Breaking entanglement-breaking by classical correlations

Stefano Pirandola

Department of Computer Science, University of York, York YO10 5GH, United Kingdom

The inevitable interaction between quantum systems and environment induces effects of decoherence which may be so strong as to destroy any initial entanglement between the systems, a phenomenon known as "entanglement breaking". Here we show the simplest examples where the combination of two entanglement-breaking channels into a joint correlated-noise environment reactivates the distribution of entanglement, with classes of entangled states which are perfectly transmitted from a middle station (Charlie) to two remote stations (Alice and Bob). Surprisingly, this reactivation is induced by the presence of purely-classical correlations in the joint environment, whose state is separable with zero discord. This paradoxical effect is proven for quantum systems with Hilbert spaces of any dimension, both finite and infinite.

I.   INTRODUCTION

The distribution of entanglement is a central topic of investigation in the quantum information community. Unfortunately, this distribution is also fragile: Quantum systems inevitably interact with the external environment whose decoherent action typically degrades their entanglement. The worst scenario is when decoherence is so strong as to destroy any input entanglement. Mathematically, this situation is represented by the concept of entanglement-breaking channel [1, 2]. In general, a quantum channel $\mathcal{E}$ is entanglement-breaking when its local action on one part of a bipartite state always results into a separable output state. In other words, given two systems, A and B, in an arbitrary bipartite state ρ_{AB}, the output state $\rho_{AB'} = (\mathcal{I}_A \otimes \mathcal{E}_B)(\rho_{AB})$ is always separable, where $\mathcal{I}_A$ is the identity channel applied to system A and $\mathcal{E}_B$ is the entanglement-breaking channel applied to system B.

Despite entanglement-breaking channels having been the subject of an intensive study by the community, they have only been analyzed under Markovian conditions of no memory. In other words, when the distribution involves two or more systems, these systems are typically assumed to be perturbed in an independent fashion, each of them subject to the same memoryless channel. For instance, consider the scheme depicted in panel (1) of Fig. 1, where a middle station (Charlie) has a bipartite system AB in some entangled state, but its communication lines with two remote parties (Alice and Bob) are affected by entanglement-breaking channels $\mathcal{E}_A$ and $\mathcal{E}_B$.

Under the assumption of memoryless channels, there is clearly no way to distribute entanglement among any of the parties. Suppose that Charlie tries to share entanglement with one of the remote parties by sending one of the two systems while keeping the other (a scenario that we call "1-system transmission" or just "single transmission"). For instance, Charlie may keep system A while transmitting system B to Bob. The action of $\mathcal{I}_A \otimes \mathcal{E}_B$ destroys the initial entanglement, so that systems A (kept) and B' (transmitted) are separable. Symmet-

rically, the action of $\mathcal{E}_A \otimes \mathcal{I}_B$ destroys the entanglement between system A' (transmitted) and system B (kept). Now suppose that Charlie sends system A to Alice and system B to Bob (a scenario that we call "2-system transmission" or "double transmission"). Since the joint action of the two channels is given by the tensor product $\mathcal{E}_A \otimes \mathcal{E}_B = (\mathcal{E}_A \otimes \mathcal{I}_B)(\mathcal{I}_A \otimes \mathcal{E}_B)$ quantum entanglement must necessarily be destroyed. In other words, since we have 1-system entanglement-breaking, then we must have 2-system entanglement-breaking.
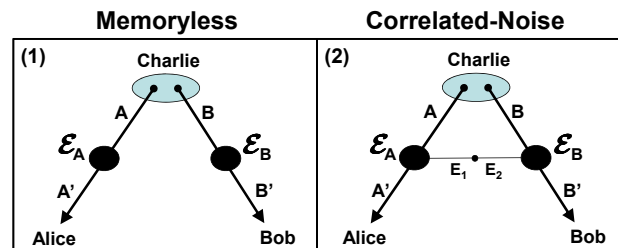

FIG. 1. Symmetric scheme for entanglement distribution in memoryless (1) and correlated-noise (2) environments. Charlie is the middle station with an entangled state of systems A and B. Alice and Bob are the remote receiving stations. Charlie may choose to keep one system and send the other to Alice or Bob (single transmission) or he may decide to send both the systems to the remote stations (double transmission). In panel (1) we consider two memoryless entanglement-breaking channels, $\mathcal{E}_A$ and $\mathcal{E}_B$. No entanglement can be distributed, neither via single transmission (Charlie → Alice or Charlie →Bob), nor via double transmission (Charlie → Alice and Bob). In panel (2) we consider the presence of correlations between the two entanglement-breaking channels. In this scenario, despite entanglement cannot be distributed by single transmission (Charlie cannot be entangled with Alice or Bob), still it can be distributed via the double transmission (so that Alice and Bob can become entangled). This reactivation of entanglement distribution is possible in the presence of classical correlations, i.e., for an environment (systems E_1 and E_2) in a purely-classical state (separable, with zero-discord).

In this paper we show that the previous implication is false when we introduce correlations (i.e., a memory) between the two entanglement-breaking channels. In other

words, in the presence of correlated-noise environments, the double transmission can successfully distribute entanglement despite the single transmission being subject to entanglement-breaking. This is equivalent to say that Charlie can transmit entanglement to Alice and Bob, despite not being able to share any entanglement with them. The most interesting fact is that the entanglement distribution via the double transmission is reactivated by the presence of separable and purely-classical correlations in the joint environment. This effect is proven for quantum systems with Hilbert spaces of any dimension, both finite (qudits) and infinite (continuous variable systems [3, 4]).

In particular, here we are interested in showing the simplest examples of correlated-noise environments which allow for a *perfect distribution* of entanglement via the double transmission (2-system entanglement-preserving) while preventing any entanglement distribution via the single transmission (1-system entanglement-breaking). These environments are constructed by using the so-called twirling operators $U \otimes U$ (or $U \otimes U^*$). A random unitary U is applied to system A and the same unitary (or its conjugate) is applied to system B. While the local action of a random unitary ($U \otimes I$ or $I \otimes U$) is entanglement-breaking, the correlated action ($U \otimes U$) perfectly preserves specific classes of entangled states (belonging to decoherent-free subspaces of the joint correlated environment).

Since these "twirling environments" are based on local operations and classical communication (LOCC), they are expected to introduce correlations which are separable (local) and, more precisely, purely-classical. This feature can be checked by considering a unitary dilation where an explicit system for the environment is introduced. For the twirling environments, such a system can be described by a classical state, i.e., separable with zero quantum discord.

Twirling environments can easily be constructed for quantum systems of any dimension. In the case of two qudits (each with Hilbert space of dimension d), the randomization of the twirling operators $U \otimes U$ (or $U \otimes U^*$) is performed over the entire unitary group. In this case, it is easy to identify states which are invariant under $U \otimes U$-twirling (Werner states [5]) and $U \otimes U^*$-twirling (isotropic states [6]). In the specific case of qubits ($d = 2$), we can restrict the randomization to the basis of the Pauli operators, with the qubit Werner state being invariant under Pauli twirling. Things are less trivial for infinite dimension, in particular, for bosonic modes. In this case, we restrict the twirling operators to the compact group of orthogonal symplectic transformations, i.e., phase-space rotations. The bosonic twirling environment so defined is non-Gaussian. It is interesting to see that, only for the $U \otimes U^*$-twirling, we can identify Gaussian states which are invariant and entangled: These are the two mode squeezed vacuum states, also known as Einstein-Podolsky-Rosen (EPR) states [4, 7].

In terms of potential impact, our work opens new pos-

sibilities for entanglement distribution in correlated-noise environments and memory channels, where the presence of correlations can be exploited to recover from entanglement breaking. Since entanglement recovery can be achieved by the injection of separable purely-classical correlations, our work poses fundamental questions on the intimate relations between local and nonlocal correlations and, more generally, between classical and quantum correlations.

The paper is structured as follows. In Sec. II, we consider qubits and we show the simplest twirling environments (correlated Pauli environments). In Sec. III, we consider the general case of qudits evolving in multidimensional twirling environments. These results can also be applied to the case of qubits. Then, in Sec. IV, we consider bosonic systems and their evolution under non-Gaussian twirling environments which are based on correlated phase-space rotations. Finally, Sec. V is for conclusion, with a number of Appendices A, B, C, D and E containing simple proofs and technical details.

II. QUBITS IN CORRELATED PAULI ENVIRONMENTS

The most strikingly simple example can be constructed for qubits considering the basis of the four Pauli operators I, X, $Y = iXZ$ and Z [8]. Given an arbitrary input state ρ_{AB} of two qubits, we consider the correlated Pauli channel

$$\mathcal{E}(\rho_{AB}) = \sum_{k=0}^{3} p_k \, (P_k \otimes P_k)\rho_{AB}(P_k \otimes P_k)^\dagger \, , \quad (1)$$

where $P_k \in \{I, X, Y, Z\}$ and p_k are probabilities. This channel is clearly simulated by random LOCCs. In fact, it is equivalent to extract a random variable $K = \{k, p_k\}$, apply the Pauli unitary P_k to qubit A, communicate k and then apply the same unitary P_k to qubit B. It is easy to check that the two-qubit channel of Eq. (1) does not change if we replace the Pauli twirling operator $P_k \otimes P_k$ with the alternative operator $P_k \otimes P_k^*$.

It is easy to write the unitary dilation of the correlated Pauli channel. It is sufficient to introduce an environment composed by two systems E_1 and E_2, each being a qudit with dimension $d = 4$ and orthonormal basis $\{|k\rangle\}_{k=0}^{3}$. Then, we can write

$$\mathcal{E}(\rho_{AB}) = \mathrm{Tr}_{E_1 E_2} \left[U(\rho_{AB} \otimes \rho_{E_1 E_2})U^\dagger \right] \, , \quad (2)$$

where the environment is prepared in the correlated state

$$\rho_{E_1 E_2} = \sum_{k=0}^{3} p_k \, |k\rangle_{E_1} \langle k| \otimes |k\rangle_{E_2} \langle k| \, , \quad (3)$$

and the unitary interaction $U = U_{E_1 A} \otimes U_{E_2 B}$ is a tensor

product of two control-Pauli unitaries,

$$U_{E_1A} = \sum_{k=0}^{3} |k\rangle_{E_1} \langle k| \otimes P_k, \ U_{E_2B} = \sum_{k=0}^{3} |k\rangle_{E_2} \langle k| \otimes P_k.$$
(4)

As evident from Eq. (3), the state of the environment is separable, which means that only separable (i.e., local-type) correlations are injected into the travelling qubits. More precisely, since $\rho_{E_1E_2}$ is expressed as a convex combination of orthogonal projectors, it is a purely-classical state, i.e., a state with zero quantum discord [9]. As a result, this environment contains correlations which are not only local but also purely classical.

Now we show the conditions under which the correlated Pauli environment is simultaneously one-qubit entanglement-breaking and two-qubit entanglement preserving. We start by considering the transmission of one qubit only, e.g., qubit A. In this case, Eq. (1) reduces to a depolarizing channel

$$(\mathcal{E}_A \otimes \mathcal{I}_B)(\rho_{AB}) = \sum_{k=0}^{3} p_k (P_k \otimes I) \rho_{AB} (P_k^\dagger \otimes I)$$

$$= p_0 \rho_{AB} + \sum_{k=1}^{3} p_k (P_k \otimes I) \rho_{AB} (P_k^\dagger \otimes I).$$
(5)

It is easy to show that $\mathcal{E}_A$ is entanglement-breaking when $p_k \leq 1/2$ for any k (see Appendix A for a simple proof). A particular choice can be $p_0 \leq 1/2$ and $p_1 = p_2 = p_3 = (1 - p_0)/3$ as for instance used in Ref. [10].

Assuming the condition of one-qubit entanglement-breaking ($p_k \leq 1/2$), Charlie is clearly not able to share any entanglement with Alice or Bob. Can he still distribute entanglement to Alice and Bob? Yes, this is possible because we can identify a class of entangled states which are invariant under the action of the correlated map (1). This class is simply given by the Werner states

$$\rho_{AB}(\gamma) := (1 - \gamma)\frac{I_{AB}}{4} + \gamma |-\rangle_{AB} \langle -| \ ,$$
(6)

with parameter $-1/3 \leq \gamma \leq 1$, where $I_{AB}/4$ is the maximally-mixed state and

$$|-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B)$$
(7)

is the maximally-entangled (singlet) state. For $\gamma > 1/3$, the two-qubit state $\rho_{AB}(\gamma)$ is known to be entangled and distillable. Since qubit Werner states are invariant under any twirling operator $U \otimes U$, i.e.,

$$(U \otimes U)\rho_{AB}(\gamma)(U \otimes U)^\dagger = \rho_{AB}(\gamma) \ ,$$
(8)

for any unitary U, they are fixed points of the correlated map (1) or, in other words, they represent a decoherence-free subspace of the correlated Pauli environment. Thus, if Charlie sends Werner states with $\gamma > 1/3$, these entangled states are perfectly distributed to Alice and Bob (two-qubit entanglement preserving).

III. QUDITS IN MULTIDIMENSIONAL TWIRLING ENVIRONMENTS

In this section we consider quantum systems whose Hilbert space has finite dimension d, i.e., qudits (in particular, we have qubits for $d = 2$). For these systems, we can easily construct classically-correlated environments which are simultaneously 1-qudit entanglement-breaking and 2-qudit entanglement-preserving.

Consider two qudits, A and B, with same dimension d and prepared in a bipartite state ρ_{AB}. Then, we call $U \otimes U$ twirling channel the following completely positive trace-preserving map

$$\mathcal{E}_{UU}(\rho_{AB}) = \int_{\mathcal{U}(d)} dU \ (U \otimes U)\rho_{AB}(U \otimes U)^\dagger \ ,$$
(9)

where the integral is over the entire unitary group $\mathcal{U}(d)$ acting on the d-dimensional Hilbert space, and dU is the Haar measure. This channel is clearly realizable by random LOCCs. In fact, it is equivalent to choose a random unitary U, apply it to the local system A, and then apply the same U to the other local system B (where the coordination of the two local unitaries is mediated by classical communication). Similarly, we can define a $U \otimes U^*$ twirling channel, by replacing the twirling operator $U \otimes U$ with the alternative twirling $U \otimes U^*$ in the definition of Eq. (9). Compactly, we refer to the $U \otimes V$ twirling channel

$$\mathcal{E}_{UV}(\rho_{AB}) = \int_{\mathcal{U}(d)} dU \ (U \otimes V)\rho_{AB}(U \otimes V)^\dagger \ ,$$
(10)

where $V = U$ or $V = U^*$.

In order to study its correlation properties we dilate this channel into an environment. Note that, since we have an integral in Eq. (10), the dilation of the channel seems to involve the introduction of continuous variable systems. In fact, the unitary group $\mathcal{U}(d)$ is described by d^2 real parameters [11], which means that we would need to employ d^2 continuous variable systems for the environment. Actually, this continuous dilation is not necessary, since can always replace the previous Haar integral with a discrete sum over a finite number of suitably-chosen unitaries. In fact, any twirling channel (10) can be written as

$$\mathcal{E}_{UV}(\rho_{AB}) = \frac{1}{K} \sum_{k=0}^{K-1} (U_k \otimes V_k)\rho_{AB}(U_k \otimes V_k)^\dagger \ ,$$
(11)

where U_k belongs to the set of unitary 2-design $\mathcal{D}$ [12, 13] and $V_k = U_k$ or $V_k = U_k^*$. The set $\mathcal{D}$ has a finite number of elements which depends of the dimension of the Hilbert space $K = K(d)$ (too see how the cardinality K scales with the dimension d, see for instance Ref. [14]). The proof of the equivalence between Eqs. (10) and (11) can be found in Ref. [12] for the $U \otimes U$ twirling channel. See Appendix B for a simple extension of the proof to the other $U \otimes U^*$ twirling channel. Note that, in the case of

qubits ($d = 2$), an example of unitary 2-design is provided by the Clifford group [12, 15], which is the normalizer of the Pauli group and typically employed in quantum error correction [16, 17].

Now using the unitary 2-design, we can dilate the twirling channel into an environment made by finite-dimensional systems, i.e., two larger qudits E_1 and E_2, each with dimension K and orthonormal basis $\{|k\rangle\}_{k=0}^{K-1}$. In fact, we can write

$$\mathcal{E}_{UV}(\rho_{AB}) = \text{Tr}_{E_1 E_2}\left[U(\rho_{AB} \otimes \rho_{E_1 E_2})U^\dagger\right] , \quad (12)$$

where the environment is prepared in the uniformly correlated state

$$\rho_{E_1 E_2} = \frac{1}{K}\sum_{k=0}^{K-1} |k\rangle_{E_1}\langle k| \otimes |k\rangle_{E_2}\langle k| , \quad (13)$$

and the unitary interaction $U = U_{E_1 A} \otimes U_{E_2 B}$ is a tensor product of two control-unitaries

$$U_{E_1 A} = \sum_{k=0}^{K-1} |k\rangle_{E_1}\langle k| \otimes U_k, \ U_{E_2 B} = \sum_{k=0}^{K-1} |k\rangle_{E_2}\langle k| \otimes V_k, \quad (14)$$

where $U_k \in \mathcal{D}$ and $V_k = U_k$ or $V_k = U_k^*$. As evident from Eq. (13), the state of the environment is separable and purely-classical (zero discord). In other words, twirling environments only contain purely-classical correlations.

Once we have characterized the correlation properties of these environments, we show the conditions under which they are simultaneously one-qudit entanglement-breaking and two-qudit entanglement preserving. First of all, let us explicitly show that one-qudit transmission is always subject to entanglement breaking. Suppose that only qudit A is transmitted by Charlie. Then, for any input state ρ_{AB}, the output state of Alice and Charlie is given by

$$(\mathcal{E}_A \otimes \mathcal{I}_B)(\rho_{AB}) =$$
$$\int_{\mathcal{U}(d)} dU \ (U \otimes I)\rho_{AB}(U^\dagger \otimes I) = \frac{1}{d} I \otimes \text{Tr}_A(\rho_{AB}) , \quad (15)$$

which means that the random map $U \otimes I$ represents an entanglement-breaking channel (similar result holds for the other random map $I \otimes V$ involved in the transmission of the other qudit B). As shown in Appendix C, the proof of Eq. (15) is a simple application of the identity

$$\langle O\rangle_U := \int_{\mathcal{U}(d)} dU \ UOU^\dagger = \frac{\text{Tr}(O)}{d} I , \quad (16)$$

which is the Haar average of a linear operator O. In turn, Eq. (16) is a simple consequence of Schur's lemma and the invariance of the Haar measure [18].

The next step is to consider two-qudit transmission from Charlie to Alice and Bob. In this case, we search for entangled states which are preserved by the correlated action of the twirling environment. Luckily, we can easily find states which are invariant under the action of the twirling operator $U \otimes V$, i.e.,

$$(U \otimes V)\rho_{AB}(U \otimes V)^\dagger = \rho_{AB} . \quad (17)$$

Thanks to this invariance, such states are fixed points of the $U \otimes V$ twirling channel of Eq. (10).

In the specific case of $V = U$, it is well known that the unique solution of Eq. (17) is provided by the multidimensional Werner states, which are themselves defined as those states invariant under $U \otimes U$ twirling [5]. Given two isodimensional qudits, A and B, their $d \times d$ Werner state is a one-parameter class defined by [5, 19]

$$\rho_{AB}(\mu) := \frac{1}{d^2 + d\mu}(I_{AB} + \mu V) \quad (18)$$

where $-1 \le \mu \le 1$ and V is the unitary flip operator $V|\varphi\rangle_A \otimes |\psi\rangle_B = |\psi\rangle_A \otimes |\varphi\rangle_B$. This state is known to be entangled for $\mu < -d^{-1}$. Thus, if Charlie has a Werner state $\rho_{AB}(\mu)$ with suitable μ (in the entanglement regime), he is able to perfectly transmit his state to Alice and Bob, who can then share and distill entanglement. This entanglement distribution from Charlie to Alice and Bob is possible, despite Charlie cannot share any entanglement with the remote parties due to the entanglement breaking condition of Eq. (15).

Coming back to Eq. (17), one can find a similar solution for $V = U^*$. In fact, as shown in Ref. [6], there exist states which are invariant under $U \otimes U^*$-twirling. These are called isotropic states, and they are defined by the one-parameter class [6]

$$\rho_{AB}(\gamma) := (1 - \gamma)\frac{I_{AB}}{d^2} + \gamma |\psi\rangle_{AB}\langle\psi| , \quad (19)$$

where the maximally mixed state $d^{-2}I_{AB}$ and the maximally entangled state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} |k\rangle_A |k\rangle_B , \quad (20)$$

are combined with parameter $-(d^2 - 1)^{-1} \le \gamma \le 1$. In general, it is entangled and distillable for $\gamma > (1 + d)^{-1}$. Thus, if Charlie has an isotropic state $\rho_{AB}(\gamma)$ with suitable γ (i.e., in the entanglement regime), he is able to perfectly transmit this state to Alice and Bob, who therefore can share and distill entanglement. Again, this is possible despite the transmission of a single qudit is subject to an entanglement-breaking channel, as expressed by Eq. (15).

It is clear that these results can be specialized to the case of qubits ($d = 2$). For qubits, the classes of multidimensional Werner states of Eq. (18) and isotropic states of Eq. (19) coincide up to a local unitary [6]. Multidimensional Werner states reduce to the qubit Werner state of Eq. (6) which is $U \otimes U$-invariant. In fact, for $d = 2$, we have $(I_{AB} + \mu V) = (\mu + 1)I_{AB} - 2\mu |-\rangle_{AB}\langle-|$ which, replaced in Eq. (18), gives the state of Eq. (6) by setting $\gamma = -\mu/(2 + \mu)$.

On the other hand, isotropic states reduce to Eq. (6), proviso that the singlet $|-\rangle_{AB}$ is replaced by the triplet

$$|+\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B \right) . \qquad (21)$$

This state is $U \otimes U^*$-invariant and known as Werner-like state. Since singlet and triplet states are connected by a local unitary, there is no difference in the quantum correlations which are contained in the state according to the two definitions. More generally, in a Werner-like state, any maximally entangled state could be considered in the place of the singlet.

IV. BOSONIC TWIRLING ENVIRONMENTS

Here we extend the analysis to the case of continuous variable systems, i.e., quantum systems with infinite dimensional Hilbert spaces ($d = \infty$). In particular, we consider the case of two bosonic modes of the electromagnetic field. The simplest generalization of the notion of twirling environment involves the use of rotations in the phase space. Given a single bosonic mode with number operator $\hat{n}$, the rotation operator is defined as $\hat{R}_\theta = \exp(-i\theta\hat{n})$. In the phase space, the action of this operator is described by the well-known rotation matrix

$$\mathbf{R}_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} . \qquad (22)$$

In terms of the second-order statistical moments, we have that the covariance matrix (CM) $\mathbf{V}$ of the input mode is transformed via the congruence

$$\mathbf{V} \rightarrow \mathbf{R}_\theta \mathbf{V} \mathbf{R}_\theta{}^T . \qquad (23)$$

Now, given an input state ρ_{AB} of two modes, A and B, we can synchronize two random rotations and define the bosonic twirling channel

$$\mathcal{E}_{\theta\theta'}(\rho_{AB}) = \int \frac{d\theta}{2\pi} (\hat{R}_\theta \otimes \hat{R}_{\theta'}) \rho_{AB} (\hat{R}_\theta \otimes \hat{R}_{\theta'})^\dagger, \quad (24)$$

where $\theta' = \theta$ or $\theta' = -\theta$. This is a non-Gaussian channel, since the twirling operator $\hat{R}_\theta \otimes \hat{R}_{\theta'}$, despite Gaussian, is not averaged using a Gaussian distribution but a uniform one. It is clearly based on random LOCCs, since random rotations are locally applied to each bosonic mode and they are correlated via classical communication.

It is interesting that the unitary dilation of this channel can be restricted to a finite-dimensional environment. The reason is because the single-mode rotation operator $\hat{R}_\theta$ belongs to the compact subgroup of the orthogonal symplectic transformations $\mathcal{K}(2) = Sp(2) \cap \mathcal{O}(2)$ (which are passive Gaussian unitaries, i.e., unitary transformations preserving both the Gaussian statistics and the energy of the state). Then, $\mathcal{K}(2)$ is isomorphic to the unitary group $\mathcal{U}(1)$, which is the multiplicative group composed by all complex numbers with module 1, also known

as the circle group. For this reason, a unitary 2-design $\mathcal{D} \subset \mathcal{U}(1)$ can be mapped into a unitary 2-design for $\mathcal{K}(2)$ [14]. As a result, we can write

$$\mathcal{E}_{\theta\theta'}(\rho_{AB}) = \frac{1}{K} \sum_{k=0}^{K-1} (\hat{R}_{\theta_k} \otimes \hat{R}_{\theta'_k}) \rho_{AB} (\hat{R}_{\theta_k} \otimes \hat{R}_{\theta'_k})^\dagger, \quad (25)$$

for a suitable set of angles $\{\theta_0, \ldots, \theta_{K-1}\}$ and where $\theta'_k = \theta_k$ or $\theta'_k = -\theta_k$. In this form, the channel is manifestly non Gaussian. Then, as before, it can be represented using two environmental qudits, E_1 and E_2, prepared in a correlated state $\rho_{E_1 E_2}$ as in Eq. (13) and interacting with the two bosonic modes via two control-unitaries as in Eq. (14), where now the unitaries are rotations in the phase space. The environmental state is not only separable but also purely-classical (zero discord), which means that only classical correlations are injected by the bosonic twirling environment.

It is easy to show that one-mode transmission is always subject to entanglement-breaking in this environment. For instance, if mode A is transmitted from Charlie to Alice, then the output state

$$\rho_{A'B} = \int \frac{d\theta}{2\pi} (\hat{R}_\theta \otimes I) \rho_{AB} (\hat{R}_\theta \otimes I)^\dagger \qquad (26)$$

is separable, no matter what the input state ρ_{AB} is. Indeed it is easy to prove that a uniformly dephasing channel as that of Eq. (26) is entanglement-breaking. For the sake of completeness, we give this simple proof in Appendix D.

The next step is to find two-mode states which are invariant under correlated phase rotations

$$(\hat{R}_\theta \otimes \hat{R}_{\theta'}) \rho_{AB} (\hat{R}_\theta \otimes \hat{R}_{\theta'})^\dagger = \rho_{AB} , \qquad (27)$$

so that they are perfectly transmitted by the bosonic twirling environment

$$\mathcal{E}_{\theta\theta'}(\rho_{AB}) = \rho_{AB} . \qquad (28)$$

For simplicity we restrict our search to zero-mean Gaussian states, therefore completely characterized by their CMs. Let us call $\mathbf{V}_{AB}$ the CM of an input Gaussian state ρ_{AB}. Then, finding a solution of Eq. (27) is equivalent to solve

$$(\mathbf{R}_\theta \oplus \mathbf{R}_{\theta'}) \mathbf{V}_{AB} (\mathbf{R}_\theta \oplus \mathbf{R}_{\theta'})^T = \mathbf{V}_{AB} . \qquad (29)$$

Depending on the type of environment, i.e., $\theta' = \theta$ (perfect correlation) or $\theta' = -\theta$ (perfect anti-correlation), we have two different classes of invariant Gaussian states.

Unfortunately, in the case of the $\hat{R}_\theta \otimes \hat{R}_\theta$ environment, the invariant Gaussian states are separable. In fact, it is easy to check that, for $\theta' = \theta$ and arbitrary θ, the unique solution of Eq. (29) is given by the quasi-normal form

$$\mathbf{V}_{AB} := \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix} = \begin{pmatrix} \alpha & & \omega & \varphi \\ & \alpha & -\varphi & \omega \\ \omega & -\varphi & \beta & \\ \varphi & \omega & & \beta \end{pmatrix} , \qquad (30)$$

with $\alpha, \beta \geq 1$ and ω, δ are real numbers (which must satisfy a set of bona-fide conditions in order to make the previous matrix a quantum CM [20]). It is easy to check that the previous CM can only describe separable Gaussian states. See Appendix E to see how to derive the CM of Eq. (30) and check its separability.

Thus, despite there exist two-mode Gaussian states ρ_{AB} which are invariant under perfectly-correlated phase rotations $\hat{R}_\theta \otimes \hat{R}_\theta$, these states must be separable. This negative result can be generalized: No entangled Gaussian state is invariant under twirlings of the form $U \otimes U$, with U Gaussian unitary (apart from the trivial case $U = \pm I$). In fact, suppose that we have an input Gaussian state ρ_{AB} with mean value $\bar{\mathbf{x}}_{AB}$ and covariance CM $\mathbf{V}_{AB}$. The action of two Gaussian unitaries $U \otimes U$ on ρ_{AB} corresponds to apply two identical displacements to its mean value

$$\bar{\mathbf{x}}_{AB} \to \bar{\mathbf{x}}_{AB} + (\mathbf{d}, \mathbf{d})^T , \qquad (31)$$

and two identical symplectic matrices to its CM

$$\mathbf{V}_{AB} \to (\mathbf{S} \oplus \mathbf{S}) \mathbf{V}_{AB} (\mathbf{S} \oplus \mathbf{S})^T . \qquad (32)$$

In general, there is clearly no possibility to find an invariant Gaussian state, since any nonzero displacement $\mathbf{d}$ maps the input state into a different output state. We then restrict the search to considering canonical Gaussian unitaries ($\mathbf{d} = \mathbf{0}$) which are one-to-one with the symplectic transformations. Unfortunately, this is still not the case. According to Euler's decomposition [4], any single-mode symplectic transformation $\mathbf{S}$ is generally decomposed into a orthogonal rotation $\mathbf{R}_\theta$, a single-mode squeezing $\mathbf{S}_r$, and another orthogonal rotation $\mathbf{R}_\omega$, where θ, ω are angles and $r \geq 1$ is a squeezing parameter. As long as squeezing is present ($r > 1$), we have that the trace of the CM changes (physically this corresponds to injecting energy into the state). As a result, the CM and, therefore, the Gaussian state must change. Thus, the only possibility is to find Gaussian states which are invariant under rotations only (which are passive transformations, i.e., preserving the trace). However, we have already seen that, despite they exist, these Gaussian states must be separable.

Luckily, the scenario is completely different when we consider the other type of environment. We can easily find entangled Gaussian states which are invariant under anti-correlated phase rotations $\hat{R}_\theta \otimes \hat{R}_{-\theta}$. One can check that, for $\theta' = -\theta$ and arbitrary θ, the unique solution of Eq. (29) is given by the CM

$$\mathbf{V}_{AB} := \begin{pmatrix} \mu \mathbf{I} & \sqrt{\mu^2 - 1} \mathbf{Z} \\ \sqrt{\mu^2 - 1} \mathbf{Z} & \mu \mathbf{I} \end{pmatrix} , \qquad (33)$$

where $\mu \geq 1$, $\mathbf{I}$ is the 2×2 identity matrix, and $\mathbf{Z} = \mathrm{diag}(1, -1)$ is the reflection matrix. This is the CM of a two-mode squeezed vacuum state, i.e., an EPR state [4]. Thus, in the presence of a $\hat{R}_\theta \otimes \hat{R}_{-\theta}$ twirling channel, despite Charlie is not able to share any entanglement with

Alice or Bob (one-mode entanglement breaking), he is still able to distribute entanglement to them by transmitting EPR states perfectly (two-mode entanglement preserving). As discussed in Ref. [21], a more general class of $\hat{R}_\theta \otimes \hat{R}_{-\theta}$ invariant states is given by the continuous variable Werner states (which are generally non-Gaussian, and they are constructed by mixing an EPR state with a tensor product of thermal states).

V. CONCLUSION AND DISCUSSION

In conclusion, we have investigated the distribution of entanglement in the presence of correlated-noise environments, in particular, twirling environments. We have considered quantum systems with Hilbert spaces of any dimension, i.e., qubits, qudits, and bosonic systems. We have assumed the condition of one-system entanglement breaking, meaning that the transmission of a single system, e.g., from Charlie to Alice, cannot distribute any entanglement. Despite this, we have shown that the distribution of entanglement is still possible when we consider the double transmission, i.e., from Charlie to both Alice and Bob. In particular, we can identify classes of entangled states which are invariant under the action of the composite environment, which means that the entanglement is perfectly preserved in the two-system transmission.

This effect must be ascribed to the correlations which are injected into the travelling systems by the twirling environment. Interestingly, these environmental noise-correlations are separable, i.e., local-type, and more precisely purely-classical, since no quantum discord can be found in the state of the environment. The fact that separability, and in particular, classicality, can be exploited to recover from entanglement-breaking is a paradoxical behavior which poses fundamental questions on the intimate relations between classical and quantum correlations.

It is important to note that, despite twirling environments being very simple examples, they are also quite artificial. As a matter of fact, such kind of perfectly correlated quantum operations are typically used by Alice and Bob in protocols of entanglement distillation (where the random twirling $U \otimes U$ is applied to transform bipartite states into Werner states, which are then distilled into maximally entangled states).

Luckily, we can also prove that the reactivation of entanglement distribution occurs in more realistic scenarios. An important non-trivial example can be given for bosonic systems. Ref. [21] considers a realistic model of correlated-noise Gaussian environment, which generalizes the standard memoryless thermal-loss environment. In this Gaussian environment, the presence of weak separable correlations is sufficient to reactivate the distribution of entanglement from Charlie to Alice and Bob, despite the thermal noise present in the single transmissions (Charlie-Alice or Charlie-Bob) being entanglement-

breaking. This case is non-trivial also because we cannot identify any decoherent-free subspace of entangled Gaussian states, which means that Gaussian entanglement cannot be preserved in the double transmission. Despite perfect preservation of entanglement being not possible, Charlie can still use the double transmission to distribute a distillable amount of entanglement to the remote parties by sending EPR states with sufficiently large squeezing.

VI.   ACKNOWLEDGEMENTS

Appendix A: Entanglement-Breaking conditions for qubit depolarizing channels

Here we show the conditions under which the depolarizing channel of Eq. (5) becomes an entanglement-breaking channel. This means to find a specific regime for the probabilities p_k characterizing the channel.

First of all note that, for Hilbert spaces of finite dimension d, a simple way to check if a quantum channel $\mathcal{E}$ is entanglement-breaking is to test it on the maximally-entangled state $|\psi\rangle_{AB}$ of Eq. (20). In other words, if $(\mathcal{E}_A \otimes \mathcal{I}_B)|\psi\rangle_{AB}\langle\psi|$ is separable, then $(\mathcal{E}_A \otimes \mathcal{I}_B)\rho_{AB}$ is separable for any input state ρ_{AB} [1]. In the case of qubits, we can test the channel on the triplet state $|+\rangle_{AB}$ of Eq. (21). We then compute the output state

$$\Phi := (\mathcal{E}_A \otimes \mathcal{I}_B)(|+\rangle_{AB}\langle+|)$$

$$= \sum_{k=0}^{3} p_k (P_k \otimes I)|+\rangle_{AB}\langle+|(P_k^\dagger \otimes I)$$

$$= p_0 |+\rangle_{AB}\langle+|$$

$$+ p_1 (X \otimes I)|+\rangle_{AB}\langle+|(X \otimes I) \qquad (A1)$$

$$+ p_2 (Y \otimes I)|+\rangle_{AB}\langle+|(Y^\dagger \otimes I)$$

$$+ p_3 (Z \otimes I)|+\rangle_{AB}\langle+|(Z \otimes I) . \qquad (A2)$$

Adopting the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and using $X|u\rangle = |u \oplus 1\rangle$, $Z|u\rangle = (-1)^u|u\rangle$ and $Y = iXZ$, we get

$$\Phi = \sum_{ijkl} \Phi_{ijkl}|i,j\rangle_{AB}\langle k,l| , \qquad (A3)$$

where the coefficients $\Phi_{ijkl} = \langle i,j|\Phi|k,l\rangle$ are the elements of the following density matrix

$$\mathbf{\Phi} = \frac{1}{2}\begin{pmatrix} p_0+p_3 & 0 & 0 & p_0-p_3 \\ 0 & p_1+p_2 & p_1-p_2 & 0 \\ 0 & p_1-p_2 & p_1+p_2 & 0 \\ p_0-p_3 & 0 & 0 & p_0+p_3 \end{pmatrix} . \qquad (A4)$$

To check the separability properties we adopt the Peres-Horodecki criterion [22, 23]. This corresponds to compute the partial transposition (PT) of the state which is given by the following linear map

$$\Phi = \sum_{ijkl} \Phi_{ijkl}|i\rangle_A\langle k| \otimes |j\rangle_B\langle l|$$

$$\to \text{PT}(\Phi) = \sum_{ijkl} \Phi_{ijkl}|i\rangle_A\langle k| \otimes (|j\rangle_B\langle l|)^T$$

$$= \sum_{ijkl} \Phi_{ijkl}|i\rangle_A\langle k| \otimes |l\rangle_B\langle j|$$

$$= \sum_{ijkl} \Phi_{ilkj}|i\rangle_A\langle k| \otimes |j\rangle_B\langle l| . \qquad (A5)$$

At the level of the density matrix we then have

$$\mathbf{\Phi} = ((\Phi_{ijkl})) \to \text{PT}(\Phi) = ((\Phi_{ilkj})) , \qquad (A6)$$

i.e., $j \longleftrightarrow l$ swapping. It is easy to check that the partially-transpose matrix

$$\text{PT}(\mathbf{\Phi}) = \frac{1}{2}\begin{pmatrix} p_0+p_3 & 0 & 0 & p_1-p_2 \\ 0 & p_1+p_2 & p_0-p_3 & 0 \\ 0 & p_0-p_3 & p_1+p_2 & 0 \\ p_1-p_2 & 0 & 0 & p_0+p_3 \end{pmatrix} \qquad (A7)$$

has eigenvalues

$$\lambda_k = \frac{1}{2} - p_k \quad (k = 0,1,2,3) . \qquad (A8)$$

Thus the partially-transposed state has the following spectral decomposition

$$\text{PT}(\Phi) = \sum_{k=0}^{3}\left(\frac{1}{2} - p_k\right)|\eta_k\rangle\langle\eta_k| , \qquad (A9)$$

with $|\eta_k\rangle$ orthogonal eigenstates. This operator is positive (≥ 0) if and only if

$$p_k \leq \frac{1}{2} , \text{ for } k = 0,1,2,3 . \qquad (A10)$$

As a result, the output state Φ is separable (and the channel is entanglement-breaking) if and only if $p_k \leq 1/2$ for any k, as reported in the main text.

Appendix B: Unitary 2-design for the $U \otimes U^*$ twirling channel

Let us consider two qudits with the same dimension d, so that the composite system is described by an Hilbert

space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ with finite dimension d^2. From the literature [12, 14], we know that we can write the following equality for any input state ρ_{AB}

$$\mathcal{E}_{UU}(\rho_{AB}) := \int_{\mathcal{U}(d)} dU \ (U \otimes U)\rho_{AB}(U \otimes U)^\dagger \quad \text{(B1)}$$

$$= \frac{1}{K} \sum_{k=0}^{K-1} (U_k \otimes U_k)\rho_{AB}(U_k \otimes U_k)^\dagger \ , \quad \text{(B2)}$$

which is valid for $U_k \in \mathcal{D}$, where $\mathcal{D}$ is a unitary 2-design with K elements. Here we can easily show that

$$\mathcal{E}_{UU^*}(\rho_{AB}) := \int_{\mathcal{U}(d)} dU \ (U \otimes U^*)\rho_{AB}(U \otimes U^*)^\dagger \quad \text{(B3)}$$

$$= \frac{1}{K} \sum_{k=0}^{K-1} (U_k \otimes U_k^*)\rho_{AB}(U_k \otimes U_k^*)^\dagger \ , \quad \text{(B4)}$$

where U_k belongs to the same design $\mathcal{D}$ as before. In a few words, the two twirling channels, $\mathcal{E}_{UU}$ and $\mathcal{E}_{UU^*}$, can be decomposed using the same unitary 2-design.

In the first step of the proof we show that $\mathcal{E}_{UU}$ and $\mathcal{E}_{UU^*}$ are connected by a partial transposition. Consider an arbitrary input state ρ_{AB} decomposed in the orthonormal basis of $\mathcal{H}$ [24]

$$\rho_{AB} = \sum_{ijkl} \rho_{ij}^{kl} |i\rangle_A \langle j| \otimes |k\rangle_B \langle l| \ . \quad \text{(B5)}$$

Its partial transposition corresponds to the transposition of system B only, i.e.,

$$\text{PT}(\rho_{AB}) = \sum_{ijkl} \rho_{ij}^{kl} |i\rangle_A \langle j| \otimes |l\rangle_B \langle k| \ . \quad \text{(B6)}$$

Then, we prove that

$$\mathcal{E}_{UU^*}(\rho_{AB}) = \text{PT}\{\mathcal{E}_{UU}[\text{PT}(\rho_{AB})]\} \ . \quad \text{(B7)}$$

In fact, by linearity we have

$$\mathcal{E}_{UU}[\text{PT}(\rho_{AB})] = \int_{\mathcal{U}(d)} dU \ (U \otimes U)\text{PT}(\rho_{AB})(U \otimes U)^\dagger$$

$$= \sum_{ijkl} \rho_{ij}^{kl} \int_{\mathcal{U}(d)} dU \ U |i\rangle_A \langle j| U^\dagger \otimes U |l\rangle_B \langle k| U^\dagger. \quad \text{(B8)}$$

Since $[U |l\rangle_B \langle k| U^\dagger]^T = U^* |k\rangle_B \langle l| (U^*)^\dagger$ we get

$$\text{PT}\{\mathcal{E}_{UU}[\text{PT}(\rho_{AB})]\} =$$

$$= \sum_{ijkl} \rho_{ij}^{kl} \int_{\mathcal{U}(d)} dU \ U |i\rangle_A \langle j| U^\dagger \otimes U^* |k\rangle_B \langle l| (U^*)^\dagger$$

$$= \int_{\mathcal{U}(d)} dU (U \otimes U^*)\rho_{AB}(U \otimes U^*)^\dagger = \mathcal{E}_{UU^*}(\rho_{AB}) \ . \quad \text{(B9)}$$

Now the second step is to combine Eq. (B7) with the unitary 2-design for $\mathcal{E}_{UU}$. First it is important to note

that the equivalence between Eqs. (B1) and (B2) is valid not only when ρ_{AB} is a density operator but, more generally, when it is an Hermitian linear operator. This extension is straightforward to prove. Suppose that the linear operator $O : \mathcal{H} \to \mathcal{H}$ is Hermitian. Then its spectral decomposition involves real eigenvalues and orthonormal eigenvectors, i.e., we can write

$$O = \sum_n O_n |\phi_n\rangle \langle \phi_n| \ , \quad \text{(B10)}$$

where $O_n \in \mathbb{R}$ and $\langle \phi_n | \phi_m \rangle = \delta_{nm}$. Now we can write

$$\mathcal{E}_{UU}(O) := \int_{\mathcal{U}(d)} dU \ (U \otimes U)O(U \otimes U)^\dagger \quad \text{(B11)}$$

$$= \sum_n O_n \int_{\mathcal{U}(d)} dU \ (U \otimes U) |\phi_n\rangle \langle \phi_n| (U \otimes U)^\dagger \quad \text{(B12)}$$

$$= \sum_n O_n \frac{1}{K} \sum_{k=0}^{K-1} (U_k \otimes U_k) |\phi_n\rangle \langle \phi_n| (U_k \otimes U_k)^\dagger \quad \text{(B13)}$$

$$= \frac{1}{K} \sum_{k=0}^{K-1} (U_k \otimes U_k)O(U_k \otimes U_k)^\dagger \ , \quad \text{(B14)}$$

where (B11)→(B12) by linearity, (B12)→(B13) by the fact that $|\phi_n\rangle \langle \phi_n|$ are projectors (and therefore states) and (B13)→(B14) by linearity again.

As a result, we can apply the equivalence between Eqs. (B11) and (B14) to the linear operator $\text{PT}(\rho_{AB})$ which fails to be a density operator when ρ_{AB} is entangled but still it is Hermitian (and unit trace) in the general case. Thus, we can write

$$\mathcal{E}_{UU}[\text{PT}(\rho_{AB})] = \frac{1}{K} \sum_{t=0}^{K-1} (U_t \otimes U_t)\text{PT}(\rho_{AB})(U_t \otimes U_t)^\dagger$$

$$= \frac{1}{K} \sum_{t=0}^{K-1} \sum_{ijkl} \rho_{ij}^{kl} U_t |i\rangle_A \langle j| U_t^\dagger \otimes U_t |l\rangle_B \langle k| U_t^\dagger \ . \quad \text{(B15)}$$

Now, using the connection in Eq. (B7) and the fact that $[U_t |l\rangle_B \langle k| U_t^\dagger]^T = U_t^* |k\rangle_B \langle l| (U_t^*)^\dagger$, we can write

$$\mathcal{E}_{UU^*}(\rho_{AB}) = \text{PT}\{\mathcal{E}_{UU}[\text{PT}(\rho_{AB})]\}$$

$$= \frac{1}{K} \sum_{t=0}^{K-1} \sum_{ijkl} \rho_{ij}^{kl} U_t |i\rangle_A \langle j| U_t^\dagger \otimes U_t^* |k\rangle_B \langle l| (U_t^*)^\dagger$$

$$= \frac{1}{K} \sum_{t=0}^{K-1} (U_t \otimes U_t^*)\rho_{AB}(U_t \otimes U_t^*)^\dagger \ , \quad \text{(B16)}$$

which gives the equivalence between Eqs. (B3) and (B4).

Appendix C: Partial Haar average of a linear operator

In this short appendix we give a simple proof of Eq. (15). Consider an Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ with

finite dimension $d_A d_B$ (where d_A and d_B are generally different). Given a linear operator $T : \mathcal{H} \to \mathcal{H}$, we can always decompose it in an orthonormal basis

$$T = \sum_{ijkl} T_{ij}^{kl} |i\rangle_A \langle j| \otimes |k\rangle_B \langle l| . \tag{C1}$$

Then, we can write the following partial Haar average, where only system A is averaged on the unitary group

$$\langle T \rangle_{U \otimes I} := \int_{\mathcal{U}(d)} dU (U \otimes I) T (U^\dagger \otimes I)$$

$$= \sum_{ijkl} T_{ij}^{kl} \left(\int_{\mathcal{U}(d)} dU \, U |i\rangle_A \langle j| U^\dagger \right) \otimes |k\rangle_B \langle l| . \tag{C2}$$

Now we use Eq. (16) with linear operator $O = |i\rangle_A \langle j|$, which gives

$$\int_{\mathcal{U}(d)} dU \, U |i\rangle_A \langle j| U^\dagger = \delta_{ij} \frac{I}{d_A} . \tag{C3}$$

Then, by replacing this expression in Eq. (C2), we get

$$\langle T \rangle_{U \otimes I} = \frac{I}{d_A} \otimes \sum_{ikl} T_{ii}^{kl} |k\rangle_B \langle l|$$

$$= \frac{I}{d_A} \otimes \mathrm{Tr}_A (T) . \tag{C4}$$

This is a simple extension of Eq. (16) to considering the presence of a second (unaveraged) system B. In particular, for T density operator, we have the result of Eq. (15).

Appendix D: Uniformly dephasing channel is entanglement-breaking

Here we prove that the uniformly dephasing channel of Eq. (26) is entanglement-breaking. First consider a pure input state $\rho_{AB} = |\varphi\rangle_{AB} \langle\varphi|$ expressed in the Fock basis of the two modes

$$|\varphi\rangle_{AB} = \sum_{kj} c_{kj} |k\rangle_A \otimes |j\rangle_B , \quad \sum_{kj} |c_{kj}|^2 = 1 . \tag{D1}$$

Since $\hat{R}_\theta |k\rangle = \exp(-i\theta k) |k\rangle$, we get

$$\rho_{A'B} = \sum_{kjk'j'} c_{kj} c_{k'j'}^* \left(\int \frac{d\theta}{2\pi} e^{-i\theta(k-k')} |k\rangle_A \langle k'| \right) \otimes |j\rangle_B \langle j'|$$

$$= \sum_{kjk'j'} c_{kj} c_{k'j'}^* \delta(k-k') |k\rangle_A \langle k| \otimes |j\rangle_B \langle j'|$$

$$= \sum_{kjj'} c_{kj} c_{kj'}^* |k\rangle_A \langle k| \otimes |j\rangle_B \langle j'| . \tag{D2}$$

Then, by re-distributing the sum, we get

$$\rho_{A'B} = \sum_k \left(\sum_j c_{kj} |kj\rangle \right) \otimes \left(\sum_{j'} c_{kj'}^* \langle kj'| \right)$$

$$= \sum_k d_k \left(\sum_j \frac{c_{kj}}{\sqrt{d_k}} |kj\rangle \right) \otimes \left(\sum_{j'} \frac{c_{kj'}^*}{\sqrt{d_k}} \langle kj'| \right) , \tag{D3}$$

where we have introduced $d_k := \sum_j |c_{kj}|^2$ in the last step (clearly $\sum_k d_k = 1$). Now introducing the pure state

$$|\eta_k\rangle := \sum_j \frac{c_{kj}}{\sqrt{d_k}} |kj\rangle , \tag{D4}$$

we can write the following spectral decomposition for the output state

$$\rho_{A'B} = \sum_k d_k |\eta_k\rangle \langle \eta_k| . \tag{D5}$$

Now we note that we can always write the tensor product

$$|\eta_k\rangle = |k\rangle \otimes |\xi(k)\rangle , \quad |\xi(k)\rangle := \sum_j \frac{c_{kj}}{\sqrt{d_k}} |j\rangle , \tag{D6}$$

so that the output state is manifestly in separable form

$$\rho_{A'B} = \sum_k d_k |k\rangle_{A'} \langle k| \otimes |\xi(k)\rangle_B \langle \xi(k)| . \tag{D7}$$

Proof can trivially be extended to mixed states via their spectral decomposition into pure states.

Appendix E: $\hat{R}_\theta \otimes \hat{R}_\theta$-invariant Gaussian states are separable

To derive the CM of Eq. (30) just check that a 2×2 real matrix $\mathbf{M}$ is invariant under rotations $\mathbf{R}_\theta \mathbf{M} \mathbf{R}_\theta^T = \mathbf{M}$ (or, equivalently, it commutes with rotations $[\mathbf{M}, \mathbf{R}_\theta] = 0$) if and only if it takes the asymmetric form

$$\mathbf{M} = \begin{pmatrix} m & t \\ -t & m \end{pmatrix} , \tag{E1}$$

with m, t real numbers. Thus, the $\mathbf{A}, \mathbf{B}, \mathbf{C}$ blocks of the CM (30) must have this general form, with $\mathbf{A}$ and $\mathbf{B}$ diagonal by the further condition of symmetry.

Then, it is easy to check that CM of Eq. (30) describes a separable Gaussian state. In fact, using suitable local rotations $\mathbf{R}_x \oplus \mathbf{R}_y$ (therefore not changing the separability properties of the state), we can transform $\mathbf{V}_{AB}$ into the simpler form

$$\mathbf{V}'_{AB}(\alpha, \beta, \gamma) = \begin{pmatrix} \alpha\mathbf{I} & \gamma\mathbf{I} \\ \gamma\mathbf{I} & \beta\mathbf{I} \end{pmatrix} , \tag{E2}$$

where $\gamma = \sqrt{\omega^2 + \varphi^2}$. Without loss of generality, suppose that $\beta \geq \alpha$ and set $\beta - \alpha := \delta$. We can always generate ρ'_{AB} with CM $\mathbf{V}'_{AB}(\alpha, \beta, \gamma)$ by applying local Gaussian channels $\mathcal{I}_A \otimes \mathcal{G}_B$ to the symmetric Gaussian state ρ''_{AB} with CM $\mathbf{V}''_{AB} = \mathbf{V}'_{AB}(\alpha, \alpha, \gamma)$. It is sufficient to choose the identity channel $\mathcal{I}_A$ and a Gaussian channel $\mathcal{G}_B$ with additive noise δ (also known as canonical B2 form [4]). It is now trivial to check that the state ρ''_{AB} is separable. In fact, $\mathbf{V}''_{AB}$ is a *bona-fide* quantum CM when its parameters α and γ satisfy the conditions $\alpha \geq 1$ and $|\gamma| \leq \alpha - 1$. Then, one can check that the partially-transposed symplectic eigenvalues of $\mathbf{V}''_{AB}$ are greater than 1, i.e., the state is separable, when $|\gamma| \leq \sqrt{\alpha^2 - 1}$, which is a condition always satisfied. Now, since ρ''_{AB} is separable, then also ρ'_{AB} and ρ_{AB} must be separable (local operations cannot create entanglement).

[1] M. Horodecki, P. W. Shor, and M. B. Ruskai, Rev. Math. Phys **15**, 629-641 (2003).

[2] A. S. Holevo, Problems of Information Transmission **44**, 3-18 (2008).

[3] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[4] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[5] R. Werner, Phys. Rev. A **40**, 4277 (1989).

[6] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206–4216 (1999).

[7] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

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

[9] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, Rev. Mod. Phys. **84**, 1655-1707 (2012).

[10] M. Sacchi, Phys. Rev. A **72**, 014305 (2005).

[11] Ch. Spengler, M. Huber and B.C. Hiesmayr, J. Phys. A: Math. Theor. **43**, 385306 (2010).

[12] C. Dankert, *Efficient Simulation of Random Quantum States and Operators*, MSc thesis, University of Waterloo (2005). See also arXiv quant-ph/0512217.

[13] C. Dankert, R. Cleve, J. Emerson and E. Livine, Phys. Rev. A **80**, 012304 (2009).

[14] D. Gross, K. Audenaert, J. Eisert, J. Math. Phys. **48**, 052104 (2007).

[15] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. on Inf. Theory **48**, 580–599 (2002).

[16] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. thesis, CalTech (1997).

[17] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. on Inf. Theory **44**, 1369–1387 (1998).

[18] G. Chiribella, *Optimal Estimation of Quantum Signals in the Presence of Symmetry*, PhD thesis, Pavia (2006).

[19] B. Synak, K. Horodecki, and M. Horodecki, J. Math. Phys. **46**, 082107 (2005).

[20] S. Pirandola, A. Serafini, and S. Lloyd, Phys. Rev. A **79**, 052327 (2009).

[21] S. Pirandola, preprint arXiv:1210.2119.

[22] A. Peres, Phys. Rev. Lett. **77**, 1413–1415 (1996).

[23] M. Horodecki, P. Horodecki, R. Horodecki, Physics Letters A **223**, 1-8 (1996).

[24] Minor remark on matrix notation. We use ρ_{ijkl} when we refer to kets $|i, j\rangle$ and bras $\langle k, l|$. We prefer to use ρ_{ij}^{kl} when we distinguish between system A ($|i\rangle_A \langle j|$) and system B ($|k\rangle_B \langle l|$). Clearly, we have $\rho_{ijkl} = \rho_{ik}^{jl}$.