Secure continuous variable teleportation and Einstein-Podolsky-Rosen steering

Q. Y. He[1,2], L. Rosales-Zárate[2], G. Adesso[3] and M. D. Reid[2]
[1]*State Key Laboratory of Mesoscopic Physics, School of Physics, Peking University, Beijing 100871 China* *
[2]*Centre for Quantum and Optical Science, Swinburne University of Technology, Melbourne 3122 Australia*† and
[3]*School of Mathematical Sciences, University of Nottingham, Nottingham NG7 2RD, United Kingdom* ‡

We investigate the resources needed for secure teleportation of coherent states. We extend continuous variable teleportation to include quantum tele-amplification protocols, that allow non-unity classical gains and a pre-amplification or post-attenuation of the coherent state. We show that, for arbitrary Gaussian protocols and a significant class of Gaussian resources, two-way steering is required to achieve a teleportation fidelity beyond the no-cloning threshold. This provides an operational connection between Gaussian steerability and secure teleportation. We present practical recipes suggesting that heralded noiseless pre-amplification may enable high-fidelity heralded teleportation, using minimally entangled yet steerable resources.

arXiv:1410.1041v2 [quant-ph] 24 Aug 2015

Quantum teleportation (QT) is a process where Alice sends an unknown quantum state to Bob at a different location by communicating only classical information [1]. QT has inspired much interest, both as a fundamental challenge and as a tool for quantum information processing [2–8]. To achieve QT, Alice and Bob share an Einstein-Podolsky-Rosen (EPR) entangled state. Teleportation was first developed for the transfer of qubit states, and was extended to continuous variable (CV) spectra by Vaidman [3] and Braunstein and Kimble (BK) [4]. In the CV case, the entanglement shared between Alice and Bob is modeled after the original EPR paradox where Alice and Bob share systems with perfectly correlated positions and anti-correlated momenta [9–12]. Gaussian states (defined as having a Gaussian Wigner function) [13] can then be useful as approximations of EPR resources [5, 6].

What type of EPR entanglement is required for CV quantum teleportation [14]? CV teleportation of a coherent state originally focused on a subset of entangled resource states, where the entanglement can be certified by the Tan-Duan criterion which treats Alice and Bob symmetrically [15–17]:

$$\Delta_{ent} = \frac{1}{4}\{[\Delta(X_A - X_B)]^2 + [\Delta(P_A + P_B)]^2\} < 1. \quad (1)$$

Here X_A,X_B and P_A,P_B are the positions and momenta of Alice and Bob's systems and ΔX^2 denotes the variance of X [18]. Once one allowed for local operations at Alice and Bob's stations to optimise the protocol, it became clear that all two-mode Gaussian entangled states could be utilised for CV QT [19, 20] with fidelity F exceeding 1/2, which is the standard benchmark for input coherent states [21].

These results however do not resolve a second fundamental question, posed by Grosshans and Grangier (GG) [22]: What type of entangled state is required, if Bob is to be sure there can be no (non-degraded) copy of his transmitted (coherent) state in the hands of a second receiver, Eve? This form of entanglement becomes the vital resource for quantum information tasks where one needs *secure* teleportation (ST). An analysis based on optimal quantum cloning tells us that, for coherent inputs, ST is achieved once the fidelity F of CV teleportation exceeds 2/3 [22, 23].

Here we solve such a longstanding question by proving that secure CV teleportation requires a stronger form of entanglement exhibiting *EPR steering* [24–26]. EPR steering refers to the correlations of the original 1935 EPR paradox [9], where one observer appears to adjust ("steer") the state of the other by local measurements. A useful criterion to certify the EPR paradox and a steering of B by A in a bipartite state is [11, 27]

$$E_{B|A}(\mathbf{g}) = \Delta(X_B - g_x X_A)\Delta(P_B + g_p P_A) < 1. \quad (2)$$

Here $\mathbf{g} = (g_x, g_p)$ where g_x, g_p are real constants, usually chosen so that $E_{B|A}(\mathbf{g})$ is the minimum possible value, denoted $E_{B|A}$. Then, B is steerable by A if $E_{B|A} < 1$. This condition is necessary and sufficient for two-mode Gaussian states [24, 28], and a quantifier of Gaussian EPR steering can be defined as a decreasing function of $E_{B|A}$ [29]. Clearly, for steering, as in the original formulation of the EPR paradox, Alice and Bob are *not* equivalent: A system can be steerable in one way but not the other [29–33]. The role of steering in teleportation was first explored by GG, who noticed that, for the original BK protocol, resources displaying EPR paradox correlations are needed to achieve ST [22]. However, the generality of such a conclusion remained unclear.

Motivated by the recent progress in EPR steering characterization and quantification [24–36], we revisit CV teleportation by considering asymmetric Gaussian resources and the whole class of protocols including those allowing an arbitrary classical gain and local pre-amplification or post-attenuation of the coherent state. For a significant class of practical resources, simple arguments reveal that ST requires a one-way (A by B) steerable resource. This leads us to formulate and prove the generalisation of the GG result: Any Gaussian resource which is useful for high fidelity ST ($F > 2/3$) via

* qiongyihe@pku.edu.cn
† lrosaleszarate@swin.edu.au; mdreid@swin.edu.au
‡ gerardo.adesso@nottingham.ac.uk

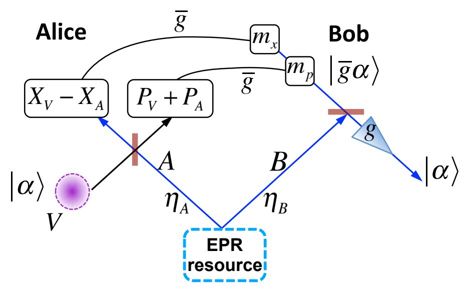

Figure 1. *Quantum tele-amplification.* A coherent state $|\alpha\rangle$ is teleported from Alice to Bob using EPR entanglement. The fidelity is optimised for a given resource by adjusting the classical gain $\bar{g}$. To teleport the original state, Bob may post-attenuate the state using $g = 1/\bar{g}$ or Alice may pre-amplify the coherent state.

an optimal protocol is necessarily two-way steerable. We further show how for particular protocols and resource states this condition becomes also sufficient.

We clarify the trade-off between required entanglement and achievable ST fidelity. While two-way steerability requires exceeding a threshold in entanglement, the latter becomes low for states of sufficient purity [29]. We propose that such states, if combined with a heralded noiseless pre-amplification of the coherent state [37], can nonetheless be useful for realising high fidelity ST. In this way, our work may contribute to the practical problem of how the fidelity of CV teleportation can be improved without increasing the entanglement (and hence energy requirements) of the EPR resource [38].

Quantum tele-amplification: We begin by considering the generalisation of the BK protocol [4], which incorporates arbitrary classical gains (Fig. 1). As with conventional CV teleportation, Alice and Bob share an EPR entangled state, often modeled by the two-mode squeezed state (TMSS) $|\psi\rangle = (1-x^2)^{1/2}\sum_{n=0}^{\infty} x^n|n\rangle_A|n\rangle_B$ [10, 11, 18]. Here $x = \tanh(r)$, where r is the squeezing parameter that determines the amount of entanglement shared between Alice and Bob; the limit of maximal EPR entanglement is reached as $r \to \infty$. Realistic conditions (e.g. losses) mean that the shared EPR resource is best described as a two-mode Gaussian state [13, 17, 19, 20, 27]. A field V (with amplitudes X_V and P_V) is prepared by a third party, Victor, in the coherent state $|\psi_{in}\rangle = |\alpha\rangle$ that is to be teleported to Bob. Alice performs a local Bell measurement of the combined quadratures $X_V - X_A$ and $P_V + P_A$, to give outcomes m_x and m_p respectively. The final stage of the teleportation is the displacement by Bob of the amplitudes of his EPR field by an amount given by Alice's readout values m_x, m_p, that are transmitted to him from Alice using classical communication.

While the BK protocol takes $\bar{g} = 1$, we allow for non-unity classical gain factors $\bar{g}_x$, $\bar{g}_p$ in the two classical channels. For simplicity, we consider equal gains, $\bar{g}_x = \bar{g}_p = \bar{g}$. This means that Bob's displacement is amplified/deamplified to $\bar{g}m_x$ and $\bar{g}m_p$. After feedback, Bob's field amplitudes are given by $X_B^f = \bar{g}X_V + (X_B - \bar{g}X_A)$, $P_B^f = \bar{g}P_V + (P_B + \bar{g}P_A)$.

Initially, we evaluate the fidelity for the protocol $|\alpha\rangle \to |\bar{g}\alpha\rangle$, called "quantum tele-amplification" when $\bar{g} > 1$ [30, 39]. Then, the desired teleported state is $|\beta_{tele}\rangle = |\bar{g}\alpha\rangle$. The fidelity, defined as $F = \langle\beta_{tele}|\rho_{out}|\beta_{tele}\rangle$ where ρ_{out} is the density operator of the output state at Bob's location, is calculated using standard techniques [4, 7, 40]. The result is $F = \frac{2}{\sigma_Q}\exp\left[-\frac{2}{\sigma_Q}\left|\beta_{out} - \beta_{tele}\right|^2\right]$ [7] where $\sigma_Q = \sqrt{(1+\sigma_X)(1+\sigma_P)}$ and $\beta_{out} = x_m + ip_m$. Here x_m, p_m and σ_X, σ_P are the means and variances of the quadratures X_B^f, P_B^f of Bob's output field. We find $\sigma_X = \bar{g}^2\sigma_{X,in} + [\Delta(X_B - \bar{g}X_A)]^2$, $\sigma_P = \bar{g}^2\sigma_{P,in} + [\Delta(P_B + \bar{g}P_A)]^2$, where $\sigma_{X/P,in}$ is the variance of $X/\ P$ for the input state ($|\alpha\rangle$) at Alice's station: We get ($\beta_{out} = \bar{g}\alpha$)

$$F = \frac{2}{\sigma_Q} = \frac{2}{1 + \bar{g}^2 + E_{B|A}(\bar{g})}\,, \tag{3}$$

where $E_{B|A}(\bar{g})$ is defined as the EPR steering parameter of Eq. (2) with $\mathbf{g} = (\bar{g}, \bar{g})$. We have restricted to two-mode Gaussian resources with equal position and momentum correlations [7], so that $|\langle X_A, X_B\rangle| = |\langle P_A, P_B\rangle|$, $\sigma_X = \sigma_P$ and $\Delta(X_B - \bar{g}X_A) = \Delta(P_B + \bar{g}P_A)$. This subclass, that we call $(X-P)$-balanced, includes EPR resources such as the TMSS with phase-insensitive losses and noise. The special BK case ($\bar{g} = 1$) reduces to $F^{BK} = \frac{1}{(1+\Delta_{ent})}$, where Δ_{ent} is the entanglement parameter of Eq. (1). More generally, we see that the fidelity in Eq. (3) is sensitive to the steering parameter.

Asymmetry and entanglement: It is known that Gaussian steerable states not satisfying the Tan-Duan entanglement condition $\Delta_{ent} < 1$ exist, and can be created for example from a two-mode squeezed state by adding asymmetric losses or thermal noise to each of the EPR channels (Fig. 2) [29, 30]. These asymmetric steerable states are *not* useful for standard BK quantum teleportation, which requires a fidelity of $F > 1/2$ and hence a resource with $\Delta_{ent} < 1$ [7].

The first point we make is that the generalisation to non-unity classical gains allows all the $(X-P)$-balanced Gaussian entangled states to be useful for QT [30]. We clarify as follows: The threshold fidelity where one can rule out all classical measure-and-prepare strategies as in Ref. [21] and hence claim QT is $F > \frac{1}{1+\bar{g}^2}$ (for $\bar{g} \geq 1$) [21, 41]. On examining (3), the condition on the resource to obtain QT reduces to:

$$Ent_{B|A}(\bar{g}) = \frac{\Delta(X_B - \bar{g}X_A)\Delta(P_B + \bar{g}P_A)}{(1+\bar{g}^2)} < 1. \tag{4}$$

The inequality $Ent_{B|A}(\bar{g}) < 1$, if satisfied, certifies entanglement between any two modes A and B ($\bar{g}$ is any real number) [42]. Further, the inequality $Ent_{B|A}(\bar{g}) < 1$ for an *optimally selected* $\bar{g} = g_{sym}^{B|A}$ that minimises $Ent_{B|A}(\bar{g})$ [30] is equivalent to Simon's positive partial transpose condition for entanglement [43], which is necessary and sufficient for two-mode Gaussian states. The parameter defined as $Ent \equiv Ent_{B|A}(g_{sym}^{B|A})$ is equal to the lowest

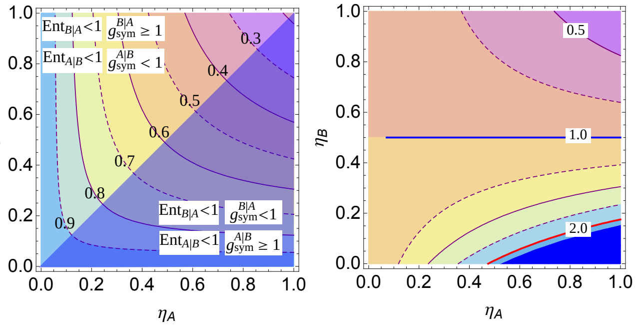

Figure 2. (Color online) *Steering for a two-mode squeezed state with lossy channels:* Here $r = 0.85$ and $\eta_{A/B}$ are the channel efficiencies. **Left:** Contour lines show the value of the entanglement parameter Ent. Higher loss on Alice's EPR channel ($\eta_A < \eta_B$) implies $g^{B|A}_{sym} > 1$ (note $g^{A|B}_{sym} = 1/g^{B|A}_{sym}$ and $\eta_A = \eta_B$ gives $g^{B|A}_{sym} = 1$). **Right:** Contour lines show the minimum value $E_{A|B}$ of $E_{A|B}(g)$, found by selecting $g = c/m$. EPR steering of Alice by Bob ($E_{A|B} < 1$) is possible only when $\eta_B > 1/2$.

symplectic eigenvalue of the partial transpose ν, which determines the logarithmic negativity a measure of entanglement [19, 20, 29, 44]. Maximum entanglement corresponds to $Ent \to 0$. Analysing the result Eq. (4), it is clear that for any Gaussian entangled resource (within the $(X-P)$-balanced class) with $g^{B|A}_{sym} \geq 1$, we can quantum teleport $|\alpha\rangle \to |\bar{g}\alpha\rangle$ (from Alice to Bob) using the classical gain set at $\bar{g} = g^{B|A}_{sym}$ [30]. When $g^{B|A}_{sym} < 1$, QT is obtained by switching the EPR channels A and B.

The value $g^{B|A}_{sym}$ quantifies the asymmetry of the resource and is calculated as $g^{B|A}_{sym} = x + \sqrt{x^2+1}$ where $x = (m-n)/2c$ and $n = \langle X_A, X_A\rangle$, $m = \langle X_B, X_B\rangle$, $c = \langle X_A, X_B\rangle = -\langle P_A, P_B\rangle$. The coefficients n, m, and c fully define the covariance matrix of Gaussian states in the $(X-P)$-balanced class. For a TMSS with losses at each channel A and B, so that η_A and η_B are the respective efficiencies, the covariances become $n = \eta_A \cosh(2r) + 1 - \eta_A$, $m = \eta_B \cosh(2r) + 1 - \eta_B$, $c = \sqrt{\eta_A \eta_B}\sinh(2r)$. The entanglement and steering parameters for this resource are given in Fig. 2. We next present a useful result that holds for all Gaussian or non-Gaussian states with covariance matrix of the $(X-P)$-balanced form.

Result (1): The amount of EPR entanglement is limited by the asymmetry parameter, according to $\nu \equiv Ent \geq (g^2_{sym} - 1)/(g^2_{sym} + 1)$, Hence, two-way steering (corresponding to $\{E_{A|B}, E_{B|A}\} < 1$) is certified if $Ent < 1/(1 + g^2_{sym})$. Two-way steerable states are constrained to be reasonably symmetric, so that $g_{sym} < \sqrt{2}$, and thus two-way steering is certified if

$$\nu \equiv Ent < 1/3. \qquad (5)$$

The condition is tight for $(X-P)$-balanced Gaussian states as shown in Fig. 3a, and it agrees with that derived in [29] in the case of arbitrary two-mode Gaussian states.

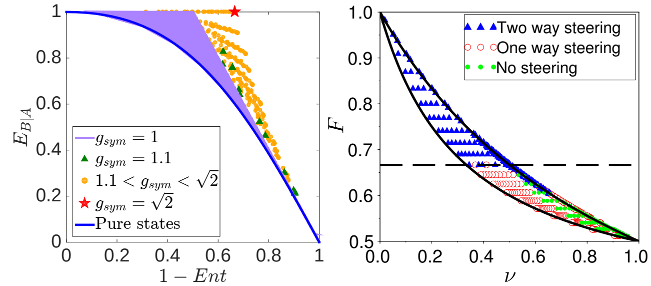

Figure 3. (Color online) *Gaussian steerability, entanglement, asymmetry, and teleportation fidelity.* **Left:** Gaussian steering of B by A occurs when $E_{B|A} < 1$ (maximum steering occurs as $E_{B|A} \to 0$). Entanglement occurs when $Ent < 1$ (maximum at $Ent \to 0$). Here we use $g^{B|A}_{sym} > 1$ for which $E_{A|B} \leq E_{B|A}$. The purple continuous region is for two-mode Gaussian symmetric states $g_{sym} = 1$, for which $Ent < 1/2$ implies two-way steerability. The orange points are for asymmetric Gaussian states, $g_{sym} > 1$. The entanglement condition $Ent < 1/3$ implies two-way steerability for all $(X-P)$-balanced states. **Right:** Optimal teleportation fidelity (using the BK, $lsatt$ or esa protocols, defined in the text) versus the entanglement parameter $\nu = Ent$ of the resource. Black-solid lines denote the MV bounds. Steering properties of lossy TMSS resources are plotted for all η_A, η_B and $r \geq 0.5$. Two-way steering is required for secure teleportation of coherent states, marked by $F > 2/3$.

The proofs are given in the Supplemental [45].

Steering and secure teleportation: We can now address the main question, namely what is the requirement on the resource to achieve no-cloning ST. Restricting to lossy TMSS states, we can see that a resource steerable A by B is required for ST. If there is no steering of A by B, the covariances imply that $\eta_B \leq 1/2$ (Fig. 2). Such a field B can be generated using a 50-50 beam splitter, that produces a second field B' satisfying $\langle X_A, X_{B'}\rangle = \langle X_A, X_B\rangle$, $\langle P_A, P_{B'}\rangle = \langle P_A, P_B\rangle$, etc. This implies that an observer Eve with access to B' can generate from the classical information (which is publicly accessible) the same teleported state as can Bob, who has access only to field B (see Fig. 1). This argument, while restricted to the lossy TMSS resource, is nonetheless quite powerful, applying to protocols with arbitrary $\bar{g}$ and local operations at Bob's station, and (similar to [36]) is not based on fidelity.

We now focus on the important case of conventional teleportation of the coherent state $|\alpha\rangle \to |\alpha\rangle$, but allowing for a broader set of Gaussian resources. Following GG, we consider *high fidelity* ST, where the no-cloning threshold for security is established by $F > 2/3$. GG revealed that for the BK protocol, $F > 2/3$ requires a resource with $\Delta_{ent} < 1/2$. We now know that this implies two-way steering of the resource [30]. Further, for symmetric resources, $g_{sym} = 1$ and $Ent \equiv \Delta_{ent}$, and we see from Result (1) and Fig. 3a that the GG condition $\Delta_{ent} < 1/2$ is the *tight* condition on the entanglement parameter $\nu = Ent$, for two-way steerability. This mo-

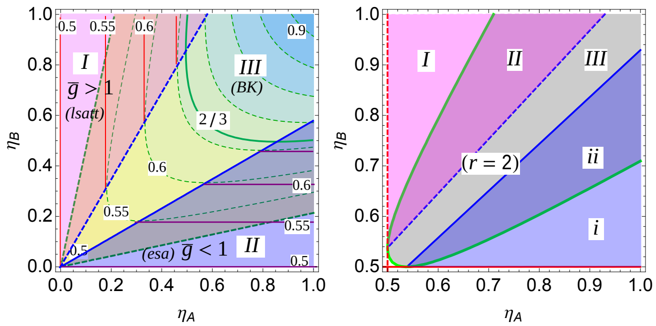

Figure 4. (Color online) *Optimising the fidelity for the teleportation $|\alpha\rangle \to |\alpha\rangle$ from Alice to Bob, using a resource with lossy channels.* **Left:** ($r = 1.0$): Contours show optimised fidelity values: We optimise via the lsatt protocol (region I), or via the esa (region II), or via the BK protocol (central coned region III). For higher $r > 0.89$, ST ($F > 2/3$) is possible using the asymmetric protocol. **Right:** ST can be achieved via the lsatt protocol (area $I+II$), or via the esa (area $i+ii$). The green curve corresponds to $\Delta_{ent} < 1/2$ so that regions II, III and ii give ST using the BK protocol. Note that for area III, ST can be only achieved by the BK. Regions I and i require asymmetric protocols for ST.

tivates us to generalise the GG result, to include asymmetric Gaussian resources and protocols.

To teleport an unknown coherent state with optimal fidelity for a given resource, local operations are needed at Alice and Bob's stations (Fig. 1). The full optimisation for all protocols is difficult, but Mari and Vitali (MV) optimised over all local Gaussian operations to derive fidelity bounds for a given entanglement value $\nu = Ent$, given by [20]

$$\frac{1+\nu}{1+3\nu} \leq F \leq \frac{1}{1+\nu}\,. \qquad (6)$$

The next result tells us that, once one allows asymmetric Gaussian protocols, the set of resources enabling ST is expanded on those satisfying the GG condition $\Delta_{ent} < 1/2$.

Result (2): All Gaussian entangled resources satisfying $\nu = Ent < 1/3$ are useful for ST of a coherent state. This entanglement threshold is the same tight entanglement threshold to certify two-way steering, Eq. (5), see Fig. 3b. For symmetric resources (where $g_{sym} = 1$) the condition weakens, and all entangled resources with $Ent < 1/2$ are useful for ST.

Proof: The MV bounds imply that for Gaussian states with $\nu = Ent < 1/3$, an optimal protocol exists that will give a fidelity $F > 2/3$. The subsequent statements follow from Result (1) and the GG condition.

We remark that two-way steerable Gaussian entangled states exist that satisfy $\nu = Ent < 1/3$ but do not satisfy the GG condition $\Delta_{ent} < 1/2$. For these states, the optimal protocol is not the BK one. It is hence useful to understand how the optimal protocols can be carried out in practice (Fig. 4). We present two simple protocols that are readily achievable experimentally and that together with the BK protocol allow, for any lossy TMSS resource, quantum teleportation with a fidelity spanning the whole range within the MV bounds, Eq. (6). In fact, our study shows that for any such entangled Gaussian resource with $Ent < 1/3$, high fidelity ST can be carried out using one of the three protocols that we call: lsatt, esa, or BK. The simplest is ***Late-stage attenuation (lsatt)***: To teleport the original state $|\alpha\rangle \to |\alpha\rangle$ when $\bar{g} > 1$, Bob locally attenuates his output field (Fig. 1). Bob may attenuate using a beam splitter which yields a new output variance of $\sigma_X = \eta\sigma_X^T + 1 - \eta$ where $\eta = 1/\bar{g}^2 = g^2 < 1$, and σ_X^T is the variance for the original output. Then from Eq. (3), the overall fidelity is $F_{A,B}^{lsatt}(g) = \frac{2}{3-g^2+E_{A|B}(g)}$ (using $\beta_{tele} = \alpha$). Standard QT with $F > 1/2$ requires a resource satisfying Eq. (4), as for quantum teleamplification. The fidelity is maximised for the choice of classical gain $\bar{g}_{opt} = (m-1)/c$, and the overall optimal fidelity becomes $F_{A,B}^{lsatt} = \frac{2}{3+n-c^2/(m-1)}$, provided $\bar{g}_{opt} > 1$ ($m > c+1$) (see Fig. 4).

Alternatively, Alice may choose to *amplify* the input coherent state at her station by a factor $g > 1$, prior to a teleportation protocol that uses a classical *attenuation* factor $\bar{g} = 1/g < 1$. We call this ***Early-stage amplification (esa)***. Suppose Alice uses at her station a TMSS amplifier [37]. Then the final amplified state at her station is given by a Gaussian state with mean $g\alpha$ and variance $\sigma_{X/P,in} = 2g^2 - 1$. The final Gaussian output after teleportation to Bob has variance $\sigma_X = \bar{g}^2\sigma_{X,in} + E_{B|A}(\bar{g})$. Substitution into Eq. (3) reveals the fidelity for the overall teleportation process to be $F_{A,B}^{esa}(\bar{g}) = F_{B,A}^{lsatt}(\bar{g})$. QT requires a resource satisfying the entanglement condition $Ent_{B|A}(\bar{g}) < 1$ with $\bar{g} < 1$. Hence, for an entangled Gaussian resource (in the $(X-P)$-balanced class) with $g_{sym}^{B|A} < 1$, the esa protocol with $\bar{g} = g_{sym}^{B|A}$ will give QT with $F > 1/2$. The overall fidelity $F_{A,B}^{esa}(\bar{g})$ is maximised for $\bar{g}_{opt} = c/(n-1)$ provided $\bar{g}_{opt} < 1$ ($n > c+1$), in which case the fidelity is given by $F_{A,B}^{esa} = F_{B,A}^{lsatt}$.

We finally give the connection with two-way steering. **Result (3):** From the MV bounds, in order to achieve $F > 2/3$, the entanglement of the resource must satisfy $Ent < 1/2$. Not all resources with $Ent < 1/2$ will allow $F > 2/3$. Restricting to the three protocols (lsatt, esa, BK), the requirement on the resource to achieve the no-cloning fidelity $F > 2/3$ is exactly for *two-way steering* (see Fig. 3b). The result is proved in the Supplemental Materials [45].

Discussion: We conclude by suggesting a further application of EPR steering to enhance the fidelity. The esa protocol relies on pre-amplification of a coherent state by a factor $g > 1$, which has a limited maximum fidelity of $1/g^2$. Recent methods propose heralding to overcome this limitation: heralded noiseless amplification of $|\alpha\rangle$ to $|g\alpha\rangle$ potentially allows fidelities approaching 1 [37]. The teleportation deamplification $|g\alpha\rangle \to |\alpha\rangle$ has fidelity $F = \frac{2}{1+\bar{g}^2+E_{B|A}(\bar{g})}$ given by Eq. (3) but where $\bar{g} = 1/g < 1$. We show in the Supplemental Material that for the TMSS resource with the optimal choice of

$\bar{g}$ ($\bar{g}_{opt} = \tanh(r)$), we get $F \to 1$. This is valid for all $r > 0$, henceforth it does not require significant entanglement of the teleportation resource. The overall fidelity becomes limited by the fidelity of the heralded amplification at Alice's site, suggesting a very promising experimental route for achieving high teleportation fidelities. We note however that there remains the requirement for EPR steerability of the resource, which for low entanglement requires resources of sufficient purity [29].

We thank the Australian Research Council for funding via Discovery and DECRA grants. QYH thanks the support of the National Natural Science Foundation of China under grants No.11274025, 61475006, and 11121091. MR thanks J. Pryde and M. Hall for discussions. GA acknowledges discussions with I. Kogias and thanks the European Research Council (ERC StG GQCOP Grant No. 637352) for financial support.

[1] C. H. Bennett *et al.,* Phys. Rev. Lett. **70**, 1895 (1993).
[2] D. Boumeester *et al.,* Nature (London) **390**, 575 (1997).
[3] L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
[4] S. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[5] A. Furusawa *et al.,* Science **282**, 706 (1998).
[6] W. P. Bowen *et al.,* Phys. Rev. A **67**, 032302 (2003).
[7] T. C. Zhang *et al.,* Phys. Rev. A **67**, 033802 (2003).
[8] H. Yonezawa, T. Aoki, and A. Furusawa, Nature (London) **431**, 430 (2004); N. Takei *et al.,* Phys. Rev. A **72** 042304 (2005); N. Takei *et al.,* Phys. Rev. Lett. **94**, 220502 (2005); M. Yukawa, H. Benichi, and A. Furusawa, Phys. Rev. A **77**, 022314 (2008).
[9] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[10] M. D. Reid and P. D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988).
[11] M. D. Reid, Phys. Rev. A **40**, 913 (1989).
[12] Z. Y. Ou *et al.,* Phys. Rev. Lett. **68**, 3663 (1992).
[13] C. Weedbrook *et al.*, Rev. Mod. Phys. **84**, 621 (2012). G. Adesso and F. Illuminati, J. Phys. A **40**, 7821 (2007).
[14] P. Badziag *et al.*, Phys. Rev. A **62**, 012311 (2000). S. Popescu, Phys. Rev. Lett. **72**, 797 (1994). F. Verstraete and H. Verschelde, Phys. Rev. Lett. **90**, 097901(2003).
[15] S. M. Tan, Phys. Rev. A **60,** 2752 (1999).
[16] L. M. Duan *et al.,* Phys. Rev. Lett. **84**, 2722 (2000).
[17] F. A. S. Barbosa *et al.,* Phys. Rev. A **84**, 052330 (2011). D. Buono *et al.,* Phys. Rev. A **86**, 042308 (2012).
[18] We consider two modes A and B, with boson annihilation operators a and b, and number eigenstates $|n\rangle_A$ and $|n\rangle_B$, respectively. Setting $\hbar = 2$, we define the quadratures as $X_A = a + a^\dagger$, $P_A = \left(a - a^\dagger\right)/i$, $X_B = b + b^\dagger$ and $P_B = \left(b - b^\dagger\right)/i$, and we use standard notation for the covariances $\langle X, Y\rangle = \langle XY\rangle - \langle X\rangle\langle Y\rangle$, with the variance $\langle X, X\rangle \equiv \Delta X^2 \equiv \sigma_X$ for the operator X.
[19] G. Adesso and F. Illuminati, Phys. Rev. Lett. **95**, 150503 (2005).
[20] A. Mari and D. Vitali, Phys. Rev. A **78**, 062340 (2008).
[21] K. Hammerer *et al.,* Phys. Rev. Lett. **94**, 150503 (2005).
[22] F. Grosshans and P. Grangier, Phys. Rev. A **64**, 010301(R) (2001).
[23] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).
[24] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007); S. J. Jones, H. M. Wiseman, and A. C. Doherty, Phys. Rev. A **76**, 052116 (2007). E. G. Cavalcanti *et al.,* Phys. Rev. A **80**, 032112 (2009).
[25] E. G. Cavalcanti, M. J. W. Hall, and H. M. Wiseman Phys. Rev. A **87**, 032306 (2013). P. Skrzypczyk, M. Navascués, and D. Cavalcanti, Phys. Rev. Lett. **112** 180404 (2014).
[26] D. J. Saunders *et al.*, Nature Phys. **6**, 845 (2010).
[27] M. D. Reid *et al.*, Rev. Mod. Phys. **81**, 1727 (2009).
[28] I. Kogias and G. Adesso, J. Opt. Soc. Am. B **32**, A27 (2015).
[29] I. Kogias, A. R. Lee, S. Ragy, and G. Adesso, Phys. Rev. Lett. **114**, 060403 (2015).
[30] Q. Y. He, Q. H. Gong, and M. D. Reid, Phys. Rev. Lett. **114**, 060402 (2015).
[31] S. L. W. Midgley, A. J. Ferris, and M. K. Olsen, Phys. Rev. A **81**, 022101 (2010); V. Händchen *et al.*, Nature Photon. **6**, 596 (2012); S. Walborn *et al.*, Phys. Rev. Lett. **106**, 130402 (2011); J. Schneeloch *et al.*, Phys. Rev. A **87**, 062103 (2013); J. Bowles *et al.*, Phys. Rev. Lett. **112**, 200402 (2014). Se-Wan Ji, M. S. Kim, and H. Nha, J. Phys. A **48**, 135301 (2015).
[32] B. Opanchuk, L. Arnaud, and M. D. Reid, Phys. Rev. A **89**, 062101 (2014).
[33] M. Piani and J. Watrous, Phys. Rev. Lett. **114**, 060404 (2015).
[34] P. Skrzypczyk, M. Navascues, and D. Cavalcanti, Phys. Rev. Lett. **112**, 180404 (2014).
[35] I. Kogias, P. Skrzypczyk, D. Cavalcanti, A. Acin, and G. Adesso, arXiv:1507.04164 (2015).
[36] T. C. Ralph and P. K. Lam, Phys. Rev. Lett. **81**, 5668 (1998). M. D. Reid, Phys. Rev. A **88**, 062338 (2013).
[37] T. C. Ralph and A. P. Lund, in Quantum Communication Measurement and Computing Proc. 9th Int. Conf. (ed. Lvovsky, A.) p155 (AIP, 2009); G. Xiang *et al.*, Nature Photon. **4**, 316 (2010); F. Ferreyrol *et al.*, Phys. Rev. Lett. **104**, 123603 (2010); M. Usuga *et al.*, Nature Phys. **6**, 767 (2010); A. Zavatta, J. Fiurasek, and M. Bellini, Nature Photon. **5,** 52 (2011).
[38] U. L. Andersen and T. C. Ralph, Phys. Rev. Lett. **111**, 050504 (2013).
[39] J. Neergaard-Nielson *et al.*, Nature Photon. **7**, 439 (2013).
[40] S. L. Braunstein, C. A. Fuchs, and H. J. Kimble, J. Mod. Opt. **47**, 267 (2000).
[41] G. Chiribella and J. Xie, Phys. Rev. Lett. **110**, 213602 (2013).
[42] V. Giovannetti *et al.*, Phys. Rev. A **67**, 022320 (2003).
[43] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[44] D. Buono *et al.*, J. Opt. Soc. Am. B **27**, A110 (2010); G. Adesso et al, Phys. Rev. A **70**, 022318 (2004); G. Adesso, A. Serafini, and F. Illuminati, Phys. Rev. A **73**, 032345 (2006).
[45] See Supplemental Materials.

Supplemental Material

Q. Y. He[2], L. Rosales-Zárate[1], G. Adesso[3] and M. D. Reid[1]
[1]*Centre for Quantum and Optical Science, Swinburne University of Technology, Melbourne 3122 Australia*
[2]*State Key Laboratory of Mesoscopic Physics, School of Physics, Peking University, Beijing 100871 China and*
[3]*School of Mathematical Sciences, University of Nottingham, Nottingham NG7 2RD, United Kingdom*

I. PROOFS

Result (1a): The amount of EPR entanglement is limited by the asymmetry parameter, according to $Ent \geq (g_{sym}^2-1)/(g_{sym}^2+1)$ where $g_{sym}=max(g_{sym}^{A|B},g_{sym}^{B|A})$.

Proof: Without loss of generality, we will assume $g_{sym}=g_{sym}^{B|A}=(m-n)/2c+\sqrt{[(m-n)/2c]^2+1}>1$, this implies that $m\geq n$. Next, $Ent_{B|A}=[m-2cg_{sym}^{B|A}+n(g_{sym}^{B|A})^2]/[1+(g_{sym}^{B|A})^2]$, using the definition of g_{sym}we can write $Ent_{B|A}$ and $(g_{sym}^2-1)/(g_{sym}^2+1)$ as:

$$Ent_{B|A} = \frac{1}{2}\left(m+n-\sqrt{\left(m-n\right)^2+4c^2}\right),$$

$$\frac{g_{sym}^2-1}{g_{sym}^2+1}=\frac{(m-n)}{\sqrt{\left(m-n\right)^2+4c^2}}.$$

We wish to prove that

$$\frac{1}{2}\left(m+n-\sqrt{\left(m-n\right)^2+4c^2}\right)=Ent_{B|A}\geq\frac{g_{sym}^2-1}{g_{sym}^2+1}=\frac{(m-n)}{\sqrt{\left(m-n\right)^2+4c^2}}.$$

Expanding this expression we notice that it is equivalent to prove that:

$$\left(m+n\right)^2c^2+\left(m-n\right)^2mn\geq\left(m-n\right)^2\left(1+m-n+2c^2\right)+2c^2\left(m-n+2c^2\right).$$

From the PPT condition $nm-c^2+1-n-m>0$, we know that $nm>c^2-1+n+m$, so we can write

$$\left(m+n\right)^2c^2+\left(m-n\right)^2mn \;\geq\; \left(m+n\right)^2c^2+\left(m-n\right)^2(c^2-1+n+m).$$

Next, we use that $-1+n+m\geq 1+m-n$, this inequality holds since we are considering $n\geq 1$. Hence we can write:

$$\begin{aligned}\left(m+n\right)^2c^2+\left(m-n\right)^2mn &\geq \left(m+n\right)^2c^2+\left(m-n\right)^2(c^2-1+n+m)\\ &\geq \left(m+n\right)^2c^2+\left(m-n\right)^2(c^2+1+m-n)\\ &\geq c^2\left[\left(m+n\right)^2+\left(m-n\right)^2\right]+\left(m-n\right)^2(+1+m-n).\end{aligned}$$

So that in order to prove that $Ent\geq(g_{sym}^2-1)/(g_{sym}^2+1)$ we need to prove that:

$$c^2\left[\left(m+n\right)^2+\left(m-n\right)^2\right]+\left(m-n\right)^2(1+m-n) \;\geq\; \left(m-n\right)^2\left(1+m-n+2c^2\right)+2c^2\left(m-n+2c^2\right).$$

Let us prove this by contradiction, hence we suppose that

$$c^2\left[\left(m+n\right)^2+\left(m-n\right)^2\right]+\left(m-n\right)^2(1+m-n)\leq\left(m-n\right)^2\left(1+m-n+2c^2\right)+2c^2\left(m-n+2c^2\right).$$

This implies that:

$$\begin{aligned}& c^2\left[\left(m+n\right)^2+\left(m-n\right)^2\right]+\left(m-n\right)^2(1+m-n)\leq\left(m-n\right)^2\left(1+m-n+2c^2\right)+2c^2\left(m-n+2c^2\right)\\ \iff\quad & c^2\left[\left(m+n\right)^2+\left(m-n\right)^2\right]\leq 2c^2\left(m-n\right)^2+2c^2\left(m-n+2c^2\right)\\ \iff\quad & \left(m+n\right)^2\leq\left(m-n\right)^2+2\left(m-n+2c^2\right)\\ \iff\quad & m^2+2mn+n^2\leq m^2-2mn+n^2+2m-2n+4c^2\\ \iff\quad & 4mn\leq 2m-2n+4c^2\\ \iff\quad & 2\left(mn-c^2\right)\leq m-n.\end{aligned}$$

But this is a contradiction since $2(nm - c^2) \geq m - n$, this is from PPT $nm - c^2 > -1 + n + m$, so that $2(nm - c^2) > -2 + 2n + 2m \geq 2m \geq m \geq m - n$ since $n - 1 \geq 0$. Therefore $Ent \geq (g_{sym}^2 - 1)/(g_{sym}^2 + 1)$ as required.

Proof for Gaussian case: Note that the Result (1a) is easily derived in the Gaussian case, since the fidelity of QAT is limited to $1/\bar{g}^2$ for any $\bar{g} \geq 1$. Hence, from the expression for the fidelity (Eq. (3)) given in the main paper, we see that $Ent_{B|A}(\bar{g}) \geq (\bar{g}^2 - 1)/(\bar{g}^2 + 1)$. Putting $\bar{g} = g_{sym}$, the result follows. The above proof is general for two-mode states.

Result (1b): Hence, two-way steering is certified if

$$Ent < 1/(1 + g_{sym}^2).$$

Two-way steerable states require a minimum symmetry, $g_{sym} < \sqrt{2}$ and thus, *two-way steering* is certified if

$$Ent < 1/3.$$

Proof: Let us suppose without loss of generality that $g_{sym} = g_{sym}^{B|A} \geq 1$, then $Ent = Ent_{B|A}(g_{sym})$. Steering of B by A is realised if $E_{B|A}(g_{sym}) < 1$ or equivalently $Ent = Ent_{B|A}(g_{sym}) < 1/(1 + g_{sym}^2)$. We note that if $E_{B|A}(g_{sym}) < 1$, then $E_{A|B}(1/g_{sym}) < 1/g_{sym}^2$ which for $g_{sym} \geq 1$ implies steering of A by B, and thus two-way steering. From Result (1), for $Ent < 1/(1+g_{sym}^2)$ to be possible, we need $1 \leq g_{sym} < \sqrt{2}$. If $g_{sym} = 1$, then $Ent < 0.5$ is sufficient for two-way steering. If $1 \leq g_{sym} < \sqrt{2}$ then $Ent < 1/3$ is sufficient for two-way steering. If $g_{sym} \geq \sqrt{2}$, then from Result (1), it is impossible to obtain $Ent < 1/3$. Thus $Ent < 1/3$ is a sufficient criterion for two-way steering, for any value of g_{sym}.

Result (3): From the MV bounds, in order to achieve $F > 2/3$, the entanglement of the resource must satisfy $Ent < 1/2$. Not all resources with $Ent < 1/2$ will allow $F > 2/3$. Restricting to the three protocols (lsatt, esa, BK), the requirement on the resource to achieve the no-cloning fidelity $F > 2/3$ is necessarily *two-way steerable.*

Proof: For the lsatt protocol, $F > 2/3$ leads to a steering condition $E_{A|B}(g) < g^2 < 1$. On dividing through by g^2, we see that this condition also implies steering of B by A i.e. $E_{B|A}(\bar{g}) < 1$, where $\bar{g} = 1/g$. The result for the esa protocol is similar. For the BK protocol $\bar{g} = 1$, the requirement $F > 2/3$ imposes the condition $\Delta_{ent} < 0.5$ derived by Grosshans and Grangier [1], and therefore using results proved in Ref. [2], also the condition that the resource be two-way steerable.

II. FIDELITY FOR QUANTUM TELE-AMPLIFICATION (QAT)

The strategy outlined in the main paper of selecting $\bar{g} = g_{sym}$ will optimise the fidelity of the amplified teleportation protocol *relative to* the quantum benchmark $1/(1 + \bar{g}^2)$ as given in the main paper. Immediately, we see that for all *symmetric* resources, the BK protocol is optimal in giving the maximum relative fidelity for the amplified teleportation scheme. For *asymmetric* resources however, the BK protocol is *not* optimal.

Figure 1 plots the relative fidelity F_g for the two-mode squeezed state (TMSS). In fact, the highly entangled TMSS cannot give QAT for high gains $\bar{g}$: the TMSS with lower r values is better for higher gain $\bar{g}$, as is the resource created by adding asymmetric loss.

We note that for all symmetric pure states, $g_{sym} = 1$ and the BK protocol gives the optimal relative fidelity. The TMSS is pure and symmetric and will enable quantum teleportation (QT) using the BK protocol, because there is symmetric entanglement that satisfies the Duan entanglement condition for all r. This is evident from Fig. 1. Interestingly, we see that the TMSS allows QT for gains up to $\coth(r/2)$ (three circles on the curves). It is interesting that at higher values of $\bar{g}$, QT is obtained by *reducing* the entanglement (decreasing the value of r) of the TMSS resource.

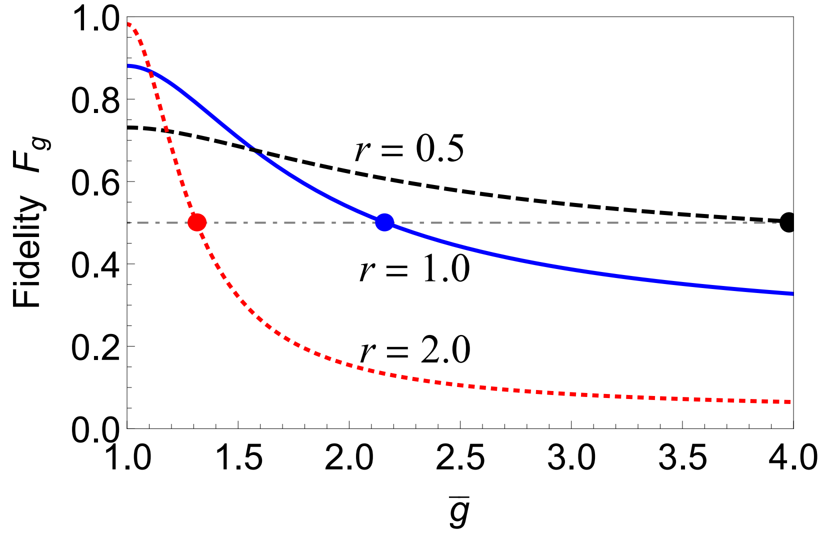

Figure 1: The fidelity $F_g \equiv \frac{F}{2/(1+\bar{g}^2)}$ for amplified teleportation $|\alpha\rangle \rightarrow |\bar{g}\alpha\rangle$ *relative to* the quantum benchmark, using a two-mode squeezed state resource. Here, $\bar{g}$ is the classical gain and r is the squeezing parameter that determines the amount of entanglement of the resource. QT is obtained for $F_g > 0.5$. We see that for quantum tele-amplification $\bar{g} > 1$, the fidelity is optimised at a lower entanglement (i.e. lower squeezing parameter r) value of the resource.

We now consider how to optimise for the maximum *absolute* fidelity $F \equiv F_{\bar{g}}^{amp}$ of the amplified teleportation QAT process: $|\alpha\rangle \rightarrow |\bar{g}\alpha\rangle$ (Alice to Bob), where $\bar{g} > 1$. Thus we ask what is the maximum *absolute* value of fidelity $F_{\bar{g}}^{amp} = 2/(1+\bar{g}^2+E_{B|A}(\bar{g}))$ (as given by Eq. (3) of the main text), for a given EPR resource. We need to minimise $1+\bar{g}^2+E_{B|A}(\bar{g})$ which leads to the condition $\bar{g} = \bar{g}_{opt}$ where

$$\bar{g}_{opt} = \frac{\langle X_A, X_B\rangle}{1+\langle X_A, X_A\rangle} \tag{1}$$

as the optimal gain, provided $\bar{g}_{opt} > 1$. In this case, the maximum fidelity is

$$F_{\bar{g}_{opt}}^{amp} = \frac{2(1+\langle X_A, X_A\rangle)}{(\langle X_B, X_B\rangle+1)(1+\langle X_A, X_A\rangle)-\langle X_A, X_B\rangle^2}. \tag{2}$$

For TMSS case, we have $\langle X_A, X_B\rangle/(1+\langle X_A, X_A\rangle) = \sinh(2r)/[1+\cosh(2r)] = 2\sinh(r)\cosh(r)/[2\cosh^2(r)] = \sinh(r)/\cosh(r) < 1$ because $n = \cosh(2r)$, $m = \cosh(2r)$, and $c = \sinh(2r)$. If the value $\bar{g}_{opt} \leq 1$, then the optimal gain is $\bar{g} = 1$, and the maximum fidelity for the TMSS is given by the BK protocol. We note that the maximum achievable fidelity for *any* amplifier process $|\alpha\rangle \rightarrow |\bar{g}\alpha\rangle$ is $1/\bar{g}^2$, as shown by the magenta curve in Fig. 2.

Since for the pure TMSS, we cannot select the optimal $\bar{g}_{opt}$ and the corresponding maximum fidelity given by Eq. (2). However, we plot the *absolute* fidelity $F_{\bar{g}}^{amp}$ versus the amplification gain $\bar{g} \geq 1$, in Fig. 2. We find as expected that the maximum absolute fidelity is for $\bar{g} = 1$, corresponding to the BK protocol.

III. THE FIDELITY FOR ATTENUATION AS PART OF A PREAMPLIFICATION PROTOCOL

We can then ask what is the maximum *absolute* value of fidelity possible for the process $|\alpha\rangle \rightarrow |\bar{g}\alpha\rangle$ shown by $F_{\bar{g}}^{amp} = 2/(1+\bar{g}^2+EPR_{B|A}(\bar{g}))$, where we consider attenuation $\bar{g} < 1$, for a given EPR resource. We need to minimise $1+\bar{g}^2+EPR_{B|A}(\bar{g})$ which leads to the condition $\bar{g} = \bar{g}_{opt}$ where

$$\bar{g}_{opt} = \frac{\langle X_A, X_B\rangle}{1+\langle X_A, X_A\rangle} \tag{3}$$

as being the optimal gain, provided $\bar{g}_{opt} < 1$. In this case, the maximum fidelity is

$$F_{\bar{g}_{opt}} = \frac{2(1+\langle X_A, X_A\rangle)}{(\langle X_B, X_B\rangle+1)(1+\langle X_A, X_A\rangle)-\langle X_A, X_B\rangle^2}. \tag{4}$$

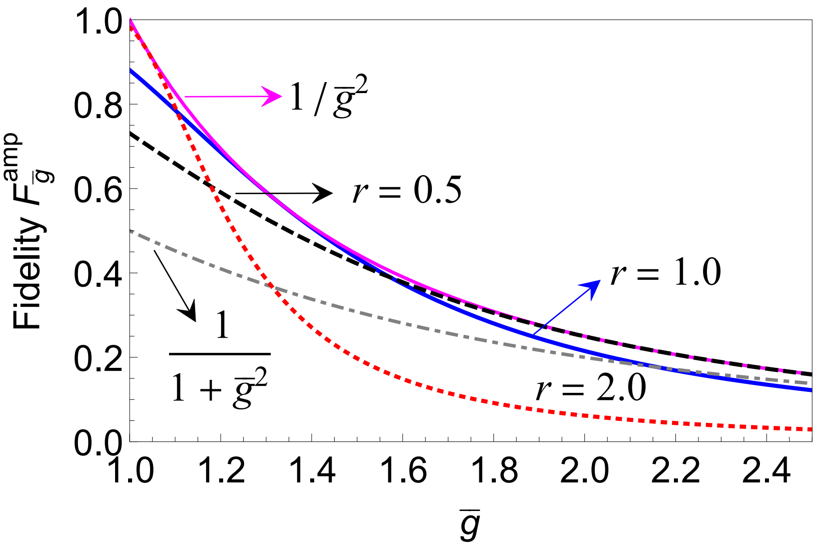

Figure 2: (Color online) The absolute fidelity for amplified teleportation $|\alpha\rangle \rightarrow |\bar{g}\alpha\rangle$ (Eq. (3) of main text) versus $\bar{g}$ using a two-mode squeezed state resource. Here, $\bar{g}$ is the classical gain and r is the squeezing parameter that determines the amount of entanglement of the resource. The threshold for QT is $F_{\bar{g}}^{amp} > \frac{1}{1+\bar{g}^2}$. Again, we see that for larger amplification $\bar{g}$ the fidelity is increased by decreasing the squeezing parameter r of the TMSS resource.

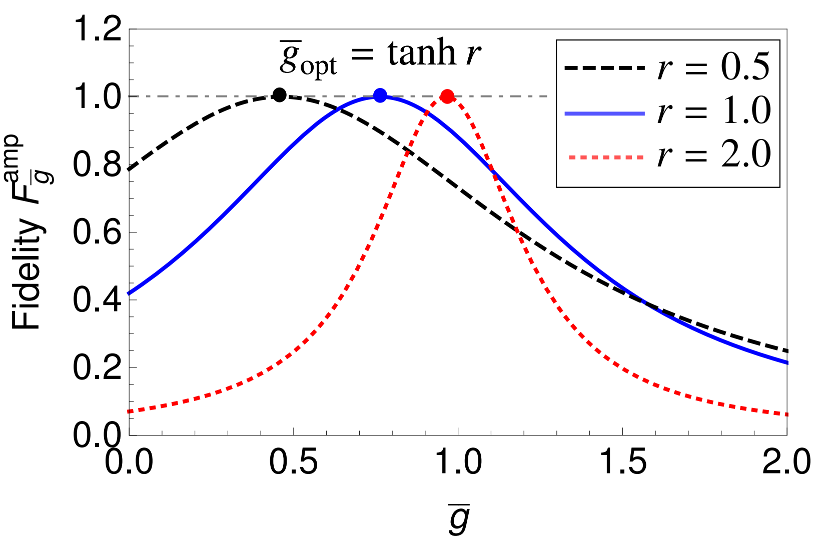

Figure 3: (Color online) The maximum *absolute* value of fidelity $F_{\bar{g}}$ possible for the attenuation teleportation process $|\alpha\rangle \rightarrow |\bar{g}\alpha\rangle$ where $\bar{g} < 1$ is $F_{\bar{g}_{opt}} = 1$ given by TMSS with the condition $\bar{g}_{opt} = \tanh(r)$.

For the TMSS, we have $\langle X_A, X_B\rangle/(1 + \langle X_A, X_A\rangle) = \sinh(2r)/[1 + \cosh(2r)] = 2\sinh(r)\cosh(r)/[2\cosh^2(r)] = \sinh(r)/\cosh(r) < 1$ because $n = \cosh(2r)$, and $m = \cosh(2r)$, $c = \sinh(2r)$. Therefore, the maximum fidelity is given by

$$F_{\bar{g}_{opt}} = \frac{2[1 + \cosh(2r)]}{[\cosh(2r) + 1]^2 - \sinh^2(2r)} = \frac{2[1 + \cosh(2r)]}{2[1 + \cosh(2r)]} = 1, \tag{5}$$

as shown by three circles on curves in Fig. 3.

Thus, to implement the strategy, one would want to preamplify $|\alpha\rangle \rightarrow |g\alpha\rangle$ ($g = 1/\bar{g} > 1$) using a heralded noiseless amplification technique. The following stage is the attenuation which gives maximum fidelity of one, for arbitrary r. Thus the fidelity will largely be determined by the fidelity of the heralded preamplification. This will be limited in practice by the g value (and the α value) given current experimental limitations. However, taking $g \sim 2$, we would need $\bar{g} = 0.5 = \tanh(r)$ which implies $r = 0.55$. This is a quite accessible squeezing parameter.

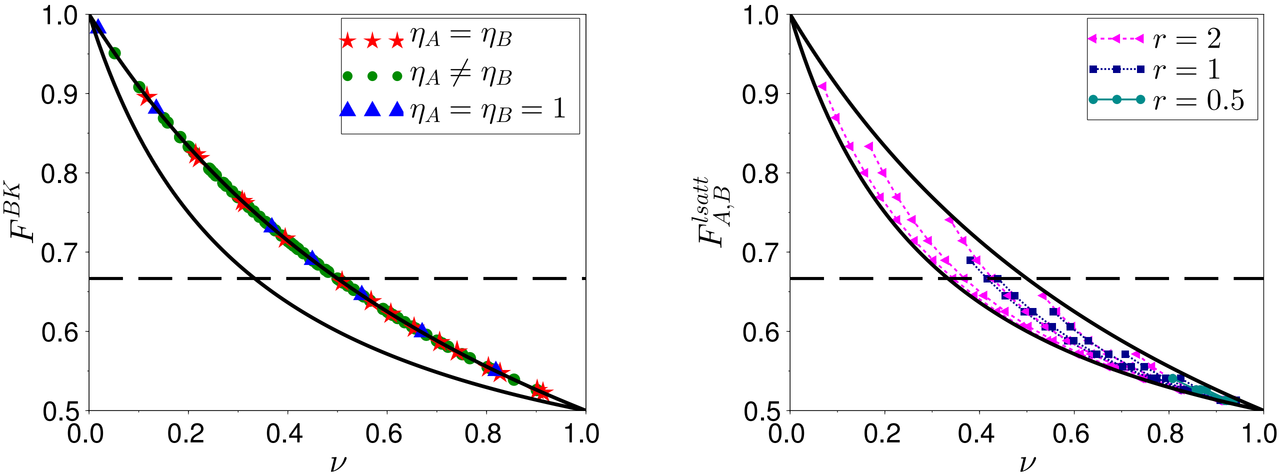

Figure 4: (Color online) Optimal teleportation fidelity versus entanglement ν of the resource. **Left:** with BK protocol, the blue triangles correspond to pure TMSS resource. Red stars correspond to mixed states with $\eta_A = \eta_B$, while green circles correspond to mixed states with $\eta_A \neq \eta_B$. Here we have used $r = 2$ and $r = 1$. Black-solid lines denote MV bounds. **Right:** with lsatt protocol, the curves with pink triangles, blue squares, and dark cyan points are asymmetric mixed states with $r = 2$, $r = 1$ and $r = 0.5$, respectively. The lines correspond to fixed values of r, we have used the following values of $\eta_A = 1,\ 0.9,\ 0.5,\ 0.3,\ ,0.1$ and $\eta_B = 0.1,\ 0.2,\ \ldots,\ 1$ respectively. Black-solid lines denote MV bounds.

IV. FIDELITY USING BK AND LSATT PROTOCOLS

It is useful to understand how the optimal protocols can be carried out. Figure 4 presents the optimal teleportation fidelity carried out with BK (left) and lsatt (right) protocols for TMSS resource with losses. Here we have considered the expressions for the fidelity for each protocol which are given in the main paper. These expressions are:

$$F^{BK} = \frac{1}{1+\Delta_{ent}},$$
$$F^{lsatt}_{A,B} = \frac{2}{3 - g_{opt}^2 + E_{A|B}(g_{opt})}.$$

Using BK protocol, secure teleportation ($F > 2/3$) is achievable when $\nu \equiv \Delta_{ent} < 0.5$ with symmetric and asymmetric resources. For both protocols, secure teleportation is harder to achieve when $r \to 0$. We require $r > 0.347$ for $\eta_A = \eta_B = 1$ to achieve ST for BK which is a lower bound than for lsatt (refer Fig. 4 of the main text). For both protocols the values of optimal fidelity lie in the MV bounds, indicated by the black solid lines.

[1] F. Grosshans and P. Grangier, Phys. Rev. A **64**, 010301(R) (2001).
[2] Q. Y. He, Q. H. Gong, and M. D. Reid, Phys. Rev. Lett. **114**, 060402 (2015).