathrm{all}}}|\Psi\rangle\langle\Psi|$. Write $|\Psi\rangle = \sum_{a,b}|a,b\rangle|\psi_{ab}\rangle$, where the vectors $|\psi_{ab}\rangle$ need not be normalized. The post-measurement state is κ. The Fuchs–van de Graaf inequality [FvdG99] gives root fidelity at least $1-e$ between κ and its ideal key comparison. By Uhlmann's theorem [Uhl76], applied to each diagonal key block, there are normalized purifications $|\xi_a\rangle_{A'B'E_{\mathrm{all}}}$ of $\kappa_{E_{\mathrm{all}}}$, with phases chosen so that

$$\frac{1}{\sqrt{d}}\sum_a \langle\xi_a|\psi_{aa}\rangle = \sqrt{F\left(\kappa, \left(d^{-1}\sum_a |a,a\rangle\langle a,a|\right)\otimes \kappa_{E_{\mathrm{all}}}\right)} \geq 1-e.$$

We may append an unused local pure ancilla and choose a common shield space with a countably infinite-dimensional complement to each Schmidt support. The partial isometries relating purifications of the same state then extend to unitaries on this shield. Therefore $|\Gamma\rangle = d^{-1/2}\sum_a |a,a\rangle|\xi_a\rangle$ reduces to a private state γ on $AA'BB'$. Fidelity monotonicity then gives

$$F(\omega,\gamma) \geq |\langle\Gamma|\Psi\rangle|^2 \geq (1-e)^2.$$

Thus a key protocol of error e supplies an approximate private state with infidelity at most $2e-e^2$, without changing its optical inputs. For entanglement generation the target already has the private-state form, with trivial shields.

Proposition 5.2 (Finite-block converse)**.** *Consider an n-use adaptive protocol satisfying (2), whose final state has squared fidelity at least $1-\varepsilon$ with a private state of key dimension $d \geq 2$. For $0 \leq \varepsilon \leq \frac{1}{2}$,*

$$(1-\varepsilon)\log_2 d \leq n f_\eta(N) + h_2(\varepsilon). \tag{42}$$

Proof. Let $\nu_i = \mathrm{Tr}(\hat{n}\bar{\rho}_{S_i})$ be the unconditional mean energy at use i. Keep all local memories, including the registers needed for adaptivity. Corollary 4.2 applies to the state before each transmission, while the intermediate LOCC maps cannot increase E_R^∞. The initial state has zero entanglement, so telescoping gives

$$E_R^\infty(\omega_{\mathrm{final}}) \leq \sum_{i=1}^n f_\eta(\nu_i). \tag{43}$$

All the quantities E_R encountered here are finite: starting from zero, the case $m=1$ of Lemma 4.1 bounds their increase at each use, and every ν_i is finite by (2).

The function f_η is nondecreasing and concave on $[0,\infty)$. For $x>0$,

$$f_\eta''(x) = -\frac{\eta}{\ln 2\, x(x+1)(qx+1)} \leq 0, \qquad \lim_{x\to\infty} f_\eta'(x) = 0. \tag{44}$$

The derivative is therefore nonnegative; continuity covers $x=0$. Jensen's inequality and the energy budget give

$$\sum_{i=1}^n f_\eta(\nu_i) \leq n f_\eta\left(\frac{1}{n}\sum_i \nu_i\right) \leq n f_\eta(N).$$

Apply Lemma 5.1 to (43) to obtain (42). □

For operational key error e, Proposition 5.2 applies with $\varepsilon = 2e - e^2$ whenever this is at most $1/2$. For any sequence of codes with $\varepsilon_n \to 0$, (42) implies $\limsup_n n^{-1} \log_2 d_n \le f_\eta(N)$. This proves the converse for both capacities in Theorem 1.1.

5.3 Achievability

Alice prepares independent copies of the two-mode squeezed vacuum

$$|\psi_N\rangle_{RS} = \frac{1}{\sqrt{N+1}} \sum_{k\ge 0} \left(\frac{N}{N+1}\right)^{k/2} |k\rangle_R |k\rangle_S \tag{45}$$

and sends S through $\mathcal{L}_\eta$. Each transmitted mode has mean photon number N. For the output ω_{RB}, its purification RBE is pure, $\omega_R = \tau_N$, and $\omega_E = \tau_{qN}$. Hence

$$S(R)_\omega - S(RB)_\omega = g(N) - g(qN) = f_\eta(N). \tag{46}$$

The hashing inequality, with classical communication from Bob to Alice, achieves this rate [DW05, GPLS09].

Here is a finite-dimensional justification that preserves the exact energy budget. For $N > 0$, truncate (45) to $0 \le k \le L$ and normalize, obtaining $|\psi_{N,L}\rangle$. Its transmitted mean N_L is at most N and tends to N. Put $s_L = \mathrm{Tr}(\Pi_{\le L}\tau_N)$ and $\tau_{N,L} = \Pi_{\le L}\tau_N\Pi_{\le L}/s_L$. Then

$$D(\tau_{N,L}\|\tau_N) = -\log_2 s_L \longrightarrow 0, \qquad D(\mathcal{L}_q(\tau_{N,L})\|\tau_{qN}) \le -\log_2 s_L.$$

The logarithm of a positive-temperature thermal state is affine in photon number. Since the two means tend to N and qN, respectively, these bounds imply $S(\tau_{N,L}) \to g(N)$ and $S(\mathcal{L}_q(\tau_{N,L})) \to g(qN)$; for $q = 0$ the latter state is vacuum. Finite-dimensional reverse hashing therefore achieves every rate below $f_\eta(N)$. For $N = 0$ the claimed rate is zero. Finally, measuring the distilled maximally entangled states gives the same number of secret bits. Thus

$$f_\eta(N) \le Q_2(\mathcal{L}_\eta, N) \le K(\mathcal{L}_\eta, N) \le f_\eta(N),$$

which completes the proof of Theorem 1.1.

Note added and AI statement. The main result of this work was obtained on 17 September 2026 with a single prompt of ChatGPT Astra (OpenAI). While refining the manuscript, we became aware of [Pir26a], whose author independently obtained the same result.

References

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Physical Review Letters* **70**(13), 1895–1899 (1993).

[BSST02] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Transactions on Information Theory* **48**(10), 2637–2655 (2002). arXiv:quant-ph/0106052.

[CLMOW14] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Communications in Mathematical Physics* **328**(1), 303–326 (2014). arXiv:1210.4583.

[DSW18] Noah Davis, Maksim E. Shirokov, and Mark M. Wilde. Energy-constrained two-way assisted private and quantum capacities of quantum channels. *Physical Review A* **97**(6), 062310 (2018). arXiv:1801.08102.

[DW05] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A* **461**(2053), 207–235 (2005). arXiv:quant-ph/0306078.

[FvdG99] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory* **45**(4), 1216–1227 (1999). arXiv:quant-ph/9712042.

[GBW21] Martina Gschwendtner, Andreas Bluhm, and Andreas Winter. Programmability of covariant quantum channels. *Quantum* **5**, 488 (2021). arXiv:2012.00717.

[GEW16] Kenneth Goodenough, David Elkouss, and Stephanie Wehner. Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels. *New Journal of Physics* **18**(6), 063005 (2016). arXiv:1511.08710.

[GGL+04] Vittorio Giovannetti, Saikat Guha, Seth Lloyd, Lorenzo Maccone, Jeffrey H. Shapiro, and Horace P. Yuen. Classical capacity of the lossy bosonic channel: the exact solution. *Physical Review Letters* **92**(2), 027902 (2004). arXiv:quant-ph/0308012.

[GLMS03] Vittorio Giovannetti, Seth Lloyd, Lorenzo Maccone, and Peter W. Shor. Entanglement assisted capacity of the broadband lossy channel. *Physical Review Letters* **91**(4), 047901 (2003). arXiv:quant-ph/0304020.

[GPLS09] Raúl García-Patrón, Stefano Pirandola, Seth Lloyd, and Jeffrey H. Shapiro. Reverse coherent information. *Physical Review Letters* **102**(21), 210501 (2009). arXiv:0808.0210.

[Har13] Aram W. Harrow. The church of the symmetric subspace. arXiv:1308.6595 (2013).

[HHHO05a] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Locking entanglement measures with a single qubit. *Physical Review Letters* **94**(20), 200501 (2005). arXiv:quant-ph/0404096.

[HHHO05b] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters* **94**(16), 160502 (2005). arXiv:quant-ph/0309110.

[HHHO09] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory* **55**(4), 1898–1929 (2009). arXiv:quant-ph/0506189.

[HW01] Alexander S. Holevo and Reinhard F. Werner. Evaluating capacities of bosonic Gaussian channels. *Physical Review A* **63**(3), 032312 (2001). arXiv:quant-ph/9912067.

[Lin75] Göran Lindblad. Completely positive maps and entropy inequalities. *Communications in Mathematical Physics* **40**(2), 147–151 (1975).

[LS23] Ludovico Lami and Maksim E. Shirokov. Attainability and lower semi-continuity of the relative entropy of entanglement, and variations on the theme. *Annales Henri Poincaré* **24**, 4069–4137 (2023). arXiv:2105.08091.

[MLG25] Francesco Anna Mele, Ludovico Lami, and Vittorio Giovannetti. Maximum tolerable excess noise in continuous-variable quantum key distribution and improved lower bound on two-way capacities. *Nature Photonics* **19**, 329–334 (2025). arXiv:2303.12867.

[MR17] Alexander Müller-Hermes and David Reeb. Monotonicity of the quantum relative entropy under positive maps. *Annales Henri Poincaré* **18**, 1777–1788 (2017). arXiv:1512.06117.

[PGBL09] Stefano Pirandola, Raúl García-Patrón, Samuel L. Braunstein, and Seth Lloyd. Direct and reverse secret-key capacities of a quantum channel. *Physical Review Letters* **102**(5), 050503 (2009). arXiv:0809.3273.

[Pir26a] Stefano Pirandola. Energy-constrained two-way capacities of pure-loss and quantum-limited amplifier channels. arXiv:2610.06832v2 (2026).

[PLOB17] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications* **8**, 15043 (2017). arXiv:1510.08863.

[PR22] Christopher Portmann and Renato Renner. Security in quantum cryptography. *Reviews of Modern Physics* **94**(2), 025008 (2022). arXiv:2102.00021.

[TGW14] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications* **5**, 5235 (2014). arXiv:1504.06390.

[Uhl76] Armin Uhlmann. The "transition probability" in the state space of a $*$-algebra. *Reports on Mathematical Physics* **9**(2), 273–279 (1976).

[VP98] Vlatko Vedral and Martin B. Plenio. Entanglement measures and purification procedures. *Physical Review A* **57**(3), 1619–1633 (1998). arXiv:quant-ph/9707035.

[VPRK97] Vlatko Vedral, Martin B. Plenio, M. A. Rippin, and Peter L. Knight. Quantifying entanglement. *Physical Review Letters* **78**(12), 2275–2279 (1997). arXiv:quant-ph/9702027.

[WPG+12] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics* **84**(2), 621–669 (2012). arXiv:1110.3234.

[WHG12] Mark M. Wilde, Patrick Hayden, and Saikat Guha. Quantum trade-off coding for bosonic communication. *Physical Review A* **86**(6), 062306 (2012). arXiv:1105.0119.

[WQ18] Mark M. Wilde and Haoyu Qi. Energy-constrained private and quantum capacities of quantum channels. *IEEE Transactions on Information Theory* **64**(12), 7802–7827 (2018). arXiv:1609.01997.

[WTB17] Mark M. Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory* **63**(3), 1792–1817 (2017). arXiv:1602.08898.