Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels

K. Goodenough,[*] D. Elkouss, and S. Wehner
QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands

One of the most sought-after goals in experimental quantum communication is the implementation of a quantum repeater. The performance of quantum repeaters can be assessed by comparing the attained rate with the quantum and private capacity of direct transmission, assisted by unlimited classical two-way communication. However, these quantities are hard to compute, motivating the search for upper bounds. Takeoka, Guha and Wilde found the squashed entanglement of a quantum channel to be an upper bound on both these capacities. In general it is still hard to find the exact value of the squashed entanglement of a quantum channel, but clever sub-optimal squashing channels allow one to upper bound this quantity, and thus also the corresponding capacities. Here, we exploit this idea to obtain bounds for any phase-insensitive Gaussian bosonic channel. This bound allows one to benchmark the implementation of quantum repeaters for a large class of channels used to model communication across fibers. In particular, our bound is applicable to the realistic scenario when there is a restriction on the mean photon number on the input. Furthermore, we show that the squashed entanglement of a channel is convex in the set of channels, and we use a connection between the squashed entanglement of a quantum channel and its entanglement assisted classical capacity. Building on this connection, we obtain the exact squashed entanglement and two-way assisted capacities of the d-dimensional erasure channel and bounds on the amplitude-damping channel and all qubit Pauli channels. In particular, our bound improves on the previous best known squashed entanglement upper bound of the depolarizing channel.

I. INTRODUCTION

Optical quantum communication over long distances suffers from innate losses [1–5]. While in a classical setting the signal can be amplified at intermediate nodes to counteract this loss, this is prohibited in a quantum setting due to the no-cloning theorem [6]. This problem can be overcome by implementing a quantum repeater, allowing entanglement over larger distances [7, 8]. The successful implementation of a quantum repeater will form an important milestone in the development of a quantum network [9]. At this stage however, physical implementations perform worse than direct transmission [10, 11]. As the experimental results improve it will be necessary to evaluate whether or not an implementation has achieved a rate not possible via direct communications. This can be done by comparing the attainable rate *with* a quantum repeater [12–19] to the capacity of the associated quantum channel (i.e. direct transmission) for that task. For future quantum networks, arguably the two most relevant tasks are the transmission of quantum information and private classical communication. The capacity of a quantum channel for these two tasks, assuming that we allow the communicating parties to freely exchange classical communication, is given by the two-way assisted quantum and private capacity. We denote these quantities by $Q_2(\mathcal{N})$ and $P_2(\mathcal{N})$, respectively.

Finding exact values for $Q_2(\mathcal{N})$ and $P_2(\mathcal{N})$, however, is highly nontrivial thus motivating the search for upper bounds for them [20]. After having shown that the squashed entanglement of a channel is a quantity that is such an upper bound [21], Takeoka, Guha and Wilde showed that there is a fundamental rate-loss trade-off in quantum key distribution and entanglement distillation over practical channels [22].

The squashed entanglement $E_{\mathrm{sq}}(A;B)_\rho$ of a bipartite state ρ_{AB} is a quantity defined as

$$E_{\mathrm{sq}}(A;B)_\rho := \frac{1}{2} \inf_{\mathcal{S}_{E\to E'}} I(A;B|E') , \qquad (1)$$

which was introduced by Christandl and Winter [23] as an entanglement measure for a bipartite state. The squashed entanglement can be interpreted as the environment E holding some purifying system of ρ_{AB}, and then squashing the correlations between A and B as much as possible by applying a channel $\mathcal{S}_{E\to E'}$ that minimizes the conditional mutual information $I(A;B|E')$. Extending this idea from states to channels, Takeoka, Guha and Wilde [21, 22] defined the squashed entanglement $E_{\mathrm{sq}}(\mathcal{N})$ of a quantum channel as the maximum squashed entanglement that can be achieved between A and B,

$$E_{\mathrm{sq}}(\mathcal{N}) := \max_{|\psi\rangle_{AA'}} E_{\mathrm{sq}}(A;B)_\rho , \qquad (2)$$

where $\rho_{AB} = \mathcal{N}_{A'\to B}(|\psi\rangle\langle\psi|_{AA'})$ is the state shared between Alice and Bob after the A' system is sent through the channel $\mathcal{N}_{A'\to B}$. They showed that $E_{\mathrm{sq}}(\mathcal{N})$ is an upper bound on the two two-way assisted capacities.

Unfortunately, there is no known algorithm for computing the squashed entanglement of a channel. This is partially due to the fact that the dimension of E' is *a priori* unbounded and that computing the squashed entanglement of a state is already an NP-hard problem [24] and thus might even be uncomputable. However, fixing the channel in (1) in general yields an upper

[*] kdgoodenough@gmail.com

bound on $E_{\text{sq}}(\mathcal{N})$. Exploiting this idea of fixing a specific "squashing channel" $\mathcal{S}_{E\to E'}$, Takeoka et al. derived upper bounds on the squashed entanglement of several channels. Notably, they used this technique to find an upper bound for the pure-loss bosonic channel.

The main contribution of this paper is an upper bound applicable to all phase-insensitive Gaussian bosonic channels. We apply this bound to the pure-loss channel, the additive noise channel and the thermal channel.

Additionally, we obtain results for finite-dimensional channels by using tools that we develop here. The first of these consists of a concrete squashing channel that we call the trivial squashing channel which can be connected with the entanglement-assisted capacity. This connection, first observed by Takeoka et al. (see [25]), allows us to compute the exact two-way assisted capacities of the d-dimensional erasure channel, and bounds on the amplitude damping channel and general Pauli channels. Second, the squashed entanglement of entanglement breaking channels is zero. Third, for channels that can be written as a convex sum of channels the convex sum of the squashed entanglement of each channel is an upper bound, i.e. $E_{\text{sq}}(\mathcal{N})$ is convex on the set of channels. We combine all three of these tools to obtain bounds for the qubit depolarizing channel.

II. NOTATION

In this section we lay out the notation and conventions that we follow in this paper.

For a quantum state ρ_A the von Neumann entropy of ρ_A is defined as $H(A) = -\mathsf{tr}\rho_A \log \rho_A$. For convenience we take all logarithms in base two and set $\log_2(\cdot) \equiv \log(\cdot)$. For a quantum state $\rho := \rho_{AB}$ the conditional entropy of system A given B is defined as $H(A|B)_\rho = H(AB)\rho - H(B)_\rho$. Here $H(B)$ is computed over the state $\rho_B = \mathsf{tr}_A(\rho_{AB})$, where we denote the partial trace over system A of a state ρ_{AB} by $\mathsf{tr}_A(\rho_{AB})$. For a tripartite state ρ_{ABE} the conditional mutual information is defined as $I(A;B|E) = H(A|E) - H(A|BE)$. Whenever there is confusion regarding the state over which we are computing an entropic quantity we will add the state as a subscript.

A quantum channel $\mathcal{N}_{A'\to B}$ is a completely positive and trace preserving map [26] between linear operators on Hilbert spaces $\mathcal{H}_{A'}$ and $\mathcal{H}_B$. A quantum channel $\mathcal{N}$ can always be embedded into an isometry $V^{\mathcal{N}}_{A'\to BE}$ that takes the input to the output system B together with an auxiliary system E that we call the environment. This isometry is called the Stinespring dilation of the channel. The action of the channel is recovered by tracing out the environment: $\mathcal{N}(\rho) = \mathsf{tr}_E(V\rho V^*)$.

We denote the d-dimensional maximally mixed state by π. The dimension of π is implicit and should be clear from the context. Let $\mathcal{N}$ be a channel with input and output dimension d. Then $\mathcal{N}$ is unital if $\mathcal{N}(\pi) = \pi$.

III. SOME PROPERTIES OF $E_{\text{sq}}(\mathcal{N})$

In this section we prove several properties of $E_{\text{sq}}(\mathcal{N})$ that will be of general use for obtaining upper bounds on the squashed entanglement of concrete channels. First we define a squashing channel that we call the trivial squashing channel and connect it to the entanglement assisted capacity of that channel, an observation previously made in [25] by Takeoka et al. Second, we prove that the squashed entanglement of entanglement breaking channels is zero. The third property is that $E_{\text{sq}}(\mathcal{N})$ is convex in the set of channels.

A. The trivial squashing channel

One possible squashing channel $\mathcal{S}_{E\to E'}$ is the identity channel, which we will call the trivial squashing channel. The state on ABE' is pure, from which it can easily be calculated that

$$\begin{aligned}
E_{\text{sq}}(\mathcal{N}) &\leq \max_{|\phi\rangle_{AA'}} \frac{1}{2} I(A;B|E) && (3)\\
&= \max_{|\phi\rangle_{AA'}} \frac{1}{2}(H(A|E) - H(A|BE)) && (4)\\
&= \max_{|\phi\rangle_{AA'}} \frac{1}{2}(H(AE) - H(E) \\
&\quad - H(ABE) + H(BE)) && (5)\\
&= \max_{|\phi\rangle_{AA'}} \frac{1}{2}(H(B) + H(A) - H(AB)) && (6)\\
&= \max_{|\phi\rangle_{AA'}} \frac{1}{2} I(A;B)\ . && (7)
\end{aligned}$$

The maximization in the right hand of (7), up to the 1/2 factor, characterizes the capacity of a quantum channel for transmitting classical information assisted by unlimited entanglement [27]. In other words, the squashed entanglement is bounded from above by one half the entanglement assisted capacity of the channel which we denote by $C_E(\mathcal{N})$. This connection, which was first observed by Takeoka et al. (see [25]), allows us to bound the squashed entanglement for all channels for which $C_E(\mathcal{N})$ is known.

B. Entanglement breaking channels

Entanglement breaking channels have zero private and quantum capacities assisted by two-way communications. We show that the squashed entanglement of these channels is also zero, following a similar approach as was done for the squashed entanglement of separable states in [28]. In order to see this note that if an entanglement breaking channel $\mathcal{N}_{\text{EB}}$ is applied to half of a bipartite state, the output is always separable and can be written as a convex combination of product states,

$$\psi_{AB} = \mathcal{I} \otimes \mathcal{N}_{\mathrm{EB}}(|\psi\rangle\langle\psi|_{AA'}) \tag{8}$$

$$= \sum_i \lambda_i |\alpha_i\rangle\langle\alpha_i|_A \otimes |\beta_i\rangle\langle\beta_i|_B , \tag{9}$$

where we denote by $\mathcal{I}$ the identity map. A possible purification of ψ_{AB} is

$$|\psi\rangle_{ABE_1E_2} = \sum_i \sqrt{\lambda}_i |\alpha_i\rangle_A |\beta_i\rangle_B |i\rangle_{E_1} |i\rangle_{E_2} , \tag{10}$$

where $\{|i\rangle_{E_1}\}$ and $\{|i\rangle_{E_2}\}$ are sets of orthonormal states. If the squashing channel consists of tracing out the E_2 system, the resulting state is

$$\sum_i \lambda_i |\alpha_i\rangle\langle\alpha_i|_A \otimes |\beta_i\rangle\langle\beta_i|_B \otimes |i\rangle\langle i|_{E_1} , \tag{11}$$

which has zero conditional mutual information.

C. Convexity of $E_{\mathrm{sq}}(\mathcal{N})$ in the set of channels

The squashed entanglement of the channel is convex in the set of channels. We prove this in the Appendix following similar ideas to the ones used in [23] to prove that the squashed entanglement is convex in the set of states. Hence, if $\mathcal{N} = \sum_j p_j \mathcal{N}_j$ with $\sum_j p_j = 1$ and $p_j \geq 0$, then

$$E_{\mathrm{sq}}(\mathcal{N}) \leq \sum_j p_j E_{\mathrm{sq}}(\mathcal{N}_j) . \tag{12}$$

IV. FINITE-DIMENSIONAL CHANNELS

To build intuition before moving to bosonic channels, let us first bound the squashed entanglement of finite-dimensional channels, i.e. channels where both the input and output dimensions are finite.

An illustrative example of the effectiveness of the trivial squashing channel is the d-dimensional erasure channel $\mathcal{E}_p^d(\rho) = (1-p)\rho + p|e\rangle\langle e|$, where ρ is a $d-$dimensional state and $|e\rangle$ is an erasure flag orthogonal to the support of any ρ on the input [26]. It is well known that $C_E(\mathcal{E}_p^d) = 2(1-p)\log(d)$ [26] and that $Q_2(\mathcal{E}_p^d) = (1-p)\log(d)$ [29]. In general we have

$$Q_2(\mathcal{N}) \leq P_2(\mathcal{N}) \leq E_{\mathrm{sq}}(\mathcal{N}) \leq \frac{1}{2} C_E(\mathcal{N}) , \tag{13}$$

where the first inequality holds since the squashed entanglement of a channel is an upper bound on $Q_2(\mathcal{N})$ and the second inequality follows from applying the trivial squashing channel. In the specific case of the erasure channel, we then must have that

$$Q_2(\mathcal{E}_p^d) = P_2(\mathcal{E}_p^d) = E_{\mathrm{sq}}(\mathcal{E}_p^d) = (1-p)\log(d) . \tag{14}$$

That is, the trivial squashing channel is the *optimal* squashing channel, yielding both two-way assisted capacities and the squashed entanglement of the d-dimensional erasure channel. We note that, up until now, this class of channels is the only class whose squashed entanglement has been calculated exactly. Independently of our work, in [30] the two-way assisted capacities of the d-dimensional erasure channel are established by computing the entanglement flux of the channel, which is also an upper bound on P_2.

A second channel we can apply the trivial isometry to is the qubit damping channel $\mathcal{N}_{AD}^{\gamma}$, a channel that models energy dissipation in two-level systems. The qubit amplitude damping channel is defined as

$$\mathcal{N}_{AD}^{\gamma}(\rho) := \sum_{i=0}^{1} A_i \rho A_i^{\dagger} , \tag{15}$$

where

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} , \; A_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \tag{16}$$

with amplitude damping parameter $\gamma \in [0,1]$. Since the entanglement assisted classical capacity of the amplitude damping channel is known [26] to be equal to

$$C_E(\mathcal{N}_{AD}^{\gamma}) = \max_{p \in \{0,1\}} [h(p) + h((1-\gamma)p) - h(\gamma p)] , \tag{17}$$

where $h(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary entropy, we immediately find the bound

$$P_2(\mathcal{N}_{AD}^{\gamma}) \leq E_{\mathrm{sq}}(\mathcal{N}_{AD}^{\gamma}) \leq \frac{1}{2} C_E(\mathcal{N}_{AD}^{\gamma}) . \tag{18}$$

A comparison of this bound with the best known lower bound, given by the reverse coherent information (RCI) $\max_p[h(p) - h(p\gamma)]$, and an upper bound $P_2(\mathcal{N}_{AD}^{\gamma}) \leq \min\{1, -\log\gamma\}$ found by Pirandola et al. [31] using an entanglement flux approach, can be seen in Figure 1.

A third interesting example are d-dimensional unital channels for which the maximally entangled state on AA' maximizes the mutual information $I(A;B)$. For these channels the trivial squashing channel gives the following compact upper bound

$$E_{\mathrm{sq}}(\mathcal{N}) \leq \frac{1}{2} I(A;B) \tag{19}$$

$$= \frac{1}{2}[H(A) + H(B) - H(AB)] \tag{20}$$

$$= \log(d) - \frac{1}{2} H(E) . \tag{21}$$

In particular, this bound holds for any Pauli channel, where we have that $d = 2$. Any Pauli channel can be written as

$$\mathcal{P}(\rho) = p_0\rho + p_1 X\rho X + p_2 XZ\rho ZX + p_3 Z\rho Z , \tag{22}$$

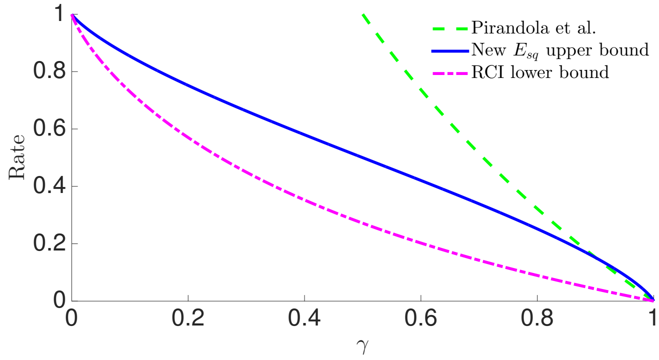

FIG. 1. Comparison of bounds for the amplitude damping channel. In dashed green the upper bound by Pirandola et al. [31], in solid blue the upper bound found in this paper and the dash-dotted magenta line is a lower bound given by the reverse coherent information [32].

with $\sum_{i=0}^{3} p_i = 1$. Choosing without loss of generality the maximally entangled state $|\Phi^+\rangle_{AA'} = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]_{AA'}$ as input on AA', we see that the output has a purification of the form

$$\sqrt{p_0}\,|\Phi^+\rangle_{AB}\,|00\rangle_E + \sqrt{p_1}\,|\Psi^+\rangle_{AB}\,|01\rangle_E + \sqrt{p_2}\,|\Psi^-\rangle_{AB}\,|10\rangle_E + \sqrt{p_3}\,|\Phi^-\rangle_{AB}\,|11\rangle_E \ . \tag{23}$$

From orthogonality of the Bell states, it can be seen that the entropy of the environment coincides with the classical entropy of the probability vector $\overline{p} = (p_0, p_1, p_2, p_3)$. That is, $H(E) = H(\overline{p})$ with $H(\overline{p}) \equiv -\sum_{i=0}^{3} p_i \log p_i$. From this it follows that

$$E_{\rm sq}(\mathcal{P}) \leq 1 - \frac{1}{2}H(\overline{p}) \ . \tag{24}$$

Hence, we also obtain that $2 - H(\overline{p})$ is the entanglement assisted classical capacity of a Pauli channel $\mathcal{P}$.

Let us now apply the bound for Pauli channels to a concrete channel, the (binary) depolarizing channel $\mathcal{D}_p$. The action of this channel is $\mathcal{D}_p(\rho) \equiv (1-p)\rho + p\pi$ for $p \in [0,1]$. This corresponds with the Pauli channel given by $\overline{p} = (1 - \frac{3p}{4}, \frac{p}{4}, \frac{p}{4}, \frac{p}{4})$. After this identification we find that

$$E_{\rm sq}(\mathcal{D}_p) \leq \frac{3p\log(p) + (4-3p)\log(4-3p)}{8} \ . \tag{25}$$

The depolarizing channel can also be written as a convex combination of two other depolarizing channels, allowing us to use the convexity of $E_{\rm sq}(\mathcal{N})$ in the set of channels to improve on the upper bound in equation (25). We can compute the squashed entanglement of each individual channel and multiply it by the appropriate weight. Using this idea (see section 2 in the Appendix), we obtain the following stronger upper bound

$$E_{\rm sq}(\mathcal{D}_p) \leq \min_{0 \leq \epsilon \leq p} (1-\alpha)\frac{3\epsilon\log(\epsilon) + (4-3\epsilon)\log(4-3\epsilon)}{8} \ . \tag{26}$$

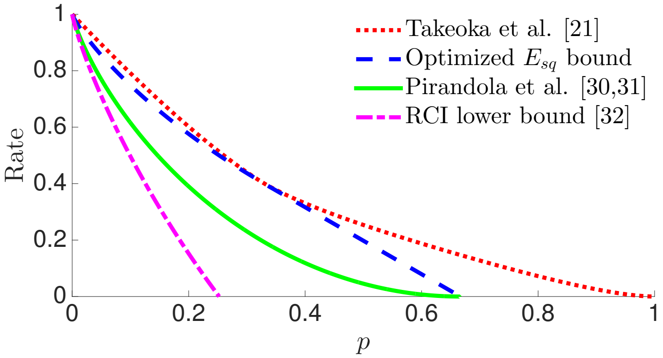

FIG. 2. Comparison of bounds for the depolarizing channel. The dotted red line is the upper bound by Takeoka et al. [21], the dashed blue line is the optimized squashed entanglement bound in this paper, the solid green line is the entanglement flux upper bound by Pirandola et al. [30, 31] and the magenta line is a lower bound given by the reverse coherent information [32].

where $\alpha = \frac{p-\epsilon}{2/3-\epsilon}$. This bound is equal to (25) for $0 \leq p \lesssim \frac{1}{3}$, after which it linearly goes to zero at $p = \frac{2}{3}$. See Figure 2 for a comparison of this new bound, the bound by Takeoka et al. [21, 33], the bound by Pirandola et al. [31], and the reverse coherent information [32].

V. PHASE-INSENSITIVE GAUSSIAN BOSONIC CHANNELS

A. An upper bound on phase-insensitive channels

In this section we discuss our main result, an upper bound on the squashed entanglement of any phase-insensitive Gaussian bosonic channel. Gaussian bosonic channels are of interest because they are used to model a large class of relevant operations on bosonic systems [34]. Phase-insensitive channels are those Gaussian bosonic channels which add equal noise in each quadrature of the bosonic systems. Imperfections in experimental setups for quantum communication with photons are modeled by phase-insensitive channels, motivating us to upper bound the squashed entanglement of all such channels. In particular this motivates the search for bounds where the input of the channel has a constraint on the mean photon number N.

Any phase-insensitive channel $\mathcal{N}_{\rm PI}$ is completely characterized by its a loss/gain parameter τ and noise parameter ν. The Stinespring dilation of such a channel consists of a beamsplitter with transmissivity $T = \frac{2\tau}{\tau+\nu+1}$ interacting with the vacuum on E_1, and a two-mode squeezer with squeezing parameter $r = \text{acosh}(\sqrt{G})$ with the amplification $G = \frac{\tau+\nu+1}{2} \geq 1$ interacting with the vacuum on E_2 [35] (see Figure 3 and the Appendix for a detailed definition of the channel). T and G also completely characterize any phase-insensitive channel. Takeoka et al. [21, 22, 33] found bounds for such channels by only considering the beamsplitter part of the Stinespring dilation. To be a valid channel, we must have that $\nu \geq |1-\tau|$. We further have that phase-insensitive channels are entanglement breaking whenever $\nu \geq \tau + 1$ [36], or equivalently, $G(1-T) \geq 1$. Hence, the squashed entanglement must be zero for channels with such parameters as discussed in the tools section.

Since we are interested in phase-insensitive Gaussian channels, we make the ansatz that a good squashing map will be a phase-insensitive channel. Numerical work suggests that, if only phase-insensitive isometries are considered, the pure-loss channel and the amplification channel separately have as optimal squashing isometry the balanced beamsplitter interacting with the vacuum. This motivates us to use the isometry consisting of two balanced beamsplitters at the outputs of the first beamsplitter and the two-mode squeezer (see Figure 3). Using this isometry we obtain a bound for all phase-insensitive channels with restricted mean photon number N (see Appendix for a derivation and a proof that the equation is monotonically non-decreasing as a function of N). This equation equals

$$g\left(\left(\nu_{BE_1'E_2'}\right)_1\right) + g\left(\left(\nu_{BE_1'E_2'}\right)_2\right) - g\left(\left(\nu_{E_1'E_2'}\right)_1\right) - g\left(\left(\nu_{E_1'E_2'}\right)_2\right) , \tag{27}$$

with $g(x) = \left(\frac{x+1}{2}\right)\log(\frac{x+1}{2}) - \left(\frac{x-1}{2}\right)\log(\frac{x-1}{2})$ [34] and

$$\begin{aligned}
\left(\nu_{E_1'E_2'}\right)_1 &= \left|\sqrt{-\tfrac{1+G^2+2N(1-T+GT(G-1))+N^2(GT-1)^2+(G-1+N(GT-1))\Omega^-}{2}}\right| \\
\left(\nu_{E_1'E_2'}\right)_2 &= \left|\sqrt{-\tfrac{1+G^2+2N(1-T+GT(G-1))+N^2(GT-1)^2-(G-1+N(GT-1))\Omega^-}{2}}\right| \\
\left(\nu_{BE_1'E_2'}\right)_1 &= \left|\sqrt{-\tfrac{1+G^2+2N(1-T+GT(G+1))+N^2(1+GT)^2+(1+G+N(1+GT))\Omega^+}{2}}\right| \\
\left(\nu_{BE_1'E_2'}\right)_2 &= \left|\sqrt{-\tfrac{1+G^2+2N(1-T+GT(G+1))+N^2(1+GT)^2-(1+G+N(1+GT))\Omega^+}{2}}\right|
\end{aligned}$$

where we have set

$$\Omega^{\pm} = \sqrt{(1+N)^2 - 4NT \pm 2G(1+N)(NT-1) + (G+GNT)^2} \; . \tag{28}$$

As $N \to \infty$, the bound above converges to its maximum value of

$$E_{\text{sq}}\left(\mathcal{N}_{\text{PI}}\right) \leq \frac{\left(1-T^2\right) G \log(\frac{1+T}{1-T}) - \left(G^2-1\right) T \log(\frac{G+1}{G-1})}{1-G^2T^2} , \tag{29}$$

Rewriting the upper bound as function of the channel parameters τ and ν [34] we obtain the upper bound

$$E_{\text{sq}}\left(\mathcal{N}_{\text{PI}}\right) \leq \frac{\zeta(1+\nu+3\tau, 1+\nu-\tau) - \tau\zeta(\tau+\nu+3, \tau+\nu-1)}{2(1+\nu+\tau)(1-\tau^2)} , \tag{30}$$

where $\zeta(a,b) = ab\log(\frac{a}{b})$.

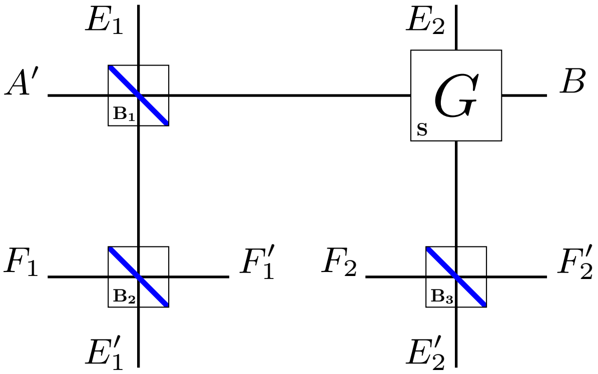

FIG. 3. A squashing isometry for any phase-insensitive Gaussian channel $\mathcal{N}_{\text{PI}}$ taking A' to B. The beamsplitter $\mathbf{B_1}$ and the two-mode squeezer $\mathbf{S}$ form the Stinespring dilation, while the balanced beamsplitters $\mathbf{B_2}$ and $\mathbf{B_3}$ form the squashing map. The beamsplitter $\mathbf{B}_1$ interacts with the vacuum on E_1 and A, and the two-mode squeezer $\mathbf{S}$ interacts with the output of $\mathbf{B}_2$ and the vacuum on E_2. The squashing isometry consists of two balanced beamsplitters $\mathbf{B_2}$ and $\mathbf{B_3}$ interacting with the vacuum on F_1 and F_2 and the output of the beamsplitter $\mathbf{B}_1$ and the two-mode squeezer $\mathbf{S}$.

B. Application to concrete phase-insensitive Gaussian channels with unconstrained photon input

1. *Quantum-limited phase-insensitive channels*

A pure-loss channel has $G = 1$. As a consequence, for pure-loss channels the bound in equation (29) reduces to $\log(\frac{1+T}{1-T})$. This bound coincides with the bound found by Takeoka et al.

In the opposite extreme we find quantum-limited amplifying channels, that is channels with $T = 1$ and $G > 1$. For these channels, the bound by Takeoka is equal to infinity while (29) is non-trivial. Concretely, it reduces to the finite value of $\log(\frac{G+1}{G-1})$. This should be compared with the exact capacities independently found by Pirandola et al. [30, 31, 37] using an entanglement flux approach, $Q_2 = P_2 = \log(\frac{G}{G-1})$.

2. *Additive noise channel*

An additive noise channel only adds noise to the input, without damping or amplifying the signal. For an additive noise channel $\mathcal{N}_{\text{add}}$ we have $T = \frac{1}{\overline{n}+1}$ and $G = \frac{1}{T} = \overline{n} + 1$, where $\overline{n}$ is the noise variance. Taking the limit of equation (29) as $G \to \frac{1}{T} = \overline{n} + 1$ we show in the Appendix that the upper bound becomes

$$\begin{aligned}
E_{\text{sq}}\left(\mathcal{N}_{\text{add}}\right) &\leq \frac{T^2+1}{2T}\log(\frac{1+T}{1-T}) - \frac{1}{\ln 2} &(31)\\
&= \frac{\overline{n}^2+2\overline{n}+2}{2\overline{n}+2}\log(\frac{\overline{n}+2}{\overline{n}}) - \frac{1}{\ln 2} \; . &(32)
\end{aligned}$$

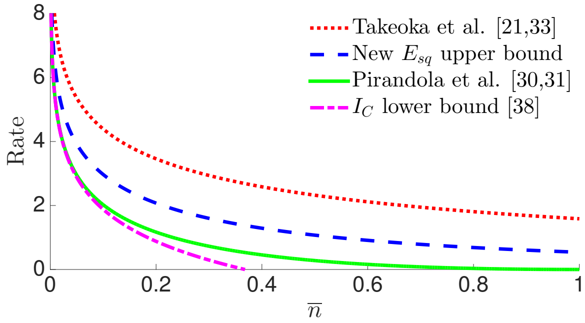

FIG. 4. Comparison of the upper bounds mentioned in this paper for the additive noise channel. The dotted red line is the upper bound by Takeoka et al. [21], the dashed blue line is the squashed entanglement bound in this paper, the solid green line is the entanglement flux upper bound by Pirandola et al. [30, 31] and the magenta line is the coherent information of the channel which is a lower bound [38].

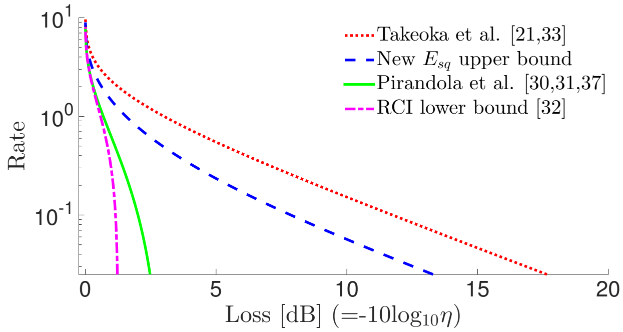

FIG. 5. Bounds on the squashed entanglement of the thermal channel with $N_B = 1$ as a function of the loss in dB. The red dotted line shows the upper bound by Takeoka et al. [21, 33], the dashed blue line the new bound reported in this paper, in solid green the bound by Pirandola et al. [30, 31, 37], and the dash-dotted line shows the reverse coherent information [32] which is a lower bound.

This should be compared with the upper bound independently found by Pirandola et al. [30, 31, 37], $\frac{\overline{n}-1}{\ln(2)} - \log \overline{n}$ and the coherent information $I_C(\mathcal{N}_{\text{add}}) = -\frac{1}{\ln(2)} - \log \overline{n}$ which is a lower bound on $P_2(\mathcal{N})$ [38]. See Figure 4 for a comparison of these bounds.

3. Thermal channel

A thermal channel is similar to the pure-loss channel, but instead of the input interacting with a vacuum state on a beamsplitter of transmissivity τ, it interacts with a thermal state with mean photon number N_B. For a thermal channel we have that $G = (1-\eta)N_B + 1$ and $T = \frac{\eta}{(1-\eta)N_B+1}$. In Figure 5 the upper bound is plotted for $N_B = 1$ together with two other bounds and the reverse coherent information, which is a lower bound on $P_2(\mathcal{N})$ [32].

4. Non-quantum limited noise for lossy channels

In experimental setups one does not measure ν, but the additional noise $\chi \geq 0$. We have the relation $\nu = 1-\tau+\chi$ where $1-\tau$ is the minimum amount of noise that will be introduced for a loss τ (the quantum-limited noise) [34]. The upper bound from (30) can then be rewritten as

$$\frac{\zeta(\chi+2+2\tau, \chi+2-2\tau) - \tau\zeta(\chi+4,\chi)}{(4+2\chi)(1-\tau^2)} \,. \tag{33}$$

C. Finite-energy bounds

For low mean photon number and certain parameter ranges the finite-energy bound in equation (27) is tighter than previous upper bounds on the two-way assisted capacities. For any energy the pure-loss bound from Takeoka et al. [21, 33] and equation (86) coincide. In Figure 6 the bound from Takeoka et al. [21, 33], is shown for an average photon number of $N = 0.1$ [39, 40] and the two-way assisted private capacity of the pure-loss channel [30, 31, 37]. The loss-parameter runs from 0 to $2 \cdot 10^{-20}$, which is the expected range of losses for fiber lengths of around 1000 kilometers. In Figure 7 we plot the upper bound by Pirandola et al. [30, 31, 37], the finite-energy bounds of Takeoka et al. [21, 33], and equation (86) for the thermal channel with $N_B = 1$. Note that the finite-energy bounds are zero only for $\eta = 0$, while the upper bound by Pirandola et al. [30, 31, 37] equals zero for $\eta \leq \frac{N_b}{N_b+1}$.

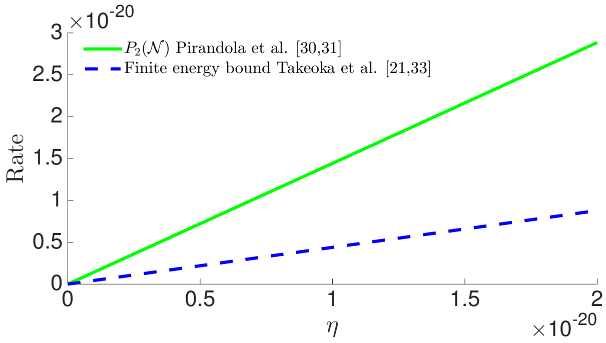

FIG. 6. Bound for the pure-loss channel with an average photon number of 0.1 and the secret key capacity [30, 31] as a function of η. The new bound in this paper coincides with the finite-energy variant of the bound by Takeoka et al., see [21, 22]. The loss parameter η ranges from 0 to $2 \cdot 10^{-20}$, which is the range of expected losses for transmissions across fibers with length $\approx$ 1000 km with an attenuation length of 22 km.

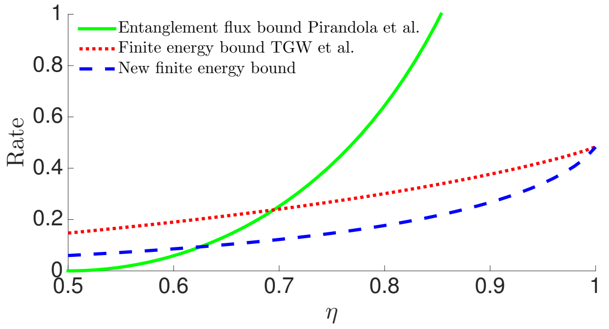

FIG. 7. Comparison of the upper bound found by Pirandola et al. [30, 31, 37] for the thermal channel with $N_B = 1$ and the two squashed entanglement finite-energy bounds with average photon number of 0.1 as a function of the loss-parameter η [21, 33].

VI. CONCLUSION

In this paper we have obtained bounds on the two-way assisted capacities of several relevant channels using the squashed entanglement of a quantum channel. For practical purposes, the most relevant of the channels considered are phase-insensitive Gaussian channels. Our bound for these channels is always nonzero, even when the corresponding channel is entanglement-breaking. This points to the existence of an even better squashing channel for phase-insensitive Gaussian channels. Future work could investigate this intriguing avenue, especially due to its relevance to the squashed entanglement of a bipartite state as an entanglement measure.

Furthermore, we have proven the exact two-way assisted capacities and the squashed entanglement of the d-dimensional erasure channel, improved the previous best known upper bound on the amplitude-damping channel and derived a squashed entanglement bound for general qubit Pauli channels. In particular, our bound applies to the depolarizing channel and improves on the previous best known squashed entanglement upper bound.

The only credible way to claim whether an implementation of a quantum repeater is good enough is by achieving a rate not possible by direct communication. Our bounds take special relevance in this context, especially for realistic energy constraints.

VII. ACKNOWLEDGEMENTS

KG, DE and SW acknowledge support from STW, Netherlands, an ERC Starting Grant and an NWO VIDI Grant. We would like to thank Mark M. Wilde and Stefano Pirandola for discussions regarding this project. We also thank Marius van Eck, Jonas Helsen, Corsin Pfister, Andreas Reiserer and Eddie Schoute for helpful comments regarding an earlier version of this paper.

[1] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache *et al.*, “Field test of classical symmetric encryption with continuous variables quantum key distribution,” *Optics Express*, vol. 20, no. 13, pp. 14 030–14 041, 2012.

[2] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, “Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of tokyo metropolitan area,” *Lightwave Technology, Journal of*, vol. 32, no. 1, pp. 141–151, 2014.

[3] A. Dixon, J. Dynes, M. Lucamarini, B. Fröhlich, A. Sharpe, A. Plews, S. Tam, Z. Yuan, Y. Tanizawa, H. Sato *et al.*, “High speed prototype quantum key distribution system and long term field trial,” *Optics express*, vol. 23, no. 6, pp. 7583–7592, 2015.

[4] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, “High-rate measurement-device-independent quantum cryptography,” *Nature Photonics*, 2015.

[5] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photonics*, 2015.

[6] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[7] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum repeaters: The role of imperfect local operations in quantum communication,” *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[8] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, “Long-distance quantum communication with atomic ensembles and linear optics,” *Nature*, vol. 414, no. 6862, pp. 413–418, 2001.

[9] S. Perseguers, G. Lapeyre Jr, D. Cavalcanti, M. Lewenstein, and A. Acín, “Distribution of entanglement in large-scale quantum networks,” *Reports on Progress in Physics*, vol. 76, no. 9, p. 096001, 2013.

[10] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, “Quantum repeaters based on atomic ensembles and linear optics,” *Reviews of Modern Physics*, vol. 83, no. 1, p. 33, 2011.

[11] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan, “Experimental demonstration of a bdcz quantum repeater node,” *Nature*, vol. 454, no. 7208, pp. 1098–1101, 2008.

[12] S. Bratzik, H. Kampermann, and D. Bruß, “Secret key rates for an encoded quantum repeater,” *Physical Review A*, vol. 89, no. 3, p. 032335, 2014.

[13] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, “Ultrafast and fault-tolerant quantum communication across long distances,” *Physical review letters*, vol. 112, no. 25, p. 250501, 2014.

[14] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature communications*, vol. 6, 2015.

[15] H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon *et al.*, "Practical quantum repeaters with parametric down-conversion sources," *arXiv preprint arXiv:1505.03470*, 2015.

[16] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 21, no. 3, pp. 1–13, 2015.

[17] N. L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 21, no. 3, pp. 1–8, 2015.

[18] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, "Overcoming lossy channel bounds using a single quantum repeater node," *arXiv preprint arXiv:1508.02811*, 2015.

[19] A. Khalique and B. C. Sanders, "Practical long-distance quantum key distribution through concatenated entanglement swapping with parametric down-conversion sources," *arXiv preprint arXiv:1501.03317*, 2015.

[20] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure key from bound entanglement," *Physical review letters*, vol. 94, no. 16, p. 160502, 2005.

[21] M. Takeoka, S. Guha, and M. M. Wilde, "The squashed entanglement of a quantum channel," *Information Theory, IEEE Transactions on*, vol. 60, no. 8, pp. 4987–4998, 2014.

[22] ——, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nature communications*, vol. 5, 2014.

[23] M. Christandl and A. Winter, "Squashed entanglement: An additive entanglement measure," *Journal of mathematical physics*, vol. 45, no. 3, pp. 829–840, 2004.

[24] Y. Huang, "Computing quantum discord is np-complete," *New Journal of Physics*, vol. 16, no. 3, p. 033027, 2014.

[25] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, "The quantum reverse shannon theorem and resource tradeoffs for simulating quantum channels," *Information Theory, IEEE Transactions on*, vol. 60, no. 5, pp. 2926–2959, 2014.

[26] M. M. Wilde, *Quantum information theory.* Cambridge University Press, 2013.

[27] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Physical Review Letters*, vol. 83, no. 15, p. 3081, 1999.

[28] M. Christandl, "The structure of bipartite quantum states," Ph.D. dissertation, University of Cambridge, 2006.

[29] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, "Capacities of quantum erasure channels," *Physical Review Letters*, vol. 78, no. 16, p. 3217, 1997.

[30] S. Pirandola and R. Laurenza, "General benchmarks for quantum repeaters," *arXiv preprint arXiv:1512.04945*, 2015.

[31] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," 10 2015. [Online]. Available: http://arxiv.org/abs/1510.08863

[32] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, "Reverse coherent information," *Physical review letters*, vol. 102, no. 21, p. 210501, 2009.

[33] M. Takeoka, S. Guha, and M. M. Wilde, "Squashed entanglement and the two-way assisted capacities of a quantum channel," in *Information Theory (ISIT), 2014 IEEE International Symposium on.* IEEE, 2014, pp. 326–330.

[34] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, p. 621, 2012.

[35] R. Garcia-Patron, C. Navarrete-Benlloch, S. Lloyd, J. H. Shapiro, and N. J. Cerf, "Majorization theory approach to the gaussian channel minimum entropy conjecture," *Physical review letters*, vol. 108, no. 11, p. 110505, 2012.

[36] V. Giovannetti, R. García-Patrón, N. Cerf, and A. Holevo, "Ultimate classical communication rates of quantum optical channels," *Nature Photonics*, vol. 8, no. 10, pp. 796–800, 2014.

[37] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "The ultimate rate of quantum cryptography," *arXiv preprint arXiv:1510.08863*, 2015.

[38] A. S. Holevo and R. F. Werner, "Evaluating capacities of bosonic gaussian channels," *Physical Review A*, vol. 63, no. 3, p. 032312, 2001.

[39] F. Benatti, M. Fannes, R. Floreanini, and D. Petritis, *Quantum information, computation and cryptography: an introductory survey of theory, technology and experiments.* Springer, 2010, vol. 808.

[40] T. F. da Silva, G. C. Amaral, G. P. Temporão, and J. P. von der Weid, "Linear-optic heralded photon source," *Physical Review A*, vol. 92, no. 3, p. 033855, 2015.

[41] M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," *Physics Letters A*, vol. 223, no. 1, pp. 1–8, 1996.

[42] A. Furusawa and P. Van Loock, *Quantum teleportation and entanglement: a hybrid approach to optical quantum information processing.* John Wiley & Sons, 2011.

[43] M. A. de Gosson, *Symplectic geometry and quantum mechanics.* Springer Science &amp; Business Media, 2006, vol. 166.

[44] J. Eisert and M. M. Wolf, "Gaussian quantum channels," *arXiv preprint quant-ph/0505151*, 2005.

[45] G. Cariolaro, *Quantum Communications (equation 11.240).* Springer International Publishing, 2015.

[46] G. Giedke, J. Eisert, J. I. Cirac, and M. B. Plenio, "Entanglement transformations of pure gaussian states," *Quantum Information &amp; Computation*, vol. 3, no. 3, pp. 211–223, 2003.

[47] A. S. Holevo and V. Giovannetti, "Quantum channels and their entropic characteristics," *Reports on progress in physics*, vol. 75, no. 4, p. 046001, 2012.

1. Bounds for convex decomposition of channels

One way of obtaining bounds on the squashed entanglement is based on decomposing the channel action as a mixture of other channels actions and bounding each of them individually.

Let $\mathcal{N}_{A'\to B}$ be a channel such that its action can be written as the convex combination of the action of two other channels $\mathcal{N}_0$ and $\mathcal{N}_1$

$$\rho_{AB} = (\mathcal{I}\otimes\mathcal{N})(\phi_{AA'}) = p(\mathcal{I}\otimes\mathcal{N}_0)(\phi_{AA'}) + (1-p)(\mathcal{I}\otimes\mathcal{N}_1)(\phi_{AA'}) \ . \tag{34}$$

Then we can always purify ρ_{AB} in the following way

$$|\rho\rangle_{ABEF_1F_2} = \sqrt{p}\,|\rho^{(0)}\rangle_{ABE}\,|0\rangle_{F_1}\,|0\rangle_{F_2} + \sqrt{1-p}\,|\rho^{(1)}\rangle_{ABE}\,|1\rangle_{F_1}\,|1\rangle_{F_2} \tag{35}$$

where

$$|\rho^{(0)}\rangle_{ABE} = V^{\mathcal{N}_0}_{A'\to BE}\,|\phi\rangle_{AA'} \tag{36}$$

and

$$|\rho^{(1)}\rangle_{ABE} = V^{\mathcal{N}_1}_{A'\to BE}\,|\phi\rangle_{AA'} \ . \tag{37}$$

That is, $|\rho^{(0)}\rangle_{ABE}$ and $|\rho^{(1)}\rangle_{ABE}$ stand for the state that we obtain after applying the channel isometry to the pure input state $|\phi\rangle_{AA'}$.

Let us apply the following channel to $|\rho\rangle_{ABEF_1F_2}$

$$\rho_{ABEF_1F_2} \mapsto \mathsf{tr}_{F_2}\left((\mathcal{I}_{AB}\otimes S^0_{E\to E'}\otimes P^{|0\rangle}_{F_1}\otimes\mathcal{I}_{F_2})(\rho_{ABEF_1F_2}) + (\mathcal{I}_{AB}\otimes S^1_{E\to E'}\otimes P^{|1\rangle}_{F_1}\otimes\mathcal{I}_{F_2})(\rho_{ABEF_1F_2})\right) \ . \tag{38}$$

Where we denote by $P^{|v\rangle}_{F_1}$ the projector onto the vector $|v\rangle$. First we trace out F_2, then

$$\rho_{ABEF_1} = p\rho^{(0)}_{ABE}\otimes|0\rangle\langle 0|_{F_1} + (1-p)\rho^{(1)}_{ABE}\otimes|1\rangle\langle 1|_{F_1} \ . \tag{39}$$

Now, let us apply the rest of the channel. We obtain

$$\rho_{ABE'F_1} = \sum_i S^i_{E\to E'}\otimes|i\rangle\langle i|_{F_1}(\rho_{ABEF_1}) = pS^0_{E\to E'}(\rho^{(0)}_{ABE})\otimes|0\rangle\langle 0|_{F_1} + (1-p)S^1_{E\to E'}(\rho^{(1)}_{ABE})\otimes|1\rangle\langle 1|_{F_1} \ . \tag{40}$$

That is, $\rho_{ABE'F_1}$ is a quantum-classical system. For states of this form the conditional mutual information can be simplified to

$$I(A;B|EF_1) = pI(A;B|E')_{S^0_{E\to E'}(\rho^{(0)}_{ABE})} + (1-p)I(A;B|E')_{S^1_{E\to E'}(\rho^{(1)}_{ABE})} \tag{41}$$

Now we can upper bound $E_{\rm sq}(\mathcal{N})$ in the following way

$$E_{\rm sq}(\mathcal{N}) \leq \max_{\phi_{AA'}} \inf_{\sum_i S^i_{E\to E'}\otimes|i\rangle\langle i|_{F_1}\otimes\mathsf{tr}_{F_2}} I(A;B|E'F_1))_{\rho_{ABEF_1}} \tag{42}$$

$$= \max_{\phi_{AA'}}\left(p\inf_{S^0_{E\to E'}} I(A;B|E')_{|\rho^{(0)}\rangle_{ABE}} + (1-p)\inf_{S^1_{E\to E'}} I(A;B|E')_{|\rho^{(1)}\rangle_{ABE}}\right) \tag{43}$$

$$\leq pE_{\rm sq}(\mathcal{N}_1) + (1-p)E_{\rm sq}(\mathcal{N}_2) \ . \tag{44}$$

The first inequality holds by restricting the squashing channels to those channels of the form in (38). Equality (43) follows since for channels of the form (38) the resulting state is a quantum-classical state as indicated in (40), and for classical quantum states the conditional mutual information of the whole state is a convex combination of the individual conditional mutual informations as shown in (41). The last inequality follows because the state that achieves the maximum squashed entanglement might be different for each channel. This method generalizes easily to any number of channels, from which it follows that if $\mathcal{N}(\rho) = \sum_i p_i\mathcal{N}_i(\rho)$ with $\sum_i p_i = 1$ and $p_i \geq 0$, then

$$Q_2(\mathcal{N}) \leq P_2(\mathcal{N}) \leq E_{\rm sq}(\mathcal{N}) \leq \sum_i p_i E_{\rm sq}(\mathcal{N}_i) \ . \tag{45}$$

2. Improved bound for the depolarizing channel

It is well known that the depolarizing channel becomes entanglement breaking for $p \geq \frac{2}{3}$ [41], which implies that P_2 is zero in that range. For $\epsilon \leq p \leq \frac{2}{3}$, we can write the output of the channel as a convex combination of the output of $\mathcal{D}_{2/3}$ and $\mathcal{D}_\epsilon$. That is, there exists some $0 \leq \alpha \leq 1$ such that

$$\mathcal{D}_p(\rho) = (1-\alpha)\mathcal{D}_\epsilon(\rho) + \alpha\mathcal{D}_{2/3}(\rho). \tag{46}$$

By expanding both sides of (46) and identifying the coefficients, we obtain

$$\alpha = \frac{p-\epsilon}{2/3-\epsilon} \tag{47}$$

which is in the range $[0,1]$ for $0 \leq \epsilon \leq p$.

Using the decomposition of the depolarizing from (46) the action of $\mathcal{D}_p$ on half of a pure entangled state takes the following form,

$$\begin{aligned}\psi_{AB} &= \mathcal{I} \otimes \mathcal{D}_p(\left|\psi\right\rangle\left\langle\psi\right|_{AA'}) &(48)\\ &= (1-\alpha)\left[(1-\epsilon)\left|\psi\right\rangle\left\langle\psi\right|_{AB} + \epsilon\cdot\pi\right] + \alpha\sum_i \lambda_i \left|\alpha_i\right\rangle\left\langle\alpha_i\right|_A \otimes \left|\beta_i\right\rangle\left\langle\beta_i\right|_B . &(49)\end{aligned}$$

Let $\rho_{AB} = ((1-\epsilon)\left|\psi\right\rangle\left\langle\psi\right|_{AB} + \epsilon\cdot\pi)$. A possible extension of ψ_{AB} is

$$\psi_{ABE'} = (1-\alpha)\rho_{AB} \otimes \left|n+1\right\rangle\left\langle n+1\right|_{E'} + \alpha\sum_{i=1}^n \lambda_i \left|\psi_i\right\rangle\left\langle\psi_i\right|_A \otimes \left|\phi_i\right\rangle\left\langle\phi_i\right|_B \otimes \left|i\right\rangle\left\langle i\right|_{E'} . \tag{50}$$

Since $\psi_{ABE'}$ is a valid extension of ρ_{AB}, this means that there exists some squashing channel $\mathcal{S}_{E\to E'}$ that takes the environment of the depolarizing channel to this particular E'. This is easy to see, first we can find a state $\left|\psi\right\rangle_{ABE'T}$ that purifies $\psi_{ABE'}$. Next, since all purifications are related by an isometry there exists some purification $V_{E\to E'T}$ that takes the environment of the channel to $E'T$. After this we trace out the system T and obtain $\psi_{ABE'}$.

Now, $\psi_{ABE'}$ is a quantum-classical system. Hence, we can decompose the conditional mutual information $I(A;B|E')$ into the sum of the mutual information conditioned on each value of E

$$\begin{aligned}I(A:B|E')_\psi &= (1-\alpha)I(A:B|E')_\rho + \alpha\sum_{i=1}^n \lambda_i I(A:B|E')_{\left|\psi_i\right\rangle\left\langle\psi_i\right|_A \otimes \left|\phi_i\right\rangle\left\langle\phi_i\right|_B \otimes \left|i\right\rangle\left\langle i\right|_{E'}} &(51)\\ &= (1-\alpha)I(A:B|E')_\rho &(52)\end{aligned}$$

Furthermore the input state that maximizes (52) is the maximally entangled state on AA'. Hence, the following bound upper bound on $E_{\mathrm{sq}}(\mathcal{D}_p)$ holds for $0 \leq \epsilon \leq p$

$$E_{\mathrm{sq}}(\mathcal{D}_p) \leq (1-\alpha)\frac{3\epsilon\log(\epsilon) + (4-3\epsilon)\log(4-3\epsilon)}{8}. \tag{53}$$

3. Squashed entanglement upper bound for any phase-insensitive Gaussian channel

In this section we discuss a proof of an upper bound for the squashed entanglement of any phase-insensitive bosonic Gaussian channel $\mathcal{N}_{\mathrm{PI}}$. Here we use the fact that any such channel can be decomposed as a beamsplitter with transmissivity T concatenated with a two-mode squeezer with squeezing parameter $r = \operatorname{acosh}(\sqrt{G})$. We first show that we can restrict the input states to the class of thermal states with mean photon number N, after which the entropic quantity of interest is written as a function of N. We then show that this function is monotonically increasing, after which we take the asymptotic limit $N \to \infty$ of the entropic quantity yielding

$$E_{\mathrm{sq}}(\mathcal{N}_{\mathrm{PI}}) \leq \frac{\left(1-T^2\right)G\log(\frac{1+T}{1-T}) - \left(G^2-1\right)T\log(\frac{G+1}{G-1})}{1-G^2T^2} . \tag{54}$$

To show this is true, we first use a different form of $E_{\mathrm{sq}}(\mathcal{N})$, which was proven by Takeoka et al. [21],

$$E_{\mathrm{sq}}(\mathcal{N}_{\mathrm{PI}}) = \frac{1}{2}\max_{\rho_{A'}}\inf_{V_{E\to E'F}}\left[H(B|E')_\omega + H(B|F)_\omega\right] . \tag{55}$$

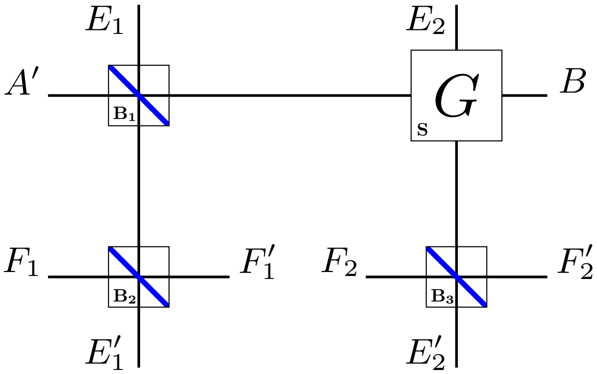

FIG. 8. A squashing isometry for any phase-insensitive Gaussian channel $\mathcal{N}_{\text{PI}}$ taking A' to B. The beamsplitter $\mathbf{B_1}$ and the two-mode squeezer $\mathbf{S}$ form the Stinespring dilation, while the balanced beamsplitters $\mathbf{B_2}$ and $\mathbf{B_3}$ form the squashing map. The beamsplitter $\mathbf{B}_1$ interacts with the vacuum on E_1 and A, and the two-mode squeezer $\mathbf{S}$ interacts with the output of $\mathbf{B}_2$ and the vacuum on E_2. The squashing isometry consists of two balanced beamsplitters $\mathbf{B_2}$ and $\mathbf{B_3}$ interacting with the vacuum on F_1 and F_2 and the output of the beamsplitter $\mathbf{B}_1$ and the two-mode squeezer $\mathbf{S}$.

There are two differences between the characterization in (55) and the one in (2). First, the maximization runs over density operators on A' instead of running over pure states on AA'. Second, instead of taking the infimum over the squashing maps, it is taken over their dilations: squashing isometries $V_{E\to E'F}$ that take the system E to E' and an auxiliary system F. The entropies are then taken on the state ω on systems $BE'F$.

The total operation, which we denote by $\mathbf{D}$, consists of the Stinespring dilation of the channel ($\mathbf{B}_1$ and $\mathbf{S}$) and the squashing isometry consisting of two balanced beamsplitters ($\mathbf{B}_2$ and $\mathbf{B}_3$), see Figure 8. We now write $H(B|E') = H(B|E_1E_2)$, where the system on E' is the output at E_1' and E_2' after the total transformation $\mathbf{D}$. E_1' is the state after the vacuum state on E_1 has interacted with the beamsplitter $\mathbf{B}_1$ and the balanced beamsplitter $\mathbf{B}_2$. Similar statements hold also for E_2', F_1' and F_2'. Since the isometry consists of two balanced beamsplitters we have that $H(B|E') = H(B|F_1'F_2') = H(B|F)$, so that $E_{\text{sq}}(\mathcal{N}) \leq H(B|E')$. After having found the state after the transformation we calculate the so-called symplectic eigenvalues of the states on $BE_1'E_2'$ and $E_1'E_2'$, from which we can find $H(B|E_1'E_2')$. To get an expression of the upper bound for $N\to\infty$, we calculate for three different regimes of G and T the asymptotic behavior of the symplectic eigenvalues, after which we show that all three regimes give rise to the same form of the upper bound.

a. Bound for finite N

A Mathematica file is included in the supplementary material to guide the reader through the calculations performed in this section. For the proof we first need to be able to calculate the entropy of a Gaussian state as a function of its covariance matrix. The entropy of an $M-$mode Gaussian state ρ can be calculated by finding the M symplectic eigenvalues $\nu_k \geq 1$ of the covariance matrix $\mathbf{\Gamma}$ of ρ [42]. It turns out that the $2M$ eigenvalues of the matrix $\mathbf{\Omega\Gamma}$ are of the form $\pm i\nu_k$ [43], where

$$\mathbf{\Omega} := \bigoplus_{k=1}^{M} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} . \tag{56}$$

The entropy of the state is then $\sum_{k=1}^{M} g(\nu_k)$, where $g(x) = \left(\frac{x+1}{2}\right)\log(\frac{x+1}{2}) - \left(\frac{x-1}{2}\right)\log(\frac{x-1}{2})$ [34].

To obtain the state at the end of the isometry we determine first the optimal state for a specified mean photon number N, after which we apply the Gaussian transformations of the Stinespring dilation of the channel and the isometry, shown in Figure 8. To find the maximizing input state on A', we follow the same approach [21, 33] as Takeoka et al. Since the concatenation of multiple Gaussian transformations is still a Gaussian transformation, having a Gaussian state as input will always give a Gaussian state on any of the outputs. From the extremality of Gaussian states for conditional entropy [44], we get that the optimal input state is a Gaussian state.

To find the optimal Gaussian state, we note that the covariance matrix of all single-mode Gaussian states can be written as [45]

$$(1+2N)\begin{bmatrix}\cosh 2r+\cos\theta\sinh 2r & \sin\theta\sinh 2r\\ \sin\theta\sinh 2r & \cosh 2r-\cos\theta\sinh 2r\end{bmatrix} \tag{57}$$

for some $r \geq 0$ and $\theta \in \mathbb{R}$. Since the channel from A' to $BE_1'E_2'F_1'F_2'$ is covariant with displacements and all unitaries $\tilde{U}$ such that the corresponding symplectic matrices $S_{\tilde{U}}$ act on the thermal state as

$$S_{\tilde{U}}\,(1+2N)\,\mathbb{I}\;{S_{\tilde{U}}}^{T} \to (1+2N)\begin{bmatrix}\cosh 2r+\cos\theta\sinh 2r & \sin\theta\sinh 2r\\ \sin\theta\sinh 2r & \cosh 2r-\cos\theta\sinh 2r\end{bmatrix}\;, \tag{58}$$

we have that $H(B|E')_\rho = H(B|E')_{\tilde{U}\rho\tilde{U}^\dagger}$. We set ρ equivalent to $\tilde{U}\rho\tilde{U}^\dagger$, defining an equivalence relation. It is clear that all states with fixed N in equation (57) define an equivalence class with respect to the equivalence relation. Since $H(B|E')_\rho = H(B|E')_{\tilde{U}\rho\tilde{U}^\dagger}$, we can set the thermal state $(1+2N)\,\mathbb{I}$ to be the representative of that equivalence class, and we only have to consider thermal states for the optimization.

The total system $\Gamma_{A'E_1'F_1E_2'F_2}$ consists then of a thermal state $\Gamma_{A'}$ with mean photon number N on A' and vacuum states on all the other inputs:

$$\mathbf{\Gamma}_{A'E_1F_1E_2F_2} = \gamma_{A'}\oplus\mathbb{I}_{E_1}\oplus\mathbb{I}_{F_1}\oplus\mathbb{I}_{E_2}\oplus\mathbb{I}_{F_2}, \tag{59}$$

$$\gamma_{A'} = \begin{bmatrix}1+2N & 0\\ 0 & 1+2N\end{bmatrix}. \tag{60}$$

The operations of the isometry are then the first beamsplitter $\mathbf{B_1}$ with transmissivity T on A' and E_1

$$\mathbf{B_1} = \begin{bmatrix}\sqrt{T} & 0 & \sqrt{1-T} & 0\\ 0 & \sqrt{T} & 0 & \sqrt{1-T}\\ -\sqrt{1-T} & 0 & \sqrt{T} & 0\\ 0 & -\sqrt{1-T} & 0 & \sqrt{T}\end{bmatrix}_{A'E_1'}\oplus\mathbb{I}_{F_1}\oplus\mathbb{I}_{E_2}\oplus\mathbb{I}_{F_2}, \tag{61}$$

the second beamsplitter $\mathbf{B_2}$ with transmissivity $\frac{1}{2}$ on E_1 and F_1

$$\mathbf{B_2} = \mathbb{I}_{A'}\oplus\begin{bmatrix}\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0\\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0\\ 0 & -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\end{bmatrix}_{E_1F_1}\oplus\mathbb{I}_{E_2}\oplus\mathbb{I}_{F_2}, \tag{62}$$

the two-mode squeezer $\mathbf{S}$ on A' and E_2 with the relation $G=\cosh^2(r)$

$$\mathbf{S} = \begin{bmatrix}\sqrt{G} & 0 & 0 & 0 & 0 & 0 & \sqrt{G-1} & 0\\ 0 & \sqrt{G} & 0 & 0 & 0 & 0 & 0 & -\sqrt{G-1}\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ \sqrt{G-1} & 0 & 0 & 0 & 0 & 0 & \sqrt{G} & 0\\ 0 & -\sqrt{G-1} & 0 & 0 & 0 & 0 & 0 & \sqrt{G}\end{bmatrix}_{A'E_1'F_1'}\oplus\mathbb{I}_{F_2}, \tag{63}$$

and finally the last beamsplitter $\mathbf{B_3}$ on E_2 and F_2 with transmissivity $\frac{1}{2}$

$$\mathbf{B_3} = \mathbb{I}_{A'} \oplus \mathbb{I}_{E_1'} \oplus \mathbb{I}_{F_1} \oplus \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}_{E_2'F_2} . \tag{64}$$

We then have that the total symplectic transformation matrix $\mathbf{D}$ is

$$\mathbf{D} = \mathbf{B_3 S B_2 B_1} \tag{65}$$

$$= \begin{bmatrix} \sqrt{GT} & 0 & \sqrt{G(1-T)} & 0 & 0 & 0 & \sqrt{G-1} & 0 & 0 & 0 \\ 0 & \sqrt{GT} & 0 & \sqrt{G(1-T)} & 0 & 0 & 0 & -\sqrt{G-1} & 0 & 0 \\ -\sqrt{\frac{1-T}{2}} & 0 & \sqrt{\frac{T}{2}} & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \\ 0 & -\sqrt{\frac{1-T}{2}} & 0 & \sqrt{\frac{T}{2}} & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 \\ \sqrt{\frac{1-T}{2}} & 0 & -\sqrt{\frac{T}{2}} & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{\frac{1-T}{2}} & 0 & -\sqrt{\frac{T}{2}} & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 \\ \sqrt{\frac{(G-1)T}{2}} & 0 & \sqrt{\frac{(G-1)(1-T)}{2}} & 0 & 0 & 0 & \sqrt{\frac{G}{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & -\sqrt{\frac{(G-1)T}{2}} & 0 & -\sqrt{\frac{(G-1)(1-T)}{2}} & 0 & 0 & 0 & \sqrt{\frac{G}{2}} & 0 & \frac{1}{\sqrt{2}} \\ -\sqrt{\frac{(G-1)T}{2}} & 0 & -\sqrt{\frac{(G-1)(1-T)}{2}} & 0 & 0 & 0 & -\sqrt{\frac{G}{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \sqrt{\frac{(G-1)T}{2}} & 0 & \sqrt{\frac{(G-1)(1-T)}{2}} & 0 & 0 & 0 & -\sqrt{\frac{G}{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} . \tag{66}$$

The covariance matrix $\mathbf{\Gamma}_{BE_1'F_1'E_2'F_2'} = \mathbf{D}\mathbf{\Gamma}_{A'E_1F_1E_2F_2}\mathbf{D}^T$ after the transformation is then

$$\begin{bmatrix} a\mathbb{I} & -b\mathbb{I} & b\mathbb{I} & c\sigma_z & -c\sigma_z \\ -b\mathbb{I} & d\mathbb{I} & e\mathbb{I} & -f\sigma_z & f\sigma_z \\ b\mathbb{I} & e\mathbb{I} & d\mathbb{I} & f\sigma_z & -f\sigma_z \\ c\sigma_z & -f\sigma_z & f\sigma_z & g\mathbb{I} & h\mathbb{I} \\ -c\sigma_z & f\sigma_z & -f\sigma_z & h\mathbb{I} & g\mathbb{I} \end{bmatrix} , \tag{67}$$

where $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and

$$a = 2G(1 + NT) - 1 \tag{68}$$

$$b = N\sqrt{2\left(GT\left(1-T\right)\right)} \tag{69}$$

$$c = (1 + NT)\sqrt{2\left(G-1\right)G} \tag{70}$$

$$d = 1 + N\left(1 - T\right) \tag{71}$$

$$e = N\left(T - 1\right) \tag{72}$$

$$f = N\sqrt{\left(G-1\right)\left(1-T\right)T} \tag{73}$$

$$g = G + \left(G - 1\right)NT \tag{74}$$

$$h = -(G-1)(1 + NT). \tag{75}$$

The covariance matrix on the subsystems E_1E_2 is then

$$\mathbf{\Gamma}_{E_1'E_2'} = \begin{bmatrix} d\mathbb{I} & -f\sigma_z \\ -f\sigma_z & g\mathbb{I} \end{bmatrix} . \tag{76}$$

Multiplying by $\mathbf{\Omega}$ gives

$$\mathbf{\Omega\Gamma}_{E_1'E_2'} = \begin{bmatrix} 0 & d & 0 & f \\ -d & 0 & f & 0 \\ 0 & f & 0 & g \\ f & 0 & -g & 0 \end{bmatrix}. \tag{77}$$

Now set $\Omega^{\pm} = \sqrt{(1+N)^2 - 4NT \pm 2G(1+N)(NT-1) + (G+GNT)^2}$. Taking the covariance matrix corresponding to $E_1'E_2'$ we find using Mathematica the symplectic eigenvalues to be

$$\left(\nu_{E_1'E_2'}\right)_1 = \left| \sqrt{-\frac{1+G^2+2N\left(1-T+GT\left(G-1\right)\right)+N^2\left(GT-1\right)^2+\left(G-1+N(GT-1)\right)\Omega^-}{2}} \right| \tag{78}$$

$$\left(\nu_{E_1'E_2'}\right)_2 = \left| \sqrt{-\frac{1+G^2+2N\left(1-T+GT\left(G-1\right)\right)+N^2\left(GT-1\right)^2-\left(G-1+N(GT-1)\right)\Omega^-}{2}} \right|. \tag{79}$$

The covariance matrix corresponding to $BE_1'E_2'$ is

$$\mathbf{\Gamma}_{BE_1'E_2'} = \begin{bmatrix} a\mathbb{I} & -b\mathbb{I} & c\sigma_z \\ -b\mathbb{I} & d\mathbb{I} & -f\sigma_z \\ c\sigma_z & -f\sigma_z & g\mathbb{I} \end{bmatrix}, \tag{80}$$

so that

$$\mathbf{\Omega\Gamma}_{BE_1'E_2'} = \begin{bmatrix} 0 & a & 0 & -b & 0 & -c \\ -a & 0 & b & 0 & -c & 0 \\ 0 & -b & 0 & d & 0 & f \\ b & 0 & -d & 0 & f & 0 \\ 0 & -c & 0 & f & 0 & g \\ -c & 0 & f & 0 & -g & 0 \end{bmatrix}, \tag{81}$$

From this the symplectic eigenvalues can be calculated to be

$$\left(\nu_{BE_1'E_2'}\right)_1 = \left| \sqrt{-\frac{1+G^2+2N\left(1-T+GT\left(G+1\right)\right)+N^2\left(1+GT\right)^2+\left(1+G+N(1+GT)\right)\Omega^+}{2}} \right| \tag{82}$$

$$\left(\nu_{BE_1'E_2'}\right)_2 = \left| \sqrt{-\frac{1+G^2+2N\left(1-T+GT\left(G+1\right)\right)+N^2\left(1+GT\right)^2-\left(1+G+N(1+GT)\right)\Omega^+}{2}} \right| \tag{83}$$

$$\left(\nu_{BE_1'E_2'}\right)_3 = 1. \tag{84}$$

We can now calculate $H(B|E_1'E_2')$,

$$H(B|E_1'E_2') = H(BE_1'E_2') - H(E_1'E_2') \tag{85}$$

$$= g\left(\left(\nu_{BE_1'E_2'}\right)_1\right) + g\left(\left(\nu_{BE_1'E_2'}\right)_2\right) - g\left(\left(\nu_{E_1'E_2'}\right)_1\right) - g\left(\left(\nu_{E_1'E_2'}\right)_2\right), \tag{86}$$

where we used that $g(1) = 0$.

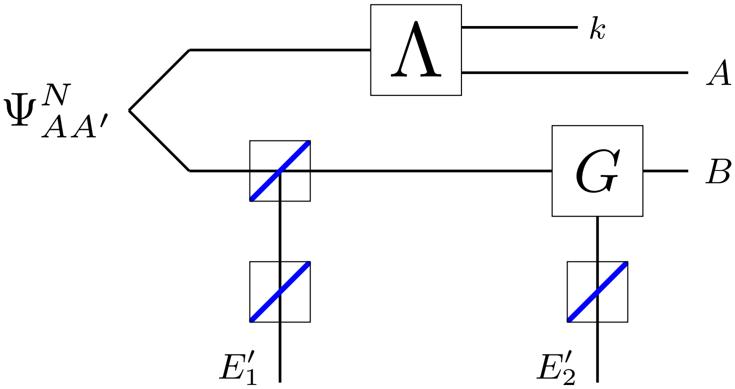

FIG. 9. Alice can perform a local operation Λ on one half of $\Psi^N_{AA'}$ that yields a state on A and a classical outcome k. The state conditioned on the outcome k on systems ABE'_1E_2 is, up to a unitary displacement on B and $E'_1E'_2$, equal to the state $\rho^{N'}$. Alice and Bob can thus simulate any lower energy scenario.

b. Monotonicity of the bound

For this section we restrict ourselves to the picture of calculating the squashed entanglement on the systems $ABE'_1E'_2$ instead of $BE'_1E'_2F'_1F'_2$, where $V_{A'\to BE'_1E'_2F'_1F'_2} := V$ is the total isometry (see Figure 8). In this picture the optimization is over the purification of the thermal state, the two-mode squeezed vacuum state Ψ^N. To show monotonicity of equation (86) in N, we use that, up to a displacement on B (conditioned on a measurement outcome k at A'), it is possible to transform the state $\Psi^N_{AA'}$ to $\Psi^{N'}_{AA'}$, using a local operation Λ_A on Alice (where $N' < N$) [46].

Suppose now that A performs the operation Λ_A on the state $\rho^N_{ABE'_1E'_2} := \mathsf{tr}_{F'_1F'_2}\left(V\Psi^N V^\dagger\right)$ after the isometry,

$$\left(\Lambda_A \otimes \mathbb{I}_{BE'_1E'_2}\right)\rho^N_{ABE'_1E'_2} = \int \mathrm{d}k\,|k\rangle\langle k| \otimes \left(\left(\mathbb{I}_A \otimes U^k_B \otimes U^k_{E'_1E'_2}\right)\rho^{N'}_{ABE'_1E'_2}\right) \tag{87}$$

$$= \int \mathrm{d}k\,|k\rangle\langle k| \otimes \rho^{N',k}_{ABE'_1E'_2}\ . \tag{88}$$

Here we used that displacement operations can always be removed by local operations [47], so that for fixed outcome k the state $\rho^{N',k}_{ABE'_1E'_2}$ is related to $\rho^{N'}_{ABE'_1E'_2} := \mathsf{tr}_{F'_1F'_2}\left(V\Psi^{N'}\right)$ by unitary displacements on B and $E'_1E'_2$. The conditional mutual information evaluated on the state $\Lambda_A \otimes \mathbb{I}_{BE'_1E'_2}\rho^N_{ABE'_1E'_2} = \tilde{\rho}^N$ then satisfies

$$I(A;B|E'_1E'_2)_{\rho^N_{ABE'_1E'_2}} \geq I(A;B|E'_1E'_2)_{\tilde{\rho}^N} \tag{89}$$

$$\geq \int \mathrm{d}k\ I(A;B|E'_1E'_2)_{\rho^{N',k}} \tag{90}$$

$$= \int \mathrm{d}k\ I(A;B|E'_1E'_2)_{\rho^{N'}} \tag{91}$$

$$= I(A;B|E'_1E'_2)_{\rho^{N'}}\ . \tag{92}$$

In equation (89) we used that the conditional mutual information can never increase under local operations on A [23]. In equation (90) we use the fact that the states $\rho^{N',k}_{ABE'_1E'_2}$ are flagged on the classical outcome k, and that the conditional mutual information of the whole state can not be smaller than the sum of the values of the conditional mutual information of the individual states [23]. In equations (91) and (92) we use the fact that all the $\rho^{N',k}_{ABE'_1E'_2}$ states are related to $\rho^{N'}_{ABE'_1E'_2}$ by local unitaries on B and $E'_1E'_2$ and that the conditional mutual information of those states thus must be equal.

That is, the conditional mutual information computed over the isometry V with input state Ψ^N is always greater than the conditional mutual information computed over the isometry V with input state $\Psi^{N'}$ if $N' < N$. This thus implies that equation (86) is a bound for all phase-insensitive Gaussian bosonic channels and all energy restrictions.

c. Expression as $N \to \infty$

To obtain an explicit form for the expression in (86) as $N \to \infty$, we expand the eigenvalues around $N = \infty$ for three different regimes of G and T using Mathematica. For $G = \frac{1}{T}$ we have

$$\left(\nu_{E_1'E_2'}\right)_1 = \sqrt{\frac{G^2-1}{G}}\sqrt{N} + \mathcal{O}\left(1\right), \tag{93}$$

$$\left(\nu_{E_1'E_2'}\right)_2 = \sqrt{\frac{G^2-1}{G}}\sqrt{N} + \mathcal{O}\left(1\right), \tag{94}$$

$$\left(\nu_{BE_1'E_2'}\right)_1 = 2N + \mathcal{O}\left(1\right), \tag{95}$$

$$\left(\nu_{BE_1'E_2'}\right)_2 = \frac{G^2+1}{2G} + o\left(1\right)\ . \tag{96}$$

Here we used the notation that $f(N) = o(h(N))$ for two functions $f(N)$ and $h(N)$ if and only if $\forall\epsilon > 0, \exists N'$ such that $\forall N > N',\ f(N) \leq \epsilon h(N)$.

Now let us introduce the equivalence relation $\rightleftarrows$ for two functions $f(N)$ and $h(N)$, so that $f(N) \rightleftarrows h(N)$ if and only if $\lim_{N\to\infty} |f(N) - h(N)| = 0$, i.e. we can safely replace $f(N)$ by $h(N)$ as $N \to \infty$. For example, we have that $g(N + c) \rightleftarrows g(N) \rightleftarrows \log(\frac{N}{2}) + \frac{1}{\ln 2}$. In particular, if $f(N) = h(N) + o(1)$, then $g(f(N)) \rightleftarrows g(h(N))$. Furthermore, this also means that if we have $f(N) = h(N) + \mathcal{O}(1)$ and $\lim_{N\to\infty} f(N) = \lim_{N\to\infty} h(N) = \infty$, then $g(f(N)) \rightleftarrows \log(\frac{h(N)}{2}) + \frac{1}{\ln 2}$. We will call these relations the asymptotic entropic relations for short.

Using these asymptotic entropic relations, we find

$$H(BE_1'E_2') - H(E_1'E_2') = g\left(\left(\nu_{BE_1E_2}\right)_1\right) + g\left(\left(\nu_{BE_1E_2}\right)_2\right) - g\left(\left(\nu_{E_1E_2}\right)_1\right) - g\left(\left(\nu_{E_1E_2}\right)_2\right) \tag{97}$$

$$\rightleftarrows g\left(\frac{G^2+1}{2G}\right) + g\left(2N\right) - g\left(\sqrt{\frac{G^2-1}{G}}\sqrt{N}\right) - g\left(\sqrt{\frac{G^2-1}{G}}\sqrt{N}\right) \tag{98}$$

$$\rightleftarrows g\left(\frac{G^2+1}{2G}\right) + \log(N) + \frac{1}{\ln 2} - \log(\sqrt{\frac{G^2-1}{4G}}\sqrt{N}) - \frac{1}{\ln 2} - \log(\sqrt{\frac{G^2-1}{4G}}\sqrt{N}) - \frac{1}{\ln 2} \tag{99}$$

$$= g\left(\frac{G^2+1}{2G}\right) + \log(\frac{4G}{G^2-1}) - \frac{1}{\ln 2} \tag{100}$$

$$= \frac{\frac{G^2+1}{2G}+1}{2}\log(\frac{\frac{G^2+1}{2G}+1}{2}) - \frac{\frac{G^2+1}{2G}-1}{2}\log(\frac{\frac{G^2-1}{2G}+1}{2}) + \log(\frac{4G}{G^2-1}) - \frac{1}{\ln 2} \tag{101}$$

$$= \frac{\left(G+1\right)^2}{4G}\log(\frac{\left(G+1\right)^2}{4G}) - \frac{\left(G-1\right)^2}{4G}\log(\frac{\left(G-1\right)^2}{4G}) + \log(\frac{4G}{G^2-1}) - \frac{1}{\ln 2} \tag{102}$$

$$\begin{aligned} &= \frac{\left(G+1\right)^2}{4G}\log((G+1)^2) - \frac{\left(G-1\right)^2}{4G}\log((G-1)^2) \\ &\quad + \underbrace{\left(-\frac{\left(G+1\right)^2}{4G} + \frac{\left(G-1\right)^2}{4G} + 1\right)}_{0}\log(4G) - \log(G^2-1) - \frac{1}{\ln 2} \end{aligned} \tag{103}$$

$$= \frac{\left(G+1\right)^2}{2G}\log(G+1) - \frac{\left(G-1\right)^2}{2G}\log(G-1) - \log(G^2-1) - \frac{1}{\ln 2} \tag{104}$$

$$= \left(\frac{G^2+2G+1}{2G}\right)\log(G+1) - \left(\frac{G^2-2G+1}{2G}\right)\log(G-1) - \log(G^2-1) - \frac{1}{\ln 2} \tag{105}$$

$$= \frac{G^2+1}{2G}\log(\frac{G+1}{G-1}) - \underbrace{\log(G+1) + \log(G-1) - \log(G^2-1)}_{0} - \frac{1}{\ln 2} \tag{106}$$

$$= \frac{G^2+1}{2G}\log(\frac{G+1}{G-1}) - \frac{1}{\ln 2} = \frac{T^2+1}{2T}\log(\frac{1+T}{1-T}) - \frac{1}{\ln 2}. \tag{107}$$

Here we used the asymptotic entropic relations in equations (98) and (99). Equation (100) is basic rewriting, equation (101) follows directly from the definition of $g(\cdot)$, and equation (102) follows from rewriting the terms. In equation

(103) we collect the terms proportional to $\log(4G)$, from which we can see that these terms sum up to zero. In equation (105) we expand the quadratic terms, collect corresponding terms in equation (106) and write the upper bound both as a function of G and T in the last equality.

For $G > \frac{1}{T}$ we get in the asymptotic limit that equations (78), (79), (82) and (83) become

$$\left(\nu_{E_1'E_2'}\right)_1 = N\left(GT-1\right) + \mathcal{O}\left(1\right), \tag{108}$$

$$\left(\nu_{E_1'E_2'}\right)_2 = \frac{G-T}{GT-1} + o\left(1\right), \tag{109}$$

$$\left(\nu_{BE_1'E_2'}\right)_1 = N\left(1+GT\right) + \mathcal{O}\left(1\right), \tag{110}$$

$$\left(\nu_{BE_1'E_2'}\right)_2 = \frac{G+T}{1+GT} + o\left(1\right). \tag{111}$$

For $G < \frac{1}{T}$ we have

$$\left(\nu_{E_1'E_2'}\right)_1 = \frac{G-T}{1-GT} + o\left(1\right), \tag{112}$$

$$\left(\nu_{E_1'E_2'}\right)_2 = N\left(1-GT\right) + \mathcal{O}\left(1\right), \tag{113}$$

$$\left(\nu_{BE_1'E_2'}\right)_1 = N\left(1+GT\right) + \mathcal{O}\left(1\right), \tag{114}$$

$$\left(\nu_{BE_1'E_2'}\right)_2 = \frac{G+T}{1+GT} + o\left(1\right) \ . \tag{115}$$

For both regimes, the eigenvalues and in particular their leading terms are always positive. We see that for both $G > \frac{1}{T}$ and $G < \frac{1}{T}$ the absolute value of the eigenvalues are the same up to ordering, so that

$$H(BE_1'E_2') - H(E_1'E_2') \rightleftarrows g\left(\frac{G+T}{1+GT}\right) + g\left(N\left(1+GT\right)\right) - g\left(N\left|1-GT\right|\right)\right) - g\left(\frac{G-T}{\left|1-GT\right|}\right) \tag{116}$$

$$\rightleftarrows g\left(\frac{G+T}{1+GT}\right) + \log(\frac{N\left(1+GT\right)}{2}) + \frac{1}{\ln 2} - \log(\frac{N\left|1-GT\right|}{2}) - \frac{1}{\ln 2} - g\left(\frac{G-T}{\left|1-GT\right|}\right) \tag{117}$$

$$= g\left(\frac{G+T}{1+GT}\right) - g\left(\frac{G-T}{\left|1-GT\right|}\right) + \log(\frac{1+GT}{\left|1-GT\right|}) \tag{118}$$

$$= g\left(\frac{G+T}{1+GT}\right) - g\left(\frac{G-T}{1-GT}\right) + \log(\frac{1+GT}{1-GT}) \ , \tag{119}$$

where in the first and second step we again used the asymptotic entropic relations. Equation (118) is basic algebraic rewriting of the logarithms. We can drop the absolute signs going from equation (118) to (119). To see this, note that $\log(-x) = \log(x) + \frac{i\pi}{\ln 2}$ for $x > 0$, where we choose the branch cut along the negative imaginary axis, and in a similar way we find that $g(-y) = \frac{-y+1}{2}\log(\frac{-y+1}{2}) - \frac{-y-1}{2}\log(\frac{-y-1}{2}) = \frac{y+1}{2}\log(-\frac{y+1}{2}) - \frac{y-1}{2}\log(-\frac{y-1}{2}) = g(y) + \frac{i\pi}{\ln 2}$ for $y \geq 1$. From this we find that $-g(-y) + \log(-x) = -g(y) + \log(x)$ for $x > 0,\ y \geq 1$. Since $\frac{G-T}{|1-GT|} > 1$ and $\frac{1+GT}{|1-GT|} \geq 0$ for $G \geq 1,\ 0 \leq T \leq 1$, we have that $-g\left(\frac{G-T}{|1-GT|}\right) + \log(\frac{1+GT}{|1-GT|}) = -g\left(\frac{G-T}{1-GT}\right) + \log(\frac{1+GT}{1-GT})$.

We can rewrite equation (119) as

$$\begin{aligned}
& g\left(\frac{G+T}{1+GT}\right) - g\left(\frac{G-T}{1-GT}\right) + \log(\frac{1+GT}{1-GT}) \qquad (120)\\
&= \frac{\frac{G+T}{1+GT}+1}{2}\log(\frac{\frac{G+T}{1+GT}+1}{2}) - \frac{\frac{G+T}{1+GT}-1}{2}\log(\frac{\frac{G+T}{1+GT}-1}{2}) - \frac{\frac{G-T}{1-GT}+1}{2}\log(\frac{\frac{G-T}{1-GT}+1}{2})\\
&\quad - \frac{\frac{G-T}{1-GT}-1}{2}\log(\frac{\frac{G-T}{1-GT}-1}{2}) + \log(\frac{1+GT}{1-GT}) \qquad (121)\\
&= \frac{(G+1)(1+T)}{2\,(1+GT)}\log(\frac{(G+1)(1+T)}{2\,(1+GT)}) - \frac{(G-1)(1-T)}{2\,(1+GT)}\log(\frac{(G-1)(1-T)}{2\,(1+GT)})\\
&\quad -\frac{(G+1)(1-T)}{2\,(1-GT)}\log(\frac{(G+1)(1-T)}{2\,(1-GT)}) + \frac{(G-1)(1+T)}{2\,(1-GT)}\log(\frac{(G-1)(1+T)}{2\,(1-GT)}) + \log(\frac{1+GT}{1-GT})\ , \qquad (122)
\end{aligned}$$

where we have used the definition of $g(\cdot)$ in the first equality and simplified the terms in the second step.

We can expand the logarithms and collect the different terms and simplify to rewrite equation (122). Let us consider one by one the terms proportional to each logarithmic term. The terms proportional to $\log(G+1)$ are

$$\begin{aligned}
&\frac{(G+1)\,(1+T)}{2\,(1+GT)} - \frac{(G+1)\,(1-T)}{2\,(1-GT)} && (123)\\
&= -\frac{\left(G^2-1\right)T}{1-G^2T^2}\ , && (124)
\end{aligned}$$

the terms proportional to $\log(G-1)$ are

$$\begin{aligned}
&-\frac{(G-1)\,(1-T)}{2\,(1+GT)} + \frac{(G-1)\,(1+T)}{2\,(1-GT)} && (125)\\
&= \frac{\left(G^2-1\right)T}{1-G^2T^2}\ , && (126)
\end{aligned}$$

the terms proportional to $\log(1+T)$ are

$$\begin{aligned}
&\frac{(G+1)\,(1+T)}{2\,(1+GT)} + \frac{(G-1)\,(1+T)}{2\,(1-GT)} && (127)\\
&= \frac{\left(1-T^2\right)G}{1-G^2T^2}\ , && (128)
\end{aligned}$$

the terms proportional to $\log(1-T)$ are

$$\begin{aligned}
&-\frac{(G-1)\,(1-T)}{2\,(1+GT)} - \frac{(G+1)\,(1-T)}{2\,(1-GT)} && (129)\\
&= -\frac{\left(1-T^2\right)G}{1-G^2T^2}\ , && (130)
\end{aligned}$$

the terms proportional to $\log(\frac{1}{2(1+GT)}) = -\log(1+GT) - 1$ are

$$\begin{aligned}
&\frac{(G+1)\,(1+T)}{2\,(1+GT)} - \frac{(G-1)\,(1-T)}{2\,(1+GT)} && (131)\\
&= 1\ , && (132)
\end{aligned}$$

and finally the terms proportional to $\log(\frac{1}{2(1-GT)}) = -\log(1-GT) - 1$ are

$$\begin{aligned}
&-\frac{(G+1)\,(1-T)}{2\,(1-GT)} + \frac{(G-1)\,(1+T)}{2\,(1-GT)} && (133)\\
&= -1\ . && (134)
\end{aligned}$$

Collecting all these terms and the $\log(\frac{1+GT}{1-GT})$ term, equation (122) becomes

$$\begin{aligned}
&-\frac{\left(G^2-1\right)T}{1-G^2T^2}\log(G+1)+\frac{\left(G^2-1\right)T}{1-G^2T^2}\log(G-1)+\frac{\left(1-T^2\right)G}{1-G^2T^2}\log(1+T)\\
&-\frac{\left(1-T^2\right)G}{1-G^2T^2}\log(1-T)\underbrace{-\log(1+GT)-1+\log(1-GT)+1+\log(\frac{1+GT}{1-GT})}_{0} && (135)\\
&=-\frac{\left(G^2-1\right)T}{1-G^2T^2}\left(\log(G+1)-\log(G-1)\right)+\frac{\left(1-T^2\right)G}{1-G^2T^2}\left(\log(1+T)-\log(1-T)\right) && (136)\\
&=\frac{\left(1-T^2\right)G\log(\frac{1+T}{1-T})-\left(G^2-1\right)T\log(\frac{G+1}{G-1})}{1-G^2T^2}\ , && (137)
\end{aligned}$$

where in the first equality we regrouped terms and used the fact that the sum of the last five terms equals zero. The second equality follows from rewriting the logarithm terms.
Setting $G=\frac{1}{T}$, the denominator of equation (137) becomes zero. Luckily, the numerator $\left(1-T^2\right)\frac{1}{T}\log(\frac{1+T}{1-T})-\left(\frac{1}{T^2}-1\right)T\log(\frac{\frac{1}{T}+1}{\frac{1}{T}-1})=\left(\frac{1}{T}-T\right)\log(\frac{1+T}{1-T})-\left(\frac{1}{T}-T\right)\log(\frac{1+T}{1-T})=0$, also becomes zero, implying that we can use L'Hôpital's rule to retrieve the limit. Differentiating the numerator from equation (137) with respect to G gives

$$\left(1-T^2\right)\log(\frac{1+T}{1-T})+\frac{2T}{\ln 2}-2GT\log(\frac{G+1}{G-1})\ , \tag{138}$$

while differentiating the denominator from equation (137) gives

$$-2GT^2\ . \tag{139}$$

so that the quotient of equation (138) and (139) gives

$$\frac{-\left(1-T^2\right)\log(\frac{1+T}{1-T})-\frac{2T}{\ln 2}+2GT\log(\frac{G+1}{G-1})}{2GT^2}\ . \tag{140}$$

Setting $G=\frac{1}{T}$ we retrieve that

$$\begin{aligned}
&\lim_{G\to\frac{1}{T}}\frac{\left(1-T^2\right)G\log(\frac{1+T}{1-T})-\left(G^2-1\right)T\log(\frac{G+1}{G-1})}{1-G^2T^2} && (141)\\
&=\lim_{G\to\frac{1}{T}}\frac{-\left(1-T^2\right)\log(\frac{1+T}{1-T})-\frac{2T}{\ln 2}+2GT\log(\frac{G+1}{G-1})}{2GT^2} && (142)\\
&=\frac{\left(T^2-1\right)\log(\frac{1+T}{1-T})-\frac{2T}{\ln 2}+2\log(\frac{1+T}{1-T})}{2T} && (143)\\
&=\frac{T^2+1}{2T}\log(\frac{1+T}{1-T})-\frac{1}{\ln 2}\ . && (144)
\end{aligned}$$

We see that for all three regimes ($G=\frac{1}{T},\ G>\frac{1}{T}$ and $G<\frac{1}{T}$) equation (86), yields equation (137) in the asymptotic limit of $N\to\infty$. From this we retrieve our claim that

$$\begin{aligned}
Q_2(\mathcal{N}_{\mathrm{PI}}),P_2(\mathcal{N}_{\mathrm{PI}})\le E_{\mathrm{sq}}(\mathcal{N}_{\mathrm{PI}})&\le\frac{H(B|E_1'E_2')+H(B|F_1'F_2')}{2} && (145)\\
&=\frac{\left(1-T^2\right)G\log(\frac{1+T}{1-T})-\left(G^2-1\right)T\log(\frac{G+1}{G-1})}{1-G^2T^2}\ . && (146)
\end{aligned}$$