Quantum steering as a resource for secure tripartite quantum state sharing

Cailean Wilkinson,[*] Matthew Thornton, and Natalia Korolkova
School of Physics and Astronomy, University of St Andrews, North Haugh, St Andrews KY16 9SS, United Kingdom

(Received 31 March 2023; accepted 17 May 2023; published 1 June 2023)

Quantum state sharing (QSS) is a protocol by which a (secret) quantum state may be securely split into shares, shared between multiple potentially-dishonest players, and reconstructed. Crucially, the players are each assumed to be dishonest, and so QSS requires that only a collaborating authorized subset of players can access the original secret state; any dishonest unauthorized conspiracy cannot reconstruct it. We analyze a QSS protocol involving three untrusted players and demonstrate that *quantum steering* is the required resource enabling the protocol to proceed securely. We analyze the level of steering required to share any single-mode Gaussian secret which enables the states to be shared with the optimal use of resources.

DOI: 10.1103/PhysRevA.107.062401

I. INTRODUCTION

Secret sharing is a cryptographic process which splits information between several players such that it is inaccessible to any individual player but can be accessed when players collaborate [1–3]. By requiring collaboration, secret sharing provides guaranteed security against small groups of dishonest actors. Secret-sharing schemes might be used, for example, by a bank manager to share the vault combination between their staff such that a number of them are required to access it.

Quantum state sharing (QSS) [4] translates this scheme to act on quantum secrets: the information describing a single quantum state (not known to the dealer) is shared between the modes of a larger multipartite system. Since no individual mode contains enough information to reconstruct the original state, only certain authorized subsets of players can access the original state through collaboration [5,6]. As in the classical case, quantum state sharing then provides security against small groups of dishonest parties.

This class of protocol aims at a variety of future uses in diverse quantum technology schemes. In secure distributed quantum computing, computations could be performed on each share individually without any single quantum computer having direct access to the underlying information [7]. The shares from different computers could then be recombined to produce the computation outcome. This form of so-called blind quantum computation allows untrusted quantum computers to be used securely without fear of data loss. Quantum state sharing may also find use in loss-tolerant quantum information distribution as a form of quantum error correction analogous to Reed-Solomon codes [8], potentially forming a crucial building block to a future quantum internet [9] or finding uses within a quantum computing stack [10].

The prototypical quantum-state-sharing scheme is (k, n)-threshold QSS, in which the secret state is split into n shares with a predefined threshold number of shares k required to reconstruct it. Any subset of shares meeting this threshold can then reconstruct the state. While this may initially present as a limited form of QSS, more complex schemes—in which a different number of shares is required depending on which shares are involved—can be built simply by distributing an uneven number of shares to each player. The primary restriction on this approach is common to any QSS scheme: to avoid breaking the no-cloning theorem a reconstruction is not possible with fewer than half of all shares. For illustration, in this paper we will consider the simplest nontrivial case: (2,3)-threshold QSS, in which any two of a total of three shares may reconstruct the original state.

Quantum state sharing was first formalized in the continuous-variable regime by Tyc and Sanders [11] with some possible implementations of (2,3)-threshold QSS utilizing two-mode squeezed-state resources later demonstrated and discussed by Lance *et al.* [12–14]. In this paper, we present a generalized version of Lance *et al.*'s protocol which allows for the use of *any generally asymmetric Gaussian resource state*. The previous protocol can be obtained as a special symmetric case of the one presented here. In contrast to previous works, we model the reconstruction process simply as a quantum channel, leaving the choice of physical implementation free. Finally, we also consider the use of this scheme for the sharing of *any* arbitrary single-mode Gaussian state, providing a complete image of tripartite Gaussian QSS.

For any quantum information task to be useful in a real-world setting, it must provide guaranteed security. For quantum state sharing, this means that the honest collaborating parties must be able to reconstruct a better copy of the original state than any adversaries in every case. With perfect entanglement, this protocol is secure for the sharing of any single-mode Gaussian state. However, increasing entanglement requires greater quantum resources and adds cost to the implementation. With the quantum technology era emerging, the thrifty and careful use of these quantum resources is becoming imperative. To that end, we analyze here the minimum required conditions under which a fully Gaussian (2,3)-threshold QSS can be considered secure and demonstrate that quantum steering is the resource required. In particular, we show that any two-mode state which is one way

[*] Corresponding author: cjw27@st-andrews.ac.uk

steerable can be used as a resource to securely share a coherent state, and we analyze the strength of steering required to share a general single-mode Gaussian state. In previous discussion of the security of continuous-variable QSS [12], the security was derived from the inclusion of classically-correlated Gaussian noise in the shares. While such noise can reduce the amount of information obtainable from a single share to an arbitrarily small degree, it leaves the protocol vulnerable to eavesdropping in the classical-noise-generation stage in a way that a fully quantum approach does not. In this paper, we consider only security derived from the no-cloning theorem, which can be further augmented by the inclusion of classical noise but is not reliant on it.

After briefly reviewing the entanglement properties of two-mode Gaussian states in Sec. II, we outline the details of the (2,3)-threshold quantum-state-sharing scheme under discussion in Secs. III and IV. We then discuss the security of the protocol for coherent states in Sec. V and for general single-mode Gaussian states in Sec. VI. Additional technical results may be found in the Supplemental Material [15].

II. GAUSSIAN RESOURCE STATES

We begin with a brief review of the properties of entangled two-mode Gaussian states, which form the resource for this protocol. At this stage, we first wish to clarify the sense in which we use the term "resource" in this paper. We depart from the formal definition used in resource theory [16] of a property that cannot be created at will by the participants using only local operations. Under that definition, this protocol would require no resource as the resource-state preparation could equivalently be absorbed into the protocol. Instead, we take a looser, more experiment-inspired definition of the resource as that property which enables the quantum advantage—and thus the resource state as that state which provides this property.

A Gaussian state is one whose Wigner function is Gaussian and, consequently, is fully characterized by its mean vector $\bar{\mathbf{r}} \in \mathbb{R}^{2n}$ and covariance matrix $\mathbf{V} \in \mathbb{R}^{2n\times 2n}$ [17]. We define elements of the covariance matrix as $\mathbf{V}_{i,j} = \langle\{\Delta^2\hat{X}_i\,;\,\Delta^2\hat{X}_j\}\rangle$, where $\{\cdots\}$ represents the anticommutator, $\Delta^2(\hat{O}) = \langle\hat{O}^2\rangle - \langle\hat{O}\rangle^2$ represents the variance of operator $\hat{O}$, and $\hat{X}^+ = (\hat{a}^\dagger + \hat{a})/\sqrt{2}$ and $\hat{X}^- = i(\hat{a}^\dagger - \hat{a})/\sqrt{2}$ represent the position $\hat{X}^+$ and the momentum $\hat{X}^-$ quadratures of each mode, respectively.

As we show in Sec. V, secure QSS requires a strict form of entanglement in which the measurement of one mode can affect the state of the second mode. This is known as Einstein-Podolsky-Rosen (EPR) steering [18,19]. The ability of one mode of a two-mode state to EPR steer the other is quantified through the steering parameter [20]

$$E_{1|2}(\mathbf{g}) = \Delta(\hat{X}_1^+ - g^+\hat{X}_2^+)\Delta(\hat{X}_1^- + g^-\hat{X}_2^-), \qquad (1)$$

where $\hat{X}_i^\pm$ represents the quadrature operators for each mode and $\Delta(\hat{O}) := \sqrt{\Delta^2(\hat{O})} = \sqrt{\langle\hat{O}^2\rangle - \langle\hat{O}\rangle^2}$ represents the square root of the variance of $\hat{O}$. Mode 2 can steer mode 1 whenever there exists a $\mathbf{g} = (g^+, g^-)^\mathrm{T} \in \mathbb{R}^2$ such that $E_{1|2}(\mathbf{g}) < 1$ with greater EPR steering as $E_{1|2} \to 0$. Notably, this quantity is directional, so a state may be steerable from mode 2 → 1 but not from 1 → 2. A state is said to be two-way steerable when it is steerable in both directions.

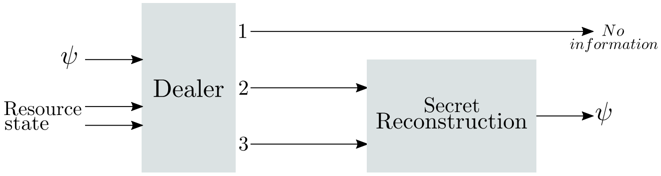

FIG. 1. Quantum-state-sharing schemes consist of two distinct subprotocols. In (2, 3)-threshold QSS, the secret state ψ is originally passed to a dealer who mixes it with an entangled resource state to produce three shares (dealer protocol), none of which contain a suitable amount of information about the secret state. Any two of these shares can then be recombined with a suitable reconstruction protocol to recover the original secret state.

The steering parameter measures the correlation between $\hat{X}_1^\pm$ and $g^\pm\hat{X}_2^\pm$, in which $g^\pm$ represents an effective scaling between the modes. Equivalently, $E_{1|2}(\mathbf{g})$ represents the extent to which the two resource modes cancel when mixed as

$$\hat{X}_1^+ - g^+\hat{X}_2^+, \quad \hat{X}_1^- + g^-\hat{X}_2^-, \qquad (2)$$

quantified by the smallness of the corresponding uncertainties.

For simplicity, we restrict our discussion to those resource states which exhibit equivalent entanglement properties in each quadrature, the $(X - P)$-balanced states. For such states, the steering parameter reduces to

$$E_{1|2}(g) = \Delta^2(\hat{X}_1^+ - g\hat{X}_2^+) = \Delta^2(\hat{X}_1^- + g\hat{X}_2^-) \qquad (3)$$

for $g^+ = g^- := g$. Although this condition is presented here for any $g \in \mathbb{R}$, it can be shown that steering is only possible for $g \in (0, \sqrt{2})$, and so it is this range that we will consider in this paper [21]. One common example of an $(X - P)$-balanced state is the two-mode squeezed vacuum state with squeezing ζ, which has steering parameter

$$E_{1|2}(g) = (1 + g^2)\cosh(2\zeta) - 2g\sinh(2\zeta). \qquad (4)$$

III. TRIPARTITE QUANTUM STATE SHARING

We now turn our attention to the specific QSS protocol we are interested in. Threshold quantum state sharing consists of two distinct stages: the *dealer protocol*, in which the single-mode secret is split into multiple shares, and the *reconstruction protocol*, in which a subset of these shares is recombined to reproduce the original secret state. Neither of these participants has any knowledge about the secret state. In (2,3)-threshold QSS, the dealer mixes the secret state with one mode of the two-mode resource state to produce an entangled system of three modes. Any two of these modes can then be used to reconstruct the original secret state, through a subprotocol which we denote $\{i, j\}$ *reconstruction* when modes i and j are used. An overview of the QSS protocol is shown in Fig. 1, and an illustration of the Wigner functions representing each stage of the process is shown in Fig. 2.

a. Dealer protocol. The dealer constructs the three shares by interfering the secret state on a balanced beam splitter

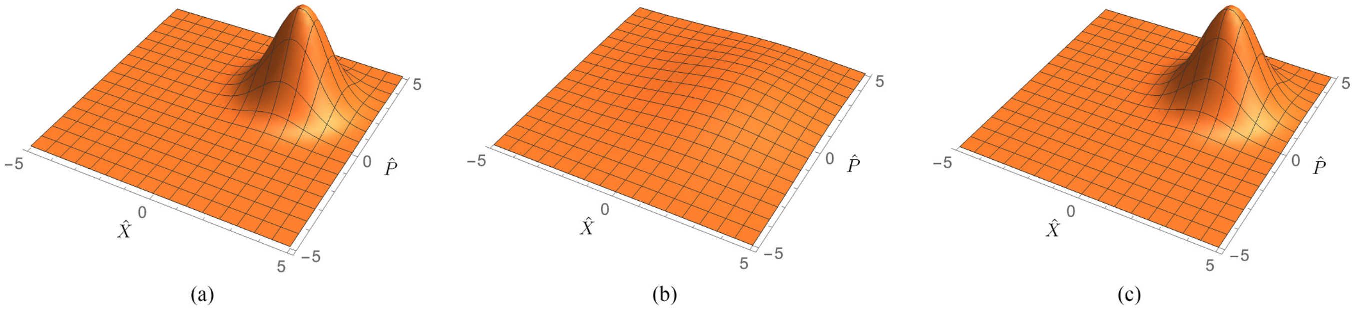

FIG. 2. Wigner functions at each stage of the QSS process: (a) input state, (b) intermediate distributed share, and (c) reconstructed output state. A single intermediate share does not contain enough information for a dishonest party to recover the original state. By combining any two shares, however, the original state can be reconstructed to a reasonable fidelity, as seen by comparing (c) to (a). This figure shows the sharing of a coherent-state secret with mean $\bar{\mathbf{r}} = (2, 2)^{\mathrm{T}}$ utilizing a two-mode squeezed vacuum resource state with 13-dB squeezing.

with one mode of the two-mode entangled resource. The three output states are then related to the input states by

$$\hat{X}_1^{\pm} = \frac{1}{\sqrt{2}}(\hat{X}_{\psi}^{\pm} + \hat{X}_{r1}^{\pm}), \tag{5}$$

$$\hat{X}_2^{\pm} = \frac{1}{\sqrt{2}}(\hat{X}_{\psi}^{\pm} - \hat{X}_{r1}^{\pm}), \tag{6}$$

$$\hat{X}_3^{\pm} = \hat{X}_{r2}^{\pm}, \tag{7}$$

where $\hat{X}_{\psi}^{\pm}$ are the quadrature operators representing the secret state and $\hat{X}_{ri}^{\pm}$ represents each mode of the resource state. Crucially, none of $\hat{X}_{1,2,3}^{\pm}$ individually contain enough information to accurately reconstruct the original state. As shown in Ref. [13], the information obtainable from each share could be further reduced with the addition of correlated classical noise without impacting the reconstructed state. Each of the three modes are distributed to a player as labeled.

b. {1,2} reconstruction. Players 1 and 2 may trivially reconstruct their state by passing each share through a second balanced beam splitter. This will effectively reverse the beam splitter used in the dealer protocol, reproducing the original separable system and leaving in one of the beam-splitter outputs the state

$$\hat{X}_{\mathrm{out}}^{\pm} = \frac{1}{\sqrt{2}}(\hat{X}_1^{\pm} + \hat{X}_2^{\pm}) = \hat{X}_{\psi}^{\pm}. \tag{8}$$

In the ideal case, with no transmission or component losses, $\hat{X}_{\psi}^{\pm}$ will be reconstructed perfectly regardless of the resource state used.

c. {1,3} and {2,3} reconstruction. Reconstructing the original state using share 3 requires a more complex disentanglement process to separate $\hat{X}_{\psi}^{\pm}$ from the resource state. We focus here on $\{1, 3\}$ reconstruction; the $\{2, 3\}$ case follows with only minor changes. Recalling from Eq. (3) that the resource state is entangled such that the modes cancel maximally when mixed with ratio $\hat{X}_{r1}^{\pm} \mp g\hat{X}_{r2}^{\pm}$ for some $g \in \mathbb{R}$, it becomes clear that in order to recover $\hat{X}_{\psi}^{\pm}$ we wish to implement the transformation

$$\begin{aligned}\hat{X}_{\mathrm{out}}^{\pm} &\to \eta[\hat{X}_{\psi}^{\pm} + (\hat{X}_{r1}^{\pm} \mp g\hat{X}_{r2}^{\pm})]\\ &= \eta(\sqrt{2}\hat{X}_1^{\pm} \mp g\hat{X}_3^{\pm}),\end{aligned} \tag{9}$$

where $\eta \in \mathbb{R}$ represents an amplification of the output state which is required to preserve the canonical commutation relations. The players can control g by adjusting the parameters of the reconstruction process (see the Supplemental Material for an example setup [15]), and so its value also acts as a unique label for a specific reconstruction setup.

This transformation produces a state with mean $\bar{\mathbf{r}} = \eta\bar{\mathbf{r}}_{\psi}$ and covariance matrix $\mathbf{V} = \eta^2\mathbf{V}_{\psi} + \eta^2 E_{1|2}(g)\mathbf{I}$: an amplified, generally noisy copy of the input state. We show in the Supplemental Material [15] that to preserve the canonical commutation relations, and thus satisfy the uncertainty theorem, this reconstruction must impose a gain of $\eta = 1/\sqrt{2 - g^2}$ on the secret state. Clearly, then, this reconstruction protocol amplifies the original state for all $g > 1$ and deamplifies it for all $g < 1$—the original state is reproduced with unity gain only for $g = 1$.

IV. UNITY-GAIN QUANTUM STATE SHARING

When the protocol is implemented for $g = 1$, the output state $\hat{\rho}_{\mathrm{out}}$ is reproduced with the same mean $\bar{\mathbf{r}}_{\psi}$ as the secret state and with covariance matrix $\mathbf{V}_{\mathrm{out}} = \mathbf{V}_{\psi} + E_{1|2}(g = 1)\mathbf{I}$. The accuracy of this reconstruction can be quantified by the fidelity $\mathcal{F} = \langle\psi|\hat{\rho}_{\mathrm{out}}|\psi\rangle$ between the original secret state ψ and the output state. When the output and input states have the same mean amplitude $\bar{\mathbf{r}}$, this fidelity can be expressed in terms of the covariance matrices as $\mathcal{F} = 2/\sqrt{\det(\mathbf{V}_{\psi} + \mathbf{V}_{\mathrm{out}})}$. The ideal fidelity for QSS implemented for $g = 1$ is then

$$\mathcal{F}_{g=1} = \frac{2}{2 + E_{1|2}(g = 1)}. \tag{10}$$

In general, for $g \neq 1$, the protocol as outlined in Sec. III will not reproduce the mean $\bar{\mathbf{r}}$ of the input state exactly. To correct for the change in $\bar{\mathbf{r}}$ introduced by the protocol and thus reconstruct the original state with unity gain, we augment it with an additional preamplification or postattenuation step. These are corrections similar to those introduced for quantum teleportation in Ref. [22], and so we also describe them as *late-stage-attenuation* (LSATT) and *early-stage-amplification* (ESA) QSS.

A. Late-stage attenuation

When the output state is an amplified copy of the input state (when $\eta > 1$, $g > 1$), the optimum correction is to attenuate the output state after the QSS reconstruction protocol. Modeling this attenuation as an ideal beam splitter with transmissivity $\tau = 1/\eta^2$ with a vacuum environment implements the transformation $\hat{X}^{\pm}_{\text{out}} \rightarrow \frac{1}{\eta}\hat{X}^{\pm}_{\text{out}} + \sqrt{1-\frac{1}{\eta^2}}\hat{X}^{\pm}_{\text{vac}}$. The corrected output state then has mean $\bar{\mathbf{r}}_{\text{out}} = \bar{\mathbf{r}}_{\text{in}}$ and covariance matrix $\mathbf{V}_{\text{out}} = \mathbf{V}_{\text{in}} + [E_{1|2}(g) + 1 - 1/\eta^2]\mathbf{I}$.

For the specific case of a coherent state secret with covariance matrix $\mathbf{V}_{\text{in}} = \mathbf{I}$, the secret state is reproduced with a fidelity of

$$\mathcal{F}_{\text{LSATT}} = \frac{2}{3 - 1/\eta^2 + E_{1|2}(g)}. \tag{11}$$

B. Early-stage amplification

When the output state is a deamplified copy of the input state (when $\eta < 1$, $g < 1$), the optimum correction is instead to amplify the input secret state prior to the dealer protocol. We model this process as an ideal amplifying channel; in practice such an amplification could be achieved by a phase-insensitive amplifier [17]. Denoting the original secret state by ψ, the amplified input to the QSS protocol can be written as $\hat{X}^{\pm}_{\text{in}} = \frac{1}{\eta}\hat{X}^{\pm}_{\psi} + \sqrt{\frac{1}{\eta^2} - 1}\hat{X}^{\pm}_{\text{vac}}$, where $1/\eta > 1$. Following the deamplifying QSS protocol, the output state will have mean $\bar{\mathbf{r}}_{\text{out}} = \eta\bar{\mathbf{r}}_{\text{in}} = \bar{\mathbf{r}}_{\psi}$ and covariance matrix $\mathbf{V}_{\text{out}} = \eta^2\mathbf{V}_{\text{in}} + \eta^2 E_{1|2}(g)\mathbf{I} = \mathbf{V}_{\psi} + [\eta^2 E_{1|2}(g) + 1 - \eta^2]\mathbf{I}$.

For a coherent-state secret, the secret state is reproduced with a fidelity of

$$\mathcal{F}_{\text{ESA}} = \frac{2}{3 - \eta^2 + \eta^2 E_{1|2}(g)}. \tag{12}$$

Of course, the introduction of an amplification stage prior to the dealer protocol would require a corresponding deamplification correction for {1, 2} reconstruction. However, since, under equal conditions, {1, 2} reconstruction will always have higher fidelity than {2, 3} or {1, 3} reconstruction, this would not affect our analysis of the security of the protocol.

V. SECURITY ANALYSIS FOR COHERENT-STATE QSS

For a quantum-state-sharing scheme to be considered secure it must be guaranteed that the collaborating parties obtain more information about the original secret than any adversary can. This security requirement can be certified through the uncertainty theorem, which imposes that only one copy of a single quantum state can exceed a fidelity of $\mathcal{F} = 2/3$, a condition termed the no-cloning limit [23]. Should the collaborators reconstruct the state with fidelity above this limit, it follows immediately that no other party can obtain as much information as them and so the protocol is secure. The optimal fidelity $\mathcal{F} = 2/3$ for duplication of a coherent state ($1 \rightarrow 2$ cloning) and its extension to $N \rightarrow M$ cloning has been studied in [24]. In this paper we assume any eavesdroppers are limited to Gaussian operations; it has been shown that with the use of non-Gaussian operations, coherent states can be cloned with fidelity up to $\mathcal{F} \approx 0.68$, and so loosening this assumption would slightly increase the following entanglement requirements [25].

To certify security for the whole protocol, each possible reconstruction ({1,2}, {1,3}, {2,3}) must individually be provably secure. Since the reconstruction fidelity obtained using shares 1 and 2 is strictly greater than any reconstruction involving share 3, it suffices to check the fidelity only for the latter case.

We have seen that whenever player 3 is involved, the general reconstruction fidelity for a given resource state, using the optimal unity-gain reconstruction protocols discussed in Sec. IV, is

$$\mathcal{F} = \begin{cases} 2/[3 - \eta^2 + \eta^2 E_{1|2}(g)] & g < 1 \quad (\eta < 1), \\ 2/[2 + E_{1|2}(g)] & g = 1 \quad (\eta = 1), \\ 2/[3 - 1/\eta^2 + E_{1|2}(g)] & 1 < g < \sqrt{2} \quad (\eta > 1), \end{cases} \tag{13}$$

where $\eta(g) = 1/\sqrt{2 - g^2}$ and $g \in (0, \sqrt{2})$ is chosen to maximize fidelity.

Comparing this reconstruction fidelity to the no-cloning limit, $\mathcal{F} > 2/3$, we reach our first result defining the entanglement requirements for secure QSS.

Result 1. A sufficient condition for a two-mode resource state to be useful for secure (2,3)-threshold QSS with a coherent-state secret is that a $g \in (0, \sqrt{2})$ exists such that the steering parameter satisfies

$$E_{1|2}(g) < \begin{cases} 1 & g \leqslant 1, \\ 2 - g^2 & g > 1. \end{cases} \tag{14}$$

Notably, while this result shows that any resource state exhibiting EPR steering for some $g \leqslant 1$ is useful for secure QSS, a greater magnitude of steering is required when the resource is steerable only for $g > 1$. This seeming asymmetry is due to where in the process the amplification correction is implemented. In LSATT QSS setups, the secret state is first mixed with the resource mode, with both amplified by the QSS scheme before being attenuated afterwards, leaving both secret and resource contributions with no net amplification. However, in ESA QSS setups, the amplification correction occurs *before* the secret is mixed with the resource, and so the resource contribution is deamplified by the QSS protocol without a corresponding amplification. The secret state is reproduced with unity gain while the resource contributions are attenuated, reducing their impact on the noise in the output state. Consequently, a higher fidelity can be achieved through ESA.

For a strict implementation of this protocol as described in Sec. III, the dealer has access to both resource modes and may choose which mode to mix with the secret state. This free choice of resource mode (i.e., a choice of relabeling modes $1 \leftrightarrow 2$) allows the dealer to decide in which direction this protocol utilizes the steering of the resource state, leading to a more general view on the requirements for secure QSS.

Result 2. All EPR-steerable states (one way and two way) are useful for the secure sharing of a coherent-state secret with a suitable dealer allocation of resource modes.

Proof. All resource states steerable from mode 2 to mode 1 for some $g \leqslant 1$ are useful for secure QSS from Result 1. Suppose instead the state is steerable only for $g > 1$: such a state is steerable in the opposite direction for $\bar{g} = 1/g < 1$. Hence, this state can be made useful for secure QSS simply by swapping the modes used in the dealer protocol. ■

This result requires the dealer to be able to arbitrarily swap resource modes, which we assume is possible in most implementations and discuss further in the Supplemental Material [15]. We note that when such swapping is not permitted,

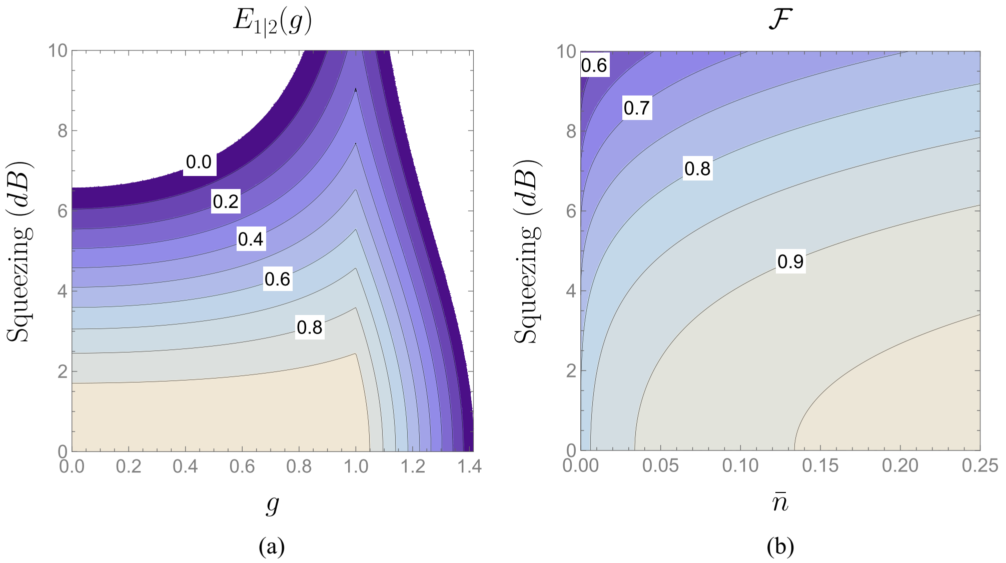

FIG. 3. (a) The minimum resource-state steering $E_{1|2}(g)$ that guarantees secure QSS for squeezed states. Lower values indicate greater steering, with $E_{1|2}(g) = 0$ representing perfect steering. Increasing the squeezing parameter increases the resource requirements for secure QSS. There is a clear preference for symmetric resource states, for which the optimal setup is at $g = 1$, with greater degrees of steering required to securely share the same squeezed states for asymmetric resources. (b) The fidelity achievable from a QSS setup using a symmetric resource state ($g = 1$) with steering parameter $E_{1|2}(g) = \frac{1}{2}$. Higher values indicate a more faithful reconstruction, with $\mathcal{F} = 1$ representing a perfect copy. Increasing squeezing in the secret state results in reduced reconstruction fidelity, while increasing the thermal photon number allows for a better reconstruction with the same resources.

Result 2 does not imply that any EPR-steerable state can be used for secure QSS. For example, if distributing one mode of the resource state prior to the other being used in the dealer protocol were desired, one would need to be careful in the choice of resource mode and of any asymmetric degradation of the shares during distribution.

The lower steering requirement when $g \leqslant 1$ also hints at another asymmetry: we show in the Supplemental Material [15] that whenever a resource state is steerable in one direction for some $g > 1$, it is always preferable to swap the modes and instead utilize steering in the opposite direction for $\bar{g} = 1/g$.

VI. SHARING OTHER GAUSSIAN SECRETS

The quantum-state-sharing scheme outlined above generalizes naturally to the sharing of any single-mode Gaussian state. In this section we explore the effectiveness of this protocol for some more general classes of Gaussian state: squeezed coherent states and squeezed thermal states.

A. Sharing arbitrary pure Gaussian states

A squeezed state is a Gaussian state in which the uncertainty in one quadrature has been reduced below the standard quantum limit at the expense of a corresponding increase in the other quadrature. These states have covariance matrix defined by the squeezing parameter ζ, $\mathbf{V} = \text{diag}(e^{-2\zeta}, e^{2\zeta})$. In general, this squeezing may be along any angle in phase space. As this protocol is phase independent, however, we may neglect the squeezing angle and thus assume for convenience that the states are squeezed along the $\hat{X}^+$ and $\hat{X}^-$ quadratures.

We consider in this section the use of our QSS protocol for the sharing of squeezed coherent states, the most general pure Gaussian state. We show in the Supplemental Material [15] that after QSS these states can be reconstructed with fidelity

$$\mathcal{F} = \frac{2}{\sqrt{(2e^{2\zeta} + \chi)(2e^{-2\zeta} + \chi)}}, \qquad (15)$$

where

$$\chi = \begin{cases} \eta^2 E_{1|2}(g) + 1 - \eta^2 & g \leqslant 1 \quad \text{(ESA)}, \\ E_{1|2}(g) + 1 - \frac{1}{\eta^2} & g \geqslant 1 \quad \text{(LSATT)} \end{cases} \qquad (16)$$

represents the g-dependent component introduced by the amplification correction. Increasing the squeezing ζ in the secret state reduces the achievable reconstruction fidelity. This fidelity for squeezed Gaussian states is shown along the $\bar{n} = 0$ axis in Fig. 3(b).

We now turn to the question of security. It is, in general, more difficult to clone states with an unknown squeezing than coherent states, with strategies optimal for cloning coherent states unable to achieve $\mathcal{F} = 2/3$ cloning fidelity when applied to states with unknown squeezing [26]. The optimal protocol for cloning squeezed states is not known, and so reaching the $\mathcal{F} > 2/3$ bound may not be necessary for security. However, the cloning fidelity for squeezed states remains upper bounded by $\mathcal{F} = 2/3$, and so this condition is still sufficient for security [27]. In the absence of an optimal protocol, here we use this upper bound as our threshold for guaranteed security.

From this fidelity threshold we can derive the following sufficient condition for the protocol's security.

Result 3. A QSS protocol for the sharing of a pure Gaussian secret state with squeezing of up to $\zeta_{\max}$ is secure if the resource state used has steering of

$$E_{1|2}(g) < \begin{cases} 1 - \frac{1}{\eta^2}\Gamma(\zeta_{\max}) & g \leqslant 1 \quad (\eta \leqslant 1), \\ \frac{1}{\eta^2} - \Gamma(\zeta_{\max}) & g \geqslant 1 \quad (\eta \geqslant 1), \end{cases} \tag{17}$$

for some $g \in (0, \sqrt{2})$, where $1/\eta^2 = 2 - g^2$ and

$$\Gamma(\zeta) = 1 + 2\cosh(2\zeta) - \sqrt{4\cosh^2(2\zeta) + 5} \geqslant 0 \tag{18}$$

is a monotonically increasing function of ζ with $\Gamma(0) = 0$.

This result is shown in Fig. 3(a). Comparing this condition to that for coherent states in Eq. (14), the effect of squeezing the secret state on QSS becomes apparent. Securely sharing a secret state with one quadrature squeezed below the vacuum limit requires a corresponding increase in entanglement above what is necessary for coherent states. The preference for symmetric resources, for which $g = 1$, remains, with less-entangled resources capable of securely sharing more squeezing when utilized symmetrically. Notably, the required extra steering tends to $\Gamma = 1$ as $\zeta \to \infty$, so even highly squeezed states and, in the limit, quadrature states can be shared securely with a suitably entangled resource state.

B. Sharing arbitrary mixed Gaussian states

Finally, we briefly discuss the potential use of this protocol for squeezed displaced thermal states: the most general possible single-mode Gaussian state. These thermal states have covariance matrix $\mathbf{V} = \tilde{n}\,\mathrm{diag}(\exp(-2\zeta), \exp(2\zeta))$, where $\tilde{n} = (2\bar{n} + 1)$ represents the average number of thermal photons $\bar{n}$ in the state prior to displacement and ζ again represents the degree to which the state is squeezed.

We show in the Supplemental Material [15] that the fidelity when sharing such states using a given resource state increases with increasing thermal photon number $\bar{n}$ and decreases with increasing squeezing ζ. As before, it does not depend on the mean amplitude $\bar{\mathbf{r}}$. Utilizing the appropriate amplification correction after the QSS stage, this protocol can achieve a reconstruction fidelity of

$$\mathcal{F} = \frac{2}{\sqrt{[\tilde{n}\chi + (\tilde{n}^2 + 1)e^{2\zeta}][\tilde{n}\chi + (\tilde{n}^2 + 1)e^{-2\zeta}]} - \sqrt{(\tilde{n}^2 - 1)[\tilde{n}^2 + \chi^2 + 2\tilde{n}\chi\cosh(2\zeta) - 1]}}, \tag{19}$$

where χ represents the impact of the amplification correction like before and is dependent on the value of g. This represents the most general measure of ideal reconstruction fidelity for the sharing of any single-mode Gaussian state. The impact of both squeezing and the average thermal photon number on the reconstruction fidelity is shown in Fig. 3(b).

Once one considers states with added thermal noise above the uncertainty limit, a greater cloning fidelity is achievable and so reaching the $\mathcal{F} > 2/3$ threshold is no longer sufficient for security. Consequently, we do not present a condition on the security of this scheme for thermal states. Some work has been done on the question of cloning thermal states [26,28], but optimality has not yet been shown for cloning fidelity. The use of this scheme for thermal states should then be carefully considered because security may not be guaranteed.

VII. CONCLUSION

We have shown here that the secure sharing of coherent states between three players is possible using a resource state exhibiting any form of EPR steering. Notably, this is a looser requirement than those for secure quantum teleportation, where a resource state must be two-way steerable to be useful [20]. Consequently, QSS could be considered a competitive alternative to quantum teleportation for secure state distribution when a set of communication channels can be trusted only collectively.

Going beyond coherent states, we have analyzed this QSS protocol for any single-mode Gaussian state, including squeezed states and thermal states. We have shown that while increased resource steering is required to share squeezed states, any pure single-mode Gaussian state is securely sharable with a suitably entangled resource state. Future work on this subject could involve a generalization to securely share the wider class of multimode Gaussian secret states. In such a case it will be of critical importance to preserve correlations between modes of the secret state. Additionally, the practical implementations of the analogous (k, n)-threshold QSS should be considered.

There is potential for QSS schemes to find uses in blind quantum computation [7] or as quantum Reed-Solomon codes for error correction [8]. By splitting the original state into shares and transmitting the shares separately, the original state can be reconstructed even if some of the shares lose fidelity in the transmission. Quantum error correction is an important subroutine both in quantum computing and in quantum state distribution. QSS schemes then may contribute to the practical implementation of a future quantum internet [9].

ACKNOWLEDGMENTS

This work has been supported by the Scottish Universities Physics Alliance (SUPA) and by the Engineering and Physical Sciences Research Council (EPSRC). C.W. acknowledges the funding from the Global Ph.D. program of the University of St. Andrews and Macquarie University. M.T. and N.K. were supported by the EU Flagship on Quantum Technologies, project PhoG (820365).

[1] A. Shamir, Commun. ACM **22**, 612 (1979).

[2] G. R. Blakley, in *1979 International Workshop on Managing Requirements Knowledge (MARK)* (IEEE, New York, 1979), pp. 313–318.

[3] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. (Wiley, New York, 1996).

[4] Quantum state sharing is distinct from quantum secret sharing, which uses quantum resources to securely share classical information [29].

[5] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[6] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[7] Y. Ouyang, S.-H. Tan, L. Zhao, and J. F. Fitzsimons, Phys. Rev. A **96**, 052333 (2017).

[8] M. Grassl, W. Geiselmann, and T. Beth, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, edited by M. Fossorier, H. Imai, S. Lin, and A. Poli, Lecture Notes in Computer Science (Springer, Berlin, 1999), Vol. 1719, pp. 231–244.

[9] S. Wehner, D. Elkouss, and R. Hanson, Science **362**, eaam9288 (2018).

[10] H. Ball, M. J. Biercuk, and M. R. Hush, Phys. Today **74**(3), 28 (2021).

[11] T. Tyc and B. C. Sanders, Phys. Rev. A **65**, 042310 (2002).

[12] A. M. Lance, T. Symul, W. P. Bowen, T. Tyc, B. C. Sanders, and P. K. Lam, New J. Phys. **5**, 4 (2003).

[13] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).

[14] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, T. Tyc, T. C. Ralph, and P. K. Lam, Phys. Rev. A **71**, 033814 (2005).

[15] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.107.062401 for technical derivations and proofs of the presented results, and additional discussion on the physical implementation of a quantum state sharing scheme.

[16] E. Chitambar and G. Gour, Rev. Mod. Phys. **91**, 025001 (2019).

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

[18] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[19] M. D. Reid, Phys. Rev. A **40**, 913 (1989).

[20] Q. Y. He, Q. H. Gong, and M. D. Reid, Phys. Rev. Lett. **114**, 060402 (2015).

[21] This can be seen by considering the channel resulting in $\hat{X}^{\pm}_{\text{out}} = 1/\sqrt{1-g^2}(\hat{X}^{\pm}_{r1} \mp g\hat{X}^{\pm}_{r2})$ for $g < 1$ and imposing the uncertainty limit on this output to get a condition for minimum $E_{1|2}(g) > 1 - g^2$. This can be converted to a condition on steering in the opposite direction for $\bar{g} = 1/g > 1$ of $E_{2|1}(\bar{g}) > \bar{g}^2 - 1$, so steering can be certified $[E_{1|2}(g) < 1]$ only for values of $g \in (0, \sqrt{2})$.

[22] Q. He, L. Rosales-Zárate, G. Adesso, and M. D. Reid, Phys. Rev. Lett. **115**, 180502 (2015).

[23] F. Grosshans and P. Grangier, Phys. Rev. A **64**, 010301(R) (2001).

[24] N. J. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301(R) (2000).

[25] N. J. Cerf, O. Krüger, P. Navez, R. F. Werner, and M. M. Wolf, Phys. Rev. Lett. **95**, 070501 (2005).

[26] S. Olivares, M. G. A. Paris, and U. L. Andersen, Phys. Rev. A **73**, 062330 (2006).

[27] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).

[28] M. Guţă and K. Matsumoto, Phys. Rev. A **74**, 032305 (2006).

[29] S. Richter, M. Thornton, I. Khan, H. Scott, K. Jaksch, U. Vogl, B. Stiller, G. Leuchs, C. Marquardt, and N. Korolkova, Phys. Rev. X **11**, 011038 (2021).